PingID Administration Guide

June 30, 2025

Table of Contents

PingID

PingID is a cloud-based, adaptive multi-factor authentication (MFA) solution that is part of PingOne for Workforce, a comprehensive cloud authentication authority.

The PingID documentation contains everything you need to know as an administrator and as an end user.

Release Notes

- General
- All

Get started with PingID (Admin)

- Introduction to PingID
- Overview of PingID authentication types
- PingID required domains, URLs, and ports
- The PingID dashboard
- Starting a PingOne trial

Use PingID (Admin)

- Configure the PingID service
- Configure PingID authentication
- PingID policy
- Add your branding to PingID
- PingID Offline MFA
- PingID User Life Cycle Management
- PingID Reporting

Integrations Use Cases (Admin)

- Integrate with PingID for PingFederate SSO
- Integrate with PingID for PingOne SSO
- Integrating PingID with your VPN/Remote access system
- Integrate PingID with SSH
- Integrating PingID with Windows login
- Integrating PingID with Windows login (passwordless)
- PingID integration for Mac login
- Integrate PingID with AD FS
- Integrate PingID with Azure AD
- Managing the PingID properties file

Use PingID (End User)

- Pairing your device with PingID
- PingID authentication for the web
- PingID authentication for VPN
- PingID authentication for Windows login
- PingID authentication for Mac login
- Managing your devices
- Transferring PingID mobile app authentication to a different device
- PingID mobile app management
- PingID desktop app management
- A lost or stolen device situation

Learn More

- PingID API documentation
- PingID Community
- PingID Support
- PingID Training (existing customers only)

Release Notes

Review release notes for features and improvements in PingID.

The PingID general release notes summarize the changes in current and previous product updates.

PingID general release notes

Subscribe for automatic updates: PingID general release notes RSS Feed

New features and improvements in PingID

June 2025

New features and improvements in PingID implemented in June 2025.

June 30

New version of PingID mobile app for Android - 3.3.2

New PingID mobile app

Learn more in Mobile app 3.3.2 (June 30, 2025) Android

June 29

New version of PingID mobile app 3.3.0

New PingID mobile app

- For iOS changes, learn more at Mobile app 3.3.0 (June 29, 2025) iOS
- For Android changes, learn more in Mobile app 3.3.1 (June 29, 2025) Android

June 10

New version of PingID integration for Windows login (version 2.12)

New PingID Integration for Windows login

Learn more at PingID integration for Windows login 2.12 (June 10, 2025).

June 3

New version of PingID integration for Windows login - passwordless (version 1.7)

New PingID Integration for Windows login

For details, see PingID integration for Windows login (passwordless) 1.7 (June 3, 2025).

May 2025

New features and improvements in PingID implemented in May 2025.

May 8

New version of PingID integration for Mac login (version 1.3.4)

New PingID Integration for Mac login

For details, see PingID integration for Mac login 1.3.4 (May 8, 2025).

April 2025

New features and improvements in PingID implemented in April 2025.

April 3

New version of PingID mobile app 3.2.0

New PingID mobile app

- For iOS changes, learn more in Mobile app 3.2.0 (April 3, 2025) iOS
- For Android changes, learn more in Mobile app 3.2.0 (April 3, 2025) Android

March 2025

New features and improvements in PingID implemented in March 2025.

March 27

Format of phone numbers in Mexico

Info PingID

The format of Mexican phone numbers that was used prior to August 2019 (adding "1" before the area code) is no longer supported.

March 10

New version of PingID mobile app 3.1.0

New PingID mobile app

- For iOS changes, learn more in Mobile app 3.1.0 (March 10, 2025) iOS
- For Android changes, learn more in Mobile app 3.1.0 (March 10, 2025) Android

February 2025

New features and improvements in PingID implemented in February 2025.

February 27

New version of PingID Integration Kit 2.28.

New PingID Integration kit for PingFederate

A new version of PingID Integration Kit 2.28 is released with a new version of PingID RADIUS PCV 3.1.0, and a new version of PingID adapter 2.16.

Learn more in PingID Integration Kit 2.28 (February 27, 2025)

February 16

New version of PingID mobile app 3.0.1 (Android only)

New PingID mobile app

Learn more in Mobile app 3.0.1 (February 16, 2025) Android

January 2025

New features and improvements in PingID implemented in January 2025.

January 28

New version of PingID mobile app 3.0

New PingID mobile app

- For iOS changes, learn more in Mobile app 3.0 (January 28, 2025) iOS
- For Android changes, learn more in Mobile app 3.0 (January 28, 2025) Android

January 23

New version of PingID desktop app 1.8.0

New PingID desktop app

For details see Desktop app 1.8.0 (January 23, 2025).

January 7

Added informative instructions to Timed Out message for users with no paired FIDO devices

Improved PingID

We've added instructions to the Timed Out message to help users who attempt to sign on when they don't have a FIDO2 biometrics device paired with their account. The Timed Out message now informs them that to authenticate, they must register a FIDO device and respond to authentication requests within 15 seconds.

Added ability to authenticate with backup device directly from authentication Error and Time Out screens

Improved PingID

We've added a link on the authentication **Error** and **Time Out** screens that enables users who don't have their paired device to authenticate with their backup device directly from those screens. This option appears only if they have a backup device configured for their account.

Added explanation for what to do if all user devices are blocked and user is unable to authenticate

Improved PingID

If all of a user's paired devices are blocked, there's now a message informing the user that they must contact their organization's administrator to unblock their device.

December 2024

New features and improvements in PingID implemented in December 2024.

December 16

Additional fields added to the PingID subscriptions report

Improved PingID

To help admins identify transactions in PingID that correlate with transactions in PingFederate, we've added the following fields to the PingID subscriptions report:

- `externaltransactionid`
- `externalsessionid`

November 2024

New features and improvements in PingID implemented in November 2024.

November 21

New version of PingID Mobile app 2.7.0

New PingID mobile app

iOS changes

Android changes.

November 20

Authentication stalls with Safari on iOS 18 and later

Fixed STAGING-24864 PingID

On mobile devices running iOS 18.0 or later, if the authentication process started in Safari and the user then left the browser to carry out MFA, there were cases where the authentication appeared to have stalled when the user returned to the browser. This issue has been fixed.

November 10

PPM expiry period reduced to 15 minutes

Info PingID

On November 3rd 2024, the grace period for expired PPM requests was reduced to 15 minutes. The grace period will be further reduced in the future.

October 2024

New features and improvements in PingID implemented in October 2024.

October 27

New version of PingID Mobile app 2.6.0

New PingID mobile app

For iOS changes, see Mobile app 2.6.0 (October 27, 2024) iOS.

For Android changes, see Mobile app 2.6.0 (October 27, 2024) Android.

September 2024

New features and improvements in PingID implemented in September 2024.

September 29

PPM expiry validation fix

Info STAGING-24153 PingID We've fixed a security vulnerability where, under certain conditions, the PPM Request validity period was extended.

To minimize interruption to existing clients, there will be a 30-minute grace period for expired PPM requests, until November 1st, when the grace period will be reduced to 15 minutes.

September 2

PingID API - error message for edituser

Info STAGING-21611 PingID

For PingID environments that have been integrated into PingOne, you cannot use the `edituser` endpoint from the PingID API to modify user details. The error message that is returned in such situations has been improved to clearly indicate why the action cannot be carried out.

August 2024

New features and improvements in PingID implemented in August 2024.

August 26

Adding grace period when requiring users to upgrade to new version of PingID

Fixed STAGING-22791 PingID

When enabling version update notifications, we've added a 7-day grace period during which users are not notified of the requirement to upgrade to the latest version of PingID mobile app. This is to provide enough time for the new version to be added to the relevant app stores before users are notified of the requirement to upgrade to the latest version.

August 5

Improved FIDO2 (passkey) authentication when using Safari Browser

Improved PingID

We've improved the authentication experience for users authenticating with a Passkey device through a Safari browser. It is no longer necessary to trigger the authentication flow by clicking a **Continue** button. The flow is now triggered automatically. Learn more in Configuring FIDO2 authentication for PingID.

Organization token subscription information included in PingID audit events

Improved PingID

The organization token field is now included in the PingID audit event information that is reported through the PingOne subscription facility.

> **Note**
>
> - This field is only available when integrating with PingFederate.
> - This field is not available for PingID Mobile app or PingID desktop app pairing events.

August 4

PingID browser cookie update - Google Chrome

Info PingID

In light of the announcement from Google that they are not continuing with their planned rollout of the Privacy Sandbox, PingID will stop using CHIPS (Cookies Having Independent Partitioned State) cookies for customers who have enabled support for iFrames via customer support. The use of cookies has thus been restored to the approach used prior to the change made in February 2024, described here.

August 1

New version of PingID Mobile app 2.5.0

For iOS changes, see Mobile app 2.5.0 (August 1, 2024) iOS.

For Android changes, see Mobile app 2.5.0 (August 1, 2024) Android.

June 2024

New features and improvements in PingID implemented in June 2024.

June 25

New version of PingID Integration Kit 2.27.

New PingID Integration kit for PingFederate

A new version of PingID Integration Kit 2.27 is released with a new version of PingID Adapter 2.15.0. For more information, see PingID Integration Kit 2.27 (June 25, 2024).

June 20

New version of PingID integration for Windows login - passwordless (version 1.6.1)

For details, see PingID integration for Windows login (passwordless) 1.6.1 (Jun 20, 2024).

June 18

New version of PingID Mobile app 2.4.0

For iOS changes, see Mobile app 2.4.0 (June 18, 2024) iOS.

For Android changes, see Mobile app 2.4.0 (June 18, 2024) Android.

June 9

New version of PingID Mobile app 2.3.0

For iOS changes, see Mobile app 2.3.0 (June 9, 2024) iOS.

For Android changes, see Mobile app 2.3.0 (June 9, 2024) Android.

PingID general release notes (older releases)

New features and improvements in PingID implemented prior to 2024.

May 2024

New features and improvements in PingID implemented in May 2024.

May 30

New version of PingID integration for SSH (version 4.3.0)

New PingID SSH integration

For details, see PingID SSH Integration 4.3.0 (May 30, 2024).

May 28

New version of PingID integration for Windows login - passwordless (version 1.6)

New PingID Integration for Windows login

For details, see PingID integration for Windows login (passwordless) 1.6 (May 28, 2024).

May 27

Aggregate passkey devices per user during authentication

New PingID

We've added the ability to aggregate all FIDO2 devices associated with a user's account during authentication. This simplifies authentication, as the user is presented with a single FIDO2 authentication method representing all of their paired FIDO2 devices, rather than seeing each device listed separately. If the user chooses to authenticate with the aggregated FIDO2 authentication method, the OS of the accessing device selects the most appropriate method for them to use to authenticate.

Learn more at Creating a FIDO policy in the PingOne Cloud Platform documentation.

May 5

New version of PingID Mobile app 2.2.0

New PingID mobile app

For iOS changes, see Mobile app 2.2.0 (May 5, 2024) iOS.

For Android changes, see Mobile app 2.2.0 (May 5, 2024) Android.

April 2024

New features and improvements in PingID implemented in April 2024.

April 18

Integration of a PingID account with PingOne - support for FIDO2 authentication method

If you have a PingID account that has been integrated with PingOne, you can now update it to support the FIDO2 authentication method. This allows you to benefit from the full range of options in the enhanced FIDO2 policy.

This feature is not yet supported for DaVinci productized flows.

Learn more: see Updating a PingID account to use PingOne FIDO2 policy for Passkey support and Configuring FIDO2 authentication for PingID.

April 2

New version of PingID Mobile app 2.1.0

New PingID mobile app

For iOS changes, see Mobile app 2.1.0 (April 2, 2024) iOS.

For Android changes, see Mobile app 2.1.0 (April 2, 2024) Android.

March 2024

New features and improvements in PingID implemented in March 2024.

March 26

Notification limit enforcement for number-matching failures

Fixed STAGING-22312

Failed number-matching attempts are now counted toward the push notification limit defined in the Limit Push Notification rule.

March 19

New version of PingID integration for Mac login (version 1.3.3)

New PingID Integration for Mac login

For details, see PingID integration for Mac login 1.3.3 (March 19, 2024).

March 4

New version of PingID mobile app for iOS (2.0.1)

Fixed PIM-6433 PingID mobile app

We've released an important fix for PingID mobile app iOS users. For details, For details, see iOS

March 3

Brand new version of PingID mobile app 2.0

New PingID mobile app

We've totally revamped the PingID mobile app to bring you a more secure, user-friendly, and feature-rich version. We've also added PingOne Verification capabilities to the app. For details, see:

- iOS
- Android

February 2024

New features and improvements in PingID implemented in February 2024.

February 21

New version of PingID integration for Windows login (version 2.11)

New PingID Integration for Windows login

For details, see PingID integration for Windows login 2.11 (February 21, 2024).

Allow users to manage their devices

New PingID

The **Client Integration** page in the admin portal now includes an option called **Enable Device Management** for both the integration with Windows login and the integration with Mac login. If you select this option, users can manage their devices from their **Devices** page, and they can also register their device the first time they try to access a resource that requires authentication ("on-the-fly registration"). See Windows and Mac login.

February 6

New version of PingID integration for Windows login - passwordless (version 1.5.1)

New PingID Integration for Windows login

For details, see PingID integration for Windows login (passwordless) 1.5.1 (February 6, 2024).

February 5

PingID browser cookie update for Google Chrome

Improved PingID

To comply with changes to Google Chrome's use of third-party cookies, we've implemented CHIPS (Cookies Having Independent Partitioned State) functionality in PingID browser cookies.

- SameSite cookie attribute support: Partitioned cookies are applied for customers that enable support for PingID to run in iframes, also known as SameSite cookies support.
- iframe support: iframe support cannot be enabled from the admin console. To enable iframe support in PingID, contact your customer support representative.

January 2024

New features and improvements in PingID implemented in January 2024.

January 17

New version of PingID integration for Mac login (version 1.3.2)

New PingID Integration for Mac login

For details, see PingID integration for Mac login 1.3.2 (January 17, 2024).

December 2023

New features and improvements in PingID implemented in December 2023.

December 6

New version of PingID integration for Mac login (version 1.3.1)

New PingID Integration for Mac login

For details, see PingID integration for Mac login 1.3.1 (December 6, 2023).

December 3

New version of PingID Mobile app 1.39

New PingID mobile app

For iOS changes, see Mobile app 1.39 (December 3, 2023) iOS.

For Android changes, see Mobile app 1.39 (December 3, 2023) Android.

November 2023

New features and improvements in PingID implemented in November 2023.

November 21

New version of PingID integration for Windows login (version 2.10.2)

New PingID Integration for Windows login

For details, see PingID integration for Windows login 2.10.2 (November 21, 2023).

October 2023

New features and improvements in PingID implemented in October 2023.

October 30

New version of PingID integration for Windows login - passwordless (version 1.5)

New PingID Integration for Windows login

For details, see PingID integration for Windows login (passwordless) 1.5 (October 30, 2023).

October 9

Number matching details in the user code screen

Improved PingID

We've updated the UX text in the Use Code screen to improve clarity so that if a user chooses to use an OTP (one-time passcode) when authenticating, they retain the option to authenticate by number matching if required.

September 2023

New features and improvements in PingID implemented in September 2023.

September 26

New version of PingID Mobile app 1.38

New | PingID mobile app

For iOS changes, see Mobile app 1.38 (September 26, 2023) iOS.

For Android changes, see Mobile app 1.38 (September 26, 2023) Android.

September 19

New version of PingID Integration Kit 2.26.

New | PingID Integration kit for PingFederate

A new version of PingID Integration Kit 2.26 is released with a new version of PingID RADIUS PCV 3.0.4. For more information, see PingID Integration Kit 2.26 (September 19, 2023).

Intermittent enforcement of SMS and voice limits

Fixed | STAGING-19252 | PingID

We've fixed an issue that sometimes prevented the enforcement of SMS and voice limits.

September 18

New version of PingID integration for Windows login (version 2.10.1)

New | PingID Integration for Windows login

For details, see PingID integration for Windows login 2.10.1 (September 18, 2023).

Issue logging on to Windows login using a Security Key in AU region when offline

Fixed | STAGING-17704 | PingID

We've fixed an issue that was preventing Windows login users whose PingID regional data center is located in Australia (AU region) from authenticating using a Security Key when offline. This issue is fixed for all users after they successfully authenticate online at least once using their security key.

September 14

Device IP address subscription information included in PingID audit events

Improved PingID

The IP address of the accessing device is now included in the PingID audit event information that is reported through the PingOne subscription facility.

VPN/SSH policy syntax updated

Improved PingID

We've updated the name of the VPN/SSH policy in the admin portal to RADIUS PCV and SSH, for clarity. For details, see Configuring a RADIUS PCV and SSH access policy

September 12

Limit Push Notification rule update

Improved PingID

To improve clarity, we've updated the UI for the Limit Push Notifications rule. We've also updated our documentation to explain how the rule is implemented in more detail. For information see Configuring a limit push notifications rule.

August 2023

New features and improvements in PingID implemented in August 2023.

August 14

Issue scrolling down from Registration and Change Devices window

Fixed STAGING-19975 PingID

We've fixed an issue that was preventing users from scrolling down from the Registration window or the Change Devices window, when viewed from a web browser on a small screen.

August 2

New version of PingID Integration for Mac login (version 1.3.0)

New PingID Integration for Mac login

For details, see PingID integration for Mac login 1.3.0 (August 2, 2023).

July 2023

New features and improvements in PingID implemented in July 2023.

July 26

Security key authentication failure when adding new Google account on Android

Fixed STAGING-20031 PingID

There were cases where PingID authentication with a security key failed when the user was trying to add a new Google account to their Android device. This issue has been fixed.

July 25

New version of PingID integration for Windows login - passwordless (version 1.4)

New PingID Integration for Windows login

For details, see PingID integration for Windows login (passwordless) 1.4 (July 25, 2023).

July 18

SMS delivery code enhancement

Improved PingID

To avoid SMS delivery issues associated with the use of Long Codes (LC) in some US territories, and to improve resiliency, Ping Identity's SMS service now uses short codes (SC) and Toll-Free Numbers (TFN) only.

July 17

Support ID added to general error messages

Improved PingID

To help the Ping Identity support team to identify the relevant log entries and troubleshoot customer issues more effectively, we've added a Support ID to all general error messages in PingID.

PingID user guide restructured

Improved PingID

We've restructured the PingID user guide to reflect the user journey - pairing and then authenticating with PingID. We've also streamlined the topic structure to focus on authentication methods, rather than platforms.

July 11

Support of FIDO2 security key device redirection with Windows RDP

Improved PingID

Windows login now supports FIDO2 security keys redirection when using Windows 10 Remote Desktop Protocol (RDP) or later.

June 2023

New features and improvements in PingID implemented in June 2023.

June 27

Number matching details added to the Use Code screen

Improved PingID

We've added details of the number required to complete a number-matching flow to the One-time passcode (OTP) screen. This can be helpful in the event that a user who is prompted to authenticate using number matching clicks the **Use Code** option before completing authentication, as they are still able to view the relevant number and complete the number-matching flow.

June 22

New version of PingID Integration Kit 2.25.

New PingID Integration kit for PingFederate

A new version of PingID Integration Kit 2.25 is released with a new version of PingID Adapter 2.14. For more information, see PingID Integration Kit 2.25 (June 22, 2023).

June 15

New version of PingID Mobile app 1.37

New PingID mobile app

For iOS changes, see Mobile app 1.37 (Jun 15, 2023) iOS.

For Android changes, see Mobile app 1.37 (June 15, 2023) Android.

June 8

Enhancements when connecting PingID and PingOne

Improved PingID

We've enhanced the process of connecting an existing PingID organization to a new PingOne environment:

- Before starting the process of connecting PingID and PingOne, PingID now performs a verification check to ensure that the license for the relevant PingOne organization is valid, and is sufficient to support the number of PingID users.

  If the license is not valid, or the number of users required exceeds the number of users permitted by the organization's PingOne license, the process is stopped. An audit message is included in the admin activity report in PingID. Customers should contact their support representative to extend their license if required, and then restart the connecting process.

- New audit events are included in the admin activity report in PingID to enable Administrators to review the synchronization status and follow up in case of any possible failures.

June 6

New version of PingID integration for Windows login (version 2.10)

New PingID Integration for Windows login

For details, see PingID integration for Windows login 2.10 (June 6, 2023).

PingID "Forgot your device?" backup authentication link unavailable

Fixed STAGING-16966 PingID

Fixed an issue that was causing the **Forgot your device?** link to disappear from the authenticating screen, even when at least one authentication method was configured for backup authentication in the web portal, and the relevant rule action was configured in PingID policy.

May 2023

New features and improvements in PingID implemented in May 2023.

May 30

PingID User Guide standalone

Improved PingID

We've moved the PingID User Guide out of the PingID Administration Guide so that it is easier for end users to access. You can find it on the Read the Docs page here.You'll also find a link to it at the end of the PingID Administration Guide.

May 22

DVORAK keyboard layout support for YubiKey (OTP)

Improved PingID

We've added support for the DVORAK keyboard layout when using Yubikey (OTP) devices. NOTE: The same keyboard layout used to register your device must be used when authenticating with that device.

May 18

Support for ECC algorithm with WebAuthn APIs for Windows Hello

Improved PingID

PingID now supports the ECC algorithm in TPM attestation, in addition to the RSA algorithm. NOTE: ECC public keys require Windows 11 22H2 or later.

May 3

New version of PingID Mobile app 1.36.1 (Android)

New PingID mobile app

For details, see Mobile app 1.36.1 (May 3, 2023) Android.

May 2

New version of PingID desktop app 1.7.5

New PingID desktop app

For details see Desktop app 1.7.5 (May 2, 2023).

April 2023

New features and improvements in PingID implemented in April 2023.

April 24

New version of PingID Mobile app 1.36

New PingID mobile app

For iOS changes see Mobile app 1.36 (April 24, 2023) iOS.

For Android changes see Mobile app 1.36 (April 24, 2023) Android.

April 18

PingID Connector

Improved PingID

We've enhanced the PingID Connector to enable the user to enter their One-time Passcode (OTP) when triggering Multi-factor Authentication (MFA). It's now possible for the user to enter a TOTP/HOTP-generated OTP when starting authentication using the Create Device Authentication endpoint.

Support for SMS and Voice calls to Kosovo

Improved PingID

We've added Kosovo to the list of countries that support one-time passcode SMS and Voice calls.

April 4

PingID policy Limit Push Notification rule issue

Fixed PID-13054 PingID

Fixed an issue that was preventing the Limit Push Notification rule from triggering in certain situations.

April 3

New version of PingID Mobile app 1.35

New PingID mobile app

For iOS changes see Mobile app 1.35 (April 3, 2023) iOS.

For Android changes see Mobile app 1.35 (April 3, 2023) Android.

February 2023

New features and improvements in PingID implemented in February 2023.

February 28

Number matching authentication method

New PingID

We've added the ability to authenticate by displaying a number on the user's accessing device and prompting the user to select the corresponding number in PingID mobile app.

This feature is supported on PingID mobile app 1.34 and later.

> **Note**
>
> If your policy includes number matching as the sole authentication method, users running PingID mobile app 1.33 or earlier will not be able to authenticate.

Number matching can only be used for web-based authentication requests. It should not be used for CLI and text-based authentication.

For information, see Configuring number matching authentication, Authenticating by number matching, and PingID Authentication API.

February 21

Limit push notifications rule

New PingID

To reduce the likelihood of a user acknowledging a malicious push notification as part of an MFA fatigue attack, we've added a new rule that enables you to limit the number of push notifications the user can receive within a given time period. This rule appears under PingID policy settings and is available for Web authentication only.

For information see:

- Configuring a limit push notifications rule in the PingID Administration Guide.
- Limit push notifications rule in the PingID API Guide.

New version of PingID Integration Kit 2.24.

New PingID Integration kit for PingFederate

A new version of PingID Integration Kit 2.24 is released with a new version of PingID RADIUS PCV 3.0.3. For more information, see PingID Integration Kit 2.24 (February 21, 2023).

February 20

New version of PingID Mobile app 1.34

New PingID mobile app

For iOS changes see Mobile app 1.34 (February 20, 2023) iOS.

For Android changes see Mobile app 1.34 (February 20, 2023) Android.

February 14

New version of PingID Integration for Mac login (version 1.2)

New PingID Integration for Mac login

For details, see PingID integration for Mac login 1.2 (February 14, 2023).

February 7

Versioning of PingID policies

Improved PingID

Policy collections are now assigned a version number to prevent policies from being modified simultaneously by multiple administrators. Each time the existing policies are modified, the version number is incremented. If the version number sent in an API request does not match the current version number, an error is returned. For details, see the documentation for the Web Authentication Policy API.

PingID language support

Improved PingID

PingID now supports the following additional languages:

- Czech
- Polish
- Hungarian

January 2023

New features and improvements in PingID implemented in January 2023.

January 31

New version of PingID Integration Kit 2.23.

New PingID Integration kit for PingFederate

A new version of PingID Integration Kit 2.23 is released with a new version of PingID RADIUS PCV 3.0.2. For more information, see PingID Integration Kit 2.23 (January 31, 2023).

January 29

New version of PingID Mobile app 1.33

New PingID mobile app

For iOS changes see Mobile app 1.33 (January 29, 2023) iOS.

For Android changes see Mobile app 1.33 (January 29, 2023) Android.

January 23

New version of PingID desktop app 1.7.4

New PingID Desktop app

A new version of PingID desktop app 1.7.4 is released. For more information, see Desktop app 1.7.4 (January 23, 2023).

January 17

New version of PingID Integration Kit 2.22

New PingID Integration kit for PingFederate

A new version of PingID Integration Kit 2.22 is released with a new version of PingID Adapter 2.13.2. For more information, see PingID Integration Kit 2.22 (January 17, 2023).

January 9

New version of PingID Mobile app 1.32

New PingID mobile app

For iOS changes see Mobile app 1.32 (January 9, 2023) iOS.

For Android changes see Mobile app 1.32 (January 9, 2023) Android.

January 3

New version of PingID integration for Windows login (version 2.9)

New PingID Integration for Windows login

For details, see PingID integration for Windows login 2.9 (January 3, 2023).

New version of PingID Integration Kit 2.21

New PingID Integration kit for PingFederate

A new version of PingID Integration Kit 2.21 is released with a new version of PingID Adapter 2.13.1. For more information, see PingID Integration Kit 2.21 (January 3, 2023).

New PingID connector flows

New PingID

Following the release of the new PingID DaVinci connector, we've added the following out-of-the-box flows:

- PingID registration sub-flow
- PingID authentication sub-flow

For more information, see the PingID connector documentation.

December 2022

New features and improvements in PingID implemented in December 2022.

December 15

PingID connector

New PingOne

The new PingID connector is available. This connector includes an increased set capabilities and is based on the PingOne API, and replaces the previous PingID connector (now called PingID Legacy Connector). For information, see PingID connector.

User Detailed Status Reports expanded

Improved PingID

We've added the following new fields to theUser Detailed Status Report:

- `fidoBackupEligibility` (boolean): Indicates whether the FIDO device (FIDO biometrics, or FIDO security key) supports credentials backup to the cloud.
- `fidoBackupState` (boolean): Indicates whether the FIDO device credentials are backed up to the cloud.

For devices that are already paired with PingID, these fields are updated on the fly.

December 14

PingID Activity report FIDO2 metadata expanded

Improved PingID

We've expanded the metadata that relates to FIDO2 biometrics devices and security keys in the PingID Activity report, and improved the format in which it is presented.

December 13

New version of PingID Mobile app 1.31

New PingID mobile app

For iOS changes see Mobile app 1.31 (December 13, 2022) iOS.

For Android changes see Mobile app 1.31 (December 13, 2022) Android.

Support of PingID mobile app PIN code

New PingID

PingID now supports the use of a PIN code on the PingID mobile app. Admins can require PIN codes for devices that do not have a device PIN only, or for all devices. This feature is supported by PingID mobile app 1.31 or later. For information, see Configuring the PingID mobile app PIN.

Notify users of new PingID mobile app versions

New PingID

PingID now enables you to notify your users that a new version of PingID mobile app is available. You can make updates mandatory, or optional, and specify the minimum version from which users are notified that an update is available. This feature is supported by PingID mobile app 1.31 or later. For information, see Enabling PingID mobile app update notifications.

November 2022

New features and improvements in PingID implemented in November 2022.

November 29

New version of PingID Integration for Mac login (version 1.1.2)

New PingID Integration for Mac login

For details, see PingID integration for Mac login 1.1.2 (November 29, 2022).

November 22

New version of PingID Integration Kit 2.20

New PingID Integration kit for PingFederate

A new version of PingID Integration Kit 2.20 is released with a new version of PingID Adapter 2.13. For more information, see PingID Integration Kit 2.20 (November 22, 2022).

November 14

User Verification discouraged

Improved PingID

To reduce friction to the user authentication flow, we've added the option to skip user verification. This feature is currently available to web users only. It will be available to Windows login users in a future version of Windows login.

For details, see (Legacy) Configuring security key authentication.

November 13

Uploading / revoking OATH tokens with the PingID API

New PingID

A new endpoint (`createorgtokens`) has been added to the PingID API to allow you to upload a list of OATH tokens that can then be mapped to individual users.

There is also a new endpoint (`revokeorgtokens`) that can be used to revoke one or more OATH tokens that you previously uploaded for use.

For details, see the new sections added under OATH token management.

November 3

New version of PingID RADIUS PCV 3.0.1

New PingID Integration kit for PingFederate

A new version of PingID Integration Kit 2.19 is released with a new version of RADIUS PCV 3.0.1. For more information, see PingID Integration Kit 2.19 (November 3, 2022).

New version of PingID integration for Windows login - passwordless (version 1.3)

New PingID Integration for Windows login

For details, see PingID integration for Windows login (passwordless) 1.3 (November 3, 2022).

October 2022

New features and improvements in PingID implemented in October

October 25

New version of PingID Mobile app 1.30

New PingID mobile app

For iOS changes see Mobile app 1.30 (October 25, 2022) iOS.

For Android changes see Mobile app 1.30 (October 25, 2022) Android.

September 2022

New features and improvements in PingID implemented in September 2022.

September 29

Added a second voice provider to improve reliability

Improved PingID

As part of the ongoing effort to improve the reliability of voice-based authentication, a second voice provider has been added for PingID.

September 15

New version of PingID Mobile app 1.29

New PingID mobile app

For iOS changes see Mobile app 1.29 (September 15, 2022) iOS.

For Android changes see Mobile app 1.29 (September 15, 2022) Android.

September 13

SMS service resiliency for Canada

Improved PingID

As part of the ongoing effort to improve the reliability of SMS-based authentication, a Canadian short code number is now being used for all SMS messages sent within Canada.

August 2022

New features and improvements in PingID implemented in August 2022.

August 31

Enforce PingOne FIDO policy for PingID

Improved PingID

You can now choose to enforce PingOne FIDO policy for PingID during authentication and registration flows.

> **Note**
>
> This feature is only available for organizations that are using a PingID environment that is integrated with PingOne or created by PingOne.
> Only the default PingOne FIDO policy is enforced. For information, see (Legacy) Configuring the FIDO2 security key for PingID. For information about PingOne FIDO policy, see the PingOne documentation on FIDO policies.

August 30

New version of PingID RADIUS PCV 3.0

New PingID Integration kit for PingFederate

A new version of PingID Integration Kit 2.18 is released with a new version of RADIUS PCV, which includes support for MS-CHAP v2, as well as other enhancements. For more information, see PingID Integration Kit 2.18 (August 30, 2022).

August 22

New version of PingID Integration for Windows login (version 2.8.4)

New PingID Integration for Windows login

For details, see PingID integration for Windows login 2.8.4 (August 22, 2022).

August 2

Improved user experience for one-time passcode

Improved PingID

You can now send a push notification to your users, when requesting a one-time passcode (OTP). When the user taps the notification PingID mobile app opens automatically, and generates an OTP. For more information, see Configuring OTP push notifications.

July 2022

New features and improvements in PingID implemented in July 2022.

July 31

PingID reports - bypass expiration, mobile log support ID, failure reason

Improved PingID

- PingID Admin Activity reports now include the expiration date of bypasses issued to users.
- PingID Activity reports now include the support ID given to mobile device logs that were received.
- If you have created subscriptions to PingID events, the information returned now includes the reason for an authentication failure.

July 28

New version of PingID Mobile app 1.28

New PingID mobile app

For iOS changes see Mobile app 1.28 (July 28, 2022) iOS.

For Android changes see Mobile app 1.28 (July 28, 2022) Android.

July 17

QR Code duration

New PingID

You can now define the number of hours for which the QR code used to register a user is valid. For details, see Configuring pairing conditions.

PingID Enrollment page

Info PingID

The legacy enrollment page is now deprecated. All customers that did not upgrade earlier have been automatically migrated to the new enrollment page. All legacy settings specific to an organization's legacy configuration are automatically applied to the new enrollment page.

July 6

New version of PingID Integration for Mac login (version 1.1.1)

New PingID Integration for Mac login

For details, see PingID integration for Mac login 1.1.1 (July 6, 2022).

June 2022

New features and improvements in PingID implemented in June 2022.

June 28

New version of PingID integration for Windows login - passwordless (version 1.2)

New PingID Integration for Windows login

For details, see PingID integration for Windows login (passwordless) 1.2 (June 28, 2022).

June 21

New version of PingID integration for Windows login (version 2.8.3)

New PingID Integration for Windows login

For details, see PingID integration for Windows login 2.8.3 (June 21, 2022).

June 15

New version of PingID integration for Windows login (version 2.8.2)

New PingID Integration for Windows login

For details, see PingID integration for Windows login 2.8.2 (June 15, 2022).

June 12

New version of PingID Mobile app 1.27

New PingID mobile app

For iOS changes see Mobile app 1.27 (June 12, 2022) iOS.

For Android changes see Mobile app 1.27 (June 12, 2022) Android.

May 2022

New features and improvements in PingID implemented in May 2022.

May 31

New version of PingID integration for Windows login (version 2.8)

New PingID Integration for Windows login

For details, see PingID integration for Windows login 2.8 (May 31, 2022).

New version of PingID Integration for Mac login (version 1.1)

New PingID Integration for Mac login

For details, see PingID integration for Mac login 1.1 (May 31, 2022).

May 23

New version of PingID Mobile app 1.26

New PingID mobile app

For iOS changes see Mobile app 1.26 (May 23, 2022) iOS.

For Android changes see Mobile app 1.26 (May 23, 2022) Android.

May 2

New version of PingID Mobile app 1.25

New PingID mobile app

For iOS changes see Mobile app 1.25 (May 2, 2022) iOS.

For Android changes see Mobile app 1.25 (May 2, 2022) Android.

April 2022

New features and improvements in PingID implemented in April 2022.

April 27

New version of PingID Integration Kit 2.17

New PingID Integration kit for PingFederate

For details, see PingID Integration Kit 2.17 (April 27, 2022).

March 2022

New features and improvements in PingID implemented in March 2022.

March 23

New version of PingID Integration Kit 2.16

New PingID Integration kit for PingFederate

We've released a new version of the PingID Integration Kit. For details, see PingID Integration Kit 2.16 (March 23, 2022).

March 10

Set a daily limit for SMS and voice-based pairing requests

Improved PingID

It is now possible to include the number of daily SMS-based and voice-based pairing requests for a user in the limits that you set with **Daily Used SMS or Voice Limit** and **Daily Unused SMS or Voice Limit**. When you enable this option, the number of pairing requests is added to the number of authentication requests and the total cannot exceed the numbers that you set. See Configuring SMS and voice authentication for PingID.

March 7

Maximum time period for recent authentication rules extended to 90 days

Improved PingID

For the three time-related policy rules - recent authentication, recent authentication from office, recent authentication from company network - the maximum period that can be defined has been extended from 30 to 90 days.

January 2022

January 25

New version of PingID integration for Windows login (version 2.7)

New PingID Integration for Windows login

We've released a new version of PingID integration for Windows login. For details, see PingID integration for Windows login 2.7 (January 25, 2022).

January 11

Push/pull subscriptions now include device model and session ID data

Improved PingID

For push/pull subscriptions in PingOne for Enterprise, the data streamed now includes:

- Device model
- Session ID for authentication attempts. This ID can be used to combine information from the various events that are included in the streamed data, such as policy and success/failure status.

For more information on subscriptions, see Subscriptions.

December 2021

New features and improvements in PingID implemented in December 2021.

December 23

Authentication policies applied when accessing an application with a newly paired device

Improved PingID

In situations where users without a paired device attempted to access an application, the successful pairing allowed them to access the application without taking into account the authentication policies defined.

An option has now been added to require that the relevant authentication policies for the application be applied even in this scenario. To enable this requirement, select the option in the Enrollment section of the PingID configuration page (*Enforce Policy evaluation after new device registration*).

December 21

New version of PingID SSH Integration (version 4.2.0)

New PingID

We've released a new version of the PingID SSH Integration. For details, see PingID SSH Integration 4.2.0 (December 21, 2021).

December 16

Added a second SMS provider to improve reliability

Improved PingID

As part of the ongoing effort to improve the reliability of SMS-based authentication, a second SMS provider has been added for PingID.

December 9

Log in to your Windows machine without a password

New PingID Integration for Windows login

You can now log in to a Windows computer without having to enter a password, using the PingID mobile app. The authentication relies on Certificate-Based Authentication, but the user experience is similar to the familiar authentication process with the PingID mobile app.

For details, see Integrating PingID with Windows login (passwordless).

December 1

Sender ID for SMS messages sent to Polish mobile numbers shows PINGID

Improved PingID

To reduce delivery problems, SMS messages sent to Polish mobile numbers now use PINGID as the sender ID.

November 30, 2021

Enhancements

PingID Integration for Mac login 1.0.3

For details, see PingID integration for Mac login 1.0.3 (November 30, 2021).

November 22, 2021

Enhancements

PingID API - offlinepairing: support for external authenticator apps

It is now possible to use the API's existing `offlinepairing` method to facilitate the migration of users registered with an external authenticator app, so that users do not have to manually pair the authenticator app with PingID. For details, see the API documentation for offlinepairing.

November 10, 2021

Enhancements

PingID Integration Kit 2.15

For details, see PingID Integration Kit 2.15 (November 10, 2021).

November 8, 2021

Enhancements

SMS service information & privacy policy

For our user's convenience, we've updated the SMS registration screen to include information about the SMS service as well as links to our privacy policy and terms and condition.

November 2, 2021

Enhancements

Web authentication policy API

You can now use the PingID API to create and update policies for web authentication. For details, see Web Authentication Policy API.

October 18, 2021

Enhancements

Accessibility improvements

As part of our ongoing efforts to improve accessibility, we've made some necessary updates to the PingID registration and authentication windows.

PingID Integration Kit 2.14

For details, see PingID Integration Kit 2.14 (October 18, 2021).

October 13, 2021

Resolved issues

Ticket ID	Description
STAGING-13693	When using the `offlinepairing` API method to pair a user via a voice number that has an extension, there were cases where a 400 server error or 500 server error was returned. This issue has been resolved.
STAGING-13694	When **Maximum Allowed Devices** was set to 1, API requests to add a second device for the user returned error 20549 ("user already exists"), rather than the correct message, 20562 ("user.exceeded.num.of.devices"). This issue has been resolved.

September 30, 2021

Enhancements

Adding existing PingID tenant to a new PingOne environment

When creating a PingOne environment, it is now possible to connect the new environment to an existing PingID tenant.

For more information, see Adding an existing PingID tenant to a new PingOne environment.

September 22, 2021

PingID integration for Windows login (version 2.5.2)

For details, see PingID integration for Windows login 2.5.2 (September 22, 2021).

July 28, 2021

Enhancements

Using risk level in PingID policies

It is now possible to include the risk level calculated by PingOne Protect (or a supported third-party risk service) when you define a PingID policy. MFA actions can be specified for each of the three risk levels - high, medium, and low. This feature requires version 2.11 of the PingID adapter (included in PingID Integration Kit 2.13) and a separate license for the integrated Risk service.

For more information, see Configuring a risk level rule (web policy).

PingID Integration Kit 2.13

For details, see PingID Integration Kit 2.13 (July 28, 2021).

July 13, 2021

Enhancements

PingID API - new parameter added for configuring expiration time of activation code

A new parameter, `hoursUntilExpiration`, has been added to the `getactivationcode` method to allow you to specify the number of hours the activation code should remain valid. This optional parameter can take any integer value between 1 and 336 (two weeks). If the `hoursUntilExpiration` parameter is not used, the activation code is valid for 48 hours.

For details, see the documentation for getactivationcode.

June 14, 2021

Resolved issues

Ticket ID	Description
STAGING-12924	Due to changes made by Apple in recent versions of iOS / macOS, users authenticating with a security key on iOS / macOS are now presented with an additional dialog where they must press Continue before authenticating with the key.

June 7, 2021

Enhancements

PingID API - new parameters added for FIDO-based authentication

Two new parameters have been added to make it possible to override the default user information text that a device displays on the account selection screen.

For details, see:

- PingID User Management API - WebAuthnStartPairing (FIDO biometrics) (new parameters: `name`, `displayName`)
- Authentication using browser redirect - PPM request for FIDO pairing with a hybrid UI (new parameters: `webauthnName`, `webauthnDisplayName`)
- Example - PingID FIDO security key

June 1, 2021

Enhancements

Generation of PingID properties file

The maximum number of PingID properties files that can be generated has been increased to five.

May 26, 2021

PingID desktop app (version 1.7.2)

For details, see Desktop app 1.7.2 (May 26, 2021).

May 11, 2021

PingID SSH Integration (version 4.1.1)

For details, see PingID SSH Integration 4.1.1 (May 11, 2021).

PingID desktop app release notes

Desktop app 1.8.0 (January 23, 2025)

New features and improvements in PingID desktop app 1.8.0

Desktop app user profiles

Improved PingID desktop app

We've added the ability to define user profiles on a single instance of PingID desktop app. Learn more in Managing PingID desktop app profiles, in the PingID End User Guide.

Desktop app 1.7.5 (May 2, 2023)

New features and improvements in PingID desktop app 1.7.5.

Users can now install PingID desktop app

Improved PingID desktop app

Users can now install the desktop app, without requiring admin permissions. For information, see Setting up PingID desktop authentication on Windows.

Security enhancements

Improved PingID desktop app

We've made some security enhancements.

Desktop app 1.7.4 (January 23, 2023)

New features and improvements in PingID desktop app 1.7.4.

Define a specific installation path

Improved PingID desktop app

You can now specify the folder path to which you want to install PingID desktop app. Browse to the required path in the UI, or add the specific command through the CLI. For information, see Setting up PingID desktop authentication on Windows and Installing the desktop app using the Windows CLI.

Language support

Improved PingID desktop app

PingID desktop app now supports the following additional languages:

- Czech
- Polish
- Hungarian

Security and reliability

Improved PingID desktop app

Improvements to security, performance, and reliability.

Issue unpairing PingID desktop app

Fixed | PID-5165/PID-5166 | PingID desktop app

We've fixed an issue related to unpairing PingID desktop app. For PingID desktop app users with a PIN code who want to unpair PingID desktop app, it is now required to enter the PingID Desktop PIN in order to unpair PingID desktop app. Users that forget their PIN code and want to unpair PingID must uninstall the app, reinstall the app, and then pair it again.

Desktop app 1.7.3 (February 22, 2022)

Enhancements

Java libraries update

We performed a Java dependencies update.

Security enhancement

We enhanced the security of PingID desktop app.

Desktop app 1.7.2 (May 26, 2021)

Resolved issues

Ticket ID	Description
PID-8682, STAGING-9142	There were cases where users opened more than one instance of the PingID desktop app, and this resulted in the unpairing of their devices. This issue has been resolved.

Desktop app 1.7.1 (April 2020)

Resolved issues

Ticket ID	Description
PID-9267, PID-9533	This version of PingID desktop app resolves a security issue.

Desktop app 1.7.0 (February 2020)

Enhancements

This version of PingID desktop app includes an upgrade to the latest LTS Java version, in order to enhance performance and security.

Resolved issues

Ticket ID	Description
PID-8979	Added graceful exit for users attempting to install PingID desktop app on a 32-bit Windows machine.

Desktop app 1.5.4 (August 2019)

Resolved issues

The issues affecting PingID desktop app upgrade process have been resolved.

It is no longer recommended upgrading to Desktop app version 1.5.3. Users of version 1.5.3 can continue using it without any service interruption.

See:

- The Admin guide:
  - PingID desktop app authentication
  - Installing the desktop app using the Windows CLI
- The User guide
  - Setting up PingID desktop authentication on Windows

Desktop app 1.5.3 (August 2019)

Known issues

The PingID desktop app version 1.5.3 is no longer available for download due to fixes required for several upgrade scenarios.

Users who have installed version 1.5.3 and have not experienced service degradation following the upgrade, can continue using it.

Desktop app 1.5.3 (July 2019)

Enhancements

The PingID desktop app has been extended to support the following new feature:

Roaming User Profiles

Support has been added for roaming user profiles. If a user's profile is synchronised with any domain roaming folder, his PingID settings will be also synchronised. The feature may be enabled or not during installation.

Desktop app 1.5.2 (October 2018)

Enhancements

The PingID desktop app has been extended to support the following new features:

Proxy Auto Configuration (PAC)

Admins now have the option to configure Proxy Auto Configuration (PAC) for the PingID desktop app, enabling you to manage networks with multiple proxies.

Kerberos proxy authentication

Admins now have the option to configure Kerberos proxy authentication. This enables the PingID app to authenticate using the Kerberos protocol, delegating the machine credentials for authentication to the organizational proxy.

Turkish language support

From v1.5.2 PingID desktop app supports the Turkish language.

Desktop app 1.5.1 (July 2018 - updated)

Enhancements

Desktop app documentation update

The documentation for Desktop app has been updated, and the admin and user actions have been placed in different sections.

- Admin-related desktop app documentation.
- See the relevant locations in the PingID End User Guide, including The PingID mobile app for iOS and Android, and PingID desktop app management.

The PingID desktop app has been extended to support the following:

PingID preparation for future 64-bit application releases

PingID Desktop app v1.5.1 provides the platform for future 64-bit application releases.

Desktop app 1.5.0 (November 2017 - updated)

Enhancements

The PingID desktop app has been extended to support the following new features:

PingID desktop app 1.5.0 proxy support

Admins now have the option to configure the PingID desktop app, so that it supports proxy for all enterprise internal communication to the internet, on enterprise desktop and laptop machines.

- **Scripts for PingID desktop app 1.5.0**
  - **SetAutoUpdateMode**:
    - The `SetAutoUpdateMode.1.5.0.bat` script for Windows platforms has been updated. If admins wish to update the desktop app's autoupdate status, they need to run the `SetAutoUpdateMode.1.5.0.bat` script. The new `SetAutoUpdateMode.1.5.0.bat` script for Windows is provided at https://github.com/pingidentity/pingid-desktop-application.
    - There is no change to the `SetAutoUpdateMode.bat` script on Windows, for desktop app version 1.4 and lower.
    - There is no change to the `SetAutoUpdateMode.sh` script for Apple Mac.
  - **SetProxyParams**:
    - The new `SetProxyParams` script is available from PingID desktop app 1.5.0, and is required in order to configure the proxy feature for Windows or Apple Mac.
    - The `SetProxyParams` scripts for both Windows and Apple Mac are provided at https://github.com/pingidentity/pingid-desktop-application.

Desktop app interface improvements for PIN code

The desktop app interface has been enhanced to display improved instructions describing the valid PIN policy requirement: 3 different nonsequential numbers for a 4-digit PIN, and 4 different nonsequential numbers for a 6-digit PIN.

Resolved issues

Ticket ID	Description
PID-4792	A case was reported where the PingID Desktop app with the PIN code feature enabled hung after several days of inactivity. This issue is now resolved.
PID-5089	In some cases, the PingID desktop app crashed when running on Windows 10 Creators version (builds 1703 and 1709). This issue is now resolved.
PID-5486	There were cases where uninstalling the desktop app did not clear historical configuration settings. This issue is now resolved.

Known issues and limitations

Autoupdate feature

Windows 10 Creators version and later: If autoupdate had been disabled in an earlier version of the PingID desktop app version, the new `SetAutoUpdateMode.1.5.0.bat` script needs to be run after the PingID desktop app is upgraded to version 1.5.0.

Proxy configuration script SetProxyParams

> **Caution**
>
> After any execution of the `SetProxyParams` script, it is imperative to shut down and reopen the PingID desktop app. Failure to do so will cause errors in the desktop app's operation.

Validation of the proxy parameters in the SetProxyParams script

Windows platforms only: When running the `SetProxyParams` script, there is no port parameter entry validation, and the configuration completes without warning, even in the case of an incorrect alphanumeric port parameter entry.

Unpairing the PingID desktop app when the PIN code setting is enabled

In Version 1.5, when the desktop app is configured to require a PIN code, the **Help>Unpair**(Windows) or **PingID>Unpair** (Mac) menu options are displayed also after the user logged in to the app, although they should only be displayed before the user has entered their PIN code. If a user wants to unpair the desktop app when logged in to the desktop app (after entering the PIN code), they should do so only via the settings (gear icon) and not using the **Help>Unpair** or **PingID>Unpair** menu options.

Unpairing from the **Help>Unpair** or **PingID>Unpair** menu is only meant for the case where the user has lost their PIN code and is unable to log in. This action will also require admin to unpair the user's desktop app from the server side, in order to permit the user to pair again.

Desktop app 1.4.0 (April 20, 2017)

Enhancements

The PingID desktop app has been extended to support the following new feature:

PingID desktop app PIN code

Admins now have the option to configure the PingID desktop app, so that the OTP screen will be hidden behind either a 4-digit or 6-digit PIN code. This elevates the security level and avoids cases of users leaving their workstation unlocked, and other users accessing the PingID OTP.

Resolved issues

Ticket ID	Description
PID-2451	The previous version of the desktop app returned a general "unknown error" message on failure of desktop related activities to communicate with the PingID server. This has been refined so that errors caused by network issues now return a "network error" message.
PID-4081	In some installations of the desktop app, part of the lower section of the app window was cut. This was due to custom DPI or custom scaling. This has been resolved. Although there remain few rare edge cases of a combination between small screen sizes and high resolution, where a tiny lower part of the screen is still cut, all UI controls are visible and the app is fully fuctional.

Ticket ID	Description
PID-4199 and PID-4206	When a user was offline and trying to unpair the desktop app, the user did not receive the correct warning that there is no connectivity and that the user may need to contact the admin in order to complete the unpairing process. This has been resolved with a clear warning, and the option buttons to either continue or cancel the unpair action.

Known issues and limitations

Desktop app window display is cut

In some rare cases of a combination between small screen sizes and high resolution, a small part of the lower section of the desktop app window display is cut. Functionality is not affected.

Desktop app 1.3.53 (January 16, 2017)

Known issues and limitations

Misleading message on Mac using Google Chrome, when downloading the desktop app installer via the Europe and Australia web portals

On completion of downloading the desktop app via the web using Google Chrome, Europe and Australian Mac users receive the following warning message: `This type of file can harm your computer. Do you want to keep PingID.pkg anyway?`

The reason is that the desktop app's certificate is signed for the North America data center, but downloaded via the Europe or Australia data centers. This warning message may be ignored.

Desktop app 1.3.53 (December 2016)

Enhancements

Installer languages for Windows

The PingID desktop app installer for Windows now provides installation instructions in the following languages: English, French, German, Italian, Japanese, Dutch, Portuguese (Portugal), Russian and Spanish.

Desktop app update capabilities

Admins can now have the flexibility to choose whether to push newer versions of the desktop app to their users using company distribution mechanism, or to grant users with the freedom to decide if and when to update the app version.

End users, whose installation of the PingID desktop app permits them control of automatic updates, now have an easier on demand menu toggle selection, which permits them to change the configuration to activate or deactivate automatic updates.

Enhanced support

A support ID reference number is added to sent logs and is displayed on the settings page of the app, for reference in further communication with the support team.

Resolved issues

Ticket ID	Description
PID-2414	A zip file is created when activating the **Send Logs** option. On completion of the transmission, the process should delete the local copy of the zip file. The deletion did not occur, and on creation of a new zip file, users received the error message `ZIP log file did not delete`. This has been resolved.
PID-2416	When a user selected the **Remove Organization** option and then **Cancel**, the **Remove Organization** icon changed to red until the user performed another action before changing back to gray. This has been resolved.

Known issues and limitations

The desktop app does not launch on Mac after custom fonts were installed

Some users who added custom fonts on their Mac were unable to launch the desktop app. Resolve the problem:

1. Open the **Font Book** application.
2. Select **Menu → File → Restore Standard Fonts**
3. Run the desktop app, which should now launch successfully.
4. Close the desktop app.
5. Reinstall the custom fonts.
6. Run the desktop app again. If it does not succeed, rerun steps 1-3 above.

Desktop app 1.2.42 (July 2016)

Enhancements

Supported languages

The PingID desktop app is now supporting the following languages: English, French (EU), French (Canadian), German, Japanese, Chinese, Dutch, Italian, Korean, Portuguese, Russian, Spanish and Thai.

Desktop app update capabilities

The PingID desktop app provides the option to check for new available versions, automatic end user notifications of available updates, and a semiautomatic update function.

Resolved issues

Ticket ID	Description
PID-1671	The uninstall process on the Windows platform has been fixed to remove all of the files from the PingID desktop app installation.
PID-1788	The PingID desktop app on Mac had styling issues and locked movement. This is resolved with an improved design.
PID-1953	The uninstall process on the Apple Mac platform has been fixed to remove all of the files from the PingID desktop app installation.
PID-2179	The PingID desktop app was not starting up, as a result of a ghost process after a process crash.
PID-2262	The memory consumption of the PingID desktop app running in the background over several hours was growing. This has been resolved by tuning the JVM threshold to reduce memory usage.

Known issues and limitations

PingID desktop app on VMs running OS X

- On VMs running OS X as a guest operating system, the PingID desktop application cannot run, and should not be used in these VM environments.

Antivirus may block PingID desktop app installation without alerting

- On a Windows 10 PC, running Avast antivirus, there was no response when launching the PingID desktop app installer, and no alert.
- Temporarily disabling the antivrus permitted normal installation of the PingID desktop app.
- The antivirus was investigated: Its status indicated "Everything up to date". Deeper inspection revealed that although the engine and database were up to date, there was a newer release of the program available.
- After updating the program, on launching the PingID installer, the antivirus alerted that it was running a 15 second check for malware. Following its check, the PingID desktop app installation proceeded normally.

PingID integration for Windows login

PingID integration for Windows login 2.12 (June 10, 2025)

New features and improvements in PingID integration for Windows login.

Detection of additional credential providers

Improved PingID Integration for Windows login

During the installation of the integration with Windows login, PingID now detects existing credential providers that could be incompatible and provides a warning to this effect.

Authentication grace period

New PingID Integration for Windows login

When using the CLI-based installation of the integration with Windows login, you can now define a period following authentication during which the user isn't asked to authenticate again if they lock their computer. Learn more in Installing the PingID integration for Windows login using CLI.

Signing on with SAM Account Name

Improved PingID Integration for Windows login

When installing the PingID integration with Windows login with the UI or CLI-based installation, you can now specify that only the user's SAM Account Name is required for identification. Learn more in Installing the PingID integration for Windows login using UI wizard and Installing the PingID integration for Windows login using CLI.

Support for multiple connected FIDO2 devices

Improved PingID Integration for Windows login

The PingID integration with Windows login can now handle situations where multiple FIDO2 devices are connected simultaneously.

RDP failure when both Windows login integration and passwordless Windows login integration are installed

Fixed TRIAGE-24837 PingID Integration for Windows login

When both the standard PingID integration with Windows login and the passwordless PingID integration with Windows login were installed on the same computer, there were cases where attempts to establish an RDP connection with another computer failed. This issue has been fixed.

Security enhancements

Security PingID Integration for Windows login

We've added a number of security enhancements.

PingID integration for Windows login 2.11 (February 21, 2024)

New features and improvements in PingID integration for Windows login.

ARM-based Windows PC Support

Improved PingID Integration for Windows login

We've added the option to install the Windows Login client on Windows PCs that are powered by ARM processors.

Support for multiple security keys

Improved PingID Integration for Windows login

When multiple security keys are connected to the same Windows machine, the user can now select the security key they want to use to authenticate, without needing to remove other security keys that are connected.

Correction to Dutch translation

Fixed STAGING-18749 PingID Integration for Windows login

The Dutch version of the message displayed to the user when authenticating with a QR code was missing the translation of the term **Manual Auth**. This issue has been fixed.

PingID integration for Windows login 2.10.2 (November 21, 2023)

New features and improvements in PingID integration for Windows login.

Security key devices not detected when an NFC reader is also present

Fixed STAGING-20908 PingID

In some circumstances, security key devices were not detected during authentication. This issue is now fixed.

PingID integration for Windows login 2.10.1 (September 18, 2023)

New features and improvements in PingID integration for Windows login.

Issue using smartcard reader

Fixed STAGING-20067 PingID

Fixed an issue that was preventing some users from using an NFC SmartCard reader with PingID Integration for Windows login 2.10.

PingID integration for Windows login 2.10 (June 6, 2023)

New features and improvements in PingID integration for Windows login.

NFC reader support

Improved PingID Integration for Windows login

Windows login now supports authentication using an NFC reader.

Windows login support of Windows locale settings

Improved PingID Integration for Windows login

PingID Integration for Windows login can now use the user-defined language setting as its default language. If multiple users are registered on the device, PingID can identify and use the language (user locale) associated with each individual user on the machine. NOTE: If the user-defined language is not supported by Windows Login, the fallback language is English.

OAEP Padding as default

Improved PingID Integration for Windows login

OAEP padding is now used as the default padding scheme with RSA encryption for offline authentication.

If you do not want to use OAEP padding for offline authentication, use the `rsa_padding` option when running the CLI installation. For information, see Installing the PingID integration for Windows login using CLI.

Security enhancements

Security PingID Integration for Windows login

We've made various security enhancements.

Support for Windows 32-bit

Info PingID Integration for Windows login

PingID Integration for Window login no longer supports Windows 32-bit Windows platforms.

Fixed an issue with Winlogon when FIPS-compliant algorithms enforced

Fixed PIM-4561 PingID Integration for Windows login

We've fixed an issue that was causing Winlogon to hang when requesting that users enter a PIN code. This issue affected for users for which FIPS compliant algorithms were enforced on their Windows machine.

PingID integration for Windows login 2.9 (January 3, 2023)

Windows login proxy settings auto-detection and PAC file support

Improved PingID Integration for Windows login

We've enhanced the Windows login proxy configuration options, to include auto-detection of proxy settings. We've also added support for the use of Proxy Auto-Configuration (PAC) file.

For information, see Installing the PingID integration for Windows login.

Apply Windows login to specific accounts

Improved PingID Integration for Windows login

We've added the ability to select to which accounts you want to apply PingID (Microsoft, or Local). This is in addition to domain accounts, which are included by default.

For information, see Installing the PingID integration for Windows login.

User Verification discouraged support for security keys

Improved PingID Integration for Windows login

To reduce friction to the user authentication flow, we've added the option to skip user verification for Windows login users.

Language support

Improved PingID Integration for Windows login

We've added support for the following languages:

- Czech
- Polish
- Hungarian

Specify username attribute

Security PingID Integration for Windows login

We've added the option to specify the attribute you want to use to verify users with Active Directory. This feature resolves a security issue. This feature resolves the security issue CVE-2022-23721.

Fixed an issue with Windows installer

Fixed PIM-3529 PingID Integration for Windows login

Fixed an issue that sometimes caused the window installer to fail during an upgrade.

Fixed an issue with Windows login security keys for RDP

Fixed PID-12640 PingID Integration for Windows login

Fixed an issue that was causing the WL offline security keys to be deleted from the registry when signing on using RDP (Remote Desktop).

PingID integration for Windows login 2.8.4 (August 22, 2022)

Windows login installer and /NORESTART parameter

Fixed STAGING-15722 PingID Integration for Windows login

Fixed an issue with the windows login CLI installation, that was affecting the /NORESTART parameter.

Windows login installer with proxy configured

Fixed PIM-3134 PingID Integration for Windows login

Fixed an issue that was preventing the Windows login installation from completing successfully when a proxy is configured.

PingID integration for Windows login 2.8.3 (June 21, 2022)

Authentication request despite Recent Authentication rule in policy

Fixed STAGING-15722 PingID Integration for Windows login

In version 2.8, when Windows login was integrated with PingID directly (not through PingFederate), there were situations where users would be asked to authenticate even though the defined Recent Authentication rule in the authentication policy should have prevented an authentication prompt.

Windows login verifies PingID properties file

Fixed PIM-3134 PingID Integration for Windows login

Beginning with version 2.8, you must use the restricted-permissions properties file that is generated when you click the **Generate** button in the **Integrate with Windows and Mac login** section. You can no longer use the properties file that is generated when you click the **Generate** button in the **Integrate with PingFederate and other clients** section. This resolves issues related to CVE-2022-23717.

Removed Windows login local privilege escalation

Fixed PIM-2897 PingID Integration for Windows login

Windows Login local privilege escalation to System account is now removed. This resolves issues related to CVE-2022-23719.

Additions to the Authentication Browser

Fixed PIM-2898 PingID Integration for Windows login

Offline HTML and JS files are now added to the Authentication Browser (similar to these employed by Authenticator Browser for Online login flow) . This resolves issues related to CVE-2022-23717.

Chromium upgrade

Fixed PID-9964 PingID Integration for Windows login

Chromium is now upgraded in Windows Login. This resolves issues related to CVE-2022-23718.

Restricted access to the properties file in the registry

Fixed PID-3315 PingID Integration for Windows login

Fixed an issue related to restricting access to the properties file in the registry. This resolves issues related to CVE-2022-23725.

PingID integration for Windows login 2.8.2 (June 15, 2022)

Fixed authentication issue for integration through PingFederate

Fixed STAGING-15655 PingID Integration for Windows login

In version 2.8, when Windows login was integrated with PingID through PingFederate, there were situations where authentication would fail.

PingID integration for Windows login 2.8 (May 31, 2022)

Security keys (offline) - improved implementation

Improved PingID Integration for Windows login

An improved implementation has been introduced for the use of security keys while offline - they are now synced from the PingID server. The installation program for the integration now includes options that allow you to indicate how PingID should relate to security keys that were added using the previous approach. For details, see Installing the PingID integration for Windows login using CLI.

The new implementation also makes it possible to use security keys with user verification in offline mode (previously this was only supported for online authentication).

Security enhancements

Security PingID Integration for Windows login

This version of the integration with Windows login includes fixes for five security-related issues.

PingID integration for Windows login 2.7 (January 25, 2022)

Enhancements

Use of OAEP padding for offline authentication

The command-line installation now includes an option to specify that OAEP padding should be used in the encryption for offline authentication. For information on setting this option, see Installing the PingID integration for Windows login using CLI.

Security keys with user verification

The existing support for security keys has been expanded to include security keys with user verification, such as keys with fingerprint readers.

Resolved issues

Ticket ID	Description
PIM-2558	There were cases where the PingID integration with Windows login stopped working after removal of Office 365. This issue has been resolved.

PingID integration for Windows login 2.5.2 (September 22, 2021)

Enhancements

Bypass proxy for communication with PingFederate

The installation process for the Windows login integration now includes an option to have communication with PingFederate bypass the proxy that you specified. For details, see Installing the PingID integration for Windows login using UI wizard and Installing the PingID integration for Windows login using CLI.

Security and reliability

Improvements to security and reliability

PingID integration for Windows login 2.5.1 (January 26, 2021)

Enhancements

Security and reliability

Improvements to security and reliability

Resolved issues

Ticket ID	Description
PID-10719	Fixed an issue that was causing an extended delay when waiting for Windows login to enter offline mode due to an unstable connection.
PID-10767	Fixed an issue that was preventing some proxies with basic authentication from working as expected.
PID-10778	Fixed an issue in PingID integration for Windows login 2.5.0 that was preventing some users signing in to Windows when the Windows Profiling Environment is enabled.

PingID integration for Windows login 2.5 (October 19, 2020)

Enhancements

Security and reliability

Improvements to security and reliability

Resolved issues

Ticket ID	Description
PID-9618	Fixed an issue when logging in to Windows in which leading or trailing spaces inserted in Username field were not being truncated.
PID-10449	Fixed a spelling error in the Client ID attribute in the OIDC request object. This is relevant when integrating PingID through PingFederate.

PingID integration for Windows login 2.4.2 (August 25, 2020)

Enhancements

PingID integration for Windows login through PingFederate

Streamline your organization's Windows login experience with PingFederate's cross organization authentication policies. You can now configure PingID credential provider to proxy through PingFederate before it accesses the PingID service, so your users can benefit from PingFederate's authentication capabilities. Example use cases include: username mapping from Window login to your LDAP directory, creating group based policies (PingFederate and PingID) and integrating on-premise or third-party authentication methods into the authentication flow.

For more information, see Integrating PingID with Windows login.

Enable co-existence (on the same machine) of PingID credential provider and third party credential providers:

We've added the following capabilities:

- Out-of-the-box MFA integration with McAfee Drive Encryption credential provider.

  For more information see the `thirdPartyCredentials` parameter in Installing the PingID integration for Windows login using CLI.

- Support for third party credential providers.

  You can now enable one or more credential providers (such as CiscoAnyConnect) to work in parallel with the PingID credential provider (exclude them from being filtered out by PingID integration with Window Login). It is recommended that you check PingID credential provider can operate successfully on a machine that includes all of your third party credential providers, before you roll out PingID Integration for Windows Login.

  For more information see the `CPWhitelist` parameter in Installing the PingID integration for Windows login using CLI.

Ability to configure HTTP request timeout value:

We've added the option to configure a HTTP request timeout value for PingID authentication with Windows login. The value can be in the range of 1sec - 30 sec. The parameter can be defined when installing PingID integration for windows login through the CLI.

We've also changed the default HTTP request timeout value from 30 sec to 10 sec.

Note: The value configured for HTTP timeout applies to heartbeat checks, and does not influence the timeout value of the embedded browser requests.

For more information, see the `HttpRequestTimeout` parameter in Installing the PingID integration for Windows login using CLI.

Resolved issues

Ticket ID	Description
PID-9402	Fixed an issue that was causing Windows login to attempt to access a dummy URL following log in to Windows.
PID-9368	Fixed an issue that was causing the PingID credential provider to consider a domain user account to be a Microsoft account in some cases.
PID-10111	Fixed an issue that was causing third party credential providers to be filtered out within a remote desktop connection.
PID-9404/PID-9447	Fixed security issues.
PID-10292	Fixed an issue with the Proxy configuration settings that was causing a problem when registering Security Keys for offline authentication.
PID-10258	Resolved an issue that was causing the service connection timeout to be longer than the default timeout value in certain cases.

PingID integration for Windows login 2.3.1 (January 28, 2020)

Enhancements

PingID integration for Windows login v2.3.1 supports TLS 1.2

To align with industry best practices and standards for security and data integrity, Ping Identity added support for TLS 1.2 in PingID integration for Windows login v2.3.1. Over the coming months, PingID integration for Windows login client versions 2.3 and lower (that support only TLS 1.1 and lower in the PingOne for Enterprise platform) will no longer allow MFA integration.

We advise all Admins to upgrade to the latest version as soon as possible.

PingID integration for Windows login 2.3 (December 3, 2019)

Enhancements

PingID integration for Windows login supports use of FIDO security key for PingID offline MFA

FIDO2 and U2F compatible security keys can now be used to access Windows login when offline. The security key must be paired specifically for offline MFA.

See the following topics:

- (Legacy) Configuring the FIDO2 security key for PingID
- Installing the PingID integration for Windows login
- Using a security key (FIDO2) for authentication in the PingID End User Guide.

Resolved issues

Ticket ID	Description
PID-7935	Fixed UI issues in the PingID Integration for Windows login installer.
PID-8807	Fixed an issue that was sometimes preventing users from logging into Windows Server via RDP.

PingID integration for Windows login 2.2 (April 08, 2019)

Enhancements

PingID support for FIDO2 Security Keys extended to Windows login

FIDO2 and U2F compatible security keys enable relying parties to offer a strong cryptographic second factor option for end user security, and to take advantage of the security benefits of FIDO2 technology. PingID now supports FIDO2 and U2F security keys for authentication with Windows login.

See (Legacy) Configuring the FIDO2 security key for PingID, in the PingID Admin Guide and Using a security key (FIDO2) for authentication in the PingID User Guide.

Support for Windows Login authentication when using multiple domains

You can now enable support for multiple domains. When enabled, this feature allows users to log in to a domain that was not specified during installation.

Resolved issues

Ticket ID	Description
PID-6263	Fixed an issue that was forcing case sensitive login when logging on to Windows login via RDP using offline authentication flow.
PID-7639	Fixed an issue that was causing Windows login to count a single failed login attempt as two failed login attempts.

Known issues and limitations

Authentication via security key not permitted for Window Login via RDP

It is not possible to authenticate with a security key when accessing Windows Login via Remote Desktop, due to current limitations with FIDO2.

Trust domain relationship failure may prevent login to Windows

In the event of a trust domain relationships failure, in some cases, after successful second factor authentication, the user may see an ERROR_TRUSTED_RELATIONSHIP_FAILURE error and may not be able to access their account.

Second factor authentication with PingID for Windows Hello

Microsoft does not currently support the addition of second factor authentication when using the Windows Hello biometric login flow.

- For PingID for Windows Login v2.2 integration and higher, if Windows Hello biometric authentication is enabled, users can either:
  - Log in using Windows Hello biometric authentication only.
  - Authenticate with their username and password. When authenticating with username and password, PingID can be used for second factor authentication.
- PingID for Windows Login v2.1 and lower does not support authentication with Windows Hello when Windows Hello is in biometrics mode.

PingID integration for Windows login 2.1 (January 31, 2019)

Enhancements

PingID Integrates with Microsoft Windows Server 2019

PingID Integration has been tested and certified for correct operation under Microsoft Windows Server 2019.

PingID integration for Windows login 2.1 (December 27, 2018)

Enhancements

Policy may be applied to Windows login and RDP

Windows Login and RDP integration may now be subject to policy settings. To configure policy for Windows Login/RDP, see Enabling a Windows login and RDP authentication policy.

Turkish language support added

This completes system-wide Turkish support.

PingID integration for Windows login 2.0 (March 28, 2018)

Enhancements

PingID integration for Windows login for Workforce

Organizations can now further enhance security by extending MFA to end users logging into Windows desktops and laptops. This includes a new client key limiting end users to authentication actions, and the ability to authenticate even when end user devices are offline using the PingID mobile application.

FIPS mode support

PingID integration for Windows now supports Windows running in FIPS mode.

Resolved issues

Ticket ID	Description
PID-5277	A case was discovered where a remote user started a session and closed the window before PingID integration for Windows completed the MFA process. This resulted in the local user at next login being presented with the MFA screen, displaying the point where the previous remote user left off. The local user was then unable to end the process, close the window, or progress in any way. This issue has been resolved.

Known issues and limitations

Admin message is not displayed on blocked screen when user is unpaired

When the bypassPolicy of PingID integration for Windows is configured to block user login, the admin message will not be displayed to users who do not have any paired devices and who are attempting to perform offline MFA (when the connection with the PingID server can't be verified at the time of login).

Username is case sensitive in offline MFA

In cases of offline MFA for RDP using the NLA method, it is important to note that username submitted is case sensitive.

PingID integration for Windows login (January 2018)

Enhancements

Windows Login reduced permissions properties file

PingID now provides a PingID properties file with client keys that have reduced permissions for Windows Login users. If you'll be distributing your properties file widely to Windows Login clients that are not within your control, use the Windows Login properties file to limit user permissions to authentication actions only.

PingID integration for Windows login 1.3 (October 2017)

Enhancements

TLS support in PingID integration for Windows login

PingID integration for Windows login now supports TLS 1.0, TLS 1.1 and TLS 1.2, as well as support upgrade from older versions.

Resolved issues

Ticket ID	Description
PID-5184	A case was discovered where disabling TLS 1.0 prevented PingID integration for Windows login from reaching the PingID service. This has been resolved.
PID-5192	A rare case was discovered where a user was prompted for PingID MFA when logging in to a server on which PingID integration for Windows login is installed, and was prompted again for PingID MFA when RDPing from that server to a different server on which PingID integration for Windows login is not installed. This is now resolved.

PingID integration for Windows login 1.2 (September 2017)

Resolved issues

Ticket ID	Description
PID-5297	A case was discovered where the PingID Windows login was configured to bypass the local login, and it also allowed users of a group lacking local login permissions to complete a local login. This issue is now resolved.

PingID integration for Windows login 1.0 (August 2016)

Enhancements

PingID secures local and remote access to Windows servers

PingID integration for Windows login has been released as a generally available feature. It provides a step up authentication to users logging into Windows server machines with the familiar PingID flow. This includes on the fly pairing, PingID's wide range of authentication methods, and co-branding as with the standard SSO MFA flow.

PingID formally supports and has been verified only with Windows password Credential Provider (CP) as the 1st factor authentication. PingID integration for Windows login is intended only for implementations of Windows machines performing as servers, due to offline limitations. If you wish to extend its use for other default Windows CPs or to client machines as well, please contact your PingID rep.

Known issues and limitations

PIN code is not supported on Windows 10

Windows 10 does not support PIN code authentication. Refer to the following thread in the Microsoft community: https://social.msdn.microsoft.com/Forums/en-US/1b960a8a-7e21-4d64-875a-a73cfc716bd6/ngc-credential-provider-on-windows-10-crashes-inside-setstringvalue-when-wrapped?forum=windowssecurity

Possible delay loading the browser for MFA, after Windows login

After rebooting the server, there may be a 10 to 15 second delay loading the embedded browser for 2nd factor authentication, after Windows login. This symptom is due to the startup launch of services, and is more prevalent on Windows 7 than on later Windows versions.

PingID integration for Windows login (passwordless)

PingID integration for Windows login (passwordless) 1.7 (June 3, 2025)

New features and improvements in PingID integration for Windows login.

Number matching support

New PingID integration for Windows login

Windows login passwordless authentication now includes support for number matching using the PingID mobile app. This requires PingID mobile app 2.4 or later.

Push notification limits for Windows login passwordless

Improved PingID integration for Windows login

A push notification limit is now applied automatically to Windows login passwordless authentication flows. After three failed or canceled sign-on attempts, the user is temporarily blocked for 2 minutes.

Enhancements to security, performance, and reliability

Improved PingID integration for Windows login

We've made various enhancements to security, performance, and reliability.

Issue signing on when using local admin rights

Fixed TRIAGE-23924 PingID integration for Windows login

We've fixed an issue that was preventing administrators from signing on using Windows login passwordless authentication when signing on to a machine using local administrator rights.

Authentication canceled when clicking outside the authentication window

Fixed TRIAGE-23422 PingID integration for Windows login

We've fixed an issue that was causing the authentication process to be canceled when clicking outside of the authentication window during authentication.

PingID integration for Windows login (passwordless) 1.6.1 (Jun 20, 2024)

New features and improvements in PingID integration for Windows login.

Issue using WebAuthn within a browser on Windows 10 and Windows 11 machines

Fixed STAGING-23313 PingID Integration for Windows login

We've fixed an issue that was preventing users from pairing or authenticating WebAuthn credentials from a browser, when using a Window 10 or Windows 11 machine that has Windows login passwordless 1.5.1 or 1.6 installed.

PingID integration for Windows login (passwordless) 1.6 (May 28, 2024)

New features and improvements in PingID integration for Windows login.

Scan manual authentication QR code using native phone camera

New PingID Integration for Windows login

It's now possible to scan the manual authentication QR code from the user's native device camera. When the user scans the manual authentication QR code with their device camera, PingID mobile app opens automatically, displaying the manual authentication key. This option is in addition to the existing option to scan the QR code from within the app.

This option requires PingID mobile app 2.3 or later, and is disabled by default. For information about how to enable it, see Installing passwordless Windows Login integration on client computers.

FIDO2 support

Improved PingID Integration for Windows login

PingID Windows login passwordless provides FIDO2 support for PingID environments that are integrated with PingOne. Learn more: Updating a PingID account to use PingOne FIDO2 policy for Passkey support.

Support for additional languages and text using Portable Object (PO) translations

New PingID Integration for Windows login

PingID Windows login passwordless now supports Portable Object (PO) translations for localized user interfaces. PO translations must be compiled into .mo files and stored in the locale folder within the application's bin directory, usually found at `C:\Program Files\Ping Identity\PingID\Windows Passwordless\bin\locale`.

Security and performance enhancements

Security PingID Integration for Windows login

This version of PingID integration for Windows login passwordless authentication includes improvements and fixes for security and performance-related issues.

Issue accessing resources on a shared network using passwordless authentication

Fixed STAGING-21497 PingID Integration for Windows login

We've fixed an issue that was preventing users from using passwordless authentication to access a shared resource or network share.

PingID integration for Windows login (passwordless) 1.5.1 (February 6, 2024)

New features and improvements in PingID integration for Windows login (passwordless).

Support for Local Security Authority (LSA)

Improved PingID Integration for Windows login

The integration for passwordless Windows login now includes support for Local Security Authority (LSA).

PingID integration for Windows login (passwordless) 1.5 (October 30, 2023)

New features and improvements in PingID integration for Windows login.

Default to Primary behavior support for compatible devices

Improved PingID Integration for Windows login

Windows Login Passwordless client now supports the **Default to Primary** option. The user is now only prompted to select a device if their primary device is not compatible with the Windows Login Passwordless client.

Automatic native language detection

Improved PingID Integration for Windows login

Windows Login Passwordless client automatically detects and switches to the language that is configured on the user's Windows machine.

CTAP library upgrade

Improved PingID Integration for Windows login

To enhance the performance of FIDO security keys within the Windows Login Passwordless client, we've upgraded the Client to Authenticator Protocol (CTAP) library. The CTPA library now complies with the latest FIDO2 (v2.1) specifications.

Support for multiple security keys

Improved PingID Integration for Windows login

When multiple security keys are connected to the same Windows machine, the user can now select the security key they want to use to authenticate, without needing to remove other security keys that are connected to the same Windows machine.

ARM-based Windows PC Support

Improved PingID Integration for Windows login

We've added the option to install the Windows Login Passwordless client on Windows PCs that are powered by ARM processors.

Security and performance enhancements

Security PingID Integration for Windows login

This version of PingID integration for Windows login passwordless authentication includes improvements and fixes for security and performance-related issues.

PingID integration for Windows login (passwordless) 1.4 (July 25, 2023)

New features and improvements in PingID integration for Windows login.

New events in Windows Event viewer

Improved PingID Integration for Windows login

We've added some Windows login passwordless-related events to the Windows Event viewer.

The new events provide administrators with user event information including online and offline authentication, failed login attempts, and RDP authentication attempts.

For information, see Troubleshooting passwordless Windows login

Windows login passwordless RDP support

Improved PingID Integration for Windows login

The Windows login passwordless remote desktop (RDP) sign-on process has been improved and now requires only one authentication request.

OAEP Padding as default

Improved PingID Integration for Windows login

OAEP padding is now used as the default padding scheme with RSA encryption for offline authentication.

If you do not want to use OAEP padding for offline authentication, use the `rsa_padding` option when running the CLI installation. For information, see Installing passwordless Windows Login integration on client computers (CLI).

NFC reader support

Improved PingID Integration for Windows login

Windows login passwordless now supports authentication using an NFC reader.

User Verification discouraged support for security keys

Improved PingID Integration for Windows login

We've added the option to skip user verification for Windows login passwordless users. This requires the relevant flag to be added as an optional parameter during installation.

> **Note**
>
> Some YubiKey devices require user verification, and will not allow the user to authenticate if the user verification discouraged flag is enabled.

For information, see Installing passwordless Windows Login integration on client computers (CLI)

Security and performance enhancements

Security PingID Integration for Windows login

This version of PingID integration for Windows login passwordless authentication includes improvements and fixes for security and performance-related issues.

Security key sign on issue

Fixed STAGING-19029 PingID Integration for Windows login

We've fixed an issue that was preventing users from signing on with a security key when the computer language was set to a non-English language.

Offline authentication issue

Fixed STAGING-19029 PingID Integration for Windows login

We've fixed an issue that was preventing users from attempting to sign on while offline, if their first offline authentication attempt failed.

PingID integration for Windows login (passwordless) 1.3 (November 3, 2022)

New features and improvements in PingID integration for Windows login passwordless authentication.

Support for ECC key pairs

Improved PingID Integration for Windows login

To improve the performance of the Windows login passwordless client, we've added support for ECC key pairs for passwordless authentication. For more information see Command-line installation Installing passwordless Windows Login integration on client computers (CLI).

Language support

Improved PingID Integration for Windows login

We've added support for the following languages:

- Czech
- Polish
- Hungarian

Security and performance enhancements

Improved PingID Integration for Windows login

This version of the integration with Windows login for passwordless authentication includes improvements and fixes for security and performance-related issues.

PingID integration for Windows login (passwordless) 1.2 (June 28, 2022)

New features and improvements in PingID integration for Windows login passwordless authentication.

Passwordless login with FIDO2 security keys

Improved PingID Integration for Windows login

- Beginning with this release, it is possible to carry out passwordless Windows login in conjunction with a FIDO2 security key. (If you set the **Resident Key** option to Required for such keys, users will not neeed TPM on their computer in order to use passwordless login.)
- A mechanism has been added to make it easier to change the level of detail recorded in the log files. For details, see Troubleshooting passwordless Windows login.
- The release also includes a number of security enhancements and performance improvements.

PingID integration for Windows login (passwordless) 1.0 (December 9, 2021)

PingID integration for Windows login passwordless authentication.

Initial version.

PingID integration for Mac login

PingID integration for Mac login 1.3.4 (May 8, 2025)

May 8

Submit button on Manual Authentication screen

Fixed PIM-7335

The Submit button on the Manual Authentication screen was mislabeled. This issue has been fixed.

Recent authentication rule ignored

Fixed TRIAGE-26595

There were situations where users were being asked to authenticate with PingID on each login even though the policy was set to "Approve" if the last authentication was less than twelve hours ago. This issue has been fixed.

PingID integration for Mac login 1.3.3 (March 19, 2024)

Manual Authentication options in UI-based installation

Fixed PingID

The MFA behavior when users could not communicate with the PingID server did not always match the option that was selected in the **Manual Authentication** window of the UI-based installation of the integration with Mac login. This issue has been fixed.

PingID integration for Mac login 1.3.2 (January 17, 2024)

Width of unlock screen on macOS 14.1 (Sonoma)

Fixed STAGING-21669 pingid

On version 14.1 of macOS, the unlock screen was displayed as a narrow window rather than taking up the full width. This issue has been fixed.

Security, performance, and reliability

Improved pingid

Improvements to security, performance, and reliability.

PingID integration for Mac login 1.3.1 (December 6, 2023)

Installation - skip domain validation

New pingid

By default, domain validation is carried out if you specify an organization domain during installation. There is now an option to skip domain validation (available in both UI and CLI installation). For details, see Installing PingID integration for Mac login using UI wizard.

Black screen after device locked with screensaver active

Fixed STAGING-19800 pingid

On certain versions of macOS, after the device was locked with a screensaver active, there were cases where a black screen was displayed rather than the login screen. This issue has been fixed.

Security, performance, and reliability

Improved pingid

Improvements to security, performance, and reliability.

PingID integration for Mac login 1.3.0 (August 2, 2023)

New installation options - attribute mapping, exclude local users

New PingID

When installing the integration with Mac login, you can now specify that an Active Directory attribute should be used for identifying users. You can also specify that PingID authentication should not be used for local user logins. For details, see Installing PingID integration for Mac login using UI wizard and Mac login command line reference.

No authentication prompt after CLI installation

Fixed STAGING-19298 PingID

There were cases where users were not getting an authentication prompt when logging back in to their Mac after carrying out a command-line installation of the integration that included use of the `--domainPostfix` parameter. This issue has been fixed.

Login failure after providing organization domain in UI installation

Fixed STAGING-19762 PingID

There were cases where users could not log in after carrying out a UI installation of the integration that included specification of an organization domain. This issue has been fixed.

PingID integration for Mac login 1.2 (February 14, 2023)

Use of OAEP padding for offline authentication

Info PingID

OAEP padding is now used by default in the encryption for offline authentication. If you do not want to use OAEP padding for offline authentication, use the `--rsa_padding` option when running the command-line installation. For details, see Mac login command line reference.

Installation verifies PingID properties file

Security PingID

Beginning with version 1.2 of the integration, you must use the restricted-permissions properties file that is generated when you click the **Generate** button in the **Integrate with Windows and Mac login** section. You can no longer use the properties file that is generated when you click the **Generate** button in the **Integrate with PingFederate and other clients** section. This resolves issues related to CVE-2022-23717.

PingID integration for Mac login 1.1.2 (November 29, 2022)

WiFi selection icon on lock screen

New PingID Integration for Mac login

To prevent situations where a user cannot log in because their computer is not currently connected to the Internet, the lock screen now contains a WiFi icon that can be clicked to select a network.

Language support

Improved PingID Integration for Mac login

We've added support for the following languages:

- Czech
- Polish
- Hungarian

Login failure after screen lock

Fixed PIM-3884 PingID Integration for Mac login

Fixed an issue that was causing login attempts to fail after the screen was locked.

PingID integration for Mac login 1.1.1 (July 6, 2022)

Support for Monterey

New PingID Integration for Mac login

The integration with Mac login can now be used on Monterey (versions 12.4 and above).

Integration users who have upgraded to Monterey

Info PingID Integration for Mac login

If users who installed the integration with Mac login on a previous version of macOS encounter problems with PingID after upgrading to Monterey (version 12.4 or above), they should run the script that is included in this release of the integration to fix the problem. The script, `RestoreAfterUpgrade.sh`, is included in the .dmg file that is provided.

PingID integration for Mac login 1.1 (May 31, 2022)

Multi-factor authentication for lock screen

New PingID Integration for Mac login

After you install the PingID integration for Mac login, multi-factor authentications is now required not just for the initial login, but also for logging in when the lock screen is displayed.

Use of OAEP padding for offline authentication

New PingID Integration for Mac login

There is now an option to specify that OAEP padding should be used in the encryption for offline authentication. For information on setting this option, see Installing the PingID integration for Mac login.

Versions of macOS supported

Info PingID Integration for Mac login

Beginning with this release, the PingID integration with Mac login is not supported on macOS 10.13 (High Sierra) and 10.14 (Mojave).

PingID integration for Mac login 1.0.3 (November 30, 2021)

Resolved issues

Ticket ID	Description
STAGING-13381	If a user closed the PingID authenticator window before authentication was completed, they were not returned to the initial Mac login screen as would be expected. This issue has been resolved.

PingID integration for Mac login 1.0.2 (February 09, 2021)

Enhancements

Four new CLI options are available:

Option	Description
ignoreConnectionErrors	The installer attempts to address the PingID authenticator heartbeat to confirm connectivity. The installer will continue the installation even if no response was received.
silent	Upon completion of the instal, the installer will prompt with a **Log out now?** message box.
very-silent	Upon completion of the instal, the installer will automatically log out.
timeout	Defines HTTP request timeout value. Permisible values are in the range 1000-30000 ms.

Run the CLI using --help for a full options list. Also, see the CLI Reference Mac login command line reference

PingID integration for Mac login 1.0.1 (October 27, 2020)

Resolved issue

Adding the organization domain in the CLI could result in the user name differing from the previously enrolled user name causing a pairing issue. i.e. johndoe@domain (CLI) is not the same as johndoe (enrolled).

The command-line installer does not explicitly ask for organization domain anymore.

PingID integration for Mac login 1.0 (September 02, 2020) (updated)

Enhancements

PingID support for Mac login

PingID Integration for Mac login has been released as a generally available feature. The Mac login agent implements an extra security layer by enforcing MFA to the login flow. Admins can install the Mac login agent using a GUI or a CLI.

For configuration details, see: PingID integration for Mac login

See also, the PingID end user guide: PingID authentication for Mac login

Known issues and limitations

The Big Sur OS is not supported.

PingID MFA Adapter for AD FS

PingID MFA Adapter for AD FS 1.4 (March 29, 2021)

Enhancements

Version 1.4 of the PingID MFA Adapter for AD FS has been released, and includes the following enhancements:

- Official support for AD FS 5.0.
- The adapter management interface in MMC now allows you to specify a PingID-specific proxy.
- For situations where the users belong to a domain that is not reflected in the login information provided, the adapter management interface in MMC now allows you to provide the relevant domain name.

See Configuring advanced settings.

PingID MFA Adapter for AD FS 1.3.2 (February 24, 2020)

Enhancements

PingID MFA Adapter for AD FS v1.3.2 supports TLS 1.2

To align with industry best practices and standards for security and data integrity, Ping Identity added support for TLS 1.2 in AD FS v1.3.2. Over the coming months, PingID MFA Adapter for AD FS client versions v1.2 and lower (that support only TLS 1.1 and lower in the PingOne for Enterprise platform), will no longer allow MFA integration.

We advise all Admins to upgrade to the latest version as soon as possible.

Resolved issues

Ticket ID	Description
PID-9323	Fixed an issue that was causing failures in PingID authentication flows when using Internet Explorer and Microsoft Edge browsers.

PingID MFA Adapter for AD FS 1.3.1 (January 28, 2020)

Enhancements

PingID MFA Adapter for AD FS v1.3.1 supports TLS 1.2

To align with industry best practices and standards for security and data integrity, Ping Identity added support for TLS 1.2 in AD FS v1.3.1. Over the coming months, PingID MFA Adapter for AD FS client versions v1.3 and lower (that support only TLS 1.1 and lower in the PingOne for Enterprise platform), will no longer allow MFA integration.

We advise all Admins to upgrade to the latest version as soon as possible.

PingID MFA Adapter for AD FS 1.3 (December 19, 2019)

Enhancements

AD FS Adapter for PingID V1.3 - Support for Chrome SameSite cookie behavior change

Support for Chrome SameSite cookie behavior change has been implemented.For all Ping products SameSite support details, see SameSite cookie support in Ping Identity products.

PingID MFA Adapter for AD FS 1.2 (July 2, 2019)

PingID MFA Adapter for AD FS v1.2

A new version of the PingID MFA Adapter for AD FS is available that resolves PID-8233.

Resolved issues

Ticket ID	Description
PID-8233	Resolved an issue that was causing intermittent authentication failures in AD FS adapter v1.1 and older.

PingID MFA Adapter for AD FS 1.1 (November 19, 2018)

Enhancements

PingID MFA Adapter for AD FS v1.1

A new version of the PingID MFA Adapter for AD FS is available that provides the following enhancements:

- **Support for multiple claim types**

  You can now choose the claim type you want to send from AD FS to the PingID MFA Adapter (UPN or Windows Account Name) when installing PingID MFA Adapter for AD FS (see Installing PingID MFA Adapter for AD FS).

- **Support for multi-domain environments**

  PingID MFA Adapter for AD FS can now query user data originating from multiple Active Directory domains, based on the user claim presented to the PingID MFA Adapter during authentication.

Resolved issues

Ticket ID	Description
PID-7242	Resolved an issue that was preventing log entries related to the PingID MFA Adapter for AD FS from printing to the event viewer.
PID-7081	Resolved an issue that was preventing admins from applying PingID group-based policy during authentication with AD FS.
PID-7080	Resolved an issue that was preventing modification of the username attribute mapping.

PingID MFA Adapter for AD FS 1.0 (September 20, 2018)

Enhancements

PingID Adapter for AD FS

The new PingID MFA Adapter for AD FS v1.0 is available for general release. This adapter allows you to secure your sign-in process using Microsoft AD FS by integrating with PingID MFA and its strong authentication capabilities.This integration allows AD FS customers to utilize PingID MFA with all PingID authentication methods (including Swipe, Fingerprint, SMS, Voice, YubiKey, Email, Desktop app) and to apply PingID policies to AD FS MFA authentication

PingID SSH integration

PingID SSH Integration 4.3.0 (May 30, 2024)

Proxies that require username and password

New PingID SSH integration

Support for proxy servers has been expanded so that you can now use the PingID integration with SSH also for proxy servers that require username/password authentication.

PingID SSH Integration 4.2.0 (December 21, 2021)

Enhancements

Obfuscation of use_base64_key field in PingID properties file

When installing the SSH integration from source files, there is now an option to specify that the `use_base64_key` field in the PingID properties file should be obfuscated, rather than leaving it as a plain text file. To use this option, include the `--with-obfuscation` switch when running the configuration utility. For details, see Installing PingID SSH using source files.

Offline MFA

There is now an option to enable offline MFA for situations where the PingID MFA service is unavailable. For details, see Enabling offline MFA in SSH integration.

Support for additional releases

The PingID integration with SSH can now be installed on Debian 10 and Ubuntu 16.04, 18.04, and 20.04.

PingID SSH Integration 4.1.1 (May 11, 2021)

Resolved issues

.

Ticket ID	Description
PID-11293	When using the PingID SSH integration, there were cases where an error was reported ("Request signature is not valid"). This issue has been resolved.

PingID SSH Integration 4.1.0 (December 29, 2020)

Enhancements

New functionality for SSH Version 4.1.0

Extended collection of client IP addresses: We now collect client IP addresses during PAM configuration.

Known Limitations

1. A tarball build might not work on systems running on i386 processors.
2. On FreeBSD, the `su` command does not work when using the native clang compiler to build PingID from a pingid tarball.
3. There will be no further binary PingID packages for CentOS version 6 and RHEL version 6.

   (RHEL version 6 and CentOS version 6 reached End of Life on November 30th, 2020.)

PingID SSH Integration (December 03, 2020)

Enhancements

For PingID SSH version 4.0.16+

Support added for binary package PingID SSH integration into SUSE (SLES and OpenSUSE).

For supported versions, see PingID SSH support information.

For installation details, see Installing PingID SSH binary package.

PingID SSH Integration 4.0.16 (October 27, 2020)

Enhancements

Performance Enhancement

PingID SSH now supports session "stickiness" across data centers (active/active support).

Additional operating systems support

- HP-UX source package installation is now supported. See Installation example for HP-UX.
- RHEL binary package insallation is now supported. See Installing PingID SSH binary package.

PingID SSH Integration 4.0.14+ (July 23, 2020)

Upgrade Recommendation - Verify proxy certification

If you are upgrading to SSH v.4.0.14+ we strongly recommend that you add the following line to the configuration file:

```
proxy_verify_cert = true
```

PingID SSH Integration 4.0.15 (July 02, 2020)

Enhancements

For PingID SSH Version 4.0.15:

AIX 7.x is now supported.

Resolved Issues

Ticket ID	Description
PID-8229	Fixed an issue where the `su` command (when configured to use the pam_pingid module) hangs on FreeBSD 12.

PingID SSH Integration 4.0.14 (April 30, 2020)

Enhancements

For PingID SSH Version 4.0.14:

- Implement package management for YUM
- Allow admins to configure self-signed certificate for proxy
- Support for CentOS 8.0

Resolved Issues

Ticket ID	Description
PID-9304	A possible heap overflow was found that could allow a Remote Code Execution attack (CVE-2020-10654) against PingID-enrolled servers. The issue has been corrected.

PingID SSH Integration 4.0.13 (October 03, 2019)

Enhancements

For PingID SSH Version 4.0.13:

- **PingID SSH PAM module now works with CentOS 7 & RHEL 7**

  Additional configuration option (`--enable-selinux`) was added to allow PingID agent to function correctly on CentOS 7 & RHEL 7 where SELinux is enforced. See Integration with RHEL-based distributions incorporating extended SELinux restrictions.

PingID SSH Integration 4.0.12 (July 01, 2019)

Enhancements

For PingID SSH Version 4.0.12:

- Support for Ubuntu 18.04
- Removed dependency on libcurl in pre-built packages (for Ubuntu and Debian)
- Support for openssl-1.1.x

Resolved issues

Ticket ID	Description
PID-8118	The following issue has been corrected: **Wrong file format for PingID SSH download**: SSH integration zip file for PingID (pingid-ssh.zip) downloaded from https://www.pingidentity.com/content/ping/en/resources/downloads/pingid.html failed to unzip on Linux. The problem was found and corrected in the distribution of version 4.0.11.

PingID SDK release notes

These release notes summarize the changes in current and previous PingID SDK updates.

PingID SDK (March 28, 2022)

Enhancements

SDK activity reports - SafetyNet attestation certificate expiration

The report **PingID SDK Admin Activity of the Last 7 Days** now includes a daily entry that indicates the expiration date of the SafetyNet attestation certificate. The report displays one such message for each SDK-based application that has the SafetyNet integrity requirement enabled.

PingID SDK (May 31, 2021)

Enhancements

Customization and trust of email domains via PingID SDK APIs

PingID SDK has been extended to support use of your organization's own trusted email domains and email addresses, using the PingID SDK APIs. This reinforces trust from the customer and also from the receiving servers. The APIs provide a further option to configure DKIM and SPF verification for outbound emails.

> **Note**
>
> As part of this feature upgrade, email template IDs have changed. Template locales are modified so that every occurrence of an underscore ("_") character is replaced with a hyphen ("-").
> To reduce confusion, the creation of unusable or invalid templates is no longer allowed. Some invalid templates have been deleted. This includes:
>
> - Templates that don't contain the required `${otp}` parameter, either in the subject or in the email body.
> - Templates that are missing "from" or "reply-to" addresses, or have an invalid address.

In the PingID SDK developer's guide, see:

- Trusted email domains
- Trusted email addresses
- Email templates
- Authenticate with email

PingID SDK (April 11, 2021)

Enhancements

PingID SDK settings file download

The admin web portal UI has been streamlined: The PingID SDK settings file download has been moved from the **Setup → PingID → Client Integration** screen to the **Setup → PingID SDK** settings screen. See Distributing the PingID SDK settings file and application ID.

PingID SDK Package 1.14.6 (March 31, 2021)

The PingID SDK 1.14.6 package is released with the following components:

PingID SDK component	Module	Submodule	Version	Status
PingID Mobile SDK	PingID Mobile SDK for Android		1.6.4	Unchanged
	PingID Mobile SDK for iOS		1.6.1	Unchanged
	PingID Mobile SDK for iOS		1.4.1	Legacy
PingID SDK Server sample code			1.4	Unchanged
PingFederate PingID SDK Integration Kit 1.12	PingFederate PingID SDK IDP Adapter 1.8.2	PingFederate PingID SDK IDP Adapter	1.8.2	Updated
		*PingID SDK CIBA Authenticator	1.1.2	Updated
		PingFederate PingID SDK IDP Selector	1.1	Unchanged
		**PingFederate Authenticator API	1.0.0.50	Unchanged
	PingFederate PingID SDK Connector		1.2.2	Unchanged

- The PingID SDK CIBA Authenticator is part of the PingFederate PingID SDK IDP Adapter jar.
    - **Important**: If the current PingFederate Authentication API version is above 1.0.0.50, you should not replace this jar file.

Enhancements

PingID SDK has been extended with the following features:

Configuring timeouts for authentication requests

You can now configure the amount of time that an authentication request lasts before timing out. You can use this feature to customize the authentication experience to your user's needs, and reduce the number of users that experience a push notification timeout on authentication attempts.

You can configure:

- `Device Timeout`: The amount of time in seconds that a new authentication request notification must reach a user's mobile device, before timing out.
- `Total Timeout`: The total amount of time in seconds that a new authentication request will last, before timing out. This includes the time for `Device Timeout`, plus the time that the user has to respond to the authentication request.

In the admin guide, see Updating a PingID SDK app's configuration.

API support for configuring timeouts for authentication requests

In addition to the timeout configuration settings in the admin UI, the PingID SDK Application Attributes API has been extended, so that customers can configure the amount of time that an authentication request lasts before timing out.

In the PingID SDK developer's guide, see Application Attributes API.

Resolved issues

Ticket ID	Description
PIDC-2513	In an installation using PingFederate with PingID SDK, a user entered an OTP and received a generic error message, instead of a message indicating that the OTP session expired. This has been resolved.

PingID SDK Package 1.14.5 (February 21, 2021)

The PingID SDK 1.14.5 package is released with the following components:

PingID SDK component	Module	Submodule	Version	Status
PingID Mobile SDK	PingID Mobile SDK for Android		1.6.4	Updated
	PingID Mobile SDK for iOS		1.6.1	Unchanged

PingID SDK component	Module	Submodule	Version	Status
	PingID Mobile SDK for iOS		1.4.1	Legacy
PingID SDK Server sample code			1.4	Unchanged
PingFederate PingID SDK Integration Kit 1.11	PingFederate PingID SDK IDP Adapter 1.8.1	PingFederate PingID SDK IDP Adapter	1.8.1	Unchanged
		*PingID SDK CIBA Authenticator	1.1.1	Unchanged
		PingFederate PingID SDK IDP Selector	1.1	Unchanged
		**PingFederate Authenticator API	1.0.0.50	Unchanged
	PingFederate PingID SDK Connector		1.2.2	Unchanged

- The PingID SDK CIBA Authenticator is part of the PingFederate PingID SDK IDP Adapter jar.
  - **Important**: If the current PingFederate Authenticator API version is above 1.0.0.50, you should not replace this jar file.

Resolved issues

Ticket ID	Description
STAGING-12150	During the SafetyNet root detection check on Android devices, an app failed for some users. This is resolved in PingID Mobile SDK for Android 1.6.4.

PingID SDK Package 1.14.4 (January 26, 2021)

The PingID SDK 1.14.4 package is released with the following components:

PingID SDK component	Module	Submodule	Version	Status
PingID Mobile SDK	PingID Mobile SDK for Android		1.6.3	Unchanged

PingID SDK component	Module	Submodule	Version	Status
	PingID Mobile SDK for iOS		1.6.1	Unchanged
	PingID Mobile SDK for iOS		1.4.1	Legacy
PingID SDK Server sample code			1.4	Unchanged
PingFederate PingID SDK Integration Kit 1.11	PingFederate PingID SDK IDP Adapter 1.8.1	PingFederate PingID SDK IDP Adapter	1.8.1	Updated
		*PingID SDK CIBA Authenticator	1.1.1	Updated
		PingFederate PingID SDK IDP Selector	1.1	Unchanged
		**PingFederate Authenticator API	1.0.0.50	Unchanged
	PingFederate PingID SDK Connector		1.2.2	Unchanged

- The PingID SDK CIBA Authenticator is part of the PingFederate PingID SDK IDP Adapter jar.
    - **Important**: If the current PingFederate Authenticator API version is above 1.0.0.50, you should not replace this jar file.

Enhancements

PingID SDK has been extended with the following features:

CIBA authenticator support for dynamic application ID

The PingID SDK CIBA authenticator now supports a configuration for dynamic application IDs. This feature enables a single CIBA authenticator to work with multiple applications. See Configuring the CIBA Authenticator for PingID SDK.

PingID SDK (January 5, 2021)

Enhancements

Mobile Authentication Framework

An open-source code project that provides an example of how to use the PingFederate Authentication API's browserless OAuth flow in iOS and Android projects. It supports selected MFA flows and provides the current state of a flow, as an end-user steps through a PingFederate authentication policy. The native iOS and Android code allows end-user interactions with the API, such as credential prompts, to be handled by an external mobile application.

The Mobile Authentication Framework package is available for download at:

- iOS: https://github.com/pingidentity/mobile-authentication-framework-ios
- Android: https://github.com/pingidentity/mobile-authentication-framework-android

PingID SDK Package 1.14.3 (December 30, 2020) - Updated

The PingID SDK 1.14.3 package is released with the following components:

PingID SDK component	Module	Submodule	Version	Status
PingID Mobile SDK	PingID Mobile SDK for Android		1.6.3	Updated
	PingID Mobile SDK for iOS		1.6.1	Updated
	PingID Mobile SDK for iOS		1.4.1	Legacy
PingID SDK Server sample code			1.4	Unchanged
PingFederate PingID SDK Integration Kit 1.10	PingFederate PingID SDK IDP Adapter 1.8	PingFederate PingID SDK IDP Adapter	1.8	Unchanged
		*PingID SDK CIBA Authenticator	1.1	Unchanged
		PingFederate PingID SDK IDP Selector	1.1	Unchanged
		**PingFederate Authenticator API	1.0.0.50	Unchanged

PingID SDK component	Module	Submodule	Version	Status
	PingFederate PingID SDK Connector		1.2.2	Unchanged

- The PingID SDK CIBA Authenticator is part of the PingFederate PingID SDK IDP Adapter jar.
  - **Important**: If the current PingFederate Authenticator API version is above 1.0.0.50, you should not replace this jar file.

> **Note**
>
> ***PingID Mobile SDK security updates***
>
> The PingID SDK 1.14.3 package includes security updates for the PingID Mobile SDK. For jailbroken detection of iOS devices and root detection of Android devices, we recommend using the latest PingID Mobile SDK versions included in this package.
>
> Applications using PingID Mobile SDK for iOS versions before 1.6.1 for authentication are regarded as missing the required data to determine whether the device is jailbroken. Those requests proceed according to the **FALLBACK RESPONSE** configuration.

Resolved issues

Ticket ID	Description
PIMC-886	Security fixes in the jailbroken detection mechanism.
PIMC-900	During the SafetyNet root detection check on Android devices, an app crashed for some users. This is resolved in PingID Mobile SDK for Android 1.6.3.

PingID SDK (December 29, 2020)

Enhancements

PingID SDK has been extended with the following features:

API support for PingID SDK application management

In addition to the existing PingID SDK application management in the admin UI, PingID SDK has been extended with the Application API and Application Attributes API, that enable customers to develop their own services for PingID SDK application management. Customers can now programatically create and maintain PingID SDK application configurations, and automate and streamline bulk creation and maintenance of application configurations.

In the PingID SDK developer's guide, see:

- Application API

- Application Attributes API

Known issues and limitations

iOS push credential configuration is only supported using the admin console

iOS push credentials cannot be configured using the PingID SDK Application API, and must be configured using the admin console.

PingID SDK Package 1.14.2 (December 2, 2020)

The PingID SDK 1.14.2 package is released with the following components:

PingID SDK component	Module	Submodule	Version	Status
PingID Mobile SDK	PingID Mobile SDK for Android		1.6.2	Updated
	PingID Mobile SDK for iOS		1.6	Unchanged
	PingID Mobile SDK for iOS		1.4.1	Legacy
PingID SDK Server sample code			1.4	Unchanged
PingFederate PingID SDK Integration Kit 1.10	PingFederate PingID SDK IDP Adapter 1.8	PingFederate PingID SDK IDP Adapter	1.8	Unchanged
		*PingID SDK CIBA Authenticator	1.1	Unchanged
		PingFederate PingID SDK IDP Selector	1.1	Unchanged
		**PingFederate Authenticator API	1.0.0.50	Unchanged
	PingFederate PingID SDK Connector		1.2.2	Updated

- The PingID SDK CIBA Authenticator is part of the PingFederate PingID SDK IDP Adapter jar.
    - **Important**: If the current PingFederate Authenticator API version is above 1.0.0.50, you should not replace this jar file.

Resolved issues

Ticket ID	Description
PIMC-874	When receiving a push notification, a toast appeared with category data.This has been resolved, so that the toast no longer appears.
IO-5984	PingFederate PingID SDK Connector 1.2.2 (October 2020): Fixed an issue that caused the provisioning engine to see email1 and Email 1 as different devices. This could cause an error when the provisioning engine tried to add a new device instead of updating the existing device.

PingID SDK (November 26, 2020)

Enhancements

PingID SDK activity report

The PingID SDK activity report has been extended with new message details. When the mobile device is not reachable to receive a push notification, the report's message field reflects the reason:

Mobile device state	PingID SDK activity report message
Mobile device in flight mode	Device Couldn't Be Reached [device name]. Device Offline.
Mobile device is pushless	Device Couldn't Be Reached [device name]. Push Disabled.

PingID SDK Package 1.14.1 (November 18, 2020)

The PingID SDK 1.14.1 package is released with the following components:

PingID SDK component	Module	Submodule	Version	Status
PingID Mobile SDK	PingID Mobile SDK for Android		1.6.1	Updated
	PingID Mobile SDK for iOS		1.6	Unchanged
	PingID Mobile SDK for iOS		1.4.1	Legacy
PingID SDK Server sample code			1.4	Unchanged

PingID SDK component	Module	Submodule	Version	Status
PingFederate PingID SDK Integration Kit 1.9	PingFederate PingID SDK IDP Adapter 1.8	PingFederate PingID SDK IDP Adapter	1.8	Unchanged
		*PingID SDK CIBA Authenticator	1.1	Unchanged
		PingFederate PingID SDK IDP Selector	1.1	Unchanged
		**PingFederate Authenticator API	1.0.0.50	Unchanged
	PingFederate PingID SDK Connector		1.2.1	Unchanged

- The PingID SDK CIBA Authenticator is part of the PingFederate PingID SDK IDP Adapter jar.
    - **Important**: If the current PingFederate Authenticator API version is above 1.0.0.50, you should not replace this jar file.

Resolved issues

Ticket ID	Description
PIMC-867	Fixed a configuration that might cause an issue in Android mobile device pairing.

PingID SDK Package 1.14 (November 4, 2020) - Updated

> **Note**
>
> The PingID SDK 1.14 package was removed from the download site due to a technical issue, and will be available soon. (November 9, 2020)

The PingID SDK 1.14 package is released with the following components:

PingID SDK component	Module	Submodule	Version	Status
PingID Mobile SDK	PingID Mobile SDK for Android		1.6	Updated
	PingID Mobile SDK for iOS		1.6	Updated

PingID SDK component	Module	Submodule	Version	Status
	PingID Mobile SDK for iOS		1.4.1	Legacy
PingID SDK Server sample code			1.4	Unchanged
PingFederate PingID SDK Integration Kit 1.9	PingFederate PingID SDK IDP Adapter 1.8	PingFederate PingID SDK IDP Adapter	1.8	Unchanged
		*PingID SDK CIBA Authenticator	1.1	Unchanged
		PingFederate PingID SDK IDP Selector	1.1	Unchanged
		**PingFederate Authenticator API	1.0.0.50	Unchanged
	PingFederate PingID SDK Connector		1.2.1	Unchanged

- The PingID SDK CIBA Authenticator is part of the PingFederate PingID SDK IDP Adapter jar.
    - **Important**: If the current PingFederate Authenticator API version is above 1.0.0.50, you should not replace this jar file.

Enhancements

PingID SDK has been extended with the following features:

Android

PingID Mobile SDK for Android v1.6 (PingID SDK package 1.14):

- **Support for Android 11 (API level 30)**

  The PingID Mobile SDK for Android was built with the latest gradle (6.1.1) and gradle plugin (3.6.1).

  Due to support for Android 11 (API level 30), the dependencies versions have changed. See the `gradle.properties` and `build.gradle` files in the Moderno sample project and application levels for the latest dependency versions and changes.

- **Debug logs level**

  The debug level has been removed from the logfile output configuration in the SDK's Android library. From this version onwards, debug level information no longer appears in local logfiles.

- **Moderno sample app (Android)**

The Moderno sample app now supports Android 11. In Android 11, whenever an app requests a permission related to location, the user-facing permissions dialog has an option called **Only this time**. If the user selects this option, the app is granted a temporary one-time permission.

The Moderno app follows best practices related to permissions for Android developers, and checks the permission before trying to access information that's guarded by that permission.

iOS

The PingID Mobile SDK for iOS v1.6 (PingID SDK package 1.14) now supports iOS 14.

Resolved issues

Ticket ID	Description
PIMC-725	Fixed a bug where the PingID Mobile SDK for Android was returning a NullPointerException.
PIMC-793	Fixed a bug in PingID Mobile SDK for iOS, for a process returning EXC_BAD_ACCESS (SIGSEGV), when attempting to access invalid memory, or attempting to access memory in a manner not allowed by the memory's protection level.

Deprecated features

Android

- Android 4.x is no longer supported.
- PingID Mobile SDK for Android v1.6 (PingID SDK package 1.14) no longer uses the cryptographic functionality of Bouncy Castle, and now uses the native Android cryptographics.

  See Google's Android developers blog for more information: https://android-developers.googleblog.com/2018/03/cryptography-changes-in-android-p.html

iOS

- iOS 8.x is no longer supported.
- PingID Mobile SDK for iOS v1.6 (PingID SDK package 1.14) is the last version supporting iOS 9.x.

PingID SDK Package 1.13 (October 28, 2020)

The PingID SDK 1.13 package is released with the following components:

PingID SDK component	Module	Submodule	Version	Status
PingID Mobile SDK	PingID Mobile SDK for Android		1.5	Unchanged

PingID SDK component	Module	Submodule	Version	Status
	PingID Mobile SDK for iOS		1.5	Unchanged
	PingID Mobile SDK for iOS		1.4.1	Legacy
PingID SDK Server sample code			1.4	Unchanged
PingFederate PingID SDK Integration Kit 1.9	PingFederate PingID SDK IDP Adapter 1.8	PingFederate PingID SDK IDP Adapter	1.8	Updated
		*PingID SDK CIBA Authenticator	1.1	Updated
		PingFederate PingID SDK IDP Selector	1.1	Unchanged
		**PingFederate Authenticator API	1.0.0.50	Updated
	PingFederate PingID SDK Connector		1.2.1	Unchanged

- The PingID SDK CIBA Authenticator is part of the PingFederate PingID SDK IDP Adapter jar.
    - **Important**: If the current PingFederate Authenticator API version is above 1.0.0.50, you should not replace this jar file.

Enhancements

PingID SDK has been extended with the following features:

PingID SDK Integration Kit 1.9 (PingID SDK 1.13 package) for PingFederate

Mobile device access support for PingFederate Authentication API

- PingID SDK's integration with the PingFederate Authentication API for end-user interactions now supports mobile device access flows. See Integration with the PingFederate Authentication API in the PingID SDK documentation.
- PingID SDK adapter core contract attributes have been extended with new values for `pingid.sdk.status` and related values for `pingid.sdk.status.reason`, for integration with the PingFederate Authentication API. New values for `pingid.sdk.status`:
    - `com.pingidentity.pingidsdk.device_paired`

- `com.pingidentity.pingidsdk.device_access_allowed`

Push notification categories

- Categories can be defined, so that any type of notification can be sent according to a category.
- Similar to iOS push notification categories, from PingID SDK adapter for PingFederate 1.8 onwards, the 'category' attribute is sent in the push payload. This attribute can be used for creating different types of push notifications, as defined in the adapter.
- The PingID SDK Authentication API has been extended with a new parameter:
  - `pushCategory`
- Dynamic parameter support has been extended with a new parameter:
  - `pingIdSdkCategory`
- PingID SDK CIBA Authenticator 1.1 (included in PingID SDK adapter for PingFederate 1.8), now supports push notification categories. See Configuring the CIBA Authenticator for PingID SDK.

Resolved issues

Ticket ID	Description
PIDC-1869	A user opened a mobile browser on an iOS device and received a push notification to approve access. In some cases, when returning to the browser, the user received an error message. This has been resolved.

PingID SDK (October 19, 2020)

Enhancements

PingID SDK has been extended with the following features:

PingID SDK support for custom Syniverse account

PingID SDK has been extended to allow customers to use a custom Syniverse account instead of Ping Identity's account or customer's custom Twilio account, providing the following benefits:

- Avoid manual back-to-back billing (Ping-Customer)
- Cost leverage for customers with massive SMS and Voice usage
- Fallback to Ping Identity's Twilio account, or customers own custom Twilio account

A new PingID SDK Syniverse configuration section was added in the Administration Guide.

See Configuring a Syniverse account for PingID SDK.

PingID SDK support for custom Twilio account

PingID SDK's existing support for custom Twilio accounts has been extended to allow customers to use a custom Syniverse account instead of Ping Identity's account as fallback, in cases of Twilio delivery failure.

See Configuring a Twilio account for PingID SDK.

PingID SDK Admin Activity Report

The PingID SDK Admin Activity Report has been extended, so that SMS and Voice event messages include information about the organization's SMS and Voice provider.

Deprecated features

The following PingID SDK API parameters are now deprecated.

If encountered, these parameters are ignored (as support for backward compatibility):

- Offline devices (voice) pairing API: `vendor` parameter.
- Authenticate with Voice: `voiceVendor` parameter.

PingID SDK Package 1.12 (July 28, 2020)

The PingID SDK 1.12 package is released with the following components:

PingID SDK component	Module	Submodule	Version	Status
PingID Mobile SDK	PingID Mobile SDK for Android		1.5	Unchanged
	PingID Mobile SDK for iOS		1.5	Unchanged
PingID SDK Server sample code			1.4	Unchanged
PingFederate PingID SDK Integration Kit 1.8	PingFederate PingID SDK IDP Adapter 1.7	PingFederate PingID SDK IDP Adapter	1.7	Updated
		PingFederate PingID SDK IDP Selector	1.1	Unchanged
		PingFederate Authenticator API	1.0.0.48	New
	PingFederate PingID SDK Connector		1.2.1	Unchanged

Enhancements

PingID SDK has been extended with the following features:

Support for PingFederate Authentication API

PingID SDK now enables customers to integrate with the PingFederate Authentication API for end-user interactions, with the following features:

- Step-up authentication
- Transaction approval

For more information see:

- PingID Administration Guide: Installing the PingID SDK Integration Kit for PingFederate and Configuring the PingID SDK adapter for PingFederate.
- PingID SDK Developer Guide: Integration with the PingFederate Authentication API.

Dynamic parameter support

Dynamic parameter support has been extended with the following new parameters:

- `pingIdSdkSmsMessage`
- `pingIdSdkSmsSender`
- `pingIdSdkLocale`
- `pingIdSdkEmailConfigurationType`
- `pingIdSdkEmailParameters`
- `pingIdSdkVoiceMessage`
- `pingIdSdkVoice`

Known issues and limitations

QR code authentication

QR code based authentication is not supported for the PingFederate Authentication API.

PingID SDK (July 7, 2020)

Enhancements

PingID SDK audit event subscriptions

PingID SDK has been extended to support audit event subscriptions for queue, delivery, bounce, and complaint email event details of user authentication and pairing via email.

If you are already subscribed for PingID SDK events, you'll automatically receive these email event details.

If you are not subscribed, you can create a subscription of type PingID SDK. See Add a Push subscription in the PingOne documentation.

Authentication API

The Authentication API has been extended with the new `approvedDeviceState` parameter. `approvedDeviceState` provides the state of an approved untrusted device, in scenarios where an authentication request from the untrusted mobile app is approved by the user using a different, trusted device.

RegistrationToken API

The RegistrationToken API has been extended with:

- The GET RegistrationToken operation, to retrieve the registration token resource.
- The new `status` parameter, that provides the registration token status value that is returned from the call.

Resolved issues

Ticket ID	Description
PIDC-2122	Fixed a case where data that included special characters such as emojis and symbols caused the response validation to fail.

PingID SDK (June 15, 2020)

Enhancements

Email events in the PingID SDK Activity Report

The PingID SDK Activity Report has been extended to present queue, delivery, bounce, and complaint email event details for user authentication and pairing email events. See the Running the PingID activity report section in the admin documentation, for information on how to run the report, and the report's output.

Resolved issues

Ticket ID	Description
PIDC-1986	A case was discovered where some Australian phone numbers were rejected in SMS pairing. This issue is now resolved.

PingID SDK (April 16, 2020)

Enhancements

Australian users to receive SMS/Voice call from Australian phone numbers

Users from Australia will now receive their authentication SMS/Voice calls from Australian phone numbers. (Previously, they were sent from US phone numbers.)

Contact your Ping representatives to add local numbers for additional countries.

PingID SDK Package 1.11 (April 1, 2020)

The PingID SDK 1.11 package is released with the following components:

PingID SDK component	Module	Submodule	Version	Status
PingID Mobile SDK	PingID Mobile SDK for Android		1.5	Updated
	PingID Mobile SDK for iOS		1.5	Updated
PingID SDK Server sample code			1.4	Unchanged
PingFederate PingID SDK Integration Kit 1.7	PingFederate PingID SDK IDP Adapter 1.6	PingFederate PingID SDK IDP Adapter	1.6	Unchanged
		PingFederate PingID SDK IDP Selector	1.1	Unchanged
	PingFederate PingID SDK Connector		1.2.1	Unchanged

Enhancements

PingID SDK has been extended with the following features:

Android

PingID Mobile SDK for Android v1.5 (PingID SDK package 1.11):

- **Support for Android API level 29**

  The SDK was built with the latest gradle (6.1.1) and gradle plugin (3.6.1).

Due to support for Android API level 29, the dependencies versions have changed. See the `gradle.properties` and `build.gradle` files in the Moderno sample project and application levels for the latest dependency versions and changes.

- **Moderno sample app (Android)**

  For ease of use, we have moved the SDK constants from the `AppPreferences.java` file to the application level `build.gradle` under the `buildTypes` section.

iOS

PingID Mobile SDK for iOS v1.5 (PingID SDK package 1.11):

Support for Xcode 11 and XCFrameworks.

> **Note**
>
> There are minor differences in the IDE setup, depending on the version of PingID Mobile SDK for iOS. See Getting started > iOS implementation in the developer documentation.
> PingID SDK supports the following software versions:
>
> - For versions of PingID SDK up to version 1.4.x:
>   - Xcode versions 8 to 10.x
>   - iOS 8+
> - For versions of PingID SDK from 1.5 and later:
>   - Xcode 11+
>   - iOS 8+

Resolved issues

Ticket ID	Description
PIMC-554	An issue was identified in the Android Moderno sample app, where the strings for the title and body were taken from the code itself, and not from the push payload. This is now resolved.
PIMC-685	Fixed a bug that could cause an iOS 13+ app to crash, when running in the background.
PIMC-724	An issue was identified in a specific flow when a pairing failed, files were deleted from the `Files` folder in the Android application package. This is now resolved.

PingID SDK Package 1.10.1 (December 31, 2019)

The PingID SDK 1.10.1 package is released with the following components:

PingID SDK component	Module	Submodule	Version	Status
PingID Mobile SDK	PingID Mobile SDK for Android		1.4.2	Updated
	PingID Mobile SDK for iOS		1.4.1	Unchanged
PingID SDK Server sample code			1.4	Unchanged
PingFederate PingID SDK Integration Kit 1.7	PingFederate PingID SDK IDP Adapter 1.6	PingFederate PingID SDK IDP Adapter	1.6	Unchanged
		PingFederate PingID SDK IDP Selector	1.1	Unchanged
	PingFederate PingID SDK Connector		1.2.1	Unchanged

Resolved issues

Ticket ID	Description
PIMC-667	Fixed a bug that could cause an Android app running in the background to crash.

PingID SDK Package 1.10 (December 24, 2019)

The PingID SDK 1.10 package is released with the following components:

PingID SDK component	Module	Submodule	Version	Status
PingID Mobile SDK	PingID Mobile SDK for Android		1.4.1	Unchanged
	PingID Mobile SDK for iOS		1.4.1	Unchanged
PingID SDK Server sample code			1.4	Unchanged
PingFederate PingID SDK Integration Kit 1.7	PingFederate PingID SDK IDP Adapter 1.6	PingFederate PingID SDK IDP Adapter	1.6	Updated

PingID SDK component	Module	Submodule	Version	Status
		PingFederate PingID SDK IDP Selector	1.1	Unchanged
	PingFederate PingID SDK Connector		1.2.1	Unchanged

Enhancements

PingID SDK has been extended with the following features:

PingID SDK Integration Kit 1.7 (PingID SDK 1.10 package) for PingFederate

CIBA authenticator support

PingID SDK now allows customers to use a Client Initiated Backchannel Authentication (CIBA) Authenticator for the purpose of authenticating users via an out-of-band authentication method on mobile devices. See Configuring the CIBA Authenticator for PingID SDK.

PingID SDK Package 1.9.1 (December 23, 2019)

The PingID SDK 1.9.1 package is released with the following components:

PingID SDK component	Module	Submodule	Version	Status
PingID Mobile SDK	PingID Mobile SDK for Android		1.4.1	Updated
	PingID Mobile SDK for iOS		1.4.1	Unchanged
PingID SDK Server sample code			1.4	Unchanged
PingFederate PingID SDK Integration Kit 1.6	PingFederate PingID SDK IDP Adapter 1.5	PingFederate PingID SDK IDP Adapter	1.5	Unchanged
		PingFederate PingID SDK IDP Selector	1.1	Unchanged
	PingFederate PingID SDK Connector		1.2.1	Unchanged

Resolved issues

Ticket ID	Description
PIMC-655	In the PingID Mobile SDK for Android, the `PingIdPushHelper` was not reachable from the developer's code due to ProGuard rules. This is now resolved.

PingID SDK (December 11, 2019)

Enhancements

Configure OTP authentication timeout

PingID SDK has been extended with the option to configure the maximum duration of the lifetime of SMS, Voice and Email passcode values for authentication requests, to enhance user experience according to your needs. The OTP lifetime duration can be configured globally with one duration value for SMS, Voice and Email methods per application, or can be configured individually with different values for each of the SMS, Voice and Email authentication methods.

The OTP lifetime may be configured from a minimum of one minute up to a maximum of 30 minutes. If not configured, the OTP lifetime defaults to the maximum 30 minutes. See Updating a PingID SDK app's configuration NOTE: All retries for a particular OTP must occur during the configured OTP lifetime. For existing applications where admins have not configured the OTP lifetime duration, all retries for a particular OTP must occur in the default 30 minutes.

PingID SDK Package 1.9 (November 25, 2019)

The PingID SDK 1.9 package is released with the following components:

PingID SDK component	Module	Submodule	Version	Status
PingID Mobile SDK	PingID Mobile SDK for Android		1.4	Unchanged
	PingID Mobile SDK for iOS		1.4.1	Updated
PingID SDK Server sample code			1.4	Unchanged
PingFederate PingID SDK Integration Kit 1.6	PingFederate PingID SDK IDP Adapter 1.5	PingFederate PingID SDK IDP Adapter	1.5	Unchanged
		PingFederate PingID SDK IDP Selector	1.1	Unchanged

PingID SDK component	Module	Submodule	Version	Status
	PingFederate PingID SDK Connector		1.2.1	Unchanged

Resolved issues

Ticket ID	Description
PIMC-643	Developers were prevented from uploading their iOS apps to the App Store due to the error: "`ERROR ITMS-90171: Invalid Bundle Structure - The binary file '<app>/PingID_SDK.framework/libswiftRemoteMirror.dylib' is not permitted`". This is now resolved.

PingID SDK Package 1.8 (September 25, 2019)

The PingID SDK 1.8 package is released with the following components:

PingID SDK component	Module	Submodule	Version	Status
PingID Mobile SDK	PingID Mobile SDK for Android		1.4	Updated
	PingID Mobile SDK for iOS		1.4	Updated
PingID SDK Server sample code			1.4	Updated
PingFederate PingID SDK Integration Kit 1.6	PingFederate PingID SDK IDP Adapter 1.5	PingFederate PingID SDK IDP Adapter	1.5	Updated
		PingFederate PingID SDK IDP Selector	1.1	Updated
	PingFederate PingID SDK Connector		1.2.1	Updated

Enhancements

PingID SDK has been extended with the following features:

PingID SDK support for custom Twilio account

PingID SDK has been extended to allow customers to use a custom Twilio account instead of Ping Identity's account, providing the following benefits:

- Avoid manual back-to-back billing (Ping-Customer)
- Cost leverage over Twilio for customers with massive SMS and Voice usage
- Consolidate customer's usage from helpdesk and audit perspective

A new PingID SDK Twilio configuration section was added in the Administration Guide. See Using a custom Twilio account with PingID SDK.

Rooted and jailbroken device detection support

PingID SDK has an integrated mobile device integrity check in its MFA flows, which allows customer mobile applications to provide reduced permissions, or deny access when a mobile device is detected as rooted or jailbroken. On iOS, the PingID SDK proprietary algorithm is used to determine if a mobile device is jailbroken.
Android, on the other hand, takes advantage of Google's SafetyNet service to determine whether the device is rooted.
A new configuration section was added in the Administration Guide . See Update a PingID SDK app's configuration.

Minimum software version requirements

The following minimum software versions are required for implementing device integrity checks and detection of rooted and jailbroken devices:

- PingID Mobile SDK for iOS version 1.4
- PingID Mobile SDK for Android version 1.4
- Android 5.0+ on end user Android devicesImplementations using PingFederate require the following additional minimum software versions:
- PingFederate version 8.2+ (all versions supporting the PingID SDK Adapter)
- PingID SDK Adapter version 1.5
- PingID SDK Selector version 1.1. If PF v9.2 or higher is used, the PingID SDK Selector is optional, and root detection can work with or without it.

Server APIs

The following PingID SDK Server APIs were extended to support rooted and jailbroken devices:

- User devices API: A new `rooted (true/false)` parameter has been added to the `device` object.
  The filter option on the GET operation is now deprecated, and is supported for backward compatibility. The new POST operation should be used instead of the filter option on GET.
- Authentication API: A new possible value of `DEVICE_ROOTED` has been added to the `reason` parameter.
  The new `rooted (true/false)` parameter in the `device` object is returned in the GET and POST response bodies.
- Registration Token A new `DEVICE_ROOTED` code is returned when a rooted or jailbroken device is detected in the POST operation. See Error handling in PingID SDK.

Mobile APIs

PingID mobile SDK for iOS and Android was extended with the following new mobile APIs:

Mobile API	Description
`setRootDetection`	Activates device integrity check flow.
`getRestrictiveOneTimePasscode`	Returns an OTP and the status of the response.
`generatePayload(final PayloadCallback callback)`	*This change affects Android only. For iOS, `generatePayload` remains unchanged. `generatePayload` returns the current mobile payload in a callback parameter, in a different thread (asynchronously). **Note** The previous Android version of `generatePayload` is deprecated (PingID Mobile SDK for Android v1.3 and earlier). The new `generatePayload(final PayloadCallback callback)` method should be used instead.

The following mobile APIs are **deprecated**:

Mobile API	Description
`getOneTimePasscode`	If the root detection feature is **disabled** in the admin console, an OTP is returned. If the root detection feature is **enabled** in the admin console, an empty string is returned. **Note** • The `getOneTimePasscode` method is deprecated, and supported for backward compatibility. The `getRestrictiveOneTimePasscode` method should be used instead. • The `getOneTimePasscode` previously returned an 8-digit OTP for iOS and a 6-digit OTP for Android devices. It now returns a 6-digit OTP for both iOS and Android devices. Developers who implemented their application code according to the earlier version of the Moderno sample app (which truncated the last 2 digits of the 8-digit OTP for iOS), should adjust their application code.
`generatePayload`	*This change affects Android only. For iOS, `generatePayload` remains unchanged. `generatePayload` returns the current mobile payload in a callback parameter. **Note** The previous Android version of `generatePayload` is deprecated (PingID Mobile SDK for Android v1.3 and earlier). The new `generatePayload(final PayloadCallback callback)` method should be used instead.

Refer to PingID SDK Mobile API for further information.

Moderno sample app

The new version of the Moderno sample app has been extended to include support for rooted and jailbroken device detection.

Developer IDE

- **iOS**: Project build settings require the target configuration of `Always Embed Swift Standard Libraries` to be set to `YES`. See iOS implementation.
- **Android**: PingID SDK component dependencies in build.gradle

  This version includes new SDK component dependencies for Android. These should be entered in the application's `gradle.build` file under `dependencies`. Developers must manually add these dependencies to their project, in order for the SDK to work, as the lib is distributed as a file and not via a repository.

  The full list of dependencies is as follows (new or changed dependency versions are highlighted in **bold**):

```
//LOGGING FACADE AND IMPLEMENTATION
 implementation 'org.slf4j:slf4j-api:1.7.26'
implementation 'com.github.tony19:logback-android-core:1.1.1-6'
implementation('com.github.tony19:logback-android-classic:1.1.1-6')
 \{ exclude group: 'com.google.android', module: 'android' }

// JWT, JWE and JOSE tokens libraries
 implementation 'org.bitbucket.b_c:jose4j:0.6.5'

//Google's gSon library to build and parse JSON format
implementation 'com.google.code.gson:gson:2.8.5'
 implementation 'commons-codec:commons-codec:1.12'

//CRYPTO
 implementation 'com.madgag.spongycastle:prov:1.58.0.0'
 implementation 'com.google.android.gms:play-services-base:16.0.1'
 implementation 'com.google.android.gms:play-services-safetynet:16.0.0'

//FireCloud Messaging Services
 implementation 'com.google.firebase:firebase-messaging:18.0.0'
```

  See Android implementation.

PingFederate PingID SDK IDP Adapter 1.5 Rooted and jailbroken device detection

The PingID SDK Adapter has been extended to support detection of rooted and jailbroken devices during pairing and authentication.

PingFederate PingID SDK Selector 1.1 Rooted and jailbroken device detection

The PingID SDK Selector has been extended to support detection of rooted and jailbroken devices.

PingFederate PingID SDK Connector 1.2.1

The PingID SDK Users API was recently improved to support usernames containing special characters such as a forward slash "/". The PingID SDK Connector has incorporated this improved username validation and encoding to support API changes.

Re-obfuscation

PingID SDK code is obfuscated for optimization. Support is now available for apps obfuscation to re-obfuscate the PingID SDK code, which previously not supported.

Validation check for payload creation without an application ID

The PingID SDK Mobile API has been extended to check that payload creation includes an application ID. If the application ID is missing, a new error code (`PIDErrorMissingAppId = -10022`) is returned.

Resolved issues

Ticket ID	Description
PIMC-419	Due to differences between the names of the header file and framework, there was a known limitation that Swift developers were required to use a bridging file in order to import the SDK. This has been resolved, so that a bridging file is no longer necessary.
PIMC-454	PingID Mobile SDK for Android was using fixed values for title and body strings. This has been resolved so that it now uses the title and body submitted in the push.
PIMC-564	Authentications failed when "Background app refresh" was turned off on the iPhone, while both the following settings were configured: • **PingID**admin console: "Extra push" was activated • **PingFederate**: "User verification regard as failure"This has been resolved.

Known issues and limitations

PingFederate integration: when rooted and jailbroken devices are blocked, only the authentication flow is supported

If the PingFederate `ROOTED/JAILBROKEN DEVICE` configuration is set to `Block` , users with rooted or jailbroken devices are blocked during authentication flows, but are granted access when automatic pairing fails.

QR authentication failure for a rooted or jailbroken device

The QR authentication transaction fails for a rooted or jailbroken device, without the option to add business logic in PingFederate or in the customer server. When a user scans the QR code on a rooted device, the QR code remains unclaimed, and the accessing web page remains unchanged, and does not progress to authentication.

Rooted Android device detection from Android 5.0

The minimum operating system supported for root detection is Android 5.0. When root detection is activated, devices with Android versions earlier than 5.0 will not be able to pair or authenticate.

Using Xcode 10.2.1, simulators for iOS 9.3 and earlier might fail to launch Swift apps

Apple reported the following known issue in the Xcode 10.2.1 release notes, which may impact the PingID SDK Moderno app: *Simulators for iOS 9.3 and earlier might fail to launch Swift apps with the message: "dyld: Library not loaded: /usr/lib/libauto.dylib". **Workaround**: Run the following command in Terminal for the relevant version of iOS:*

```
sudo mkdir '/Library/Developer/CoreSimulator/Profiles/Runtimes/iOS 9.3.simruntime/Contents/Resources/
RuntimeRoot/usr/lib/swift'
```

See https://developer.apple.com/documentation/xcode_release_notes/xcode_10_2_1_release_notes?language=objc. Initialization of PingID SDK instance in Android apps::

An extreme case was discovered where the PingID SDK instance remained null instead of initialized after execution of `PingID.init` in an Android app. As a workaround, check if the instance remains null , and if so, then reinitialize it.

PingID SDK Package 1.7 (September 12, 2019)

The PingID SDK 1.7 package is released with the following components:

PingID SDK component	Module	Submodule	Version	Status
PingID Mobile SDK	PingID Mobile SDK for Android		1.3	Unchanged
	PingID Mobile SDK for iOS		1.3	Updated
PingID SDK Server sample code			1.3	Unchanged
PingFederate PingID SDK Integration Kit 1.5	PingFederate PingID SDK IDP Adapter 1.4	PingFederate PingID SDK IDP Adapter	1.4	Unchanged
		PingFederate PingID SDK IDP Selector	1.0	Unchanged
	PingFederate PingID SDK Connector		1.2	Unchanged

Enhancements

Following Apple's update to their iOS push requirements, the extra verification is now sending a regular push instead of a silent one.

- There is no change to the user experience.
- Other than changing the PingID Mobile SDK for iOS to v1.3 in customer apps, no development changes are required.

Resolved issues

Ticket ID	Description
PIDC-1704	The same OTP for offline (email, voice, SMS) authentication could be reused in the same user authentication session. This has been resolved.

Known issues and limitations

Following an upgrade of the APNS push notification client, when changing the APNS certificate via the admin console, the verification process is now limited to verification of the certification expiration date only.

PingID SDK (September 3, 2019)

Resolved issues

Ticket ID	Description
PIDC-1778	Fixed an issue that was preventing silent push notifications from being received by PingID mobile SDK running on iOS v13.0.

PingID SDK (August 27, 2019)

Resolved issues

Ticket ID	Description
PIDC-1761	Usernames containing the forward slash (/) character resulted in an HTTP 404 Page Not Found error. This has been resolved, permitting use of the '/' character, subject to username rules. Refer to the "username" parameter of the Users API in the PingID SDK developer guide.

PingID SDK Package 1.6 (May 29, 2019)

The PingID SDK 1.6 package is released with the following components:

PingID SDK component	Module	Submodule	Version	Status
PingID Mobile SDK	PingID Mobile SDK for Android		1.3	Unchanged
	PingID Mobile SDK for iOS		1.2	Unchanged
PingID SDK Server sample code			1.3	Unchanged
PingFederate PingID SDK Integration Kit 1.5	PingFederate PingID SDK IDP Adapter 1.4	PingFederate PingID SDK IDP Adapter	1.4	Updated
		PingFederate PingID SDK IDP Selector	1.0	Unchanged
	PingFederate PingID SDK Connector		1.2	Unchanged

Enhancements

PingID SDK has been extended with the following features:

PingFederate PingID SDK IDP Adapter 1.4

PingID SDK now supports PingFederate's native forward proxy server definition in PingFederate's **run.properties** file (see Configuring the PingID SDK adapter for PingFederate), which allows PingFederate to get the PingID SDK server address dynamically.

Deprecated features

Proxy configuration in the PingID SDK properties file

Definition of the **pingidsdk_proxy_url** entry in the PingID SDK properties file is deprecated.

> **Note**
>
> Although the **pingidsdk_proxy_url** configuration is deprecated, it is still supported. If configuration entries are defined in both the PingFederate **run.properties** and the PingID SDK properties files, the definition in the PingID SDK properties file will take precedence.

PingID SDK Package 1.5 (May 15, 2019)

The PingID SDK 1.5 package is released with the following components:

PingID SDK component	Module	Submodule	Version	Status
PingID Mobile SDK	PingID Mobile SDK for Android		1.3	Unchanged
	PingID Mobile SDK for iOS		1.2	Unchanged
PingID SDK Server sample code			1.3	Unchanged
PingFederate PingID SDK Integration Kit 1.4	PingFederate PingID SDK IDP Adapter 1.3	PingFederate PingID SDK IDP Adapter	1.3	Unchanged
		PingFederate PingID SDK IDP Selector	1.0	Unchanged
	PingFederate PingID SDK Connector		1.2	Updated

Enhancements

PingID SDK has been extended with the following features:

PingID SDK Integration Kit 1.4 (PingID SDK 1.5 package) for PingFederate

PingID SDK Connector 1.2 for PingFederate

- Fixed a library issue that prevented users from being deprovisioned in PingFederate 8.1.4 and earlier.
- Fixed an issue that caused the connector to use the wrong EU hostname.
- Added a PingID SDK configuration file upload option to speed up configuration in PingFederate 9.0 and later.

See PingID SDK Connector Guide

PingID SDK (May 7, 2019)

Enhancements

Improved SMS authentication service

PingID SDK has an improved SMS authentication service with a more rapid delivery of OTP messages. The pool of SMS dispatching phone numbers has been enlarged. As a result, users may experience delivery of some of their SMS OTP messages sent from telephone numbers that they have not previously seen.

PingID SDK (April 29, 2019)

Enhancements

Customizable OTP retries and block durations

PingID SDK has been extended with the option for admins to configure the number of failed OTP retry attempts users are allowed per application and per authentication method (SMS, email, mobile etc.), before they should start over.
In addition, admins can set individual block durations per application and per authentication method. This flexibility enhances the user experience by reducing the block duration, or allowing users more retries before they have to start over. Further, it provides compliance with security regulations that may require a longer block duration for specific applications.
See Updating a PingID SDK app's configuration.

PingID SDK Package 1.4 (March 20, 2019)

The PingID SDK 1.4 package is released with the following components:

PingID SDK component	Module	Submodule	Version	Status
PingID Mobile SDK	PingID Mobile SDK for Android		1.3	New
	PingID Mobile SDK for iOS		1.2	Unchanged
PingID SDK Server sample code			1.3	New
PingFederate PingID SDK Integration Kit 1.3	PingFederate PingID SDK IDP Adapter 1.3	PingFederate PingID SDK IDP Adapter	1.3	New
		PingFederate PingID SDK IDP Selector	1.0	Unchanged
	PingFederate PingID SDK Connector		1.1	Unchanged

Enhancements

PingID SDK has been extended with the following features:

Support for Android 8.1

PingID Mobile SDK

PingID Mobile SDK has been updated to support Android 8.1. (API version 27) as PingID Mobile SDK's latest Android build tools version. Other than configuring the set of dependency versions listed in IDE integration and Implement the PingID SDK in your code, this upgrade maintains backward compatibility with existing applications, and requires no other changes to application code.

Moderno sample app

The Moderno sample app has been updated to support Android 8.1.

PingID SDK Integration Kit 1.3 (PingID SDK 1.4 package) for PingFederate

Support for virtual hosts

PingFederate supports virtual host names from version 9.2 onwards (see https://support.pingidentity.com/s/document-item?bundleId=pingfederate-93&topicId=adminGuide%2Fpf_c_virtualHostNames.html). The PingID SDK Integration Kit 1.3 for PingFederate (PingID SDK 1.4 package) has been extended to support this feature with PingFedrate 9.2+.

If HTML templates were configured for previous versions, remove the "`<base href>`" tag in the HTML template header in order to support virtual hosts.

Adapter context parameters

It is now possible to define parameters which provide extra context to the PingID SDK Adapter HTML template, in order to support additional server logic. For example, when processing a particular type of transaction such as a money transfer, the adapter may be directed to display an alternative success screen, or different texts. See Dynamic parameter attributes.

HTTP parameter tracking

PingFederate versions until 9.1.x require a Selector to track HTTP parameters through the authentication policy workflow.

From version 9.2, PingFederate no longer requires the Selector for that purpose. See **Tracked HTTP Parameters** in https://support.pingidentity.com/s/document-item?bundleId=pingfederate-93&topicId=adminGuide%2Fpf_t_defineAuthenticationPolicies.html.

The PingID SDK Integration Kit 1.3 for PingFederate (PingID SDK 1.4 package) has been extended to support this feature when using PingFederate 9.2+.

Adding the "`payload`" parameter to the tracked HTTP parameters removes the need to configure and maintain a selector (**Selector Type** = "`PingID SDK Payload Handling Selector <ver>`") in the PingID SDK Adapter's authentication flow.

Support dynamic success, error and timeout screen display

New parameters provide developers the ability to override display of the HTML template's configured success, error and timeout message screens. See Dynamic parameter attributes.

Moderno sample app

Transaction approval

The Moderno sample app has been extended to include transaction approval examples for the PF adapter flow (already supported in the API implementation), using context-related information (dynamic parameters).

PingID SDK Package 1.3 (January 31, 2019)

The PingID SDK 1.3 package is released with the following components:

PingID SDK component	Module	Submodule	Version	Status
PingID Mobile SDK	PingID Mobile SDK for Android		1.2	New
	PingID Mobile SDK for iOS		1.2	New
PingID SDK Server sample code			1.2	New
PingFederate PingID SDK Integration Kit 1.2	PingFederate PingID SDK IDP Adapter 1.2	PingFederate PingID SDK IDP Adapter	1.2	New
		PingFederate PingID SDK IDP Selector	1.0	Unchanged

PingID SDK component	Module	Submodule	Version	Status
	PingFederate PingID SDK Connector		1.1	Unchanged

Enhancements

PingID SDK has been extended with the following features:

QR code based authentication

QR code based authentication is now available for PingID SDK, providing secure passwordless authentication for both customer server and PingFederate implementations. PingID SDK authentication flows optimize the user experience, and allow the user to choose between the already supported push based authentication and the new passwordless login option, which is particularly significant in cases where a user logs on from a public computer. Refer to Supported PingID SDK adapter for PingFederate flows and Supported multifactor authentication (MFA) methods for further information.

Transaction approval for PingFederate

Transaction approval using context-related information (dynamic parameters) is now available for the PingID SDK adapter for PingFederate. Refer to Supported PingID SDK adapter for PingFederate flows and Supported multifactor authentication (MFA) methods for further information.

Multiple apps on one PingID SDK adapter

Support for linking multiple apps to one PingID SDK adapter. (Previously, a separate adapter was required for each app.) Refer to Configuring the PingID SDK adapter for PingFederate(**Create and configure an adapter → APPLICATION ID**) for further details.

Proxy support

Proxy support for the PingID SDK adapter for PingFederate. Refer to Know the PingID SDK using the Moderno sample app (**PingID SDK properties file**) for further information.

Mobile APIs

PingID mobile SDK for iOS and Android was extended with the following new mobile APIs:

Mobile API	Description
`setAuthenticationUserSelection`	Set the authentication result of the user's selection in the customer app (APPROVE, DENY, or BLOCK). [NOTE] ==== `setAuthenticationUserSelection` has new parameters in PingID SDK Mobile SDK 1.2. The previous version of `setAuthenticationUserSelection` is supported for backward compatibility. ====
`isDeviceTrusted`	Returns the trusted status of the current device.

Mobile API	Description
`validateAuthenticationToken`	Validates the authentication token of a QR code scan.
`authenticationTokenStatus`	Retrieves the token status when it changes.

Refer to PingID SDK Mobile API for further information

Moderno sample app

Support of QR code based authentication

Mobile camera permissions were added, as part of QR code based authentication support. Refer to the code samples included in the PingID SDK Integration Kit package available at PingID Downloads.

PingID SDK (January 8, 2019)

Enhancements

View detailed audit information for PingID SDK application creation

The audit messages in the PingID SDK activity report have been extended to reflect further details about PingID SDK application creation events. The report indicates whether the admin selected PingID SDK's default app configuration settings, or opted to retrieve settings from PingID SDK's configuration of another app.

PingID SDK (December 12, 2018)

Enhancements

PingID SDK has been enhanced with improved error management. The following new status codes have been added:

- FORBIDDEN
- SMS_VOICE_SUSPENDED

PingID SDK Package 1.2 (November 21, 2018)

The PingID SDK 1.2 package is released with the following components:

PingID SDK component	Module	Submodule	Version	Status
PingID Mobile SDK	PingID Mobile SDK for Android		1.1.1	Unchanged
	PingID Mobile SDK for iOS		1.1	Unchanged
PingID SDK Server sample code			1.1	Unchanged
PingFederate PingID SDK Integration Kit 1.1	PingFederate PingID SDK IDP Adapter 1.1	PingFederate PingID SDK IDP Adapter	1.1	New
		PingFederate PingID SDK IDP Selector	1.0	Unchanged
	PingFederate PingID SDK Connector		1.1	New

Enhancements

PingID SDK has been extended with the following features:

PingFederate PingID SDK IDP Adapter 1.1 Voice authentication support

The PingID SDK Adapter provides an out-of-the-box integration between PingID SDK and PingFederate user authentication flow. This adapter reduces the integration effort for PingFederate Customer IAM customers. The PingID SDK Adapter previously supported the Mobile SDK, SMS and Email authentication methods, and has been extended to support Voice authentication.

For further details refer to The PingID SDK adapter for PingFederate.

The PingID SDK Package can be downloaded from the PingID downloads page https://www.pingidentity.com/en/resources/downloads/pingid.html.

PingFederate PingID SDK Connector 1.1

The PingID SDK Connector 1.1 has been extended to include:

- Support for three voice number user attributes.
- Support for primary device authentication configuration.
- Improved error handling and reporting when PingID users contain no ID.

For further details, refer to PingFederate PingID SDK Connector Guide 1.1 and PingFederate PingID SDK Connector 1.1 Release Notes.

Known issues and limitations

The PingID SDK Adapter may not support some network proxies.

PingID SDK (October 31, 2018)

Enhancements

PingID SDK has been extended with the following feature:

PingID SDK Admin Activity Report

PingID now includes an augmented security report detailing recent PingID SDK related admin activities (default: last 7 days). This report can be run within PingOne Admin Console, or streamed as part of the subscription feature. See Running the PingID SDK Admin Activity Report for details.

PingID SDK (August 12, 2018)

Enhancements

PingID SDK has been extended with the following features:

PingID SDK voice support

PingID SDK REST API now supports voice as an alternative method for authentication and transaction approval, including fully customizable and multilingual voice messages for select locales.

- Admin guide:
  - Configuration: Updating a PingID SDK app's configuration
- Developer guide:
  - Overview: Considerations for voice pairing and authentication
  - Pairing API: Offline devices (voice) pairing API
  - Authentication API: Authenticate with Voice

PingID SDK (August 9, 2018)

Enhancements

PingID SDK has been extended with the following features:

View detailed audit information for SMS and Voice message

Detailed audit messages for SMS and Voice authentication transactions are now available as part of the PingID SDK activity report.

SMS and Voice message audit entries now include details about the event, from initiation to delivery. Details may include vendor name, phone number (masked), type, status, price, and carrier name.

SMS and Voice transaction information is now streamed to Splunk and can be viewed and analysed when you subscribe to PingID audit events through the PingOne subscription facility.

PingID SDK (July 18, 2018)

Enhancements

PingID SDK has been extended with the following features:

Detection of uninstalled and reinstalled apps on user devices

PingID SDK permits greater flexibility handling scenarios when an application has been uninstalled from a user device without being unpaired from the server, or reinstalled on a user device.

- `UNINSTALLED_APPLICATION` (error code)
- `DEVICE_MUST_BE_TRUSTED` (error and status code)

Known issues and limitations

Requirement for Swift bridging file

Due to differences between the names of the header file and framework, Swift developers must use a bridging file in order to import the SDK.

PingID SDK (June 25, 2018)

Enhancements

PingID SDK has been extended with the following features:

PingID SDK adapter for PingFederate, including a customisable HTML UI

PingID SDK has been extended to integrate with PingFederate as an authentication solution. The PingID SDK Adapter replaces the customer server in some of the flows, by providing an out-of-the-box integration between PingID SDK and PingFederate user authentication flow. This adapter reduces the integration effort for PingFederate Customer IAM customers.
The PingID SDK Adapter supports all PingID SDK authentication methods: Mobile SDK, SMS and Email.

- PingID SDK Connector, which synchronizes PingID SDK users with PingFederate.
- PingID mobile SDK support for the PingID SDK adapter for PingFederate.

Moderno sample application

- The Moderno sample application now supports offline and fallback OTP flows (iOS and Android).
- The Moderno sample application includes sample code with options for PingID SDK with integration with PingFederate, and for PingID SDK without integration with PingFederate.

Documentation

- Documentation has been restructured and improved, providing an enhanced experience for developers and admins.

Resolved issues

Ticket ID	Description
PIMC-302 and PIMC-303	The Moderno application did not permit sign in when a user was configured on the server to bypass MFA. This issue is now resolved for both iOS and Android.

Known issues and limitations

Moderno sample application:

- The OTP flow for adding a device doesn't contain a retry OTP flow. After entering a wrong or invalid OTP, the user is redirected back to the login screen of the app (iOS and Android)
  .
- The sample Moderno v1.1 application for Android supports Google Chrome browsers only, and the browser version must support the Chrome Custom Tabs library.
- Distorted screens (iOS):

  When using Xcode 9.2 to create apps that deploy to iOS 8 and later, images in the asset catalog may be corrupted when viewed on devices running iOS 8.3 and earlier. This may be handled by building the app using Xcode 9.1, or use Xcode 9.2 and set the deployment target to iOS 8.4 or later.
  Refer to: https://developer.apple.com/library/content/releasenotes/DeveloperTools/RN-Xcode/Chapters/Introduction.html#//apple_ref/doc/uid/TP40001051-CH1-SW936
  .

PingID SDK (May 31, 2018)

Enhancements

Enhanced user experience with dedicated SMS subaccounts

PingID SDK supports a dedicated subaccount for pairing and authentication with SMS one time passcodes (OTPs). You can determine the amount of dedicated phone numbers and the country-code from which the SMS messages will be sent to the users.

For further details and to activate subaccounts, contact Ping Support.

PingID SDK (March 28, 2018)

Enhancements

PingID SDK User API

The User API has been extended to support the following:

- Updating a user's first and last names when the user is inactive.
- Suspending a user across all applications in the organization, or to take the user out of the suspended state.

Backwards compatibility is supported where the older endpoint and parameters are used.

PingID SDK (March 15, 2018)

Enhancements

PingID SDK email support

PingID SDK REST API now supports email as an alternative method for authentication and transaction approval, including fully customizable and multilingual email text.

Deprecated features

SMS pairing endpoint

The new endpoint

`/accounts/{accountId}/applications/{applicationId}/users/{username}/smspairings`

replaces `/accounts/{accountId}/applications/{applicationId}/users/{username}/pairings`

which is now deprecated.

Backwards compatibility is supported where the older endpoint is used.

deviceType parameter

The `deviceType` parameter should no longer be used.

Backwards compatibility is supported where this parameter is used.

PingID Mobile SDK 1.0.2 (21 February 2018)

Enhancements

Registration modes

During a device pairing process, PingID SDK attempts to pair using remote notifications. When successful, the paired device can receive push notifications for ongoing authentication and transaction approvals. If the remote notifications fail, PingID SDK attempts to pair without remote notifications, in which case the paired device can be used as an authenticating device using a one time passcode.

In addition to the existing registration mode (remote notifications with automatic fallback to one time passcode) as described above, PingID mobile SDK has now been extended to support a greater diversity of registration modes. There are now also the options to restrict device registration to either a mode using remote notifications exclusively, or to a mode using a one time passcode exclusively.

Device registration without verification

Device registration has been extended to allow the ability to define the option for an existing active user to pair a new device without the need to verify the new device via the primary device.

Resolved issues

Ticket ID	Description
PIMC-245 PIMC-276	A case was discovered when a device was unpaired and then paired again, an entry for a new device was generated in the list of devices for the user. This issue has been resolved, so that unpairing and pairing the device again will reflect the same single device entry on the list of devices for that user. (**Android** and **iOS**)
PIMC-295 PIMC-309 PIMC-332 PIDC-707	When a device was unpaired on the server side only, the device would fail on the first subsequent login, and would be led into the pairing process on the second login. This has been resolved so that when a device is unpaired only on the server side, it is automatically unpaired on the mobile on the next login attempt, and it will be led directly into the pairing process. (**Android** and **iOS**)
PIDC-347 PIDC-719	If an application ID was set into the mobile application in upper case, it was impossible to pair a user. This issue has been resolved, and the application ID is no longer case sensitive.
PIDC-792	The PingID SDK documentation has been updated to reflect that the `ACCESS_FAILED` error code was replaced by the `UNAUTHORIZED` code.

Resolved in the Moderno demo application

- The progress spinner continued to spin on the paired authenticating device after successful completion of adding a new device. This is resolved so that the spinner disappears once the new device is added. (**Android**)
- When the app was in the background, transaction notifications were only partially displayed. This issue is resolved so that transaction notifications are fully displayed when the app is in the background. (**Android**)

- If a user disabled push notifications, authentication worked correctly in pushless mode, but the pairing process would still attempt to use push notifications. This issue has been resolved, so that when a user has disabled push notifications, pairing will also be performed in pushless mode. (**iOS**)
- The terms "Hosting server" and "Hosting app" have been replaced with the new terminology of "Customer server" and "Customer app", bringing **Android** into alignment with **iOS**.
- The **Unpair from PingID** menu option has been removed from the app. On the **Login** screen there is now no menu at all. On the **Home** screen there is a menu comprising only the single **Logout** option. This aligns the **Android** and **iOS** behavior.

(Ticket IDs: PIMC-262, PIMC-264, PIMC-265, PIMC-282, PIMC-283, PIMC-284, PIMC-313)

SDK code changes

PingID SDK component dependencies in build.gradle (Android)

This version includes new SDK component dependencies for Android. These should be added in the application's `gradle.build` file under `dependencies`. Developers must manually add these dependencies to their project, in order for the SDK to work, as the lib is distributed as a file and not via a repository.

The full list of dependencies is as follows:

```
compile 'org.slf4j:slf4j-api:1.7.7'
compile 'com.github.tony19:logback-android-core:1.1.1-6'
compile('com.github.tony19:logback-android-classic:1.1.1-6') {
    exclude group: 'com.google.android', module: 'android'
}
compile 'com.nimbusds:nimbus-jose-jwt:4.11'
compile 'com.google.code.gson:gson:2.6.2'
compile 'commons-codec:commons-codec:1.5'
compile 'com.madgag:sc-light-jdk15on:1.47.0.3'
compile 'com.madgag:scprov-jdk15on:1.47.0.3'
compile 'com.google.android.gms:play-services-base:10.2.1'
compile 'com.google.firebase:firebase-messaging:10.2.1'
```

Refer to Getting started with Android in PingID SDK for details.

Note

Developers upgrading from PingID SDK 1.0.0 should replace the dependency

```
compile 'io.jsonwebtoken:jjwt:0.7.0'
```

with

```
compile 'com.nimbusds:nimbus-jose-jwt:4.11'
```

as reflected in the updated dependency list above.

Registration mode for pairing (Android and iOS)

The new registration modes use the `Supported MFA type` parameter, which must be added into the PingID SDK initialization:

- **Android**:

  Backward compatibility is maintained with the old initialization

  ```
  PingID.init(<Android application object>, <Application ID>, <Object implementing
  PingIDSDKEvents>,<Push sender ID>);
  ```

  which will continue to support remote notifications with automatic fallback to one time passcode.

  In order to specify the registration mode, initialize the PingID SDK singleton, as described in the initialization step at Getting started with Android in PingID SDK, and repeated below with the new registration mode (`Supported MFA type`) parameter:

  ```
  PingID.init(<Android application object>, <Application ID>, <Object implementing
  PingIDSDKEvents>,<Push sender ID>, <Supported MFA type>);
  ```

  Arguments:

  - `Android application object` : The Android application instance of the customer mobile application.
  - `Application ID` : The application identifier from the Ping Identity web portal.
  - `Object implementing PingIDSDKEvents` : The object which implements the PingIDSDKEvents interface.
  - `Push sender ID` : The GCM/FCM sender ID.
  - `Supported MFA type` : The registration mode for pairing. Possible values:

Registration mode value	Description
`Automatic`	MFA supports remote notifications with automatic fallback to one time passcode.
`EnforceRemoteNotifications`	MFA supports remote notifications only.
`DisableRemoteNotifications`	MFA will not support remote notifications and will only support one time passcode.

- **iOS**:

  Backward compatibility is maintained with the old initialization

  ```
  (void)initWithAppID:(nonnull NSString *)appID
  ```

  which will continue to support remote notifications with automatic fallback to one time passcode.

In order to specify the registration mode, use the new initialization:

```
(void)initWithAppID:(nonnull NSString *)appID supportedMfa:(PIDSupportedMfaType)supportedMfaType;
```

defined as follows:

```
/**
 Supported MFA types

 - PIDSupportedMfaTypeAutomatic:                   MFA supports remote notifications with automatic
fallback to one time passcode
 - PIDSupportedMfaTypeEnforceRemoteNotifications:  MFA supports remote notifications only
 - PIDSupportedMfaTypeDisableRemoteNotifications:  MFA will not support remote notifications and
will only support one time passcode
 */
typedef NS_ENUM(NSUInteger, PIDSupportedMfaType)
{
    PIDSupportedMfaTypeAutomatic                  =   0,
    PIDSupportedMfaTypeEnforceRemoteNotifications =   1,
    PIDSupportedMfaTypeDisableRemoteNotifications =   2
};
```

Known issues and limitations

Initializing a second pairing before completion of the first pairing process on the same device

If a user starts a new pairing process on a device which is still running the process of a previous attempted pairing, it may cause a race condition (**Android** and **iOS**).

- If the admin console shows that a device or multiple devices are paired with the server, but the user cannot authenticate, then admins should unpair the affected devices, and the user should start a new pairing process.
- Developers should create the necessary logic in their applications to prevent users from initiating a new pairing process while there is already a pairing request in progress.

PingID SDK (November 2017)

Enhancements

PingID Mobile SDK SMS support

PingID mobile SDK REST API now supports SMS as an alternative method for authentication and transaction approval, including fully customizable and multilingual SMS text.

Device nickname

PingID SDK now supports the ability to rename users' devices.

Deprecated features

PATCH method in Authentication API

The PATCH method in the Authentication API is no longer available, and is replaced by the new PUT method.

PingID SDK (July 2017)

Enhancements

PingID SDK

PingID SDK has been released as a generally available feature. PingID SDK enables developers of mobile apps on iOS or Android to include advanced functionality that is on-brand and customizable within their mobile applications. This allows organizations to preserve their brand experience, rather than force customers to download a separate MFA application.

Please refer to PingID SDK developer documentation.

Known issues and limitations

Application ID in upper case prevents user pairing

If the application ID is set into the mobile application in upper case, it is impossible to pair a user (PIDC-347).

In the developers' sample app ("Moderno")

- **Unpairing from mobile unpairs users from client only**:

  Unpairing from the mobile in the developers' sample app ("Moderno"), unpairs the user from the client only (local unpair). The user should also be unpaired from the server side.

- **Android: The progress spinner continues spinning after adding a new device**:

  Android: After adding a new device in the Moderno app, the progress spinner on the primary device continues to spin after approval has completed, and does not disappear (PIMC-265).

PingID mobile app release notes

iOS

This section details the release notes for PingID mobile app for iOS.

Mobile app 3.3.0 (June 29, 2025) iOS

New features and improvements in PingID mobile app 3.3.0

Support for TOTP one-time passcodes

New PingID mobile app

We've added support for the use of TOTP one-time passcodes that aren't linked to a PingID account.

Security, performance, and reliability

Improved PingID mobile app

We've made some general improvements to security, performance, and reliability.

Download PingID mobile app for iOS.

Mobile app 3.2.0 (April 3, 2025) iOS

New features and improvements in PingID mobile app 3.2.0

Security, performance, and reliability

Improved PingID mobile app

We made some general improvements to security, performance, and reliability.

Download PingID mobile app for iOS.

Mobile app 3.1.0 (March 10, 2025) iOS

New features and improvements in PingID mobile app 3.1.0

Security, performance, and reliability

Improved PingID mobile app

We made some general improvements to security, performance, and reliability.

Download PingID mobile app for iOS.

Mobile app 3.0 (January 28, 2025) iOS

New features and improvements in PingID mobile app 3.0

Share digital credentials with PingID

New PingID mobile app

PingID mobile app 3.0 introduces a digital credentials wallet (Creds) that includes the following features:

- Store and manage digital credentials that you receive from your organization in the PingID mobile app's new **Creds** tab.
- Securely share your Creds with an organization when requested.

Learn more in Manage and share Creds, in the PingID End User guide.

Mobile app 2.7.0 (November 21, 2024) iOS

New features and improvements in PingID mobile app 2.7.0.

Security, performance, and reliability

Improved PingID mobile app

We made some general improvements to security, performance, and reliability.

Support for iOS 14.x and earlier

Info PingID mobile app

From the next version, PingID mobile app will not support iOS 14.x and earlier.

Download PingID mobile app for iOS.

Mobile app 2.6.0 (October 27, 2024) iOS

New features and improvements in PingID mobile app 2.6.0.

Security, performance, and reliability

Improved PingID mobile app

We made some general improvements to security, performance, and reliability.

Download PingID mobile app for iOS.

Mobile app 2.5.0 (August 1, 2024) iOS

New features and improvements in PingID mobile app 2.5.0.

Accessibility improvements

Improved PingID mobile app

As part of our ongoing efforts to improve accessibility, we've made some necessary updates to the PingID mobile app.

Security, performance, and reliability

Improved PingID mobile app

We made some general improvements to security, performance, and reliability. We also made some more specific improvements to the performance and reliability of PingID mobile app when deleting a PingID user account from the admin portal directory.

Download PingID mobile app for iOS.

Mobile app 2.4.0 (June 18, 2024) iOS

New features and improvements in PingID mobile app 2.4.0.

PingID In-App help for PingOne Verify

New PingID mobile app

We've added a section to the PingID mobile app in-app help that focuses on common questions about PingOne Verify.

Accessibility improvements

Improved PingID mobile app

As part of our ongoing efforts to improve accessibility, we've made some necessary updates to the PingID mobile app.

Security, performance, and reliability

Improved PingID mobile app

We made some general improvements to security, performance, and reliability. We also made some more specific improvements to the performance and reliability of PingID mobile app when deleting a PingID user account from the admin portal directory.

Download PingID mobile app for iOS.

Mobile app 2.3.0 (June 9, 2024) iOS

New features and improvements in PingID mobile app 2.3.0.

Scan manual authentication QR code using phone camera (windows login passwordless)

New PingID mobile app

When authenticating with PingID for windows login passwordless solution, it's possible to scan the manual authentication QR code directly using a mobile device camera. When the user scans the manual authentication QR code with their device camera, PingID mobile app opens automatically, displaying the manual authentication key. Learn more NOTE: This option requires Windows login passworldless 1.6 or later.

Errors in Hungarian text

Fixed PIM-6506 PingID mobile app

We've fixed some UI text errors that appeared in the Hungarian language version of the PingID mobile app.

PingID does not unpair when a PingIDuser account is deleted

Fixed STAGING-22956 PingID mobile app

We've fixed an issue that was preventing the unpairing of the PingID mobile app when deleting a PingID user account from the admin portal directory.

Security, performance, and reliability

Improved PingID mobile app

We made some general improvements to security, performance, and reliability. We also made some more specific improvements to the performance and reliability of PingID mobile app when deleting a PingID user account from the admin portal directory.

Download PingID mobile app for iOS.

Mobile app 2.2.0 (May 5, 2024) iOS

New features and improvements in PingID mobile app 2.2.0.

Lock screen notification enhancements

Improved PingID mobile app

We've updated the lock screen notification to include the name of the organization and its icon. The lock screen notification appearance has also been redesigned.

To show all authentication details on the lock screen, you must enable **Show authentication information** in the admin portal.

Security, performance, and reliability

Improved PingID mobile app

Improvements to security, performance, and reliability.

Download PingID mobile app for iOS.

Mobile app 2.1.0 (April 2, 2024) iOS

New features and improvements in PingID mobile app 2.1.0.

Some buttons and text were obscured when using larger fonts

Fixed | STAGING-22472 | PingID mobile app

We've fixed an issue that was that was impacting users who prefer to use large fonts. To maintain an optimal user experience, the app font size can only be increased to a size within which all text and buttons are still visible on the screen.

Detailed authentication information not appearing on the lock screen

Fixed | STAGING-22485 | PingID mobile app

We've fixed an issue that was preventing some users from viewing the map and the detailed authentication information that should appear after a long tap on the lock screen notification banner (for environments where **Show Authentication Information** is enabled).

Authentication very slow in some instances

Fixed | PIM-6468 | PingID mobile app

We've fixed an issue that was causing authentication to take an unusually long amount of time in some instances.

Authentication hanging on the loading page in some instances

Fixed | PIM-6466 | PingID mobile app

We've fixed an issue that was causing authentication to hang on the loading page in some instances.

Security, performance, and reliability

Improved | PingID mobile app

Improvements to security, performance, and reliability.

Download PingID mobile app for iOS.

Mobile app 2.0.1 (March 4, 2024) iOS

New features and improvements in PingID mobile app 2.0.1.

Issue upgrading to PingID mobile app 2.0

Fixed | PIM-6433 | PingID mobile app

We fixed an issue that was causing PingID mobile app to crash for some iOS users when upgrading to PingID mobile app 2.0.

Download PingID mobile app for iOS.

Mobile app 2.0 (March 3, 2024) iOS

New features and improvements in PingID mobile app 2.0.

We've totally revamped the PingID mobile app. Version 2.0 brings you the following features:

New and enhanced UI/UX

New PingID mobile app

We've refreshed the PingID mobile app UI, bringing you a more Intuitive design with a user-friendly voice and tone, for a visually appealing app.

PingOne Verify Support

New PingID mobile app

Now you can provide your users with secure ID verification within the PingID mobile app. For details, see the:

- Admin experience in the PingOne Cloud platform documentation.
- User experience in the PingID User Guide.

Simple and straightforward Approve authentication flow

New PingID mobile app

We've developed the most straightforward authentication flow to make authentication even easier. Your users now simply tap Approve and they're in! To improve security, you can also include a map indicating the location from which the authentication request originated. For details, see Approving a notification message in the PingID User Guide.

Improved security for one-time passcodes

Improved PingID mobile app

We've changed one-time passcodes to time-based OTPs (TOTPs), for more secure authentication.

QR Code Info Modal for a better registration experience

Improved PingID mobile app

We've added a QR code information modal to help users know where they should look to find their registration QR code, without leaving the registration flow.

Scan button added to the home screen

New PingID mobile app

We've added a camera scan button 

to the PingID mobile app home screen. This enables users to start a Registration, Manual Authentication, or Verification flow from the home screen with just one tap.

In-App Help

New PingID mobile app

We've added an In-app help, so that users can find answers to common questions without needing to leave the app. If more information is required, the In-app help also includes a link to the PingID User Guide.

Security, performance, and reliability

Improved PingID mobile app

We've made improvements to security, performance, and reliability.

Download PingID mobile app for iOS.

Mobile app 1.x (iOS)

New features and improvements covering PingID mobile app 1.x releases.

Mobile app 1.39 (December 3, 2023) iOS

New features and improvements in PingID mobile app 1.39.

Security, performance, and reliability

Improved PingID mobile app

Improvements to security, performance, and reliability.

Support for iOS 13.x and lower

Info PingID mobile app

PingID mobile app does not support iOS 13.x and lower.

Download PingID mobile app for iOS.

Mobile app 1.38 (September 26, 2023) iOS

New features and improvements in PingID mobile app 1.38.

Security, performance, and reliability

Improved PingID mobile app

Improvements to security, performance, and reliability.

Support for iOS 13.x and lower is ending

Info PingID mobile app

From the next version, PingID mobile app will not support iOS 13.x and lower.

Download PingID mobile app for iOS.

Mobile app 1.37 (Jun 15, 2023) iOS

New features and improvements in PingID mobile app 1.37.

Number matching using an Apple Watch

Improved PingID mobile app

We've added the ability to respond to a number-matching authentication request using an Apple Watch. This feature is supported on PingID mobile app 1.37 or later.

For information, see Authenticating using your Apple Watch.

Security, performance and reliability

Improved PingID mobile app

Improvements to security, performance, and reliability.

Download PingID mobile app for iOS.

Mobile app 1.36 (April 24, 2023) iOS

New features and improvements in PingID mobile app 1.36.

Number matching biometrics

Improved PingID mobile app

We've enhanced the user experience if using Number Matching when device biometrics is set to Enabled or Required.

Key rotation issue

Fixed STAGING-18254 PingID mobile app

Fixed an issue related to PingID mobile app key rotation, when the app was used for offline authentication

Security, performance and reliability

Improved PingID mobile app

Improvements to security, performance, and reliability.

Download PingID mobile app for iOS.

Mobile app 1.35 (April 3, 2023) iOS

New features and improvements in PingID mobile app 1.35.

Security, performance and reliability

Improved PingID mobile app

Improvements to security, performance, and reliability.

Download PingID mobile app for iOS.

Mobile app 1.34 (February 20, 2023) iOS

New features and improvements in PingID mobile app 1.34.

Security, performance and reliability

Improved PingID mobile app

Improvements to security, performance, and reliability.

Download PingID mobile app for iOS.

Mobile app 1.33 (January 29, 2023) iOS

New features and improvements in PingID mobile app 1.33.

Warning message no longer displayed unless location data is required

Improved PingID mobile app

As part of our efforts to reduce the collection of location data, PingID mobile app no longer displays a warning message when the user kills the PingID mobile app, unless the organization's policy specifically requires location data.

Security, performance, and reliability

Improved PingID mobile app

Improvements to security, performance, and reliability.

Support for iOS 12.x and lower

Info PingID mobile app

PingID mobile app does not support iOS 12.x and lower.

Download PingID mobile app for iOS.

Mobile app 1.32 (January 9, 2023) iOS

New features and improvements in PingID mobile app 1.32.

Automatic cipher key rotation

New PingID mobile app

We've added a mechanism to automatically rotate mobile cipher keys.

Minimizing user location data collection

Improved PingID mobile app

To address requests to reduce the collection of location data, PingID mobile app no longer requests location data or permissions, unless the organization's policy specifically requires it.

Language support

Improved PingID mobile app

PingID mobile app now supports the following additional languages:

- Czech
- Polish
- Hungarian

Accessibility improvements

Improved PingID mobile app

As part of our ongoing efforts to improve accessibility, we've made some necessary updates to the PingID mobile app.

Security, performance, and reliability

Improved PingID mobile app

Improvements to security, performance, and reliability.

QR camera black screen

Fixed STAGING-16736 PingID mobile app

We fixed an issue that was causing the QR scanning camera to occasionally show a black screen rather than allow the user to scan the QR code.

Support for iOS 12.x and lower is ending

Info PingID mobile app

From the next version, PingID mobile app will not support iOS 12.x and lower.

Download PingID mobile app for iOS.

Mobile app 1.31 (December 13, 2022) iOS

New features and improvements in PingID mobile app 1.31.

Support of PingID mobile app PIN code

New PingID mobile app

PingID mobile app supports the use of a PIN code. When this feature is enabled, users are required to create a PIN code and use it to authenticate with the PingID mobile app. Admins can enforce PIN codes for devices that do not have a device PIN only, or for all devices.

For information, see Configuring the PingID mobile app PIN.

Notify users of new PingID mobile app versions

New PingID mobile app

Users can now be notified that an update to PingID mobile app is available. Users can click a link in the notification to update. Depending on the configuration, updates can be mandatory or optional.

For information, see Enabling PingID mobile app update notifications.

Security, performance, and reliability

Improved PingID mobile app

Improvements to security, performance, and reliability

Fixed an OTP refresh issue

Fixed STAGING-16736 PingID mobile app

Fixed an issue that was preventing the one-time passcode (OTP) from automatically refreshing between authentication attempts.

Download PingID mobile app for iOS.

Mobile app 1.30 (October 25, 2022) iOS

New features and improvements in PingID mobile app 1.30.

Accessibility improvements

Improved PingID mobile app

As part of our ongoing efforts to improve accessibility, we've made some necessary updates to the PingID mobile app.

Performance, security and reliability

Improved PingID mobile app

Improvements to performance, security, and reliability.

Download PingID mobile app for iOS.

Mobile app 1.29 (September 15, 2022) iOS

New features and improvements in PingID mobile app 1.29.

Time-sensitive notifications

New PingID mobile app

Users can now configure their device to receive time-sensitive push notifications from PingID Mobile app. Time-sensitive notifications are notifications that you receive even when your device is in Focus mode. For more information, see Enabling time-sensitive notifications in Focus Mode.

Performance, security and reliability

Improved PingID mobile app

Improvements to performance, security, and reliability.

Download PingID mobile app for iOS.

Mobile app 1.28 (July 28, 2022) iOS

New features and improvements in PingID mobile app 1.28.

Performance and reliability

Improved PingID mobile app

Improvements to security, performance, and reliability.

Download PingID mobile app for iOS.

Mobile app 1.27 (June 12, 2022) iOS

New features and improvements in PingID mobile app 1.27.

Accessibility

Improved PingID mobile app

As part of our ongoing efforts to improve accessibility, we've made some necessary updates to the PingID mobile app.

Performance and reliability

Improved PingID mobile app

Improvements to security, performance, and reliability.

Download PingID mobile app for iOS.

Mobile app 1.26 (May 23, 2022) iOS

New features and improvements in PingID mobile app 1.26.

Performance and reliability

Improved PingID mobile app

Improvements to security, performance, and reliability

Fixed a mobile app stability issue

Fixed STAGING-15370 PingID mobile app

Fixed an issue that could potentially cause PingID Mobile app to crash or to be unpaired for some devices.

Download PingID mobile app for iOS.

Mobile app 1.25 (May 2, 2022) iOS

Enhancements

Accessibility improvements

As part of our ongoing efforts to improve accessibility, we've made some necessary updates to the PingID mobile app.

Performance and reliability

Improvements to performance and reliability.

Download PingID mobile app for iOS.

Mobile app 1.24 (April 13, 2022) iOS

Enhancements

Warning message when unpairing a device

To ensure a user does not unintentionally unpair a device we've updated the warning message that appears immediately after a user clicks **Unpair device** to clarify that if a user unpairs a device, they may lose access to their work resources.

Security, performance and reliability

Improvements to security performance and reliability.

Download PingID mobile app for iOS.

Mobile app 1.23 (March 20, 2022) iOS

Enhancements

Security, performance and reliability

Improvements to security performance and reliability.

Download PingID mobile app for iOS.

Mobile app 1.22 (March 2, 2022) iOS

Enhancements

Security, performance and reliability

Improvements to security performance and reliability.

Resolved issues

Ticket ID	Description
PIM-2967	Fixed an issue that caused iOS devices to transition into pushless mode.

Download PingID mobile app for iOS.

Mobile app 1.21 (Febrary 6, 2022) iOS

Enhancements

Easily update camera permissions

We've added the ability for users who have denied permission to access the camera in the past to access their device camera settings from within PingID mobile app, so they can grant the relevant permissions when required.

Accessibility improvements

As part of our ongoing efforts to improve accessibility, we've made some necessary updates to the PingID mobile app.

Performance and reliability0

Improvements to performance and reliability.

Deprecated features

Support for iOS 11.x and lower

PingID mobile app does not support iOS 11.x and lower.

Download PingID mobile app for iOS.

Mobile app 1.20 (January 13, 2022) iOS

Enhancements

Information regarding location of accessing device

We've improved the location map to include more specific information. The map now includes text showing the location, device type and the browser type for the accessing device.

Support for iOS 15

This version supports iOS 15, and all relevant dependencies have been updated accordingly.

Support for OAEP padding for offline use cases

We've added support for OAEP padding for offline use cases. To take advantage of this feature, the relevant clients must be updated (Windows Login, Mac Login, and the PingID Adapter). To support backward compatibility, we also continue to support current client implementations.

Accessibility improvements

As part of our ongoing efforts to improve accessibility, we've made some necessary updates to the PingID mobile app's VoiceOver screen reader.

Performance and reliability

Improvements to performance and reliability.

Resolved issues

Ticket ID	Description
PIM-2993	Fixed a bug that was sometimes causing users to see zeros instead of a one-time passcode.

Deprecated features

Support for iOS 11.x and lower is ending

From the next version, PingID mobile app will no longer support platforms older than iOS 12.

Download PingID mobile app for iOS.

Mobile app 1.18 (December 2, 2021) iOS

Enhancements

Information regarding location of accessing device

We're adding a map to PingID mobile app push notifications that will show the general region in which an accessing device is located. This could help a user to identify an unauthorized attempt to sign on to their account. The location is generated using Reverse IP lookup, and the map is only shown on the user's authenticating device when relevant location information is available. In future versions we'll be adding more details about location and device type.

For new organizations this feature is enabled automatically. For existing organizations, the feature must be enabled in the admin portal (see Displaying details of accessing device).

Repositioning of the Report Fraud button

We've improved the position of the Report Fraud button, so it's less likely a user will tap it unintentionally.

Accessibility improvements

As part of our ongoing efforts to improve accessibility, we've made some necessary updates to the PingID mobile app.

Performance and reliability

Improvements to performance and reliability.

Resolved issues

Ticket ID	Description
PIM-2667/PIM-2559	Fixed some spelling errors that appeared in the Dutch version of PingID mobile app.

Download PingID mobile app for iOS.

Mobile app 1.17 (November 11, 2021) iOS

Enhancements

Warning message displays when shutting down PingID mobile app

We've added a message to inform the end user that shutting down PingID will decrease device security. The message is displayed when a user attempts to kill PingID mobile app.

Performance and reliability

Improvements to performance and reliability.

Resolved issues

Ticket ID	Description
PIM-2569	Fixed an issue that was causing PingID mobile app to crash for some users when accessing resources using a VPN.

Download PingID mobile app for iOS.

Mobile app 1.16 (October 25, 2021) iOS

Enhancements

Performance, security, and reliability

Improvements to performance, security, and reliability.

Download PingID mobile app for iOS.

Mobile app 1.15 (August 19, 2021) iOS

Enhancements

Support for future release of Windows Login passwordless flows

This version of PingID mobile app includes support for passwordless authentication with Windows login. To increase security, use of One Time Password supports the use of letters as well as numbers during certain Windows login passwordless flows.

Performance, security, and reliability

Improvements to performance, security, and reliability.

Download PingID mobile app for iOS.

Mobile app 1.14 (June 27, 2021) iOS

Enhancements

New welcome screen

We've added a welcome screen, to provide the following information to the end user:

- General overview of PingID mobile app
- How to pair your device with PingID mobile app for the first time
- How to restore PingID mobile app when upgrading or changing your device
- What to do if you can't unpair PingID mobile app yourself

The welcome screen appears when the user opens PingID mobile app for the first time. It is also accessible from the **Pair your device (QR code)** window **Info** button.

One-time passcode (OTP) enhancements

When opening the PingID mobile app, only a valid OTP is displayed and the OTP now appears more rapidly. NOTE: Dotted lines may appear in place of numbers for a few moments, until a valid OTP is shown.

Performance, security, and reliability

Improvements to performance, security, and reliability.

Mobile app 1.13 (January 7, 2021) iOS

Enhancements

Support for iOS 14 location permissions

Permission location has been updated to support precise location requirements in iOS 14.

Photo permissions updated

Photo permissions has been enhanced, so that if a user selects a profile picture, iOS 14 provides PingID mobile app with permissions to access and use only that picture.

Performance, security, and reliability

Improvements to performance, security, and reliability.

Mobile app 1.12 (September 24, 2020) iOS

Enhancements

Device biometrics enforcement

This version of PingID mobile app supports policy enforcement of the use of a biometrics device when pairing or authenticating with PingID.

Performance and reliability

Improvements to performance and reliability.

Mobile app 1.11 (June 30, 2020) iOS

Enhancements

Performance and reliability

Improvements to performance and reliability.

Deprecated features:

Support for iOS v10.x and lower

This version of PingID mobile app does not support iOS 10.x and lower.

Resolved issues

Ticket ID	Description
PIM-1909	Fixed an issue that was preventing some users from authenticating correctly with push notifications.

Mobile app 1.10.0 (December 30, 2019) iOS

Enhancements

This version of PingID mobile app includes the following enhancements:

Face ID background icon support

The Face ID background icon is now presented on all supported devices.

Face ID consent requests

Depending on organization policy, some devices that support Face ID might be required to approve face scans upon authentication for consent and improved security.

User enrollment via email

User experience has improved for users enrolling through email links, with a redirection to the PingID app instead of Safari.

Performance and reliability

Improvements to performance and reliability

Known issues

Issue preventing the biometric dialog from displaying on authentication screen

It's recommended to upgrade to the latest iOS version to avoid a known issue in iOS 13.0 through 13.1.1 that prevents the biometric dialog from displaying in the authentication screen.

Mobile app 1.9 (July 28, 2019) iOS

Enhancements

This version of PingID mobile app for iOS includes the following enhancements:

Multiple regions support

New support for multiple regions helps your organization more easily comply with international regulations.

Performance and reliability

Improvements to performance and reliability

Mobile app 1.8.7 (May 21, 2019) iOS

Enhancements

This version of PingID mobile app for iOS includes the following enhancements:

Transfer PingID to a new device

When a user gets a new device restored from their old device, they can now use the PingID app on their old device to change devices and pair the new one.

Performance and reliability

Improvements to performance and reliability

Mobile app 1.8.6 (March 4, 2019) iOS

Enhancements

This version of PingID mobile app for iOS includes the following enhancements:

Performance and reliability

Improvements to performance and reliability

Mobile app 1.8.5 (October 24, 2018) iOS

Enhancements

This version of PingID mobile app for iOS includes the following enhancements:

Turkish language support

Added Turkish language support for PingID Mobile app and Apple Watch.

Performance and reliability

Improvements to performance and reliability

Mobile app 1.8.4 (September 5, 2018) iOS

Enhancements

This version of PingID mobile app for iOS includes the following enhancements:

Native iPad support

PingID mobile app now includes native iPad support.

Performance and reliability

Improvements to performance and reliability

Mobile app 1.8.3 (July 15, 2018) iOS

Enhancements

This version of PingID mobile app for iOS includes the following enhancements:

Support for iPhone X

PingID mobile app is now supported on the iPhone X.

Performance and reliability

Improvements to performance and reliability

Deprecated features

Support for iOS v9.x and lower

From this version, PingID mobile app no longer supports platforms older than iOS 9.

Support for WatchOS 2 and lower

From this version, PingID mobile app no longer supports WatchOS 2 and lower.

Mobile app 1.8.2 (March 22, 2018)

Enhancements

This version of PingID mobile app includes the following enhancements:

Performance and reliability

Improvements to performance and reliability

Resolved issues

Error during copy/paste of pairing key

Fixed an issue that was causing an error during copy/paste of pairing key on mobile devices

Mobile app 1.8.1 (March 14, 2018)

Enhancements

This version of PingID mobile app includes the following enhancements:

Support for General Data Protection Regulation (GDPR) requirements

Added enhanced privacy for supporting GDPR requirements.

Performance and reliability

Improvements to performance and reliability

Mobile app 1.8.0 (December 18, 2017) iOS

Enhancements

This version of PingID mobile app for iOS includes the following enhancements:

Added support for manual authentication flow

Added support for manual authentication flow. Manual authentication can be used during service interruptions, or network connectivity issues.

Apple Watch authentication speed

Improved authentication speed on Apple Watch.

Performance and reliability

Improvements to performance and reliability.

Deprecated features

Support of iOS v7.x and lower

From this version, PingID mobile app only supports iOS v8.0 and higher.

Archive 2017 and earlier: PingID Mobile app for iOS

22 August, 2017: PingID Mobile app 1.7.6

Enhancements

This version of PingID mobile app for iOS includes the following enhancements:

Performance and reliability

Improvements to performance and reliability.

31 January, 2017: PingID Mobile app 1.7.4

Enhancements

This version of PingID mobile app for iOS includes the following enhancements:

MDM enforcement support

Added MDM enforcement support.

Error messages for pairing policy

Added detailed error messages upon pairing policy failure.

Status bar for post authentication screens

Added a 'Back to' (status bar) to post authentication screens.

Performance and reliability

Improvements to performance and reliability.

December 4, 2016: PingID Mobile app 1.7.3

Enhancements

This version of PingID mobile app for iOS includes the following enhancements:

Performance and reliability

Improvements to performance and reliability.

November 15, 2016: PingID Mobile app 1.7.2

Enhancements

This version of PingID mobile app for iOS includes the following enhancements:

Performance and reliability

Improvements to performance and reliability.

October 7, 2016: PingID Mobile app 1.7.1

Enhancements

This version of PingID mobile app for iOS includes the following enhancements:

iOS 10 support

Added support for iOS 10.

Performance and reliability

Improvements to performance and reliability.

August 31, 2016: PingID Mobile app 1.7

Enhancements

This version of PingID mobile app for iOS includes the following enhancements:

iOS 7.0 support

Added support for iOS 7.0 and later.

Performance and reliability

Improvements to performance and reliability.

July 7, 2016: PingID Mobile app 1.6.4

Enhancements

This version of PingID mobile app for iOS includes the following enhancements:

Language support

The following languages are now supported: Dutch, Italian, Japanese, Korean, Portuguese, Russian, Thai, and Chinese.

Performance and reliability

Improvements to performance and reliability.

May 31, 2016: PingID Mobile app 1.6.3

Enhancements

This version of PingID mobile app for iOS includes the following enhancements:

Apple Watch

Improved authentication responsiveness on Apple Watch.

Performance and reliability

Improvements to performance and reliability.

March 3, 2016: PingID Mobile app 1.6.2

Enhancements

This version of PingID mobile app for iOS includes the following enhancements:

Performance and reliability

Improvements to performance and reliability.

January 19, 2016: PingID Mobile app 1.6.1

Enhancements

This version of PingID mobile app for iOS includes the following enhancements:

iOS 9 support

Compiled for iOS 9.

Australian datacenter

Added support for an Australian data center.

Authentication cancellation

Authentication cancellation from the server support.

Performance and reliability

Improvements to performance and reliability.

November 15, 2015: PingID Mobile app 1.5

Enhancements

This version of PingID mobile app for iOS includes the following enhancements:

Language support

Support French, German and Spanish native languages.

Silent authentication

Support silent authentication without any user interaction.

Performance, security, and reliability

Improvements to performance, security, and reliability.

June 29, 2015: PingID Mobile app 1.4

Enhancements

This version of PingID mobile app for iOS includes the following enhancements:

Apple Watch support

Added support for the Apple Watch application for authentication and One Time Passcode.

Interactive notification

Added an interactive notification option. User slides the notification to the left to confirm authentication on the lock screen (iOS 8+).

Touch ID authentication

Added the option to authenticate with fingerprint (when feature is activated by admin)

Performance, and reliability

Improvements to performance, and reliability

Resolved Issues
Minor UI enhancement

Fixed an issue through a minor UI enhancement.

May 19, 2015: PingID Mobile app 1.3

Enhancements

This version of PingID mobile app for iOS includes the following enhancements:

User organization details and services list

- The main screen now lists the organizations that the user is registered with, replacing the list of services.
- The services list of each company is now shown under the company name: SSO, VPN and SSH. Additional services can be added in the future.

Remove company

Users can click the company name in PingID mobile app to remove it.

Disable swipe authentication

There is now an option to disable swipe through settings and authenticate with OTP only, following customer requests. This option is useful for scenarios where a data network is not available.

Performance, and reliability

Improvements to speed optimization, performance, and reliability.

April 4, 2014: PingID Mobile app 1.2.1

Enhancements

This version of PingID mobile app for iOS includes the following enhancements:

Performance, and reliability

Improvements to performance, and reliability.

Resolved Issues
Device Keychain

Fixed an issue in the device Keychain that was causing authentication errors.

March 9, 2014: PingID Mobile app 1.2

Enhancements

This version of PingID mobile app for iOS includes the following enhancements:

Company name added to 'My services'

Company name added to 'My services' on the home screen.

European PingID data center activation code format

Support added for European PingID data-center activation code format.

Enable iPhone lock/sleep screen after authentication

Enable lock/sleep screen after the authentication process has ended.

SSL deep inspection

Added SSL deep inspection (security feature).

Performance, and reliability

Improvements to performance, and reliability, including swipe screen performance.

July 2, 2014: PingID Mobile app 1.0

The first version of PingID mobile app is now available in the Apple store.

Android

This section details the release notes for PingID mobile app for Android.

Mobile app 3.3.2 (June 30, 2025) Android

New features and improvements in PingID mobile app 3.3.2

Bug fix - crash during identity verification

New PingID mobile app

We've fixed an issue that was causing the app to crash during identity verification.

Download PingID mobile app for Android.

Mobile app 3.3.1 (June 29, 2025) Android

New features and improvements in PingID mobile app 3.3.1

Support for TOTP one-time passcodes

New PingID mobile app

We've added support for the use of TOTP one-time passcodes that are not linked to a PingID account.

Certificate Transparency enforcement

Info PingID mobile app

In preparation for the addition of native Certificate Transparency (CT) support included in the forthcoming Android 16 release, we removed the current support for CT enforcement.

Security, performance, and reliability

Improved PingID mobile app

We've made some general improvements to security, performance, and reliability.

Download PingID mobile app for Android.

Mobile app 3.2.0 (April 3, 2025) Android

New features and improvements in PingID mobile app 3.2.0

Security, performance, and reliability

Improved PingID mobile app

We made some general improvements to security, performance, and reliability.

Download PingID mobile app for Android.

Mobile app 3.1.0 (March 10, 2025) Android

New features and improvements in PingID mobile app 3.1.0

Security, performance, and reliability

Improved PingID mobile app

We made some general improvements to security, performance, and reliability.

Download PingID mobile app for Android.

Mobile app 3.0.1 (February 16, 2025) Android

Error message when using offline MFA

Fixed STAGING-25543 PingID mobile app

When using offline MFA with version 3.0 of the PingID app for Android, there were situations where the app displayed the error message "This isn't the correct authenticating device. Please try again". This issue has been fixed.

Mobile app 3.0 (January 28, 2025) Android

New features and improvements in PingID mobile app 3.0

Share digital credentials with PingID

New PingID mobile app

PingID mobile app 3.0 introduces a digital credentials wallet (Creds) that includes the following features:

- Store and manage digital credentials that you receive from your organization in the PingID mobile app's new **Creds** tab.
- Securely share your Creds with an organization when requested.

Learn more in Manage and share Creds, in the PingID End User guide.

Download PingID mobile app for Android.

Mobile app 2.7.0 (November 21, 2024) Android

New features and improvements in PingID mobile app 2.7.0.

Security, performance, and reliability

Improved PingID mobile app

We've made improvements to security, performance, and reliability.

Support for Android 8.x and earlier

Info PingID mobile app

From the next version, PingID mobile app will not support Android 8.x and earlier.

Download PingID mobile app for Android.

Mobile app 2.6.0 (October 27, 2024) Android

New features and improvements in PingID mobile app 2.6.0.

Security, performance, and reliability

Improved PingID mobile app

We've made improvements to security, performance, and reliability.

Download PingID mobile app for Android.

Mobile app 2.5.0 (August 1, 2024) Android

New features and improvements in PingID mobile app 2.5.0.

Accessibility improvements

New PingID mobile app

As part of our ongoing efforts to improve accessibility, we've made some necessary updates to the PingID mobile app.

Security, performance, and reliability

Improved PingID mobile app

We've made improvements to security, performance, and reliability.

Download PingID mobile app for Android.

Mobile app 2.4.0 (June 18, 2024) Android

New features and improvements in PingID mobile app 2.4.0.

PingID In-App help for PingOne Verify

New PingID mobile app

We've added a section to the PingID mobile app in-app help that focuses on common questions about PingOne Verify.

Accessibility improvements

New PingID mobile app

As part of our ongoing efforts to improve accessibility, we've made some necessary updates to the PingID mobile app. NOTE: This option requires Windows login passworldless 1.6 or later.

Issue causing PingID mobile app to crash during upgrade

Fixed PIM-6818 PingID mobile app

We've fixed an issue that was affecting some users when upgrading from PingID mobile app 2.2.0 to 2.3.0.

Security, performance, and reliability

Improved PingID mobile app

We've made improvements to security, performance, and reliability.

Download PingID mobile app for Android.

Mobile app 2.3.0 (June 9, 2024) Android

New features and improvements in PingID mobile app 2.3.0.

Scan manual authentication QR code using phone camera (windows login passwordless)

New PingID mobile app

When authenticating with PingID for windows login passwordless solution, it's possible to scan the manual authentication QR code directly using a mobile device camera. When the user scans the manual authentication QR code with their device camera, PingID mobile app opens automatically, displaying the manual authentication key. Learn more NOTE: This option requires Windows login passworldless 1.6 or later.

Errors in Hungarian text

Fixed PIM-6506 PingID mobile app

We've fixed some UI text errors that appeared in the Hungarian language version of the PingID mobile app.

Security, performance, and reliability

Improved PingID mobile app

We've made improvements to security, performance, and reliability.

Download PingID mobile app for Android.

Mobile app 2.2.0 (May 5, 2024) Android

New features and improvements in PingID mobile app 2.2.0.

Lock screen notification enhancements

Improved PingID mobile app

We've updated the lock screen notification to include the name of the organization and its icon, the name of the app or account the user wants to access, and the city in which the accessing device is located. The lock screen notification appearance has also been redesigned.

To show all authentication details on the lock screen, you must enable **Show authentication information** in the admin portal.

Security, performance, and reliability

Improved PingID mobile app

We've made improvements to security, performance, and reliability.

Download PingID mobile app for Android.

Mobile app 2.1.0 (April 2, 2024) Android

New features and improvements in PingID mobile app 2.1.0.

Some buttons and text were obscured when using larger fonts

Fixed STAGING-22472 PingID mobile app

We've fixed an issue that was that was impacting users who prefer to use large fonts. To maintain an optimal user experience, the app font size can only be increased to a size within which all text and buttons are still visible on the screen.

Security, performance, and reliability

Improved PingID mobile app

We've made improvements to security, performance, and reliability.

Download PingID mobile app for Android.

Mobile app 2.0 (March 3, 2024) Android

New features and improvements in PingID mobile app 2.0.

We've totally revamped the PingID mobile app. Version 2.0 brings you the following features:

New and enhanced UI/UX

New PingID mobile app

We've refreshed the PingID mobile app UI, bringing you a more Intuitive design with a user-friendly voice and tone, for a visually appealing app.

PingOne Verify Support

New PingID mobile app

Now you can provide your users with secure ID verification within the PingID mobile app. For details, see the:

- Admin experience in the PingOne Cloud platform documentation.
- User experience in the PingID User Guide.

Simple and straightforward Approve authentication flow

New PingID mobile app

We've developed the most straightforward authentication flow to make authentication even easier. Your users now simply tap Approve and they're in! To improve security, you can also include a map indicating the location from which the authentication request originated. For details, see Approving a notification message in the PingID User Guide.

Improved security for one-time passcodes

Improved PingID mobile app

We've changed one-time passcodes to time-based OTPs (TOTPs), for more secure authentication.

QR Code Info Modal for a better registration experience

Improved PingID mobile app

We've added a QR code information modal to help users know where they should look to find their registration QR code, without leaving the registration flow.

Scan button added to the home screen

New PingID mobile app

We've added a camera scan button to the PingID mobile app home screen. This enables users to start a Registration, Manual Authentication, or Verification flow from the home screen with just one tap.

In-App Help

New PingID mobile app

We've added an In-app help, so that users can find answers to common questions without needing to leave the app. If more information is required, the In-app help also includes a link to the PingID User Guide.

Security, performance, and reliability

Improved PingID mobile app

We've made improvements to security, performance, and reliability.

Download PingID mobile app for Android.

Mobile app 1.x (Android)

New features and improvements covering PingID mobile app 1.x releases.

Mobile app 1.39 (December 3, 2023) Android

New features and improvements in PingID mobile app 1.39.

Security, performance and reliability

Improved PingID mobile app

Improvements to security, performance, and reliability.

Mobile app 1.38 (September 26, 2023) Android

New features and improvements in PingID mobile app 1.38.

Security, performance and reliability

Improved PingID mobile app

Improvements to security, performance, and reliability.

Mobile app 1.37 (June 15, 2023) Android

New features and improvements in PingID mobile app 1.37.

Security, performance and reliability

Improved PingID mobile app

Improvements to security, performance, and reliability.

Mobile app 1.36.1 (May 3, 2023) Android

New features and improvements in PingID mobile app 1.36.1.

Authentication failure after offline authentication

Fixed STAGING-19241 PingID mobile app

Fixed an issue that caused authentication to occasionally fail after using offline authentication at least once in PingID mobile app 1.36.

Mobile app 1.36 (April 24, 2023) Android

New features and improvements in PingID mobile app 1.36.

Number matching biometrics

Improved PingID mobile app

We've enhanced the user experience if using Number Matching when device biometrics is set to Enabled or Required.

Key rotation issue

Fixed STAGING-18254 PingID mobile app

Fixed an issue related to PingID mobile app key rotation, when the app was used for offline authentication

Security, performance and reliability

Improved PingID mobile app

Improvements to security, performance, and reliability.

Download PingID mobile app for Android.

Mobile app 1.35 (April 3, 2023) Android

New features and improvements in PingID mobile app 1.35.

Performance, security, and reliability

New PingID mobile app

Improvements to performance, security and reliability.

Download PingID mobile app for Android.

Mobile app 1.34 (February 20, 2023) Android

New features and improvements in PingID mobile app 1.34.

Performance, security, and reliability

Improved PingID mobile app

Improvements to performance, security and reliability.

Download PingID mobile app for Android.

Mobile app 1.33 (January 29, 2023) Android

New features and improvements in PingID mobile app 1.33.

Security, performance, and reliability

Improved PingID mobile app

Improvements to security, performance, and reliability.

Download PingID mobile app for Android.

Mobile app 1.32 (January 9, 2023) Android

New features and improvements in PingID mobile app 1.32.

Automatic cipher key rotation

New PingID mobile app

We've added a mechanism to automatically rotate mobile cipher keys.

Minimizing user location data collection

Improved PingID mobile app

To address requests to reduce the collection of location data, PingID mobile app no longer requests location data or permissions, unless the organization's policy specifically requires it.

Language support

Improved PingID mobile app

PingID mobile app now supports the following additional languages:

- Czech

- Polish
- Hungarian

Accessibility improvements

Improved PingID mobile app

As part of our ongoing efforts to improve accessibility, we've made some necessary updates to the PingID mobile app.

Security, performance, and reliability

Improved PingID mobile app

Improvements to security, performance, and reliability.

Download PingID mobile app for Android.

Mobile app 1.31 (December 13, 2022) Android

New features and improvements in PingID mobile app 1.31.

Support of PingID mobile app PIN code

New PingID mobile app

PingID mobile app supports the use of a PIN code. When this feature is enabled, users are required to create a PIN code and use it to authenticate with the PingID mobile app. Admins can enforce PIN codes for devices that do not have a device PIN only, or for all devices.

Notify users of new PingID mobile app versions

New PingID mobile app

Users can now be notified that an update to PingID mobile app is available. Users can click a link in the notification to update. Depending on the configuration, updates can be mandatory or optional. \{link in the admin guide}

Security, performance, and reliability

Improved PingID mobile app

Improvements to security, performance, and reliability

Fixed an OTP refresh issue

Fixed STAGING-16736 PingID mobile app

Fixed an issue that was preventing the one-time passcode (OTP) from automatically refreshing between authentication attempts.

Download PingID mobile app for Android.

Mobile app 1.30 (October 25, 2022) Android

New features and improvements in PingID mobile app 1.30.

Support of Android 13

Info PingID mobile app

PingID mobile app now supports Android 13.

Accessibility improvements

Improved PingID mobile app

As part of our ongoing efforts to improve accessibility, we've made some necessary updates to the PingID mobile app.

Performance, security, and reliability

Improved PingID mobile app

Improvements to performance, security and reliability.

Download PingID mobile app for Android.

Mobile app 1.29 (September 15, 2022) Android

New features and improvements in PingID mobile app 1.29.

Performance, security, and reliability

Improved PingID mobile app

Improvements to performance, security and reliability.

Download PingID mobile app for Android.

Mobile app 1.28 (July 28, 2022) Android

New features and improvements in PingID mobile app 1.28.

Performance, security, and reliability

Improved PingID mobile app

Improvements to performance, security and reliability.

Fixed an issue with the organizations list

Fixed PIM-3479 PingID mobile app

Fixed an issue that was preventing users from viewing a complete list of organizations paired with their account when more than five organizations are added.

Download PingID mobile app for Android.

Mobile app 1.27 (June 12, 2022) Android

New features and improvements in PingID mobile app 1.27.

Performance, security, and reliability

Improved PingID mobile app

Improvements to performance, security and reliability.

Download PingID mobile app for Android.

Mobile app 1.26 (May 23, 2022) Android

New features and improvements in PingID mobile app 1.26.

Performance and reliability

Improved PingID mobile app

Improvements to security, performance, and reliability

Download PingID mobile app for Android.

Mobile app 1.25 (May 2, 2022) Android

Enhancements

Accessibility improvements

As part of our ongoing efforts to improve accessibility, we've made some necessary updates to the PingID mobile app.

Performance and reliability

Improvements to performance and reliability.

Download PingID mobile app for Android.

Mobile app 1.24 (April 13, 2022) Android

Enhancements

Warning message when unpairing a device

To ensure a user does not unintentionally unpair a device we've updated the warning message that appears immediately after a user clicks **Unpair device** to clarify that if a user unpairs a device, they may lose access to their work resources.

Security, performance and reliability

Improvements to security, performance and reliability.

Resolved Issues

Ticket ID	Description
PIM-3217	We fixed an issue that was preventing some users of PingID mobile app 1.23 from authenticating, or using a one-time passcode.

Download PingID mobile app for Android.

Mobile app 1.23 (March 20, 2022) Android

Enhancements

Security, Performance and reliability

Improvements to security, performance and reliability.

Download PingID mobile app for Android.

Mobile app 1.21 (February 6, 2022) Android

Enhancements

Easily update camera permissions

We've added the ability for users who have denied permission to access the camera in the past to access their device camera settings from within PingID mobile app, so they can grant the relevant permissions when required.

Accessibility improvements

As part of our ongoing efforts to improve accessibility, we've made some necessary updates to the PingID mobile app.

Performance and reliability

Improvements to performance and reliability.

Deprecated features

Support for Android 7.x and lower

PingID mobile app does not support Android 7.x and lower.

Download PingID mobile app for Android.

Mobile app 1.19 (January 6, 2022) Android

Enhancements

Information regarding location of accessing device

We've improved the location map to include more specific information. The map now includes text showing the location, device type and the browser type for the accessing device.

Support for OAEP padding for offline use cases

We've added support for OAEP padding for offline use cases. To take advantage of this feature, the relevant clients must be updated (Windows Login, Mac Login, and the PingID Adapter). To support backward compatibility, we also continue to support current client implementations.

Accessibility improvements

As part of our ongoing efforts to improve accessibility, we've made some necessary updates to the PingID mobile app's TalkBack screen reader.

Performance, security, and reliability

Improvements to performance, security, and reliability.

Deprecated features

Support for Android 7.x and lower is ending

From the next version, PingID mobile app will no longer support platforms older than Android 8.

Download PingID mobile app for Android.

Mobile app 1.18 (December 2, 2021) Android

Enhancements

Information regarding location of accessing device

We're adding a map to PingID mobile app push notifications that will show the general region in which an accessing device is located. This could help a user to identify an unauthorized attempt to sign on to their account. The location is generated using Reverse IP lookup, and the map is only shown on the user's authenticating device when relevant location information is available. In future versions we'll be adding more details about location and device type.

This feature is available for users running Android 8 or later.

For new organizations this feature is enabled automatically. For existing organizations, the feature must be enabled in the admin portal (see Displaying details of accessing device).

Repositioning of the Report Fraud button

We've improved the position of the Report Fraud button, so it's less likely a user will tap it unintentionally.

Recent apps screen

The PingID app now appears on the recent apps screen.

Accessibility improvements

As part of our ongoing efforts to improve accessibility, we've made some necessary updates to the PingID mobile app.

Performance and reliability

Improvements to performance and reliability.

Resolved Issues

Ticket ID	Description
PIM-2667/PIM-2559	Fixed some spelling errors that appeared in the Dutch version of PingID mobile app.

Download PingID mobile app for Android.

Mobile app 1.17 (November 11, 2021) Android

Enhancements

Performance, security, and reliability

Improvements to performance, security, and reliability.

Deprecated features

Refresh OTP using a shake

We've removed the ability to refresh the PingID mobile app one-time password (OTP) by shaking your Android device.

Download PingID mobile app for Android.

Mobile app 1.16 (October 25, 2021) Android

Enhancements

Performance, security, and reliability

Improvements to performance, security, and reliability.

Download PingID mobile app for Android.

Mobile app 1.15 (August 19, 2021) Android

Enhancements

Support for future release of Windows Login passwordless flows

This version of PingID mobile app includes support for passwordless authentication with Windows login. To increase security, use of One Time Password supports the use of letters as well as numbers during certain Windows login passwordless flows.

Performance, security, and reliability

Improvements to performance, security, and reliability.

Download PingID mobile app for Android.

Mobile app 1.14.1 (July 1, 2021) Android

Resolved issues

Offline authentication issue associated with PingID mobile app for Android 1.14

Fixed an issue with background location that was causing offline authentication to fail in PingID mobile app 1.14

Mobile app 1.14 (June 27, 2021) Android

Enhancements

New welcome screen

We've added a welcome screen, to provide the following information to the end user:

- General overview of PingID mobile app
- How to pair your device with PingID mobile app for the first time
- How to restore PingID mobile app when upgrading or changing your device
- What to do if you can't unpair PingID mobile app yourself

The welcome screen appears when the user opens PingID mobile app for the first time. It is also accessible from the **Pair your device (QR code)** window **Info** button.

One-time passcode (OTP) enhancements

When opening the PingID mobile app, only a valid OTP is displayed and the OTP now appears more rapidly. NOTE: Dotted lines may appear in place of numbers for a few moments, until a valid OTP is shown.

Performance, security, and reliability

Improvements to performance, security, and reliability.

Deprecated features

Support for Android 6 and lower

This version of PingID mobile app does not support Android 6.x and lower.

Mobile app 1.13 (January 7, 2021) Android

Enhancements

Support for Android 11

This version supports Android 11, and all relevant dependencies have been updated accordingly.

Improved support for accessing the user's location in the background

This version now supports the fine and background location enhancements added in Android 11, and presents the relevant options to the end user.

Camera settings enhancement

We now harness the native camera framework when initiating QR and self facing cameras, to improve performance.

Performance and reliability

Improvements to performance and reliability.

Deprecated features

Support for Android 6 and lower due to end soon

The next version of PingID mobile app will not support Android 6 and lower.

Mobile app 1.12.2 (October 27, 2020) Android

Enhancements

Performance and reliability

Improvements to performance and reliability.

Resolved issues

Registration issue associated with PingID mobile app for Android 1.12.1

Fixed an issue that was causing registration to fail for some users running PingID mobile app for Android 1.12.1.

Mobile app 1.12.1 (September 29, 2020) Android

Enhancements

Performance and reliability

Improvements to performance and reliability

Resolved issues

Registration and authentication issue associated with PingID mobile app for Android 1.12.0

Fixed an issue that was causing authentication and registration to fail for some users running PingID mobile app 1.12.0 for Android

Mobile app 1.12 (Sepember 24, 2020) Android

Enhancements

Device biometrics enforcement

This version of PingID mobile app supports policy enforcement of the use of a biometrics device when pairing or authenticating with PingID.

Performance and reliability

Improvements to performance and reliability.

Mobile app 1.11 (August 6, 2020) Android

Enhancements

Support for biometrics for Android

We enhanced the use of biometrics authentication with PingID to include face and iris on supported devices. We also improved the use of fingerprint authentication with PingID mobile app.

Performance and reliability

Improvements to performance and reliability

Deprecated Features

Support for Android 5.x and lower

This version of PingID mobile app does not support Android 5.x and lower.

Known Limitations

Limitations of face and iris recognition support on some Android devices

Due to Android biometrics API security limitations, face and iris recognition are not supported on some Android devices.

On a limited number of these devices, face or iris recognition is supported when fingerprint recognition is also configured on the device.

Mobile app 1.10 (April 20, 2020) Android

Enhancements

Android 10 support

PingID mobile app now supports Android v10.

Performance and reliability

Improvements to performance and reliability

Resolved issues

Notification sounds while device in silent mode

Fixed an issue with notification sounds when the PingID banner is presented while a device is in silent mode.

Mobile app 1.9.2 (March 16, 2020) Android

This version of PingID mobile app is only available from the PingID downloads page.

Enhancements

Performance and reliability

Improvements to performance and reliability

Resolved issues

Google play services error when running PingID mobile app

Fixed an issue in which some devices that do not have Google play services return an error when running PingID mobile app. This issue is found when downloading PingID mobile app v1.9.1 from the PingID downloads page, and is fixed in v1.9.2

Mobile app 1.9.1 (August 14, 2019) Android

EnhancementsThis version of PingID mobile app includes the following enhancements:

Secure notification banners for Android Q users

Android Q users gain a new authentication experience with more secure notification banners when authentication is required.

Performance and reliability

Improvements to performance and reliability

Mobile app 1.9 (July 23, 2019) Android

Enhancements

This version of PingID mobile app includes the following enhancements:

Multiple regions support

New support for multiple regions helps your organization more easily comply with international regulations.

Performance and reliability

Improvements to performance and reliability

Mobile app 1.8.7 (May 21, 2019) Android

Enhancements

This version of PingID mobile app includes the following enhancements:

Performance and reliability

Improvements to performance and reliability

Mobile app 1.8.5 (October 24, 2018) Android

Enhancements

This version of PingID mobile app includes the following enhancements:

Turkish language support

Added Turkish language support.

Performance and reliability

Improvements to performance and reliability

Mobile app 1.8.4.1 (October 2, 2018) Android

Enhancements

This version of PingID mobile app includes the following enhancements:

Performance and reliability

Improvements to performance and reliability

Resolved issues

Error causing some devices to be reported as rooted

Fixed an issue that was causing some devices to be reported as rooted.

Mobile app 1.8.4 (September 5, 2018) Android

Enhancements

This version of PingID mobile app includes the following enhancements:

Performance and reliability

Improvements to performance and reliability

Deprecated features

Support for Android v5.x and lower

From this version, PingID mobile app no longer supports Android v5 and lower.

Mobile app 1.8.2 (March 22, 2018)

Enhancements

This version of PingID mobile app includes the following enhancements:

Performance and reliability

Improvements to performance and reliability

Resolved issues

Error during copy/paste of pairing key

Fixed an issue that was causing an error during copy/paste of pairing key on mobile devices

Mobile app 1.8.1 (March 14, 2018)

Enhancements

This version of PingID mobile app includes the following enhancements:

Support for General Data Protection Regulation (GDPR) requirements

Added enhanced privacy for supporting GDPR requirements.

Performance and reliability

Improvements to performance and reliability

Mobile app 1.8.0 (December 18, 2017) Android

Enhancements

This version of PingID mobile app includes the following enhancements:

Added support for manual authentication flow

Added Support for manual authentication flow. Manual authentication can be used during service interruptions, or network connectivity issues.

Improved function when "Super Su" app disabled.

Improved the ability for PingID mobile app to function when the "Super Su" app is disabled.

Performance and reliability

Improvements to performance and reliability.

Archive 2017 and earlier: PingID Mobile app for Android

22 August, 2017: PingID Mobile app 1.7.6

Enhancements

This version of PingID mobile app for iOS includes the following enhancements:

Performance and reliability

Improvements to performance and reliability.

31 January, 2017: PingID Mobile app 1.7.4

Enhancements

This version of PingID mobile app for iOS includes the following enhancements:

MDM enforcement support

Added MDM enforcement support.

Error messages for pairing policy

Added detailed error messages upon pairing policy failure.

Status bar for post authentication screens

Added a 'Back to' (status bar) to post authentication screens.

Performance and reliability

Improvements to performance and reliability.

December 4, 2016: PingID Mobile app 1.7.3

Enhancements

This version of PingID mobile app for iOS includes the following enhancements:

Performance and reliability

Improvements to performance and reliability.

November 15, 2016: PingID Mobile app 1.7.2

Enhancements

This version of PingID mobile app for iOS includes the following enhancements:

Performance and reliability

Improvements to performance and reliability.

October 7, 2016: PingID Mobile app 1.7.1

Enhancements

This version of PingID mobile app for iOS includes the following enhancements:

iOS 10 support

Added support for iOS 10.

Performance and reliability

Improvements to performance and reliability.

August 31, 2016: PingID Mobile app 1.7

Enhancements

This version of PingID mobile app for iOS includes the following enhancements:

iOS 7.0 support

Added support for iOS 7.0 and later.

Performance and reliability

Improvements to performance and reliability.

July 7, 2016: PingID Mobile app 1.6.4

Enhancements

This version of PingID mobile app for iOS includes the following enhancements:

Language support

The following languages are now supported: Dutch, Italian, Japanese, Korean, Portuguese, Russian, Thai, and Chinese.

Performance and reliability

Improvements to performance and reliability.

May 31, 2016: PingID Mobile app 1.6.3

Enhancements

This version of PingID mobile app for iOS includes the following enhancements:

Apple Watch

Improved authentication responsiveness on Apple Watch.

Performance and reliability

Improvements to performance and reliability.

March 3, 2016: PingID Mobile app 1.6.2

Enhancements

This version of PingID mobile app for iOS includes the following enhancements:

Performance and reliability

Improvements to performance and reliability.

January 19, 2016: PingID Mobile app 1.6.1

Enhancements

This version of PingID mobile app for iOS includes the following enhancements:

iOS 9 support

Compiled for iOS 9.

Australian datacenter

Added support for an Australian data center.

Authentication cancellation

Authentication cancellation from the server support.

Performance and reliability

Improvements to performance and reliability.

November 15, 2015: PingID Mobile app 1.5

Enhancements

This version of PingID mobile app for iOS includes the following enhancements:

Language support

Support French, German and Spanish native languages.

Silent authentication

Support silent authentication without any user interaction.

Performance, security, and reliability

Improvements to performance, security, and reliability.

June 29, 2015: PingID Mobile app 1.4

Enhancements

This version of PingID mobile app for iOS includes the following enhancements:

Apple Watch support

Added support for the Apple Watch application for authentication and One Time Passcode.

Interactive notification

Added an interactive notification option. User slides the notification to the left to confirm authentication on the lock screen (iOS 8+).

Touch ID authentication

Added the option to authenticate with fingerprint (when feature is activated by admin)

Performance, and reliability

Improvements to performance, and reliability/**Resolved Issues**

Minor UI enhancement

Fixed an issue through a minor UI enhancement.

May 19, 2015: PingID Mobile app 1.3

Enhancements

This version of PingID mobile app for iOS includes the following enhancements:

User organization details and services list

- The main screen now lists the organizations that the user is registered with, replacing the list of services.
- The services list of each company is now shown under the company name: SSO, VPN and SSH. Additional services can be added in the future.

Remove company

Users can click the company name in PingID mobile app to remove it.

Disable swipe authentication

There is now an option to disable swipe through settings and authenticate with OTP only, following customer requests. This option is useful for scenarios where a data network is not available.

Performance, and reliability

Improvements to speed optimization, performance, and reliability.

April 4, 2014: PingID Mobile app 1.2.1

Enhancements

This version of PingID mobile app for iOS includes the following enhancements:

Performance, and reliability

Improvements to performance, and reliability.**Resolved Issues**

Device Keychain

Fixed an issue in the device Keychain that was causing authentication errors.

March 9, 2014: PingID Mobile app 1.2

Enhancements

This version of PingID mobile app for iOS includes the following enhancements:

Company name added to 'My services'

Company name added to 'My services' on the home screen.

European PingID data center activation code format

Support added for European PingID data-center activation code format.

Enable iPhone lock/sleep screen after authentication

Enable lock/sleep screen after the authentication process has ended.

SSL deep inspection

Added SSL deep inspection (security feature).

Performance, and reliability

Improvements to performance, and reliability, including swipe screen performance.

July 2, 2014: PingID Mobile app 1.0

The first version of PingID mobile app is now available in the Apple store.

PingID Integration Kit for PingFederate

PingID Integration Kit 2.28 (February 27, 2025)

New features and improvements in PingID Integration Kit 2.28 for PingFederate.

The PingID Integration Kit 2.28 for PingFederate is released with the following components:

PingID Integration Kit component	Version	Status
PingID Adapter	2.16	New
PingID RADIUS PCV	3.1.0	New
PingID SaaS Connector	1.1.1	Unchanged

PingID Adapter authentication from two different tenants

New PingID Integration kit for PingFederate

It is now possible to authenticate from two separate instances of the PingID Adapter, where each instance points to a different tenant. This allows users to authenticate to more than one organization.

PingID Adapter support for Microsoft EAM integration

Fixed STAGING-25038 PingID Integration kit for PingFederate

We've added the `eamAmr` attribute to the list of PingID authentication attributes. This allows you to map the attribute and use it to evaluate PingFederate policies upon successful authentication with PingID. Additionally, it facilitates integration with Microsoft Entra ID's External Authentication Methods (EAM).

Learn more in PingID authentication attributes.

Blast-RADIUS security enhancement

Improved PingID Integration kit for PingFederate

We've made some enhancements to the RADIUS PCV client security configuration to mitigate the risk of a Blast-RADIUS attack.

Learn more in the PingID RADIUS PCV parameters reference guide.

Direct OTP Validation enhancements

Improved PingID Integration kit for PingFederate

We've expanded the capabilities of the Direct OTP validation field. It is now possible to perform OTP (one-time passcode) validation for RADIUS clients that do not support access-challenge, or lack a Delegate PCV configuration, as well as for clients opting to use LDAP as an Attribute Source within the Delegate PCV setup.

Learn more in the PingID RADIUS PCV parameters reference guide.

PingID `Service ID` field removed

Info PingID Integration kit for PingFederate

The PingID Service ID field is deprecated and is removed from PingFederate.

> **Note**
>
> In RADIUS 3.0.4 or earlier, where the PingID `Service ID` field still exists, if the field is populated, an error message informs administrators that the field value should be updated to `VPN`.

OTP fallback inadvertently triggered

Fixed STAGING-19409 PingID Integration kit for PingFederate

We've fixed an issue that was preventing OTPs from being received during a push service outage, and inadvertently causing RADIUS PCV to trigger OTP fallback.

PingID Integration Kit 2.27 (June 25, 2024)

New features and improvements in PingID Integration Kit 2.27 for PingFederate.

The PingID Integration Kit 2.27 for PingFederate is released with the following components:

PingID Integration Kit component	Version	Status
PingID Adapter	2.15	New
PingID RADIUS PCV	3.0.4	Unchanged
PingID SaaS Connector	1.1.1	Unchanged

PingID Adapter attributes

Fixed STAGING-20564 PingID Integration kit for PingFederate

We've added the following attributes to the PingID Adapter:

- `pingid.authentication.accessing.device.country`

- `pingid.authentication.accessing.device.ip.reputation`

Learn more: PingID authentication attributes.

Configuration replication request triggered unnecessarily in PingFederate

Fixed | STAGING-13107 | PingID Integration kit for PingFederate

We've fixed an issue that was incorrectly triggering the Configuration Replication required message in PingFederate when in cluster mode.

Issue resolving the Resume URL in the SLO flow

Fixed | STAGING-22691 | PingID Integration kit for PingFederate

We've fixed an issue with one of the SLO (Single Log Off) flows that was preventing the Resume URL from resolving correctly.

Security enhancements

Improved | PingID Integration kit for PingFederate

We've made some security enhancements.

PingID Integration Kit 2.26 (September 19, 2023)

New features and improvements in PingID Integration Kit 2.26 for PingFederate.

The PingID Integration Kit 2.26 for PingFederate is released with the following components:

PingID Integration Kit component	Version	Status
PingID Adapter	2.14	Unchanged
PingID RADIUS PCV	3.0.4	New
PingID SaaS Connector	1.1.1	Unchanged

Direct OTP validation for RADIUS PCV clients

Improved | PingID Integration kit for PingFederate

We've added the option to perform OTP validation for RADIUS clients that do not support access-challenge and do not have a Delegate PCV configured.

PingID properties file encrypted

Improved | PingID Integration kit for PingFederate

From RADIUS PCV 3.0.4 and later, the PingID properties file is encrypted after it is uploaded to PingFederate.

> **Note**
>
> If you are upgrading from an earlier version, to ensure the properties file is encrypted, you need to upload it to the PingID RADIUS PCV instance in PingFederate.

More efficient resource consumption

Improved PingID Integration kit for PingFederate

We have improved resource consumption when the RADIUS Server is in communication with PingID server.

Security enhancements

Improved PingID Integration kit for PingFederate

We've made some security enhancements.

PingID Integration Kit 2.25 (June 22, 2023)

New features and improvements in PingID Integration Kit 2.25 for PingFederate.

The PingID Integration Kit 2.25 for PingFederate is released with the following components:

PingID Integration Kit component	Version	Status
PingID Adapter	2.14	New
PingID RADIUS PCV	3.0.3	Unchanged
PingID SaaS Connector	1.1.1	Unchanged

PingID properties file obfuscated and encrypted

Improved PingID Integration kit for PingFederate

From PingID Adapter 2.14 and later, the PingID properties file is encrypted and obfuscated.

> **Note**
>
> From PingID Adapter 2.14 and later, the PingID properties file is obfuscated automatically. However, to ensure it is also encrypted, you need to download a new copy of the PingID properties file and then upload it to the PingID Adapter instance in PingFederate.

Support for additional Phone and Voice attributes

Improved PingID Integration kit for PingFederate

We've added support for a secondary attribute for SMS and Voice. For information, see Configuring a PingID Adapter instance.

PingID Integration Kit 2.24 (February 21, 2023)

New features and improvements in PingID Integration Kit 2.24 for PingFederate.

The PingID Integration Kit 2.24 for PingFederate is released with the following components:

PingID Integration Kit component	Version	Status
PingID Adapter	2.13.2	Unchanged
PingID RADIUS PCV	3.0.3	New
PingID SaaS Connector	1.1.1	Unchanged

PingID RADIUS PCV authentication failure

Fixed PID-12922 PingID Integration kit for PingFederate

We fixed an issue that was causing authentication to fail on mobile devices when a Delegate PCV is not defined.

PingID Integration Kit 2.23 (January 31, 2023)

New features and improvements in PingID Integration Kit 2.23 for PingFederate.

The PingID Integration Kit 2.23 for PingFederate is released with the following components:

PingID Integration Kit component	Version	Status
PingID Adapter	2.13.2	Unchanged
PingID RADIUS PCV	3.0.2	New
PingID SaaS Connector	1.1.1	Unchanged

PingID RADIUS PCV error

Fixed PID-12884 PingID Integration kit for PingFederate

We've fixed an issue that was causing an error if a Delegate PCV is not defined.

PingID Integration Kit 2.22 (January 17, 2023)

New features and improvements in PingID Integration Kit 2.22 for PingFederate.

The PingID Integration Kit 2.22 for PingFederate is released with the following components:

PingID Integration Kit component	Version	Status
PingID Adapter	2.13.2	New
PingID RADIUS PCV	3.0.1	Unchanged
PingID SaaS Connector	1.1.1	Unchanged

Warning messages removed

Fixed PIM-4131 PingID Integration kit for PingFederate

We've fixed an issue that was generating warning messages unnecessarily when running PingFederate server.

PingID Integration Kit 2.21 (January 3, 2023)

New features and improvements in PingID Integration Kit 2.21 for PingFederate.

The PingID Integration Kit 2.21 for PingFederate is released with the following components:

PingID Integration Kit component	Version	Status
PingID Adapter	2.13.1	New
PingID RADIUS PCV	3.0.1	Unchanged
PingID SaaS Connector	1.1.1	Unchanged

Fixed error introduced during PingID adapter upgrade

Fixed PIM-3529 PingID Integration kit for PingFederate

We've fixed an issue that was causing an error when importing a configuration during a PingID adapter upgrade.To prevent this error, Offline Authentication Encryption is now set to OAEP by default. This resolves issues related to CVE-2022-40722.

> **Note**
>
> Admins that are upgrading from PingID Adapter version 2.12 or earlier to the latest version and do not want to use OAEP padding must configure the **Offline Authentication Encryption** in the UI to **None**.

PingID Integration Kit 2.20 (November 22, 2022)

New features and improvements in PingID Integration Kit 2.20 for PingFederate.

The PingID Integration Kit 2.20 for PingFederate is released with the following components:

PingID Integration Kit component	Version	Status
PingID Adapter	2.13	New
PingID RADIUS PCV	3.0.1	Unchanged
PingID SaaS Connector	1.1.1	Unchanged

OAEP Padding

Improved PingID Integration kit for PingFederate

It is now possible to specify that OAEP padding should be used in the encryption for offline authentication through the PingFederate UI. OAEP padding is enabled by default for new PingID Adapter instances.

> **Note**
>
> This feature is backward compatible, and when updating an existing PingID Adapter your configuration is saved. However, you will see an error message in the PingFederate UI until you define the OAEP padding configuration manually in the UI. For instructions on enabling this option through the PingFederate UI, see Configuring offline MFA (PingID Adapter).

Binary attribute support

New PingID Integration kit for PingFederate

PingID Adapter now supports the option to define various Active Directory attributes as binary attributes.

PingID Adapter offline authentication language support

New PingID Integration kit for PingFederate

PingID Adapter now supports the following additional languages for offline authentication:

- Czech
- Polish
- Hungarian

Dependent packages updates

Improved PingID Integration kit for PingFederate

As part of our ongoing maintenance improvements, we've updated all PingID Adapter-related dependent packages with known security vulnerabilities.

PingID Integration Kit 2.19 (November 3, 2022)

The PingID Integration Kit 2.19 for PingFederate is released with the following components:

PingID Integration Kit component	Version	Status
PingID Adapter	2.12	Unchanged
PingID RADIUS PCV	3.0.1	New
PingID SaaS Connector	1.1.1	Unchanged

Resolved issues

With the release of PingID RADIUS PCV 3.0.1, the following issues have been resolved.

Ticket ID	Description
PIM-3774	Fixed an issue that was preventing LDAP group attributes from being populated correctly.

PingID Integration Kit 2.18 (August 30, 2022)

The PingID Integration Kit 2.18 for PingFederate is released with the following components:

PingID Integration Kit component	Version	Status
PingID Adapter	2.12	Unchanged
PingID RADIUS PCV	3.0	Updated
PingID SaaS Connector	1.1.1	Unchanged

PingID RADIUS PCV 3.0

PingID RADIUS PCV 3.0 is released and includes the following enhancements:

- We've added support for MS-CHAP v2 RADIUS Server authentication protocol. For information, see Configuring RADIUS PCV for MS-CHAPv2.
- PingID RADIUS PCV can now receive user attributes from Active Directory, without using the AD as the first factor.
- We've made improvements to enhance performance and security.

Resolved issues

With the release of PingID RADIUS PCV 3.0, the following issues have been resolved.

Ticket ID	Description
PIM-3370	Fixed an issue that was preventing PingID RADIUS PCV from using the relevant timeout value configured in PingFederate when creating a connection with LDAP.

PingID Integration Kit 2.17 (April 27, 2022)

The PingID Integration Kit 2.17 for PingFederate is released with the following components:

PingID Integration Kit component	Version	Status
PingID Adapter	2.12	Updated
PingID RADIUS PCV	2.10	Unchanged
PingID SaaS Connector	1.1.1	Unchanged

PingID adapter (version 2.12)

Version 2.12 of the PingID adapter has been released, and this version makes it possible to specify that OAEP padding should be used in the encryption for offline authentication. For instructions on enabling this option, see Configuring offline MFA (PingID Adapter).

PingID Integration Kit 2.16 (March 23, 2022)

The PingID Integration Kit 2.16 for PingFederate is released with the following components:

PingID PingIDIntegration Kit component	Version	Status
PingID Adapter	2.11.1	Unchanged
PingID RADIUS PCV	2.10	Updated
PingID SaaS Connector	1.1.1	Unchanged

RADIUS PCV plugin (version 2.10)

Version 2.10 of the RADIUS PCV plugin has been released, and includes the following enhancements:

- In the attribute mapping rules, you can now define OGNL expressions to fine-tune attribute mapping.
- Under **Member of Groups**, it is now possible to specify an LDAP group attribute other than *memberOf*.
- User passwords can now contain commas.

For more information, see PingID RADIUS PCV parameters reference guide.

PingID Integration Kit 2.15 (November 10, 2021)

The PingID Integration Kit 2.15 for PingFederate is released with the following components:

PingID PingIDIntegration Kit component	Version	Status
PingID Adapter	2.11.1	Unchanged
PingID RADIUS PCV	2.9.1	Unchanged
PingID SaaS Connector	1.1.1	Updated

Enhancements

Updates to PingID SaaS Connector

The PingID SaaS Connector component has been updated to use newer versions of libraries that had vulnerabilities reported.

PingID Integration Kit 2.14 (October 18, 2021)

The PingID Integration Kit 2.14 for PingFederate is released with the following components:

PingID PingIDIntegration Kit component	Version	Status
PingID Adapter	2.11.1	Updated
PingID RADIUS PCV	2.9.1	Updated
PingID SaaS Connector	1.0.1	Unchanged

Enhancements

Updates to PingID Adapter and PingID RADIUS PCV

The PingID adapter and PingID Radius PCV components have been updated to use newer versions of libraries that had vulnerabilities reported.

PingID Integration Kit 2.13 (July 28, 2021)

The PingID Integration Kit 2.13 for PingFederate is released with the following components:

PingID Integration Kit component	Version	Status
PingID Adapter	2.11	Updated
PingID RADIUS PCV	2.9	Unchanged

PingID Integration Kit component	Version	Status
PingID SaaS Connector	1.0.1	Unchanged

Enhancements

Using risk level in PingID policies

With the introduction of PingID Adapter 2.11, it is now possible to include the risk level calculated by PingOne Protect (or a supported third-party risk service) when you define a PingID policy. MFA actions can be specified for each of the three risk levels - high, medium, and low. This feature requires a separate license for the integrated Risk service.

For more information, see Configuring a risk level rule (web policy).

PingID Integration Kit 2.12 (March 24, 2021)

The PingID Integration Kit 2.12 for PingFederate is released with the following components:

PingID Integration Kit component	Version	Status
PingID Adapter	2.10	Updated
PingID RADIUS PCV	2.9	Updated
PingID SaaS Connector	1.0.1	Unchanged

PingID adapter (version 2.10)

Version 2.10 of the PingID adapter has been released, and includes the following enhancements:

- It is now possible to use "chained attributes" when defining the LDAP data source for an IdP adapter. An example of where you can use this approach is to write OGNL expressions to define custom user groups that can be used in PingID policies (in addition to those groups defined in the directory). See Configuring a PingID Adapter instance.
- Restrictions have been added to limit the ability to add a new device during password reset.

RADIUS PCV plugin (version 2.9)

Version 2.9 of the RADIUS PCV plugin has been released, and includes the following enhancements:

- It is now possible to add vendor-specific attributes to the definition of a PingID RADIUS PCV so that they are sent during authentication. See PingID RADIUS PCV parameters reference guide.
- When defining multiple RADIUS clients for a PCV, it is now possible to add a label for each client. See Configuring a RADIUS server on PingFederate.
- In the definition of a PingID RADIUS PCV, you can now specify a label and icon to show on the PingID app's authentication screen instead of the default text and icon (options are part of the "advanced fields"). See PingID RADIUS PCV parameters reference guide.

PingID Integration Kit 2.11 (December 2, 2020) (updated)

The PingID Integration Kit 2.11 for PingFederate is released with the following components:

PingID Integration Kit component	Version	Status
PingID Adapter	2.9	Updated
PingID RADIUS PCV	2.7	Updated
PingID SaaS Connector	1.0.1	Unchanged

Resolved issues

With the release of PingID Integration Kit 2.11, the following issues have been resolved.

Ticket ID	Description
PID-8027	Fixed an issue that prevented users to perform offline authentication when `LDAP DATA SOURCE FOR DEVICES` is set but `LDAP DATA SOURCE` left empty.
PID-8115	Fixed an issue that some LDAP Data Store configurations were ignored by PingID Adapter when querying the Data Store.
PID-9852	Fixed an interoperability issue between PingID Adapter and PingID RADIUS PCV.
PID-6717	Fixed a Unicode Issue that prevented user names with Unicode characters (ex. ü) to authenticate
PID-10528	Fixed an issue when **objectGUID** was mapped to the `Username` field: Now the**objectGUID** is decoded the same way as Active Directory decodes it. **Important** The `Username` mapping feature was first introduced in PingID Adapter v2.8. If you already use **objectGUID** in the `Username` attribute mapping field, please contact Support before upgrading.

PingID Integration Kit 2.10 (August 25, 2020) (updated)

The PingID Integration Kit 2.10 for PingFederate is released with the following components:

PingID Integration Kit component	Version	Status
PingID Adapter	2.8	Updated
PingID RADIUS PCV	2.6	Unchanged

PingID Integration Kit component	Version	Status
PingID SaaS Connector	1.0.1	Unchanged

Enhancements

Support for Integration of PingID for Windows Login through PingFederate

PingID Adapter 2.8 now supports Integration of PingID for Windows Login through PingFederate.

For more information, see Integrating PingID with Windows login.

Mapping the LDAP attribute to the PingID User attribute

We've added a new PingID User attribute. The attribute value is the LDAP name attribute that defines the user name used by PingID.

For more information, see Configuring a PingID Adapter instance (Windows login).

Known issues and limitations

PingID Adapter incorrectly parsing `objectGUID` attribute values from LDAP (29 October, 2020)

When using LDAP to retrieve user information, if the PingID Adapter is configured to use the LDAP `objectGUID` attribute, the value of this attribute is incorrectly transformed and stored.

This issue will be fixed in a future version. It is recommended not to use the `objectGUID` attribute until the issue is fixed.

PingID Integration Kit 2.9 (June 24, 2020)

The PingID Integration Kit 2.9 for PingFederate is released with the following components:

PingID Integration Kit component	Version	Status
PingID Adapter	2.7	Unchanged
PingID RADIUS PCV	2.6	Updated
PingID SaaS Connector	1.0.1	Unchanged

Enhancements

PingID RADIUS PCV (with integrated RADIUS server) now logs events to the PingFederate audit log

- PingID RADIUS PCV Audit logging is not supported for PingFederate releases prior to release 10
- Configuration provisions for users of PingFederate versions 10.0.0 and 10.0.1 are set out in the PingID Administration Guide here: Installing the PingID Integration Kit for VPN

- For PingFederate releases 10.0.2 and later, Audit logging is configured in the PingFederate admin portal. See Administrator audit logging and Security audit logging.

PingID Integration Kit 2.8 (April 30, 2020)

The PingID Integration Kit 2.8 for PingFederate is released with the following components:

PingID Integration Kit component	Version	Status
PingID Adapter	2.7	New
PingID PCV	2.5	Unchanged
PingID SaaS Connector	1.0.1	Unchanged

Enhancements

PingID attributes for use with PingFederate policy

Admins can now use PingID authentication attributes from the PingID adapter when creating PingFederate policies. This enables admins to create more accurate policies, based on information obtained by PingID, for a higher level of security.

- For a list of attributes that can be used by PingFederate policy upon successful authentication with PingID, see PingID authentication attributes.
- For instructions on how to create the relevant PingFederate policy, see Integrate with PingID for PingFederate SSO.

Retain PingID cookie after SLO

It is now possible to choose to retain the PingID cookie when a user performs SLO (single logout) from PingFederate. WARNING: This option prevents a full clean up of the user trace on the machine after SLO (single logout) and may expose your user accounts to additional security risks. This option should only be used with full understanding of the security implications.

PingID Integration Kit 2.7 (September 24, 2019)

The PingID Integration Kit 2.7 for PingFederate is released with the following components:

PingID Integration Kit component	Version	Status
PingID Adapter	2.6	New
PingID PCV	2.5	Unchanged
PingID SaaS Connector	1.0.1	Unchanged

Enhancements

PingID Adapter v2.6

- FIDO passwordless authentication infrastructure

  PingID Adapter v2.6 includes important updates and changes required to support the forthcoming release of FIDO passwordless authentication.

- PingID Adapter support for multiple branded URLs in PingFederate

  PingID Adapter now supports the use of multiple branded URLs for use in PingFederate. This feature requires PingFederate v9.2 and higher, and does not require any specific configuration in the PingID Adapter.

  To use this feature in conjunction with SLO (Single Log Out), requires PingFederate v9.2.3 or higher.

  For further details, refer to the documentation Supporting multiple access mode.

Resolved issues

Ticket ID	Description
PID-8286	Fixed an issue that was requesting that values be manually entered for the**LDAP Search Scope** and **Cookie Duration** fields when upgrading from a much older version of PingID Adapter. These fields are automatically populated with default values during the upgrade process.
PID-7348	Fixed an issue when running the heartbeat validation that was causing an error in some cases if using a proxy with PingID Adapter.

PingID Integration Kit 2.6 (January 8, 2019)

The PingID Integration Kit 2.6 for PingFederate is released with the following components:

PingID Integration Kit component	Version	Status
PingID Adapter	2.5	New
PingID PCV	2.5	New
PingID SaaS Connector	1.0.1	Unchanged

Enhancements

Multiple access mode (PingID Adapter 2.5)

In addition to the traditional organization-owned single-user device, (for example, an employee's laptop or desktop computer), the PingID Adapter has been extended to support the following use cases:

- An organization-owned multiple-users device, for example, a kiosk or shared tablet.
- A device not owned by the organization, that is used by single or multiple users.
- Configuration for prevention of storage of user information and long-lived sessions on certain devices (typically devices used by multiple users). This will require users to sign-on and re-authenticate on each subsequent login.
- Provide users with the ability to indicate that the browser used for access is running on a public device, or on a device not regularly used for secure access. This assures users that they can securely login without concern about user information being kept on that device.

> **Note**
>
> The multiple access mode requires PingFederate 9.2 and PingID Integration Kit 2.6 (packaged as part of the PingFederate 9.2 bundle).

For further details, refer to the documentation Supporting multiple access mode.

PingID PCV 2.5 unicode encryption support

The encryption method of the Radius State attribute has been enhanced to support non-standard VPN clients that will only accept unicode encoding.

PingID Integration Kit 2.5 (October 31, 2018)

Enhancements

Adapter 2.4

- Single logout (SLO)
  - PingID MFA is now synchronized with the PingFederate single logout for all protected resources. From Adapter version 2.4, single logout terminates both PingFederate and PingID MFA sessions, and requires both 1st factor and MFA for a user's next login.
- Turkish language support:
  - From v2.4, the PingID Adapter has been extended to support Turkish.

PCV 2.4

Multiple Attributes Mapping Rules have been extended to map the LDAP email address, first name and last name source attributes to PingID. See PingID RADIUS PCV parameters reference guide for details.

PingID Integration Kit 2.4 (October 4, 2018)

Enhancements

A new version of the PingID Integration Kit was released providing PingID offline MFA for mobile only users. This feature enables users to authenticate manually from their mobile devices in order to access resources on the same device. The new version includes:

- PingID Adapter v2.3.0
- PingID RADIUS PCV v2.3.1 (No change)
- PingID SaaS Connector - v1.0.1 (No change)

See Authenticating manually, in the PingID User Guide. NOTE: The ability to authenticate manually from a mobile device in order to access resources on the same device requires PingID mobile app v1.8.4 or higher.

Known issues and limitations

- **PingID screens display incorrectly when using Android's native browser for Manual Authentication**

  There's a known issue for users of devices running Android v5.0 OS when using the Android's native browser to perform Manual Authentication from a mobile device in order to access resources on the same device, that causes some of the PingID screens not to display correctly. Other browsers, such as Chrome or Firefox do display PingID screens correctly.

- **Manual Authentication flow stops without displaying an error message**

  When using Manual Authentication flow to access resources on a mobile device that does not have PingID mobile app installed, if the user selects **Authenticate**:

  - On iOS devices: Chrome attempts to search for PingID, and the Manual Authentication flow is stopped.
  - On Android devices: the Manual Authentication flow is stopped, and the user does not receive an error message, due to limitations in the native Android OS.

PingID Integration Kit 2.3.1 (July 5, 2018)

A new version of the PingID Integration Kit was released and includes:

- PingID RADIUS PCV v2.3.1
- PingID Adapter v2.2
- PingID Connector 1.0.1

Enhancements

PingID RADIUS PCV v2.3.1

The following enhancements were made to PingID RADIUS PCV:

- You can define a separate list of LDAP group names that you want to exclude from PingID authentication. If a user is a member of the bypass group, the user will not be required to authenticate via PingID regardless any group membership or policies applied.
- It is now possible to configure a newline between different device entries within a RADIUS server challenge message.

Resolved issues

Ticket ID	Description
PID-6471/PID-6529	Fixed issues that occurred when using the PingID memberOf group configuration when the RADIUS PCV VPN is in 'no challenge' mode.
PID-6477	There were cases where if the RADIUS PCV was in "no challenge" mode and OTP in password separator was configured as 'comma', that first factor authentication failed. This bug is fixed in RADIUS PCV v2.3.1.
PID-6387	An edge case was discovered where it was possible for a user to register an SMS, voice or email-based authentication device which does not meet company policy, even though the **RESTRICT** configuration option was selected. This issue is now resolved.

PingID Integration Kit 2.2 (May 17, 2018)

A new version of the PingID Integration Kit was released and includes:

- PingID RADIUS PCV v2.2
- PingID Adapter v2.2

Resolved issues

Ticket ID	Description
PID-6354	In PingID RADIUS PCV v2.0 and v2.1, in rare cases, when more than one user connected to the company VPN in parallel, the RADIUS server had a parsing error of the LDAP server attribute mapping response. As a result, some users could be granted with the wrong privileges, affecting their session and causing them to bypass MFA. This issue is resolved in RADIUS PCV v2.2.
ADPT-7819	To improve PingID adapter performance, referral chasing has been disabled for LDAP queries in PingID Adapter V2.2 and higher.

PingID Integration Kit 1.4 (May 18, 2017)

PingID Integration Kit 1.4

PingID Integration Kit 1.4 is released with the following new features:

PingID Adapter 1.4

- Built-in, user friendly, migration path from a variety of third party MFA systems to PingID.
- Support for successful SSO during PingID service issues.
- Added the ability to configure the adapter's LDAP search scope.
- Adapter version sent to the PingID service, as part of the authentication request.
- Automatic support for the Europe and Australia regions' data centers.

PingID RADIUS PCV V1.4

- Added OTP collection mode in the password field. This capability is useful for VPN models / remote access systems / services which support the RADIUS protocol, but do not support RADIUS Access-Challenge. This mode also supports RADIUS clients, which send the user collected OTP to the RADIUS server using the password field, for example Amazon Workspaces.
- Username attribute mapping: The RADIUS PCV can now map between usernames sent by a RADIUS client and another set of usernames, retrieved from an LDAP attribute, and are used by PingID as usernames. This aligns the organization to a single set of PingID usernames. For example, if the RADIUS client is sending a sAMAccountName as the username, the RADIUS PCV can substitute it with the matching UserPrincipalName retrieved from the local Active Directory before sending the authentication request to the PingID service.

Resolved issues

Ticket ID	Description
ADPT-6840	A case was discovered where the adapter returned an error when querying LDAP attributes, and did not populate the LDAP fields. This is now resolved by the ability to configure the adapter's LDAP search scope.

PingID Integration Kit 1.3 (January 27, 2016)

The PingID Integration Kit 1.3 for PingFederate is released.

The new version includes:

- Added support for the group, phone, and email LDAP attributes to the PingID adapter.
- Added new adapter configuration fields for Cookie Duration, Refresh UserID Cookie, and Application Name.

See Installing the PingID Integration Kit for PingFederate for instructions.

PingID Integration Kit 1.2 (June 29, 2015)

The PingID Integration Kit 1.2 for PingFederate is released.

The new version includes:

- Updated cookie encryption to use JSON Web Encryption (JWE).
- UTF-8 character support for first and last name.

See Installing the PingID Integration Kit for PingFederate for instructions.

Introduction to PingID

PingID is a cloud-based authentication service that binds user identities to mobile devices.

During the PingID authentication process, the PingID service sends an authentication request to the user's mobile device. No password response is required: the user just swipes to authenticate.

You can use PingID for any of these solutions:

PingOne SSO

Use PingID as a secondary authentication solution for PingOne single sign-on (SSO) in the cloud. A PingOne administrator can enable PingID in minutes.

PingFederate SSO

Use PingID as either a secondary or primary authentication solution for federated SSO through PingFederate. A PingFederate administrator can install and configure a PingID adapter that negotiates with the PingID service.

VPNs

Use PingFederate and PingID for multi-factor authentication (MFA) from your VPN. This solution uses PingFederate with a password credential validator (PCV) for PingID for identity access management, and PingOne for user management. You need only a few additional settings to enable PingID authentication for your VPN.

Passwordless authentication

- Use PingID with biometrics or a security key to provide passwordless authentication for Web authentication through PingFederate.
- Use PingID mobile application to provide passwordless authentication for Windows login.

You can configure your SSO infrastructure for PingID authentication to:

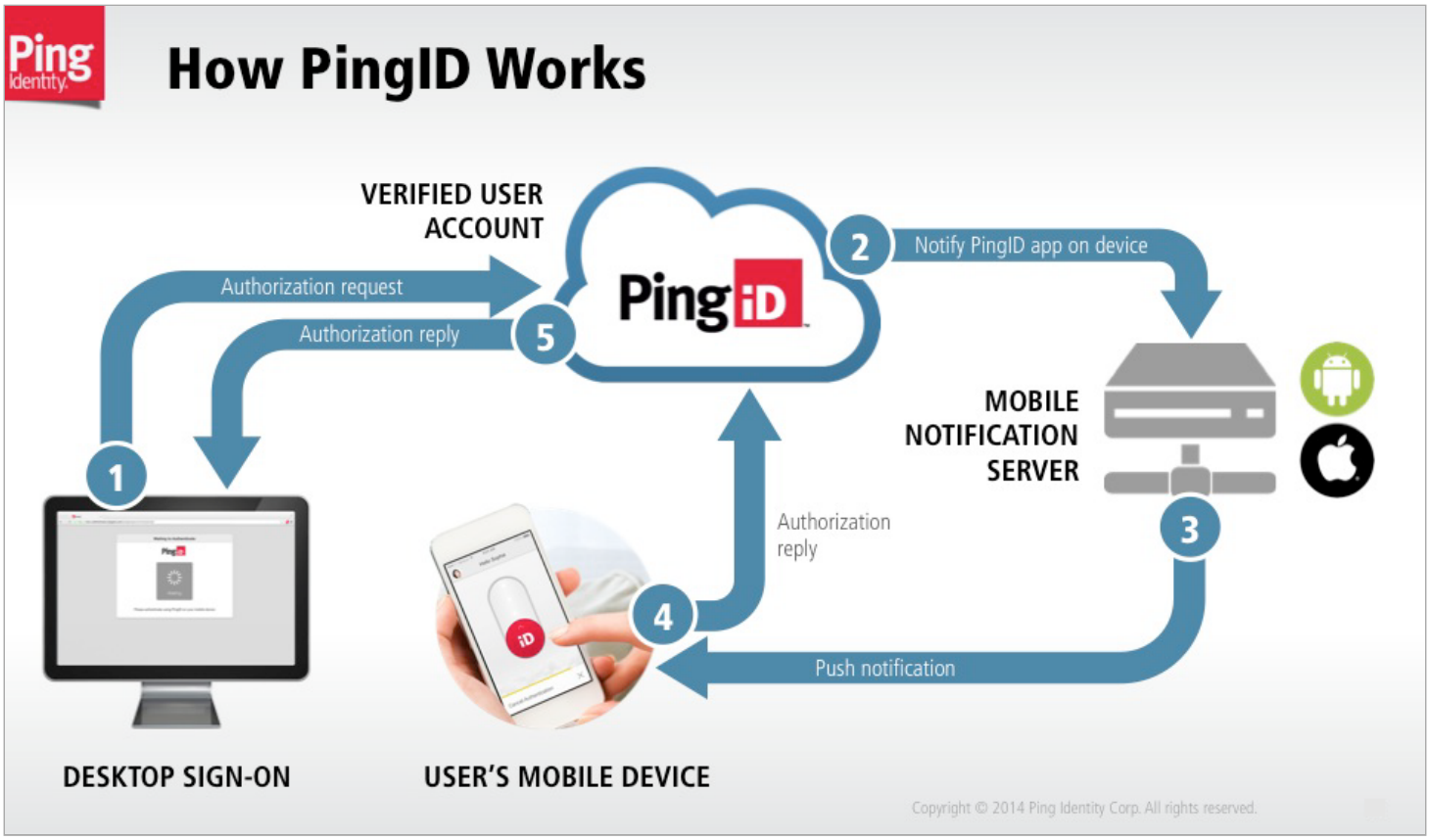
- Use primary authentication only for SSO to PingOne, and then use PingID as secondary authentication whenever a user attempts to access certain applications.
- Use PingID when a user is outside of your organization's intranet.
- Use PingID only for customers that use SSO to connect to your Managed Service Provider (MSP) account on PingOne.
- Use the PingID API and PingID client integration settings to integrate PingID with your VPN or remote access system and authenticate remote SSO.

PingID is a service that runs on the PingOne platform, a mobile app for Apple® iOS or Google Android™ devices, and an adapter and PCV for PingFederate. These components work together to provide a secure means of authentication for members of your organization, partners, or customers.

If you have a PingOne SSO account, PingID is ready for you to use. To use the PingID service solely for PingFederate federated SSO, SSO through your VPN, or for custom client integrations, you need to register for the PingID Enterprise service with PingOne. You configure and manage the PingID service using the PingOne admin portal.

Try PingID for free and see the value it can bring to your organization. For more information, see Starting a PingOne trial.

> **Note**
>
> Consider the security guidelines outlined in the PingID Hardening Guide when configuring your implementation of PingID. For more information, see PingID Security Hardening Guide.



Your PingID setup depends on your SSO infrastructure. For more information, see:

- SSO with PingID and PingOne
- Federated SSO with PingID and PingFederate
- PingID authentication for PingOne using PingFederate as the identity bridge
- PingID authentication for VPNs

Overview of PingID authentication types

After defining user groups and end user accounts in your organization, determine which authentication method they will use.

PingID supports several types of authentication for users:

- PingID Mobile App. This includes the fingerprint biometrics, facial recognition, swipe, mobile soft token, and Apple Watch authentication methods.
- FIDO2 biometrics
- Security key

- Desktop Soft Token
- Authentication app
- OATH token
- YubiKey™- Yubico OTP
- Email OTP
- SMS and Voice

As an administrator, you determine which authentication methods the users in your organization use. For example, you can use a lenient method such as SMS and move to stricter methods at a later stage, such as biometrics authentication.

> **Note**
>
> The only authentication method enabled by default is the swipe method. You must manually enable any other authentication method. For more information, see Configuring authentication for the PingID mobile app.

PingID Mobile App

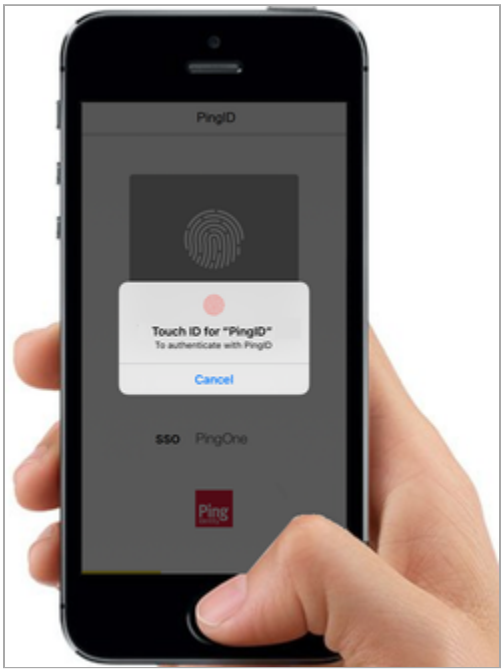
Biometrics: Fingerprint

The fingerprint authentication uses a device's native capability to scan and authenticate the user's fingerprint.

Fingerprint authentication is supported on devices that support biometrics and is included in the PingID mobile app Supported operating systems.

You can set the fingerprint authentication rollout mode with the following settings:

- Disable fingerprint authentication.
- Enable for iOS, Android, or both, in one of the following modes:
  - **Enable**: If the user has a supporting device and has enabled the fingerprint scan option, they are authenticated by fingerprint.
  - **Require**: Users with supporting devices are required to set up their fingerprint scan option and authenticate with it.
  - **Enforce**: Fingerprint scanning by the PingID app is required on every authentication, even if the user unlocked the device using their fingerprint.



For more information, see Configuring biometrics authentication for the PingID mobile app.

Biometrics: Facial Recognition

PingID supports facial recognition. Authentication by facial recognition is model dependent for Apple and Android devices.

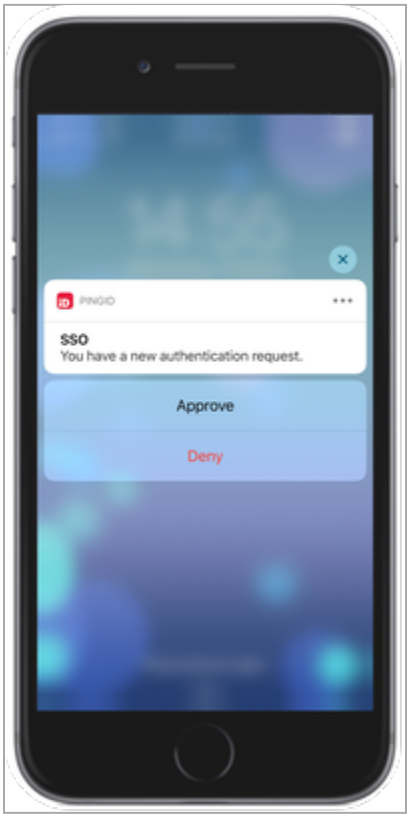
Both facial recognition and fingerprint authentication results are transparently passed through to the PingID app. For configuration information, see Configuring biometrics authentication for the PingID mobile app.

- **Apple**: Apple uses Face ID for some iPhone and iPad devices. These devices are configured for Face ID or Touch ID, but not both. Devices that support Face ID include:
  - iPhone: iPhone XS Max, iPhone XS, iPhone XR, iPhone X
  - iPad: iPad Pro 12.9" (third generation), iPad Pro 11"

  For the most recent information from Apple, see iPhone and iPad models that support Face ID.
- **Android Platforms**: Facial data is acquired using the device's camera. If the user attempts to authenticate with an unlocked screen, only fingerprint authentication is available. On a locked screen, fingerprint authentication and facial recognition are both available on supported devices.

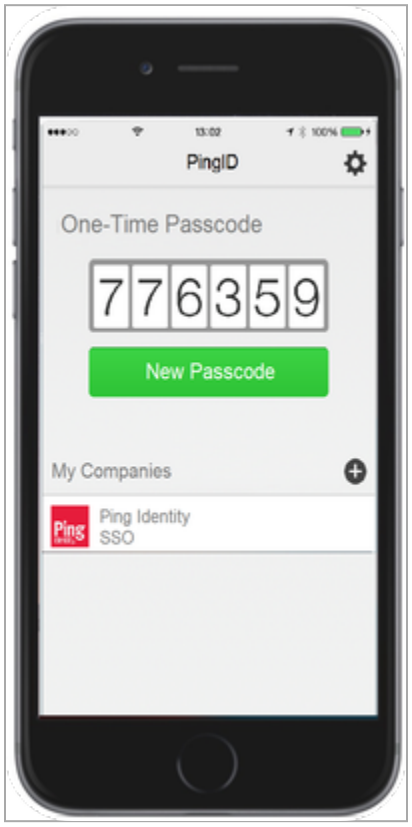
Swipe/Lock Screen Buttons

An authentication request is sent to the PingID mobile application via a push message on the end user's device. Then the user can respond to the authentication request directly on the lock screen, or launch the application and manually swipe the PingID button to approve the authentication request.



Mobile Soft Token

A user can generate a one-time passcode (OTP) with the PingID app for iOS or Android. This OTP can be used for authentication in cases where the user's mobile is offline, such as when there is no network connection, or in any other use case set by the administrator as an organization's policy.



Apple Watch

If a user has an Apple Watch connected to their iPhone, the PingID app automatically presents the **Approve** or **Deny** authentication actions on the Apple Watch, so the user can authenticate without needing to access their device.

FIDO2 biometrics

The user can take advantage of FIDO2 strong cryptographic authentication, using built-in FIDO2 platform biometrics on their device.

Biometrics are supported for the following devices:

- Windows Hello
- Apple Mac (Touch ID)

- iOS biometrics
- Android biometrics

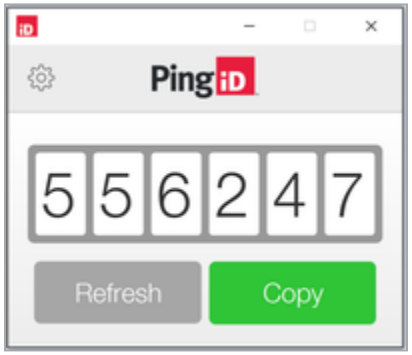
For more information, see (Legacy) Configuring FIDO2 biometrics for PingID.

Security key

The user can authenticate with any FIDO2 compliant security key or wearable device. The security key allows relying parties to offer a strong cryptographic authentication option for end user security. For more information, see (Legacy) Configuring the FIDO2 security key for PingID.

Desktop Soft Token

If the organization has approved the use of the PingID desktop app, users can generate an OTP from the local installation of the desktop app on their Windows or Mac computer. For more information, see PingID desktop app authentication.



Authentication app

If the organization has approved the use of external Time-based One-time Password (TOTP) authenticator apps, such as Google authenticator, a user can generate an OTP from the authenticator app on their device. For more information, see Configuring authenticator app authentication for PingID.

OATH token

An OATH token is a secure OTP that can be used for two factor authentication and is OATH compliant. For more information, see https://openauthentication.org/.

Use hardware OATH tokens where there are no provisions for connection to the Internet, USB connections, or mobile phones. Such connections might be disallowed for security reasons. For more information, see Configuring OATH token authentication for PingID.

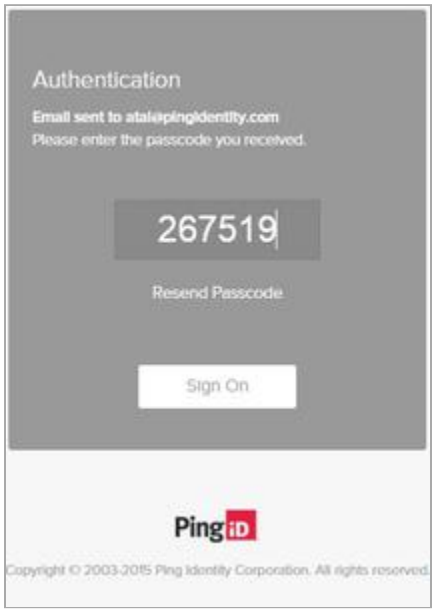
YubiKey™- Yubico OTP

The user must click a YubiKey with Yubico OTP capabilities to authenticate. Select this method of authentication if you've distributed YubiKey hardware tokens to users who are not authenticating using a mobile device.

YubiKeys that are FIDO2 compliant can be used as either a YubiKey or a Security key. For more information, see Configuring YubiKey authentication (Yubico OTP) for PingID.

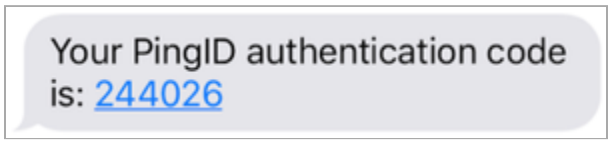
Email OTP

If you have users who aren't using devices that support the PingID mobile application, you can choose to enable this method of authentication. The user is authenticated by providing a 6-digit OTP sent by email to their email address. For more information, see Configuring email authentication for PingID.



SMS and Voice

If you have users who aren't using devices that support the PingID mobile application, you can enable this authentication method of authentication. The user is authenticated by providing a 6-digit OTP sent to the user's mobile device or landline phone, using SMS or voice channels.



For more information, including SMS and Voice usage limits, see SMS and voice authentication.

PingID regional data centers

When you create your organization in PingOne, choose the PingID regional data center location for your organization.

The PingID service is currently installed at the following regional data centers:

- North America (East and West Coasts)
- Europe
- Australia

All PingID service installations are hosted in the Amazon cloud.

Although each data center can service PingID users from any location, the location of your data center is important. It provides additional benefits, including:

- Better compliance with European, Australian, and New Zealand regulations and companies' standards.
- Users' personally identifiable information (PII) is stored in the specified regional hosting facility only.

- Optimized network speed for regional users.

For more information on registering a PingOne account and defining the data center location for your organization, see Creating an organization.

Limitations

- After you create and register your organization in PingOne, it is not possible to migrate from one data center to another.
- A user must have the PingID mobile app v1.9 or later installed to pair the PingID mobile app to two or more organizations that are not using the same data center.

SSO with PingID and PingOne

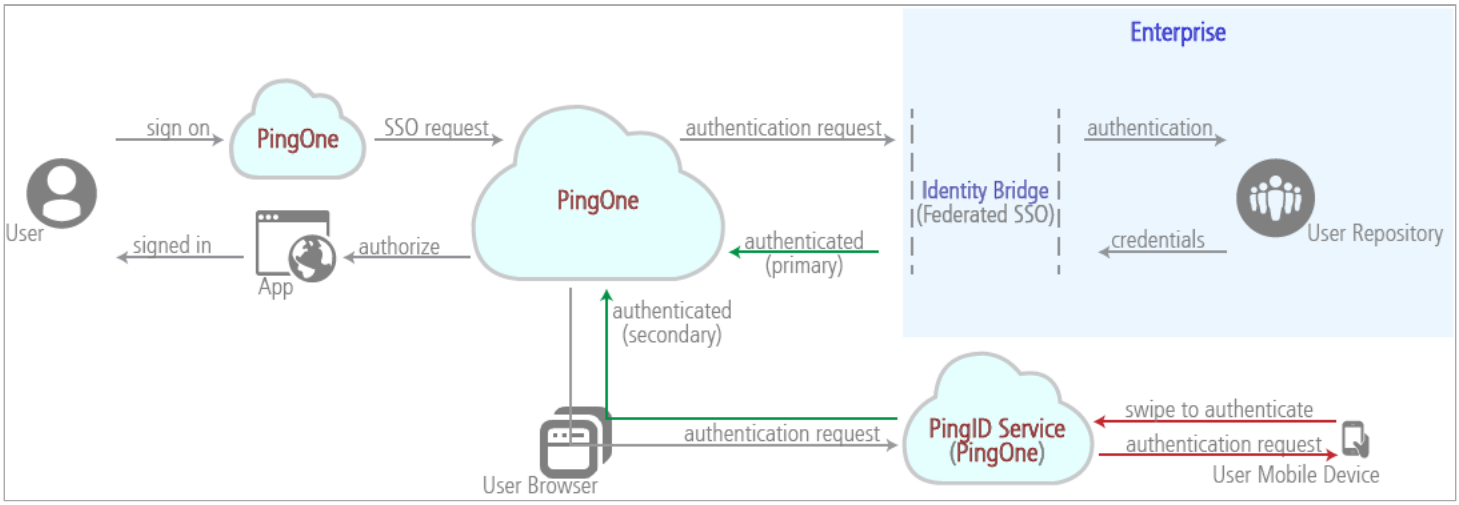
If you're using PingOne for single sign-on (SSO), adding PingID as your secondary authentication solution is a simple process of creating an authentication policy and assigning PingID as the authenticating entity.

For more information about creating an authentication policy, see Creating or updating an authentication policy.

For more information about configuring PingID, see Integrate with PingID for PingOne SSO.

Federated SSO

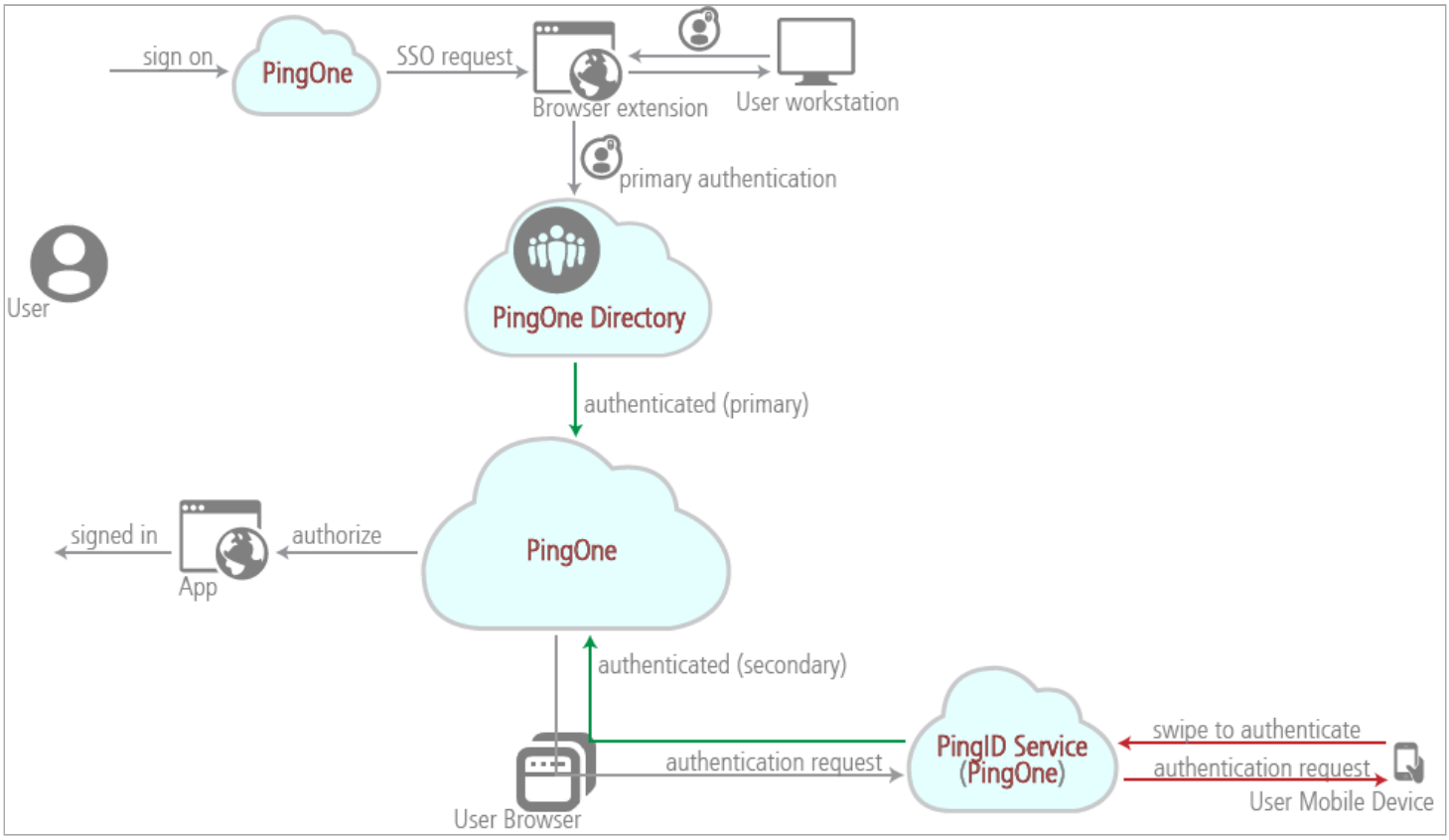
For federated SSO, the following diagram shows your users' standard SSO process with PingID.



For more information, see Federated SSO with PingOne.

Basic SSO

For basic SSO, the following diagram shows your users' standard sign-on process with PingID as a second authentication solution.

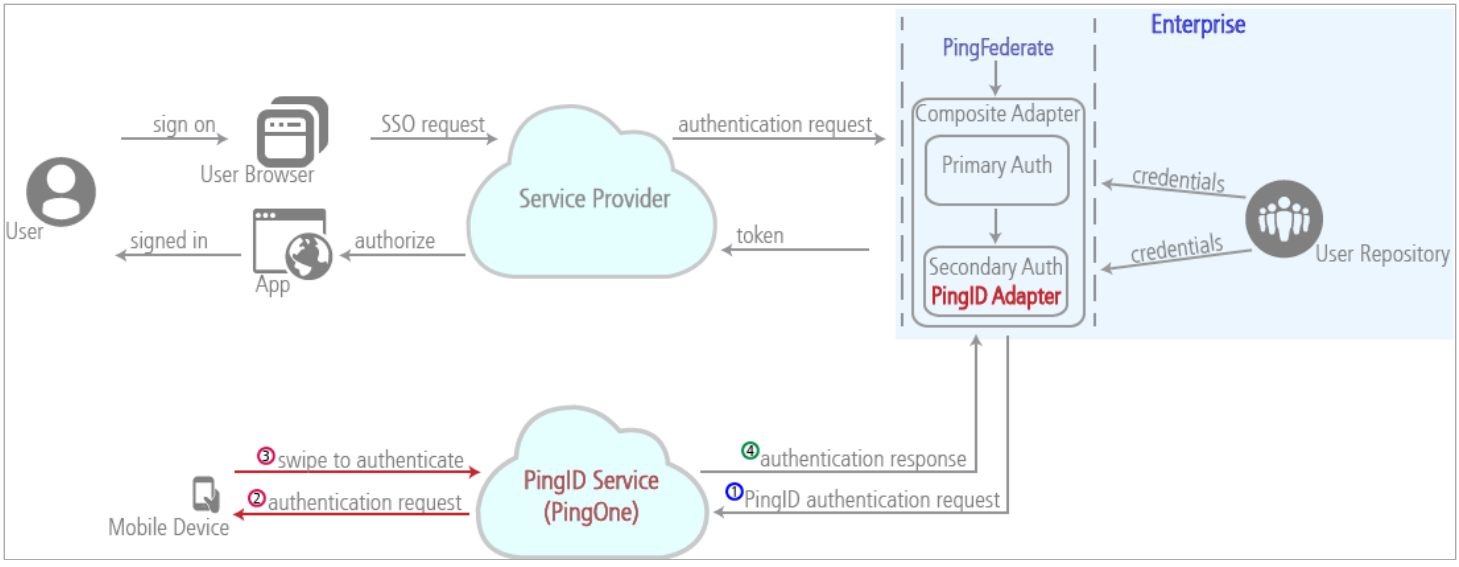


For more information, see Basic SSO (password vaulting).

Federated SSO with PingID and PingFederate

If you're using PingFederate for single sign-on (SSO) within your organization, you can add PingID as your secondary or primary authentication solution by installing the PingID Integration Kit and adding the PingID adapter to your PingFederate configuration.

The following diagram shows your enterprise users' standard SSO process using the PingID adapter.



For more information on installing and configuring PingID, see Integrate with PingID for PingFederate SSO.

PingID authentication for PingOne using PingFederate as the identity bridge

When you're using PingFederate as your PingOne identity bridge, you can use PingID for authentication on either the PingOne side or the PingFederate side.

Using PingID on the PingFederate side is useful when:

- You want to apply advanced PingFederate policy settings (for example, a custom adapter selector) to your PingID authentication.
- You want to use PingID for primary authentication.

For more information on configuring PingID for PingFederate, see Integrate with PingID for PingFederate SSO.

For more information on configuring PingID for PingOne, see Integrate with PingID for PingOne SSO.

PingID authentication for VPNs

You can use PingFederate and PingID for multi-factor authentication (MFA) from your VPN.

Configure your VPN for PingID and use PingFederate for identity access management for your users. You'll use PingOne for user management. For more information and instructions, see Integration for devices using a RADIUS server.

PingID supports the following VPNs:

- Cisco® Adaptive Security Appliance (ASA)
- Checkpoint® VPN
- Juniper® SA Series SSL VPN Appliances
- Palo Alto GlobalProtect®

You can integrate your VPN for PingID using RADIUS or SAML, these are standard protocols and any VPN that supports them, can be integrated. For more information, see Integration for devices using a RADIUS server.

PingID Service Management

PingID runs as a service on the PingOne platform, whether it is used for PingOne or PingFederate single sign-on (SSO).

If you have a PingOne SSO account, PingID is ready to use. To use the PingID service solely for PingFederate federated SSO, SSO through your VPN, or custom client integrations, you must register for the PingID Enterprise service with PingOne. You configure and manage the PingID service using the PingOne admin portal.

Use the PingID service management features to:

- Manage user access to the PingID service, such as disabling, temporarily bypassing, or removing users.
- Unpair a lost or damaged mobile device from the PingID service.
- Monitor user activity.
- Manage PingID service availability.
- Enable client integration.

The client integration settings are necessary only when:

- Your organization is using PingID for PingFederate SSO, or PingFederate is your PingOne identity bridge.

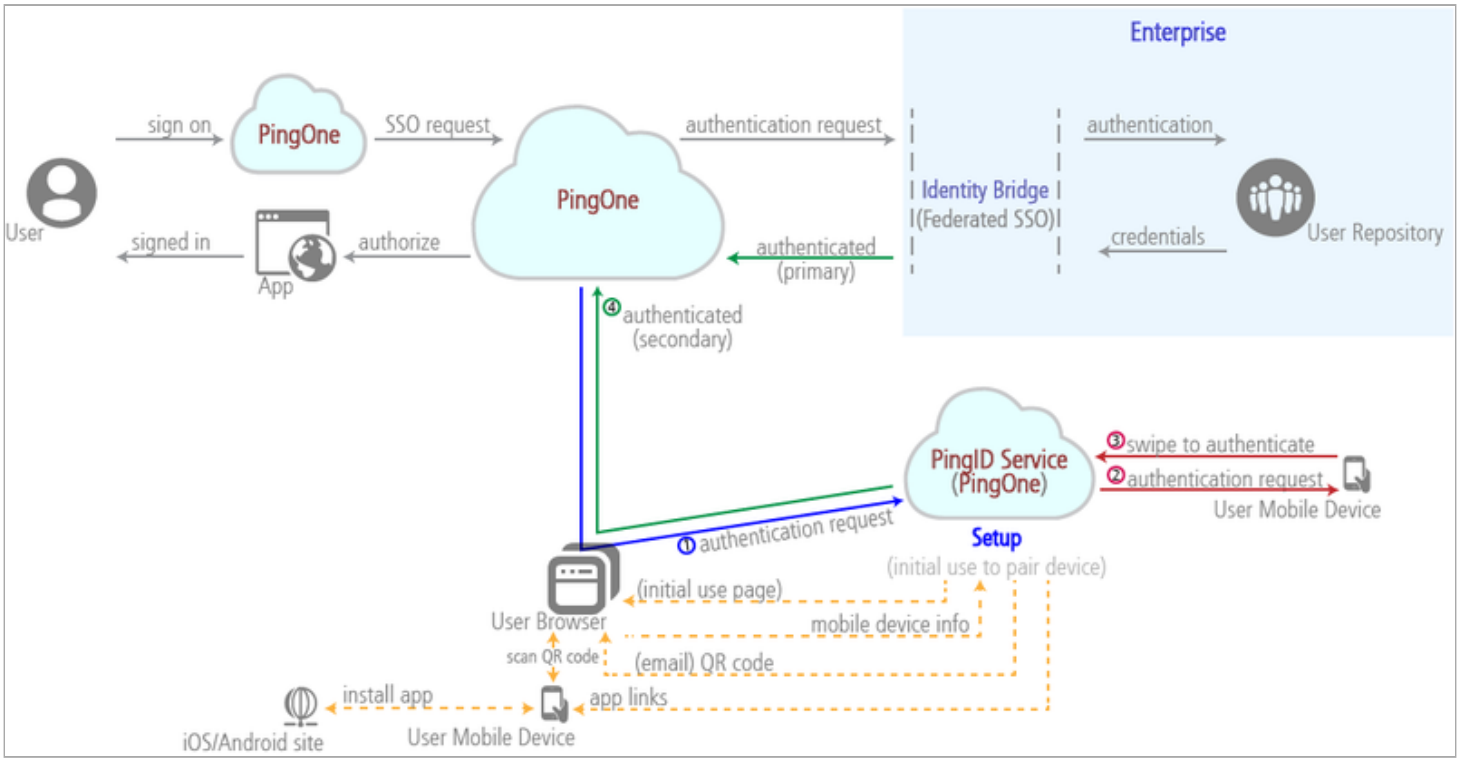
> **Note**
>
> In either of these cases, download a PingID settings file for use by your PingFederate administrator.

- You will be creating your own custom integration using the PingID API.

> **Note**
>
> In this case, activate PingID authentication for third-party clients and applications.

The settings file for download supports both types of integrations.

How It Works



> **Note**
>
> For basic SSO applications, an identity bridge isn't used and user credentials are sent to the PingOne directory. For more information, see Basic SSO (password vaulting) and Federated SSO with PingOne.

The PingID dashboard

The PingID dashboard enables you to analyze the use of multi-factor authentication (MFA) in your organization. It improves security by providing insights into usage and entry statistics, and it can pickup potential risks, anomalies, user trends, and roll-out progress.

{{{ Video removed }}}

To view the PingID dashboard, open the Admin portal and navigate to **DASHBOARD → PingID**.

Click any of the dashboard charts for a more detailed display with filters.

A couple of points to take into account when viewing the data displayed in the charts:

- Data refresh rate is subject to a 15-minute delay.
- Data displayed on the **SMS/Voice** chart is based on SMS and voice calls sent by the Twilio service. Data is aggregated based on Twilio report logs and represented with an approximation of the cost. So there may be some differences between chart data and the final billing amount.

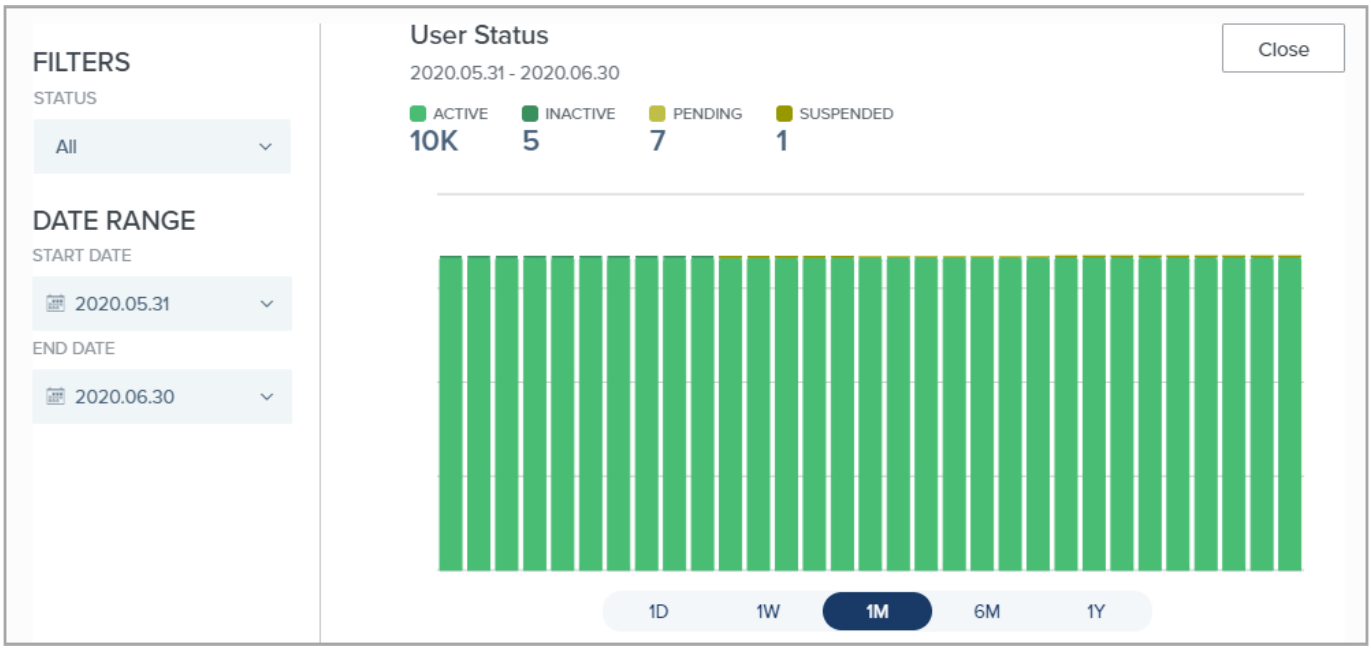
The following sections provide details about each of the chart types.

User status and devices

User status and devices

The **User Status** chart displays user status information for the specified time period. The **Users Devices** chart can display either the distribution of the paired devices in the organization by authentication method, or the distribution of the versions of the PingID mobile app that users have installed.

User Status



The user status chart includes four statuses:

Active

The user's PingID account is created, and the user has completed registration and paired the account with a device. The user can perform any of the permitted PingID functions.

Inactive

The administrator created the user's PingID account but either the account is not yet activated, or an activation message and code was sent but the activation code has expired.

Pending

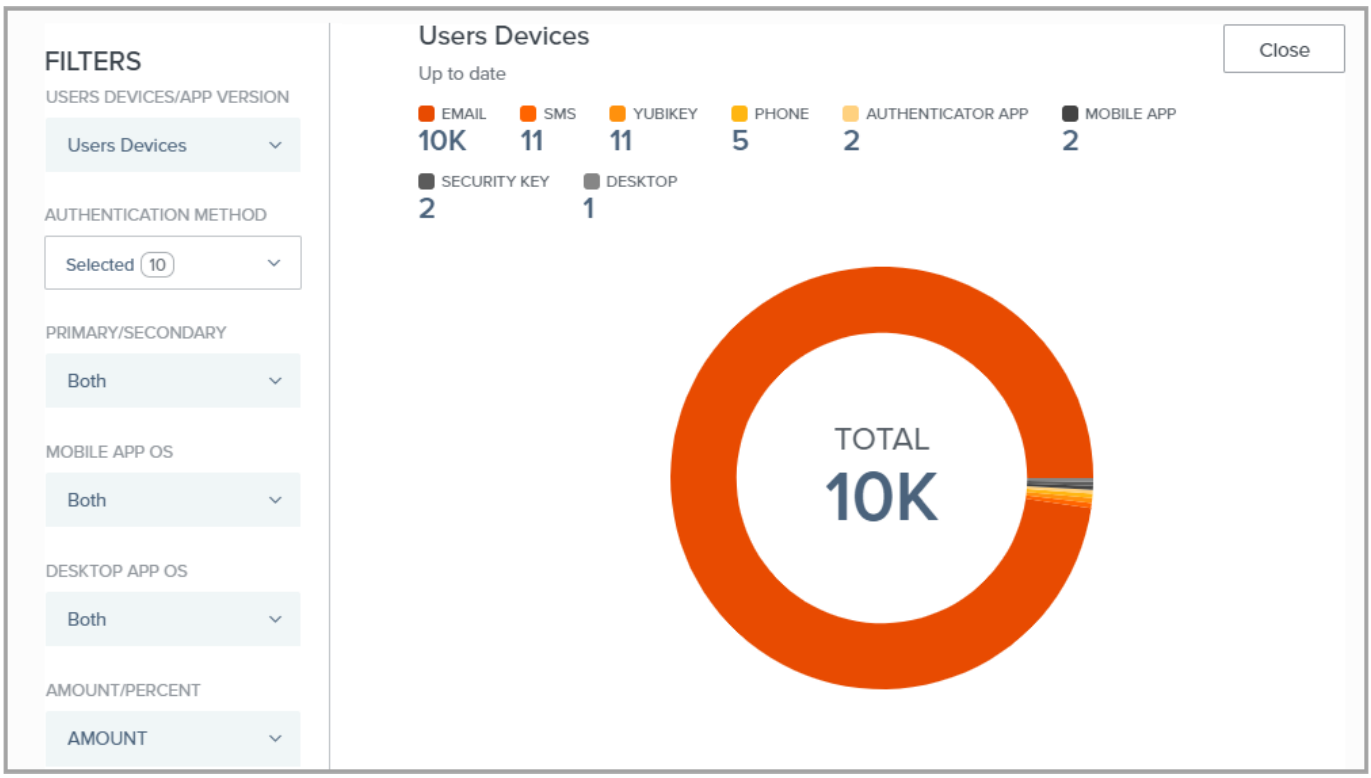
The user account was activated, but no device was paired for the user. This is a combination of **Pending Activation** and **Pending Change Device** in PingID User Detailed Status Report fields.

Suspended

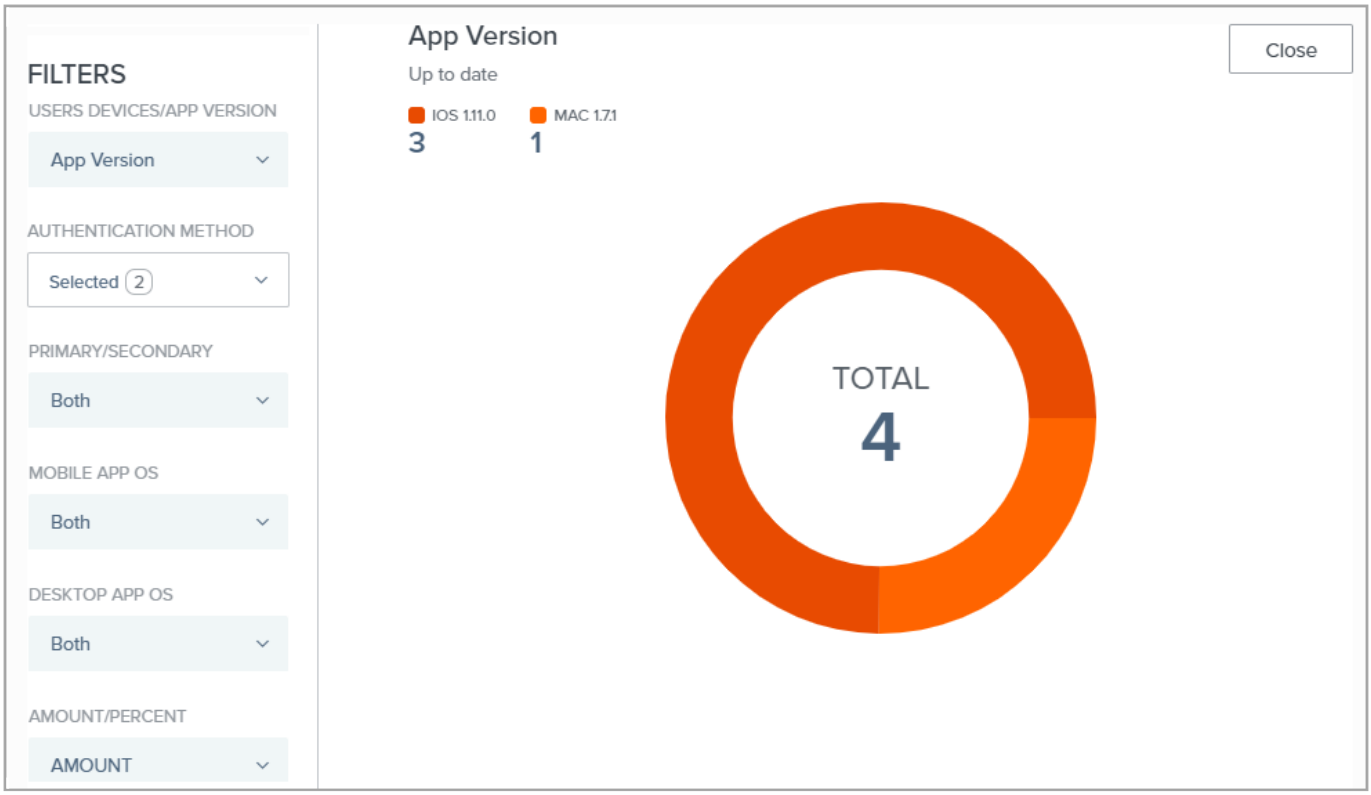
The administrator suspended this user's ability to be authenticated by PingID. This may occur, for example, for security reasons if a user can't find the registered device.

User Devices

Users' devices chart showing the distribution of the total paired devices in the organization by authentication method:



Users' devices chart showing the distribution of versions of the PingID mobile app that users have installed:



> **Note**
>
> For the different categories, the string displayed combines the name of the operating system with the version of the PingID mobile app installed, for example, *iOS 1.11.0* (operating system iOS with version 1.11.0 of the mobile app installed).

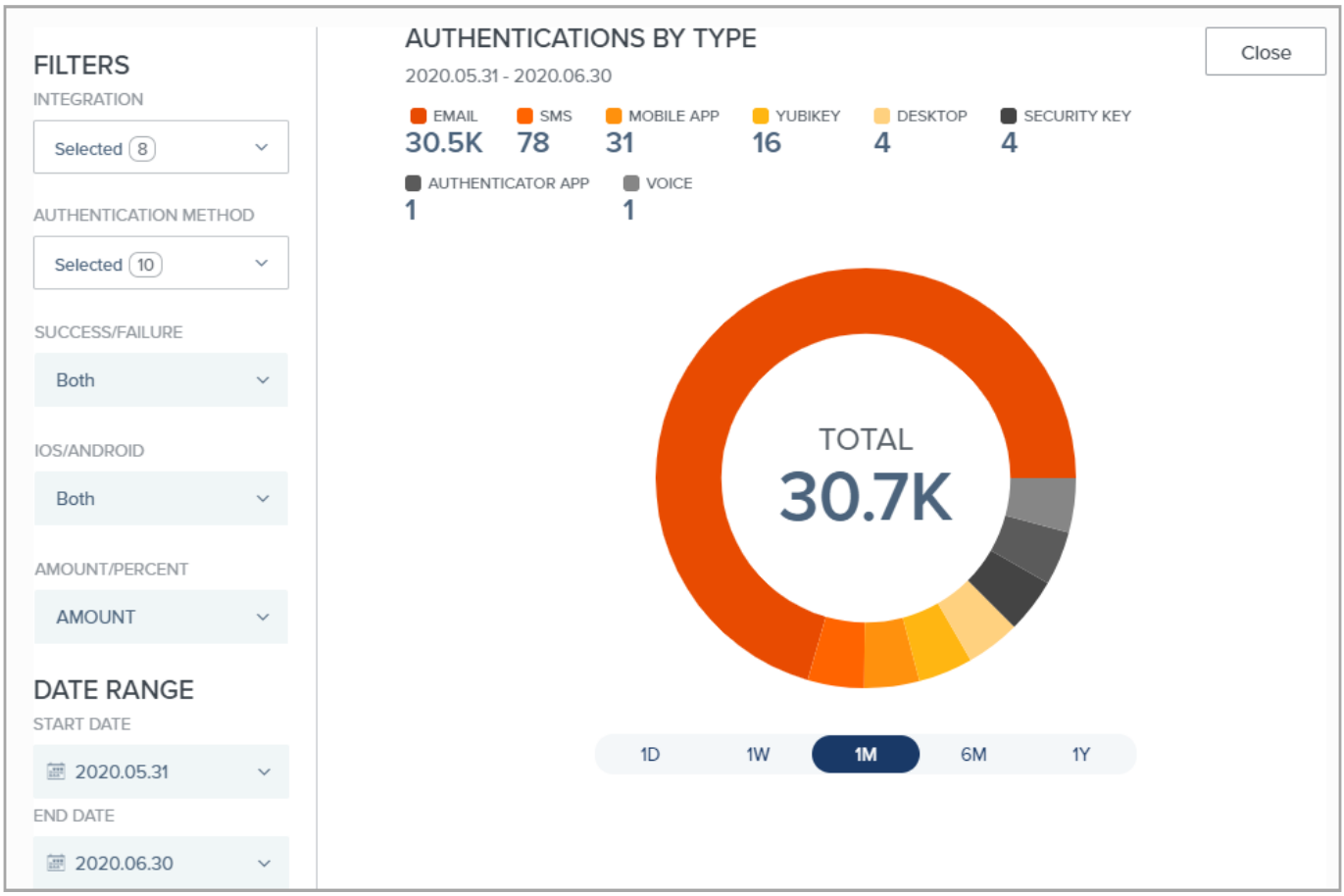
For more information, see:

- Managing users: PingID User Life Cycle Management
- Device management
- Reporting user status and device type: PingID User Detailed Status Report fields

Authentications by type

Authentications by type

The **Authentications by Type** chart shows the distribution of authentications by authentication method over the specified period.



For more information, see:

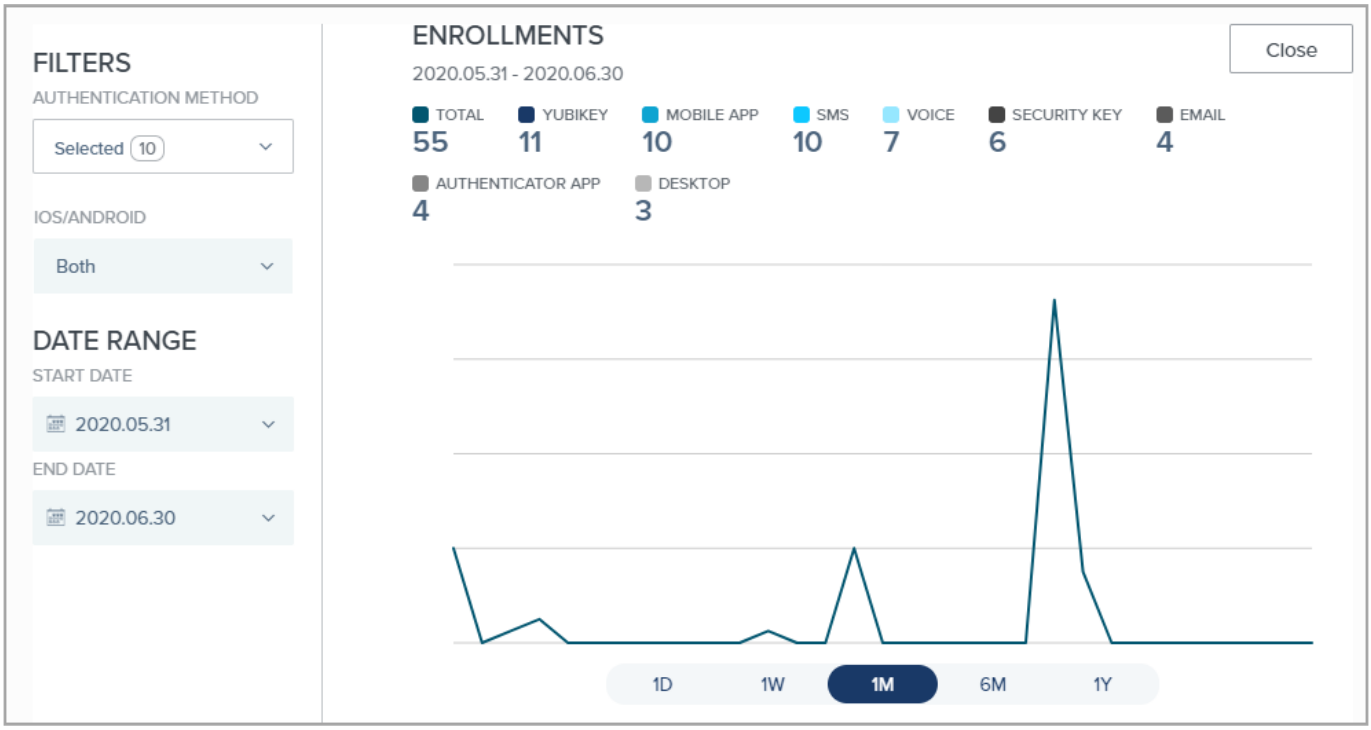
- Overview of PingID authentication types
- Configure PingID authentication

Enrollments

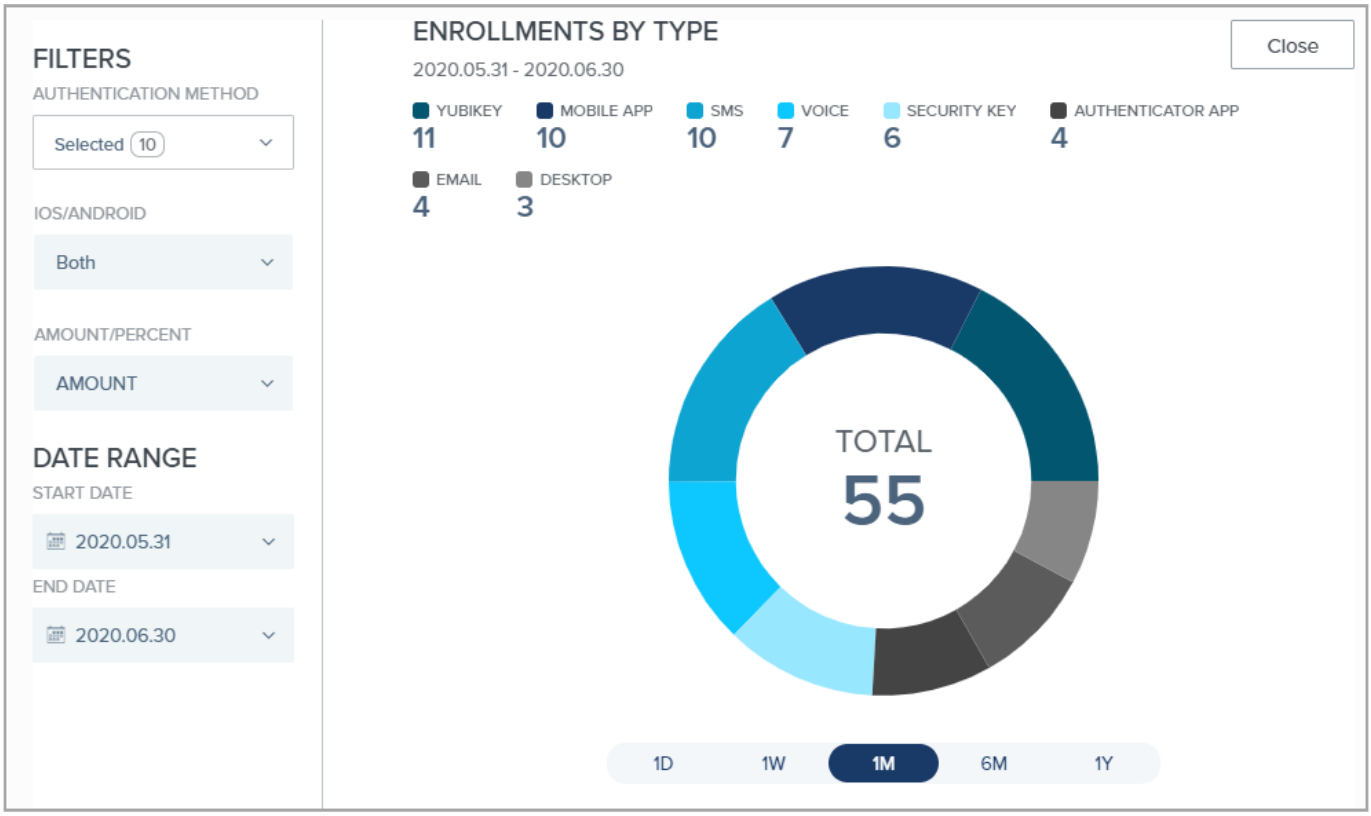
Enrollments

The **Enrollments** chart shows the number of new enrollments over time during the period specified.

== Enrollments



== Enrollments by type



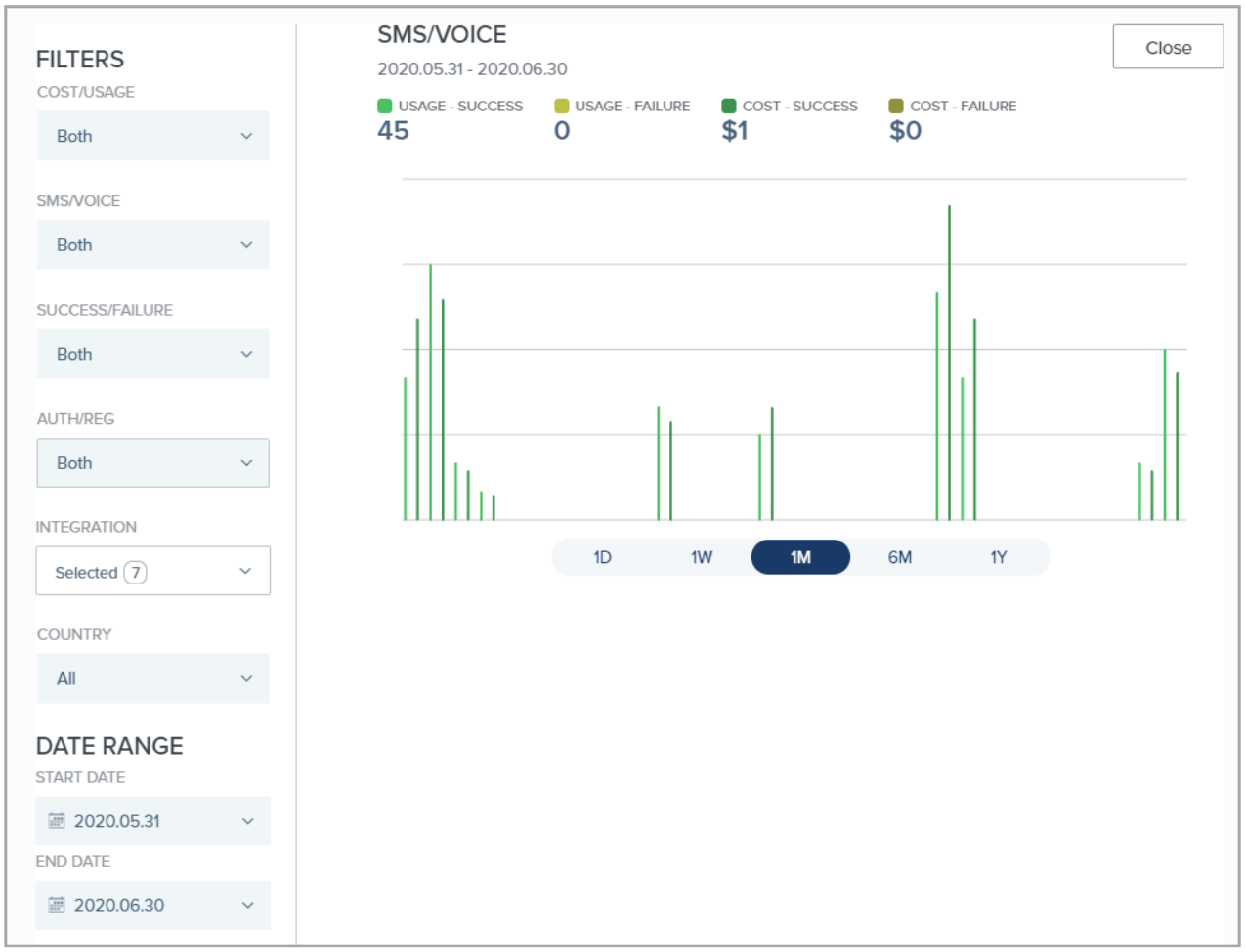
The **Enrollments by Type** chart shows the number of enrollments by type for the period specified.

For more information about device enrollment, see Managing your devices.

SMS and voice

SMS/Voice

The **SMS/Voice** chart shows success/failure information for SMS-based and voice-based enrollment and authentication, and the total cost for successful/failed attempts.



For more information on SMS-based and voice-based authentication, see:

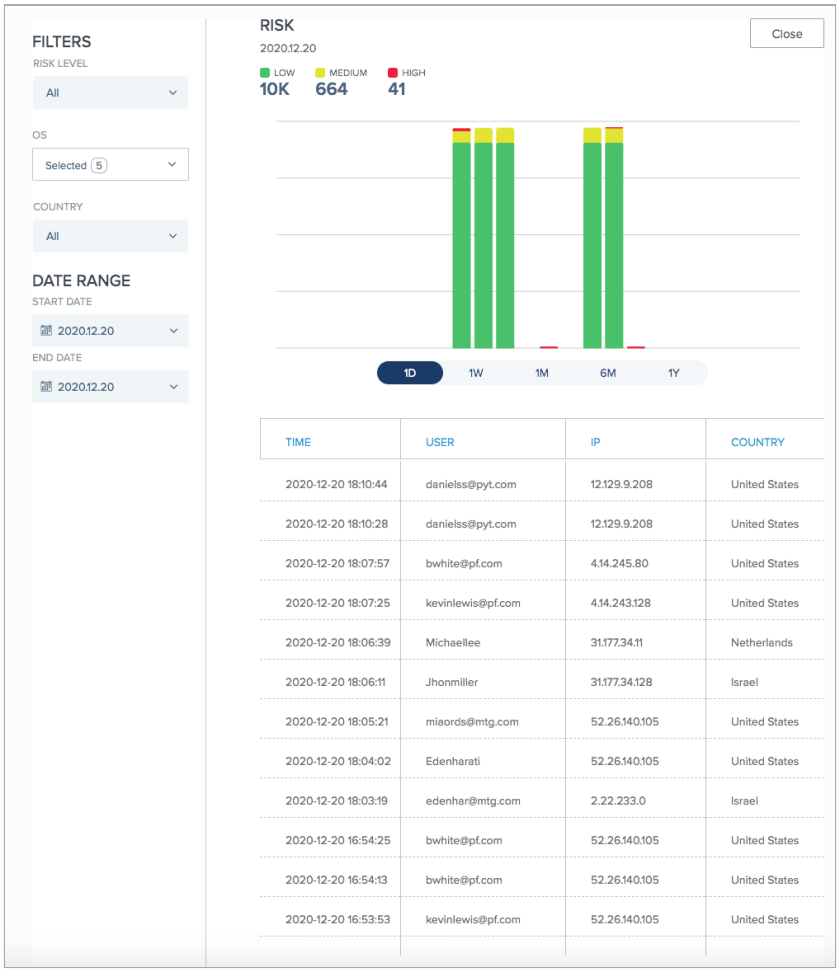
- Using SMS or voice authentication with PingID
- SMS and voice authentication

Risk

Risk

The **Risk** chart shows the distribution of risk evaluation results (Low, Medium, High) for authentication attempts during the specified time period.

> **Important**
>
> This chart is not available by default. If you do not see the chart and want to benefit from the additional intelligence and security information that it provides, contact your Ping Identity sales representative.



Data is displayed only for authentication policies that include the *user risk behavior* rule.

For more information on risk evaluation, see:

- Configuring an app or group-specific authentication policy
- Configuring a risk level rule (web policy)

PingID required domains, URLs, and ports

The following URLs must be accessible for the admin console and end user dock.

URL	Purpose
https://admin.pingone.com	The URL for admins to connect to the organization's PingOne and PingID accounts for administration and management purposes
https://desktop.pingone.com	Each organization has its unique user dock sign-on page URL, prefixed by https://desktop.pingone.com/
https://www.pingidentity.com/en/resources/downloads/pingid.html	The PingID clients download page, including the SSH, VPN, PingFederate SSO integration kits, desktop app, Windows login, Windows login passwordless, and Mac login integration clients

The following two tables show the access level required for each integration or client app. Where the first table shows "Yes", the appropriate domain is shown in the second table. In addition, port 443 must be open for the selected domains to enable HTTPS traffic.

Integration/Client App	Server Level Access		Client/Browser Level Access	
API	Authenticator	API	Authenticator	
PingID Adapter	Yes	Yes	No	Yes
RADIUS PCV	Yes	No	No	No
SSH	Yes	No	N/A	N/A
Win Login	N/A	N/A	Yes	Yes
Mac Login	N/A	N/A	Yes	Yes
ADFS	Yes	Yes	No	Yes
Mobile Clients	N/A	N/A	Yes	No
Desktop Apps Clients	N/A	N/A	Yes	No
Custom API Apps & Integrations	Yes	No	N/A	N/A

PingID PingIDCloud Service	Region	Domain
API	North America (NA)	idpxnyl3m.pingidentity.com ohi-idpxnyl3m.pingidentity.com ore-idpxnyl3m.pingidentity.com

PingID PingIDCloud Service	Region	Domain
Authenticator		authenticator.pingone.com
API	Europe (EU)	idpxnyl3m.pingidentity.eu fra-idpxnyl3m.pingidentity.eu ire-idpxnyl3m.pingidentity.eu
Authenticator		authenticator.pingone.eu
API	Australia (AU)	idpxnyl3m.pingidentity.com.au
Authenticator		authenticator.pingone.com.au

Organizations that permit the download and usage of the PingID desktop app or other PingID integrations should also permit access to the PingID products download page URL, also with port 443 open.

> **Note**
>
> If you use email for PingID one-time passcodes (OTP), ensure that your email system allows delivery of OTP messages. For more information, see https://aws.amazon.com/blogs/messaging-and-targeting/amazon-ses-ip-addresses/.

PingID supported browsers

PingID is part of PingOne for Enterprise. All browsers supported by PingOne for Enterprise are supported by PingID.

For the most up-to-date list of supported browsers, see Supported Environments on the PingOne for Enterprise requirements page.

Resetting your Admin portal password

If you forget your password to the PingOne Admin portal, reset it from the sign-on page.

About this task

> **Note**
>
> If you enter the wrong credentials three times, your account is locked for a 15 minute period.

Steps

1. On the Admin portal sign-on page, click **Change My Password**.

   Result:

   The **Recover Password** window displays.

2. Enter your email address and click **Submit**.

   Result:

You will receive an email link with instructions to reset your password.

Configure the PingID service

Configure the PingID features you require according to your organization's security policies.

To configure the PingID service, go to **Setup → PingID → Configuration**.

- Configuring the PingID support message
- Configuring the PingID enrollment settings
- Configuring device management
- To configure authentication methods, see Configure PingID authentication.

Configuring the PingID support message

Configure a support message to appear on various authentication screens during the authentication process.

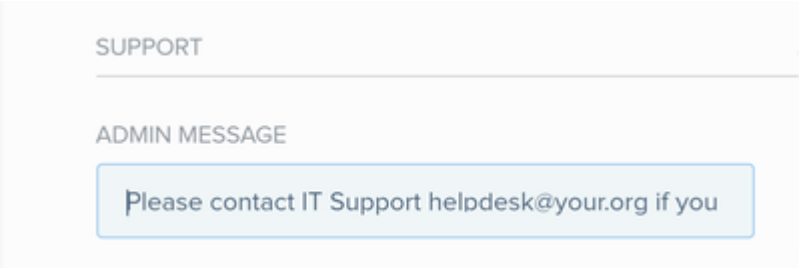
About this task

> **Note**
>
> PingID Authenticator supports Content Security Policy (CSP) to prevent unverified scripts from running in the PingID environment. CSP-supported browsers will not execute custom scripts defined in the **Admin Message** field.
> To benefit from the latest security enhancements, always update your web browsers to include the latest security features and security patches.

Steps

1. Sign on to the admin console.
2. Go to **Setup → PingID → Configuration**.
3. In the **Support** section, enter a message in the **Admin Message** field to display to your users during authentication.

> **Note**
>
> You can include HTML tags, if required.



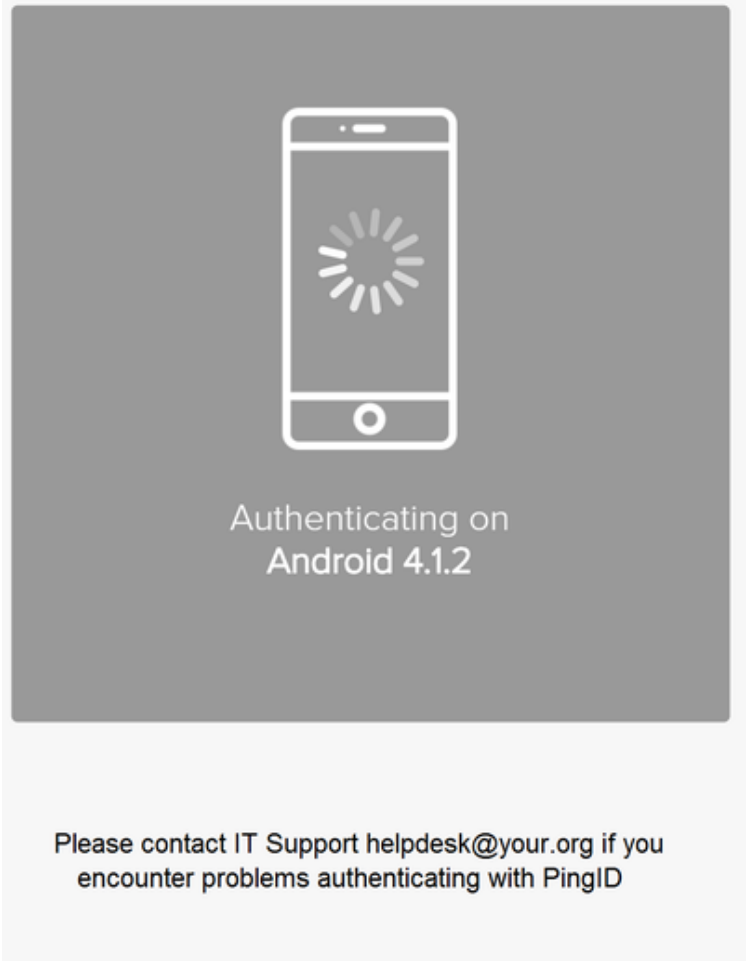
Example:

```
Please contact IT Support helpdesk@your.org if you encounter problems authenticating with PingID.
```

1. Click **Save**.

   Result:

   The support message displays on the authentication screens during the authentication process.



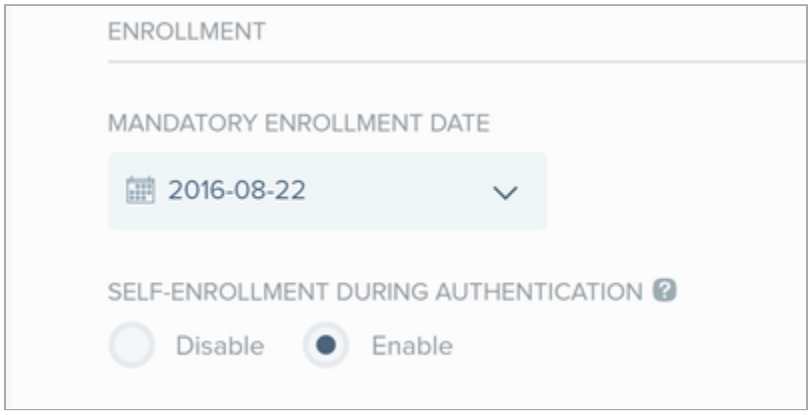
> **Note**
>
> It can take up to two minutes for changes to take effect.

Configuring the PingID enrollment settings

Customize the PingID enrollment experience.

Steps

1. Sign on to the admin console.
2. Go to **Setup → PingID → Configuration**.
3. In the **Enrollment** section:



1. In the **Mandatory Enrollment Date** field, select a final date for your users to enroll for the PingID service.

   Before this date, users can click **Not Now** to skip the enrollment process and still sign on to the service. After this date, the **Not Now** button is not available. Users must first enroll in PingID to sign on.

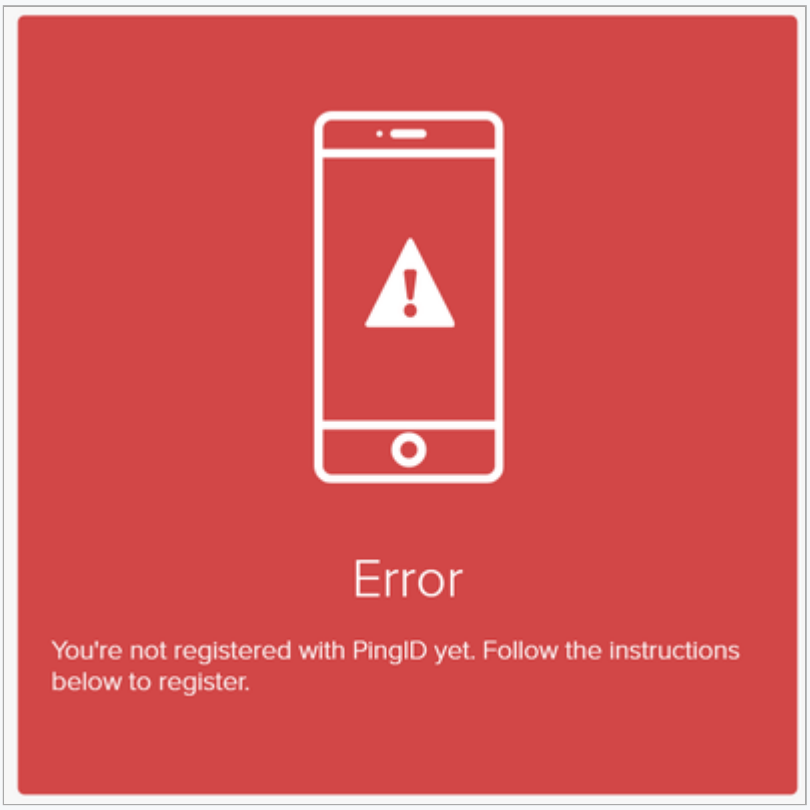
   > **Note**
   >
   > Entering a past date will force users to enroll with PingID upon first sign on.

2. In the **Self-Enrollment During Authentication** section, permit or disable end-user self-enrollment for all PingID services on their first authentication.

   The default selection is **Enabled**. This option allows the organization to implement customized business logic on first authentications.

Important

When self-enrollment is **Disabled**, users who are not registered for at least one authentication method will receive an error screen on their first authentication attempt and will not be able to complete authentication and self-enrollment.



To reduce confusion when disabling self-enrollment, enter an appropriate message in the **Admin Message** field, as shown in the following example.

```
New users should register at the following link: <Registration URL>. For other support issues, contact the help desk.
```

Before disabling self-enrollment, we recommended that you use a mechanism to trap the error status, and apply the customized logic. Develop this customization using PingID APIs. For more information, see The PingID API.

3. **Enforce Policy evaluation after new device registration** - this option ensures that in situations where users without a paired device attempt to access an application, the relevant authentication policies for the application will be applied in order to control access to the application after the user has successfully paired their device.

4. Click **Save**.

Device management

You can choose whether users can pair multiple devices and if they can manage their own devices.

Depending on the allowed configuration, the PingID default **Devices** page enables users to pair, unpair, and rename their devices, as well as define their primary device. Users can access the **Devices** page through a URL, the dock, or the **Settings** button on the default PingID authentication page. The **Devices** page lists all authentication devices associated with the user's account. You can also allow users limited device management in the PingID mobile app.

In the admin portal, you can configure the following options:

- The number of devices a user can pair with PingID. The maximum is 20.
- Whether users are allowed to unpair and change devices using the PingID mobile app.
- Whether users are allowed to access their **Devices** page to manage their devices on the web. You can restrict access to the **Devices** page to users with at least one paired device.
- Whether PingID sends an email notification to users when a new device is paired to their account.
- For users that have more than one paired device, define which device is presented to the user for authentication in the PingID default UI. Select one of the following options:
  - **Default to Primary**: Prompts the user to authenticate with their primary device, if permitted by the PingID policy. Otherwise, authenticate using the next permitted device.
  - **Prompt User to Select**: Allow the end user to choose their authentication method. When prompted to authenticate, the user is presented with a list of the authentication methods they have paired to their account. Only authentication methods permitted by the relevant PingID policy are shown.

> **Note**
>
> These fields are only visible if two or more devices are permitted in the **Maximum Allowed Devices** field.

If a user forgets or loses their device, and none of their paired devices are available, configure backup authentication to provide an alternative method of authentication based on user email and phone attributes stored in your organization's user directory.

For more information about the user experience, see Managing your devices.

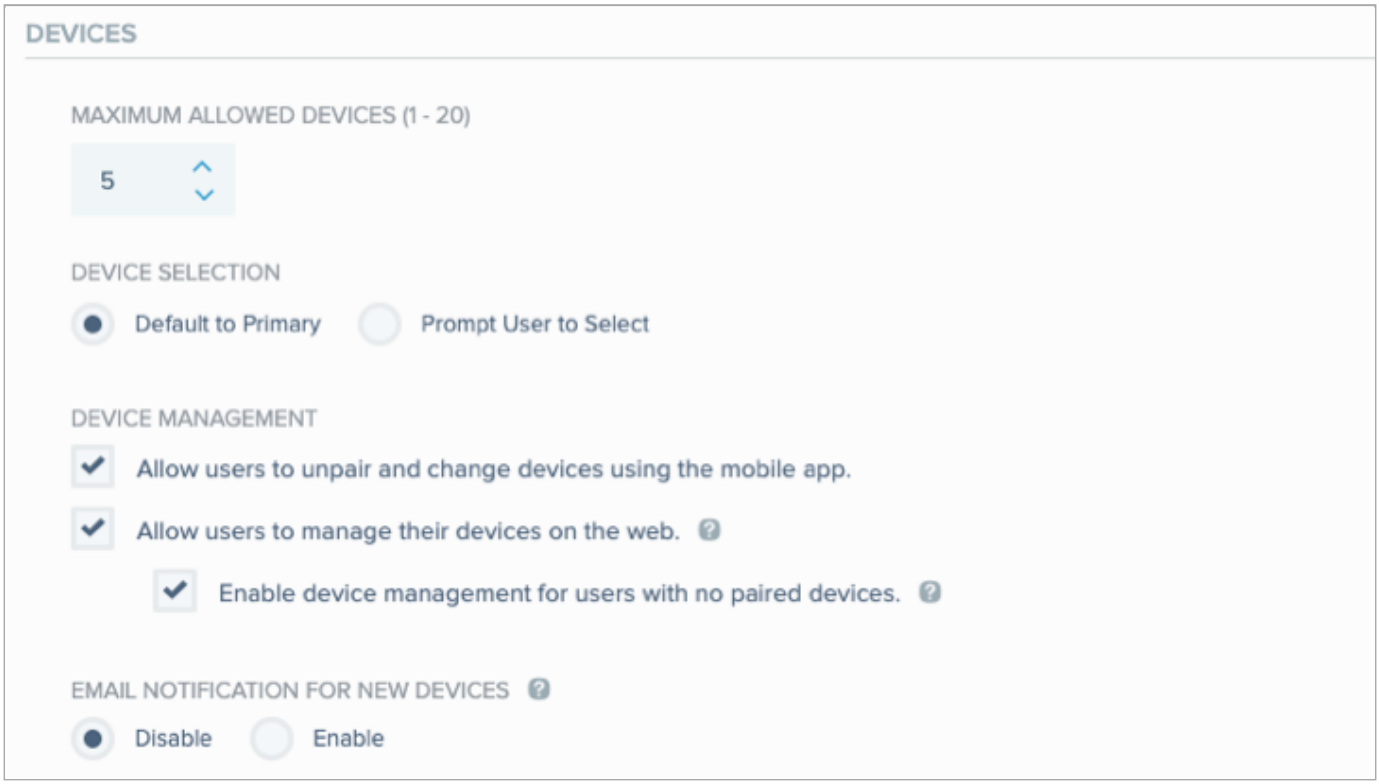
To manage user activity, including disabling or unpairing one or more devices and defining the primary device for a user, see PingID User Life Cycle Management.

Configuring device management

Configure the user device management settings.

Steps

1. Sign on to the admin console.
2. Go to **Setup → PingID → Configuration**.



3. In the **Devices** section, define the maximum devices a user can pair and how devices are presented when authenticating. From the **Maximum Allowed Devices** list, select the maximum number of devices that a user can pair with their account or app. The default value is 1, and the maximum value is 20.

> **Note**
>
> When a user adds more than one device, the devices appear on their **Devices** page and are listed in the order in which they were added. The most recently added device appears last in the list.

4. In the **Devices Selection** section, select one of the following options.

   Choose from:

   - **Default to Primary**: Prompts the user to authenticate with their primary device. If the primary device is not allowed by the PingID policy, the secondary permitted device is presented. Applies to PingID Web, API, RADIUS, and SSH default interfaces. For more information, see Policy evaluation.
   - **Prompt User to Select**: Allows the user to choose from the list of authentication methods paired with their account. Only authentication methods permitted by the relevant PingID policy are shown. Applies to PingID Web, API, RADIUS (when supporting challenge mode), and SSH default interfaces.

     > **Note**
     >
     > The **Devices Selection** section only appears if you select two or more devices from the **Maximum Allowed Devices** list.

5. In the **Device Management** section, configure the following options.

Check box	Description
Allow Users to Unpair and Change Devices Using the Mobile App	Allows users to unpair and change devices from within the PingID mobile app. + **Note** To enable this option for users paired to more than one data center, the **Allow users to unpair and change devices using the mobile app**" check box must be enabled for all data centers, and the data centers must be in the same location.
Allow Users to Manage Their Devices on the Web	Allows users to manage their devices on the web through their **Devices** page. For more information, see Managing your devices.
Enable Device Management for Users with No Paired Devices	Allows users to manage their devices even if they do not have a device paired with their account. This check box is optional.

6. In the **Email Notification for New Devices** field, click **Enable** to send an email to notify a user each time a device is paired with their account, and allow the user to report suspected fraud if they did not pair the device.

> **Note**
> Email notifications are fully customizable. For more information, see Configuring email notifications.

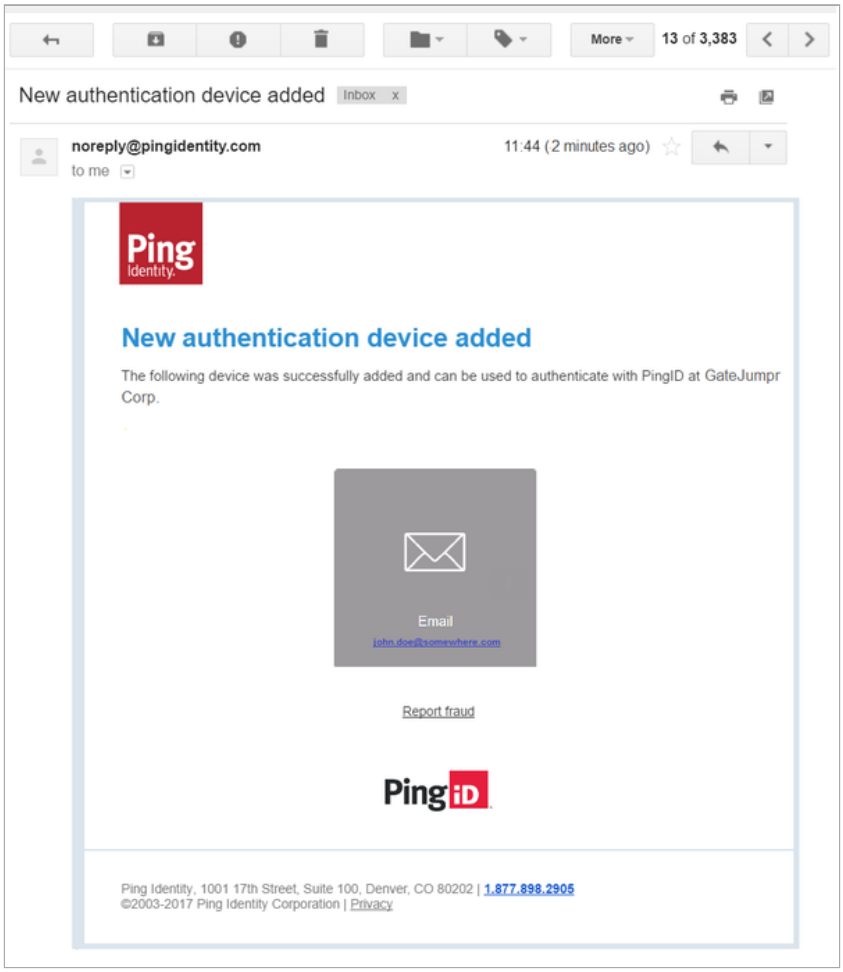
7. Click **Save**.

Configuring email notifications

Configure PingID to send an email notification to the user each time a new device is paired to ensure users are aware of every attempt to pair a device with their account and to enable them to report suspected fraud.

There is a separate email template for each device type. The email templates are customizable and can include elements such as branding or specific text. To customize the email, contact your Ping Identity representative.

The following image is an example of the default email notification template.



How to report fraud

Notification emails contain a link to report fraud in case the user receives a notification email without having paired a new device.

> **Note**
>
> - Repeated clicks on the **Report Fraud** link will trigger the Fraud Reported alert, but will not duplicate an entry in the activity log.
> - The **Report Fraud** link is valid for up to 30 days.

Administrators can access the details of devices paired by users through the PingID activity report. For more information, see Running the PingID activity report. You can filter the report to view only entries that contain **Fraud Reported** in the **Message** column.

How PingID receives the user's email address

When an authentication activity occurs following the pairing of a device, the PingID server receives the user's most up-to-date email address from your organization's identity provider (IdP) and uses it to send the notification email to the user.

To define email addresses, configure the script variables or parameters, as shown in the following table.

Email address source	Reference	Remarks
RADIUS	PingID RADIUS PCV parameters reference guide	In the General Parameters table, see **Multiple Attributes Mapping Rules**
PingID API	PingID API - AddUser	See AddUser
AD FS	Configuring advanced settings	See **Email Attribute** in step 5.
Azure AD	Configuring PingID MFA for Microsoft Azure AD Conditional Access	See step 3d.
PingID for PingFederate	Configuring a PingID Adapter instance	See **Email Attribute** in step 5.
PingOne SSO stand alone	Connecting to an identity repository	

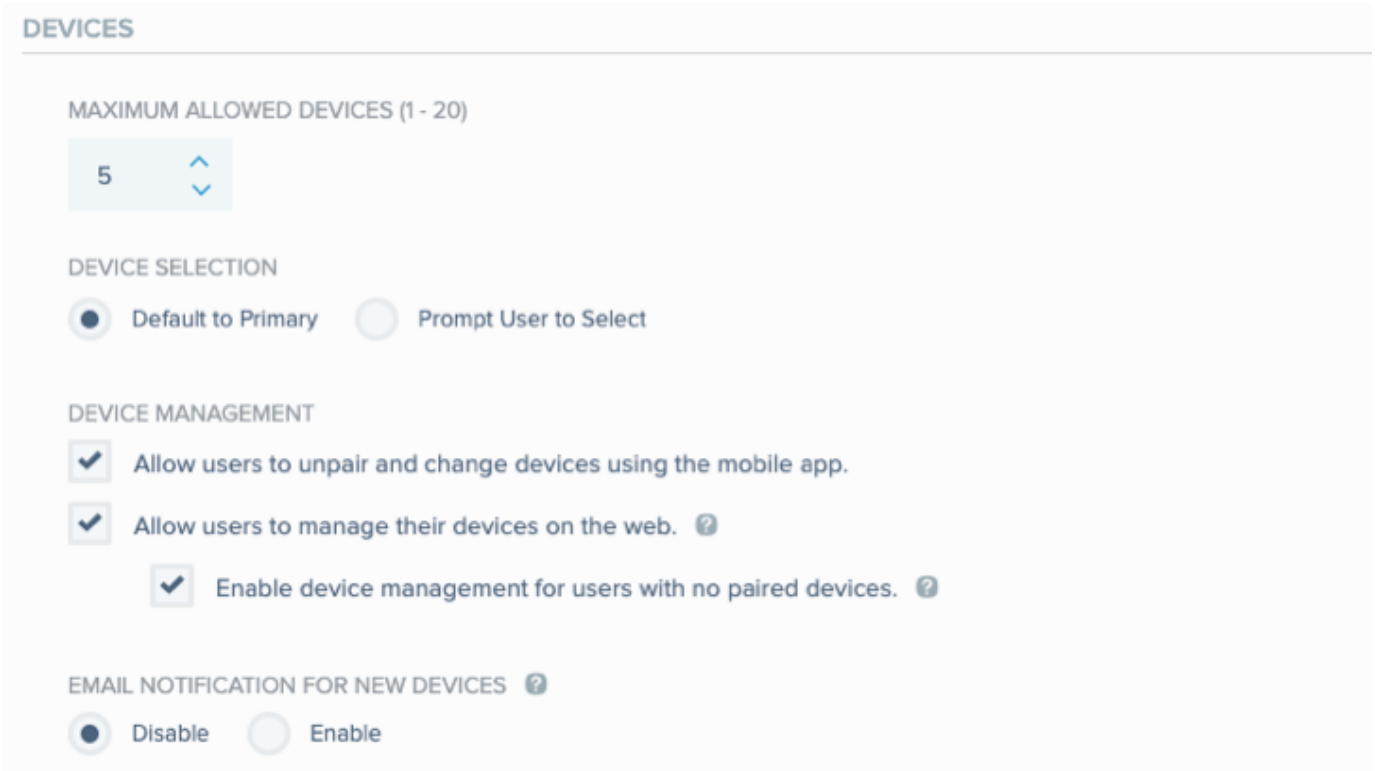
Configuring email notifications

About this task

To enable email notifications when a user pairs a new device:

Steps

1. Sign on to the admin console.
2. Go to **Setup → PingID → Configuration** and go to the **DEVICES** section.



3. In the **EMAIL NOTIFICATION FOR NEW DEVICES** section, click **Enable**.

4. Click **Save**.

Result

Users will receive a notification email each time a device is paired with their account or app.

Configuring evaluation expiration

If your organization is currently evaluating PingID, configure the policy that will apply when your PingID evaluation period ends.

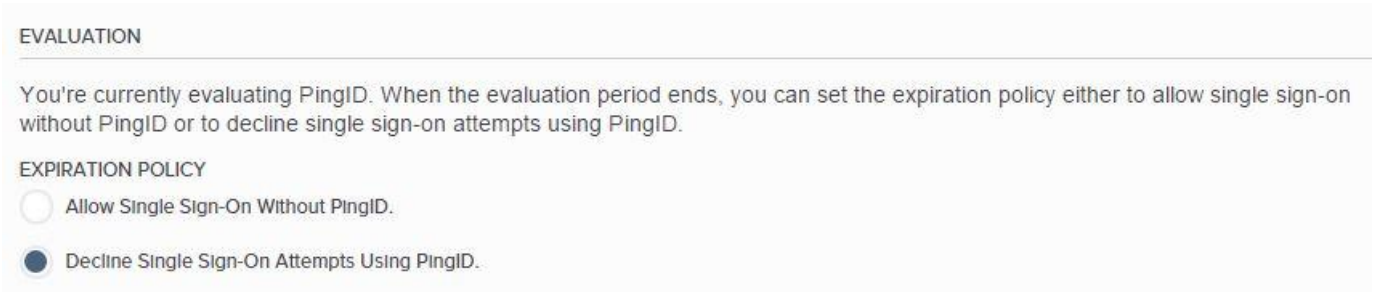
Steps

1. Sign on to the admin console.
2. Go to **Setup → PingID → Configuration**.
3. In the **Evaluation** section, select one of the following expiration policies:

   Choose from:

   - To allow users to sign on to any service using only their first-factor authentication, click **Allow Single Sign-On Without PingID**. This is the default selection.
   - To enforce signing on with PingID when the evaluation period ends, click **Decline Single Sign-On Attempts Using PingID**.

     > **Note**
     >
     > The selected expiration policy will only apply after the evaluation period expires.



4. Click **Save**.

Configure PingID authentication

You can configure PingID authentication options according to your organization's security policy and the different use cases relevant to your organization.

PingID mobile app authentication

- Configure biometrics authentication for the PingID mobile app
- Configure the duration of new authentication requests
- Configure one-time passcode fallback
- Configure direct passcode usage
- Configure authentication when the device is locked
- Enable or disable location collection
- Define the authenticating app appearance

PingID desktop app authentication

- Configure the PingID desktop app
- Configure the PingID desktop app PIN
- Reset a user's desktop app PIN
- Enable or disabling automatic updates
- Configure PingID Proxy for the PingID desktop app
- Configure Proxy Auto Configuration
- Configure Kerberos proxy authentication
- Set up PingID desktop app on Windows using the UI
- Install the desktop app using the Windows CLI
- Set up PingID desktop app on a Mac using the UI
- Install the desktop app using the Mac CLI
- Troubleshoot the desktop app

FIDO2 biometrics

(Apple Touch ID, iOS biometrics, Windows Hello, and Android biometrics capabilities)

- FIDO2 biometrics requirements and limitations
- Configure passwordless authentication
- Configure MFA authentication
- FIDO2 biometrics use cases

FIDO2 security key

- FIDO2 security key requirements and limitations
- Configure security key authentication
- FIDO2 security key use cases

YubiKey authentication

- Configure YubiKey authentication

OATH token authentication

- Configure OATH token authentication

Email authentication

- Configure email authentication
- Customize emails

SMS and voice authentication

- Configure SMS and voice authentication
- Language localization for voice authentication
- Language localization for SMS authentication
- Using a custom Twilio account with PingID
- SMS and voice usage limits

Additional options

- Pre-populate or restrict user registration data
- Configure backup authentication methods
- Enable advanced authentication policy
- Configure the phone number attribute in PingOne
- Configure LDAP attributes in PingFederate
- Disable pairing for a specific authentication method
- Remove authentication methods

Next steps...

To apply policies to authentication methods, see PingID policy settings.

Configuring authentication for the PingID mobile app

Users can download the PingID mobile app from the app store to any Android or iOS device.

The PingID app enables users to authenticate with:

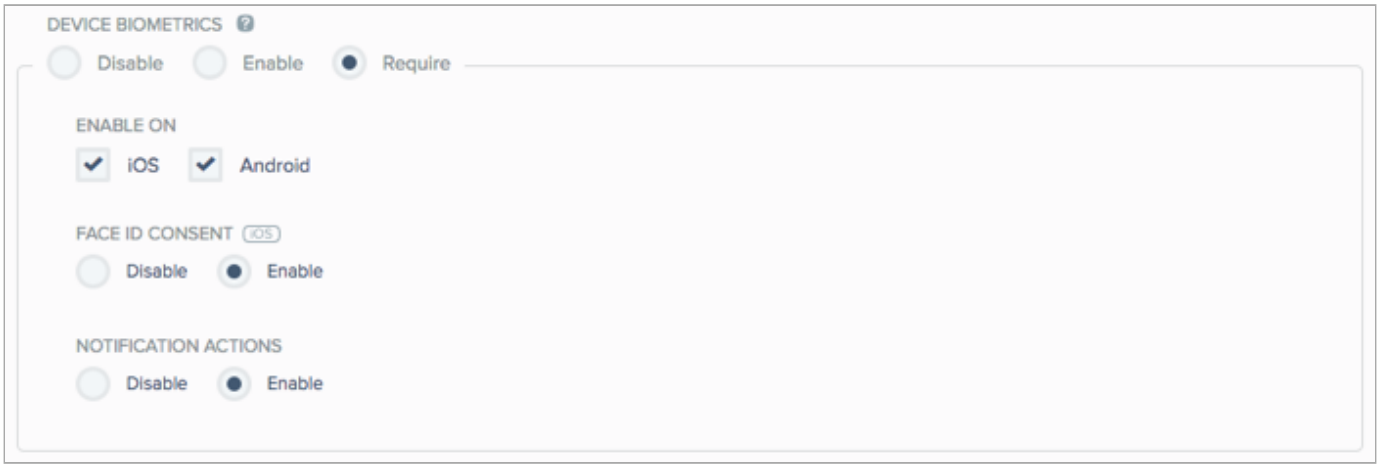
- Swipe authentication. This is authentication method is enabled by default.
- Biometrics authentication. If enabled, this authentication method allows users to authenticate using their device biometrics, such as fingerprint or Face ID.
- One-time passcode (OTP). If configured, the PingID mobile app generates an OTP that the user can use in place of swipe or biometrics.

Configuring biometrics authentication for the PingID mobile app

Allow users to authenticate using their fingerprint or Face ID.

Steps

1. In the PingID admin portal, go to **Setup → PingID → Configuration**, and in the **Mobile App Authentication** section, go to the **DEVICE BIOMETRICS** section.



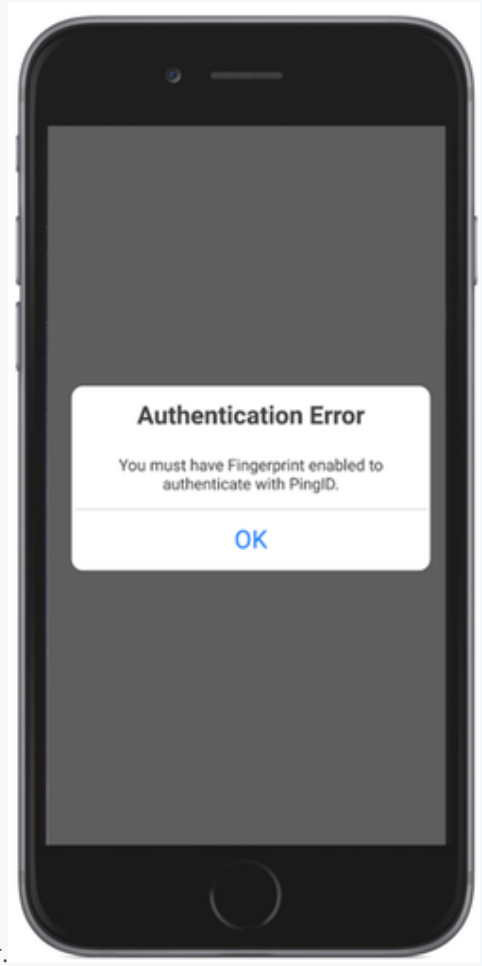
2. Enable or to require device biometrics:

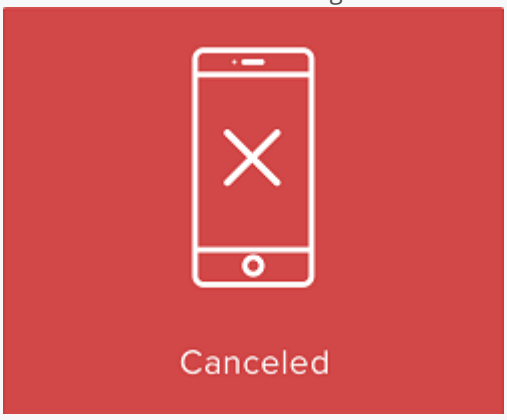
   Choose from:

   - **Disable**: Disable device biometrics. Users are not able to authenticate using their device biometrics.
   - **Enable**: Enable users to authenticate with their device biometrics.
   - **Require**: Force users to authenticate with their device biometrics. Users with devices that do not support biometrics are prompted to authenticate using swipe authentication.

Note

If a user's mobile device supports biometrics, but they have not configured biometrics authentication on their device, they cannot sign on. The user receives an Authentication Error message on their mobile device and a Canceled message on their web browser.





3. In the **Enable On** section, select the check box for each operating system on which you want to enable biometrics (**iOS**, **Android**).

Note

If biometrics authentication is disabled for an operating system, or the device does not support biometrics, the standard swipe method of authentication is used.

4. **Optional:** By default, iOS device users are only asked to authorize the use of Face ID for PingID authentication when pairing PingID with their device. To prevent users inadvertently authenticating using Face ID if their phone is unlocked, force users to explicitly approve a Face ID consent notification.

   > **Note**
   >
   > This option is available on devices with the PingID mobile app 1.10.0 and later, and Face ID enabled.

   1. To enable Face ID consent, in the **Device Biometrics** section, click either **Enable** or **Require**.
   2. Click **iOS**.
   3. In the **Face ID Consent** field, click **Enable**.

5. If you select **Require** in the **Device Biometrics** section, in the **Notification Actions** section, select one of the following options:

   Choose from:

   - **Disable**: Disable notification actions for PingID mobile app. The user is unable to approve or deny PingID mobile app authentication requests from the locked screen:
   - Android: The user cannot swipe down on the notification banner, and the **Approve** or **Deny** buttons are not available.
   - iOS: The user cannot see alternative actions when swiping to the left on the notification banner.
   - **Enable**: Enable notification actions for PingID mobile app. The user can approve or deny PingID mobile app authentication requests from within the notification message on their locked screen. This is the default selection.
   - Android: When the screen is locked, the user might receive a notification to authenticate, depending on the mobile device's notification configuration. When swiping down on the notification banner, the user can select the **Approve** or **Deny** buttons.
   - iOS: The user receives a notification banner and can swipe to the left on the notification banner to see the **Approve** and **Deny** buttons.

6. To prevent users from bypassing the required biometrics authentication and using the passcode fallback on the mobile app, configure the **Device Passcode Fallback** field.

   If biometrics authentication fails, by default, the user falls back to the device's passcode to authenticate.

   > **Note**
   >
   > This configuration is only relevant to iOS when the following conditions apply:
   > - **Device Biometrics** is set to **Require**.
   > - **iOS** is selected.
   > - **Notification Actions** is set to **Disable**.

   Choose from:

   - **Disable**: When the **Disable** option is selected, users are prevented from using the passcode fallback and cannot bypass the required biometrics authentication on the application.
   - Only users with biometrics defined on their device, such as fingerprints or face scan, can authenticate successfully.

- If the authentication is unsuccessful, users can retry up to the maximum number of retries permitted by the OS. This is not configurable.
- If all retries are unsuccessful, access is denied, and a notification is displayed on both the accessing device browser and the mobile app.
- **Enable**: When the **Enable** option is selected, and biometrics authentication fails, the user can use the device's passcode to authenticate with PingID. This is the default selection.

> **Important**
>
> - PingID 1.6.4 and later support device passcode fallback.
> - Mobile device management (MDM) can be used to prevent the user from updating the mobile lock abilities, or adding other users' fingerprints to a mobile device.
> - If there are users who have installed the mobile app before this setting was applied, the settings apply the next time the user is online.

7. Click **Save**.

> **Note**
>
> Samsung Galaxy S5 devices have a known bug that can cause fingerprint data to become corrupted, preventing PingID from launching properly. Specifically:
> - The data corruption issue is a device problem (not a bug in PingID) as can be seen from sites such as: https://gs5.gadgethacks.com/how-to/4-ways-fix-your-galaxy-s5-s-dysfunctional-fingerprint-scanner-0158909/
> - If biometrics authentication is configured by the administrator for the organization, S5 device owners may experience a PingID launch problem due to fingerprint data corruption. This may occur even if the S5 devices were not configured for fingerprint support.

The following tables describe the user experience according to the operating system and configuration setting combination.

Table 1. Cases Matrix for iPhone iOS 8+ Devices

Biometrics configured on device	State	Disable notification actions	Banner actions on locked screen	Banner actions on unlocked screen	User swipes banner right on locked screen	User presses (taps) banner on unlocked screen
Yes	Enabled	N/A (There is no option to change this in the UI.)	1. Swipe left. The **Deny** and **Approve** buttons are displayed. 2. When approved, unlock with Touch ID or passcode.	Swipe the banner down to display the **Approve** and **Deny** buttons. When approved, authentication completes. No biometrics are required.	Unlock with Touch ID or passcode. When approved, the PingID app opens and requests biometrics authentication.	The PingID app opens and requests biometrics authentication.

Biometrics configured on device	State	Disable notification actions	Banner actions on locked screen	Banner actions on unlocked screen	User swipes banner right on locked screen	User presses (taps) banner on unlocked screen
Yes	Required	Disabled (Checked)	• There is no swipe left option. • The user must open the app and use biometrics authentication.	• Banner display only. • No actions.	The PingID app opens and requests biometrics authentication.	The PingID app opens and requests biometrics authentication.
Yes	Required	Enabled (Unchecked)	1. Swipe left. The **Deny** and **Approve** buttons are displayed. 2. Once approved, unlock with Touch ID or passcode.	Swipe the banner down to display the **Approve** and **Deny** buttons. When approved, authentication completes.	The PingID app opens and requests biometrics authentication.	The PingID app opens and requests biometrics authentication.
Not configured / Not supported	Enabled	N/A	1. Swipe left. 2. The **Deny** and **Approve** buttons are displayed. 3. When 'approved', unlock with passcode.	Swipe the banner down to display the **Approve** and **Deny** buttons. When approved, authentication completes.	Unlock with passcode. When approved, the PingID app opens and requests swipe authentication.	The PingID app opens and requests swipe authentication.
Not configured / Not supported	Required	Disabled (Checked)	There is no swipe left option.	• Banner display only. • No actions.	Unlock with passcode. When approved, the PingID app opens and displays an error.	The PingID app displays an error.

Biometrics configured on device	State	Disable notification actions	Banner actions on locked screen	Banner actions on unlocked screen	User swipes banner right on locked screen	User presses (taps) banner on unlocked screen
Not configured / Not supported	Required	Enabled (Unchecked)	1. Swipe left. The **Deny** and **Approve** buttons are displayed. 2. Once approved, unlock with passcode. 3. The PingID app displays an error.	Swipe the banner down to display the **Approve** and **Deny** buttons. When approved, the PingID app displays an error.	Unlock with passcode. When approved, the PingID app opens and displays an error.	The PingID app displays an error.

Table 2. Cases Matrix for Android 5.0+ Devices

Yes	Enabled	N/A	Show content: 1. A notification is displayed. 2. Swipe down to display the **Deny** and **Approve** buttons. 3. When approved, the user is prompted to unlock the device using fingerprint, and authentication completes. Hide content: 1. Displays a notification without the **Deny** and **Approve** buttons. 2. Tap the notification to reach the prompt to unlock. 3. When unlocked, the PingID app opens, requesting fingerprint authentication. Do not show notifications: 1. Lights the screen and sounds a beep. 2. Unlock the device.	The PingID app opens and requests fingerprint authentication.	1. The user is prompted to unlock the device. 2. When unlocked, the PingID app opens and requests fingerprint authentication.

Fingerprint configured on device	State	Disable notification actions	Banner actions on locked screen	Banner actions on unlocked screen	User taps on banner on locked screen
			3. The PingID app opens, requesting fingerprint authentication.		

Yes	Required	Disabled (Checked)	Show content: 1. Displays a notification without the **Deny** and **Approve** buttons. 2. Tap the notification to reach the prompt to unlock. 3. fingerprint Hide content: 1. Displays a notification without the **Deny** and **Approve** buttons. 2. Tap the notification to reach the prompt to unlock. 3. When unlocked, the PingID app opens, requesting fingerprint authentication. Do not show notifications: 1. Lights the screen and sounds a beep. 2. Unlock the device. 3. The PingID app opens, requesting fingerprint authentication.	The PingID app opens and requests fingerprint authentication.	1. The user is prompted to unlock the device. 2. When unlocked, the PingID app opens and requests fingerprint authentication.

Yes	Required	Enabled (Unchecked)	Show content: 1. A notification is displayed. 2. Swipe down to display the **Deny** and **Approve** buttons. 3. When approved, the user is prompted to unlock the device using fingerprint, and authentication completes. Hide content: 1. Displays a notification without the **Deny** and **Approve** buttons. 2. Tap the notification to reach the prompt to unlock. 3. When unlocked, the PingID app opens, requesting fingerprint authentication. Do not show notifications: 1. Lights the screen and sounds a beep. 2. Unlock the device.	The PingID app opens, requesting fingerprint authentication.	The PingID app opens and requests fingerprint authentication.

Fingerprint configured on device	State	Disable notification actions	Banner actions on locked screen	Banner actions on unlocked screen	User taps on banner on locked screen
			3. The PingID app opens, requesting fingerprint authentication.		
Not configured / Not supported	Enabled	N/A	• No banner display. • The app prompts for PingID swipe.	• No banner display. • The app prompts for PingID swipe.	The PingID swipe screen is displayed.

Not configured / Not supported	Required	Disabled (Checked)	Show content: 1. Displays a notification without the **Deny** and **Approve** buttons. 2. Tap the notification to reach the prompt to unlock. 3. When unlocked, the PingID app displays an error. Hide content: 1. Displays a notification without the **Deny** and **Approve** buttons. 2. Tap the notification to reach the prompt to unlock. 3. When unlocked, the PingID app displays an error. Do not show notifications: 1. Lights the screen and sounds a beep. 2. Unlock the device. 3. The PingID app displays an error.	The PingID app displays an error.	The PingID app displays an error.

Not configured / Not supported	Required	Enabled (Unchecked)	Show content: 1. A notification is displayed. 2. Swipe down to display the **Deny** and **Approve** buttons. 3. When approved, the user is prompted to unlock the device using fingerprint, and the PingID app displays an error. Hide content: 1. Displays a notification without the **Deny** and **Approve** buttons. 2. Tap the notification to reach the prompt to unlock. 3. When unlocked, the PingID app displays an error. Do not show notifications: 1. Lights the screen and sounds a beep. 2. Unlock the device. 3. The PingID app displays an error.	The PingID app displays an error.	The PingID app displays an error.

Configuring the duration of new authentication requests

Configure the amount of time that an authentication request lasts before timing out.Customize the authentication experience to your user's needs and reduce the number of users that experience a push notification timeout when attempting to authenticate using the PingID mobile app.

About this task

An authentication request consists of the following two parts, both of which are configurable:

- Device Timeout: the maximum time allowed for a new authentication notification request to reach a user's mobile device before timeout occurs. The default value is 25 seconds.
- Total Timeout: the total amount of time a new authentication request has to reach a user's mobile device before timeout occurs. The difference between the device timeout and total timeout indicates the amount of time the user has to respond upon receiving an authentication request before timeout occurs. The default value is 40 seconds.

You can configure timeout values per service, such as Web SSO, Windows login, API, SSH, or VPN, or set global timeout values that are applied to all services. You can increase the timeout values to extend the amount of time a user has to complete authentication on their mobile device before timeout occurs.

This is useful for users with a slow internet connection, for example. You can also use this feature with the direct passcode usage feature to enable users with slow connections to use a one-time password (OTP) to authenticate immediately, rather than responding through a push notification or waiting for the notification to timeout. For more information, see Configuring direct passcode usage.

Changes to the default timeout configuration are applied per organization to all authentication requests, including retry authentication attempts.

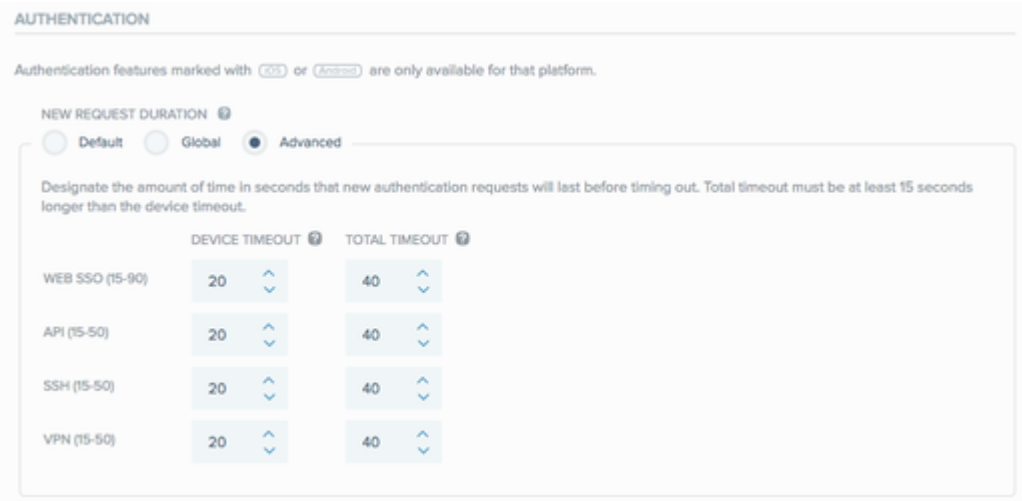
> **Note**
>
> If push notifications are disabled for a user in the PingID mobile app (**Swipe Settings → Disable Swipe**), the user is directed to the fallback OTP flow immediately, and no timeout period is applied.

Steps

1. In the admin console, go to **Setup → PingID → Configuration**.
2. In the **New Request Duration** section of the **Authentication** section, select one of the following options:

   Choose from:

   - To apply the default timeout values, click **Default**.
   - To apply custom timeout values globally to all services, click **Global**. Use the arrows  to adjust the values, or enter the values in the **Device Timeout** and **Total Timeout** fields.
   - To define timeout values per service, click **Advanced**. For each service that you want to customize, use the arrows  to adjust the values, or enter the values in the **Device Timeout** and **Total Timeout** fields.



> **Note**
>
> The range of valid timeout values are shown in parentheses next to each service name. If you do not change a value, PingID uses the default value. For each entry, the value in the **Total Timeout** field must be at least 15 seconds greater than the value in the **Device Timeout** field.

1. Click **Save**.

   Result:

   The changes are saved and applied to users upon their next authentication attempt.

Configuring one-time passcode fallback

The one-time passcode (OTP) fallback setting allows administrators to configure whether users can fall back to an OTP when the mobile app response times out.

About this task

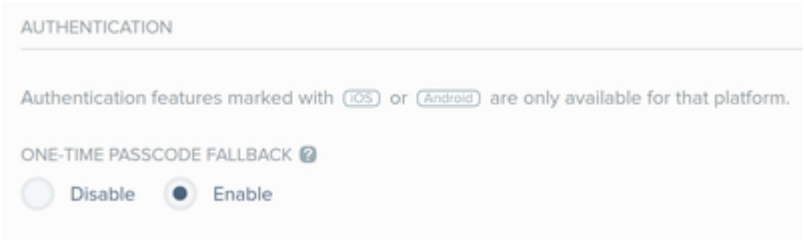
Disabling this setting helps to enforce a security policy that requires authentication by biometrics only. The default setting is **Enable**.

> **Note**
>
> - You can also enable direct OTP selection to allow users to authenticate with an OTP immediately, without waiting for the authentication request to time out. For more information, see Configuring direct passcode usage.
> - If you are using PingOne DaVinci to orchestrate your PingID flows, and want to disable OTP fallback, you must disable it in the flow settings node in DaVinci, as well as the Admin portal.

Steps

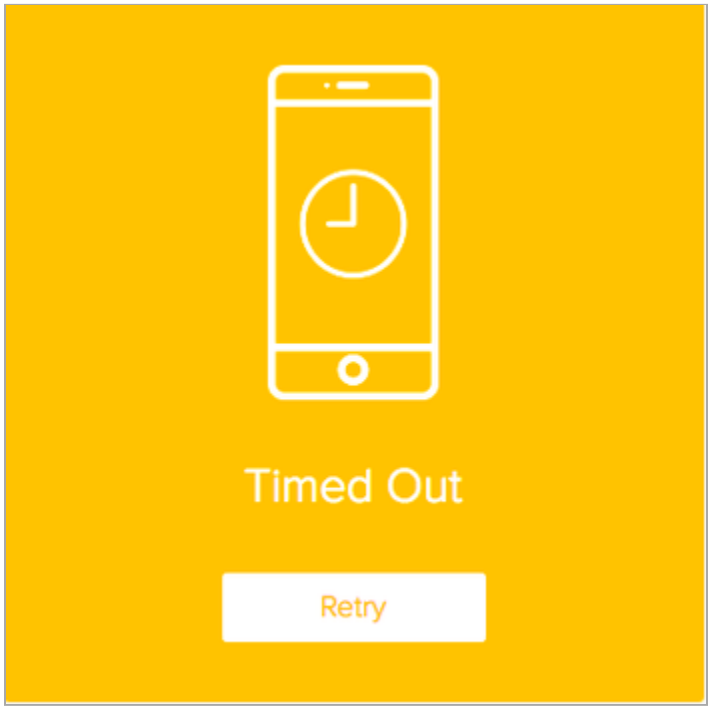
1. In the PingID admin portal, go to **Setup → PingID → Configuration**.

2. In the **One-Time Passcode Fallback** section of the **Authentication** section, select one of the following options:

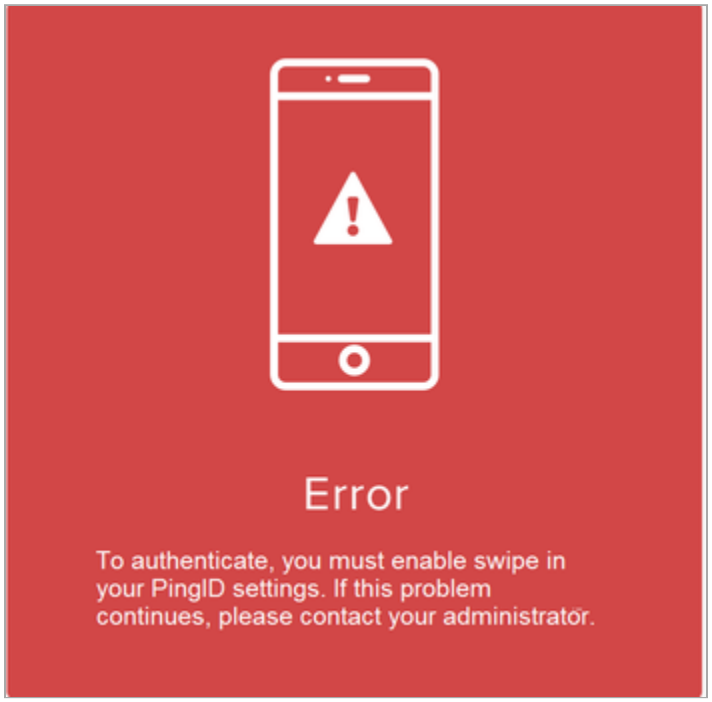


Choose from:

- To disable authenticating with an OTP when the mobile app response times out, click **Disable**. If the request times out or the user's mobile is offline, the user receives the yellow **Timed Out** message.



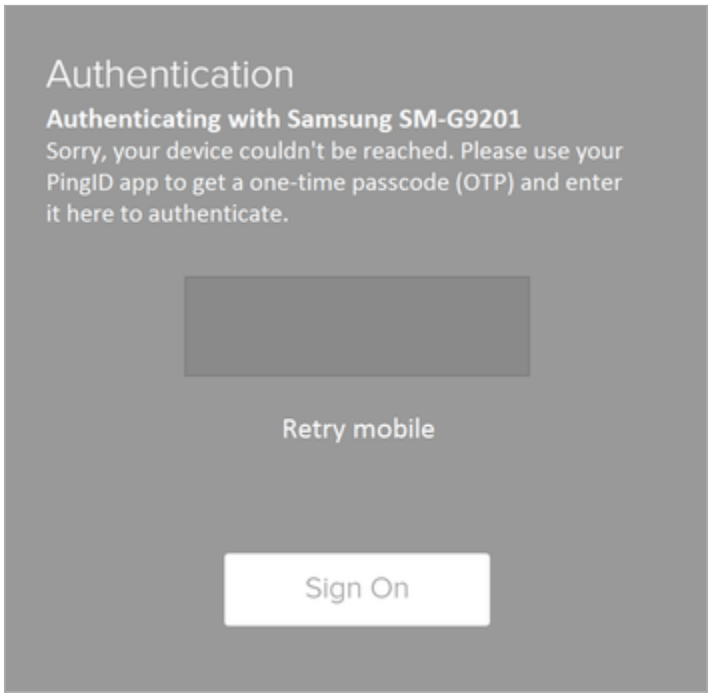
If the user's mobile is in no push mode, the user will receive the following error message.



To configure push mode, go to **Settings → Swipe Settings → Enable Swipe → Off** in the PingID mobile app.

> **Caution**
>
> Users with mobile devices that do not support push notifications will not be able to authenticate if the **Disable** setting is selected.

- To enable authenticating with an OTP when the mobile app response times out, click **Enable**. This is the default setting. If the request times out, the user can authenticate using an OTP.



3. Click **Save**.

Configuring direct passcode usage

Direct passcode usage allows users authenticate with a one-time passcode (OTP) immediately, without waiting for a push notification to arrive or to timeout.

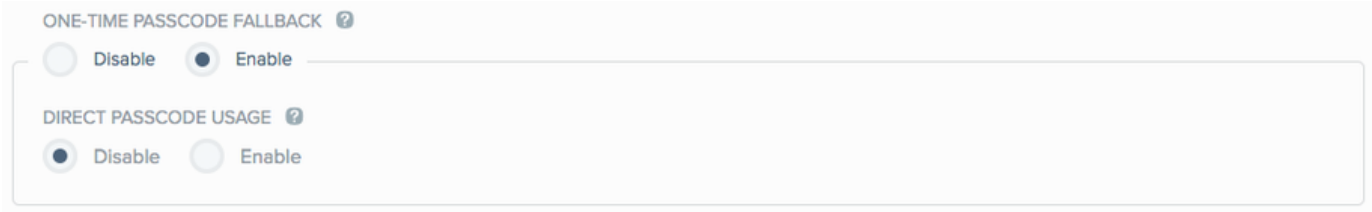
About this task

If direct passcode usage is enabled, users awaiting a push notification will see a **Use Code** button in their web browser, allowing them to bypass the push notification and authenticate directly with an OTP. This is a convenient option for users without a strong network connection.

> **Note**
>
> If you are using PingOne DaVinci to orchestrate your PingID flows and want to disable the Direct Passcode Usage feature, you must disable it in the flow settings node in DaVinci, and in the Admin portal.

Steps

1. In the admin console, go to **Setup → PingID → Configuration**.
2. In the **One-Time Passcode Fallback** section of the **Authentication** section, click **Enable**.



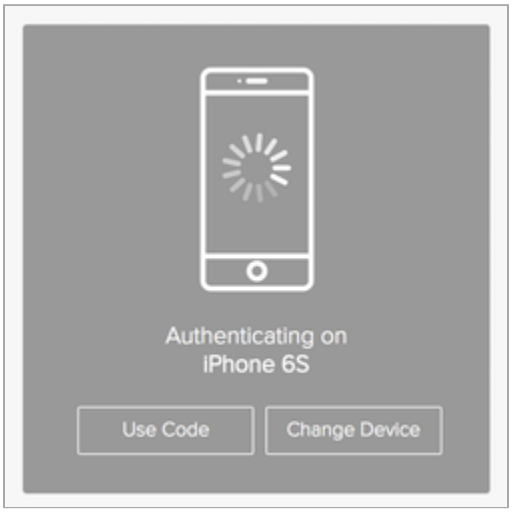
   Result:

   The **Direct Passcode Usage** section displays.

3. In the **Direct Passcode Usage** section, click **Enable**.
4. Click **Save**.

Result

When a user authenticates through the web, they can click **Use Code** and enter the OTP that appears on the PingID mobile app, rather than waiting for a push notification to arrive or timeout. For more information, see Authenticating using a one-time passcode.



> **Note**
>
> If a user clicks **Use Code**, they can still authenticate using a push notification if it arrives before the user completes authentication using the OTP.

Configuring the PingID mobile app PIN

As an extra layer of security, you can require users to enter a 4- or 6-digit PIN code to access the PingID mobile app.

About this task

You can require a PIN code to access PingID mobile app for:

- Devices that don't already have device biometrics or a device PIN code defined
- All devices

If this option is enabled:

- A user is prompted to create a PIN code when they pair the mobile app. The PIN code must include at least 3 or 4 different digits for PIN lengths of 4 and 6 digits, respectively. Digits must not be in ascending or descending sequence, such as 1234 or 4321.
- A user is prompted to enter the PIN code each time they launch the PingID app.
- The mobile app is locked after 3 minutes of inactivity, and the user is required to enter the PIN to unlock it.
- In the event of 3 consecutive incorrect PIN entries, the user is blocked from accessing the app for 2 minutes. This applies to both the PIN entry and the PIN change windows. Lockdown takes effect from the time of the lock, irrespective of whether the desktop app remains open or is closed and relaunched.
- The mobile app must be online for a user to pair the app. However, a user who is offline can still create a PIN, enter the PIN to access the mobile app, or change their PIN.
- The mobile app must be online for any change in PIN configuration to take effect, such as enabling or disabling the PIN or changing its length. The user can change their PIN from the PingID mobile app settings.

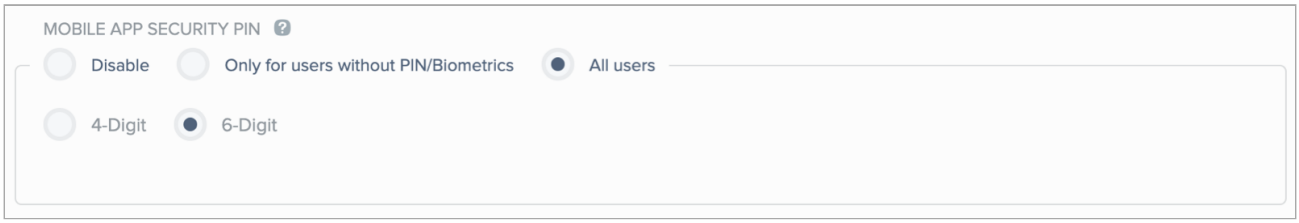
- If a user pairs the mobile app to more than one organization, the user must create only one PIN, according to the most restrictive organization requirements. For example:
  - If only one organization has enabled the **Mobile Security PIN** feature, the user is required to enter their PIN to use the mobile app for authentication to all organizations, including those which do not require the PIN.
  - If one organization requires a **4-Digit** PIN and a second organization requires a **6-Digit**, the user will be required to enter a 6-digit PIN.
- If the PIN code is already enabled, and the administrator changes the length of the PIN code required, users must first enter the app using the old PIN and then create a new PIN of the new length.
- It is not possible for the user to reset their PIN. If forgotten, to create a new PIN, the user must unpair their device, and then define their PIN code when pairing their device again.

Steps

1. In the admin portal, go to **Setup → PingID → Device & Pairing**.
2. In the **Pairing Conditions** section, under **Mobile App Security PIN**, select one of the following:

   Choose from:

   - **Only for users without device PIN/Biometrics**: Only users without device PIN or biometrics are required to enter a PIN to use PingID mobile app.
   - **All users**: All users must enter a PIN code to use PingID mobile app.
   - **Disable**: Do not require a PIN code to use PingID mobile app.

3. Select either **4-Digit** or **6-Digit** to indicate the PIN length. Click **Save**.

Result

If an administrator edits the PingID mobile app configuration to require a PIN code, changes are implemented at the user level according to the PingID version and the user flow:

- Users installing the PingID mobile app for the first time are prompted to create a PIN during the mobile app pairing flow.
- Users with the PingID mobile app 1.31 or later already paired are prompted to define a PIN code the next time the user opens the PingID mobile app while online.
- Users with the PingID mobile app earlier than 1.31 already paired must update the PingID mobile app for the changes to take effect. The user is prompted to define a PIN code the next time they launch the new version of the mobile app.

Enabling PingID mobile app update notifications

You can choose to notify users when a new version of PingID mobile app is available. You can make it mandatory, optional, or dependent on the version that they already have installed.

About this task

If you enable updates, you can choose which type of update notifications you require per OS (iOS or Android). Choose from:

- **Required updates**: Notify the user when a new version is available. The user must update to the new version to continue using PingID mobile app. The user cannot skip the update and will not be able to authenticate with PingID until they update to the latest version.

  > **Note**
  >
  > A 7-day grace period is implemented from the time that you save this configuration, to allow enough time for the new version to be added to the relevant app stores before users are notified of the requirement to upgrade to the latest version.

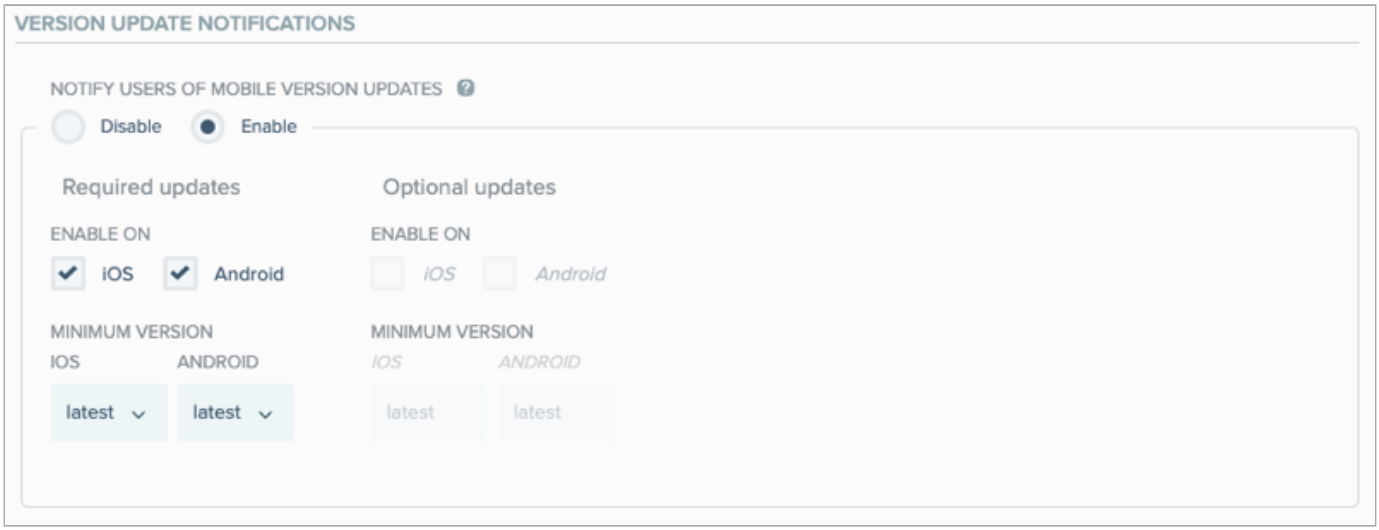
- **Optional updates**: Notify the user when a new version is available. The notification includes the option to skip the update and install it at a later date.

Steps

1. In the admin portal, go to **Setup → PingID → Device & Pairing**.
2. To enable notifications when a new version of the mobile app is available, in the **Version Update Notifications** section, under**Notify Users of Mobile Version Updates,** select **Enable**.

   Result:

   You'll see options to enable notification of updates for iOS or Android that either require the user to update or inform the user of the option to update to the latest version.



3. For each OS (iOS or Android):
   1. Select the relevant check box to specify whether updating to the latest version is optional or required.
   2. Specify the **Minimum Version** from which update notifications should be sent.
   3. Click **Save**.

Configuring OTP push notifications

You can configure PingID to send a push notification to your users and automatically open PingID mobile app on their device, when requesting a one time passcode.

About this task

When this option is enabled, if a user starts a flow that requires them to enter an OTP, the user no longer has to open their app and search for an OTP. PingID sends a push notification to the user's device. When the user taps the notification, PingID mobile app opens automatically and generates a new OTP.

Steps

1. In the admin console, go to **Setup → PingID → Configuration**.
2. In the **Mobile App Authentication** section, in the **OTP Push Notifications** field, click **Enable**.

3. Click **Save**.

Configuring number matching authentication

Number matching allows the user to authenticate by matching the number displayed on the user's accessing device with the corresponding number in PingID mobile app.

About this task

Configure number matching as an allowed authentication method in PingID policy, and optionally as an authentication action within a policy rule.

For information, see Policy and rule authentication methods.

For the user experience, see Configuring number matching authentication.

> **Note**
>
> - Number matching requires PingID mobile app 1.34 or later.
> - If **Mobile app biometrics** is set to **Require** in the **Configuration** tab, the user must authenticate successfully using biometrics and then authenticate using number matching.

Displaying details of accessing device

When an authentication request is sent to a mobile device, you can have it include details of the accessing device, such as a map showing its location.

> **Note**
>
> This feature determines the location of the accessing device using its IP address and only supports IPv4. As a result, the location shown on the map might be less accurate compared to other location-detection methods.

About this task

Use the **Show Authentication Information** setting to disable/enable this option.

Steps

1. In the PingID admin portal, go to **Setup → PingID → PingID Settings → Configuration**.
2. In the **Mobile App Authentication** section, set **Show Authentication Information** to Disabled or Enabled.

Configuring authentication when the device is locked

Configure the **Authentication While Device Is Locked** setting to enable or disable users using swipe to authenticate with PingID without unlocking their devices. The default setting is **Enable**.

About this task

> **Note**
>
> This configuration is supported on the mobile app 1.7 and later and is only relevant for swipe authentication on devices running Android versions later than Android Q.

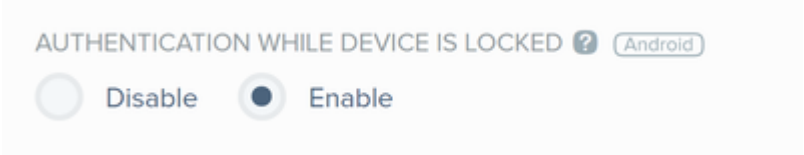
For details about the user experience for authenticating with an Android device, see the PingIDEnd User Guide.

Steps

1. In the admin console, go to **Setup → PingID → Configuration**.
2. In the **Authentication While Device Is Locked** section of the **Mobile App Authentication** section, click one of the following:

   Choose from:

   - **Disable**: Users must unlock their device before authenticating.
   - **Enable**: Users can authenticate without first unlocking their mobile device.



3. Click **Save**.

Enabling or disabling location collection

The PingID mobile app can collect user location information to provide valuable contextual information for use in current and future risk-based policies and data analytics.

About this task

Location collection is defined per organization and is not enabled by default. Location is only collected when a policy that requires it is configured. If enabled, when installing the PingID mobile app, end users are prompted to allow the PingID mobile app the relevant permissions to collect location information. Users can disable location collection by the PingID app in their mobile device settings.

Location-based policies already defined in your system might deny users access during authentication. We recommend that you enable location collection for all organizations to enable you to apply location-based policy rules and to allow for behavioral analysis in the future.

When changing location collection configuration at the organization level:

- Changes will apply to the end user's mobile device the next time the end user authenticates online.
- If a mobile device is paired with more than one organization, changing location services for one organization level affects all organizations with which the device is paired.

Steps

- If you are enabling location collection for an organization:
  - Configure a policy that requires location collection. For more information, see PingID policy settings.
- If you are disabling location collection for an organization:
  - When pairing a device with the PingID mobile app, users are not prompted to allow location collection when pairing a new device.

    > **Note**
    >
    > Although location collection remains enabled, if location collection is disabled at the organization level, PingID will not collect location information from the user's device.

  - If the user has the PingID mobile app installed and has granted permission to location collection, the collection of location information will stop the next time the user authenticates online. The user is not prompted to authorize this change and location is not collected, regardless of whether location collection settings for PingID are allowed or denied.
- If you are re-enabling location collection for an organization:
  - When installing the PingID mobile app on a device and pairing, users are prompted to allow location collection permissions when pairing the device with the organization.

    > **Note**
    >
    > Android users running Android Q and later must select **Allow all the time**.

  - If the user already has PingID installed and did not grant permission to location collection in the past, their device will prompt them to grant permission the next time they open the PingID app.

> **Important**
>
> A user authenticating through the lock screen is not prompted to allow location permissions, and location collection is not enabled. To approve location permissions, the user must unlock their device and open the PingID app. After the user approves location collection, PingID collects location information.

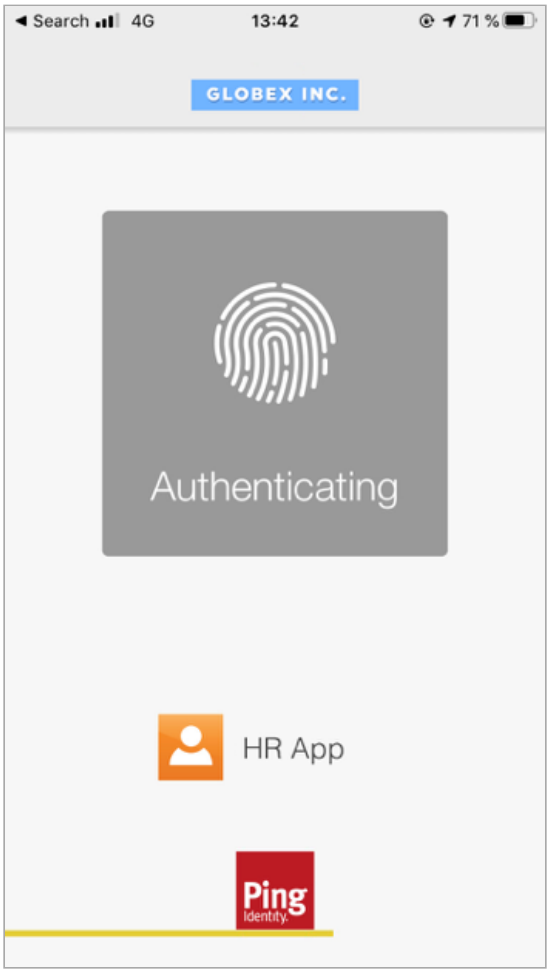
If a user is paired with a different organization that has not enabled location collection, location information will not be collected.

Defining the authenticating app appearance in the PingID mobile app

Configure the PingID mobile app authentication screen to display the name and icon of the app originating the push notification authentication request.

About this task

The following image shows a custom authentication screen in the PingID mobile app.



Steps

1. In the relevant identity provider (IdP), define the name and icon that PingID displays on the authentication screen.

Application IdP	Steps
PingOne Apps	Define the app name in the **Application Name** field and the icon in the **Graphics** field. For more information, see: ◦ Add or update a SAML-enabled application ◦ Add or update an OIDC application
PingFederate Apps	Define the app name in the **Application Name** field and the icon in the **Application Icon URL** field. For more information, see: ◦ Managing SP connections ◦ Identifying the SP. See the Application Name and Application Icon URL entries.
PingID API Apps	The app name and logo are defined using either: ◦ The `appName` and `appIconUrl` sub-attributes. For more information, see Example PPM request. ◦ The `sp_logo` and `sp_name` of the StartAuthentication API. For more information, see the AuthenticateOnline entry.

PingID desktop app authentication

The PingID desktop app is a one-time passcode (OTP) generator and can be installed on a PC or Mac. The PingID desktop app works similarly to the PingID mobile app's OTP generator.

The PingID desktop app supports an option to secure the OTP window with either a 4-digit or 6-digit PIN code. This elevates the security level by preventing unauthorized users from accessing the PingID OTP on an unlocked workstation.

The PingID desktop app is available for the following platforms and versions:

- Microsoft Windows 10 and 11
- Microsoft Windows Server 2016 and 2019
- Apple Mac OS X 11+

The PingID desktop app does not run on an Apple Mac OSX virtual machine (VM).

> **Note**
>
> The PingID desktop app requires a minimum of 155 MB RAM and 212 MB free disc space.

An end user can authenticate in both online and offline modes with the PingID desktop app OTP generator. Users can only pair devices in online mode. The desktop app must be online for a change in PIN configuration to take effect, such as enabling or disabling the PIN or changing its length.

For information about the user experience, see PingID End User Guide.

> **Note**
>
> - Different end users using the same PC have different PingID accounts and undergo a unique authentication process. Each end user only sees their own organizations.
> - When a user is registered to two different organizations, each organization's administrators can only see the details of their own organization's end users.
> - Roaming user profiles:
>   - Roaming user profiles are available from version 1.5.3 for the Windows desktop app.
>   - To enable roaming user profiles, users must be unpaired and any previous installation of the desktop app must be uninstalled.
>   - All terminals available for roaming users must have the desktop app installed with user roaming profiles support enabled.

Configuring the PingID desktop app

Enable and configure the PingID desktop app so that your users can install and authenticate.

About this task

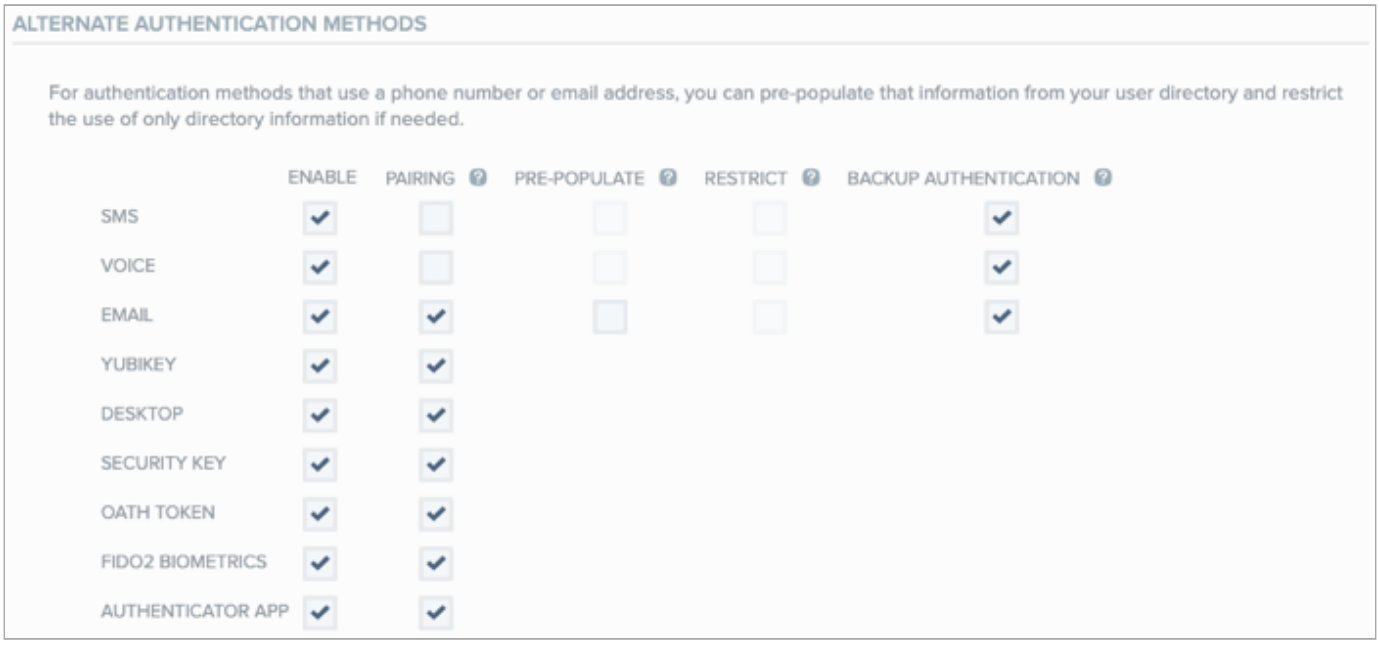
You can optionally:

- Require users to enter a 4 or 6-digit PIN code to access the PingID desktop app. For more information, see Configuring the PingID desktop app PIN.
- Disable automatic updates. When you enable the PingID desktop app, automatic software updates are enabled by default. To disable automatic updates, see Enabling or disabling PingID desktop app automatic updates.

- Configure the PingID proxy for the desktop app, and enable or disable PingID proxy for end users. You can allow PingID desktop app to work with a proxy using a self-signed certificate, or local CA-signed certificate. You can also give users the option to temporarily disable their proxy. For more information, see Configuring PingID Proxy for the PingID desktop app.
- Install the desktop app using the Windows CLI. For more information, see Installing the desktop app using the Windows CLI.

Steps

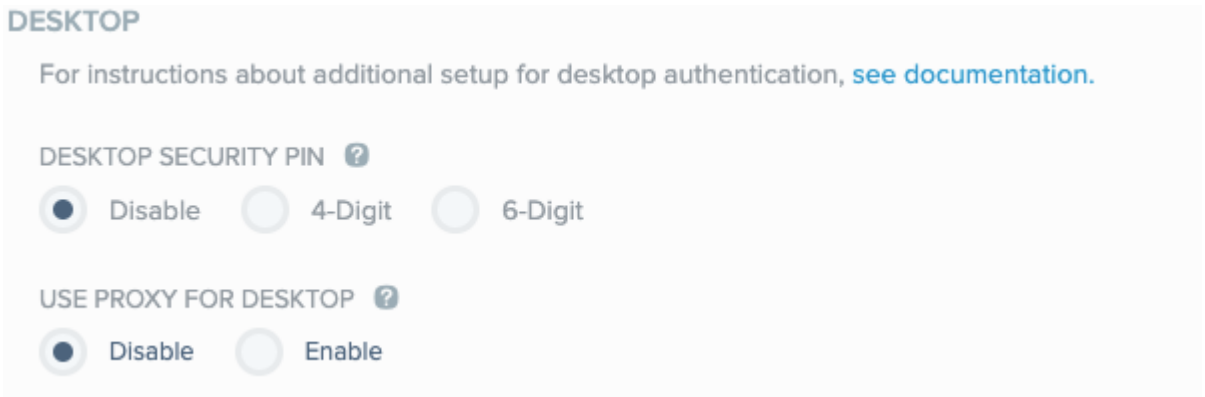
1. In the PingID admin portal, go to **Setup → PingID → Configuration**.
2. Go to the **Authentication → Alternate Authentication Methods** section.



3. In the **Desktop** row, select the **Enable** check box. The **Pairing** check box is selected automatically.

   Result:

   The ability to pair and authenticate with PingID desktop is enabled for all users in that organization, and the **Desktop Security PIN** field is displayed.



4. **Optional:** To require users to enter a PIN code when accessing the desktop app, from the **Desktop Security PIN** section, select one of the following options:

Choose from:

- **4-Digit**: Require the user to enter a 4-Digit code in order to access the desktop app.
- **6-Digit**: Require the user to enter a 6-Digit code in order to access the desktop app.
- **Disable**: The user is not prompted to enter a PIN code when launching the desktop app. This is the default setting.

> **Note**
>
> For more information, see Configuring the PingID desktop app PIN.

5. **Optional:** Configure the PingID proxy for the desktop app. For more information, see Configuring PingID Proxy for the PingID desktop app.
6. Click **Save**.

Configuring the PingID desktop app PIN

As an extra layer of security, you have the option to require users to enter a 4 or 6-digit PIN code to access the PingID desktop app.

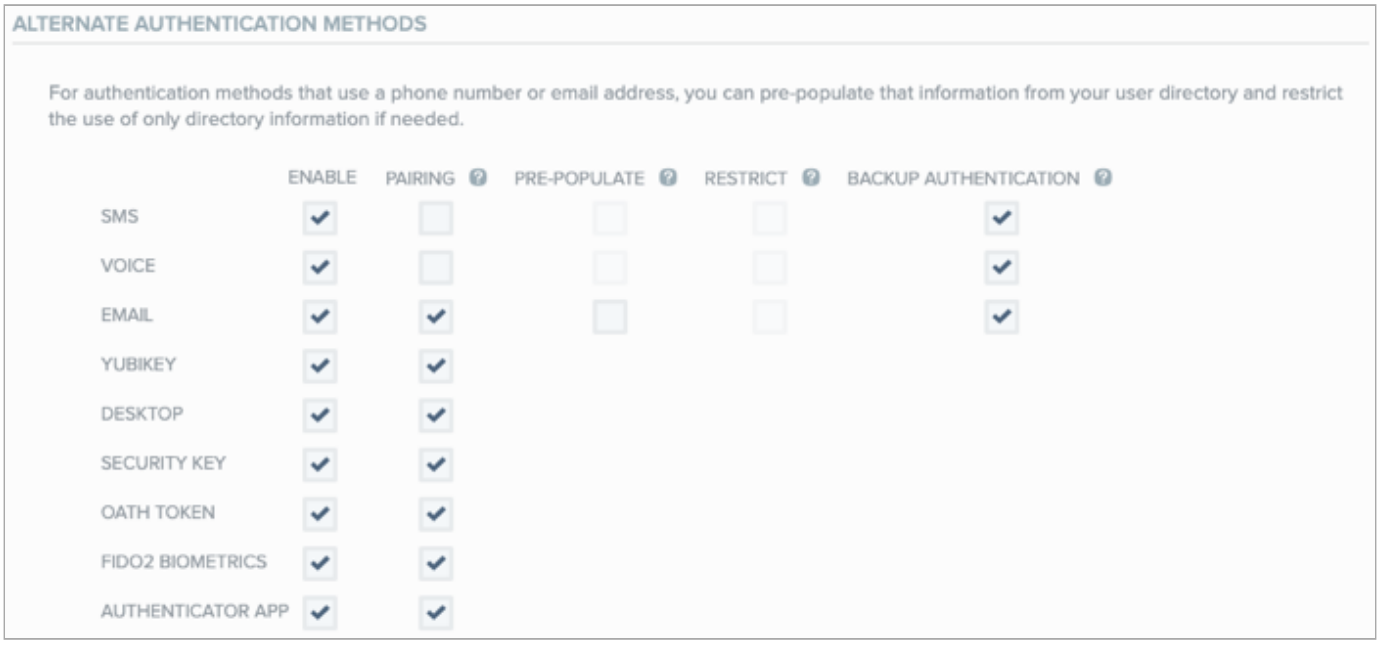
About this task

If this option is enabled:

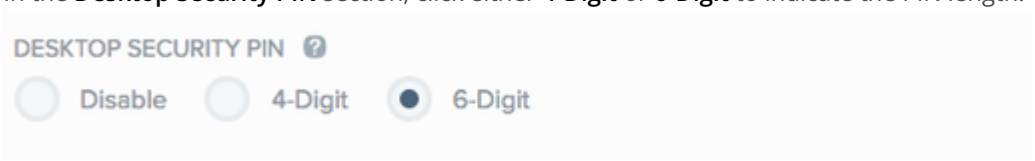
- A user is prompted to create a PIN code when they pair the desktop app. The PIN code must include at least 3 or 4 different digits for PIN lengths of 4 and 6 digits, respectively. Digits must not be in ascending or descending sequence, such as 1234.
- A user is prompted to enter the PIN code each time they launch the PingID app.
- The desktop app is locked after 3 minutes of inactivity, and the user is required to enter the PIN to unlock it.
- In the event of 3 consecutive incorrect PIN entries, the user is blocked from accessing the app for 2 minutes. This applies to both the PIN entry and the PIN change windows. Lockdown takes effect from the time of the lock, irrespective of whether the desktop app remains open or is closed and relaunched.
- The desktop app must be online for a user to pair the app. However, a user who is offline can still create a PIN, enter the PIN to access the desktop app, or change their PIN.
- The desktop app must be online for a change in PIN configuration to take effect, such as enabling or disabling the PIN or changing its length.
- If a user pairs the desktop app to more than one organization, the user must create only one PIN, according to the most restrictive organization requirements. For example:
  - If only one organization has enabled the **Desktop Security PIN** feature, the user is required to enter their PIN to use the desktop app for authentication to all organizations, including those which do not require the PIN.
  - If one organization requires a **4-Digit** PIN and a second organization requires a **6-Digit**, the user will be required to enter a 6- digit PIN.
- If the PIN code is already enabled, and the administrator changes the length of the PIN code required, users must first enter the app using the old PIN and then create a new PIN of the new length.

Steps

1. In the admin portal, go to **Setup → PingID → Configuration**.
2. Go to the **Alternate Authentication Methods** section and in the **Desktop** row, select **Enable**.



3. In the **Desktop Security PIN** section, click either **4-Digit** or **6-Digit** to indicate the PIN length. Click **Save**.



Result

If an administrator edits the PingID desktop configuration to require a PIN code, changes are implemented at the user level according to the PingID version and the user flow.

- Users installing the PingID desktop app for the first time are prompted to create a PIN at the end of the desktop app pairing flow.
- Users with the PingID desktop app 1.4 or later already paired are prompted to define a PIN code the next time the user opens the PingID desktop app while online.
- Users with the PingID desktop app earlier than 1.4 already paired must update the PingID desktop app for the changes to take effect. The user is prompted to define a PIN code the next time they launch the new version of the desktop app.

Resetting a user's desktop app PIN

About this task

For users running PingID desktop app 1.74 or later, it is not possible for them to reset their own PIN. To help a user create a new PIN, do the following:

Steps

1. Ask the user to uninstall the desktop app from their local machine.
2. Unpair the user's device from the PingID service. For more information, see Unpairing a user's device from the PingID service

   Result:

   The user's desktop app service is unpaired.
3. The user should install and pair the desktop app again and create a new PIN code. For more information, see Setting up PingID desktop app.

Enabling or disabling PingID desktop app automatic updates

PingID:resourceid: pingid_desktop_app_auto_updates

Configure the PingID desktop app to check for software updates automatically. This feature is enabled by default.

About this task

You can enable or disable automatic updates manually, or create a script. The process varies between Mac, Windows desktop app 1.5 and later, and Windows desktop app 1.4 and earlier.

- If the `autoupdatemode` parameter has any value other than `disable`, or has not been defined, then `autoupdatemode` assumes the value of `enable` on that PC or Mac.
- The desktop app references the `autoupdatemode` parameter at startup. If the `autoupdatemode` value is changed, the change is only reflected the next time the desktop app is started.
- The `autoupdatemode` parameter is configured at machine level. If there are multiple instances of the desktop app installed on a machine, the setting of the `autoupdatemode` is applied to all instances.

> **Note**
>
> For sample scripts for each PingID desktop app version, see the Ping Identity GitHub. All scripts require administrator privileges to run them.

Steps

1. To enable or disable automatic updates:

   Choose from:

   - Mac:

     1. Create a new preferences file: `/Library/Preferences/com.pingidentity.pingid.plist`.
     2. In the `/Library/Preferences/com.pingidentity.pingid.plist` preferences file, create a key and name it `autoupdatemode`, with the value `enable` or `disable`.
     3. Convert the `/Library/Preferences/com.pingidentity.pingid.plist` file to binary.

        ```
        plutil -convert binary1 /Library/Preferences/com.pingidentity.pingid.plist
        ```

4. From the preferences file, load the `autoupdatemode` parameter (`enable` or `disable`) as its active setting.

```
defaults import  /Library/Preferences/com.pingidentity.pingid.plist/Library/
Preferences
com.pingidentity.pingidplist
```

- Windows with desktop app 1.5 and later:

1. Open the `props.fileprefs` file.
   - 32-bit: `\Program Files (x86)\Ping Identity\PingID\app\props.fileprefs`
   - 64 bit: `C:\Program Files\Ping Identity\PingID\app\props.fileprefs`
2. Add the following code to the `props.fileprefs` file.
   - To enable automatic updates:

```
com.pingidentity.pingid.pctoken.PRODUCTION.autoupdatemode=enable
```

   - To disable automatic updates:

```
com.pingidentity.pingid.pctoken.PRODUCTION.autoupdatemode=disable
```

3. Save and then close the file.

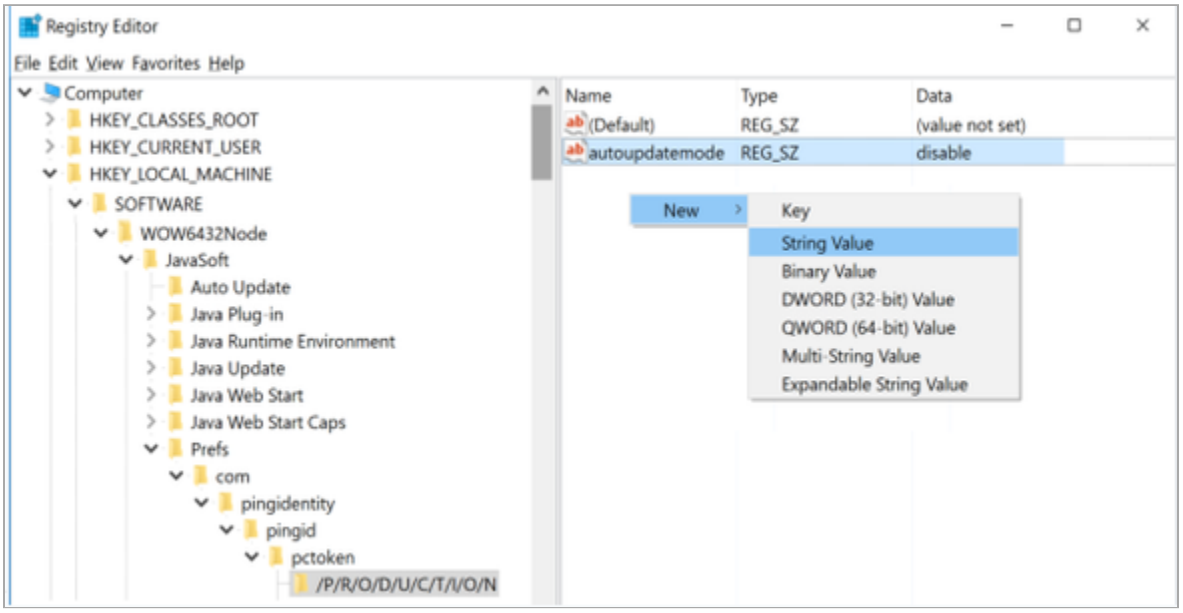
- Windows with desktop app 1.4 and earlier:

1. In the Windows registry, create the `autoupdatemode` parameter as a `String Value`.
   - 32-bit:

```
HKEY_LOCAL_MACHINE\SOFTWARE\JavaSoft\Prefs\com\pingidentity\pingid
\pctoken\/P/R/O/D/U/C/T/I/O/N\autoupdatemode
```

   - 64-bit:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\JavaSoft\Prefs\com\
\pingidentity\pingid\pctoken\/P/R/O/D/U/C/T/I/O/N\autoupdatemode
```



Configuring PingID Proxy for the PingID desktop app

Configure the PingID desktop app to support proxy for all enterprise internal communication to the internet on enterprise desktop and laptop machines.

Before you begin

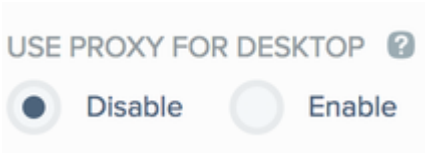
To obtain the latest version of the `SetProxyParams` script, see https://github.com/pingidentity/pingid-desktop-application.

Steps

1. In the PingID admin portal, go to **Setup → PingID → Configuration**.
2. In the **Use Proxy For Desktop** field, select one of the following options, and then click **Save**.

   Choose from:

   - **Enable**: Enable the use of PingID desktop app with the enterprise proxy, according to the mode configured in the `SetProxyParams` script.
   - **Disable**: Disable use of PingID desktop app with a proxy. This is the default selection.

   > **Note**
   >
   > Even if the **Use Proxy For Desktop** setting is enabled enterprise-wide in the admin portal, administrators can require the desktop app installations on specific desktops and laptops to always work without a proxy.

3. If **Use Proxy For Desktop** is set to **Enable**, modify the `SetProxyParams` script.

> **Note**
>
> The `SetProxyParams` script is configured at machine level. If there are multiple instances of the desktop app installed on a machine, the setting of the `SetProxyParams` is applied to all instances.

Choose from:

- Restrictive mode: Forces users to use the desktop app with the enterprise proxy. The proxy toggle does not appear on the desktop app menu.
  - Windows:

    ```
    SetProxyParams.bat host port [username] [password] -r
    ```

  - Mac:

    ```
    sudo sh SetProxyParams.sh host port [username] [password] -r
    ```

- Permissive mode: Provides users an option to enable or disable use of the proxy from the desktop app menu, to accommodate authentication in different work modes, from within the enterprise network, or externally. For more information, see Enabling or disabling your proxy for PingIDdesktop.
  - Windows:

    ```
    SetProxyParams.bat host port [username] [password]
    ```

  - Mac:

    ```
    sudo sh SetProxyParams.sh host port [username] [password]
    ```

- Disabled mode: Disables use of the desktop app with a proxy on specific devices.
  - Windows:

    ```
    SetProxyParams.bat disable
    ```

  - Mac:

    ```
    sudo sh SetProxyParams.sh disable
    ```

    Where:

Parameter	Description
`host`	Proxy host IP address or host name.

Parameter	Description
`port`	Proxy port number.
`username`	Mandatory if the proxy requires credentials. Empty if the proxy does not require credentials.
`password`	Mandatory if the proxy requires credentials. Empty if the proxy does not require credentials.
`-r`	Mandatory for restrictive mode. Empty for permissive mode.

> **Note**
>
> To configure Proxy Auto Configuration (PAC) for the desktop app, see Configuring Proxy Auto Configuration for the PingID desktop app.
> To configure Kerberos proxy authentication for the desktop app, see Configuring Kerberos proxy authentication for the PingID desktop app.

4. **Optional:** To allow the PingID desktop app to work with a proxy, using a self-signed certificate or local CA-signed certificate, complete the following steps:

    1. Ensure that the Java Development Kit (JDK) `keytool` utility is installed.
    2. Download a copy of the certificate that is installed on the proxy in DER format, and then save it to the local hard drive.
    3. Open the integrated terminal and navigate to the Java Runtime Environment (JRE) security directory inside the PingID root directory.

    The default paths are:

    - Windows: `C:\Program Files (x86)\Ping Identity\PingID\runtime\lib\security`
    - Mac: `/Applications/PingID.app/Contents/PlugIns/Java.runtime/Contents/Home/jre/lib/security`

        1. Add the certificate to the JRE certificate trust store.

            ```
            keytool -import -keystore cacerts -file <certificate file> -storepass changeit
            ```

Configuring Proxy Auto Configuration for the PingID desktop app

Proxy Auto Configuration (PAC) enables you to manage networks that have multiple proxies, so that you can configure different proxy servers for different URLs, and replace proxies dynamically by editing and updating the PAC file.

Steps

1. On the relevant user's machine, configure the PAC URL:

Choose from:

- Windows:
    1. Open the Internet Explorer configuration window and click the **Network** tab.
    2. In the **Use Automatic Configuration Script** field, enter the URL of the PAC file you want to use. Click **OK**.
- Mac:
    1. Go to **System Preferences → Network**, click **Advanced**, and then go to the **Proxies** tab.
    2. Select the **Automatic Proxy Configuration** check box.
    3. In the Proxy Configuration File **URL** field, enter the URL of the PAC file that you want to use. Click **OK**.

2. On the relevant user's machine, configure the PingID desktop app to work with PAC according to your operating system.

   Choose from:

   - Windows 32-bit: From the command line, enter `"C:\Program Files\Ping Identity\PingID\ProxyHelperSetup.exe" -pac`.
   - Windows 64-bit: From the command line, enter `"C:\Program Files(x86)\Ping Identity\PingID\ProxyHelperSetup.exe" -pac`.
   - Mac: In a terminal window, enter `sudo /Applications/PingID.app/Contents/MacOS/ProxyHelperSetup -pac`, and then enter the admin password when prompted.

3. Test the communication with the proxy server.
    1. Pair the PingID desktop app.
    2. Open the PingID log file.

       Result:

       If the PingID desktop app can communicate with PingID cloud server, the `Proxy configuration is PAC` entry appears during application startup. If there is no communication, indicated by an `unknown error` message when pairing the PingID desktop app, either the proxy is not working correctly, or there is a configuration problem.

Configuring Kerberos proxy authentication for the PingID desktop app

The PingID app supports proxy authentication using the Kerberos protocol, delegating the machine credentials for authentication to the organizational proxy.

Before you begin

> **Important**
>
> Install the PingID desktop app 1.5.2 or later.

About this task

The PingID desktop app supports proxy authentication using the Kerberos protocol, delegating the machine credentials for authentication to the organizational proxy. The HTTP client uses Simple and Protected GSSAPI Negotiation Mechanism (SPNEGO) to negotiate the authentication method.

When Kerberos is the agreed protocol, the client uses a ticket generated by the Key Distribution Center (KDC) for the proxy authentication that can be used multiple times. The Kerberos ticket expiry period might vary according to the KDC configuration.

Steps

1. Ensure that a Kerberos token is initialized on the user's operating system.
    1. From the command line or terminal window, run `klist` to verify that a valid Kerberos token is available.
2. From the command line or terminal window, enter the following command:

    Choose from:

    - Windows:

    ```
    "C:\Program Files(x86)\Ping Identity\PingID\ProxyHelperSetup.exe"
    <host> <port> -kerberos
    ```

    - Mac:

    ```
    sudo /Applications/PingID.app/Contents/MacOS/ProxyHelperSetup
    <host> <port> -kerberos
    ```

3. From the command line or terminal window, enter the following command to test Proxy Auto Configuration (PAC) with Kerberos:

    Choose from:

    - Windows:

    ```
    "C:\Program Files(x86)\Ping Identity\PingID\ProxyHelperSetup.exe"
    -pac -kerberos
    ```

    - Mac:

    ```
    sudo /Applications/PingID.app/Contents/MacOS/ProxyHelperSetup -pac -kerberos
    ```

Installing the PingID desktop app (Admin)

Install the PingID desktop app using the command-line interface (CLI) or the UI wizard.

- To install on Windows:
    - To use the UI wizard, see Setting up PingID desktop authentication on Windows.
    - To use the CLI, see Installing the desktop app using the Windows CLI.

- To install on Mac:
  - To use the UI wizard, see Setting up PingID desktop app on a Mac.
  - To use the CLI, see Installing the desktop app using the Mac CLI.

Installing the desktop app using the Windows CLI

Install the PingID desktop app using the command-line interface (CLI). This is useful for deploying on multiple machines in batch mode.

About this task

> **Note**
>
> Running the installer from the command line requires administrator permissions.

Steps

1. Download the PingID desktop app installer from the PingID desktop download page.
2. Open a Command Prompt window with administrator permissions.
3. Create a `.bat` or `.cmd` file containing the following commands for the PingID desktop app, or run the installer directly from the command line, to supply the parameter values. `<full filepath of the PingID desktop installation>\PingID-<version>.exe [/SILENT][/VERYSILENT] [/TASKS="roaminguserprofiles"] [/SUPPRESSMSGBOXES] [/SP-] <full output log filepath>][/DIR<full_dirpath>]`

   The following table describes each parameter value.

Parameter	Description
`/SILENT` or `/VERYSILENT`	The background window and installation progress window are displayed by default. To hide them, include one of the following parameters. **`/SILENT`** Hides the background window and shows the installation process window. **`/VERYSILENT`** Hides the background window and the installation process window.

Parameter	Description
`/TASKS= "roaminguserprofiles"`	To add support for roaming user profiles, append this parameter. Available for version 1.5.3 and later. There are several conditions to its use. When the parameter is not used in a fresh installation: ◦ When using the `/SILENT` or `/VERYSILENT` parameters, the UI is not shown and the roaming profile setting is unavailable. ◦ Otherwise, the roaming profile setting is shown in the UI unchecked, and can be changed by the user. When the parameter is used in a fresh installation: ◦ In SILENT or VERYSILENT mode, the UI is not shown and roaming profile is used. ◦ Otherwise, the roaming profile setting is shown in the UI as checked, and can be changed by the user. For an upgrade from a previous version or reinstall of the same version: ◦ This CLI setting is ignored. ◦ In SILENT or VERYSILENT mode, the UI is not shown. The previous installation setup is maintained. ◦ Otherwise, the UI will be shown but the roaming profile check box will be not be shown.
`/SP-`	Disables the prompt `"This will install… Do you wish to continue?"` that appears by default when the installation starts.
`/SUPPRESSMSGBOXES`	Instructs the installer to suppress message boxes. It only has an effect when combined with `/SILENT` or `/VERYSILENT`. The default response in situations where there's a choice is: ◦ `Yes` in `Keep newer file?` situations. ◦ `No` in `File exists, confirm overwrite` situations. ◦ `Abort` in <full output log filepath> `Abort/Retry` situations. ◦ `Cancel` in `Retry/Cancel` situations. ◦ `Yes` (continue) in `DiskSpaceWarning, DirExists, DirDoesntExist, NoUninstallWarning, ExitSetupMessage,` and `ConfirmUninstall` situations. ◦ `Yes` (restart) in `FinishedRestartMessage` and `UninstalledAndNeedsRestart` situations.
`/LOG= ```	◦ `/LOG` < without an assigned value will create a log file in the user's TEMP directory, detailing file installation and actions taken during the installation process. ◦ / `LOG=<full output log filepath>` allows you to specify a fixed path or filename to use for the log file. If a file with the specified name already exists, it will be overwritten. If the file cannot be created, the installer will abort with an error message.
`/DIR=` <full_dirpath>	Defines the path to which you want to install the app. A fully qualified pathname must be specified in the format `x:\directorypath`. If no path is defined, the default path is used.

Example: **`C:\Users\Admin\Downloads\PingID-1.5.0.exe /VERYSILENT /SUPPRESSMSGBOXES /SP- /LOG="C:\Users\Admin\Temp\Logs\PingIDDesktopAppLog.log"`**

This example instructs the installer to install the PingID desktop app, with the following settings:

◦ Runs the installer executable, located in the Downloads folder.

◦ Does not display the background window and installation progress window (`/VERYSILENT` parameter).

- Does not display message boxes and prompts (`/SUPPRESSMSGBOXES` and `/SP-` parameters).
- Sends the log output to a customized destination (`/LOG` parameter).

4. To verify the installation, test that a user can open the desktop app instance on their Windows machine and pair their device.

   For more information, see Setting up PingID desktop authentication on Windows.

Installing the desktop app using the Mac CLI

Install the PingID desktop app using the command line. This is useful for deploying on multiple machines in batch mode.

About this task

> **Note**
>
> Running the installer from a Terminal window requires administrator permissions.

Steps

1. Download the installer for the PingID desktop app from the PingID desktop download page.
2. Open a Terminal window and enter the following command. `sudo installer -pkg <installer package filepath> -target <installation destination filepath> /`
   - *<installer package filepath>* is the downloaded installer package's full filepath.
   - *<installation destination filepath>* is the full filepath location that will host the PingID desktop app installation with its initial configuration.

     Example:[.codeph]``sudo installer -pkg $HOME/Downloads/PingID.pkg -target /Applications /
     ``

   This command uses the PingID desktop app installer package downloaded to the default Downloads directory and installs it in the Applications directory.
3. When prompted, enter the administrator password.

Result

The PingID desktop app is silently installed, using the application defaults. A message displays indicating the installation is successful.

Troubleshoot the PingID desktop app

The PingID desktop app does not open

If the PingID desktop app does not open:

1. Check for a running instance of the PingID desktop app and terminate it.
   - Windows: Go to **Task Manager → Processes**, locate the PingID process, and click **End Task**.
   - Mac: Go to **Apple Menu → Force Quit Applications**.

2. Restart the PingID desktop app.

The PingID desktop app one-time passcode (OTP) is rejected by the authentication screen

If the OTP generated by the PingID desktop app is rejected by the authentication screen:

1. In the PingID desktop app, click **Refresh**.
2. Copy the new OTP to the clipboard.
3. Go to the authentication page in the browser and paste the new OTP, or enter it manually.
4. If the problem persists, contact your administrator or support team.

When adding a new device, the PingID desktop app does not appear as an authentication method

If the available authentication methods do not include the PingID desktop app, contact your system administrator or support desk. The organization's security policy might not approve usage of the PingID desktop app for authentication.

Unable to install the PingID desktop app

The installer wizard window does not appear when the installer is activated, and it appears as though the wizard cannot run. This might be caused by:

Missing administrator privileges on the machine

Contact your organization's system administrator to update permissions, or to implement the installation.

Antivirus software blocking the PingID desktop app installation without alerting or reporting it

The following scenario occurred on a Windows 10 PC running Avast antivirus. There was no response when launching the PingID desktop app installer and no alert. The following steps resolved this issue:

- Temporarily disabling the antivirus to permit normal installation of the PingID desktop app.
- Determining whether an antivirus update was available. The antivirus indicated `Everything up to date`. Further investigation revealed that although the engine and database were up to date, a newer release of the program was available.
- After updating the program and launching the PingID installer, the antivirus alerted that it was running a 15-second check for malware. After that check, the PingID desktop app installation proceeded normally.

The PingID desktop app does not launch on Mac after the installation of custom fonts

If the PingID desktop app does not launch on a Mac after custom fonts are installed:

1. Open the Font Book application.
2. Go to **Menu → File → Restore Standard Fonts**.
3. Run the PingID desktop app. It should now launch successfully.
4. Close the PingID desktop app.
5. Reinstall the custom fonts.

6. Run the PingID desktop app again. If it does not launch successfully, repeat steps 1-3.

There is a new requirement to create a PIN on the PingID desktop app

Previously, when the PingID desktop app was launched or accessed, the OTP screen was immediately visible. Now the desktop app opens with a prompt to create a PIN.

This is the result of an organizational security policy decision to secure the desktop app with either a 4 or 6-digit PIN.

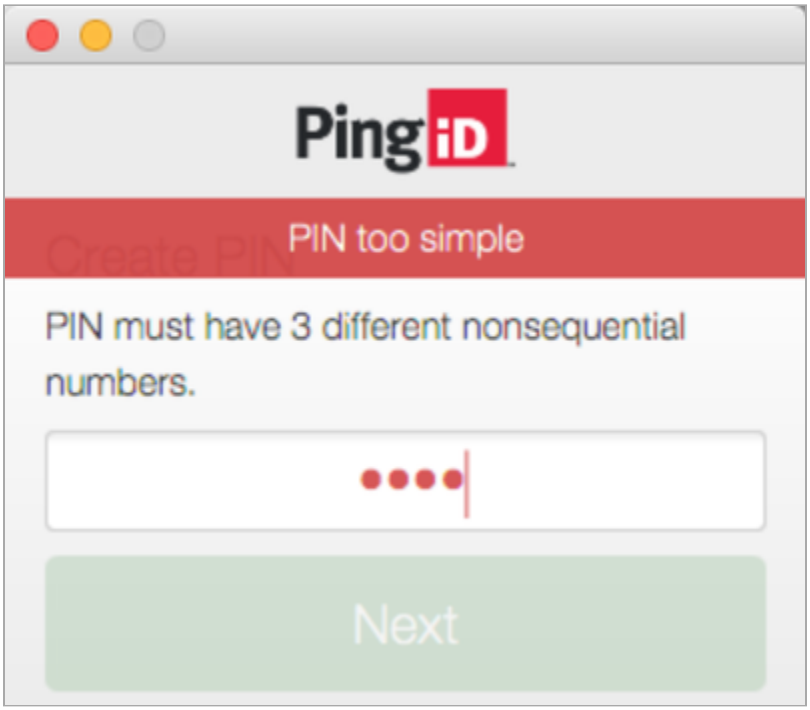
Users can choose the PIN codes to use for desktop app access. Follow the instructions on the desktop app screen to create the PIN.

> **Note**
>
> PingID enforces a PIN numbering policy that rejects repeated or consecutive numbering patterns.

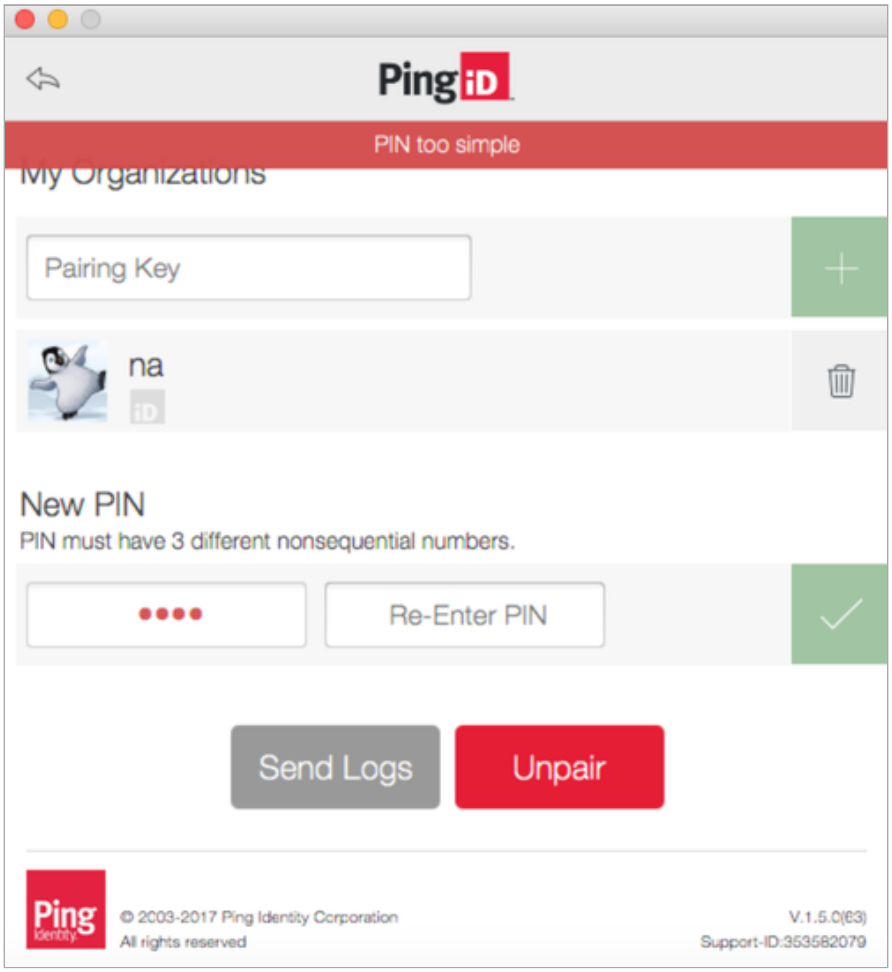
The PingID desktop app displays the message "PIN too simple"

When creating a PIN for the first time, or when changing the PIN, the PingID desktop app rejects the entry and displays `PIN too simple`.

Create PIN example



Change PIN example



PingID enforces a PIN numbering policy that will reject repeated or consecutive numbering patterns. Choose a new PIN with a more random sequence of digits.

The PingID desktop app displays the Locked screen, although the PIN was entered earlier

Although the correct PIN was entered earlier in the day, or even few minutes earlier, the desktop app now displays the **Locked** screen.

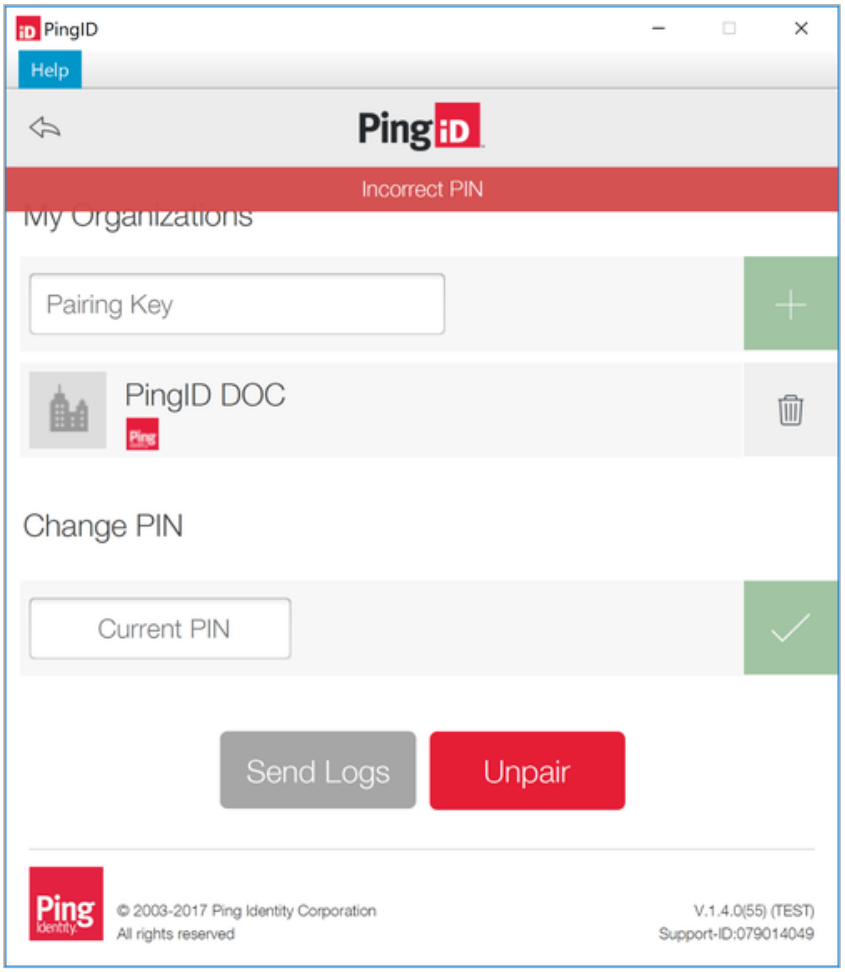
This is the normal behavior when the PingID desktop app is secured with a PIN code. After 3 minutes of inactivity on the desktop app, the app reverts to the **Locked** screen and prompts for PIN input. Enter the PIN to gain access to the OTP screen.

The PingID desktop app displays the message "Incorrect PIN"

After entering the current PIN, either to access the desktop OTP screen or when attempting to change the PIN, the desktop app displays `Incorrect PIN`.

Enter PIN example

Change PIN example



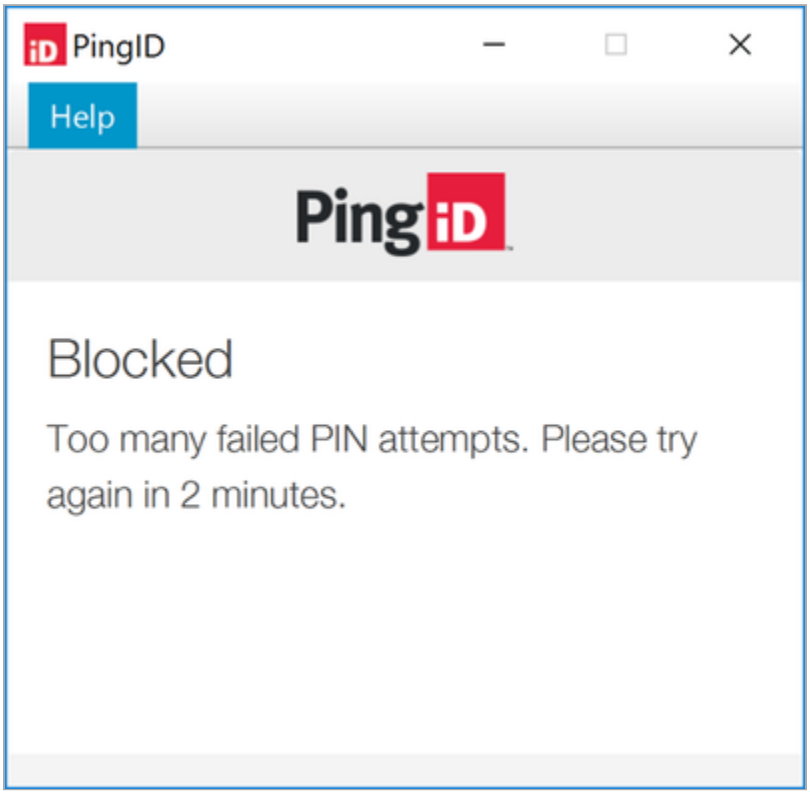
This can result from the following:

- The PIN entered is incorrect. Check that all the digits are entered in the correct sequence.
- The PIN is for a different installation of the desktop app or on another machine. Check that the desktop app is accessed from the correct user account on the correct computer.

If the above solutions are not successful, unpair the desktop app and pair it again or contact your administrator or support team.

The PingID desktop app displays the "Blocked" screen

After entering the PIN, either to access the desktop OTP screen or when attempting to change the PIN, the desktop app displays the **Blocked** screen.



This is the result of entering the PIN incorrectly three consecutive times. The `Incorrect PIN` message would have been displayed after each of the first two incorrect PIN entries. The desktop app is locked for 2 minutes. Lockdown takes effect from the time of the lock, irrespective of whether the desktop app has remained open or has been closed and relaunched.

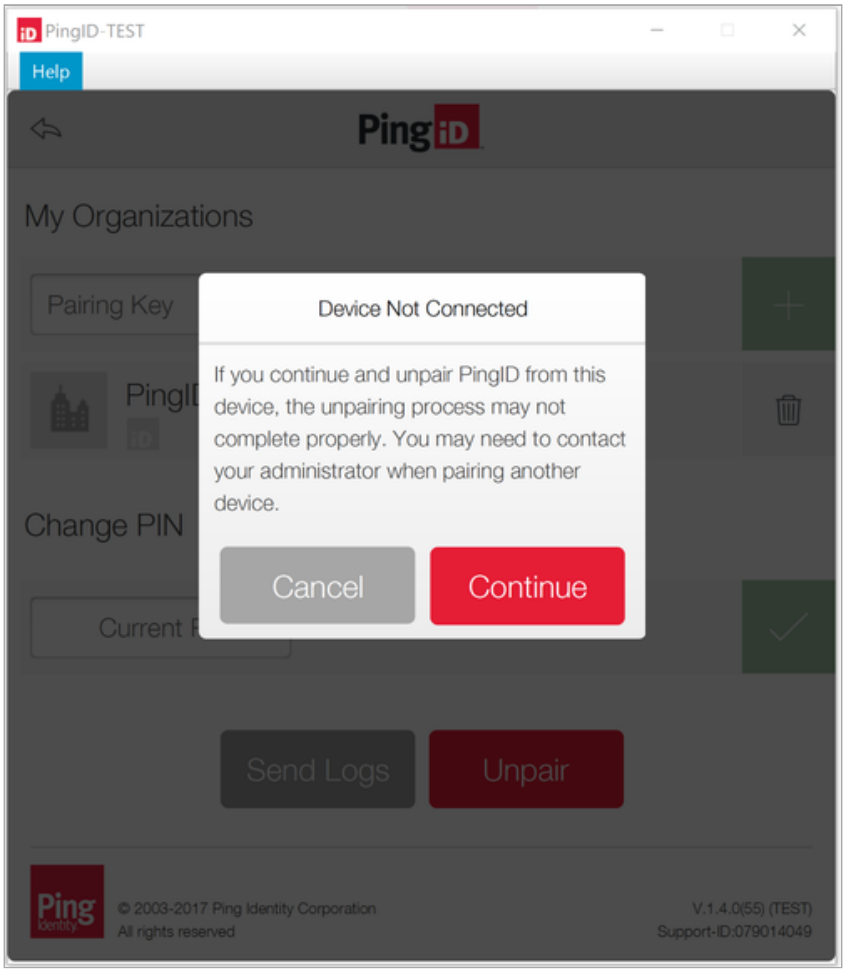
After 2 minutes, the app reverts to the **Locked** screen.

A user forgot the PIN for their PingID desktop app

If a user forgets their desktop app PIN, see Resetting a user's desktop app PIN.

The PingID desktop app displays the "Device Not Connected" screen

If a user unpairs the desktop app and the **Device Not Connected** screen is displayed, the user's computer is in offline mode.

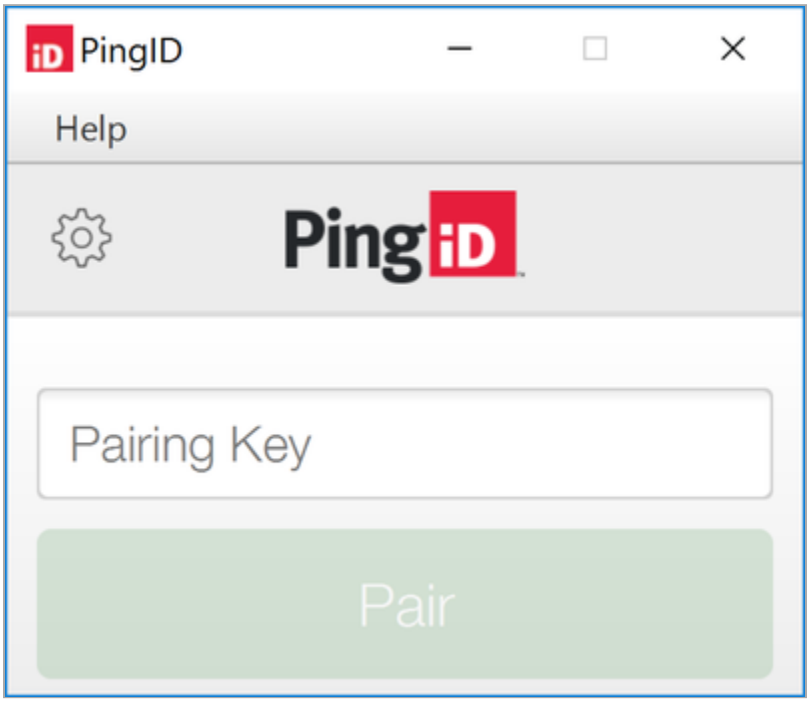


The local desktop app can be successfully unpaired in offline mode, but the entry for the desktop app in PingID's list of services still exists. This will prevent the user from pairing the desktop app again.

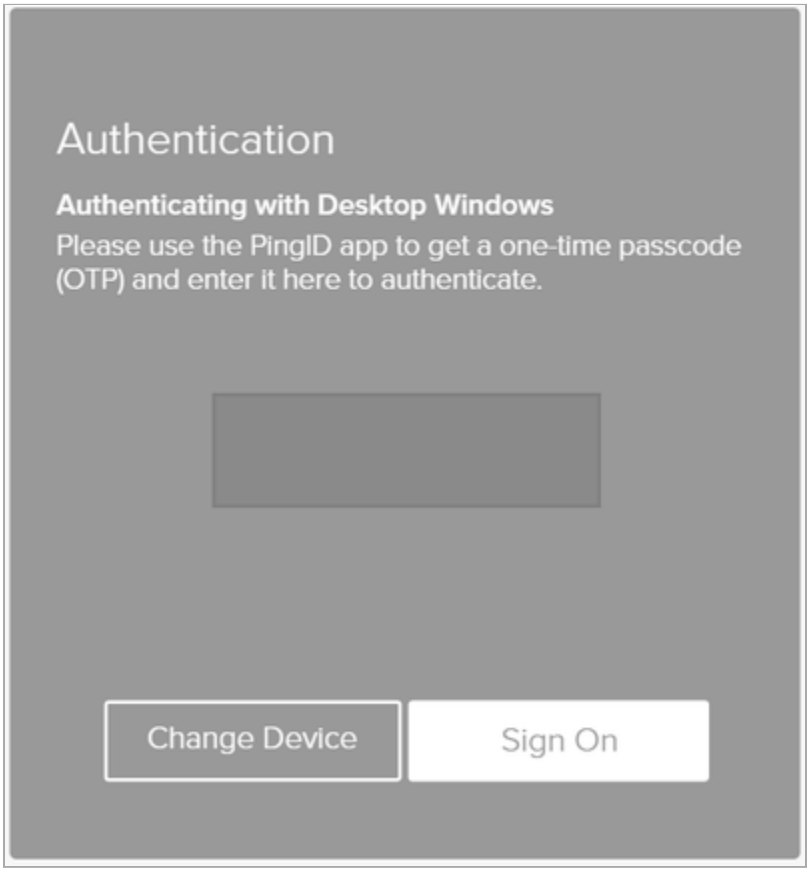
The user must contact the administrator to unpair the desktop app in PingID's list of services. Alternatively, if the user removes the desktop app from their list of devices, the entry for the desktop app in PingID's list of services will be unpaired.

The authentication screen prompts for the PingID desktop app OTP, but the PingID desktop app is not paired

If a user has unpaired the desktop app and wants to pair it again, when they launch the app they are prompted to enter a pairing key.



The user then connects to a service protected by PingID, expecting the enrollment screen with the link to an alternate authentication method, from which they could navigate to the desktop setup supplying them with a new pairing key. Instead of the enrollment screen, the authentication screen displays immediately, prompting the user to enter an OTP from the desktop app.



The user cannot provide the OTP because the desktop app is unpaired and is unable to get a pairing key to pair the desktop app.

This can be caused by unpairing the desktop app while in offline mode, leaving the entry for the desktop app intact in PingID's list of services. Contact the administrator or support team to unpair the desktop app in PingID's list of services.

When trying to access the PingID desktop app, the user receives the `No network connection` error

If the user sees the `no network connection` error when using the PingID desktop app, it might indicate that there is a problem with your connection to the proxy.

- The user might be signing on to PingID from outside the company network and did not turn off their proxy connection. If so, they should disable their proxy connection. For more information, see Enabling or disabling your proxy for PingIDdesktop.
- If this is not the case, contact customer support for further assistance.

Blocked message seen by user when signing on to PingID desktop app

If the proxy is configured locally on the users PingID desktop app, but use of proxy is not approved on the Admin portal, the user will see the following error messages when signing on to the PingID desktop app with their proxy enabled.

Pair PingID Desktop app certification issue

Clients using self-signed cacerts can run in to this problem. Two options are available:

- Workaround method: Whitelist the PingID endpoints so requests that go to *.pingone.com and *.pingidentity.com still go through the proxy, but SSL/TLS termination/decryption does not apply. This avoids the certificate issue.
- Preferred method: A self-signed certificate should be added manually by the administrator. Because the bundled JavaFX app uses its own JRE with its own cacerts, other cacerts like Windows are not acceptable, and an error might be received.

FIDO2 authentication

PingID supports the use of the FIDO2, FIDO2 biometrics, and FIDO2 security keys for authentication.

PingID supports the use of the FIDO2 protocol, and PingID FIDO2 Server is a FIDO2 certified product.

Users can authenticate with FIDO2 security keys, passkeys, or FIDO2-compatible accessing devices by using a gesture that is enabled by built-in biometrics support on the devices.

PingID's FIDO2 compliance provides security benefits, including protection against phishing, man-in-the-middle, and replay attacks. This includes the following FIDO2 protocol security measures:

- Based on public key cryptography
- Ensures that private keys remain on the FIDO2 device only
- Does not employ server-side shared secrets, that could otherwise be compromised
- Isolates services from accounts
- Does not employ a third party in the FIDO2 protocol

Enhanced FIDO2 authentication support

To benefit from enhanced FIDO2 authentication, you'll need to integrate a PingID account with a PingOne environment. You can:

- Create a new PingID account that is managed by a PingOne environment: the enhanced FIDO2 authentication method is enabled by default. Legacy FID02 biometrics and Security Key authentication methods are not available. Learn more in Creating a new PingID environment in PingOne.
- Update an existing PingID account that is integrated with a new PingOne environment to benefit from the enhanced FIDO2 authentication method. For more information, see: Updating a PingID account to use PingOne FIDO2 policy for Passkey support.

  Learn more: Integrating a PingID account with a PingOne environment.

FIDO2 integration modes

PingID supports the following FIDO2 integration modes:

- PingID's out of the box solution, using the PingID UI and the pingone.com domain. For more information, see:
  - Using Windows Hello for authentication
  - Using Apple Mac Touch ID for authentication
  - Using a security key (FIDO2) for authentication
  - Using Android biometrics for authentication
- API-based, using a custom UI that is not hosted by PingID, and a custom domain. For more information, see:
  - FIDO pairing workflow
  - FIDO authentication workflow
  - FIDO passwordless authentication workflow
- Hybrid mode, also API-based using a custom UI for registration that is not hosted by PingID, and PingID's default UI for authentication. This mode leverages the pingone.com domain. For more information, see PPM request for FIDO authentication with a hybrid UI.

Configuring FIDO2 authentication for PingID

PingID supports the FIDO2 authentication method. FIDO2 authentication allows users to authenticate using passkeys and other FIDO2-compatible authenticators.

About this task

Passkeys are FIDO credentials that are discoverable by browsers or housed within native applications or security keys for passwordless authentication. There are a wide range of devices that can be used as a passkey, including Windows Hello, iOS 14 and later, Android 7.0 and later, Apple Mac machines with fingerprint authentication capabilities, and FIDO2 security keys. PingID also supports non-discoverable credentials (FIDO2 devices that are not defined as passkeys).

To learn more about passwordless authentication using Passkeys, see Configuring passwordless authentication for passkeys.

> **Important**
>
> PingID receives confirmation that a device has the relevant WebAuthn FIDO2 capabilities with the authenticating browser. If the capabilities are not sufficient, such as the browser is not supported, the OS does not support biometric authentication, or a compatible authentication method is not defined, the user will be unable to authenticate with the passkey device and might be unable to authenticate at all if that is their only authenticating device.

To enable users to authenticate using FIDO2 authentication, the high-level flow is as follows:

Steps

1. In the Admin portal, enable FIDO2 authentication.

   For more information, see Configuring passwordless authentication for passkeys or Configuring FIDO2 authentication method for MFA authentication.

2. **Optional:** Define a PingID policy.

   For more information, see Authentication policy.

3. Have the user register their FIDO2 biometrics device and pair it with their PingID account to create a trust between the device and the user's account, so they can use it authenticate during the sign-on process.

   For more information, see the following sections in the PingID User Guide:

   - Using Windows Hello for authentication
   - Using Apple Mac Touch ID for authentication
   - Using a security key (FIDO2) for authentication
   - Using Android biometrics for authentication

FIDO2 authentication requirements and limitations

The following list details the requirements and limitations when using FIDO2 with PingID.

FIDO2 passkey requirements and limitations are constantly evolving. For a list of the most up-to-date operating systems and browsers supported, see Device support.

General requirements:

To use FIDO authentication make sure that:

- The PingID environment is integrated with PingOne. Learn more.
- You enable FIDO2 authentication method in the admin portal. If you have an account that was previously using the security key or FIDO2 biometrics authentication methods, see also Updating a PingID account to use PingOne FIDO2 policy for Passkey support.
- The user must perform registration and authentication with a WebAuthn supported browser (such as the latest versions of Google Chrome, Safari, or Microsoft Edge), that is running on a WebAuthn supported platform (such as Windows, MacOS, iOS, or Android).
- PingID supports FIDO2 and U2F security keys.

  > **Note**
  >
  > U2F security keys can only generate a single credential per domain. A device can only be paired by one user per domain.

- YubiKeys can be paired for either:
  - Security Key FIDO2 authentication
  - YubiKey OTP authentication

  PingID YubiKeys that feature one-time passcode (OTP) support only, or for which you only want to use OTP authentication, should be paired as a YubiKey authentication method rather than as a security key. For more information, see Configuring YubiKey authentication (Yubico OTP) for PingID.

Passwordless authentication requirements:

- When configuring a PingFederate policy for passwordless authentication with FIDO2 passkeys, you must use PingID Integration kit 2.7 or later, with PingFederate v9.3 or later.
- To enable passwordless authentication, FIDO2 requires Discoverable Credentials. Make sure that in the relevant FIDO2 policy make sure that the **Discoverable Credentials** field is set to either **Preferred** or **Required**.

General limitations:

- FIDO2 authentication is only supported for Web authentication, and Windows and Mac login machines.
- WebAuthn timeout is defined for 2 minutes. The actual timeout value might vary depending on the browser used.

- A user can pair more than one FIDO2 credential with their account, however, they cannot pair the same FIDO2 credentials with their account more than once.
- Some browser versions might not support FIDO2 authentication when using incognito or private mode.
- If an an iOS or Mac Touch ID device is paired with PingID, clearing history and website data from the device's Safari settings will prevent a user from using PingID to authenticate. The user must unpair their device and then pair the device again to authenticate with PingID.
- Security keys can be used for web-based authentication through WebAuthn supporting browsers only.

Second factor authentication limitations:

- Android devices that are paired within a workspace can only be used to authenticate in the same workspace.

For troubleshooting, see the relevant section in the PingID User Guide.

Windows login and Mac login limitations:

Users authenticating as part of a Windows login, Windows login (passwordless), or Mac login authentication flow can only authenticate using a security key. PingID determines whether a passkey is a security key based on the Authenticator Attachment and the Transports attributes that are presented in the AuthenticatorAttestationResponse. Learn more about these authentication flows:

- Integrating PingID with Windows login
- Integrating PingID with Windows login (passwordless)
- PingID integration for Mac login

Configuring passwordless authentication for passkeys

FIDO2 passwordless authentication enables you to identify and authenticate a user based on the FIDO2 protocol without requiring the user to enter their username and password.

About this task

To configure FIDO2 passwordless authentication, you must configure a PingFederate policy for a passwordless authentication flow. FIDO2 must then be enabled in the administrative console.

The process of registering a FIDO2 passkey is the same for both a passwordless and a multi-factor authentication flow. The user is directed to the relevant flow, according to your organization's configuration. Once registered, the same FIDO2 passkey can be used to authenticate with either flow.

> **Note**
>
> This feature requires PingFederate 9.3 or later. For more information, see FIDO2 authentication requirements and limitations.

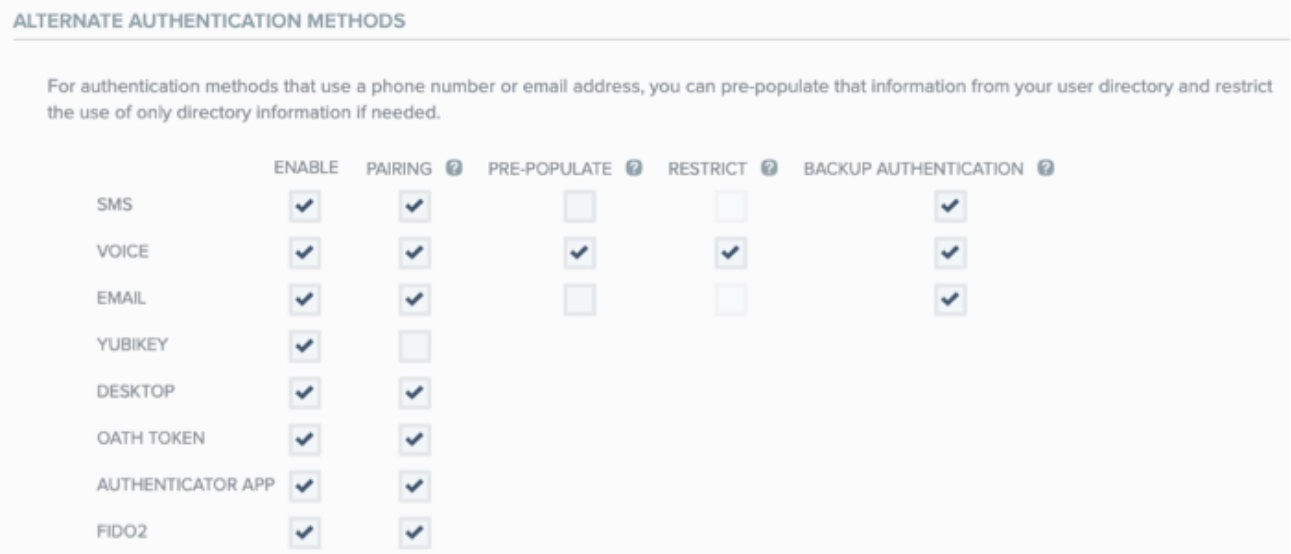
Steps

1. In the PingFederate administrative console, create a policy for passwordless authentication.

   For more information, see Configuring a PingFederate policy for passwordless authentication with FIDO2 passkeys.

2. Sign on to the PingID admin console and enable FIDO2 authentication.

   1. Go to **Setup → PingID → Configuration**.
   2. Go to the **Alternate Authentication Methods** section, and in the **FIDO2** row, select the **Enable** check box.



   3. Click **Save**.

3. To ensure your FIDO2 policy allows the use of Discoverable Credentials. Non-discoverable credentials cannot be used for passwordless authentication flows.

   1. In the PingOne admin portal, go to **Authentication → FIDO**.
   2. On the FIDO Policies page, in the relevant FIDO policy, in the Discoverable Credentials field, select either **Preferred** or **Required**. For information, see Adding a FIDO policy.

Result

The changes are saved, and users can pair a passkey and use it for passwordless authentication.

Configuring FIDO2 authentication method for MFA authentication

To allow users to pair and authenticate using passkeys for MFA (Multi-factor authentication), enable FIDO2 authentication in the admin portal.

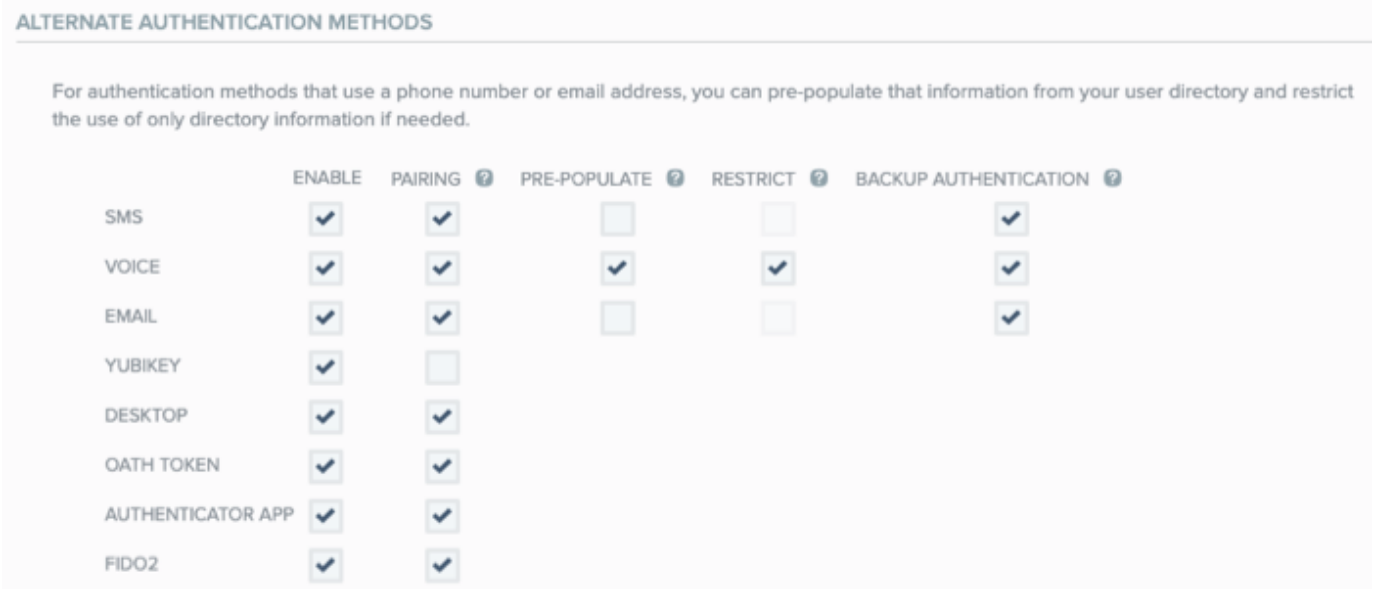
About this task

Users must enter their username (and password, if required), and are then prompted to authenticate with their passkey.

> **Note**
>
> To configure passwordless authentication for passkeys using the FIDO2 authentication method, see Configuring passwordless authentication for passkeys.

Steps

1. Sign on to the admin portal.
2. Go to **Setup → PingID → Configuration**.
3. Go to the **Alternate Authentication Methods** section, and in the **FIDO2** row, select the **Enable** check box.



4. Click **Save**.

Result

Users can pair and authenticate passkey devices. For examples, see Using Windows Hello for authentication, Using Apple Mac Touch ID for authentication, and Using Android biometrics for authentication in the PingID End User Guide.

Updating a PingID account to use PingOne FIDO2 policy for Passkey support

If you have a PingID account that has been integrated with PingOne you can update it to support the FIDO2 authentication method. This allows you to benefit from the full range of options in the enhanced FIDO2 policy.

Before you begin

The FIDO2 authentication method is only available for PingID accounts that have been integrated into a PingOne environment.

About this task

The FIDO2 authentication method replaces the deprecated FIDO biometrics and security key authentication methods and offers expanded configuration options and support for a wide range of FIDO authentication devices, including cloud-synced FIDO devices.

If you have already integrated your PingID account with a PingOne environment, update it to use the enhanced FIDO2 policy.

Warning

- Updating to FIDO2 permanently inactivates the legacy FIDO2 biometrics and Security Key authentication methods and cannot be undone. Note that at this stage, the FIDO2 authentication method cannot be used with DaVinci-based flows.
- After updating a PingID account to use the FIDO2 authentication method it is no longer possible to unlink the PingID account from the PingOne environment. Deleting the PingOne environment will also delete the PingID account.

Steps

1. Sign on to the Admin portal and go to **Setup → PingID → Configuration**

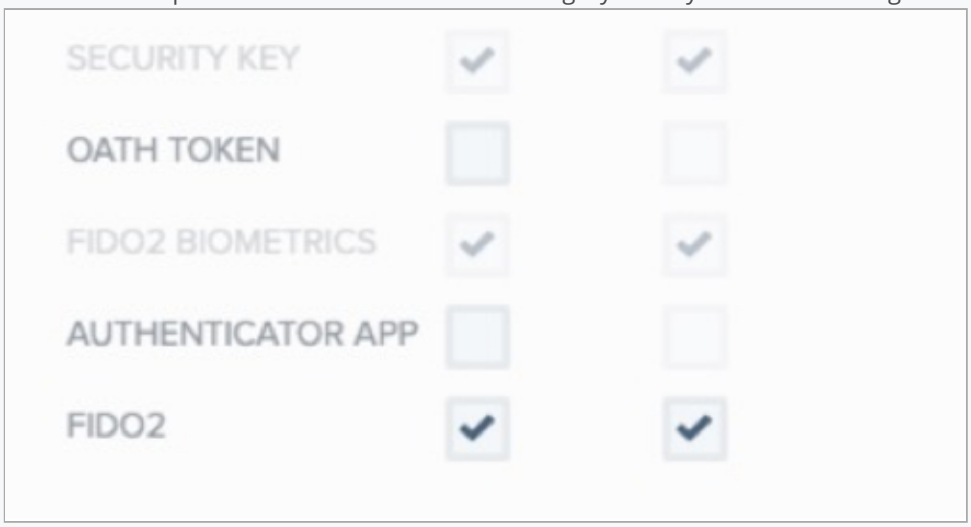
   Result:

   After your PingID account is successfully integrated into a PingOne environment in the **Alternate Authentication Methods** section, you'll see a new entry for the FIDO2 authentication method.

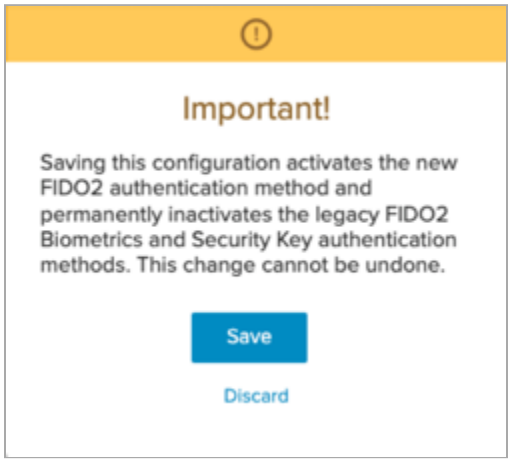
2. In the **Alternate Authentication Methods** section, in the **FIDO2** row, make sure the **Enable** and **Pairing** check boxes are selected.

   Note

   If you previously enabled Security Key or FIDO2 Biometrics authentication methods, those options are greyed out. These authentication options are removed and become legacy when you save the configuration changes.

3. Click **Save**. You'll see the following warning message:



Result

All Security Key or FIDO2 Biometrics authentication methods and associated configurations are upgraded to the FIDO2 authentication method.

In PingOne, the FIDO2 policy shows the full range of options available, as well as the default Passkey and Security Key policies. To learn more about FIDO2 policy configuration, see Creating a FIDO policy in the PingOne Cloud Platform documentation.

Frequently asked questions when upgrading biometrics and security key to FIDO2 authentication

This section addresses frequently asked questions when upgrading from FIDO2 biometrics and security key authentication methods to FIDO2 authentication.

What are the benefits of upgrading to FIDO2 authentication?

- FIDO2 offers expanded configuration options and support for a wider range of FIDO2 authentication devices, including cloud-synced FIDO2 devices.
- FIDO2 replaces the deprecated FIDO2 biometrics and security key authentication methods.

Can I use a single FIDO2 passkey to authenticate across different browsers and devices?

- You can use the same FIDO2 credential (passkey) to authenticate across different browsers and devices within the same ecosystem (for example, Apple or Google ecosystem).
- To ensure users can authenticate with a FIDO2 device across different browsers and devices within the same ecosystem, in the FIDO2 policy, set **Backup Eligibility** to **Allow**. This allows authentication with passkeys and devices using cloud-synced credentials.

Learn more in FIDO policies in the PingOne documentation.

Can I upgrade to FIDO2 from within the legacy PingID admin portal?

The FIDO2 authentication method is only available for PingID accounts that are integrated with a PingOne environment.

To upgrade to FIDO2 authentication:

1. Make sure your PingID account is integrated into a PingOne environment.

Learn more in Setting up an environment for strong authentication (MFA).

2. In the legacy PingID admin portal, upgrade to FIDO2 authentication.

   Learn more in Updating a PingID account to use PingOne FIDO2 policy for Passkey support.

3. If you have a PingOne MFA policy that uses legacy FIDO2 biometrics and security key authentication methods, update it. Learn more in Updating a PingID account to use PingOne FIDO2 policy for Passkey support.

What impact will upgrading have on security keys and FIDO2 biometrics devices that are already paired to users accounts?

- Security keys and FIDO2 Biometrics devices already paired to user accounts are automatically upgraded to FIDO2.
- Users can continue to authenticate with their existing devices.

What happens to PingID policies that have "security key" defined as an allowed authentication method?

- The affected policies are automatically updated to use FIDO2 as the allowed authentication method.

Can I define different authentication policies for different FIDO2 devices, such as FIDO2 security keys and Windows Hello devices?

- In a future release, it will be possible to define multiple FIDO2 policies and apply them to different devices, such as FIDO2 security keys and Windows Hello devices.
- PingOne's current FIDO2 policy provides many configuration options. For example, specific supported FIDO2 devices can be configured in the FIDO policy under **Authenticator Attachment** as **Platform**, **Cross-platform**, or **Both**.

  Learn more in FIDO policies in the PingOne documentation.

Can I roll back to the legacy FIDO2 biometrics and security key authentication methods after upgrading to the FIDO2 authentication method?

- Upgrading to the FIDO2 authentication method permanently deactivates the legacy FIDO2 biometrics and security key authentication methods and cannot be undone. These options are grayed out in the legacy PingID admin portal, and they're removed from PingOne policies and replaced with the FIDO2 authentication method.

If I've migrated a PingID account to a PingOne environment and upgraded to the FIDO2 authentication method, can I revert my PingID account to the legacy PingID admin portal?

- After migrating a PingID account to a PingOne environment and upgrading to FIDO2, you cannot revert to the legacy PingID admin portal.
- Deleting the PingOne environment also deletes the PingID account.

Legacy FIDO2 authentication methods

PingID supports the use of the FIDO2, FIDO2 biometrics, and FIDO2 security keys for authentication.

This section describes configuration for legacy FIDO2 biometrics and FIDO2 security key authentication methods.

The FIDO2 authentication method replaces the deprecated FIDO biometrics and security key authentication methods and offers expanded configuration options and support for a wide range of FIDO authentication devices, including cloud-synced FIDO devices. Learn more about FIDO2 here.

(Legacy) Configuring FIDO2 biometrics for PingID

PingID supports FIDO2 platform biometrics. Users can authenticate on their FIDO2-compatible accessing device using a gesture that is enabled by the device's built-in biometrics.

About this task

Supported devices include Windows Hello, iOS and iPadOS devices 14 and later, Android devices 7.0 and later, and Apple Mac machines with fingerprint authentication capabilities.

If a passwordless flow is configured, the passwordless flow is enabled by FIDO2 platform biometrics. For more information, see (Legacy) Configuring FIDO2 passwordless authentication.

> **Important**
>
> PingID receives confirmation that a device has the relevant WebAuthn FIDO2 capabilities with the authenticating browser. If the capabilities are not sufficient, such as the browser is not supported, the OS does not support biometric authentication, or a compatible authentication method is not defined, the user will be unable to authenticate with the FIDO2 biometrics device and might be unable to authenticate at all if that is their only authenticating device.

To enable users to authenticate using FIDO2 platform biometrics, the high-level flow is as follows

Steps

1. In the Admin portal, enable FIDO2 platform biometrics.

   For more information, see (Legacy) Configuring FIDO2 passwordless authentication or (Legacy) Configuring FIDO2 biometrics for MFA authentication.

2. **Optional:** If required, define a PingID policy.

   For more information, see Authentication policy.

3. Have the user register their FIDO2 biometrics device and pair it with their PingID account to create a trust between the device and the user's account, so they can use it authenticate during the sign-on process.

   For more information, see the following sections in the PingID User Guide:

   - Using Windows Hello for authentication
   - Using Apple Mac Touch ID for authentication
   - Using a security key (FIDO2) for authentication
   - Using Android biometrics for authentication

(Legacy) FIDO2 biometrics authentication requirements and limitations

The following list details the requirements and limitations when using FIDO2 platform biometrics with PingID.

General requirements:

> **Important**
>
> For PingID environments that are integrated with PingOne: From April 15th 2024, the FIDO2 Biometrics and Security Key authentication methods are deprecated and replaced by the more advanced FIDO2 authentication method. Learn more: Updating a PingID account to use PingOne FIDO2 policy for Passkey support.

- FIDO2 biometrics authentication is supported for web authentication only.
- Define an appropriate FIDO2 platform authentication method on the accessing device to pair the device, such as fingerprint or Face ID. If no platform authentication method is defined, the user will not be able to pair the device or authenticate with PingID.
- Perform registration and authentication with a WebAuthn supported browser, such as the latest versions of Google Chrome, Safari, or Microsoft Edge.
- Avoid the use of the same FIDO2 biometrics device by more than one user.
- Passwordless authentication using Mac Touch ID through a Chrome browser is only supported for devices paired after February 23, 2021. Users with devices that were paired to PingID before February 23, 2021 should unpair their device and then pair it again, in order to use passwordless authentication with a Chrome browser.

FIDO Passkey requirements:

FIDO passkey requirements and limitations are constantly evolving. For a list of the most up-to-date operating systems and browsers supported, see Device support.

Passwordless authentication requirements:

- When creating a PingFederate policy for passwordless authentication with FIDO2 biometrics, you must use PingID Integration kit 2.7 or later, with PingFederate v9.3 or later.

General limitations:

- WebAuthn timeout is defined for 2 minutes. The actual timeout value might vary depending on the browser used.
- PingID does not support Android-key attestation.
- A user can pair more than one FIDO2 biometrics device with their account, however, they cannot pair the same FIDO2 biometrics device with their account more than once.
- Some older browser versions might not support FIDO2 biometrics when using incognito or private mode.
- If an an iOS or Mac Touch ID device is paired with PingID, clearing history and website data from the device's Safari settings will prevent a user from using PingID to authenticate. The user must unpair their device and then pair the device again to authenticate with PingID.

Second factor authentication limitations:

- Android devices that are paired within a workspace can only be used to authenticate in the same workspace.

For troubleshooting, see the relevant section in the PingID User Guide.

(Legacy) Configuring FIDO2 passwordless authentication

FIDO2 passwordless authentication enables you to identify and authenticate a user based on the FIDO2 protocol without requiring the user to enter their username and password.

About this task

> **Note**
>
> This topic is for passwordless authentication using legacy FIDO2 biometrics. For FIDO2 authentication method, see Configuring passwordless authentication for passkeys.

To configure FIDO2 passwordless authentication, you must configure a PingFederate policy for a passwordless authentication flow. FIDO2 biometrics must then be enabled in the administrative console.

The process of registering a FIDO2 device is the same for both passwordless and secondary authentication flows. The user is directed to the relevant flow, according to your organization's configuration. Once registered, the same FIDO2-compliant device can be used to authenticate with either flow. For more information, see Setting up Windows Hello authentication.

> **Note**
>
> This feature requires PingFederate 9.3 or later. For more information, see (Legacy) FIDO2 biometrics authentication requirements and limitations.

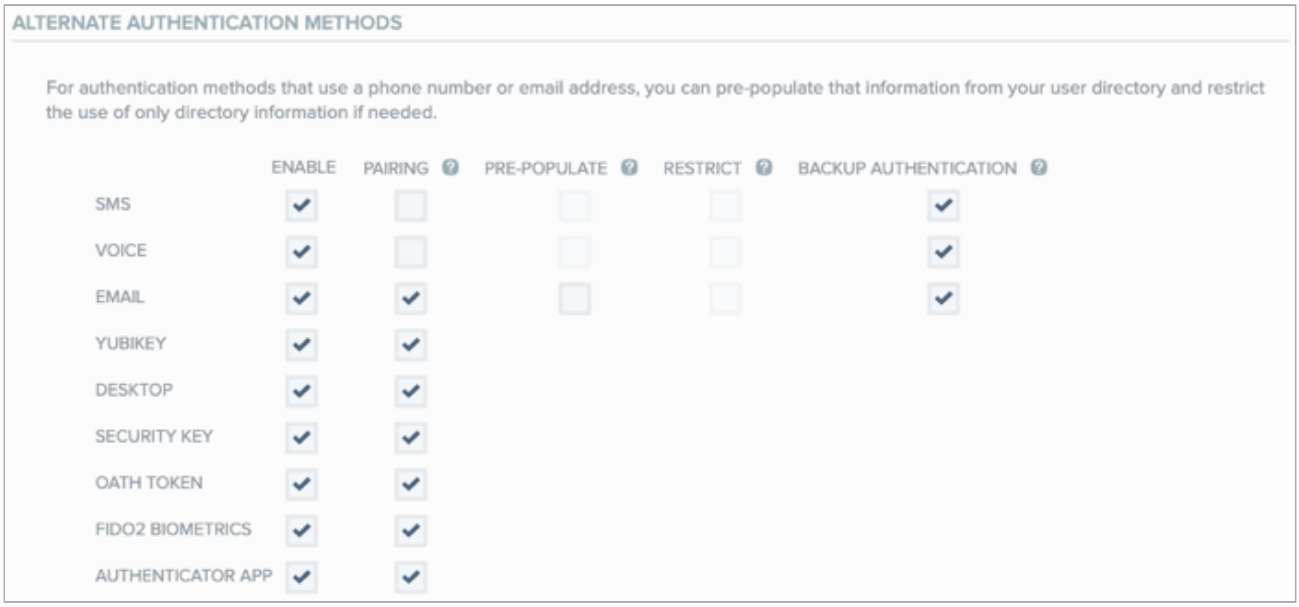
Steps

1. In the PingFederate administrative console, create a policy for passwordless authentication.

   For more information, see (Legacy) Configuring a PingFederate policy for passwordless authentication with FIDO biometrics.

2. Sign on to the PingOne for Enterprise admin console and enable FIDO2 biometrics.

   1. Go to **Setup → PingID → Configuration**.
   2. Go to the **Alternate Authentication Methods** section, and in the **FIDO2 Biometrics** row, select the **Enable** check box.



3. Click **Save**.

Result

The changes are saved, and users can pair and authenticate with gestures defined on their FIDO2 biometrics accessing device. For more information, see Using Windows Hello for authentication.

(Legacy) Configuring FIDO2 biometrics for MFA authentication

To allow users to pair and authenticate using the built-in biometrics on their device for MFA (Multi-factor authentication), enable FIDO2 biometrics in the admin portal.

About this task

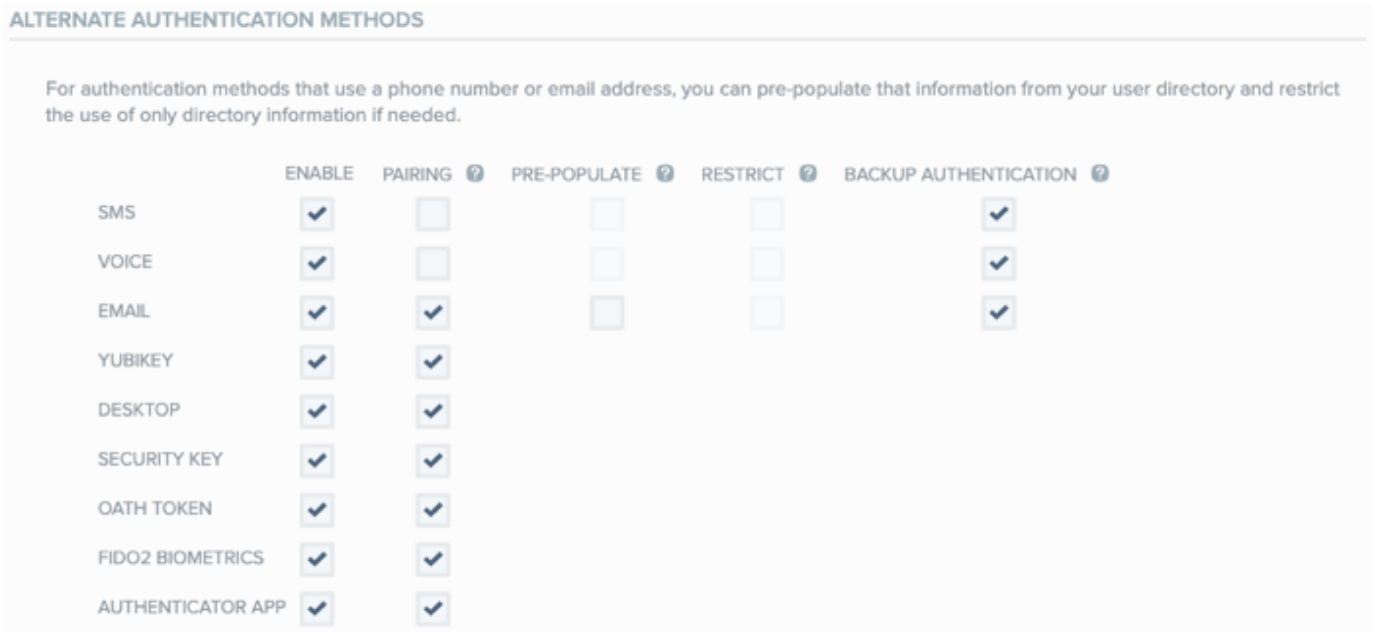
Users must enter their username (and password, if required), and are then prompted to authenticate with their device biometrics.

> **Note**
>
> This topic is for authentication using legacy FIDO2 biometrics. To configure passwordless authentication for passkeys using the FIDO2 authentication method, see Configuring passwordless authentication for passkeys.

Steps

1. Sign on to the admin portal.
2. Go to **Setup → PingID → Configuration**.

3. Go to the **Alternate Authentication Methods** section, and in the **FIDO2 Biometrics** row, select the **Enable** check box.



4. Click **Save**.

Result

Users can pair and authenticate with gestures defined on their FIDO2 biometrics accessing device. For more information, see Using Windows Hello for authentication, Using Apple Mac Touch ID for authentication, and Using Android biometrics for authentication in the PingID End User Guide.

(Legacy) FIDO2 biometrics use cases

The following table outlines several common use cases and their expected behaviors when using FIDO2 biometrics authentication.

> **Note**
>
> If policy rules are configured, the results might vary from those described in the table. For more information, see PingID authentication policy.

Paired devices	Browser	Results	Reason
FIDO2 biometrics device only	WebAuthn Platform compliant	The browser prompts the user to authenticate using their FIDO2 biometrics device.	FIDO2 biometrics is the only authentication method, and the browser supports WebAuthn platform, so the user can authenticate using their FIDO2 biometrics device.

Paired devices	Browser	Results	Reason
• FIDO2 biometrics (primary) • Email • SMS	WebAuthn platform compliant	The browser prompts the user to authenticate using their FIDO2 biometrics device. If the **Prompt to Select** setting is enabled, FIDO2 Biometrics appears in the list of authentication options.	The browser supports FIDO2 biometrics, which is the user's primary device.
• FIDO2 biometrics - Windows Hello (primary) • FIDO2 biometrics - Android device • Email • SMS	WebAuthn platform complaint	If the user tries to access their account with their Android device, they are prompted to authenticate using that device, even though it is not their primary device.	If more than one FIDO2 biometrics device is paired with a user's account, when accessing with a FIDO2 device, the browser prompts the user to authenticate with the current accessing device, regardless of which FIDO2 device is the primary device.
FIDO2 biometrics only	Not WebAuthn Platform compliant	The browser displays the following message: `This browser doesn't support your current authentication method. Try a different browser or contact your administrator.`	The browser doesn't support the user's current authentication method. The user must either use a different browser that is WebAuthn compliant, such as the latest version of Chrome or Microsoft Edge, or use a FIDO2 biometrics device that is paired with their account.
• FIDO2 biometrics (primary) • Email • SMS	Not WebAuthn platform compliant	The browser prompts the user to authenticate using the next paired device. In this example, the user must authenticate using email or SMS. If the **Prompt to Select** setting is enabled, FIDO2 biometrics does not appear in the list of authentication options.	The browser is not Webauthn platform compliant and does not support the user of a FIDO2 biometrics device. The FIDO2 biometrics option is not shown and only the secondary authentication methods are presented to the user.

(Legacy) Configuring the FIDO2 security key for PingID

Configure FIDO2 security key for PingID authentication. FIDO2 and U2F-compatible security keys enable relying parties to offer a strong cryptographic authentication option for end user security.

You can use a security key hardware authenticator to cover many use cases, including those of sensitive environments or users working in environment with limited device or phone access, such as hospitals, financial institutions, or federal buildings.

FIDO2 security keys are fully backward compatible with U2F, enabling PingID to support both FIDO2 and U2F security keys.

When security key authentication is enabled, the user registers the security key and pairs it with their PingID account. This creates a trust between the security key and the user's account, so they can use the security key to authenticate during the sign-on process.

> **Note**
>
> Use security keys for web-based authentication through WebAuthn supporting browsers only.

Passwordless security key

You can configure a PingFederate policy to allow users to authenticate with their security key as a first factor authentication, eliminating the need to enter a users name or password, and providing a frictionless and secure sign on experience.

To configure passwordless authentication using a security key:

1. (Legacy) Configuring security key authentication with Resident Key set to **Required**.
2. Configure a PingFederate policy for passwordless authentication with a security key (see (Legacy) Configuring a PingFederate policy for passwordless authentication with a security key).

For information about security key requirements and limitations, see (Legacy) Security key authentication requirements and limitations.The process of registering a security key is the same for both passwordless and secondary authentication flows. The user is directed to the relevant flow, according to your organization's configuration. Once registered, the same security key can be used to authenticate via either flow (see Setting up your security key in the PingID User Guide).

Manual authentication with a FIDO2 security key

PingID integration with Windows login supports the use of FIDO2 security keys for manual authentication, such as if a user does not have an internet or network connection when signing on.

- FIDO2 security key for manual authentication is supported by PingID Integration for Windows login 2.3 or later.
- U2F security key for manual authentication is only supported by PingID Integration for Windows login 2.3 - 2.7.x.

Users must pair a security key and authenticate successfully at least once online, to use it when offline. For more information, see the PingID End User Guide.

(Legacy) Security key authentication requirements and limitations

When using security keys with PingID, the following requirements and limitations apply:

Important

For PingID environments that are integrated with PingOne: From April 15th 2024, the FIDO2 Biometrics and Security Key authentication methods are deprecated and replaced by the more advanced FIDO2 authentication method. Learn more: Updating a PingID account to use PingOne FIDO2 policy for Passkey support.

- Security keys are supported for Web authentication only.
- PingID supports FIDO2 and U2F security keys.

  Note

  U2F security keys can only generate a single credential per domain. A device can only be paired by one user per domain.

- Security keys can be used for web-based authentication through WebAuthn supporting browsers only.

  Note

  If a browser supports the use of a security key, the browser also supports WebAuthn.

- When authenticating with a mobile device, use of FIDO2 and U2F security keys with PingID:
  - Is supported on Android 7 and later
  - Is supported on iOS 13.3 and later
- Registration and authentication must be performed with a WebAuthn supported browser, such as the latest versions of Google Chrome or Microsoft Edge.
- The use of FIDO2 security keys for manual (offline) authentication:
  - Requires PingID Integration for Windows login 2.3 or later.
- WebAuthn timeout is defined for 2 minutes. The actual timeout value might vary depending on the browser used.
- PingID does not support security keys that require a signed attestation using ECDAA in packed attestation format.
- A user can pair more than one security key with their account.
- The same security key can be used by more than one user if each user is pairing the security key to a different account.
- A user cannot pair the same security key with their account more than once.
- YubiKeys can be paired for either:
  - Security Key FIDO2 authentication
  - YubiKey OTP authentication

  PingID YubiKeys that feature one-time passcode (OTP) support only, or for which you only want to use OTP authentication, should be paired as a YubiKey authentication method rather than as a security key. For more information, see Configuring YubiKey authentication (Yubico OTP) for PingID.

- The following limitations should be considered when configuring security key authentication with PingID:
  - Some browsers do not support the use of a FIDO2 security key when **User Verification**is set to **Required**.
  - Some browsers do not allow authentication with a security key when the security key is paired as a resident key.
  - Some browsers do not support security key registration when**Resident Key** is set to **Required**.
- Windows login supports the use of FIDO2 security keys.

> **Note**
>
> If user verification has been set to Required for security keys in the admin portal, this will not affect offline authentication, and users will be able to use their security key for offline authentication without user verification.

Passwordless security key

To use a security key for passwordless authentication:

- The security key must support the use of a resident key, and be paired as a resident key.
- When creating a PingFederate policy for passwordless authentication with a security key you must use PingID Integration kit 2.10 or later, with PingFederate v9.3 or later.

Some browsers do not support the security key passwordless authentication flow. Passwordless authentication with a security key has been successfully tested on:

- Windows 10 machines running the latest version of Windows Edge, FireFox, Opera, and Chrome.
- Apple Mac 10.15 (Catalina) machines running the latest versions of Windows Edge, Opera, and Chrome.
- Testing has also been performed successfully on Apple Mac 11 (Big Sur), and Mac 12.4 (Monterey).

Security keys supported

PingID is a FIDO2-certified service and supports any FIDO2 key that complies with the FIDO2 standard.

(Legacy) Configuring security key authentication

Use the FIDO2 security key for web-based authentication only. The browser with which the user is accessing their resources must support WebAuthn, such as the latest version of Google Chrome or Mozilla Firefox.

About this task

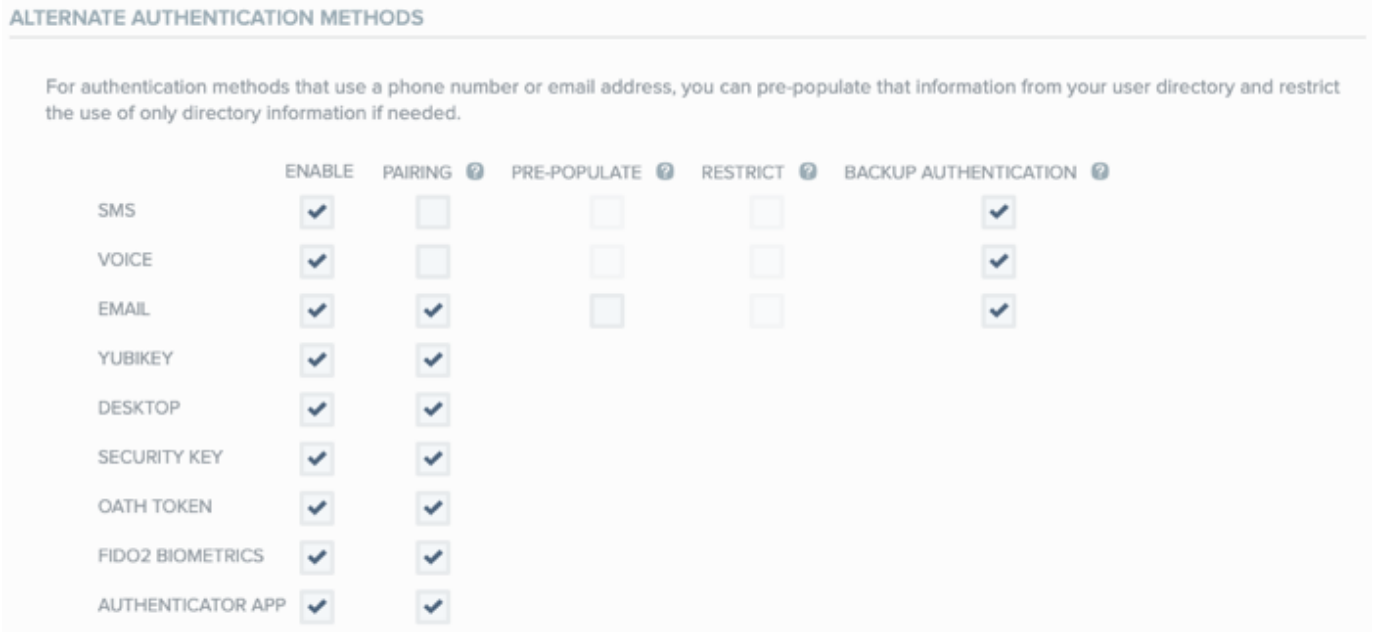
> **Note**
>
> Define the use of security keys for offline authentication when installing the PingID Integration for Windows Login.

Important

If the browser does not support WebAuthn, the user will be unable to authenticate with the security key and might be unable to authenticate if that is their only authenticating device.

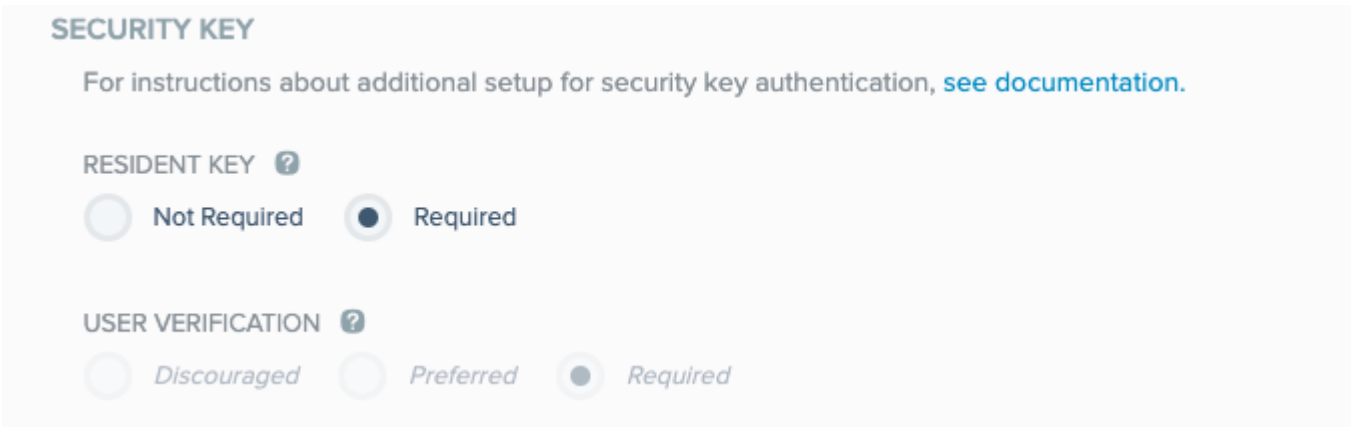
Steps

1. Sign on to the admin console.
2. Go to **Setup → PingID → Configuration**.
3. Go to the **Alternate Authentication Methods** section, and in the **Security Key** row, select the **Enable** check box.



Result:

The ability to pair and authenticate with a security key is enabled for all users in that organization, and additional security key configuration fields are shown.



4. In the **Enable** column, select the **Security Key** check box.

5. **Optional:** In the **Security Key** section, configure the following fields:
   - **Resident Key**. When set to Required, the private key is saved on the security key. To enforce passwordless authentication on all authentication attempts, set this field to **Required**.
   - **User Verification**. This option requires the user to perform a gesture using their security key, to validate their identity (for example, using their fingerprint, or entering a PIN code). Select either:

     Choose from:

   - **Required**: only security keys that support user verification can be used to authenticate. When the **Resident Key** field is set to **Required**, this option is automatically set to **Required**.
   - **Preferred** (default): user verification is performed if the user's security key supports it, and is skipped if not supported.
   - **Discouraged**: user verification is not performed, even when supported by the user's security key. In cases where user verification is required by the security key itself, this setting does not override the device setting.

   > **Caution**
   >
   > When user verification is changed from preferred to required, it will automatically unpair all security keys that have not undergone user verification during registration or authentication in the past. To identify security keys that have not been registered as security keys that support user verification, see the `fidoUserVerification` field in the PingID User Detailed Status Report fields.

   > **Note**
   >
   > To enable passwordless authentication with a security key, you also need to create a PingFederate policy for passwordless authentication with a security key.

6. To enforce the PingOne FIDO policy during authentication and registration, select the**Enforce PingOne FIDO Policy** check box.

   > **Note**
   >
   > - This feature is only available for organizations that are using a PingID environment that is integrated with PingOne or created by PingOne.
   > - Only the default PingOne FIDO policy is enforced. To edit the policy or change the default policy, see Managing FIDO policies.

7. Click **Save**.

Result

Users can pair and authenticate with their security keys.

(Legacy) Security key use cases

The following table outlines common use cases and their expected behaviors when using security key authentication.

> **Note**
>
> The results can vary from those described in the table if policy rules are applied. For more information, see PingID authentication policy.

Paired devices	Browser	Results	Reason
Security key only	WebAuthn compliant	The user is prompted to authenticate using their security key.	Security key is the only allowed authentication method and the browser supports WebAuthn, so the user can authenticate using their security key.
• Security key (primary) • Email • SMS	WebAuthn compliant	The user is prompted to authenticate using their security key. If **Prompt to Select** is enabled, security key appears in the list of authentication options.	The browser supports security key, which is the user's primary device.
Security key only	WebAuthn compliant	`Something went wrong. Try again later.` displays.	The user did not tap the security key within the required time, or the relevant browser window was not selected when they tapped the security key button. The user should click **Retry** and authenticate again.
Security key only	Not WebAuthn compliant	`Cannot authenticate with this device` displays.	The browser does not support the user's current authentication method. The user should try a different browser that is WebAuthn compliant, such as the latest version of Chrome.
• Security key (primary) • Email • SMS	Not WebAuthn compliant	The user is prompted to authenticate using the next paired device, in this case email or SMS. If **Prompt to Select** is enabled, security key does not appear in the list of authentication options.	The browser is not WebAuthn compliant and does not support the use of a security key. Secondary authentication method is presented to the user.

Configuring YubiKey authentication (Yubico OTP) for PingID

The YubiKey is a hard token that acts as a hardware authenticator. By combining PingID and YubiKey, an enterprise gives their users an additional, secure form of strong authentication.

YubiKeys can be paired for either:

- Yubico OTP authentication
- Security Key FIDO2/U2F authentication

> **Note**
>
> If you have a YubiKey that is FIDO2 compliant, to take advantage of FIDO2 capabilities, pair the device as a security key. For more information, see (Legacy) Configuring the FIDO2 security key for PingID.

A YubiKey hardware authenticator can be used in sensitive environments or for users working in environment with limited device or phone access, such as hospitals, financial institutions, or federal buildings.

The YubiKey hardware gives your enterprise a variety of form factors to allow the user to authenticate combined with the contextual awareness of PingID. YubiKey doesn't require a battery or network connectivity, so it's always on and accessible for MFA.

When YubiKey authentication is enabled, the user registers their personal YubiKey and pairs it with their PingID account. This creates a trust between the YubiKey and the user's account so they can use the YubiKey to authenticate during the sign on process.

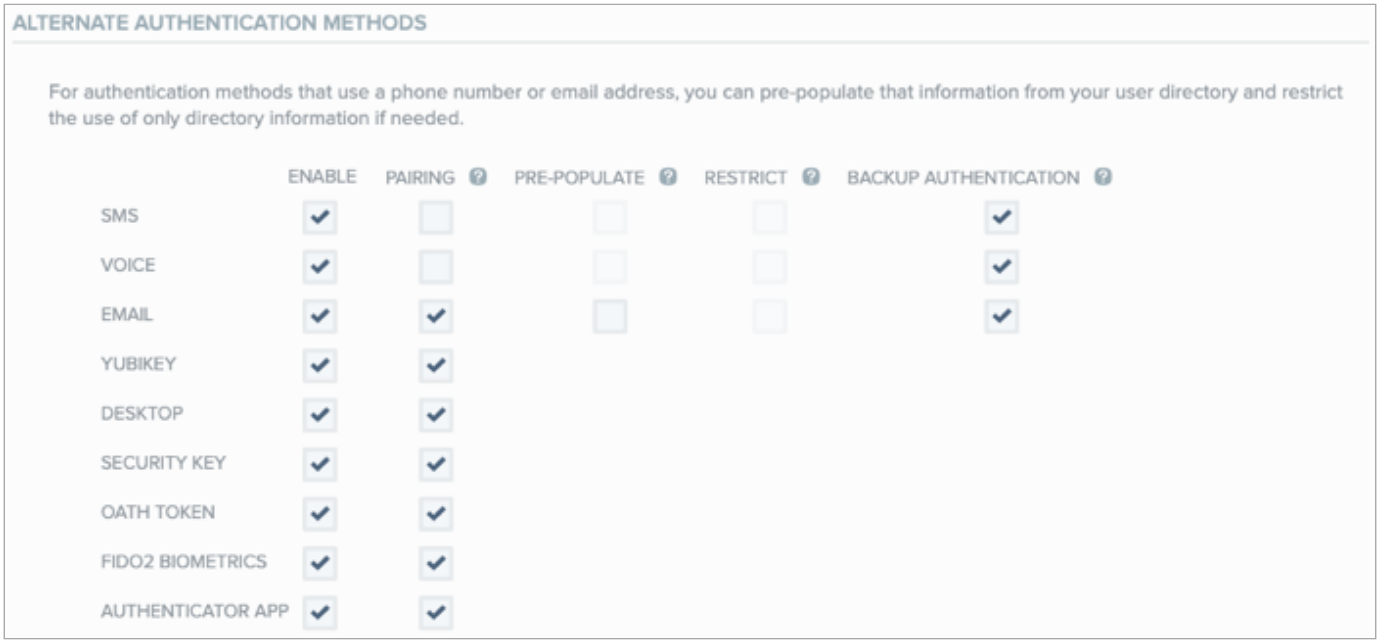
For information about the user experience, see the PingID End User Guide.

> **Important**
>
> To find the YubiKey models that support Yubico OTP, see the YubiKey products page.

Configuring YubiKey authentication

Steps

1. In the admin console, go to **Setup → PingID → Configuration**.
2. Go to the **Alternate Authentication Methods** section.



3. In the **Enable** column, select the **YubiKey** check box.
4. Click **Save**.

Result

Users can now pair and authenticate with their YubiKeys.

Configuring OATH token authentication for PingID

An OATH token is a secure one-time passcode (OTP) that can be used for two-factor authentication and is OATH compliant.

Hardware OATH tokens are used where there are no provisions for connection to the Internet, USB connections, or mobile phones, which might be disallowed for security reasons. For more information, see https://openauthentication.org/.

PingID supports hardware OTP tokens that are OATH compliant:

- HOTP SHA-1 devices
- TOTP SHA-1 devices with 30 or 60 second OTP refresh intervals
- Any of the above devices that use a PIN code

PingID does not:

- Sell hardware tokens
- Recommend any particular hardware token manufacturer

The following OATH tokens have been checked for user authentication by PingID.

Manufacturer	Model	Type
Feitian	Display card	TOTP-60-sec
Feitian	OTP c200	TOTP-60-sec
Feitian	Display card	HOTP
Gemalto	EZIO display card	TOTP-30sec
HyperSecu	c100 token	HOTP
HyperSecu	Edge plus	TOTP-60sec
HyperSecu	c200 token	TOTP-30sec
HyperSecu	HyperOTP	TOTP-60sec
HyperSecu	Edge plus	TOTP-30 sec
Protectimus	Protectimus TWO	TOTP-30sec

For information about the user registration, see the PingID End User Guide. NOTE: In the event of three consecutive failed authentication attempts with an OATH token, the user will have to wait two minutes before trying to authenticate again.

Configuring OATH token authentication

Before you begin

To configure OATH tokens, you must have the following items from each token manufacturer and for each supplied token model:

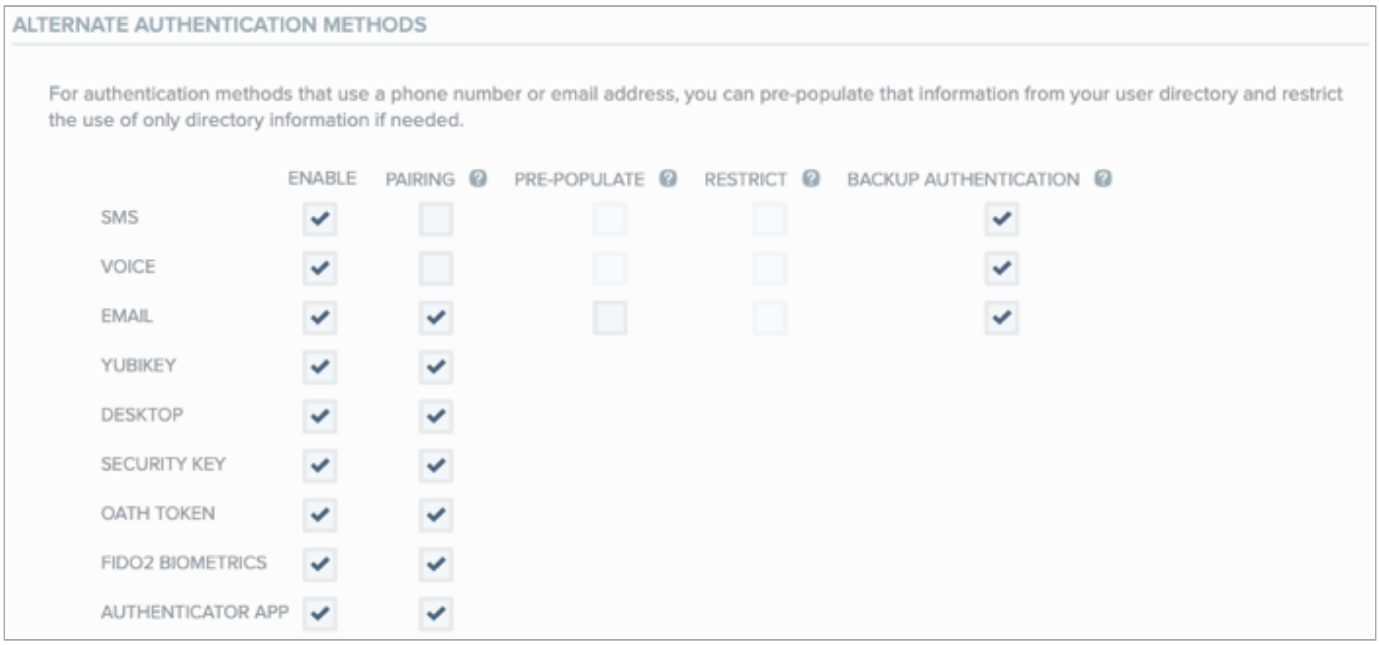
- A token seed file. The seed file can be either:
  - A .txt file consisting of lines with a comma separating the token serial numbers and secret keys (without spaces)
  - A .csv file with the token serial numbers and secret keys in different cells (without spaces or commas)

  The secret keys are strings of hexadecimal digits.
- For each seed file, a single associated token type of either TOTP or HOTP.
- For TOTP types, a refresh interval of 30 or 60 seconds. The default is 30.

> **Note**
>
> For HOTP types, a start counter can appended as an additional field in the seed file. If absent, it defaults to zero.

Steps

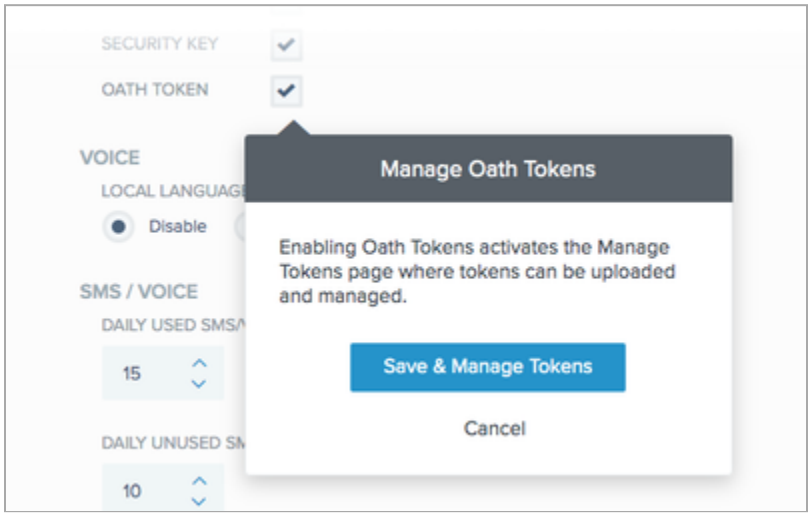
1. In the PingOne admin portal, go to **Setup → PingID → Configuration**.
2. Go to the **Alternate Authentication Methods** section.



3. In the **Enable** column, select the **OATH Token** check box.

   Result:

   The **Manage OATH Tokens** modal opens.

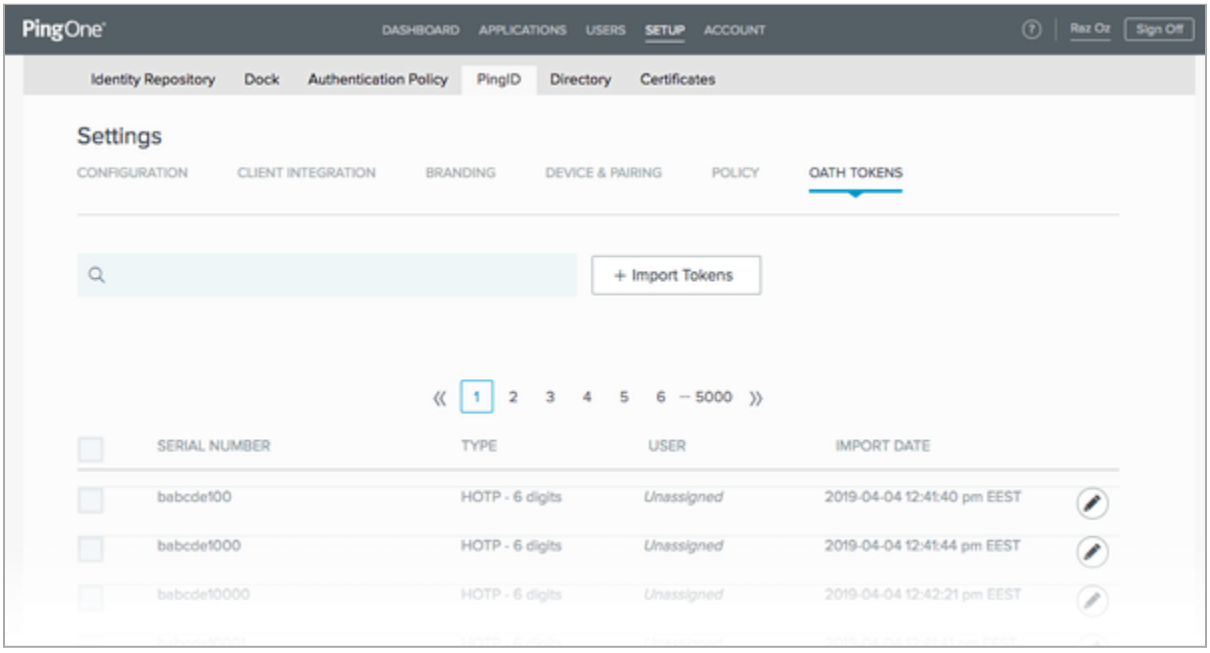


4. Click **Save & Manage Tokens**.

   Result:

   The **OATH Tokens** tab opens and shows a list of previously saved tokens.

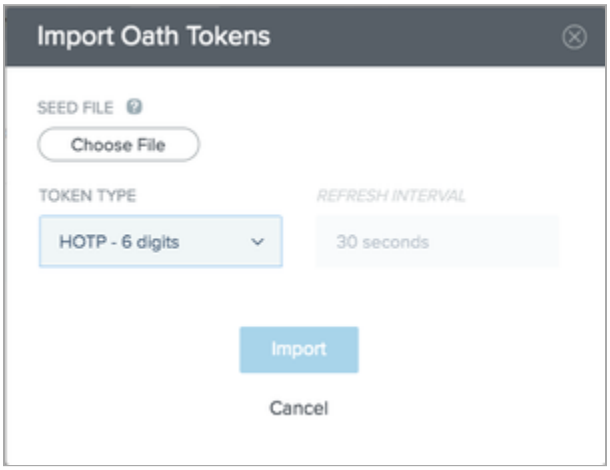
> **Note**
>
> If there are no saved tokens, the list will be empty.



5. Click **+ Import Tokens**.

   Result:

   The **Import OATH Tokens** modal opens.



6. Click **Choose File**.
7. Navigate to your token seed file and select it.

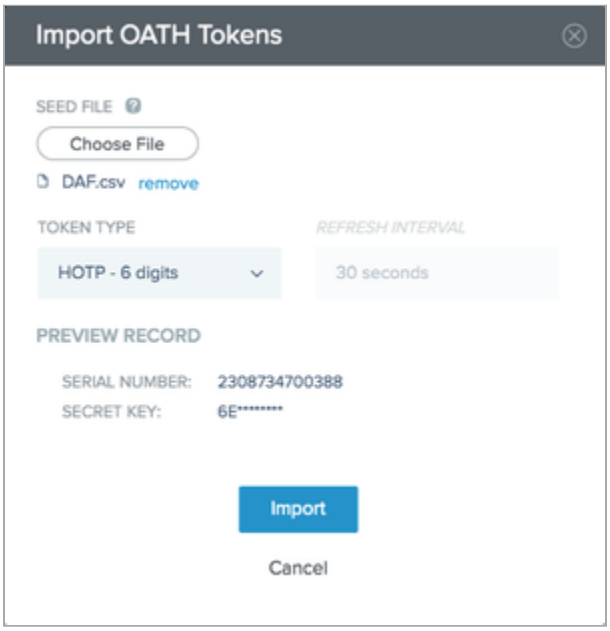
   Example:

   A user imports a single token from a file called `DAF.csv` with the following seed.

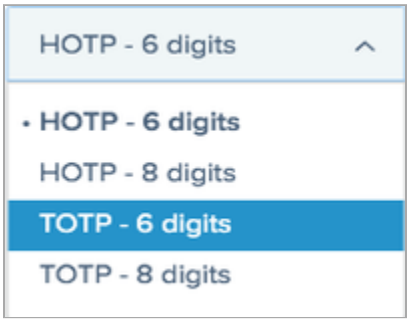
   ```
   2308734700388,6EBD59F71A634C48C4619CB33F6C385C9237C9BA
   ```

   Result:

   The **Import OATH Tokens** modal shows the token information.

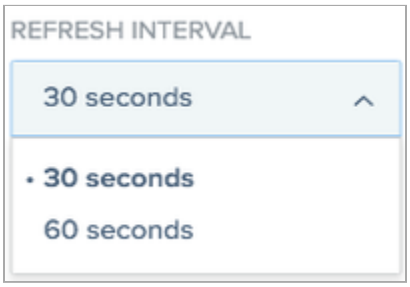


8. From the **Token Type** list, select the token type.



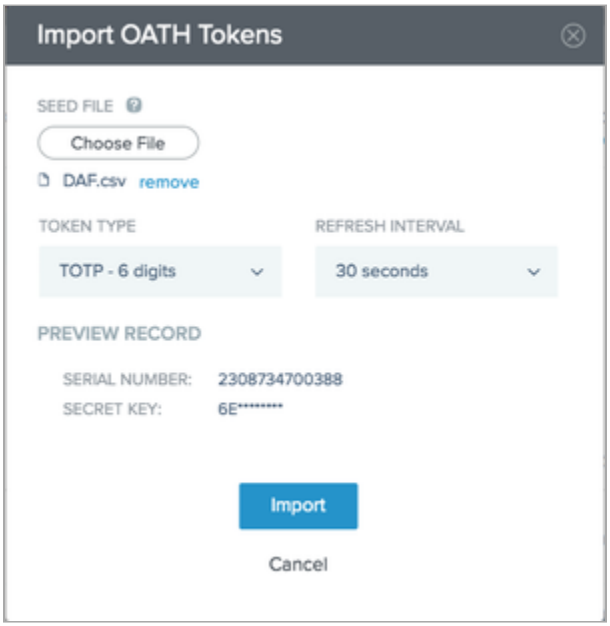
Example:

A selection of **TOTP - 6 Digits** enables the **Refresh Interval** list.



Result:

The **Import OATH Tokens** modal now looks as follows.



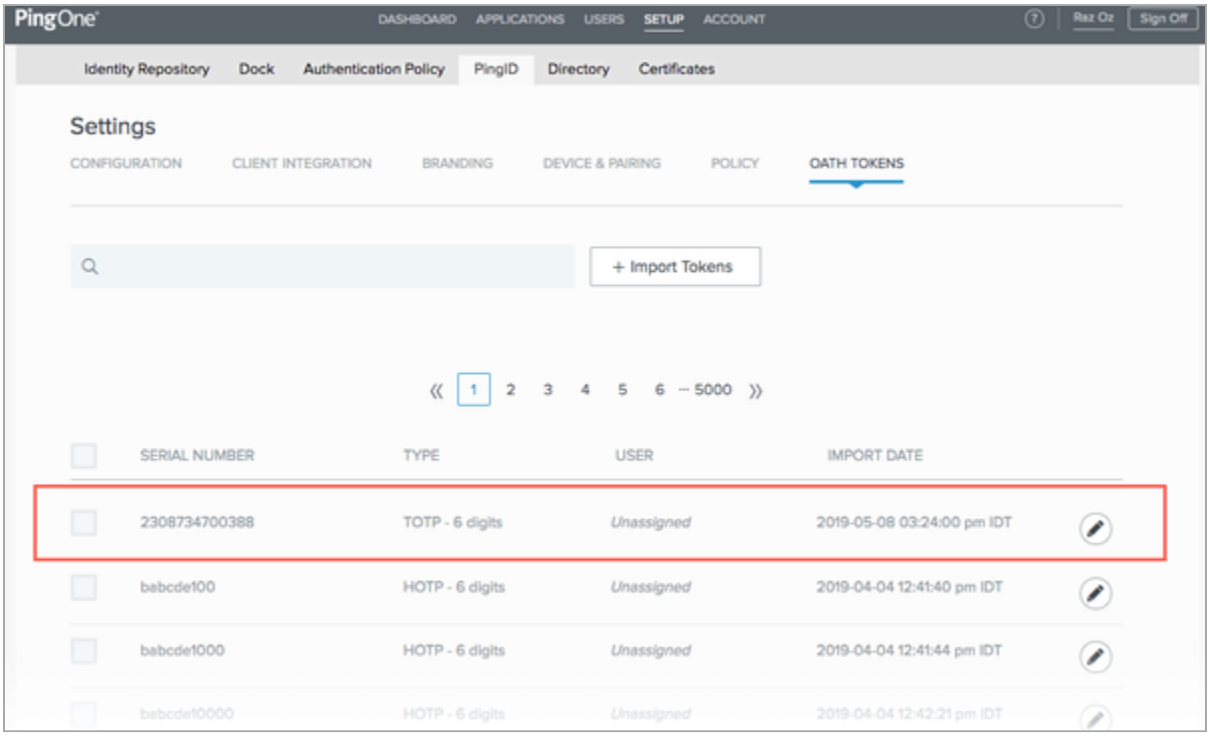
> **Note**
>
> The **Preview Record** section shows information from the first record in the `.csv` file.

9. **Optional:** If applicable, from the **Refresh Interval** list, select the refresh interval.
10. Click **Import**.

> **Note**
>
> To return to the **Import OATH Tokens** modal, go to **Setup → PingID → OATH Tokens**, and then click **+ Import Tokens**.

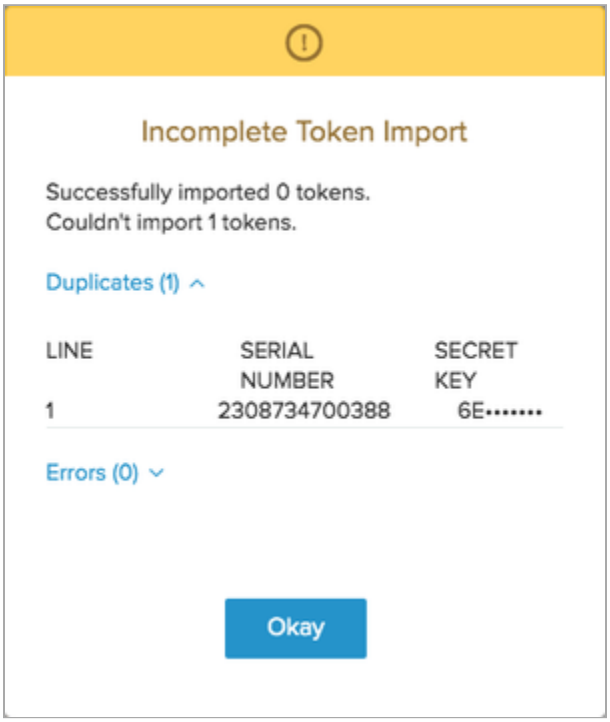
Result:

The newly imported tokens appear at the top of the **OATH Tokens** list.



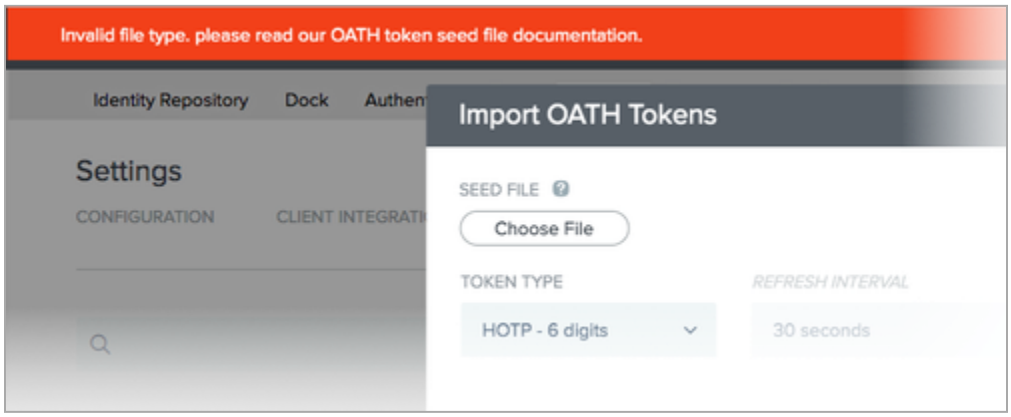
Troubleshooting

- If your seed file contains entries that duplicate existing tokens, the **Incomplete Token Report** error is displayed.



Remove the duplicate entries from the seed file and try again.

- If your seed file is invalid, you will receive the following error message.



Configuring email authentication for PingID

If you have users who use devices that don't support the PingID mobile application, or you want to provide users with an additional authentication option, you can enable email authentication.

When email authentication is configured, and the user signs on to their account or app, they are sent an email with a 6-digit one-time passcode (OTP) to authenticate with. The OTP is valid for up to 30 minutes.

For information about the user experience, see the PingID End User Guide.

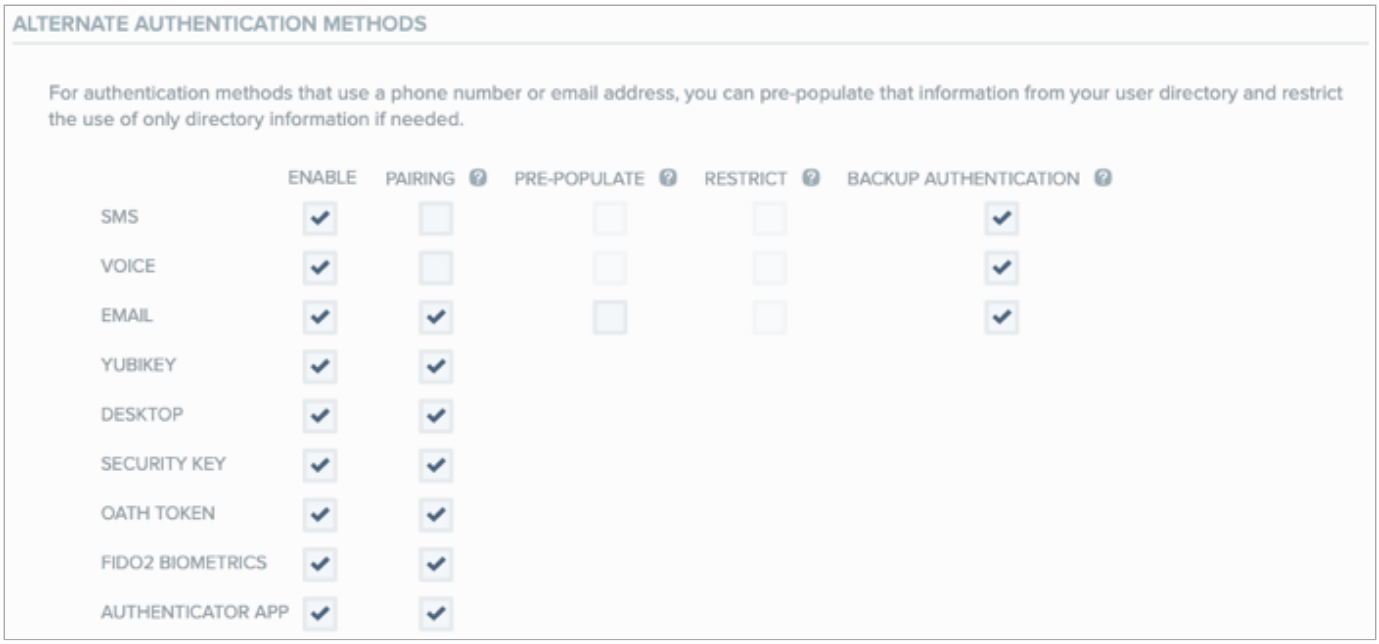
> **Note**
>
> To prevent users from registering their device for Email authentication, and allow existing users to continue to authenticate, see Disabling pairing for a specific authentication method. This option is useful if you want to phase out Email authentication, in favor of more secure authentication methods.

Configuring email authentication

About this task

Steps

1. In the PingOne admin portal, go to **Setup → PingID → Configuration**.
2. Go to the **Alternate Authentication Methods** section.



3. In the **Email** row, select the **Enable** check box.
4. Configure email authentication according to the following table.

Check box	Description
Pre-Populate	To pre-populate the user's field with the email address stored in your user directory, in the **Email** row, select the **Pre-Populate** check box. For more information, see Pre-populating or restricting user registration data.
Restrict	To restrict the user to select only the email address stored in your user directory, in the **Email** row, select the **Restrict** check box. For more information, see Pre-populating or restricting user registration data.

Check box	Description
Backup Authentication	To enable email as a backup authentication method, in the **Email** row, select the **Backup Authentication** check box. For more information, see Configuring backup authentication methods. **Note** You can enable email for backup authentication, even if the **Enable** check box is not selected in the **Email** row.

5. Click **Save**.

> **Note**
>
> If you use email for PingID OTP, for guidance to ensure that your email system will allow delivery of OTP messages, see https://aws.amazon.com/blogs/messaging-and-targeting/amazon-ses-ip-addresses/.

Email customization

Four email customizations are available:

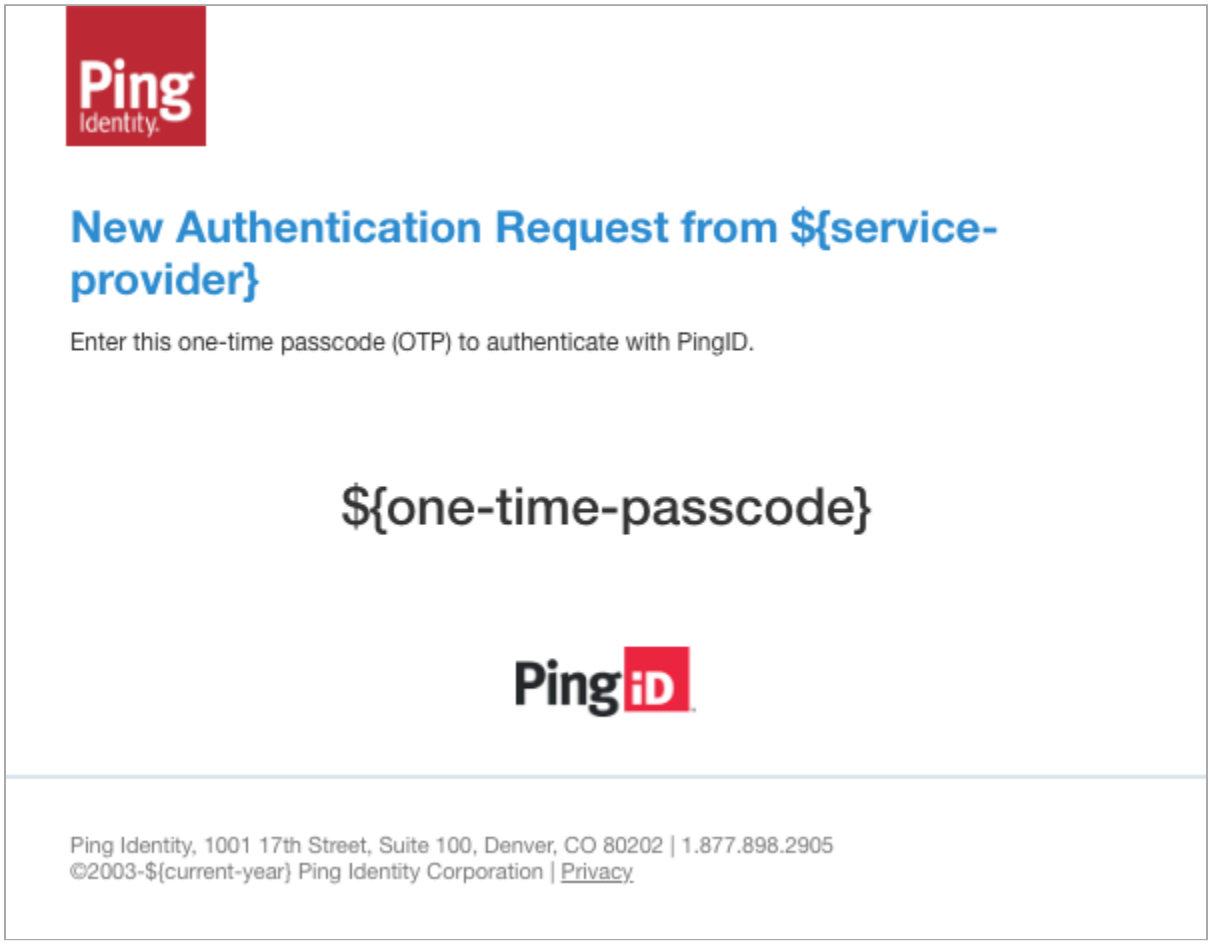
1. Customize the email "From" address to change the default address of `noreply@pingidentity.com` to `noreply@yourdomain.com`.
2. Customize the email "Replyto" address to change the default address of `noreply@pingidentity.com` to `noreply@yourdomain.com`.
3. Customize the email "Subject" line.

> **Note**
>
> To change items 1 to 3 above, sign on to the Ping Identity Support Portal and open a case.

4. Customize the email message body. PingID supplies templates to customize the body of notification mails. To download the templates, see PingID email templates. Download the `.zip` file and extract it. The included `readme.txt` file contains a directory list of templates.

Editing the template for a new authentication request

Open the `New Email Authentication Request.html` file in a text editor. The template is shown in the following image.



This template has two variables, `${one-time-passcode}` and `${service-provider}`. You can replace any of the HTML content, as long as you retain the `${one-time-passcode}` variable. The `${service-provider}` and `${current-year}` variables are optional.

> **Note**
>
> If you include images in any templates, they must be URL references to publicly available assets. Ping Identity does not host the images used in templates.

After making your changes, contact PingID Customer Support to upload the template.

Editing the template for email pairing

Open the `Email Authentication Pairing.html` file in a text editor. The template is shown in the following image.

This template has one mandatory variable, `${one-time-passcode}`. You can replace any of the HTML content, as long as you retain the `${one-time-passcode}` variable. The `${current-year}` variable is optional.

> **Note**
>
> If you include images in any templates, they must be URL references to publicly available assets. Ping Identity does not host the images used in templates.

After making your changes, contact PingID Customer Support to upload the template.

Configuring authenticator app authentication for PingID

You can use PingID with any external authenticator app that can generate a standard time-based one-time password (TOTP), such as Google Authenticator or Microsoft Authenticator.

External authenticator apps are a useful solution in cases such as:

- An organization cannot allow the PingID mobile app on their devices, as PingID must be added to the allow list.
- An organization wants to use a single authenticator app and has users that must authenticate to multiple organizations.

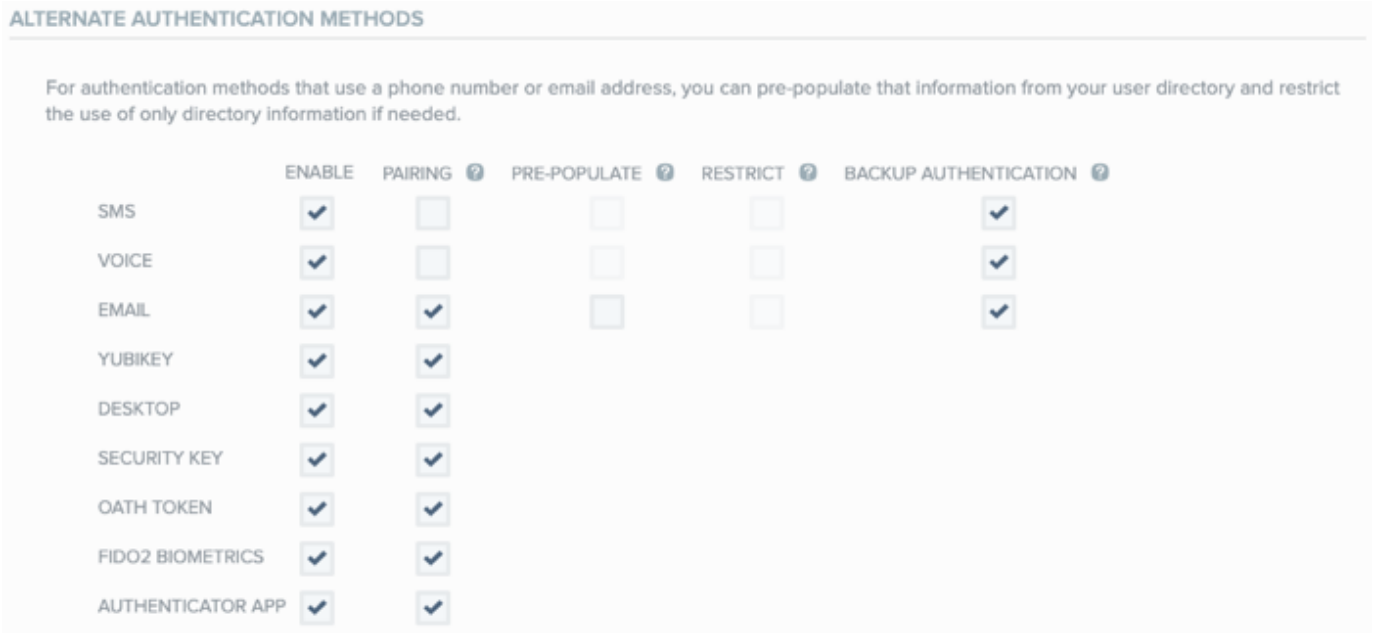
Users can use an authenticator app to access an account or application through the web, VPN, Mac login, or SSH. When authentication app authentication is enabled, users can download the authenticator app of their choice and pair it with their PingID account. Users can pair more than one authenticator app with their account.

For more information, see the PingID End User Guide.

Configuring authenticator app authentication

Steps

1. In the admin portal, go to **Setup → PingID → Configuration**.
2. Go to the **Alternate Authentication Methods** section.

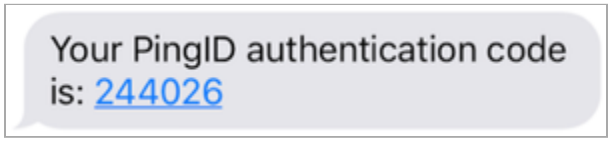


3. In the **Authenticator App** row, select the **Enable** check box.
4. Click **Save**.

SMS and voice authentication

You can enable SMS or voice authentication for users without devices that support the PingID mobile application.

When configured, a 6-digit one-time passcode (OTP) is sent to the user's mobile device or landline phone, using SMS or telephony voice channels. The OTP is valid for up to 30 minutes.



You can:

- Specify or restrict the user to a specific phone number. For more information, see Pre-populating or restricting user registration data.
- Localize voice authentication calls to match the language defined in the browser from which the user authenticates. For more information, see Enabling language localization for voice authentication.

To view usage limits for SMS and voice, see SMS and voice usage limits.

> **Note**
>
> To prevent users from registering their device for SMS or voice authentication, and allow existing users to continue to authenticate, see Disabling pairing for a specific authentication method. This option is useful if you want to phase out SMS and voice authentication, in favor of more secure authentication methods.

The following list describes the conditions and limitations of SMS and voice authentication:

- Phone numbers with extensions are supported for voice calls. The phone number must be followed by a comma and the extension number. For example:
  - The phone number +12025550123 with the extension 2992 is entered as +12025550123,2992.
  - The extension can include the # or * characters. For example, +12025550123,#2992 or +12025550123,2992#.
  - If there is more than one extension, a comma should separate the extension and the nested extension. For example, +12025550123,#2992,#2991.
  - Each comma generates a 2-second pause. After the call is answered, the extension is dialed after 2 seconds. If a pause is required for longer than 2 seconds, add an additional comma for each additional 2-second pause. For example, in +12025550123,#2992,,,#2991, three commas generate a 6-second pause before the nested extension.
- Virtual numbers are not supported, and delivery success rates for virtual numbers are therefore likely to be lower than fixed numbers.
- Because of Chinese regulatory limitations, use of voice OTPs in China is disabled.
- In some cases, SMS OTPs in China may be blocked because of Chinese regulatory limitations. Therefore, it is recommended to use the Twilio Verify service in China. To enable this service, contact your Ping Identity sales representative.
- In India and Saudi Arabia, PingID sends OTPs through SMS in transactional mode.
- Twilio doesn't support the use of SMS OTPs in Iran. For users in Iran, if the first attempt to request an OTP using SMS fails due to this limitation, sending the request a second time triggers fallback to Vonage, which does support the use of SMS OTPs in Iran.
- Transactional SMS messages include "PingID" as part of the sender ID.
- Customers that are using Ping Identity's SMS default account might receive SMS messages from a pre-registered alphanumeric Sender ID. This is necessary in countries with regulations that require Ping Identity to use a pre-registered Sender ID. For a list of requirements by country, see Twilio requirements s and Vonage requirements.
- Additional sender ID numbers are available for the PingID SMS and voice OTP services so users can receive OTP text messages or voice calls from a different number. Generally, after the new number is set, the user will receive the PingID SMS or voice OTP from that number in the future. In cases of SMS or voice delivery technical issues, the user can receive the OTP text messages or voice calls from a new number, provided by a fallback SMS provider.

> **Note**
>
> Voice authentication end users should change their voicemail password from their device default, or disable voicemail if using PingID voice OTP. An attacker could potentially direct an OTP voice call to a voicemail by calling the victim at the same time. In the event of an attack, the OTP will be recorded in the voicemail and will be subject to its password protection.

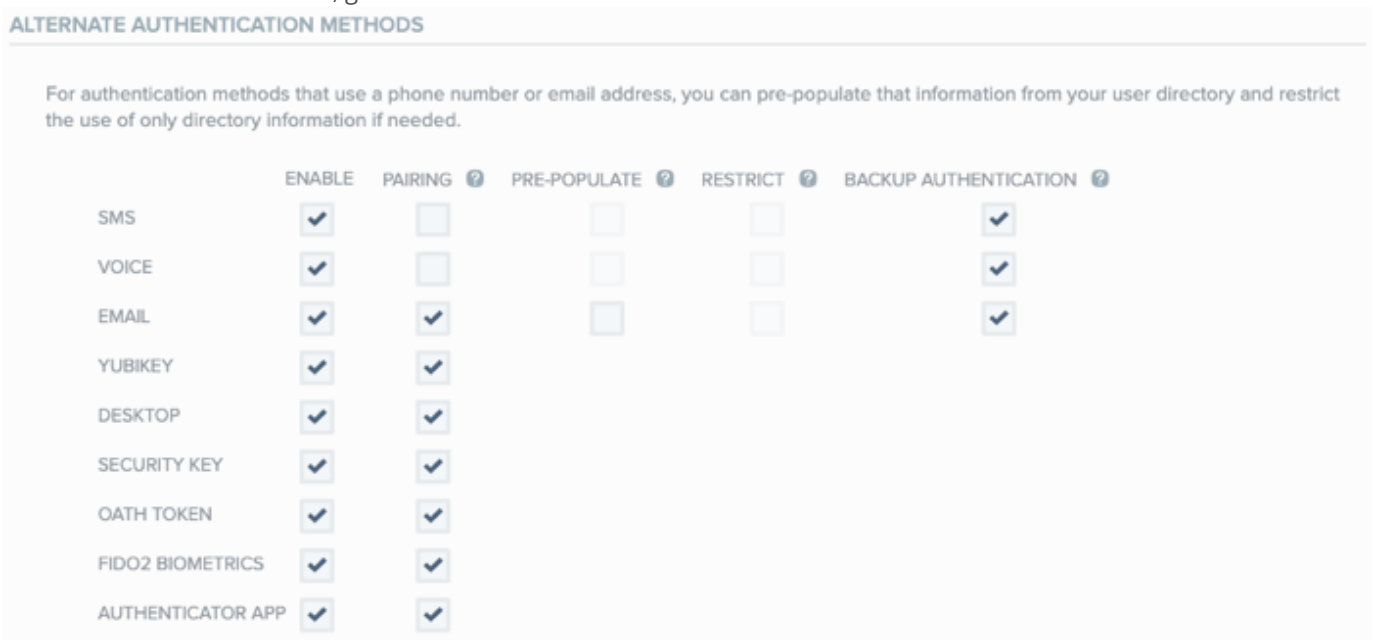
For information about the user experience, see the PingID End User Guide.

Configuring SMS and voice authentication for PingID

You can enable SMS or voice authentication with PingID.

Steps

1. In the admin console, go to **Setup → PingID → Configuration**.
2. In the **Authentication** section, go to **Alternate Authentication Methods**.



3. Select the authentication methods you want to enable.

Option	Steps
SMS	In the **SMS** row, select the **Enable** check box.
Voice	In the **Voice** row, select the **Enable** check box.

4. Configure SMS and voice authentication according to the following table.

Option	Steps
Pre-populate the user's field with the SMS or voice numbers stored in your user directory when registering for PingID.	In the relevant row, select the **Pre-Populate** check box. For more information, see Pre-populating or restricting user registration data.
Restrict the user to select only the SMS or voice phone numbers stored in your user directory when registering with PingID.	In the relevant row, select the **Restrict** check box. For more information, see Pre-populating or restricting user registration data.

Option	Steps
Enable the SMS or voice entries stored in your user directory to be used as a backup authentication method.	In the relevant row, select the **Backup Authentication** check box. For more information, see Configuring backup authentication methods. **Note** You can enable SMS or voice for backup authentication even if the **SMS** or **Voice** check boxes are not selected.
Change the daily limit for SMS/voice messages.	◦ In the **Daily Used SMS/Voice Limit** field, enter the maximum number of SMS authentication requests the user can receive and respond to per day. Enter a number between 1 and 50. The default value is 15. ◦ In the **Daily Unused SMS/Voice Limit** field, enter the maximum number of SMS authentication requests the user can receive and not respond to per day. Enter a number between 1 and 50. The default value is 10. ◦ If you want to also place a limit on the number of SMS-based and voice-based pairing requests for a user, select the**Enforce for pairing requests** option. When you enable this option, the number of pairing requests is added to the number of authentication requests and the total cannot exceed the limits that you set.
Localize voice calls to the language defined by the user's browser.	In the **Local Language For Voice Calls** section, select **Enable**. If **Disable** is selected, or the user's browser settings use a language is not one of the supported languages, English is selected by default. This section is only applicable when the **Voice** check box is selected. **Note** For a list of supported languages, see Enabling language localization for voice authentication.

5. Click **Save**.

Enabling language localization for voice authentication

If voice is selected as an alternate authentication method, enable localization of the voice message a user receives.

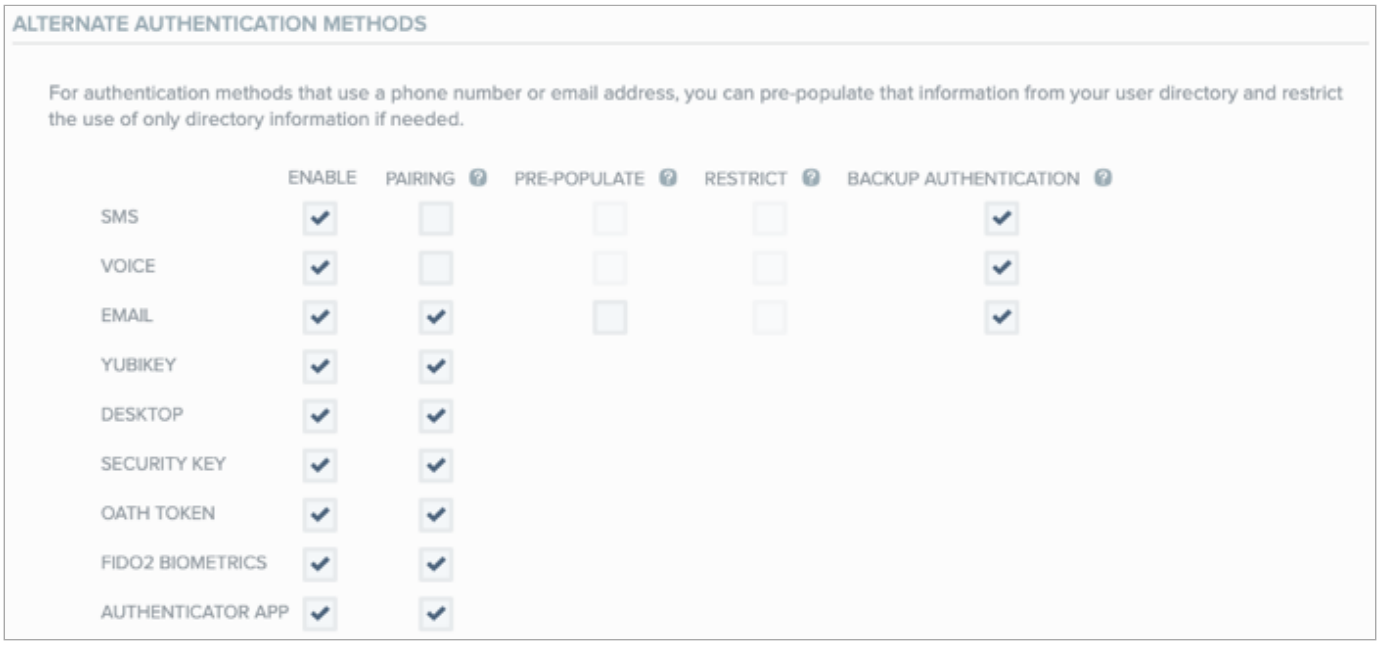
About this task

The language is defined by the language settings of the web browser from which the user initiated the authentication request. PingID provides customizable message texts for each of the supported languages. Currently supported languages are listed in PingOne for Enterprise language support.

If the user's browser is set to a language that is not supported, English is used.

Steps

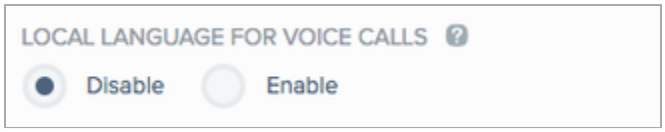
1. In the PingID admin portal, go to **Setup → PingID → Configuration**.
2. In the **Authentication** section, go to **Alternate Authentication Methods**.



3. In the **Enable** column, make sure the **Voice** check box is selected.

   Result:

   The **Local Language For Voice Calls** field is displayed.



4. To localize voice calls to the language defined by the user's browser, from the **Local Language For Voice Calls** section, select **Enable**.

> **Note**
>
> If the language used in the browser is not one of the supported languages or if **Disable** is selected, the default language of English is used.

5. Click **Save**.

Enabling and customizing language localization for SMS authentication in PingID

If SMS is selected as an alternate authentication method, enable localization and customization of the SMS message a user receives.

Language localization applies to both registration and authentication. The language is defined by the language settings of the web browser on the device from which the user initiated the authentication or registration request. For a list of supported languages, see PingOne for Enterprise language support.

> **Note**
>
> - If the user's browser is set to a language that is not supported, the default language of English is used.
> - All account types support localization. Customization is supported for full accounts only.
> - SMS messages longer than 67 characters might incur additional charges. The SMS service provider might split longer messages into several shorter messages, each billed on its own.

When localizing or customizing the SMS messages:

- You can enable localization only using predefined messages for all supported languages. For more information, see Enabling language localization for SMS authentication.
- You can use the basic online SMS message editor. For more information, see Managing online customization of the SMS authentication message.
- You can use offline editing for multiple-language SMS messages with language inclusion and exclusion. For more information, see Managing offline customization of the SMS authentication message.

Enabling language localization for SMS authentication

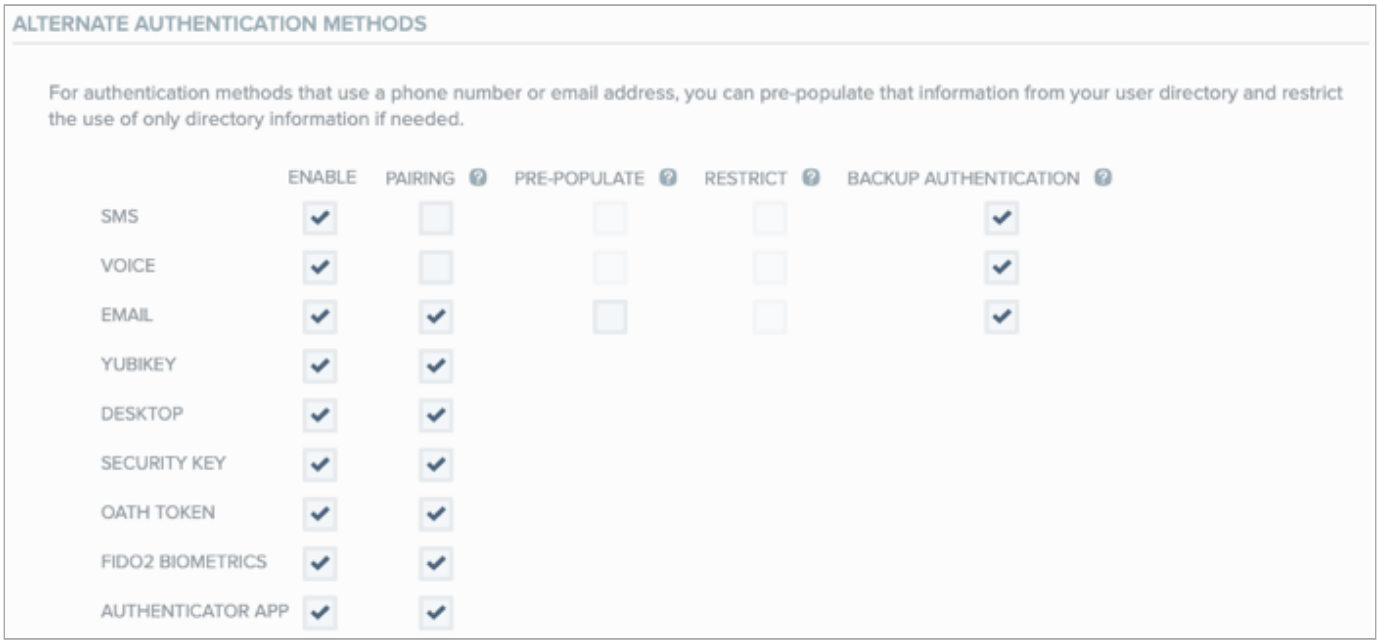
Enable localization to ensure that SMS messages on a user's device will appear in the language set for the device browser.

About this task

If the language used in the browser is not one of the supported languages, the default language of English is used.

Steps

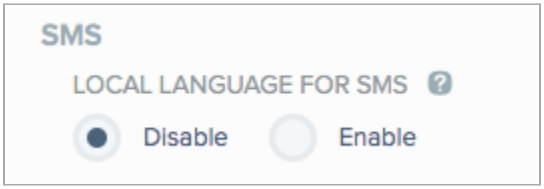
1. Sign on to the admin console.
2. In the PingID admin portal, go to **Setup → PingID → Configuration**.
3. In the **Authentication** section, go to **Alternate Authentication Methods**.



4. In the **Enable** column, ensure that **SMS** is selected.

   Result:

   The **Local Language For SMS** section is displayed.



5. To enable language localization, click **Enable**.
6. Click **Save**.

Managing online customization of the SMS authentication message

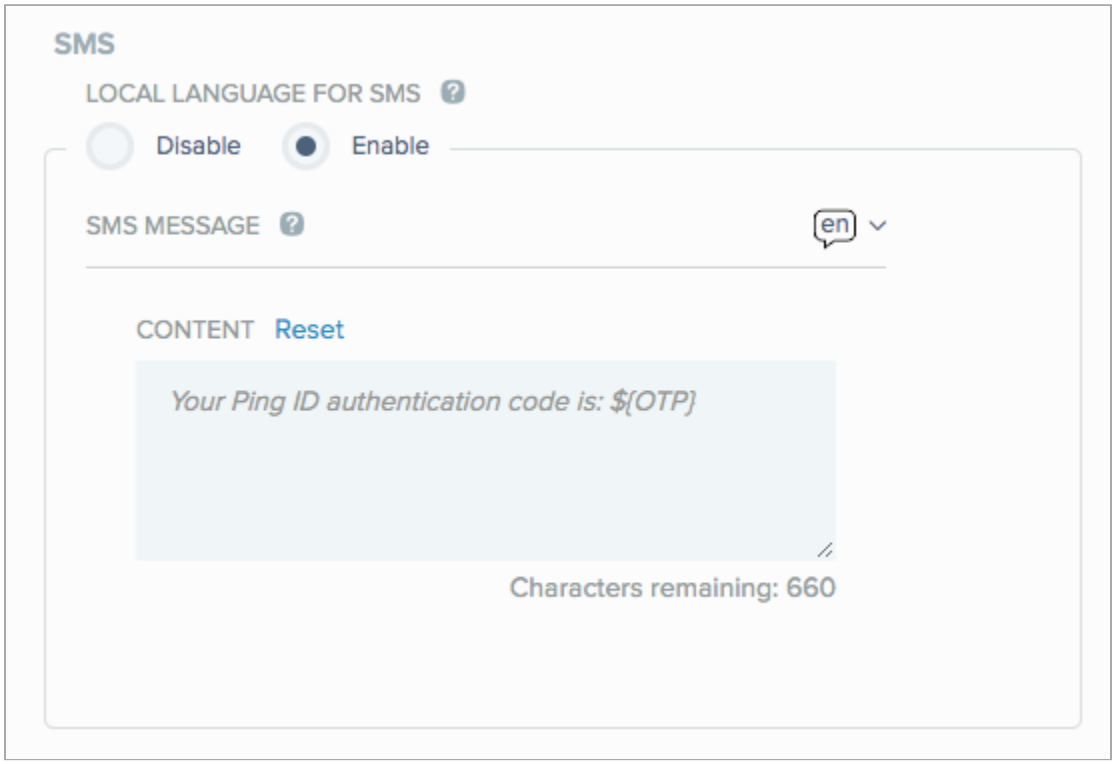
You can customize the SMS authentication message in the PingID admin portal.

Steps

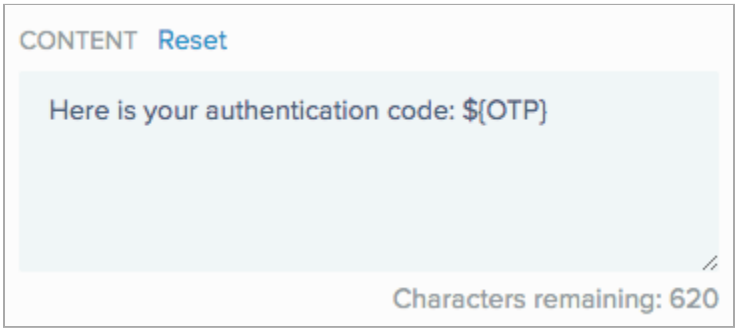
1. Follow steps 1-5 of Enabling language localization for SMS authentication.

   Result:

   The **Local Language For SMS** section expands.

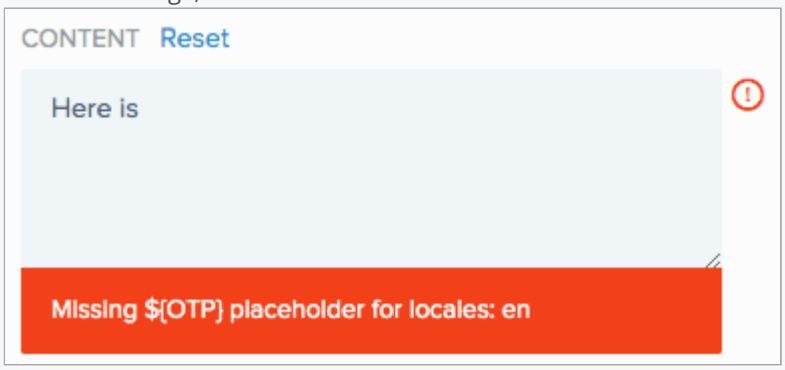


2. In the **Content** field, configure the SMS authentication message, or accept the default.



Note

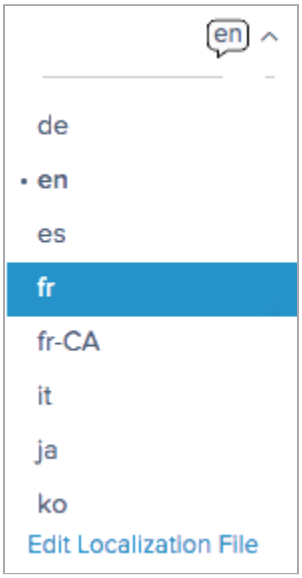
The editor will display an error message if the one-time passcode (OTP) system variable is missing. The variable must be surrounded curly braces and can be upper or lower case, such as `${OTP}`.
To revert back to the default message, click **Reset**.



3. Click **Save**.

Next steps

To customize additional languages, click the **Language** icon, and then select a language from the list.



Edit the SMS message as described previously, and then click **Save**.

> **Note**
>
> If your locale does not allow you to type in the language of choice, you must use the offline method described in Managing offline customization of the SMS authentication message.

Managing offline customization of the SMS authentication message

Offline customization provides a central place to manage all of your PingID localizations and allows for the inclusion and exclusion of languages.

About this task

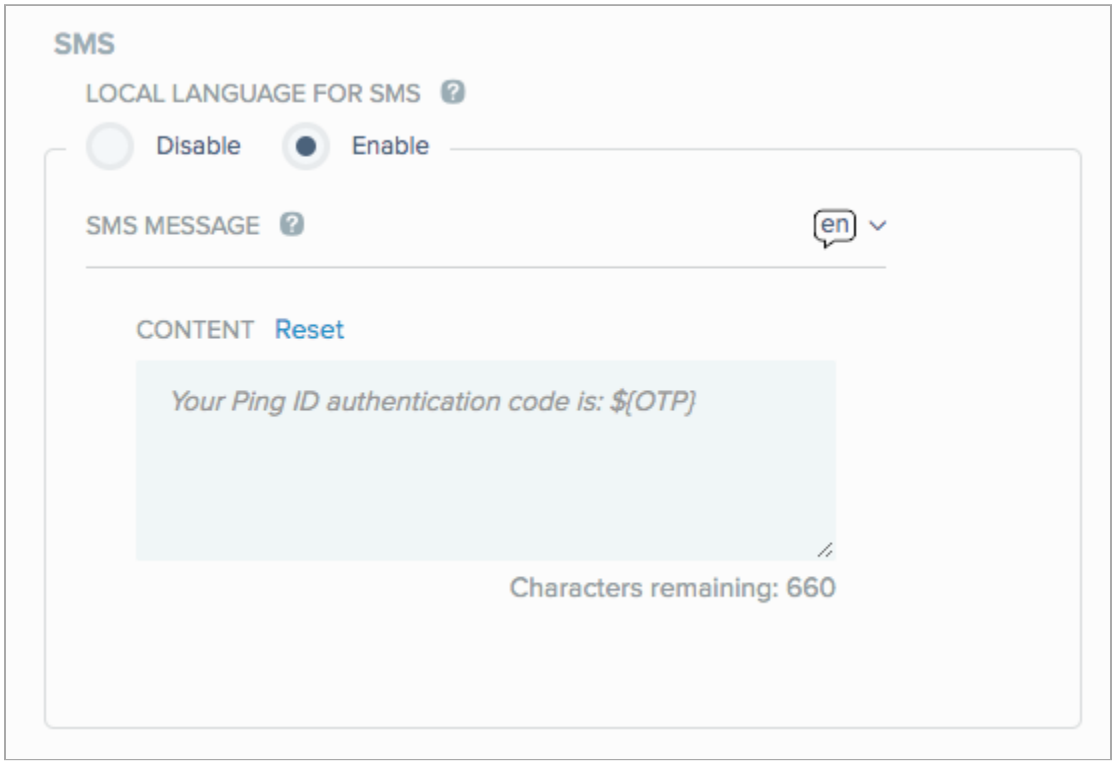
To edit language messages outside of your selected language, download the message `.zip` file, extract the message files, edit them, rebuild the .zip file, and upload it to the PingID admin portal.

Steps

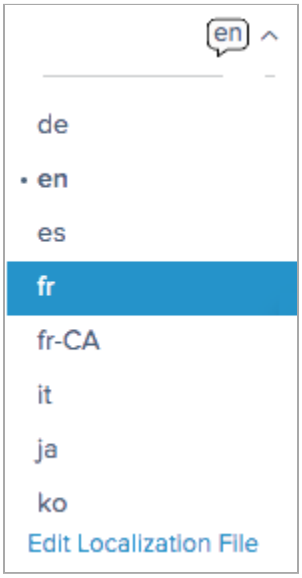
1. Follow steps 1-5 of Enabling language localization for SMS authentication.

   Result:

   The **Local Language For SMS** section expands.



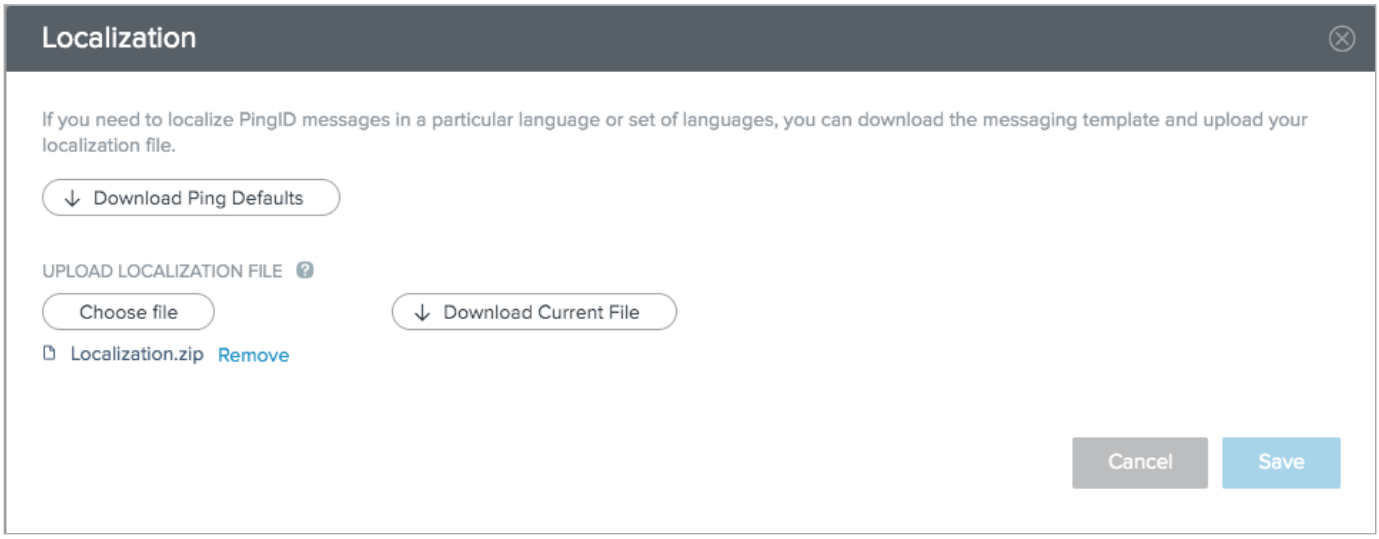
2. Click the **Language** icon, and then select a language from the list.



3. To start the offline customization procedure, click **Edit Localization File**.

   Result:

   The **Localization** window opens.



4. For first-time customization, click **Download Ping Defaults**. If you are continuing from an earlier customization, click **Download Current File**.

   Choose from:

   - **Download Ping Defaults**: You receive a file called `LocalizationsTemplate.zip`.
   - **Download Current File**: You receive a file called `Localizations.zip`.

     The `LocalizationsTemplate.zip` file contain a properties text file for each supported language.

     Localization_de.properties
     Localization_en.properties
     Localization_es.properties
     Localization_...ca.properties
     Localization_fr.properties
     Localization_it.properties
     Localization_ja.properties
     Localization_ko.properties
     Localization_nl.properties
     Localization_pt.properties
     Localization_ru.properties
     Localization_th.properties
     Localization_tr.properties
     Localization_zh.properties

     Each of the properties files is a text file with the same layout.

```
pingid.sms.msg.authentication=Your Ping ID authentication code is: ${OTP}
pingid.enrollment.content.description=Great news! Your company is giving you the simplicity of
PingID, so you can sign on to all your applications with the added security of a swipe on your
mobile device. Enter your email address, and we'll send you a link to download PingID.
pingid.non.app.enrollment.text=I want to use a different authentication method.
```

5. Extract the `.zip` file.

As a concrete example, we will edit the English file and remove several languages.

1. Open `Localization_en.properties` in a text editor.
2. Locate the line commencing with `pingid.sms.msg.authentication=`.
3. Change the line to your desired message, such as `pingid.sms.msg.authentication=Here is your Ping ID authentication code: ${OTP}`.

   There are several rules for editing language properties files and creation of the `.zip` file:

   - The OTP variable is in curly braces \{..}
   - Do not edit the other lines because they are used in other parts of the system.
   - You can revert the SMS authentication message to the default for the language by setting `pingid.sms.msg.authentication=` (without a value) or simply deleting the line.
   - The `.zip` file must be a flat structure containing only the desired language files, without any folder structures. Attempts to upload invalid `.zip` structures returns the error message: `File doesn't contain any valid localizations`.
   - Only files with filenames complying with the `Localization_<locale>.properties` naming convention are uploaded.
   - Files whose filenames do not comply with the `Localization_<locale>.properties` naming convention are ignored. This permits inclusion of instruction and maintenance files in the `.zip`, for example `readme.txt`.
   - Localization files for unsupported locales are ignored.

   > **Caution**
   >
   > The localization properties files are shared across several customizations, currently SMS and Enrollment co-branding. For more information, see Customizing the PingID enrollment page (legacy).

4. Save the file.
5. To remove several languages, in the directory of properties files, delete all of the files except the following:

   Localization_de.properties
   Localization_en.properties
   Localization_fr.properties
   Localization_it.properties
   Localization_nl.properties
   Localization_pt.properties

6. Pack the remaining properties into a new `.zip` file, and give it a new name, such as `Localizations_<ABC>.zip`

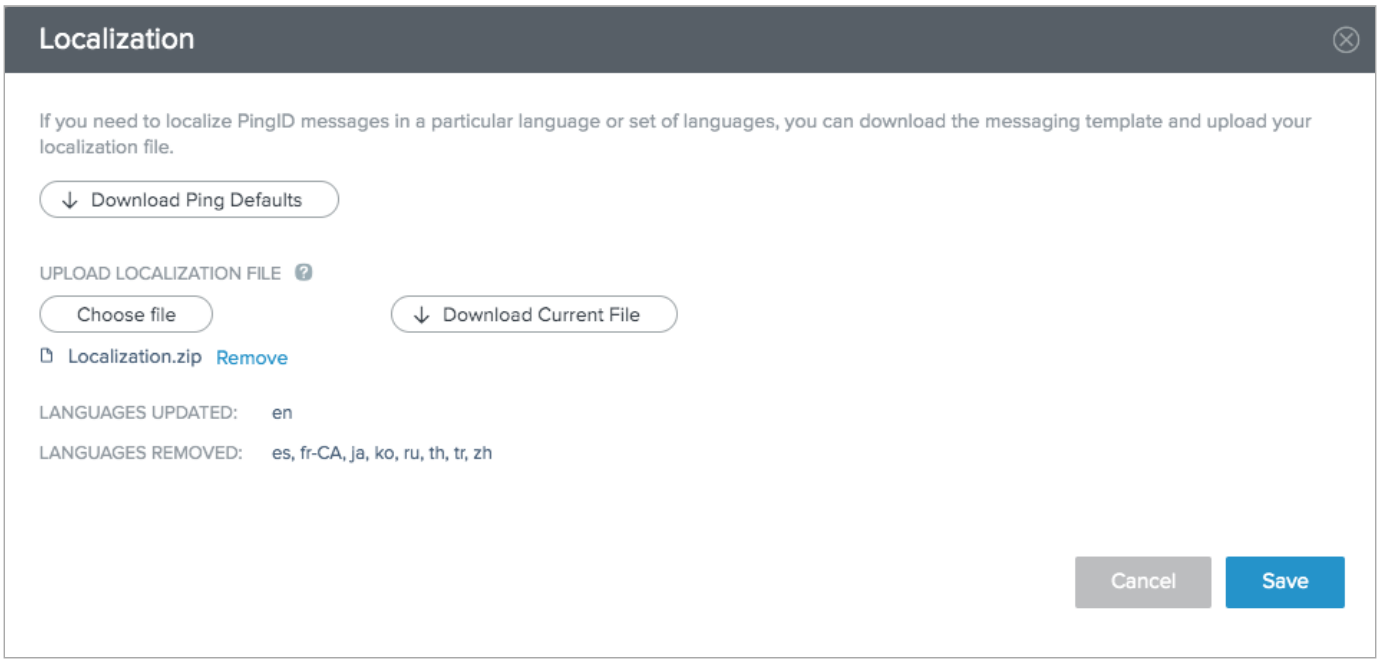
   The name is unimportant because it is not preserved in the system.

> **Important**
>
> The `.zip` file must be a flat structure containing only localization properties files and without any folder structures.
>
> - Attempts to upload invalid zip structures returns the error message: `File doesn't contain any valid localizations`.
> - Only files with filenames complying with the `Localization_<locale>.properties` naming convention are uploaded.
> - Files whose filenames do not comply with the `Localization_<locale>.properties` naming convention are ignored. This permits inclusion of instruction and maintenance files in the `.zip`, for example `readme.txt`.
> - Localization files for unsupported locales are ignored.

6. Upload your new `Localizations_<ABC>.zip` file.
7. In the PingID admin portal, go to the **Localization** window, and then click **Choose File**.
8. Select `Localizations_<ABC>.zip`.

   Result:

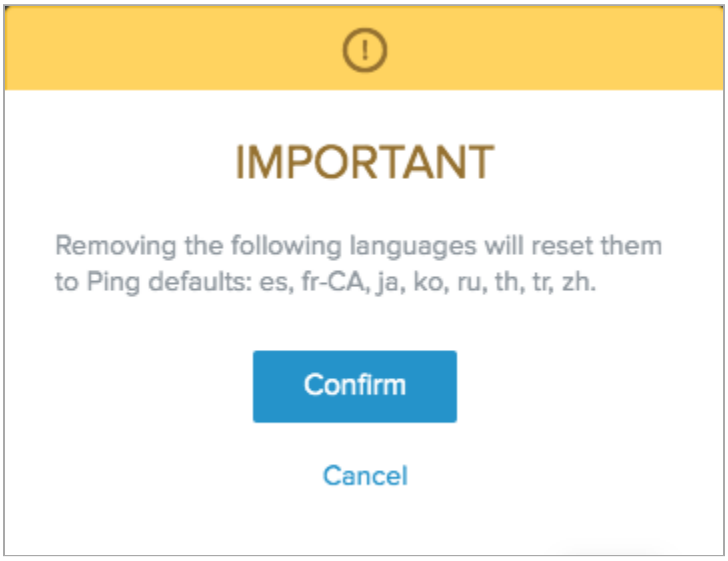
   You are shown confirmation.



9. Click **Save**.

   Result:

   You are asked for final confirmation.



10. To complete the procedure, click **Confirm**.
    - If there are no language removals, you must click **Save** to complete the upload.
    - You can return to edit your localizations. In step 2, click **Download Current File**. The downloaded file is always called `Localizations.zip`. Then proceed from step 3.
11. Go to **Setup → PingID → Configuration** and confirm your edit by checking your SMS message settings.

Offline customization: additional actions

For additional tasks for offline customization of the SMS authentication message, see the following sections.

Restoring a previously removed language

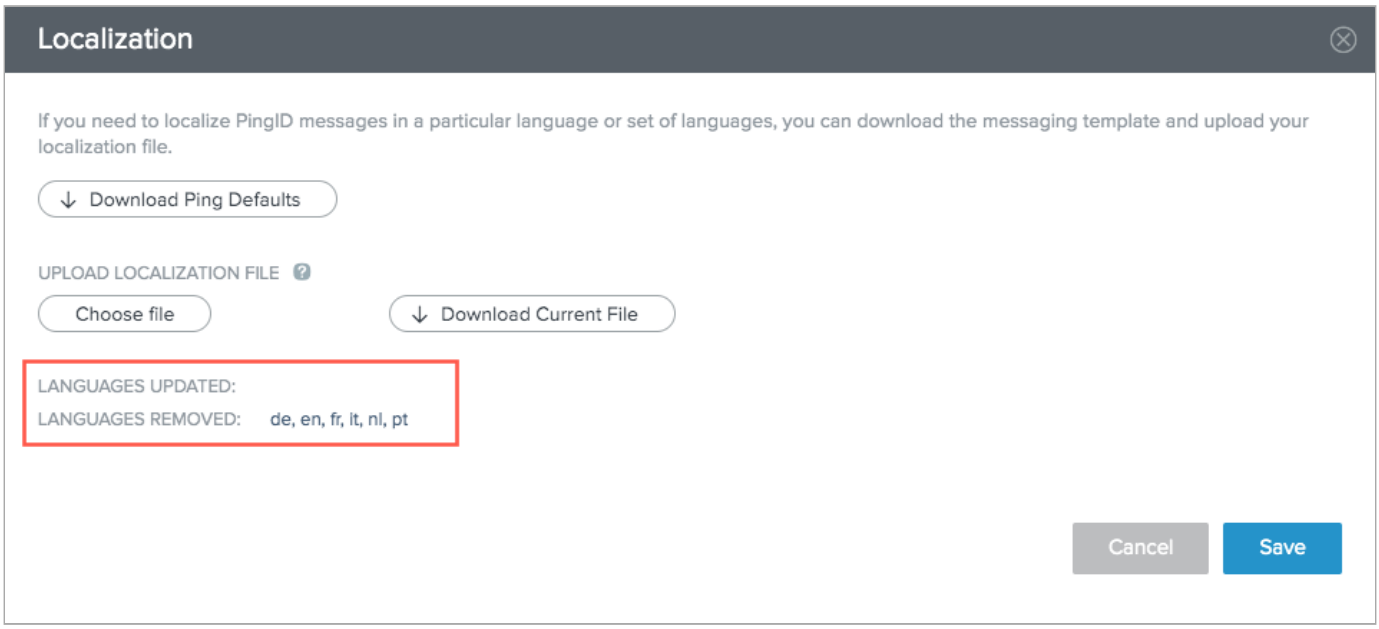
1. In the admin portal, go to the **Localizations** window.
2. Click **Download Current File** and extract it.
3. If you do not have the default `.zip` file, click **Download Ping Defaults**.
4. Copy the relevant language properties file from the template to your extracted files directory.
5. Edit the language properties files as required.
6. Rebuild the `.zip` properties file.
7. Upload the zipped file.

Reverting to default languages and SMS texts

> **Note**
>
> The following steps use the example in Managing offline customization of the SMS authentication message.

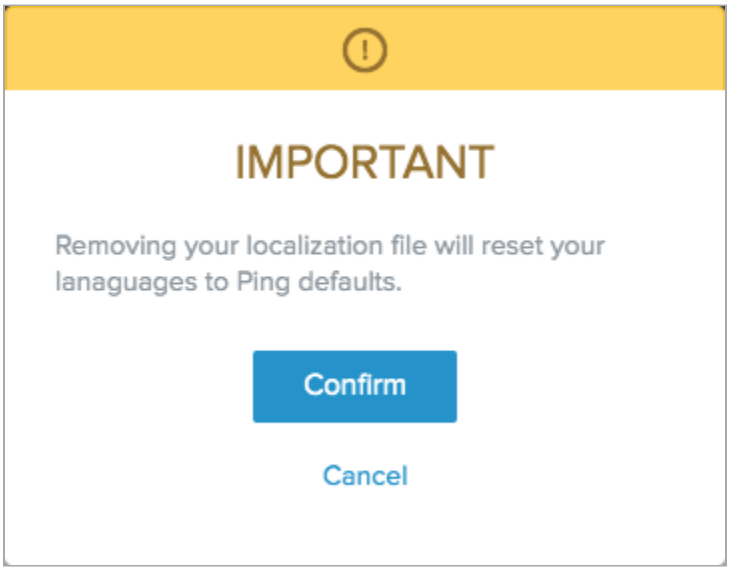
1. In the admin portal, go to the **Localizations** window.
2. Under **Choose File**, click **Remove**.

   The proposed action is summarized.



3. Click **Save**.

   A confirmation window opens.



4. Click **Confirm**.

   All languages become available with their default SMS messages.

Using a custom Twilio account with PingID

If you have an existing custom Twilio account, you can configure PingID to use it for SMS or voice authentication.

The following conditions apply:

- **Daily used SMS/voice limits:** These limits are not enforced for Twilio accounts. For more information, see SMS and voice usage limits.
- **Billing:** You must set up your Twilio billing arrangements before configuring PingID to use your account.
- **Multiple Twilio accounts:** If you have several Twilio accounts, you can only use one of them. If you have sub-accounts, you can use either:
  - The main account
  - A single sub-account of the main account
- **Inactive PingID Accounts:** Only an administrator can delete a Twilio account configuration in PingID if the PingID account becomes inactive. To delete a custom Twilio account from PingID, see Managing a Twilio account.
- **Preregistering a Sender ID**: Customers using a custom Twilio account should be aware that some countries require SMS messages to be sent using a preregistered alphanumeric Sender ID. For information, see Twilio requirements by country.

To configure a custom Twilio account, see Configuring a Twilio account.

To manage a custom Twilio account, see Managing a Twilio account.

Configuring a Twilio account

Before you begin

- Ensure that you have your Twilio account SID and Auth Token available. You can copy them from the Twilio dashboard.
- Configure one or more origination phone numbers.

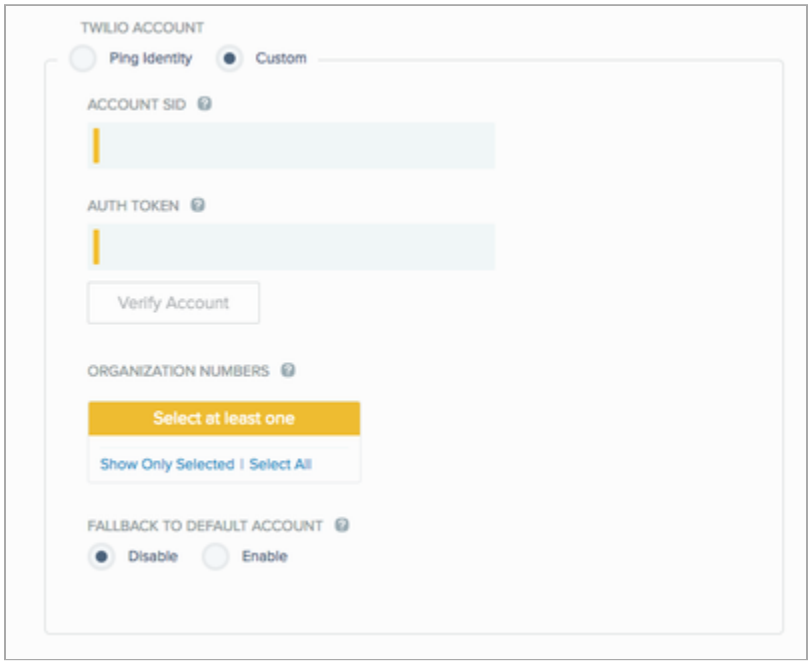
About this task

> **Note**
>
> PingID uses Twilio for voice and SMS. By enabling your own Twilio account, you are taking responsibility for sending SMS and voice messages.

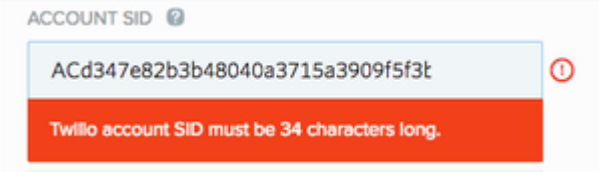
To configure PingID to use a Twilio account:

Steps

1. In the PingID admin portal, go to **Setup → PingID → Configuration**.
2. Go to the **Alternate Authentication Methods** section and ensure that **SMS** or **Voice** is checked.
3. In the **Twilio Account** section, select **Custom**.



4. In the **Account SID** field, enter your Twilio account SID.

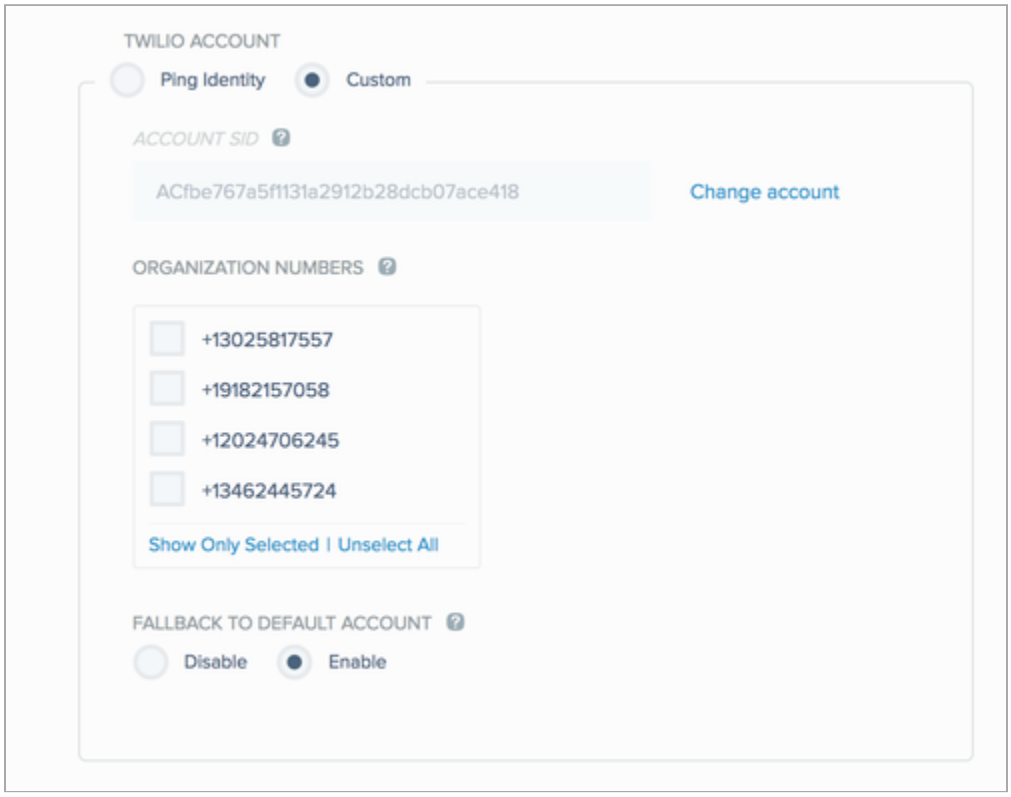
> **Note**
>
> If the SID is less than 34 characters, the following error message is displayed.
>
> 
>

5. In the **Auth Token** field, enter your Twilio Auth Token.

6. Click **Verify Account**.

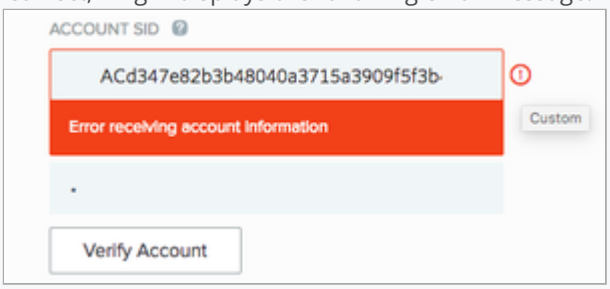
   Result:

   If the account was successfully verified, the Twilio account is validated to PingID, and the **Organization Numbers** list displays a list of originating numbers from Twilio.



Note

- If there are no originating phone numbers in the Twilio account, it does not validate to PingID.
- If the Auth Token is incorrect, PingID displays the following error message.



7. From the **Organization Numbers** list, select at least one originating telephone number to use.

Note

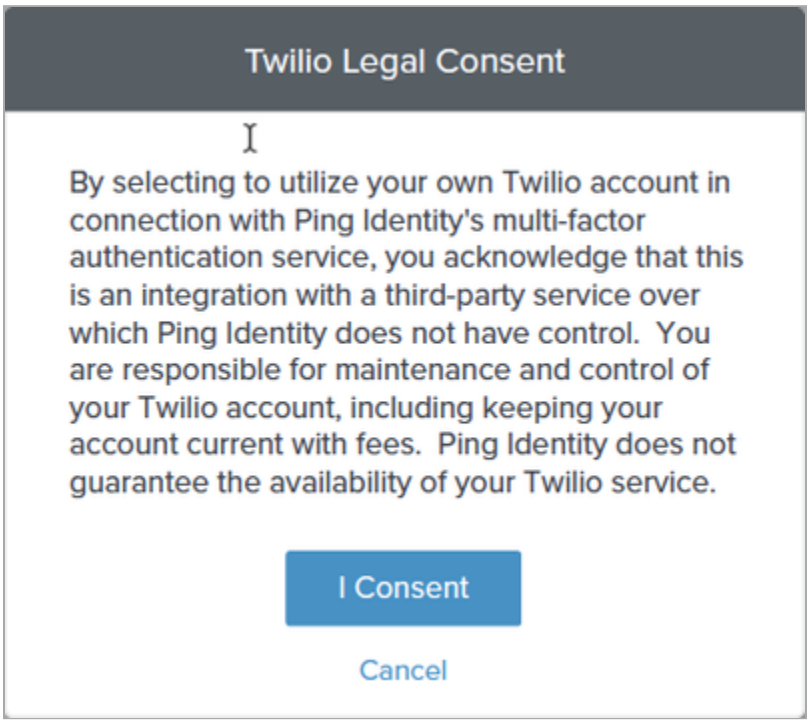
- Twilio allows you to define phone numbers for use with either voice, SMS, or both. PingID uses the same number for both voice and SMS and will relate to the Twilio defined numbers. Twilio numbers that are defined as voice-only or SMS-only are filtered out from the numbers list to avoid operational errors.
- Twilio allows the use of sender IDs in place of telephone numbers for commercial use or to comply with regulations requiring SMSs to be sent as **transactional**, rather than **promotional**.

When using the PingID account, all originating numbers are defined as transactional with a senderID in Twilio. To achieve the same functionality in a custom Twilio account, you must configure it directly in Twilio. ** PingID does not display sender IDs defined in Twilio. PingID displays phone numbers, as shown in step 6.

8. To fall back to PingID if Twilio becomes unavailable, in the **Fallback to Default Account** section, select **Fallback to Default Account**.

> **Note**
>
> - The following errors will cause fallback:
>   - All API errors, but not SMS delivery errors.
>   - No origination number was found on the Twilio account
> - If originating the SMS or voice event with the tenant's own account and admin did not define a fallback to PingID's account, the event originates from Ping's account.
> - If a transaction was charged to a specific account (Ping or custom), subsequent transactions might not be charged to the same account. The account charged for each transaction is determined on an individual basis. PingID always prioritizes the custom account.
> - During fallback, you are billed at PingID's rates and not at any preferential rates from Twilio. PingID originating numbers and setup parameters are used.

9. In the **Twilio Legal Consent** window, click **I Consent**.



> **Note**
>
> You are only asked for legal consent when entering a new SID.

10. Click **Save**.

Managing a Twilio account

Managing a Twilio account includes changing the originating numbers, fallback settings and updating or deleting a custom account.

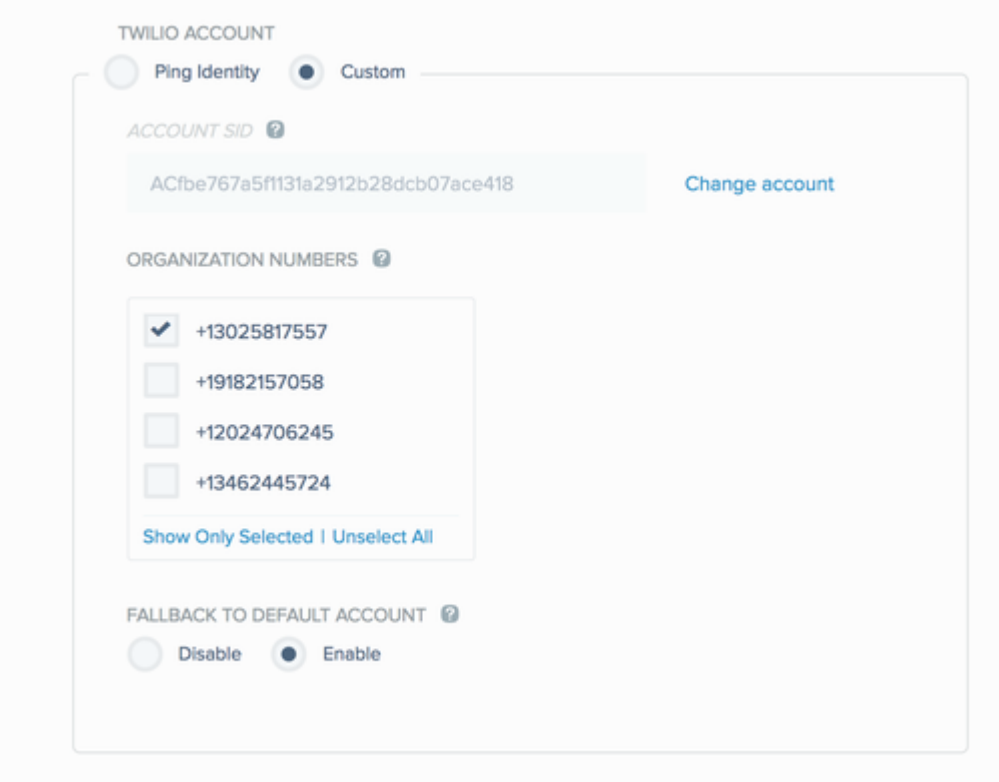
About this task

Managing an account includes:

- Changing active originating numbers and fallback setting (as in Configuring a Twilio account)
- Changing to another account
- Deleting the custom account

Steps

1. In the PingID admin portal, go to **Setup → PingID → Configuration**.
2. In the **Twilio Account** section, from the **Organization Numbers** list, select at least one originating telephone number to use.



3. Manage your Twilio account according to the following table.

Option	Description
Fallback To Default Account	To default to the Ping Identity Twilio account in the event of an error with your account, in the **Fallback To Default Account** section, select **Enable**. This option is disabled by default.
Change Account	To switch to a different account, click **Change Account**. For more information, see Configuring a Twilio account.
Ping Identity radio button	To delete the active custom account, click the **Ping Identity** radio button.

4. Click **Save**.

SMS and voice usage limits

For users choosing the SMS or voice option, the number of SMS or voice transactions are constrained depending on your organization's PingID account type.

SMS and voice usage falls into two categories: used and unused.

Used

The number of SMS or voice authentication requests a user can receive and respond to each day.

Unused

The number of SMS or voice authentication requests a user can receive and not respond to each day.

Administrators can configure these limits for licensed organizations according to the table below. The daily counters reset every night at midnight UTC.

PingID SMS and voice usage limits

Usage Type	PingID Trial Limit	PingID Licensed Limit
Enrollment	100	Unlimited
Authentication	5 per user per day (used or unused)	• Used: 15 (default). Configurable to a value between 1-50 per user per day. • Unused: 10 (default). Configurable to a value between 1-50 per user per day.

> **Note**
>
> SMS or voice transaction constraints are unrelated to SMS or voice fees, which are billed according to your organization's actual usage.

PingID language support

PingID supports a wide variety of languages.

PingID supports the following languages:

- French (EU)
- French (Canadian)
- German

- Japanese
- Chinese
- Dutch
- Italian
- Korean
- Portuguese
- Russian
- Thai
- Turkish
- Polish
- Czech
- Hungarian

The language displayed is defined as follows:

- **PingID mobile app**: according to the language defined in the user's mobile device language settings.
- **PingID authentication and registeration screens**: according to the language settings of the web browser that is used.
- **SMS and Voice messages**: you can define the languages supported. The language displayed is according to the language settings of the web browser being used. For more information, see Enabling and customizing language localization for SMS authentication in PingID.

> **Note**
>
> To prevent users from registering their device for SMS or voice authentication, and allow existing users to continue to authenticate, see Disabling pairing for a specific authentication method. This option is useful if you want to phase out SMS and voice authentication, in favor of more secure authentication methods.

The following list describes the conditions and limitations of SMS and voice authentication:

- Phone numbers with extensions are supported for voice calls. The phone number must be followed by a comma and the extension number. For example:
  - The phone number +12025550123 with the extension 2992 is entered as +12025550123,2992.
  - The extension can include the # or * characters. For example, +12025550123,#2992 or +12025550123,2992#.
  - If there is more than one extension, a comma should separate the extension and the nested extension. For example, +12025550123,#2992,#2991.
  - Each comma generates a 2-second pause. After the call is answered, the extension is dialed after 2 seconds. If a pause is required for longer than 2 seconds, add an additional comma for each additional 2-second pause. For example, in +12025550123,#2992,,,#2991, three commas generate a 6-second pause before the nested extension.
- Because of Chinese regulatory limitations, use of voice OTPs in China is disabled.

- In some cases, SMS OTPs in China may be blocked because of Chinese regulatory limitations. Therefore, it is recommended to use the Twilio Verify service in China. To enable this service, contact your Ping Identity sales representative.
- In India and Saudi Arabia, PingID sends OTPs through SMS in transactional mode.
- Transactional SMS messages include "PingID" as part of the sender ID.
- Additional sender ID numbers are available for the PingID SMS and voice OTP services so users can receive OTP text messages or voice calls from a different number. Generally, after the new number is set, the user will receive the PingID SMS or voice OTP from that number in the future. In cases of SMS or voice delivery technical issues, the user can receive the OTP text messages or voice calls from a new number, provided by a fallback SMS provider.

> **Note**
>
> Voice authentication end users should change their voicemail password from their device default, or disable voicemail if using PingID voice OTP. An attacker could potentially direct an OTP voice call to a voicemail by calling the victim at the same time. In the event of an attack, the OTP will be recorded in the voicemail and will be subject to its password protection.

For information about the user experience, see the PingID End User Guide.

Pre-populating or restricting user registration data

For SMS, voice, and email authentication, you can pre-populate or restrict registration to corporate information that is already defined in your organization's user directory.

About this task

These configurations are applied during initial registration and during the registration of additional devices if you have enabled multiple-device capability.

Pre-Populate

When registering for PingID, the email, SMS, or voice field is pre-populated with the information defined in your user directory. The user can edit the information or replace it with a different address or phone number.

Restrict

When registering for PingID, the email, SMS, or voice field is pre-populated with the information defined in your user directory. The information is read-only and cannot be edited by the end user. If information in the user directory is missing or invalid for a specific device type, the user is not presented with the option to register with that device.

> **Note**
>
> Applying the **Restrict** option to an authentication method removes that method when pairing with PingID SSH, VPN, and Windows login integrations, as well as for local users.

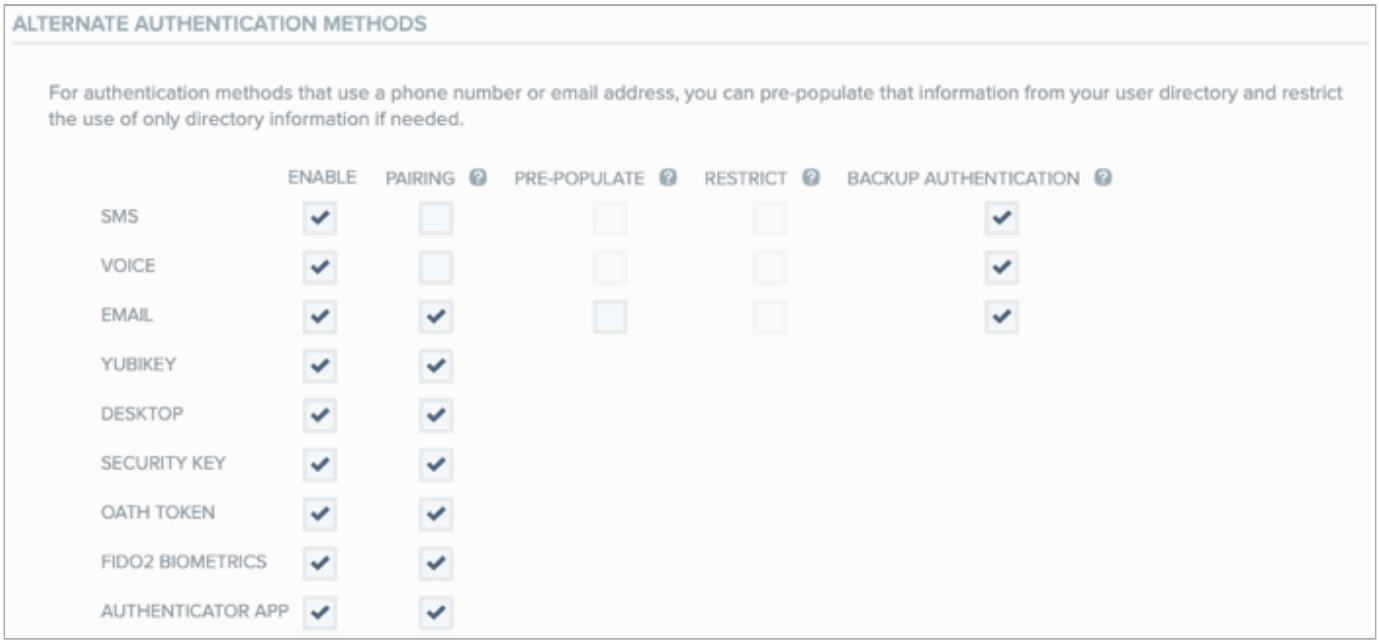
Information must be saved to your user directory in Google Library format, which specifies that all phone numbers must include "+" and the international country code. No manipulation or validation is performed when information is extracted from the user directory. For example, if a phone number is not stored in an international format, a prefix is not added, which might cause an error when trying to continue the registration flow. For information about configuring attributes in your user directory, see Configuring the phone number attribute in PingOne and Configuring LDAP attributes in PingFederate.

Important

When PingID is integrated with PingFederate as the identity provider (IdP), confirm that the attribute names under **Setup → Dock → Configuration → Attribute Mapping** that are passed to PingFederate exist and match the required SAML message attribute names.

Steps

1. Sign on to the PingID admin portal and go to **Setup → PingID → Configuration**.
2. In the **Authentication** section, go to the **Alternate Authentication Methods** section.



3. In the **Enable** column, ensure that the relevant authentication methods are selected. Configure the authentication methods as described in the following table.

Choice	Description
Pre-Populate	To pre-populate the user entry field with the SMS or voice numbers stored in your user directory when registering for PingID, in the relevant row, select the **Pre-Populate** check box.
Restrict	To restrict the user to select only the SMS or voice phone numbers stored in your user directory when registering for PingID, in the relevant row, select the **Restrict** check box.

4. Click **Save**.

Configuring backup authentication methods

Configure backup authentication so that a user can still sign on if they do not have access to their primary authentication device, such as if they forget their device at home, or their device is lost or stolen.

Before you begin

Ensure the relevant attributes are configured in your user directory and are up-to-date.

Attributes must be entered in the correct format. For more information, see Configuring the phone number attribute in PingOne, Configuring LDAP attributes in PingFederate, Integrate PingID with AD FS, step 5 of Configuring advanced settings, and Configuring PingID MFA for Microsoft Azure AD Conditional Access.

About this task

Backup authentication uses the email and phone attributes stored in your organization's user directory to send a one-time passcode (OTP) to the user through SMS, voice, or email. This option is available for web SSO only.

If you enable one or more backup authentication types, and the user has at least one valid phone number or email address listed in the user directory, a **Forgot Your Device?** link is shown on the authentication screen. When the user clicks **Forgot Your Device?**, they are presented with a list of the backup authentication options available for their account.

If a policy is applied to your organization, the **Forgot Your Device?** link only appears if either the authenticate rule action, or a rule action with a fallback, such as fingerprint with OTP fallback, is applied to the policy.

You can include the following directory attributes as options for backup authentication:

- Email
- Secondary email
- Voice
- SMS

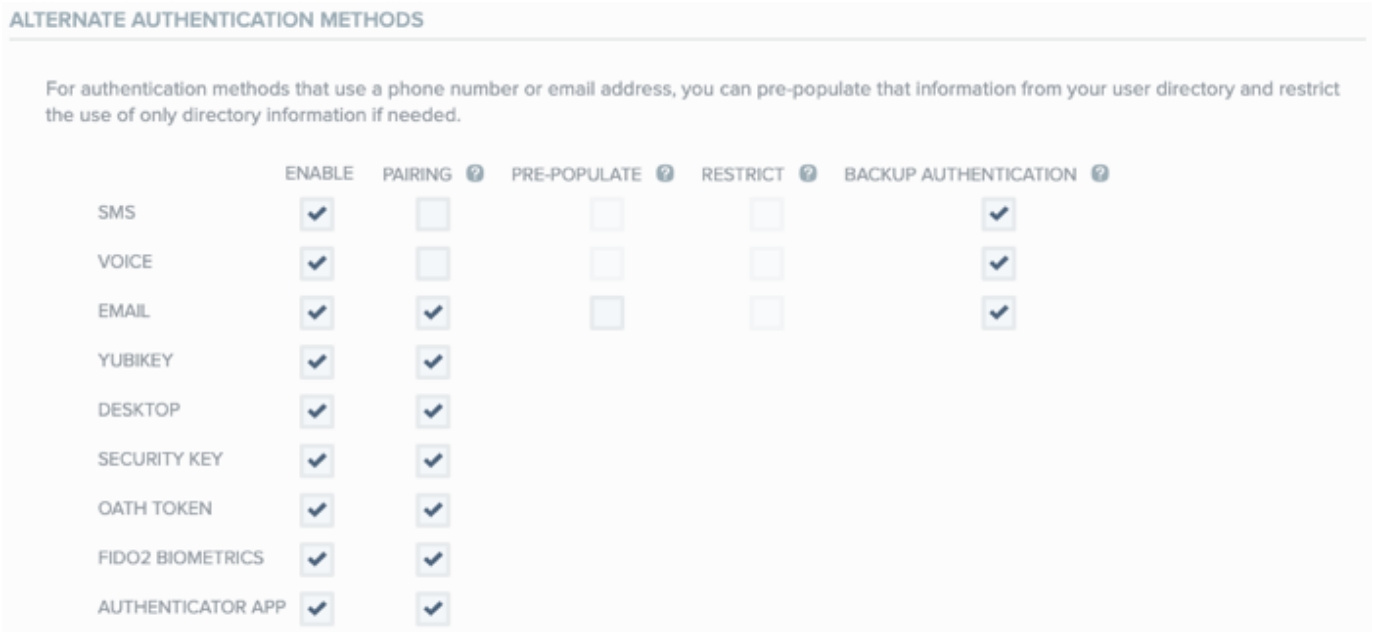
Phone numbers must be saved in Google Library format, which specifies that all phone numbers must include "+" and the international country code. Only attributes listed in the required format are displayed as a backup authentication method.

> **Note**
>
> PingOne supports the use of a single email address and a single phone number, which can be used for both SMS and Voice.

Steps

1. Sign on to the admin portal and go to **Setup → PingID → Configuration**.

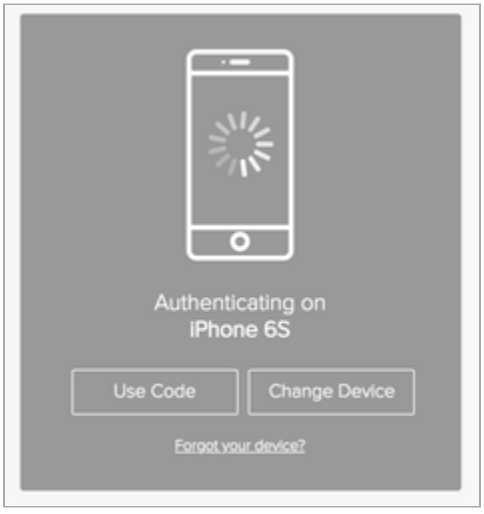
2. In the **Authentication** section, go to **Alternate Authentication Methods**.



3. To enable an authentication method as backup authentication, in the relevant row, select the **Backup Authentication** check box.
4. Click **Save**.
5. To select backup authentication as an allowed authentication method when creating a PingID policy, see PingID policy.

Result

The next time a user signs on or performs an action that requires authentication, if they have a valid backup authentication method, they can click **Forgot Your Device?** and authenticate with a backup device.



> **Note**
>
> When the user clicks **Forgot Your Device?**, PingID sends a device change notification to the paired device and invalidates the original authentication request. To view the user flow, see Authenticating using a backup device.

Enabling advanced authentication policy

To enforce authentication policy settings, you must enable the **Enforce Policy** setting.

About this task

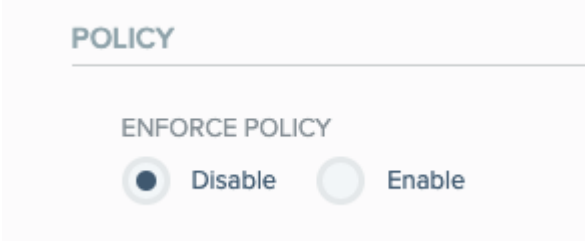
For instructions on configuring an authentication policy, see PingID policy.

Steps

1. Sign on to the admin portal, and go to **Setup → PingID → Configuration**.
2. In the **Authentication** section, go to **Enforce Policy**.

Choose from:

- **Disable** (default): The device requirements, device pairing conditions, and policy configurations are ignored.
- **Enable**: The device requirements, device pairing conditions, and policy configurations are applied for authentications.



> **Note**
>
> You can edit and save changes to the policy settings while **Enforce Policy** is set to **Disable**. Changes will take effect only when you select **Enable**.

1. Click **Save**.

Configuring the phone number attribute in PingOne

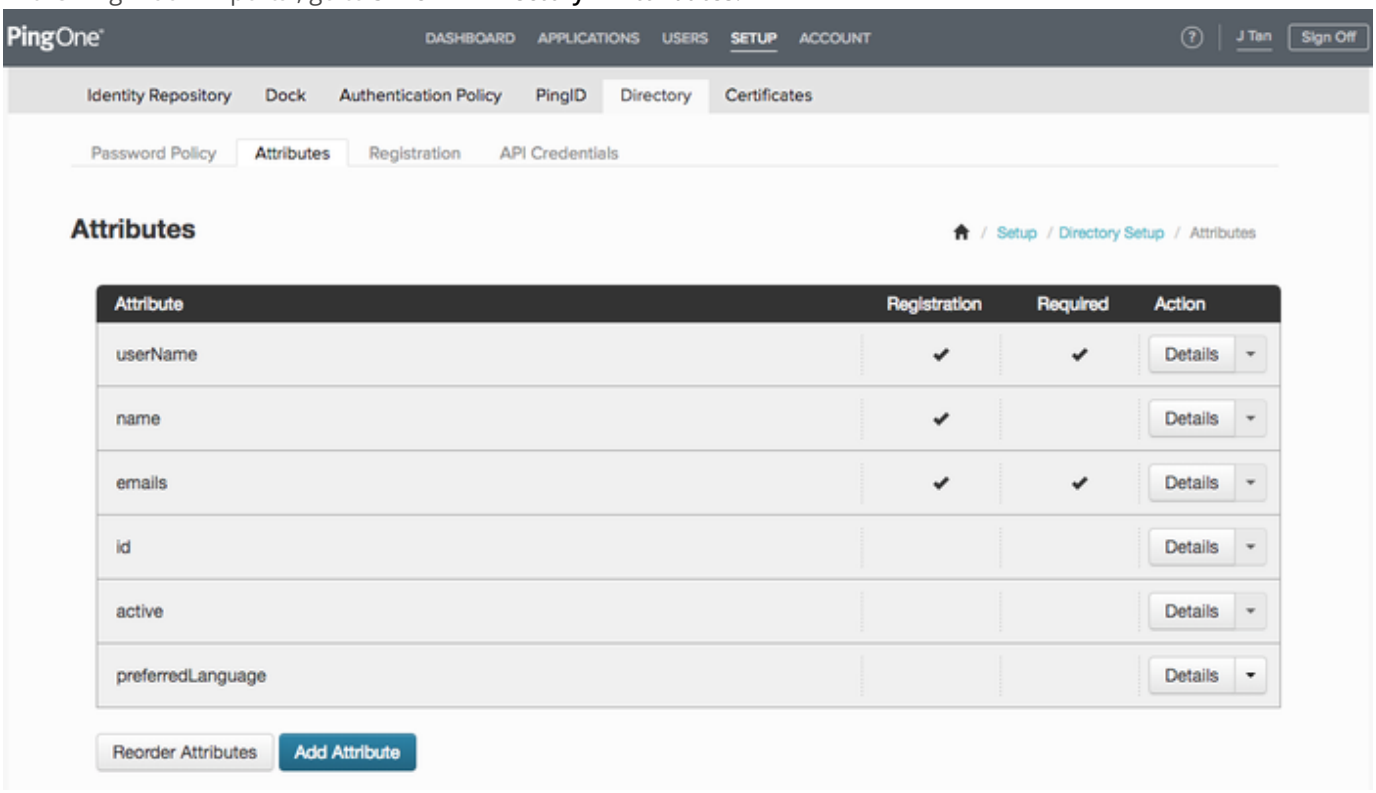
If you are using PingOne as your identity provider (IdP) and want to enable backup authentication or pre-populate or restrict registration data, you must first define the phone number attribute in the PingOne directory.

About this task

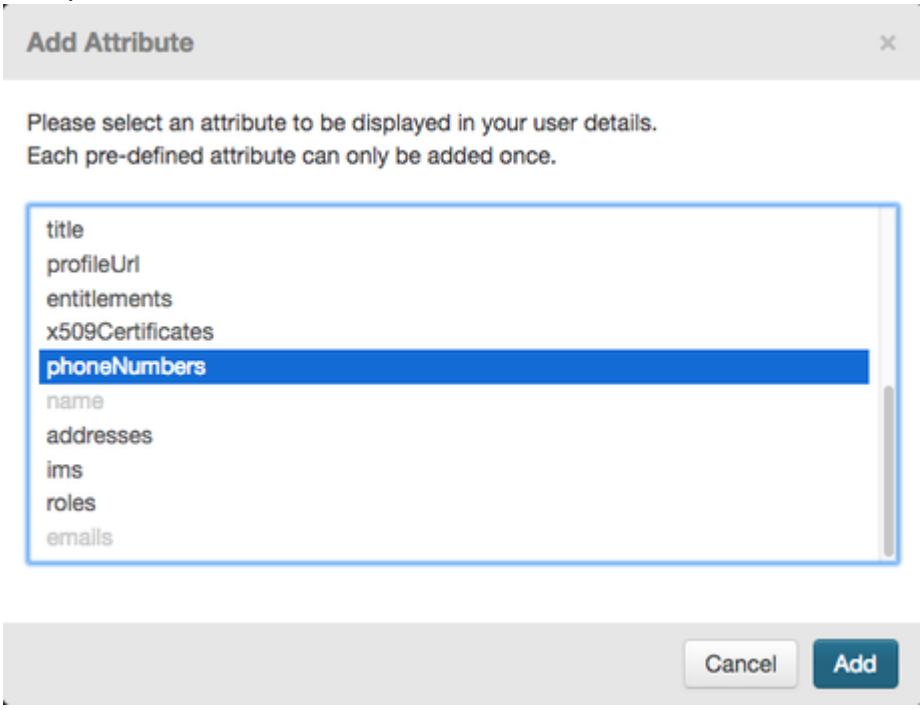
For more information, see Configuring backup authentication methods and Pre-populating or restricting user registration data.

Steps

1. In the PingID admin portal, go to **SETUP → Directory → Attributes**.

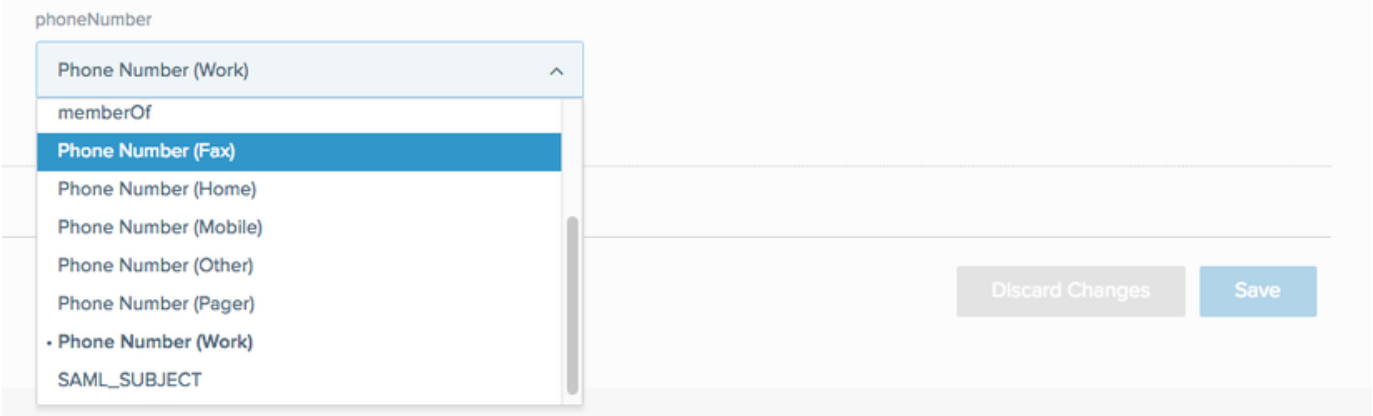


2. If the **phoneNumbers** attribute is not listed, click **Add Attribute** and then select the **phoneNumbers** attribute. Click **Add**.



> **Note**
>
> This ensures that the relevant phone number attributes appear as options when configuring user details.

3. Go to **SETUP → Dock → Configuration**.
4. In the **ATTRIBUTE MAPPING** section, from the **phoneNumber** list, select the phone number attribute you want to use.



5. To add a phone number for a specific user, go to **Users → User Directory → Users**. For the relevant user entry, click **Edit** and add the user's phone number to the relevant phone number field. Click **Save**.

> **Note**
>
> You must enter phone numbers in Google Library format, which specifies that all phone numbers must include "+" and the international country code.

Configuring LDAP attributes in PingFederate

If you are using PingFederate as your identity provider (IdP) and want to enable backup authentication or pre-populate or restrict user data, you must first configure the relevant attributes in the PingID adapter.

Before you begin

Ensure that PingFederate is connected to an LDAP data source.

About this task

For more information, see Configuring backup authentication methods and Pre-populating or restricting user registration data.

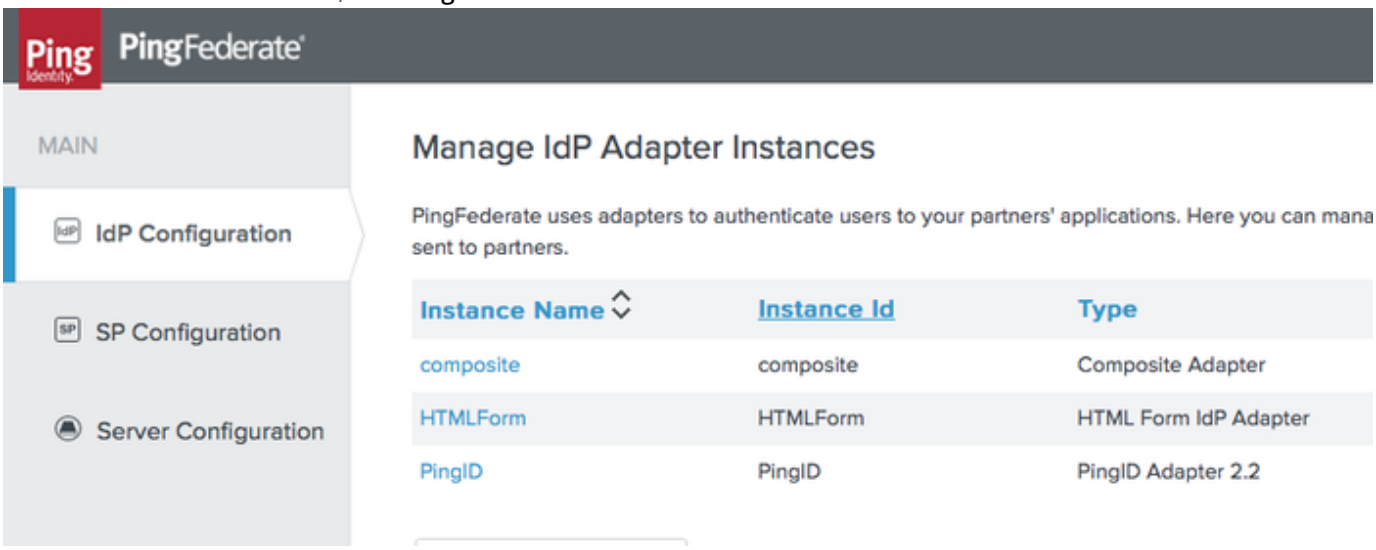
Steps

1. Sign on to the PingFederate administrative console, and go to the **Manage IdP Adapter Instances** window.

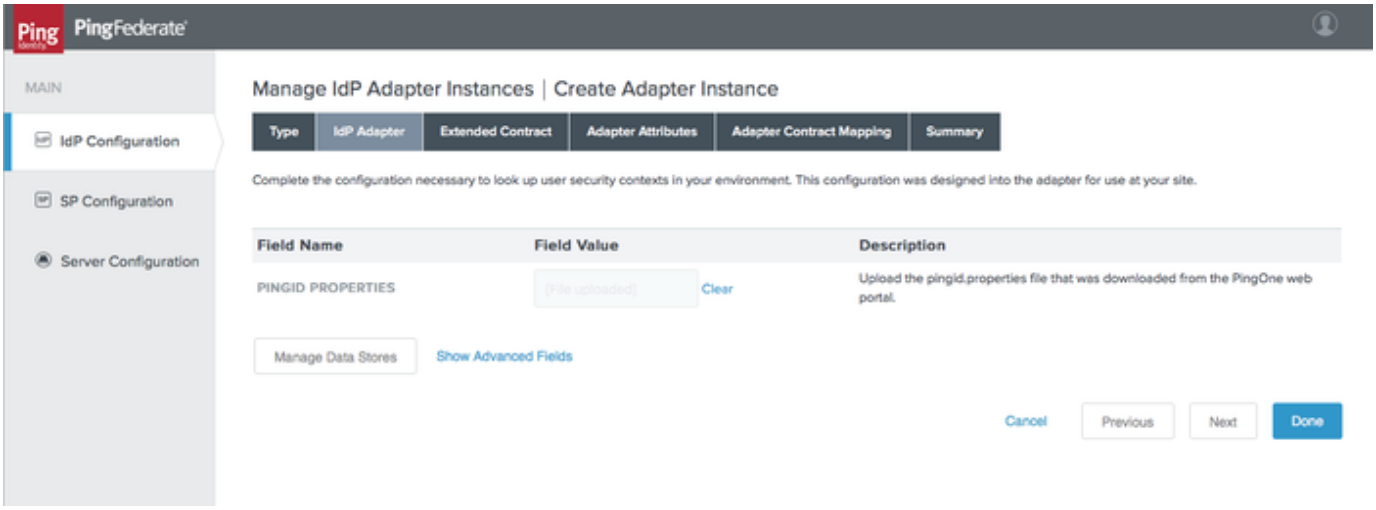
   Choose from:

   - PingFederate 10.0 and earlier: Go to **IdP Configuration → Application Integration → Adapters**.
   - PingFederate 10.1 and later: Go to **Authentication → Integration → IdP Adapters**.

2. In the **Instance Name** column, click **PingID**.



3. Click **Show Advanced Fields**.



4. Fill in the relevant fields, and then click **Done**.

Field	Description
Email Attribute	The LDAP attribute containing the user email address.
Secondary Email Attribute	The LDAP attribute containing an additional user email address.
Phone Attribute	The LDAP attribute of the phone number used for SMS messages, as well as voice calls if **Voice Number** attribute is left empty.
Voice Number Attribute	The LDAP attribute of the phone number used for voice calls. If left empty, the **Phone Attribute** is used for voice calls.

> **Note**
>
> The **Phone Attribute** and **Voice Number Attribute** fields must use the Google Library format, which specifies that all phone numbers must include "+" and the international country code.

Disabling pairing for a specific authentication method

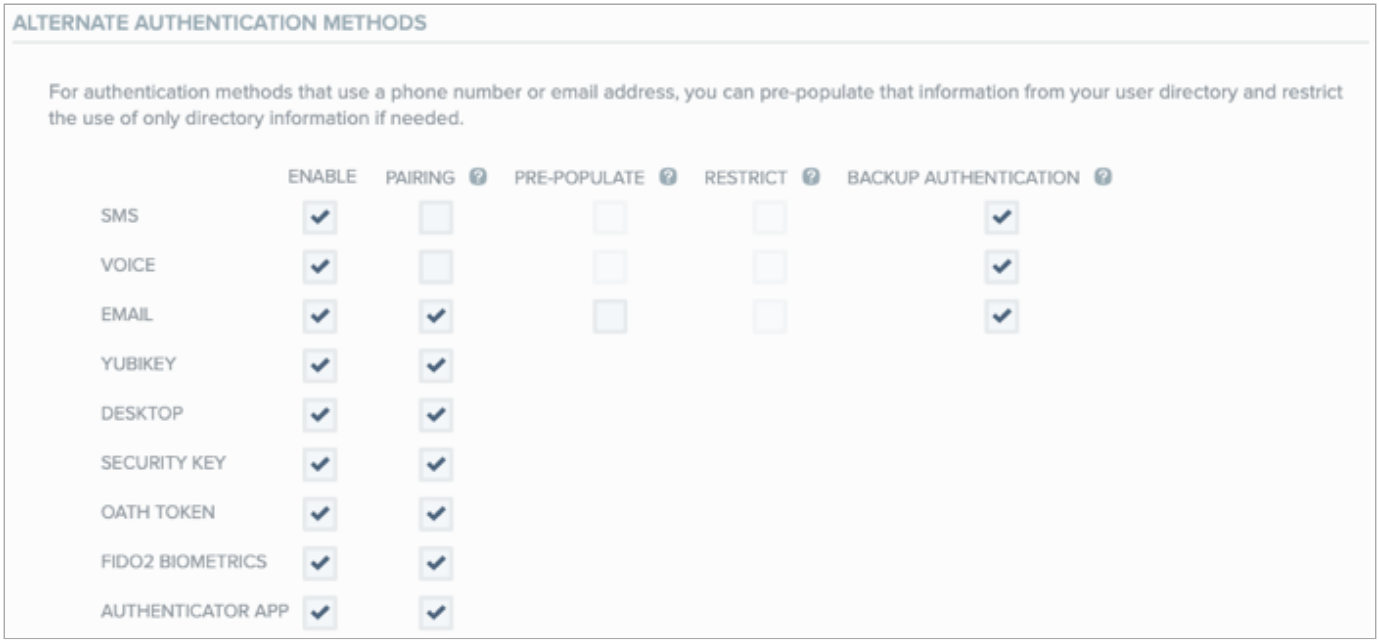
You can prevent users from pairing a specific authentication method, such as SMS, voice, or email. This is useful if you would like to phase out a specific method of authentication, without blocking existing users from authenticating.

About this task

If you disable the ability to pair a specific authentication method, it is it does not affect authentication for existing users, or the use of that authentication method as a backup authentication method. NOTE: This option is reversible. If pairing of an authentication type has been disabled, you can select the relevant pairing checkbox to re-enable pairing for that authentication type.

Steps

1. In the PingID admin portal, go to **Setup → PingID → Configuration**.
2. In the **Authentication** section, go to **Alternate Authentication Methods**.



3. In the **Pairing** column, clear the check box for each authentication type that you want to disallow pairing. Click **Save**.

   Result:

   After save is complete, users that want to pair a device no longer see the option to pair with the disallowed device. Existing users can continue to authenticate if already paired with that authentication method.

> **Note**
>
> The **Enable** check box must remain selected so that users already paired with that authentication method can continue to authenticate with PingID.

Removing authentication methods

You can remove an authentication method to disallow its use when authenticating with PingID.

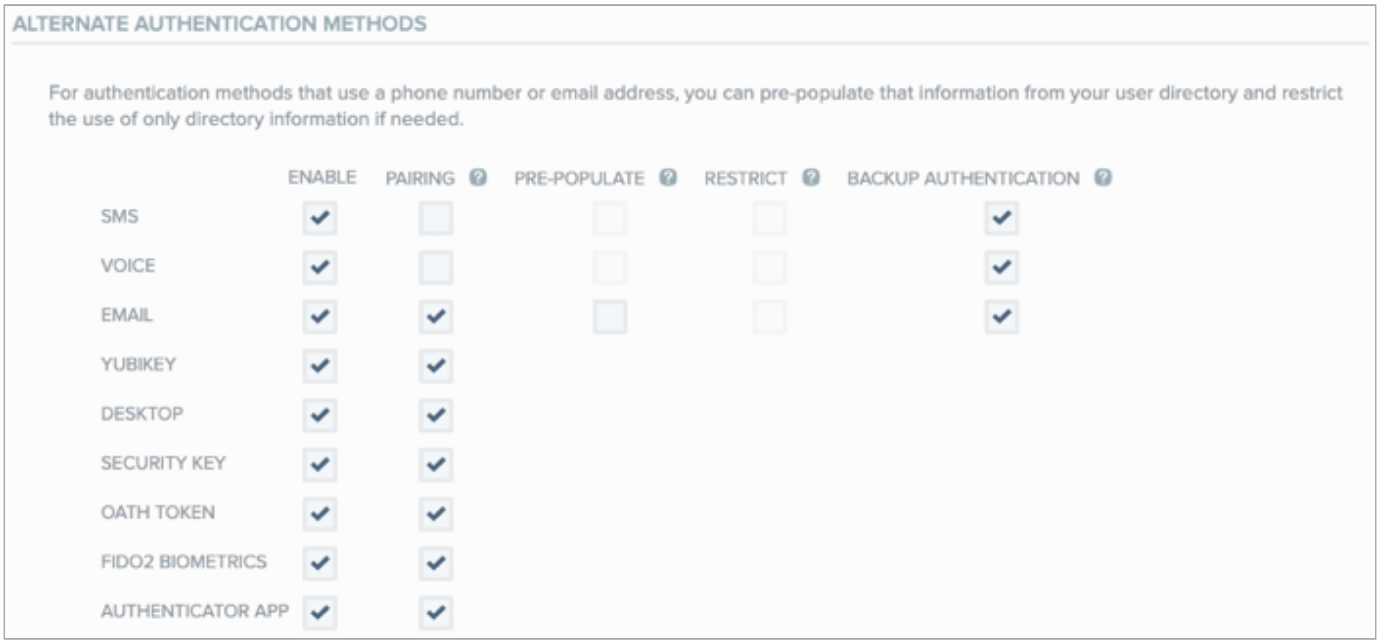
About this task

> **Note**
>
> Removing an authentication method prevents new users from registering and existing users from authenticating with the selected authentication method. If you want to prevent registration, and allow existing users to continue to authenticate with that authentication method, see Disabling pairing for a specific authentication method.

> **Note**
>
> You cannot remove an authentication method if that method is being used for an authentication policy. Remove the method from the authentication policy first, and then clear the relevant check box in the **Alternate Authentication Methods** section.

Steps

1. In the PingID admin portal, go to **Setup → PingID → Configuration**.
2. In the **Authentication** section, go to **Alternate Authentication Methods**.



3. In the **Enable** column, clear the check box for each authentication type that you want to disallow. Click **Save**.

PingID policy settings

The average employee requests access to resources and apps from many locations, networks, and devices, while threats from security attacks and vulnerabilities grow exponentially. With PingID's policy features, you can manage the balance between security and convenience and provide employees with easy and secure access to corporate resources.

The PingID policy introduces three concepts:

Device posture policies

Allows you to specify the requirements of the end user's mobile device, such as specifying permitted or disallowed models, or banning the use of devices that are jailbroken, using an old operating system or mobile app version, or are not lock enabled.

Device pairing policies

Allows you to specify the conditions under which the PingID pairing process should take place, such restricting MFA onboarding to within your company's network.

Authentication policies

Allows you to specify the conditions under which the authentication process should take place and which authentication method to use. For example:

- It might not be necessary to require users to do multiple step up authentications if they're already authenticated within a session and are located at the office.
- You can apply more robust security measures if users are accessing the system from outside the office, or for the first time from a new device.
- You can allow or restrict access based on geofences or network IP definitions.

> **Note**
>
> If you are using PingOne DaVinci to orchestrate your PingID flows, you must include the Evaluate Policy capability in the relevant flow.

Enabling PingID policy

To ensure that the PingID policy settings you have configured are applied to your organization, you must enable **Enforce Policy**.

About this task

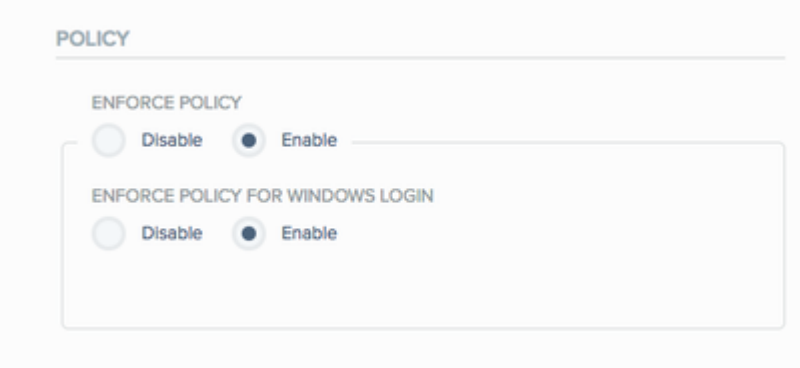
> **Note**
>
> If you are using PingOne DaVinci to orchestrate your PingID flows, PingID policy is always enabled.

Steps

1. In the PingID admin portal, go to **Setup → PingID → Configuration**.
2. In the **POLICY** section, configure the **ENFORCE POLICY** section.

Choose from:

- **Enable**: The device requirements, device pairing conditions, and policy configurations are applied for authentications.
- **Disable**: The device requirements, device pairing conditions, and policy configurations are ignored.



> **Note**
>
> Changes can be edited and saved while **ENFORCE POLICY** is set to **Disable**. The changes will take effect when you select **Enable**.
> For policy for integration with Windows login, see Enabling a Windows login and RDP authentication policy.

Device and pairing policy

Policy settings, combined with the device and pairing configurations, allow you to apply the optimal balance between company security requirements and usability for end users.

The **Device & Pairing** tab allows you to specify the requirements of the end user's device, and the **Pairing Conditions** section allows you to specify the conditions under which the pairing process should take place.

The **DEVICE & PAIRING** tab is found in **Setup → PingID → Device & Pairing**. It contains the following settings sections:

DEVICE REQUIREMENTS

The hardware, software, and configuration prerequisites of mobile devices that users must satisfy to perform PingID authentication and pairing.

PAIRING CONDITIONS

Configurations that define the relevant conditions to permit PingID device pairing. The pairing process is allowed only for accessing requests originating from the specified IP addresses.

Device requirements overview

The following topics describe the types of policy rules that appear in the **Device Requirements** configuration section:

- Configuring an allowed devices policy
- Configuring a disallowed devices policy

- Configuring a minimum OS policy
- Configuring a device lock policy
- Configuring a no rooted or jailbroken devices policy
- Configuring the minimum PingID version
- Configuring the enforcement of device biometrics
- Configuring Mobile Device Management (MDM)

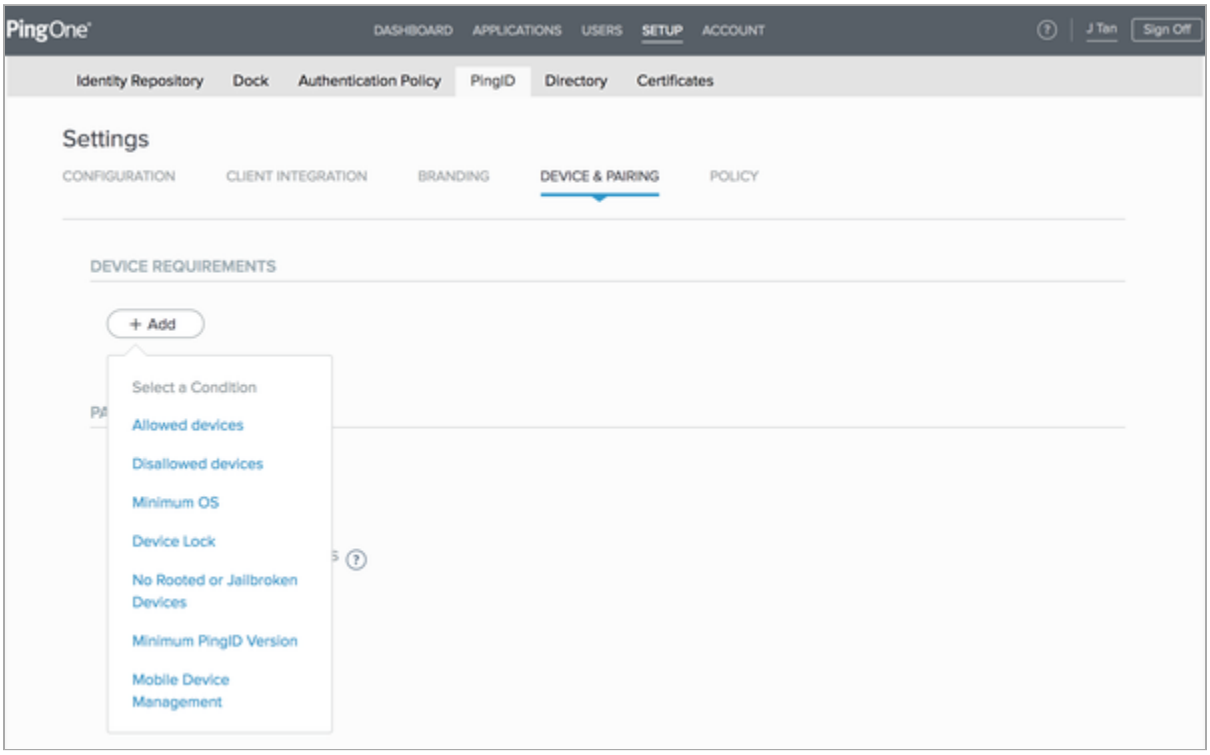
> **Note**
>
> - If you choose the same device under both allowed and disallowed devices, then the disallowed selection takes precedence.
> - The device requirement is not relevant when the mobile app (the swipe or biometrics authentication methods) is not in use.
> - The list of supported devices is dynamic and can change as new models are introduced into the market. For example, several models produced by the following vendors are supported: Apple, HTC, LG, Motorola, and Samsung.

Configuring an allowed devices policy

Configure which device models are allowed for PingID authentication.

Steps

1. In the PingID admin portal, go to **Setup → PingID → DEVICE & PAIRING**.



2. In the **DEVICE REQUIREMENTS** section, click **Add**. From the **Select a Condition** menu, select **Allowed Devices**.
3. Select one or more brands.

   Result:

   The models for the selected brands are displayed.
4. From the list of models, select one or more models to allow.

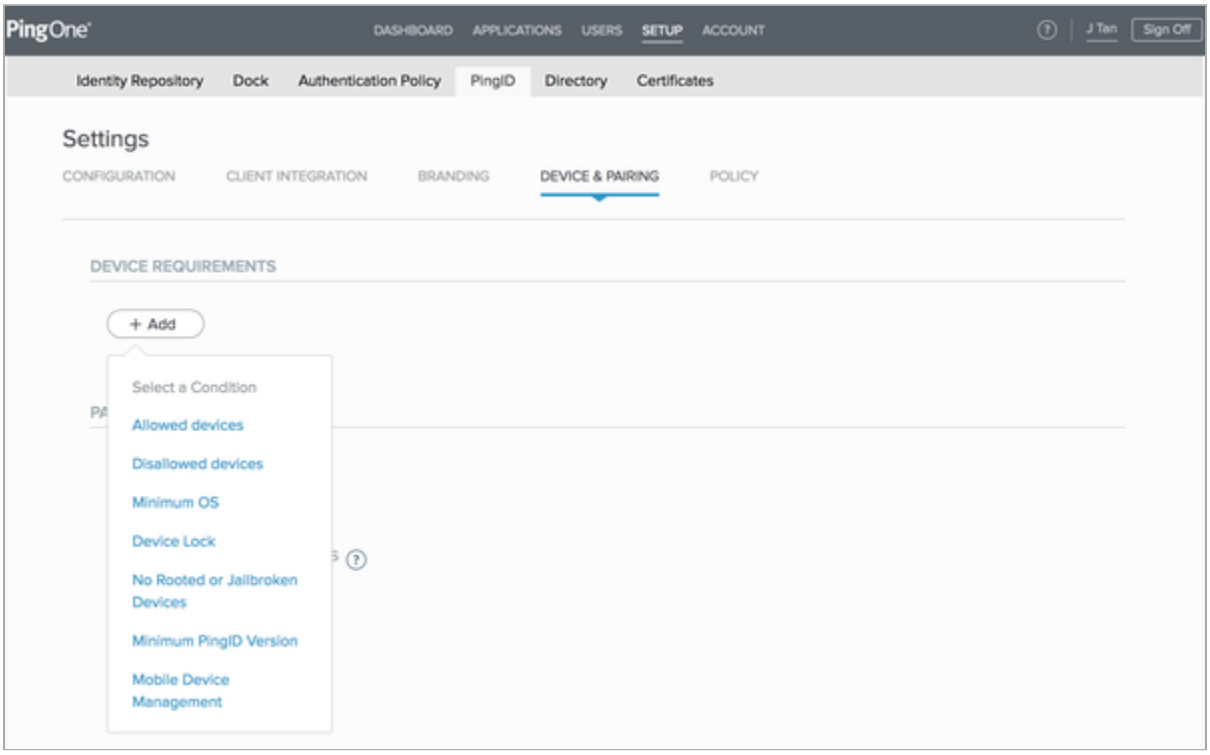
   > **Note**
   >
   > If you want to allow all models for the selected brands, including models that do not appear in the list, select the **All models** option.
5. Click **Save**.

Configuring a disallowed devices policy

Determine which device models are not permitted for PingID authentication.

Steps

1. In the PingID admin portal, go to **Setup → PingID → DEVICE & PAIRING**.



2. In the **DEVICE REQUIREMENTS** section, click **Add**. From the **Select a Condition** menu, select **Disallowed Devices**.
3. Select one or more brands.

   Result:

   The models for the selected brands are displayed.
4. From the list of models, select one or more models to disallow.

   > **Note**
   >
   > If you want to disallow all models for the selected brands, including models that do not appear in the list, select the **All models** option.
5. Click **Save**.

Configuring a minimum OS policy

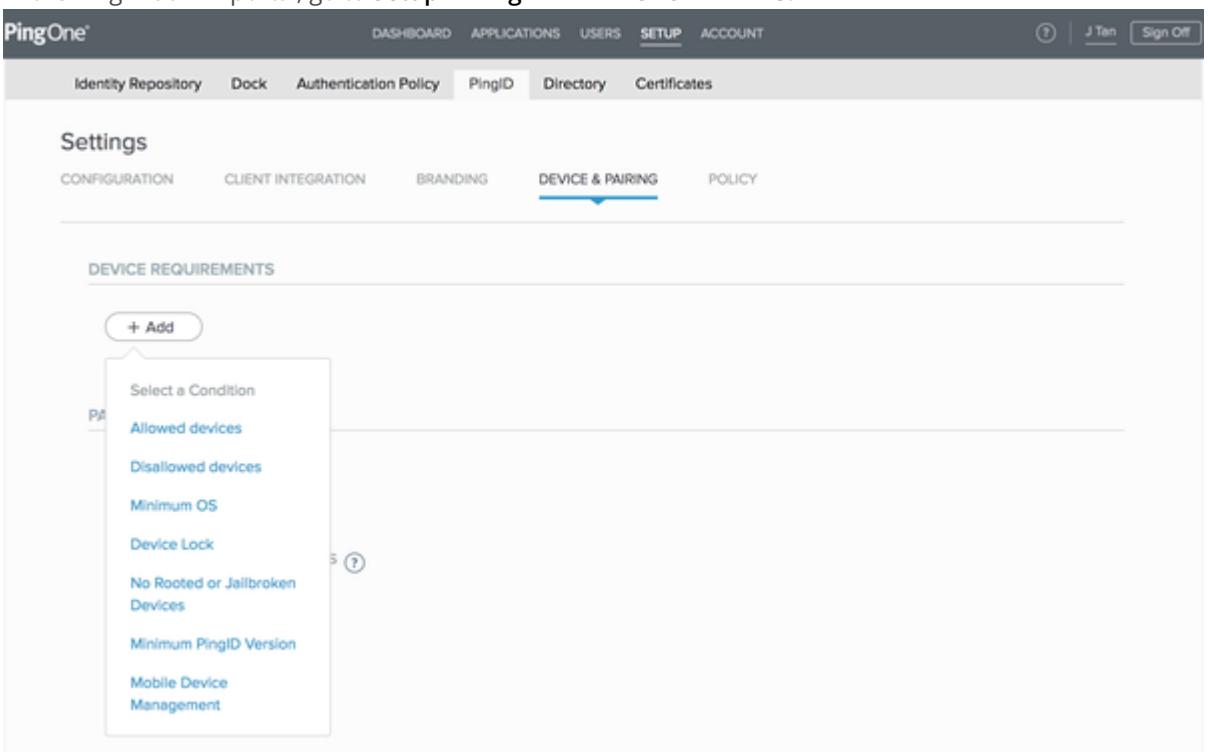
Determine the minimum OS versions for Android and iOS mobile devices that are allowed for PingID authentication. You can block older and less secure OS versions.

About this task

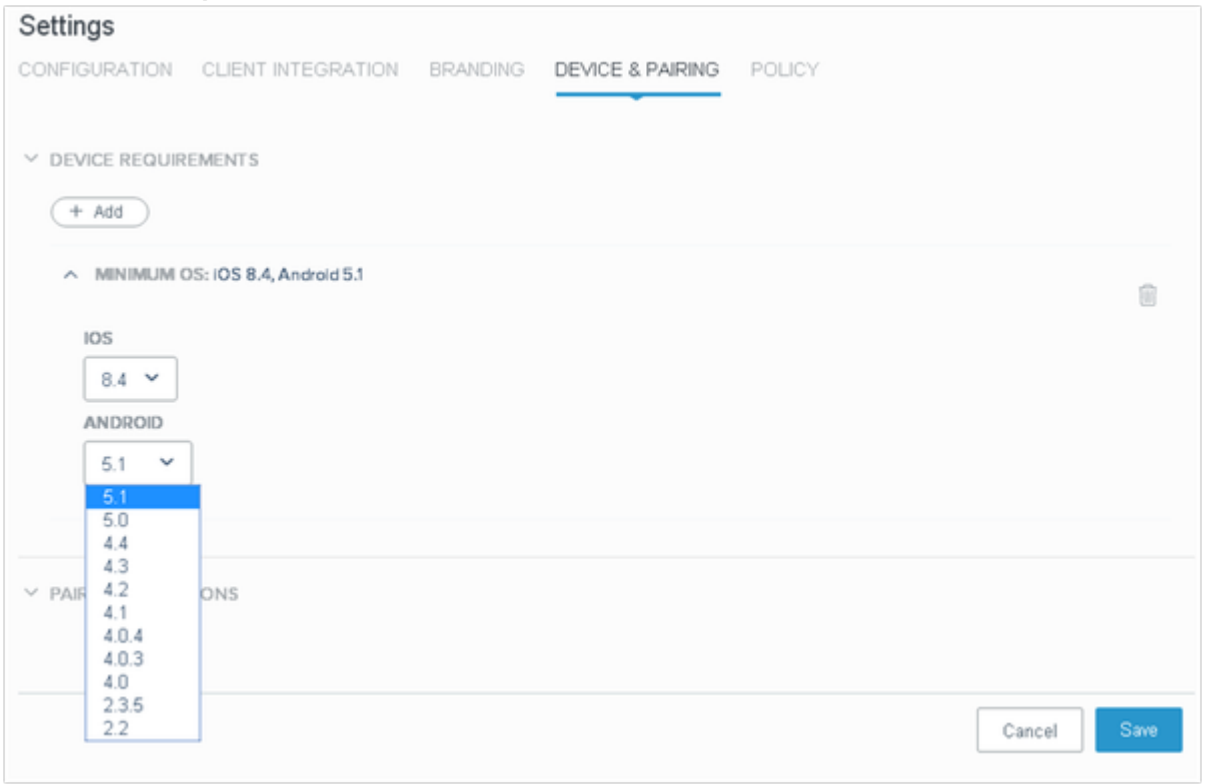
> **Note**
>
> The list of supported operating systems is dynamic and can change as new versions are introduced. Discontinued support of older versions might also impact the minimum supported OS version.

Steps

1. In the PingID admin portal, go to **Setup → PingID → DEVICE & PAIRING**.



2. In the **DEVICE REQUIREMENTS** section, click **Add**. From the **Select a Condition** menu, select **Minimum OS**.



3. From the **iOS** and **Android** lists, select the minimum permitted OS version.

4. Click **Save**.

Configuring a device lock policy

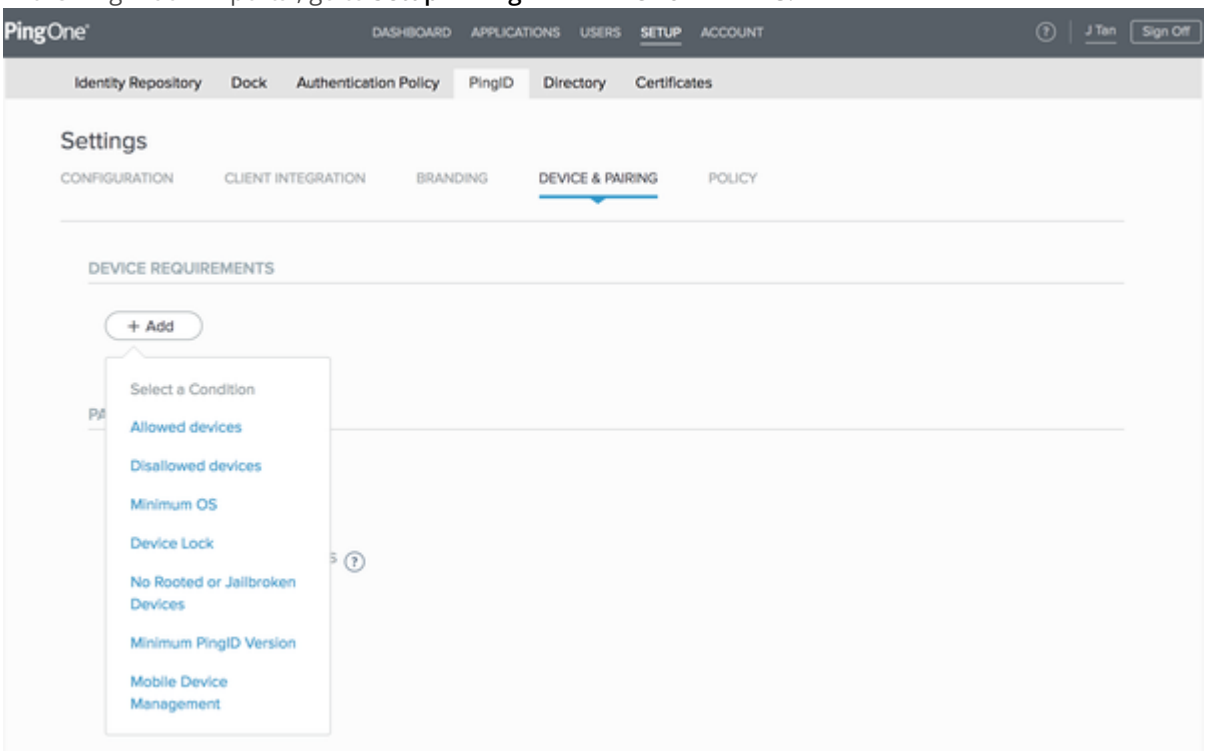
Determine whether the authenticating device must have its lock feature enabled for it to be allowed for PingID authentication.

About this task

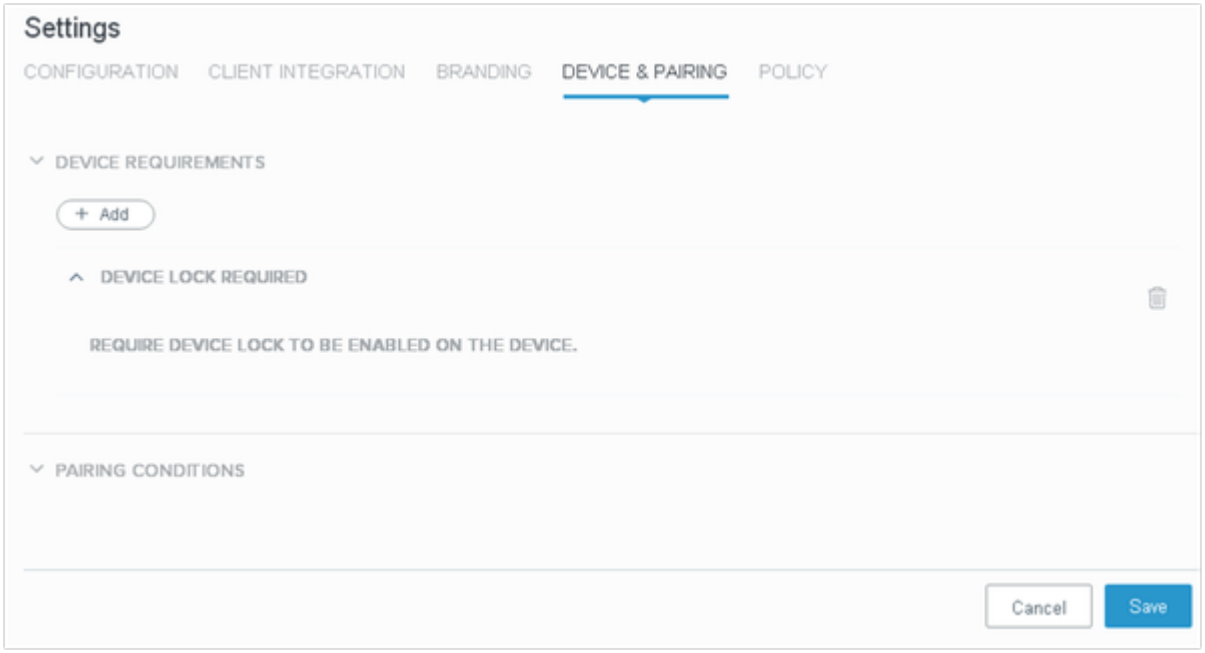
> **Important**
>
> For iOS authenticating devices, the device lock requirement can only be implemented on iOS8 devices and up. iOS7 devices with this policy will be denied with the message `Cannot pair. Device doesn't meet policy. Device lock is disabled`.

Steps

1. In the PingID admin portal, go to **Setup → PingID → DEVICE & PAIRING**.



2. In the **DEVICE REQUIREMENTS** section, click **Add**. From the **Select a Condition** menu, select **Device Lock**.



3. Click **Save**.

Configuring a no rooted or jailbroken devices policy

Determine whether to allow the use of jailbroken or rooted devices.

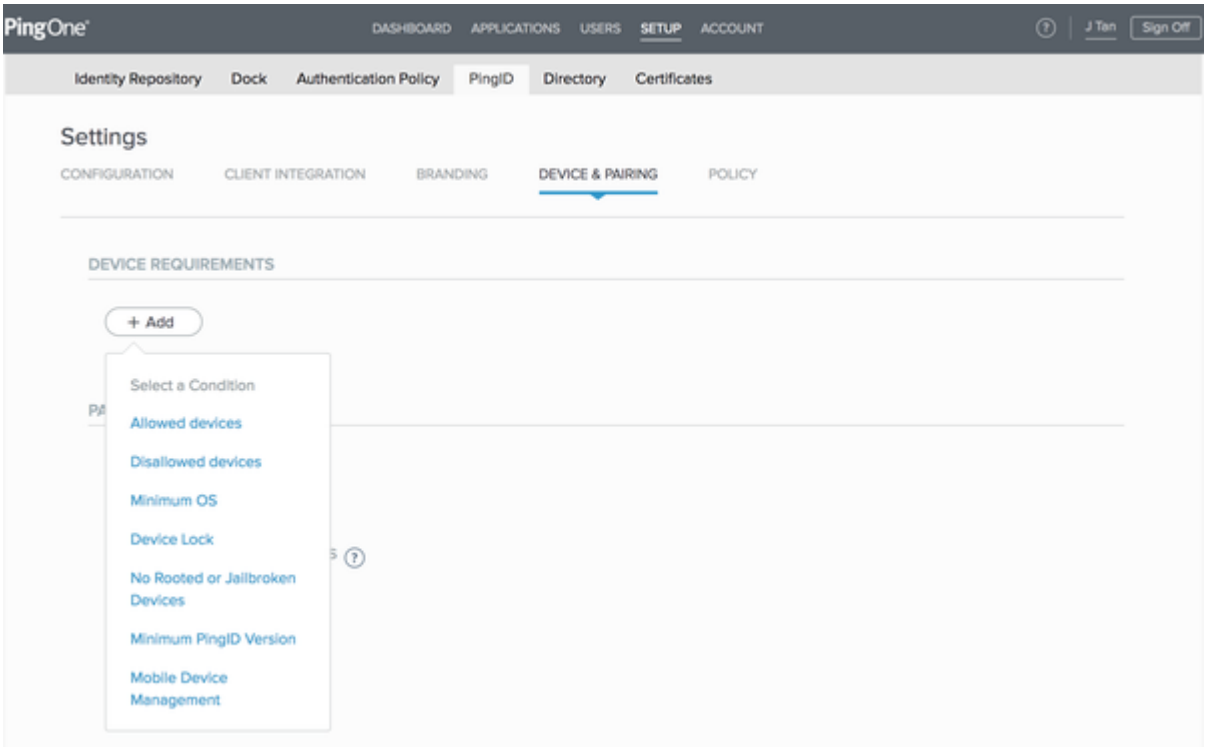
About this task

You might want to block rooted and jailbroken devices as they can be more vulnerable to attacks.

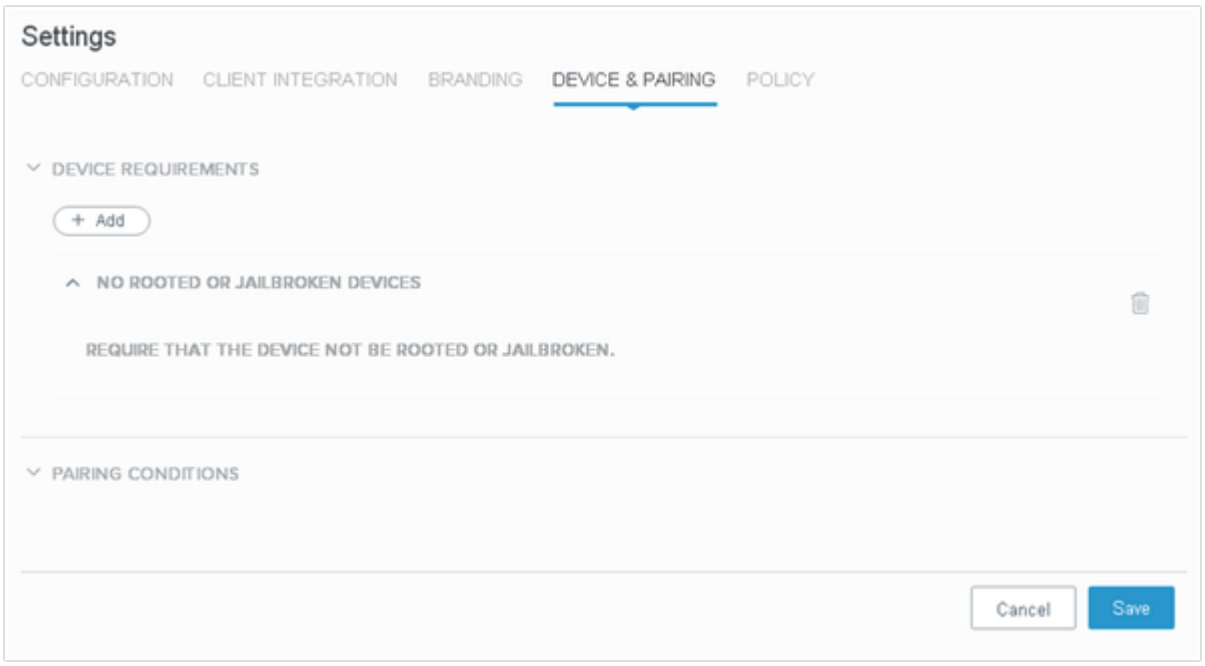
> **Note**
>
> Detection checks for rooted and jailbroken devices are updated periodically, in line with the latest protection against vulnerabilities.

Steps

1. In the PingID admin portal, go to **Setup → PingID → DEVICE & PAIRING**.



2. In the **DEVICE REQUIREMENTS** section, click **Add**. From the **Select a Condition** menu, select **No Rooted or Jailbroken Devices**.



3. Click **Save**.

Configuring the minimum PingID version

Determine the minimum versions of the PingID mobile app for Android and iOS devices that are permitted for PingID authentication.

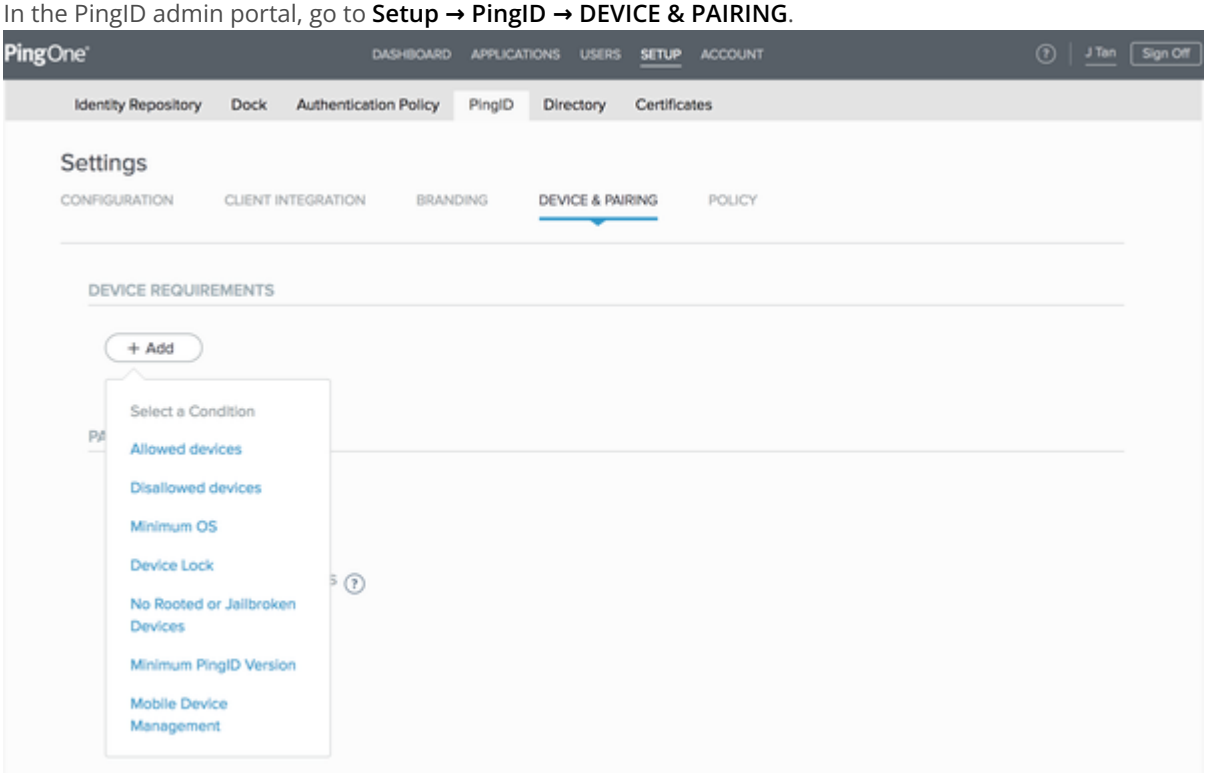
About this task

You can require your users to use new features or disallow older versions of the mobile app.

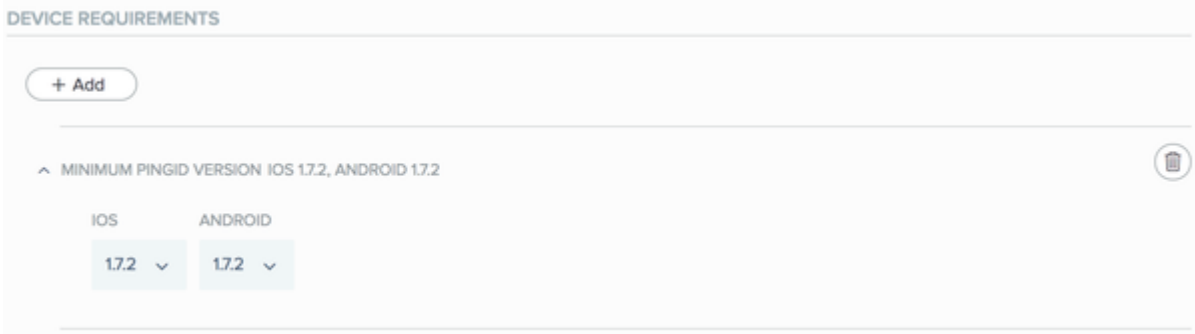
> **Note**
>
> The list of supported mobile apps is dynamic and can change as new versions are introduced into the market. Discontinued support of older versions might also impact the minimum supported version.

Steps

1. In the PingID admin portal, go to **Setup → PingID → DEVICE & PAIRING**.



2. In the **DEVICE REQUIREMENTS** section, click **Add**. From the **Select a Condition** menu, select **Minimum PingID Version**.
3. From the **iOS** and **Android** lists, select the minimum permitted PingID mobile app version.



4. Click **Save**.

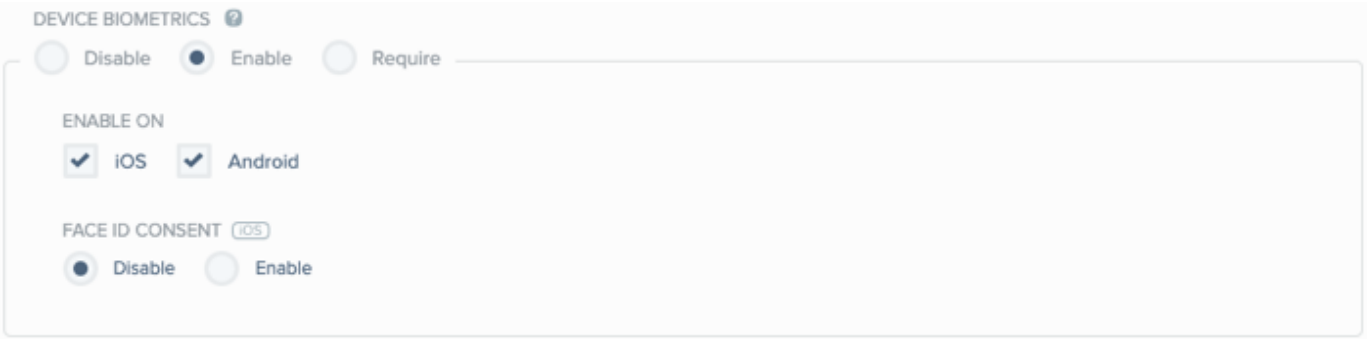
Configuring the enforcement of device biometrics

Enforce the use of a device that includes a hardware biometrics sensor, when pairing or authenticating with PingID.

Before you begin

Before configuring the Biometrics Device posture policy, make sure the following options are configured in the **Configuration** tab, **Device Biometrics** area:

- **Device Biometrics**: Select either **Enable** or **Require**.



> **Note**
>
> If this option is set to **Disabled**, the Device & Pairing **Device Requirements**drop down list shows the Device Biometrics option, but it is disabled.

- **Enable On**: Select the **iOS** and **Android** check boxes. If the relevant check box is not selected, when a user signs on the policy is bypassed.

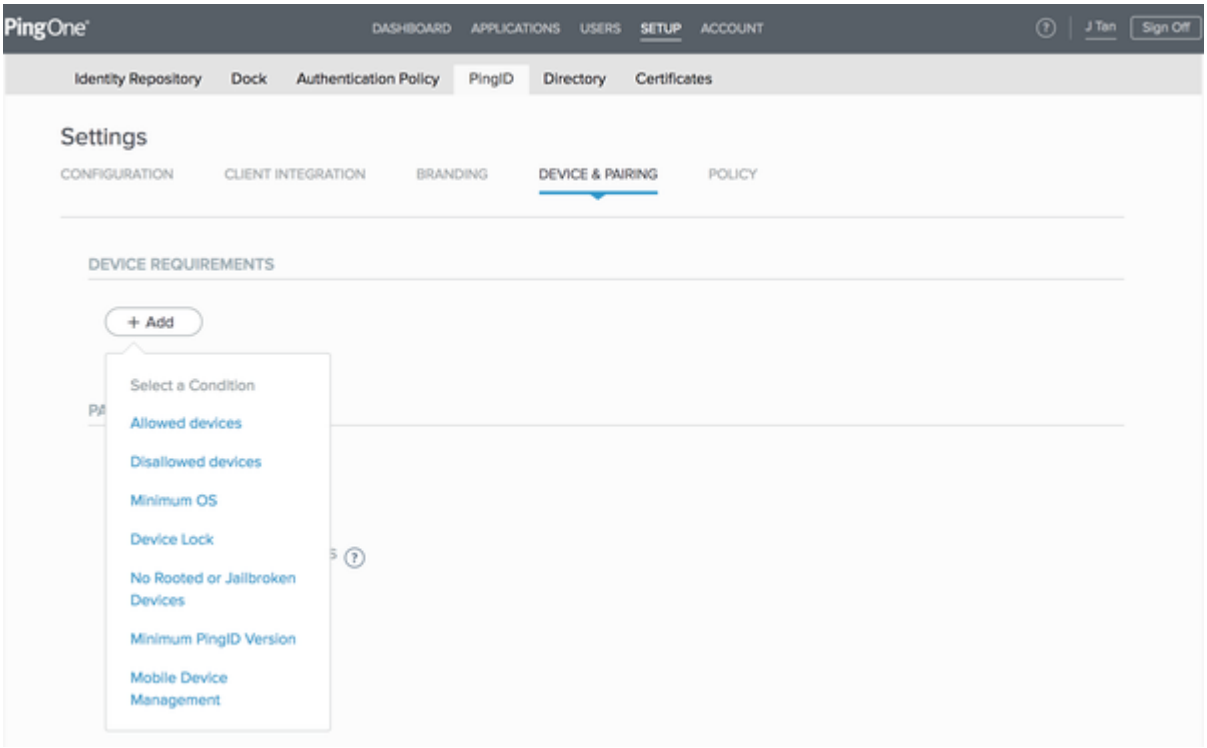
About this task

Use the **Device Biometrics** policy to enforce the use of a device that includes a hardware biometrics sensor when pairing or authenticating with PingID. The user does not have to activate the biometrics sensor or define their biometrics before pairing or authenticating with the device.

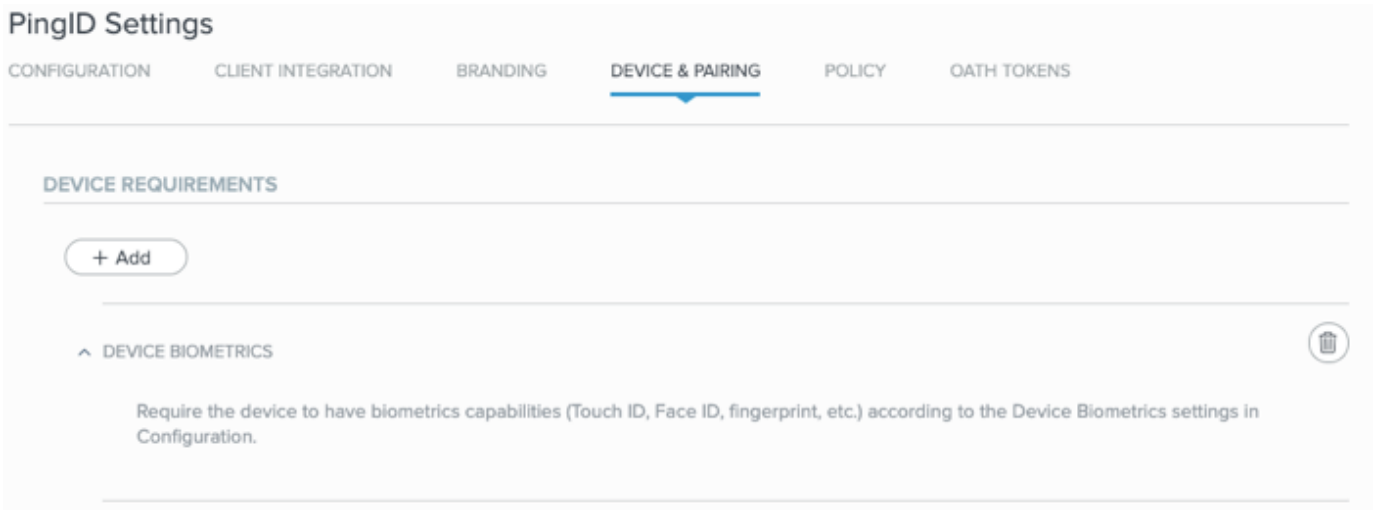
The Device Biometrics policy is supported by PingID mobile app 1.12 or later. The policy is not evaluated for users running earlier versions of PingID mobile app.

Steps

1. In the admin console, go to **Setup → PingID → DEVICE & PAIRING**.



2. In the **DEVICE REQUIREMENTS** section, click **Add**.
3. From the **Select a Condition** menu, select **Device Biometrics**.



4. Click **Save**.

Configuring Mobile Device Management (MDM)

This section describes the steps to configure PingID's MDM integration, which verifies that devices connected through the PingID mobile app are managed by the organization's MDM infrastructure.

MDM is the administration of mobile devices, such as smartphones, tablet computers, and laptops. It can also be applied to desktop computers. Organizations can control activities of their employees by implementing MDM products or services. MDM primarily deals with corporate data segregation, securing emails and corporate documents on mobile devices. MDM enforces corporate policies, and supports the integration and management of mobile devices including laptops and handhelds of various categories.

Note

- The PingID MDM feature can only be used when the organization integrates with an MDM system.
- Two MDM systems cannot manage the same mobile device.
- This solution should work with any MDM system from the major vendors. PingID is officially supported with the following MDM solutions:
  - MobileIron
  - Workspace ONE UEM (formerly known as AirWatch)
  - Microsoft Intune

Flow

The basic flow comprises the following stages:

1. In the PingID admin portal, generate a token for MDM or manually enter or edit a token.
   - See Setting up MDM configuration in PingID for the first time.
2. Configure the third-party MDM system for PingID integration:
   1. Generate and configure an APNS certificate for iOS in the MDM system. For examples see:
      - Installing an APNs certificate for iOS in Workspace ONE UEM
      - Installing an APNs certificate for iOS in MobileIron
      - Installing an APNs certificate for iOS in Microsoft Intune
   2. Configure Android for Work in the MDM system so that the PingID app configuration can be pushed to managed phone sets. For examples, see:
      - Configuring Android for Work for Workspace ONE UEM
      - Configuring Android for Work for MobileIron
      - Configuring Android for Work for Microsoft Intune
   3. In the organization's MDM system, add PingID as a managed app and configure the token that was generated in the PingID admin portal. For examples, see:
      - Configuring Workspace ONE UEM for PingID MDM integration
      - Configuring MobileIron for PingID MDM integration

        - For Microsoft Intune, see Adding the PingID app for iOS in Microsoft Intune and Adding the PingID app for Android in Microsoft Intune

3. After configuration, the MDM system distributes the token to its managed devices.
4. At pairing and authentication time, the PingID server compares the user's token with current active tokens. PingID permits administrators to define more than one active token.
    - If there is no match between the user's token with PingID's current active tokens, the pairing or authentication flow is halted.
    - If the user's token matches a current active token on the PingID server, the pairing or authentication flow will progress.

Ongoing maintenance

As part of periodic MDM maintenance activities, you can generate new tokens for the PingID app and revoke old tokens. For more information, see the following topics:

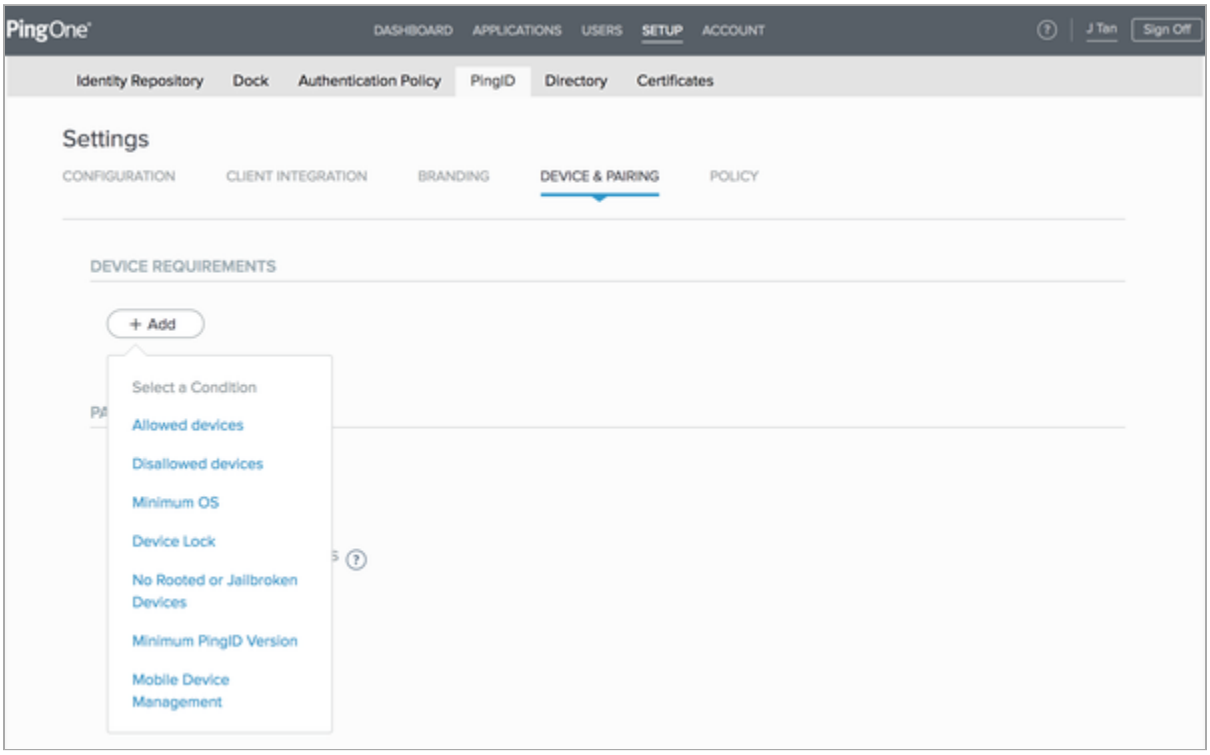
- For PingID:
    - Adding a new MDM token
    - Revoking an MDM token
    - Rotating MDM tokens
- For the supported MDM systems:
    - Updating a PingID token in Workspace ONE UEM
    - Updating a PingID token in MobileIron
    - Updating a PingID token in Microsoft Intune

Setting up MDM configuration in PingID for the first time

Set up the initial MDM configuration for PingID for the organization's MDM to operate with PingID multi-factor authentication (MFA).

Steps

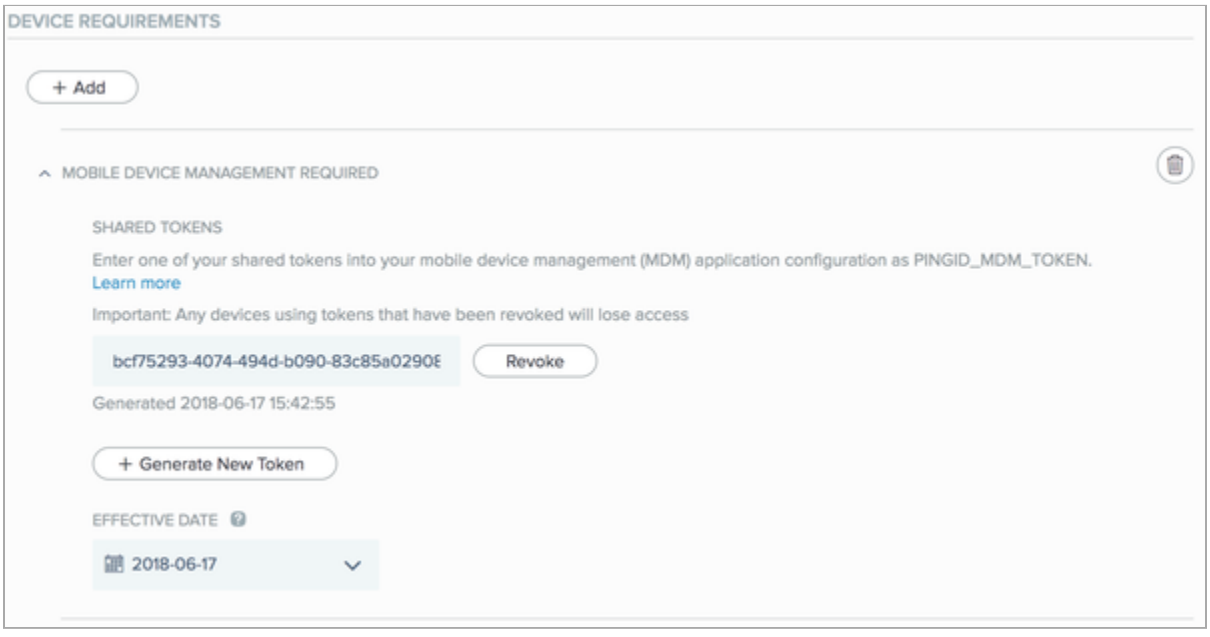
1. In the admin console, go to **Setup → PingID → DEVICE & PAIRING**.



2. In the **DEVICE REQUIREMENTS** section, click **+Add**.
3. From the **Select a Condition** list, select **Mobile Device Management**.

   Result:

   The **Mobile Device Management** section is displayed.



   - The generated **SHARED TOKEN** key is in UUID format.
   - The key value is editable. Administrators can use their own key value.

4. From the **EFFECTIVE DATE** list, select a future date.

> **Caution**
>
> This will allow time to distribute the token to all managed devices, before the MDM requirement takes effect. If the effective date is not a future date, all users will be blocked until the token is distributed by the MDM system to managed devices.

5. Click **Save**.

Next steps

Configure the organization's MDM system. For more information, see Third-party MDM system configuration for PingID integration.

Adding a new MDM token

Add a new MDM token in PingID.

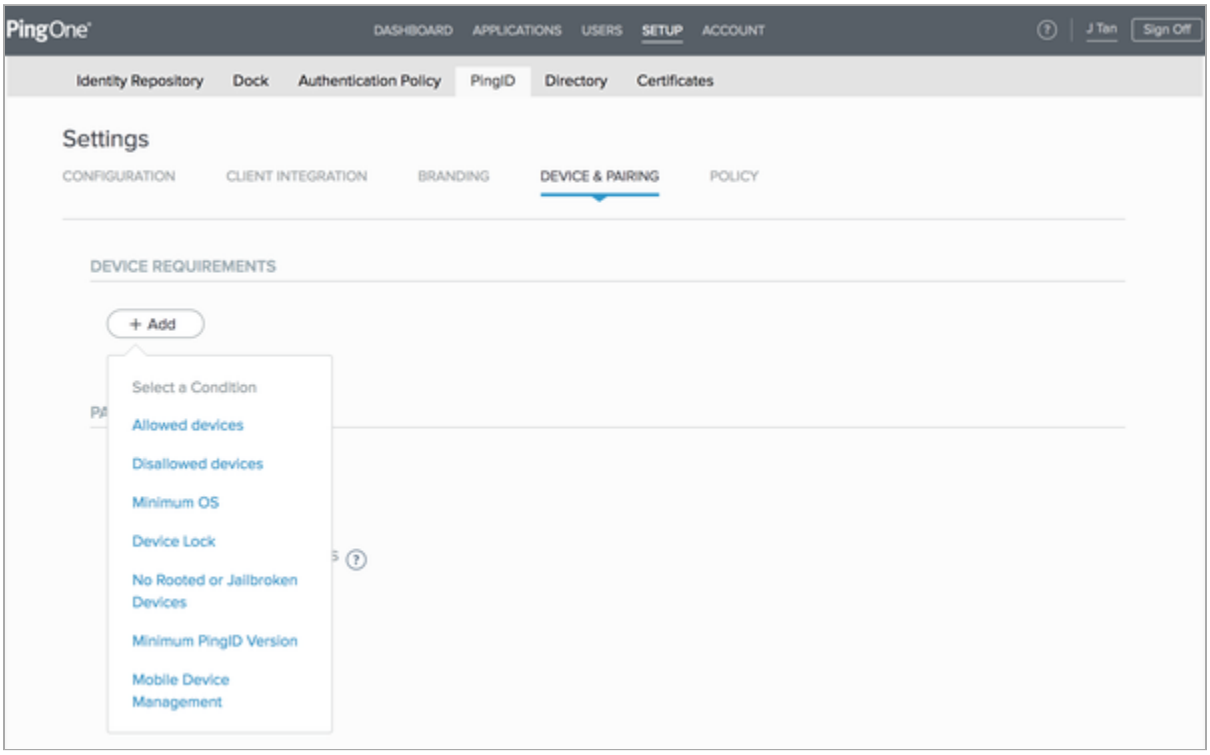
About this task

Multiple keys can coexist, for example, for allowing time for rotating keys and the time it takes to phase in new keys and retire old ones. PingID checks all listed keys to verify a match with the key submitted in the authentication request.

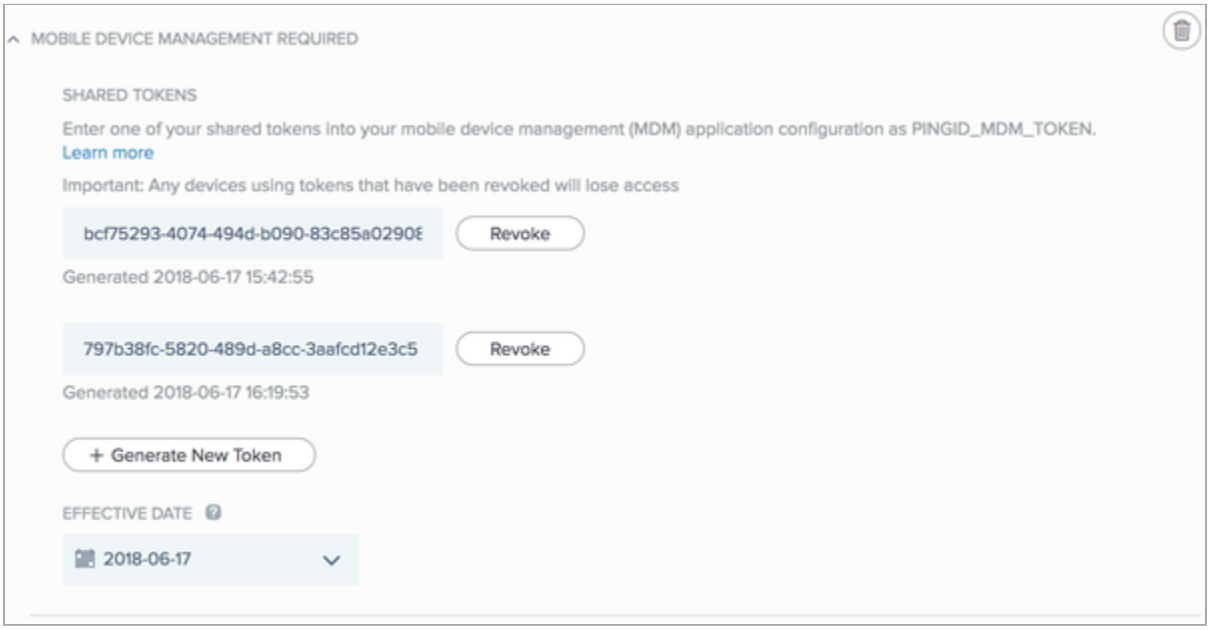
> **Note**
>
> The MDM does not retain multiple values for the same token. Support for multiple keys is provided through PingID.

Steps

1. Go to **Setup → PingID → DEVICE & PAIRING**.
2. In the **DEVICE REQUIREMENTS** section, click **+Add**.



3. From the **Select a Condition** list, select **Mobile Device Management**.
4. Click the **Expand** icon for **MOBILE DEVICE MANAGEMENT REQUIRED**.
5. Click **+ Generate New Token** to create a new PingID key for MDM.



> **Note**
>
> The generated date following each token indicates the date and time of its creation.

6. Click **Save**.

7. Copy the value of the new **SHARED TOKEN** key.
8. Update the token key in the MDM system:
    1. Sign on to the MDM system, and go to the app configuration settings page.
    2. Update the `PINGID_MDM_TOKEN` token key.
    3. Delete the existing key value. In its place, paste the value of the new **SHARED TOKEN** key that you copied from the PingID admin portal.

    See the following examples for the supported MDM systems:

    - Updating a PingID token in Workspace ONE UEM
    - Updating a PingID token in MobileIron
    - Updating a PingID token in Microsoft Intune

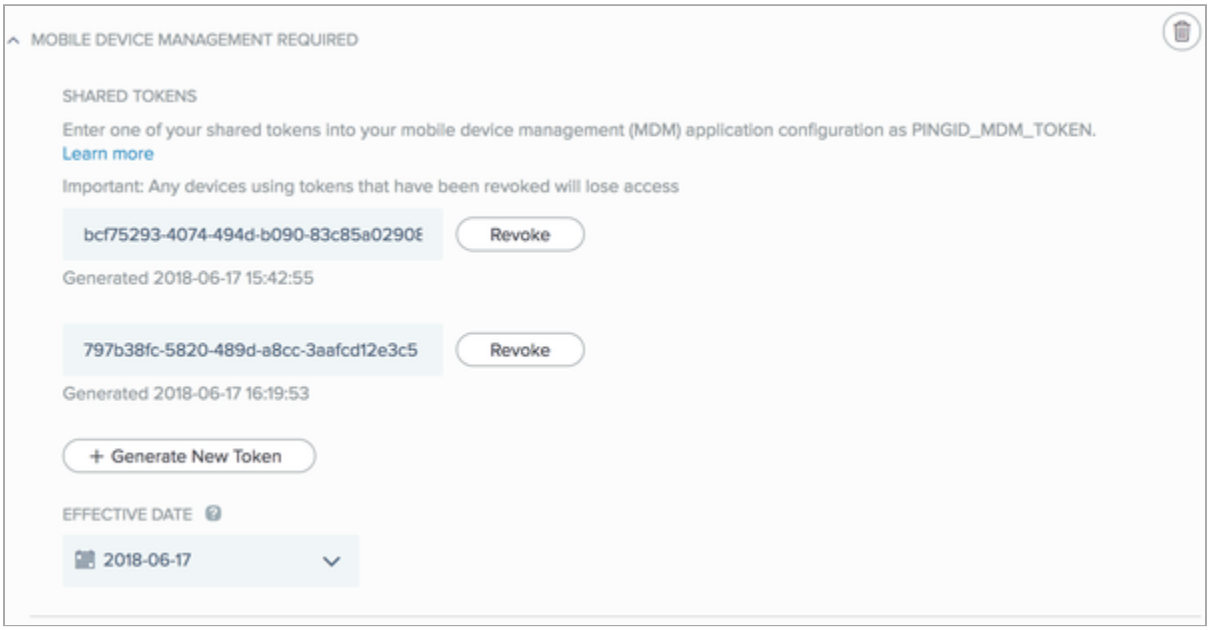
Revoking an MDM token

Organizational security policies might require periodic revocation of retired or obsolete tokens to prevent use of old tokens for authentication.

Steps

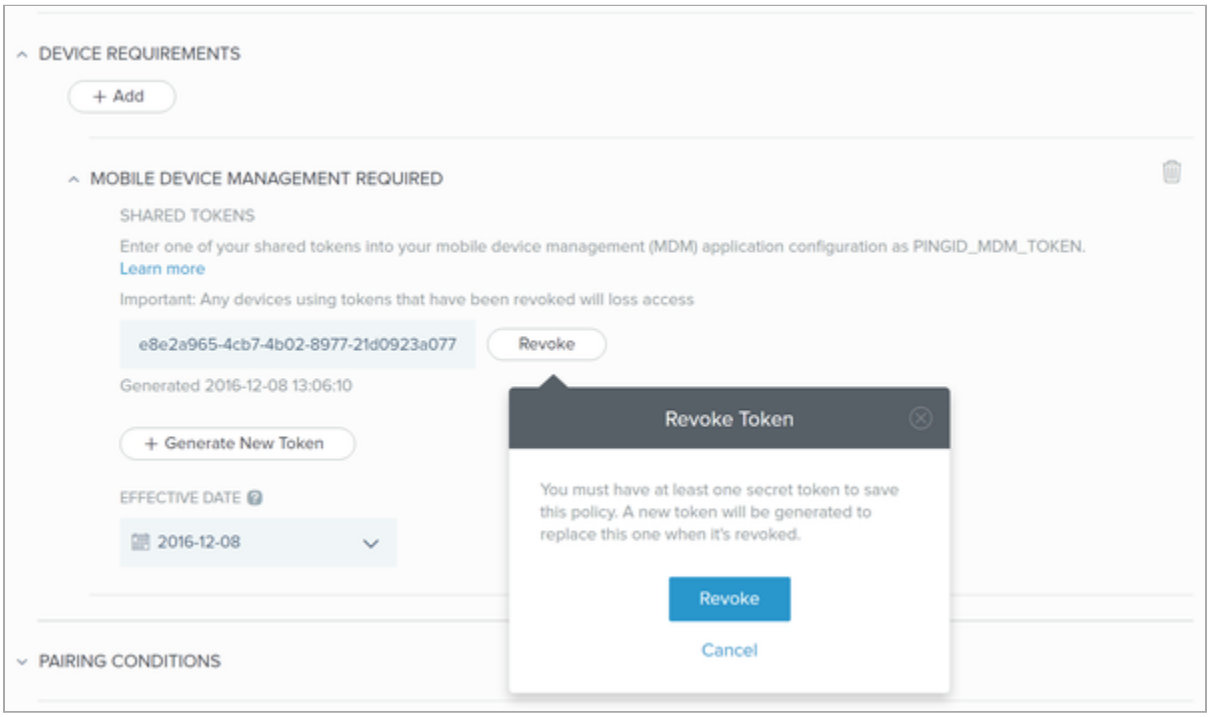
1. Go to **Setup → PingID → DEVICE & PAIRING**.
2. Click the **Expand** icon for **DEVICE REQUIREMENTS**.
3. Click the **Expand** icon for **MOBILE DEVICE MANAGEMENT REQUIRED** to expand the section.
4. Scroll the list of tokens to identify and locate the old token to be revoked.

> **Note**
>
> The generated date following each token indicates the date and time of its creation.



5. Click **Revoke** to remove the associated key.

> **Note**
>
> A minimum of one token must be retained. When there is only one token, clicking **Revoke** will offer the option to replace the existing token with a new generated token.



> **Caution**
>
> If a new token was generated as the result of revoking the single listed token, all devices will be prevented from authenticating until the new token value is both updated in the MDM, and distributed to all devices. Consider setting the **EFFECTIVE DATE** to a future date to permit time for distribution of the new token to all devices.

6. Click **Save**.

Rotating MDM tokens

Organizational security policies might require periodic rotation of MDM tokens to prevent use of old tokens for authentication.

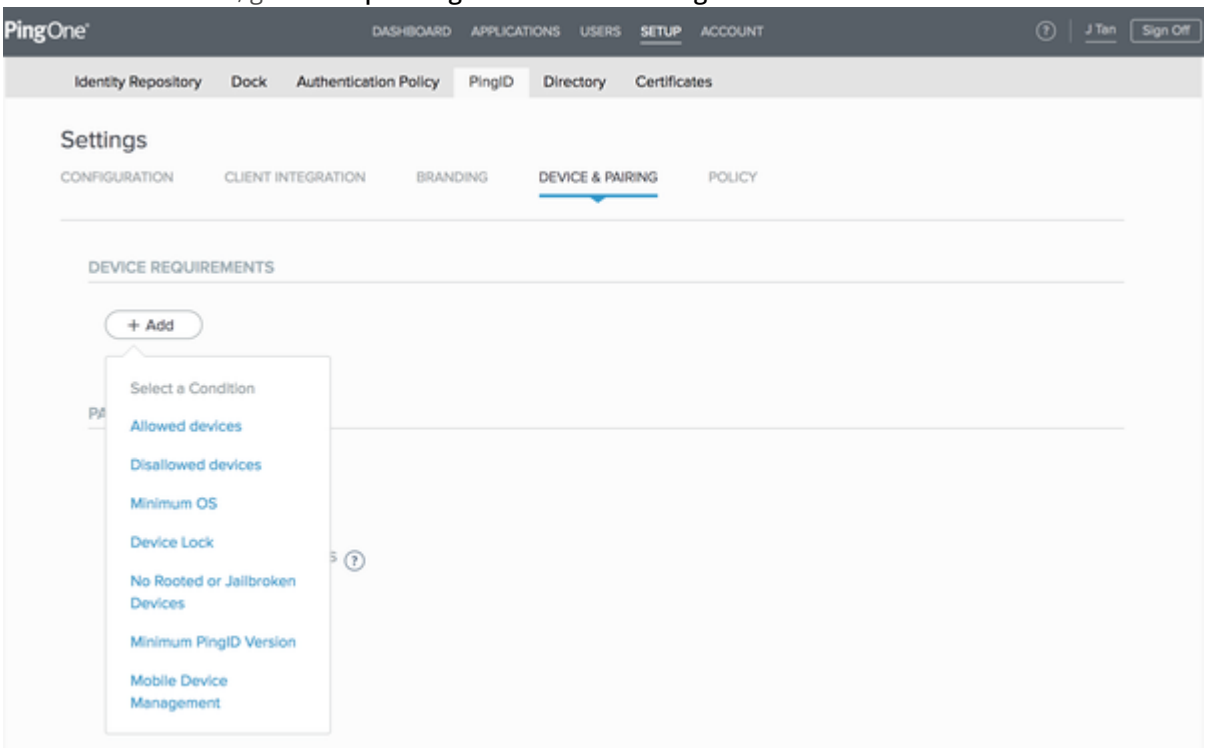
About this task

Rotation is implemented by adding a new token, distributing it to all managed devices, and then removing (revoking) the old token.

> **Important**
>
> More than one token should coexist to permit token rotation without blocking users from authentication.

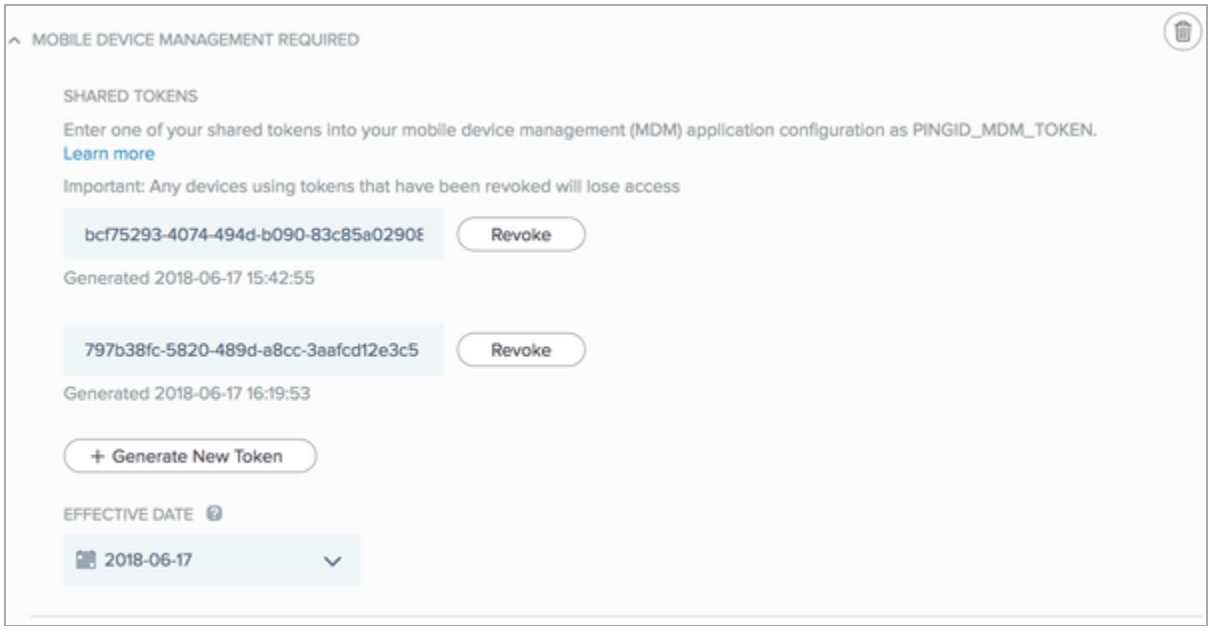
Steps

1. In the admin console, go to **Setup → PingID → Device & Pairing**.



Identify and locate the old token to be revoked.

> **Note**
>
> The generated date following each token indicates the date and time of its creation.



Third-party MDM system configuration for PingID integration

Configuration of any third party mobile device management (MDM) system for the purpose of integrating with PingID typically requires the following steps.

1. Generate and configure an Apple Push Notification Service (APNS) certificate for iOS in the MDM system.
2. Configure Android for Work in the MDM system so that the PingID app configuration can be pushed to managed phone sets.
3. In the organization's MDM system, add PingID as a managed app, and configure the token that was generated in the PingID admin portal.

Examples of these configuration steps are available for the officially supported MDM systems:

- Configuring Workspace ONE UEM for PingID
- Configuring MobileIron for PingID
- Configuring Microsoft Intune for PingID

Configuring Workspace ONE UEM for PingID

To manage the PingID app using Workspace ONE UEM (formerly known as AirWatch), you must apply several configuration settings.

The initial Workspace ONE UEM configuration comprises the following:

1. Installing an APNs certificate for iOS in Workspace ONE UEM
2. Configuring Android for Work for Workspace ONE UEM
3. Configuring Workspace ONE UEM for PingID MDM integration

Ongoing maintenance

As part of MDM maintenance activities, new tokens for the PingID app can be generated and old tokens revoked. For more information, see the following topics:

- In PingID:
  - Adding a new MDM token
  - Revoking an MDM token
  - Rotating MDM tokens
- In Workspace ONE UEM:
  - Updating a PingID token in Workspace ONE UEM

> **Note**
>
> The previous configuration steps are for use cases where PingID MFA authenticating devices are managed by the Workspace ONE UEM MDM. In cases where PingFederate is used to apply policies on accessing devices managed by Workspace ONE UEM, see Workspace ONE UEM Integration Kit.

Installing an APNs certificate for iOS in Workspace ONE UEM

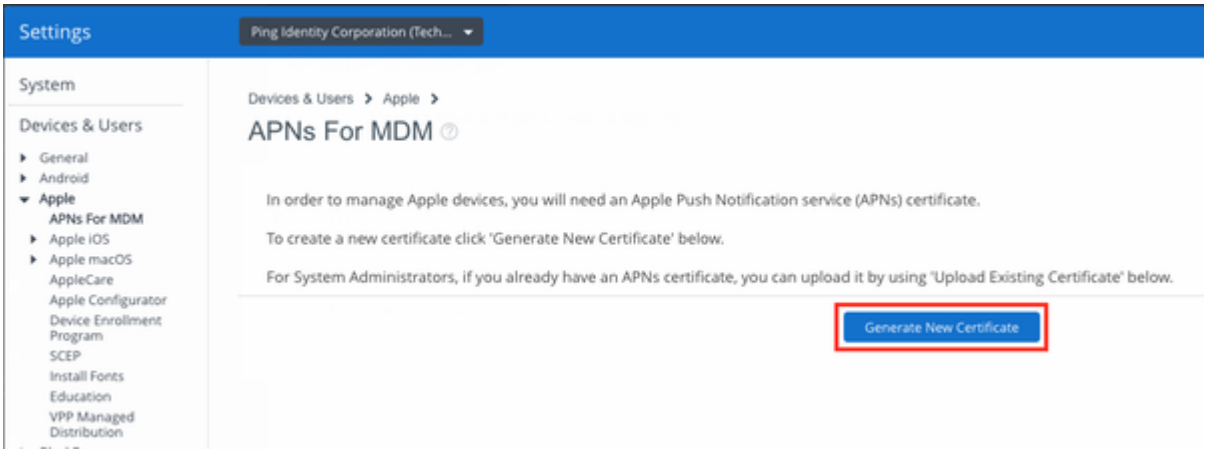
Install an Apple Push Notification service (APNs) certificate in Workspace ONE UEM.

About this task

To support iOS devices, an Apple mobile device management (MDM) certificate must be installed in the organization's MDM.

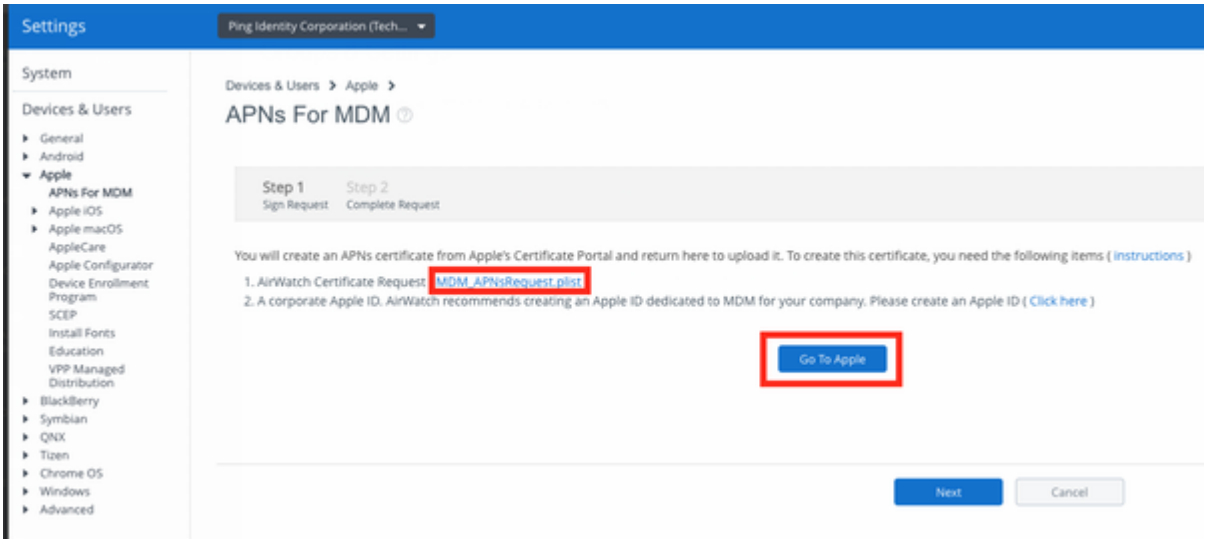
Steps

1. In the Workspace ONE UEM admin console, download an APNS certificate signing request (CSR).
   1. Go to **Settings → Apple → APNs for MDM**.
   2. Click **Generate New Certificate**.

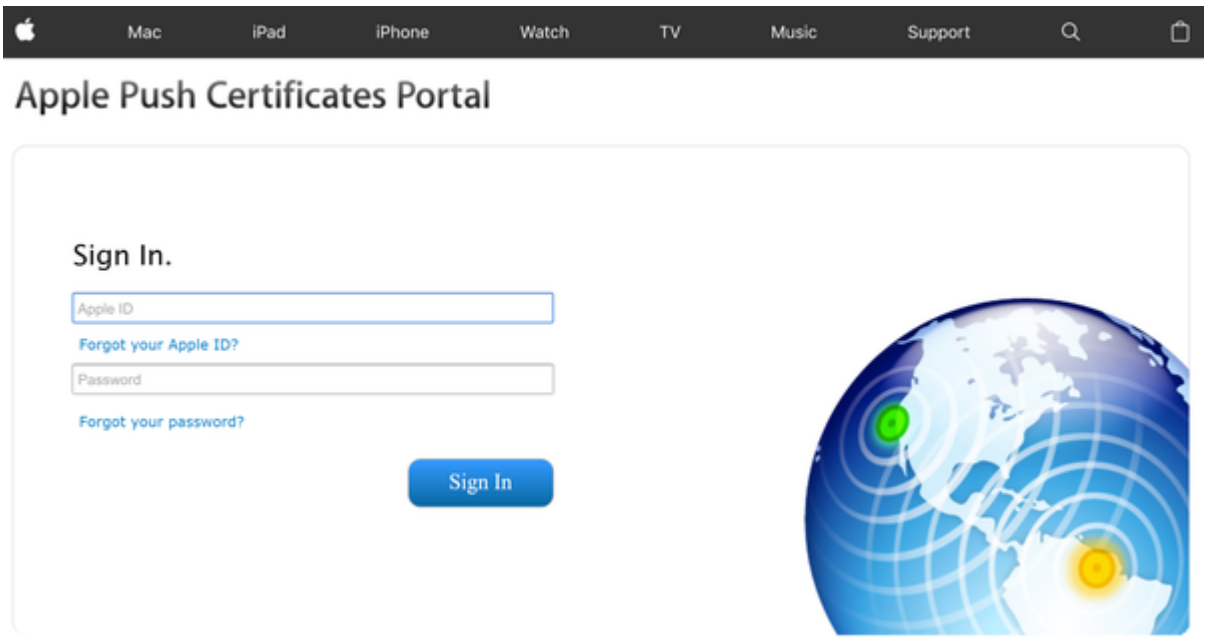


3. Click **MDM_APNsRequest.plist**.

4. Click **Go To Apple**.



2. Sign on to the Apple Push Certificates Portal.

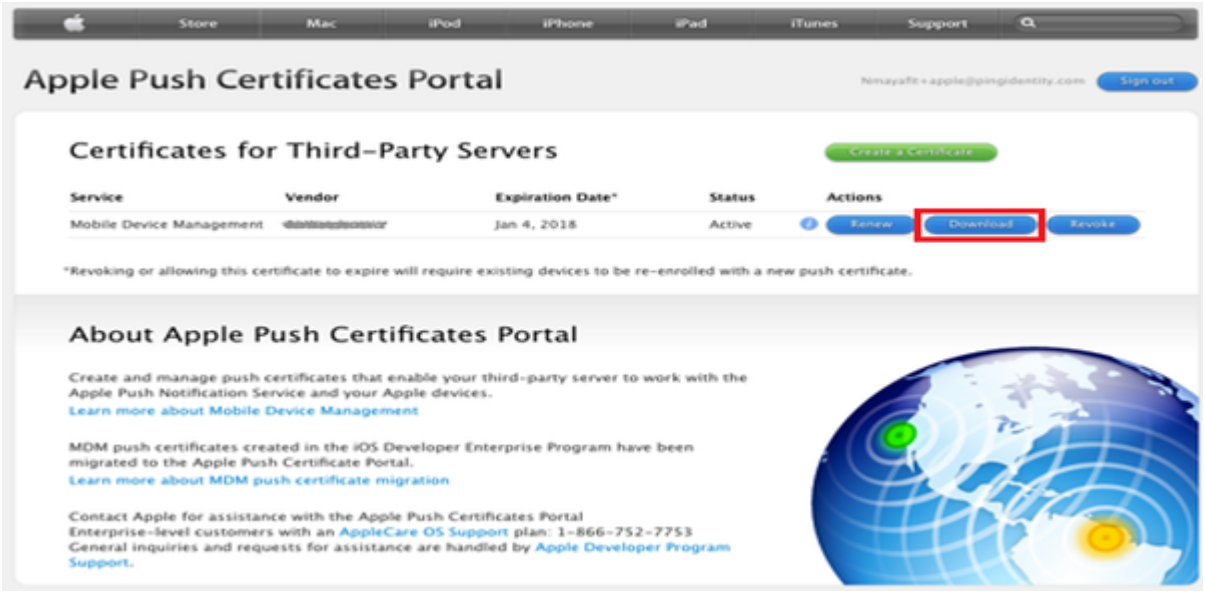


3. Click **Create a Certificate** on either the **Get Started** window or the **Certificates for Third-party Servers** window.

> **Note**
>
> If your organization does not yet have any Apple Push Certificates, the **Get Started** section is displayed. Otherwise, the **Certificates** list view window is displayed.
>
> 
>

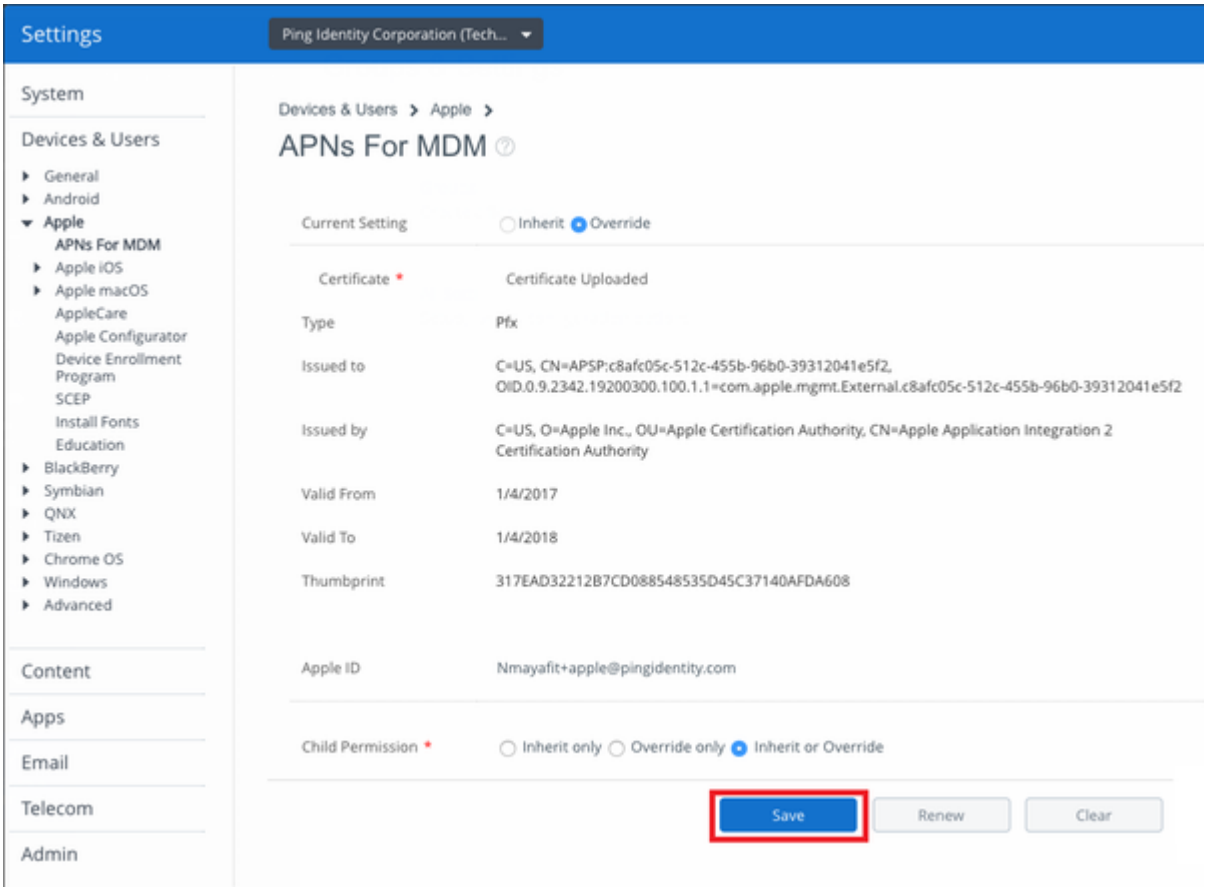
4. To browse for the CSR file created earlier, click **Choose File**, and then click **Upload**.

5. Click **Download**.



6. Upload the APNs certificate in Workspace ONE UEM.

    1. Go to **Devices & Users → Apple → APNs for MDM**.



7. Click **Save**.

Configuring Android for Work for Workspace ONE UEM

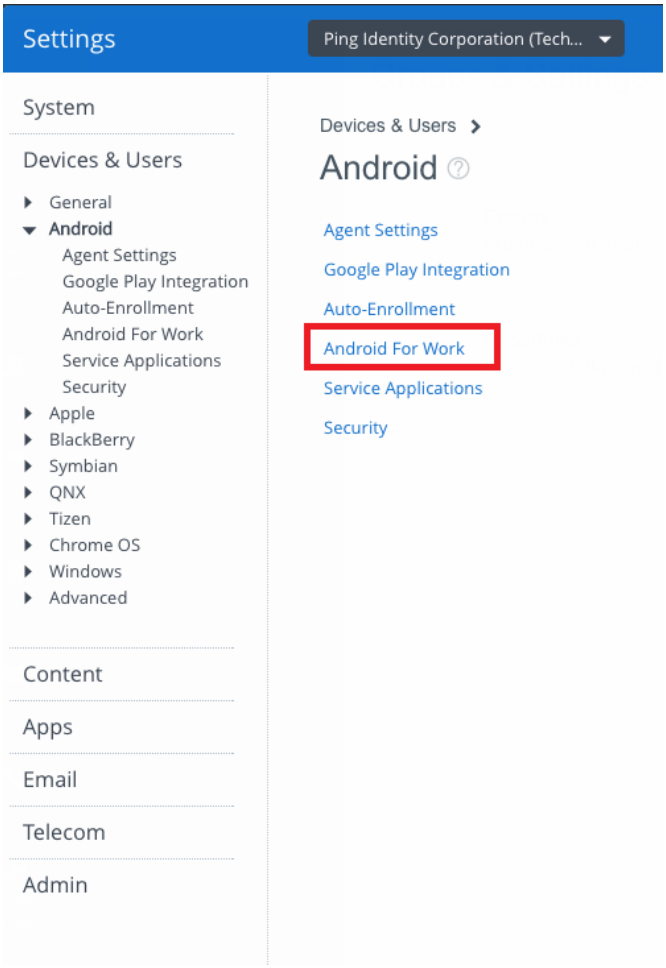
Configure Android for Work for the organization's mobile device management (MDM) so the PingID app configuration can be pushed to Android devices.

About this task

> **Note**
>
> This is an example configuration of Android for Work with G Suite. Android for Work can also be configured for MDM without G Suite.

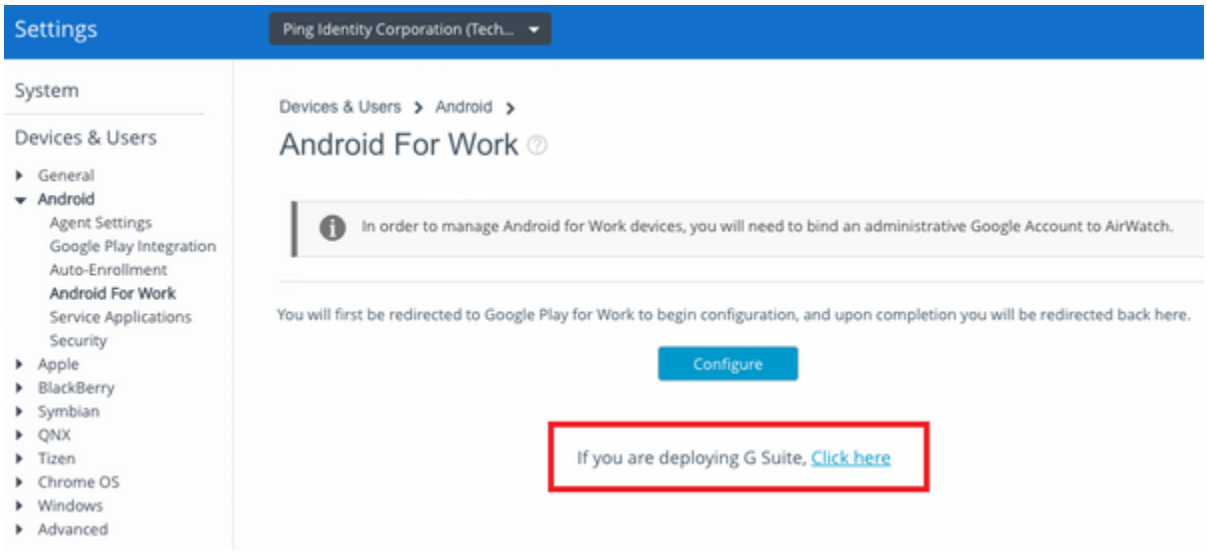
Steps

1. In Workspace ONE UEM, go to **Settings → Devices & Users → Android → Android For Work**.

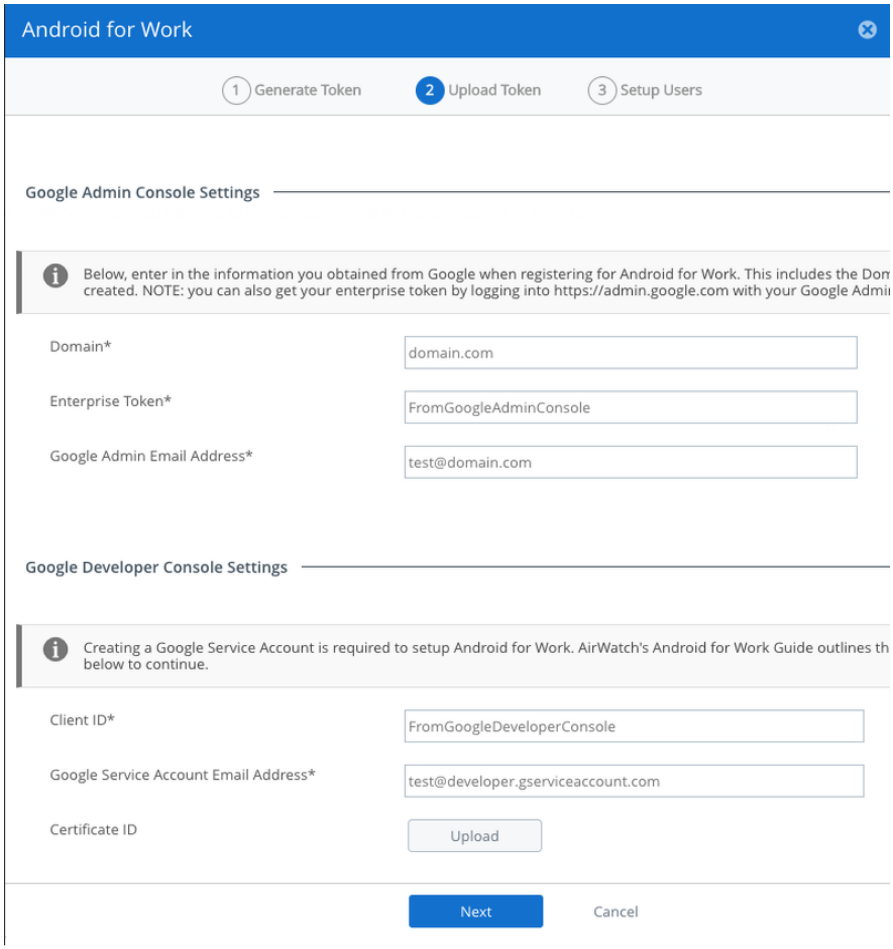


2. Click **Click here**.

   The browser redirects to G Suite, and on completion of the configuration, returns to Workspace ONE UEM.



3. In Workspace ONE UEM, in the **Android For Work** window, click **Configure**, and fill in the required details.



Configuring Workspace ONE UEM for PingID MDM integration

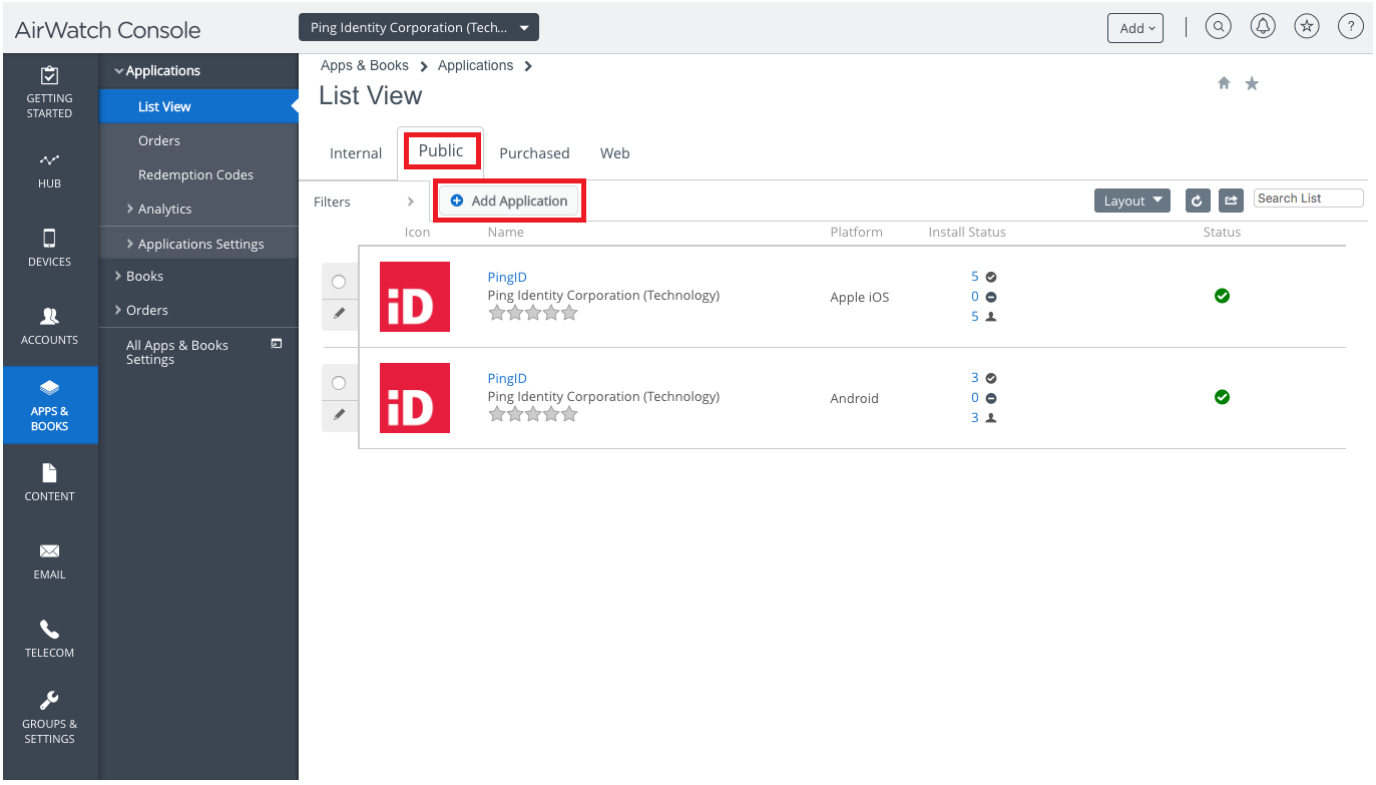
Configure PingID as a mobile device management (MDM) managed app in Workspace ONE UEM (formerly known as AirWatch).

About this task

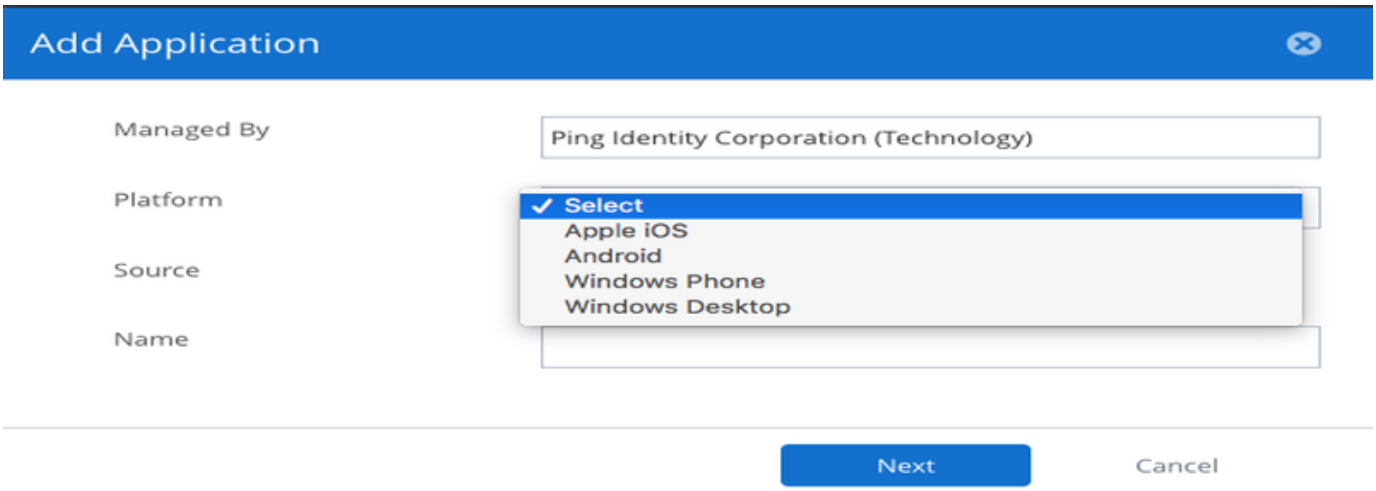
> **Important**
>
> The procedure detailed here is the iOS example for the configuration of Workspace ONE UEM for PingID MDM integration. The procedure for Android is identical. If the organization's MDM manages both iOS and Android devices, configure and save the entire procedure separately for each platform.

Steps

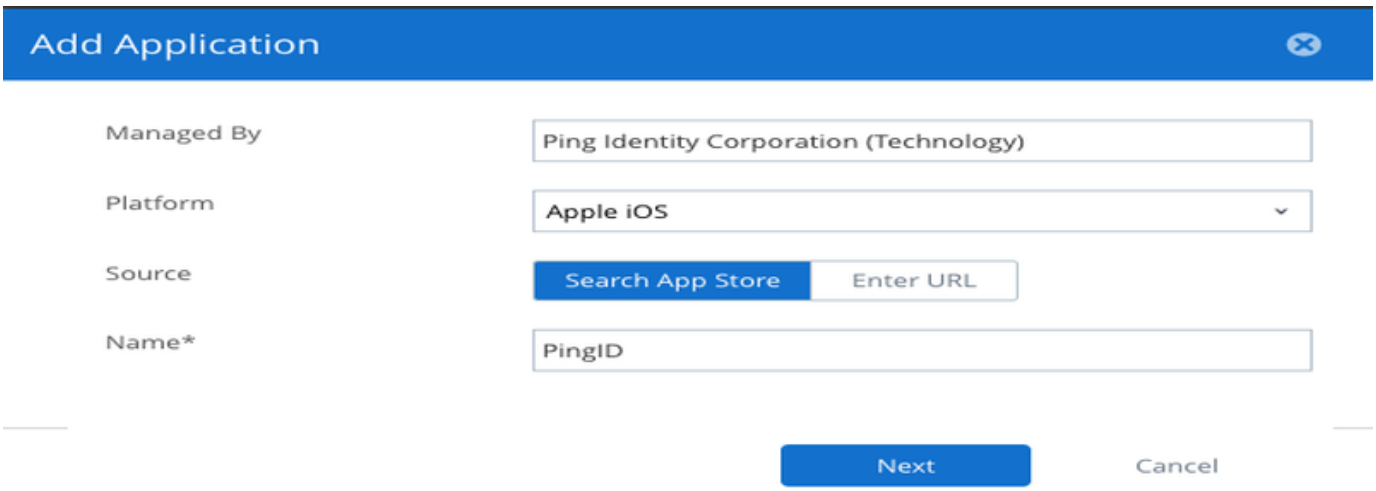
1. In the Workspace ONE UEM admin console, go to **Apps & Books → Applications → List View**
2. On the **Public** tab, click **Add application**.



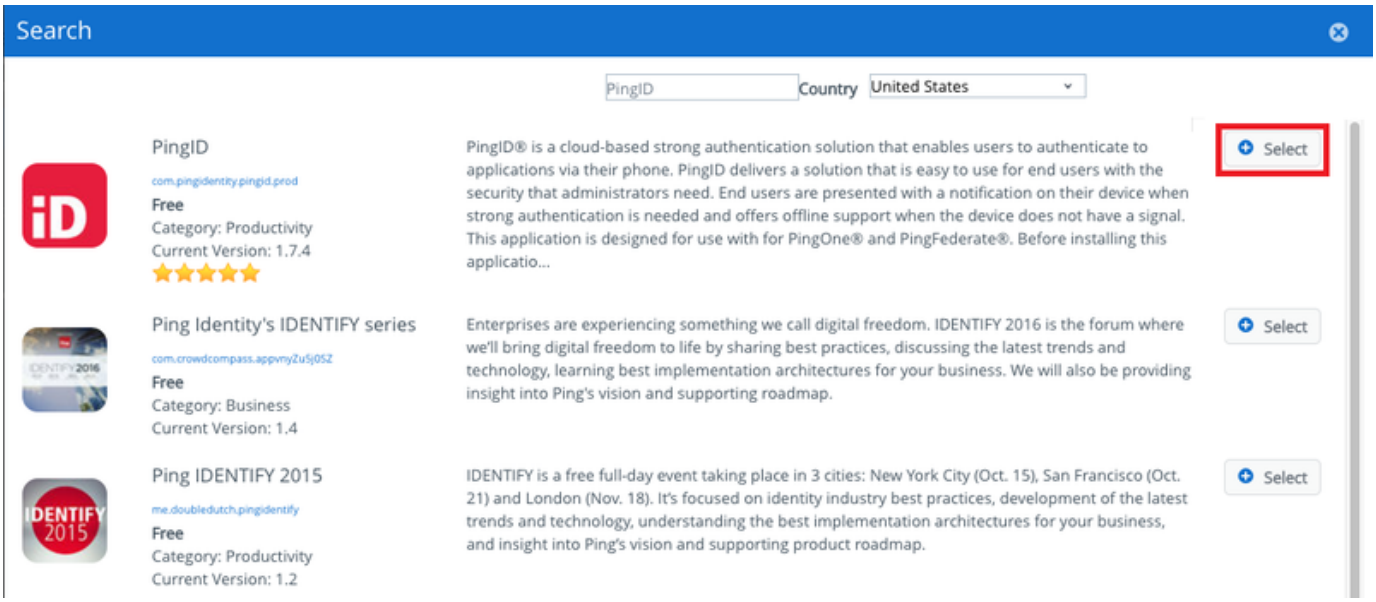
3. From the **Platform** list, select **Apple iOS**.



4. In **Source** field, click **Search App Store**.

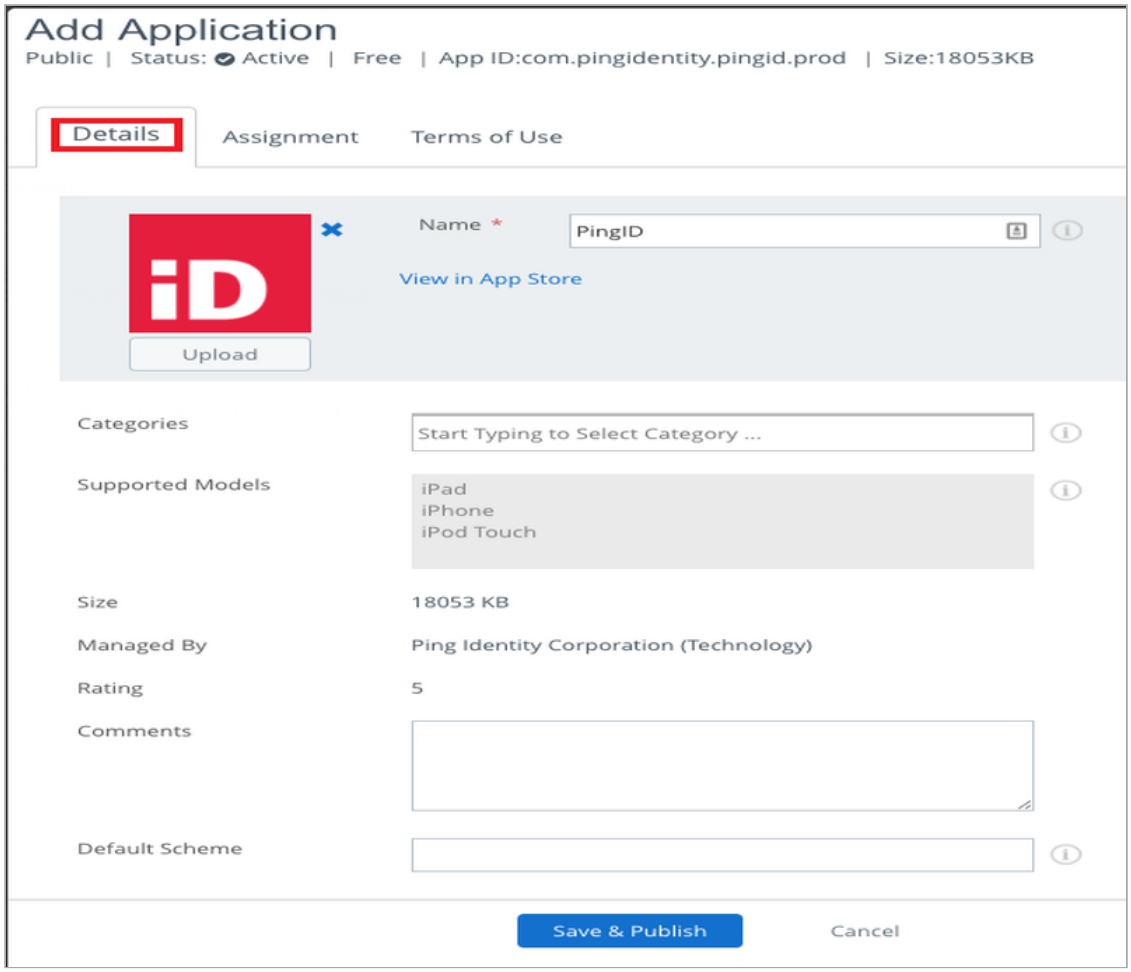


5. In **Name** field, enter `PingID`.
6. Click **Next**.
7. In the mobile app store, for the PingID mobile app, click **Select**.



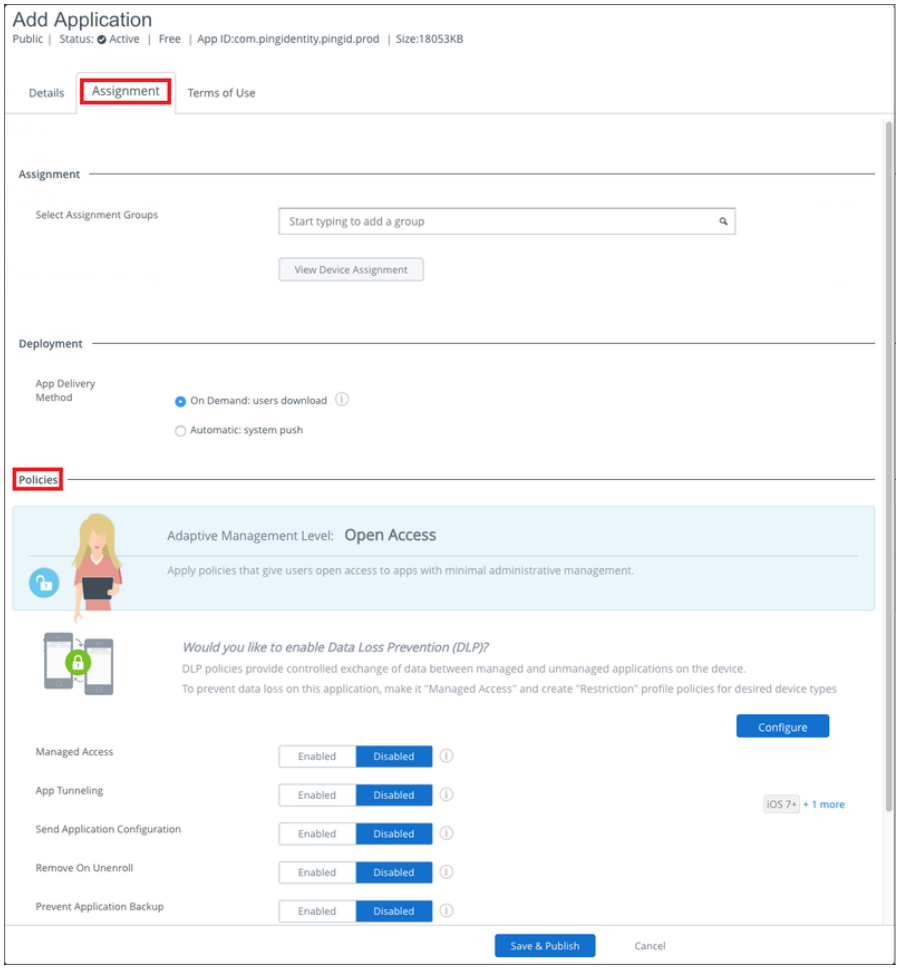
Result:

The PingID mobile app's details are displayed in the **Details** tab.



8. Click the **Assignment** tab.

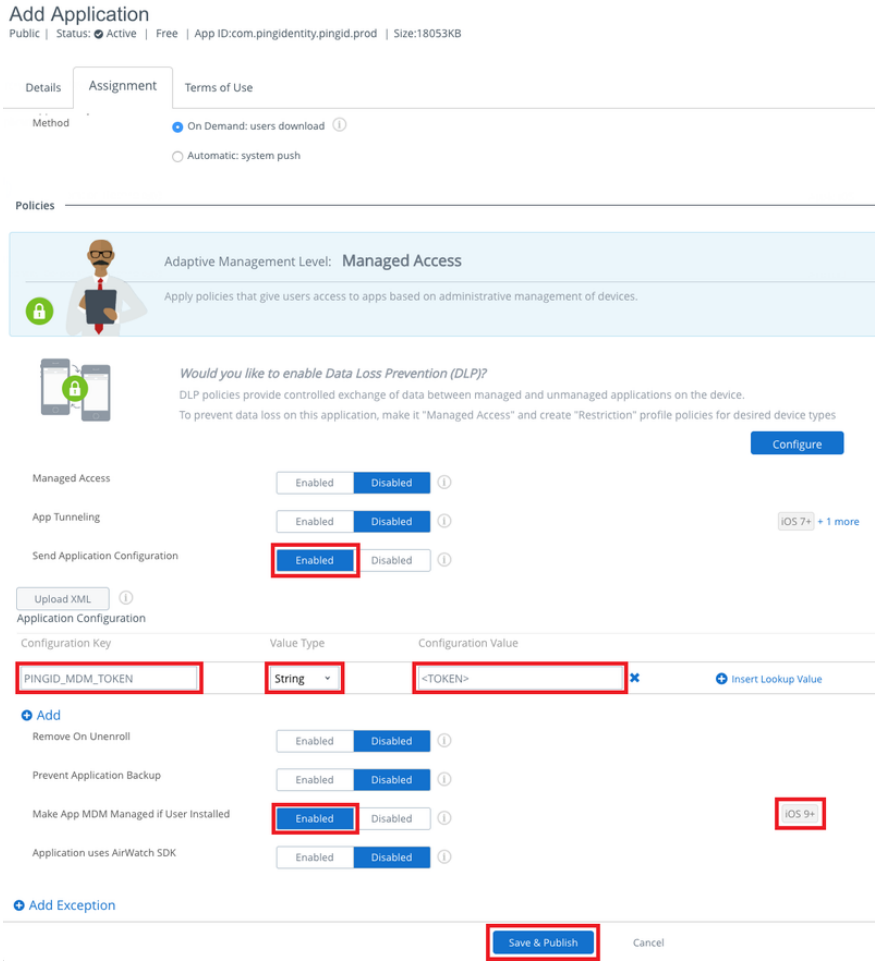
9. Go to the **Policies** section.



10. In the **Send Application Configuration** field, click **Enabled**.

    Result:

The **Application Configuration** section displays.



11. In the **Application Configuration** section, enter the following parameter values.

Parameter	Value
Configuration Key	`PINGID_MDM_TOKEN`. **Note** ◦ For iOS, the value `PINGID_MDM_TOKEN` must be entered manually. ◦ For Android, the value `PINGID_MDM_TOKEN` is prepopulated.
Value Type	`STRING`
Configuration value	The token string value for MDM, as generated in the PingID admin web configuration page.

12. In the **Make app MDM Managed If User Installed** field, click **Enabled**.

> **Note**
>
> This option transitions a non-managed app downloaded from the app store to a managed app. The user must approve it on their device.

> **Important**
>
> ***For Apple devices earlier than iOS 9 and Android devices***
>
> Users must execute the following steps:
>
> 1. Unpair the PingID mobile app on the iOS device.
> 2. Uninstall the PingID mobile app from the iOS device.
> 3. Reinstall the PingID mobile app, from the MDM's app catalog.
> 4. Pair the newly installed, MDM managed PingID mobile app.
>
> ***For Apple devices with iOS 9 and later***
>
> The user receives a notification on their device to approve the transition to MDM management. After user approval, the PingID mobile app installed on the iOS device is managed by the MDM.

13. Click **Save & Publish**.

> **Important**
>
> Repeat the entire configuration process for Android. The prerequisite to the Android app configuration is Configuring Android for Work for Workspace ONE UEM.

Updating a PingID token in Workspace ONE UEM

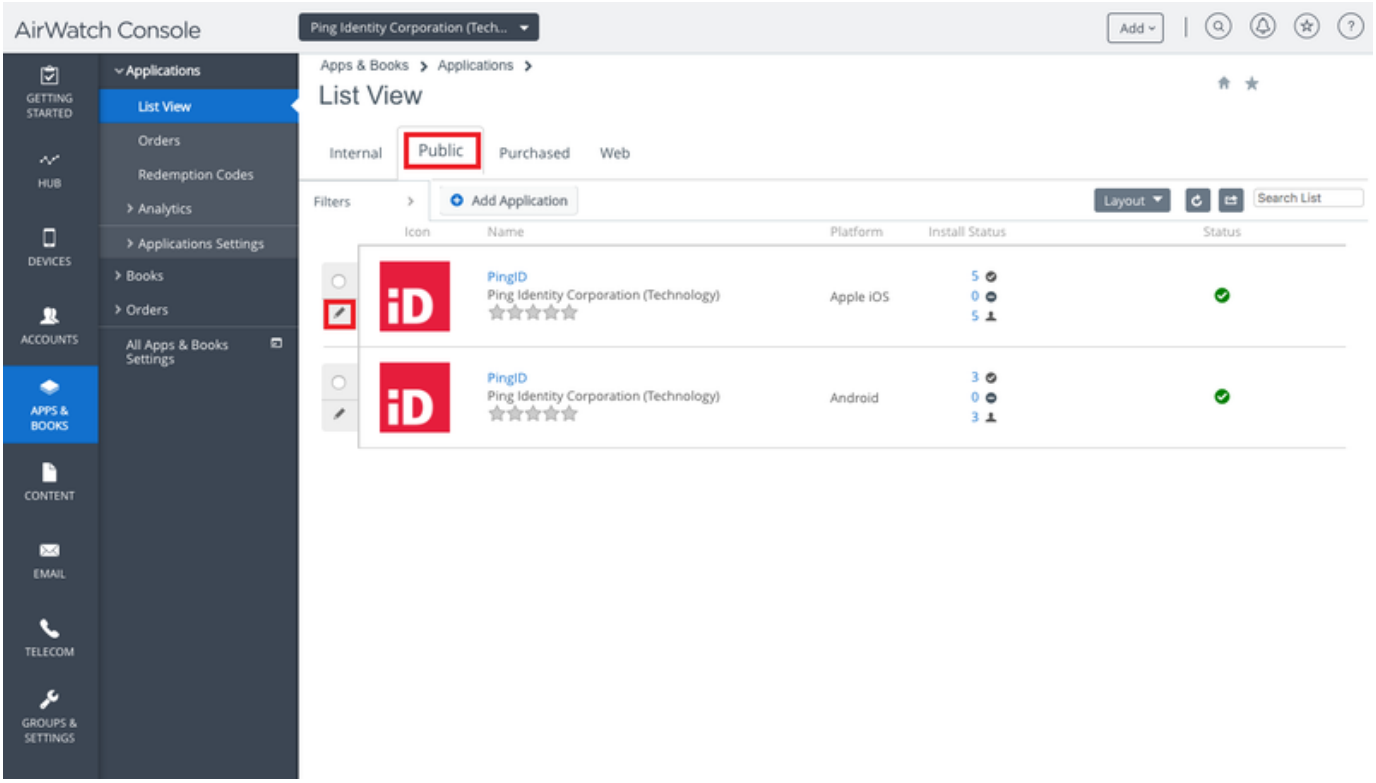
Update the token PingID managed app in Workspace ONE UEM for iOS.

About this task

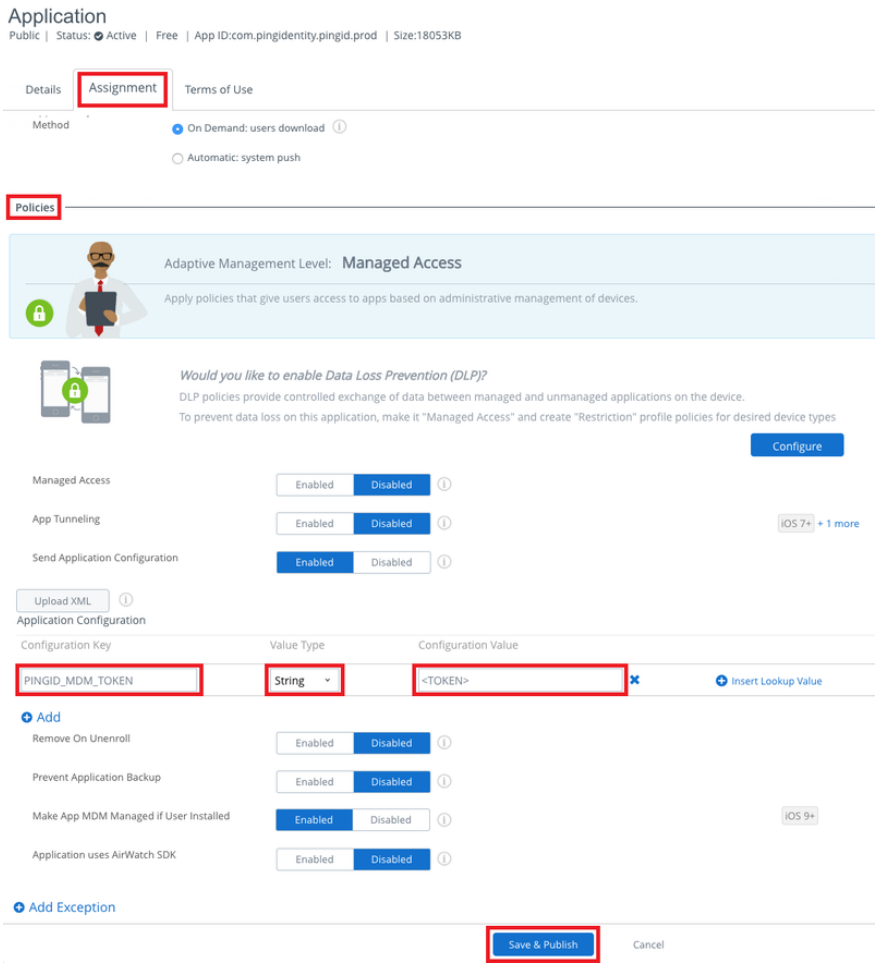
> **Important**
>
> You must configure and save the entire procedure separately for each platform.

Steps

1. In the Workspace ONE UEM admin console, go to **Apps & Books → Applications → List View**.
2. On the **Public** tab, select the **PingID iOS** app to edit, and then click the **Pencil** icon.



3. Click the **Assignment** tab.



4. Go to the **Policies** section.

5. In the **Application Configuration** section, enter the following parameter values.

Parameter	Value
Configuration Key	`PINGID_MDM_TOKEN`. **Note** ◦ For iOS, the value `PINGID_MDM_TOKEN` must be entered manually. ◦ For Android, the value `PINGID_MDM_TOKEN` is prepopulated.
Value Type	`STRING`
Configuration value	The token string value for MDM, as generated in the PingID admin web configuration page.

6. Click **Save & publish**.

> **Important**
>
> Repeat the entire process for Android.

Configuring MobileIron for PingID

To manage the PingID app using MobileIron, you must apply several configuration settings .

The initial MobileIron configuration comprises the following:

1. Installing an APNs certificate for iOS in MobileIron
2. Configuring Android for Work for MobileIron
3. Configuring MobileIron for PingID MDM integration

Ongoing maintenance

As part of mobile device management (MDM) maintenance activities, new tokens for the PingID app can be generated and old tokens revoked. For more information, see the following topics:

- For PingID:
  - Adding a new MDM token
  - Revoking an MDM token
  - Rotating MDM tokens
- For MobileIron:
  - Updating a PingID token in MobileIron

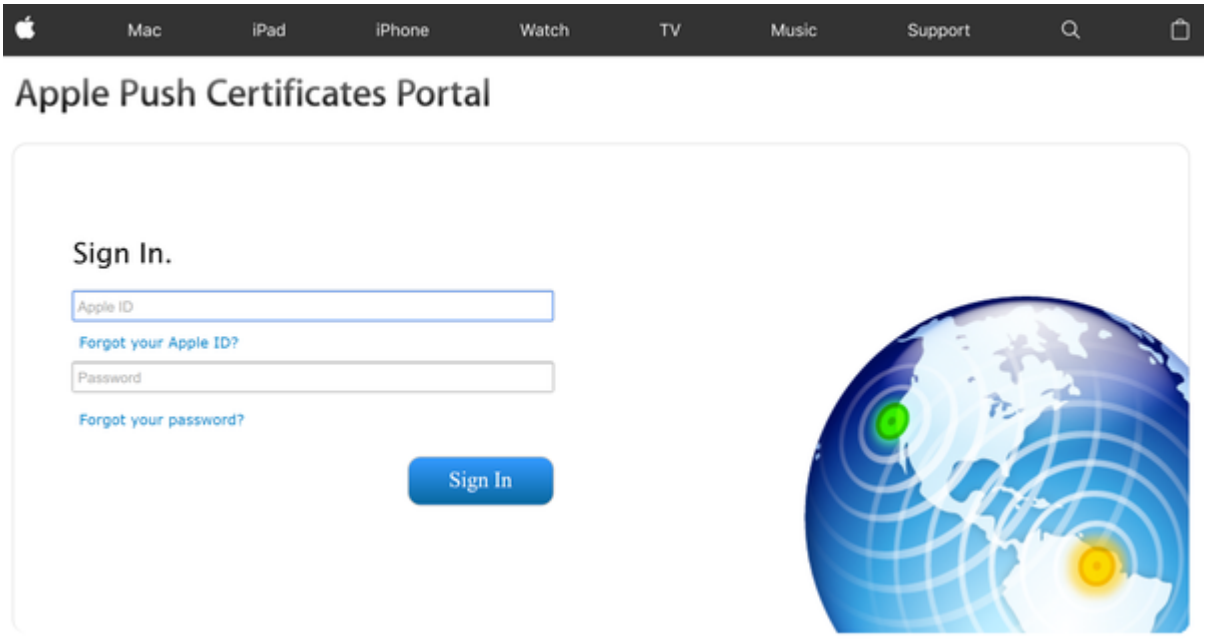
> **Note**
>
> The previous configuration steps are for use cases where PingID multi-factor authentication (MFA) authenticating devices are managed by the MobileIron MDM. In cases where PingFederate is used to apply policies on accessing devices managed by MobileIron, see PingFederate MobileIron Integration Kit.

Installing an APNs certificate for iOS in MobileIron

To support iOS devices, install an Apple mobile device management (MDM) certificate in the organization's MDM.

Steps

1. In the MobileIron admin console, download an Apple Push Notification service (APNs) Certificate Signing Request (CSR):
   1. Go to **Admin → Apple/iOS → MDM Certificate → Download**.
   2. Click **Download File**.
2. Sign on to the Apple Push Certificates Portal.

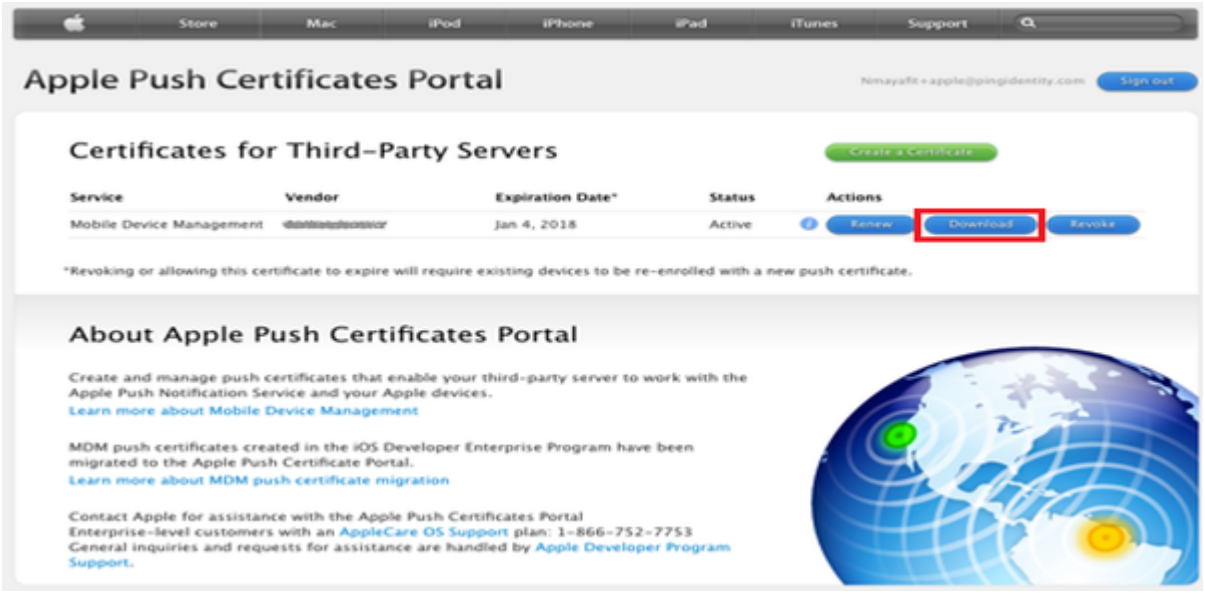


3. Click **Create a Certificate** on either the **Get Started** window, or the **Certificates for Third-party Servers** window.

> **Note**
>
> If your organization does not yet have any Apple Push Certificates, the **Get Started** section is displayed. Otherwise, the **Certificates** list view window is displayed.

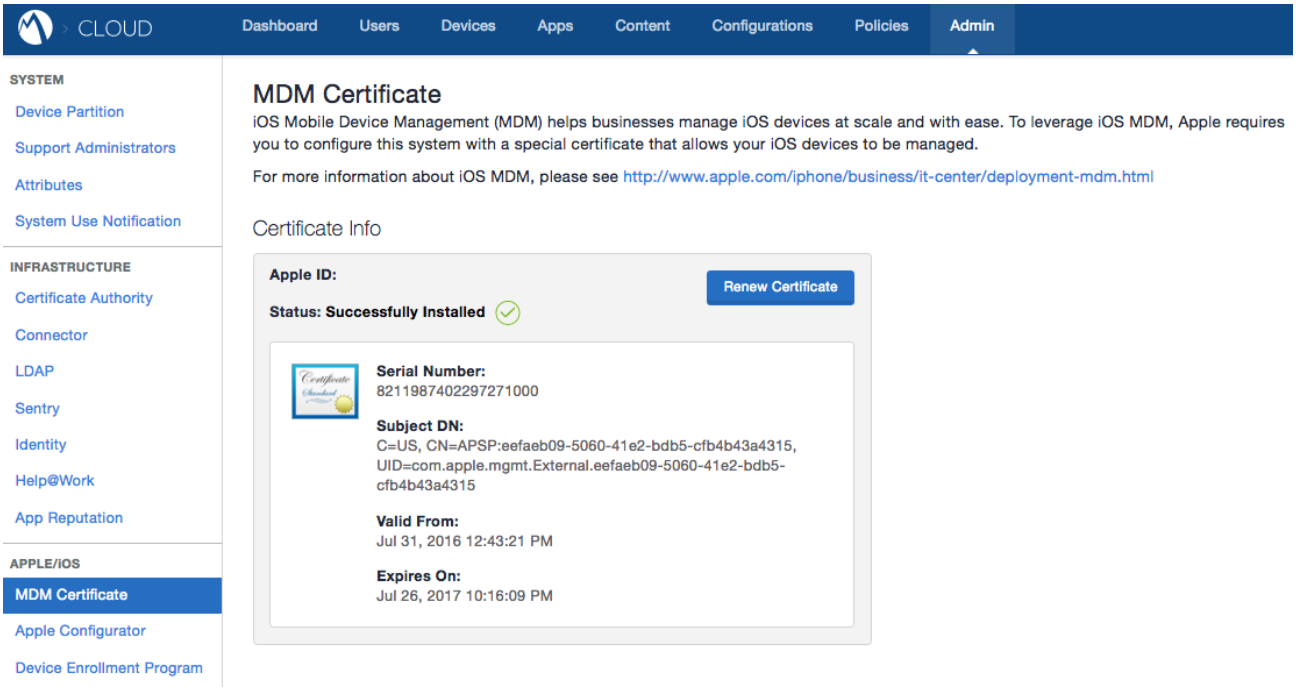
4. To browse for the CSR file created earlier, click **Choose File**, and then click **Upload**.

5. Click **Download**.



6. Upload the APNs certificate in MobileIron.

    1. Go to **Admin → Apple/iOS → MDM Certificate**.



7. Click **Save**.

Configuring Android for Work for MobileIron

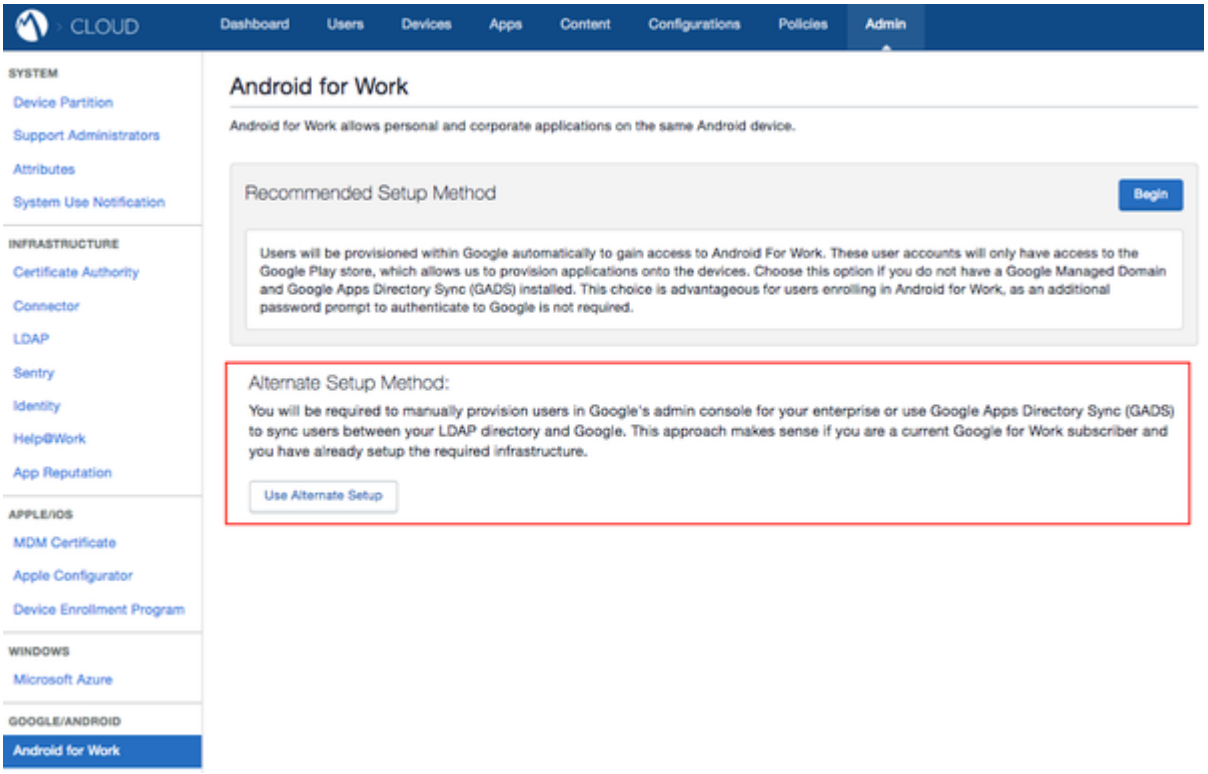
Configure Android for Work for the organization's mobile device management (MDM) so the PingID app configuration can be pushed to Android devices.

About this task

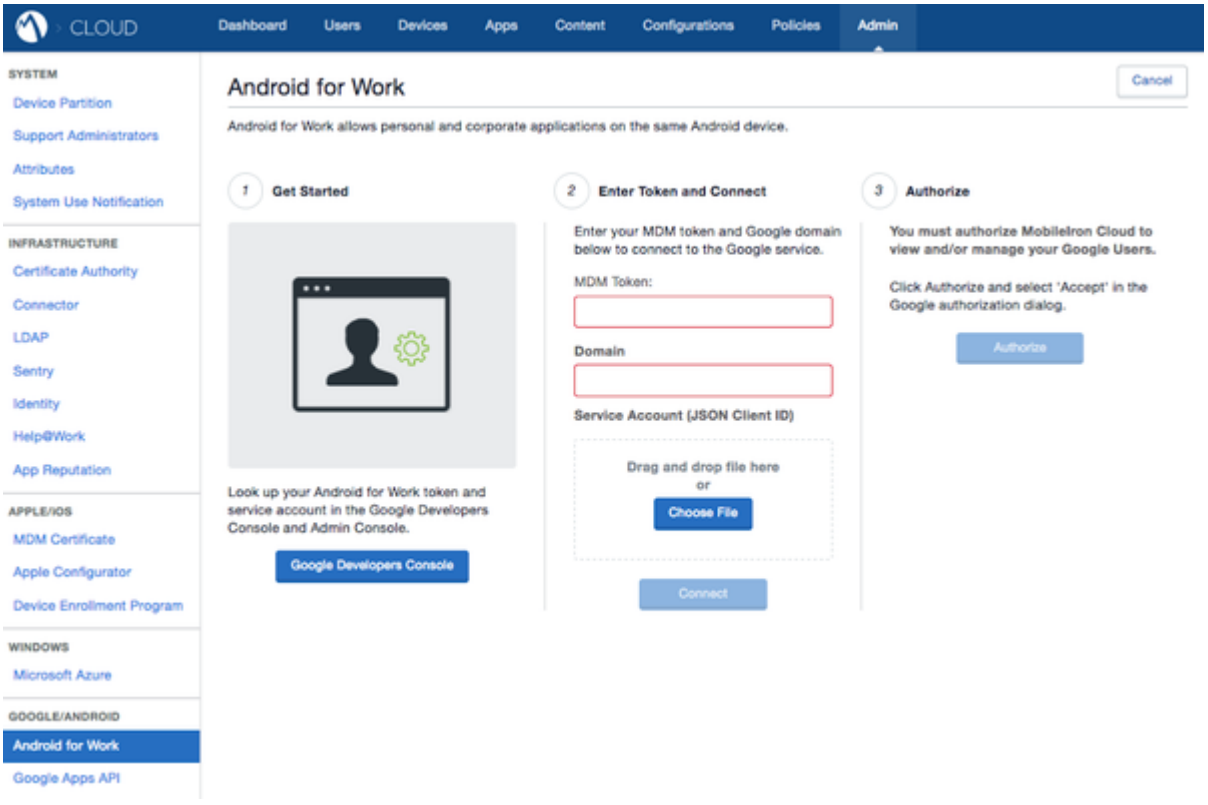
> **Note**
>
> This is an example configuration of Android for Work with G Suite. You can configure Android for Work MDM without G Suite.

Steps

1. Go to **Admin → Google/Android → Android for Work**, and then click **Use Alternate Setup**.



2. In **Get Started** section, click **Google Developers Console**, and follow the on-screen instructions.



3. In MobileIron's admin portal, under **Enter Token and Connect**, connect to your organization's Google service.

4. In the **MDM Token** field, enter the token from the previous step.

5. In the **Domain** field, enter the domain by uploading the JSON file created earlier from the Google Developers Console, and click **Connect**.
6. To enable MobileIron to manage your Google users, click **Authorize**.

Configuring MobileIron for PingID MDM integration

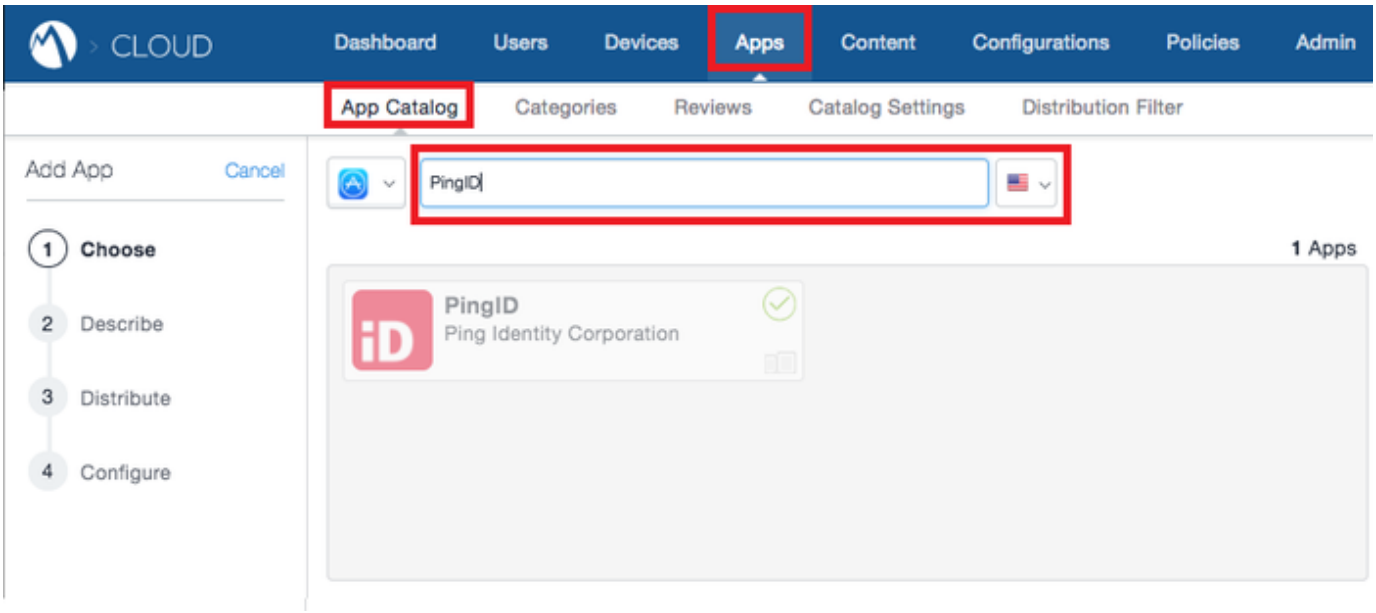
Configure PingID as a mobile device management (MDM) managed app in MobileIron.

About this task

> **Important**
>
> The procedure detailed below is the iOS example for the configuration of MobileIron for PingID MDM integration. The procedure for Android is identical. If the organization's MDM manages both iOS and Android devices, configure and save the entire procedure separately for each platform.

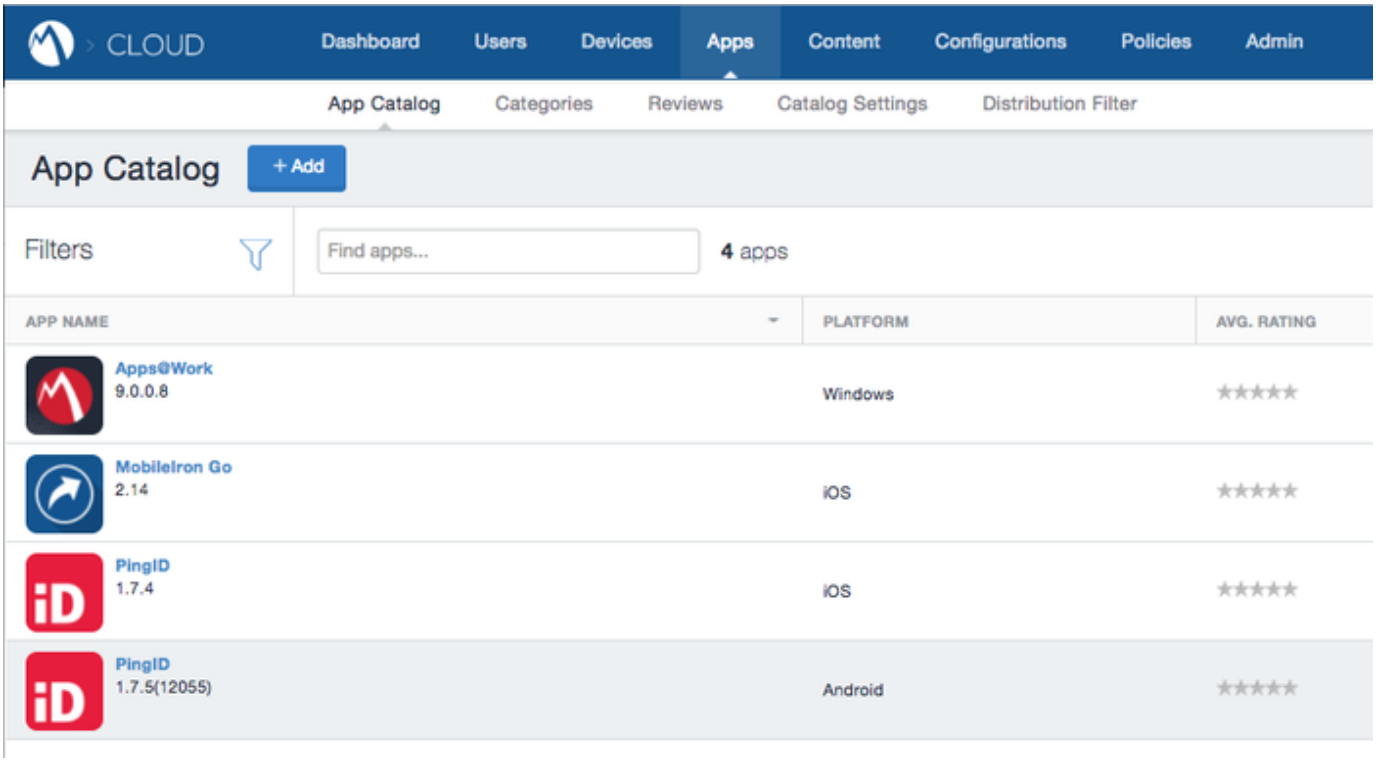
Steps

1. In the MobileIron admin console, go to **Apps → App Catalog**.
2. Choose the desired app store, and then search for PingID.

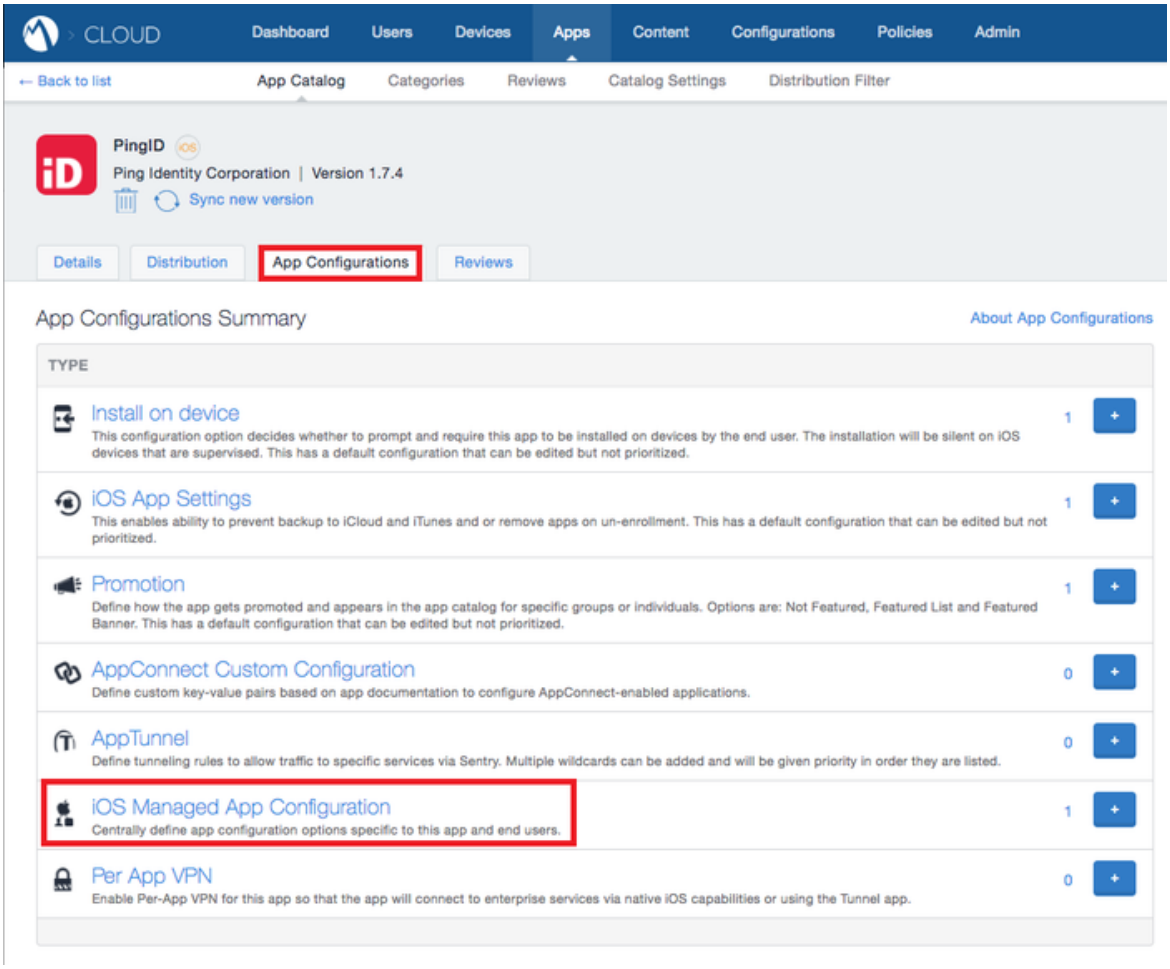


> **Note**
>
> The following steps describe the procedure for managing the PingID app for iOS. Repeat the procedure for the PingID app for Android.

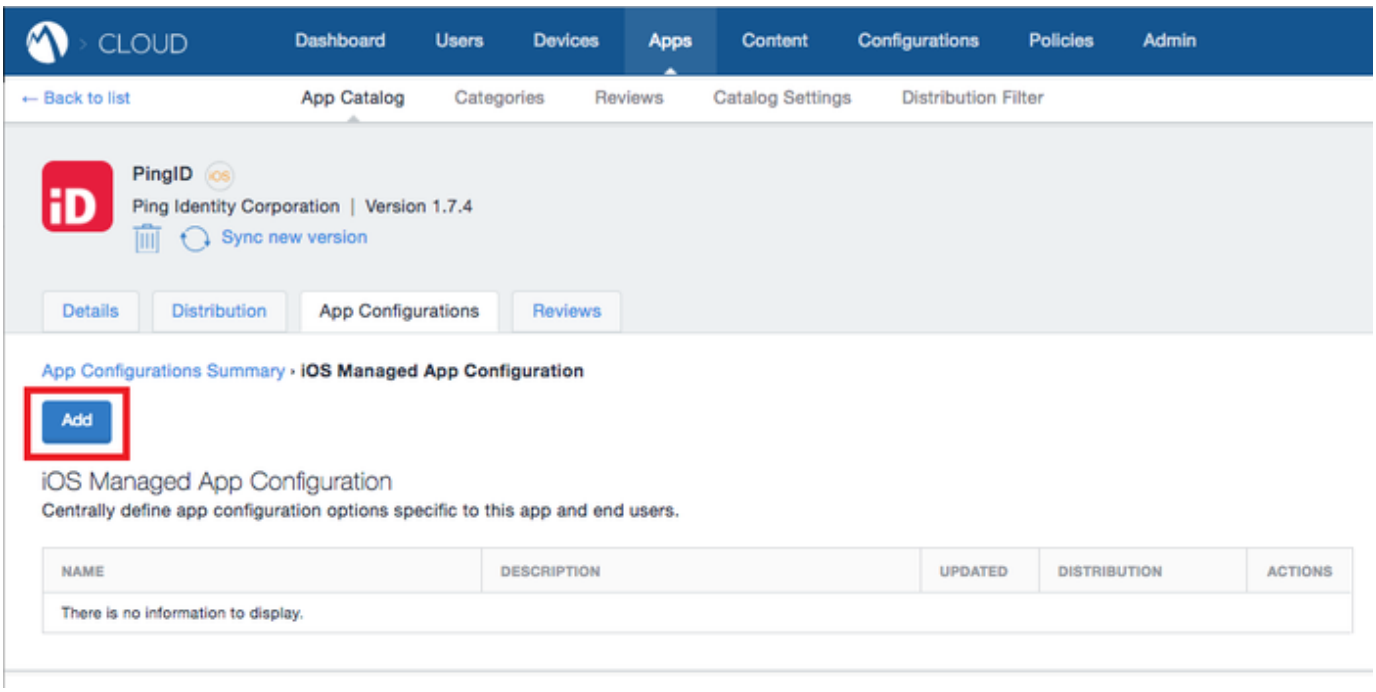
3. Select the PingID mobile app for iOS.



4. On the **App Configurations** tab, select **iOS Managed App Configuration**.

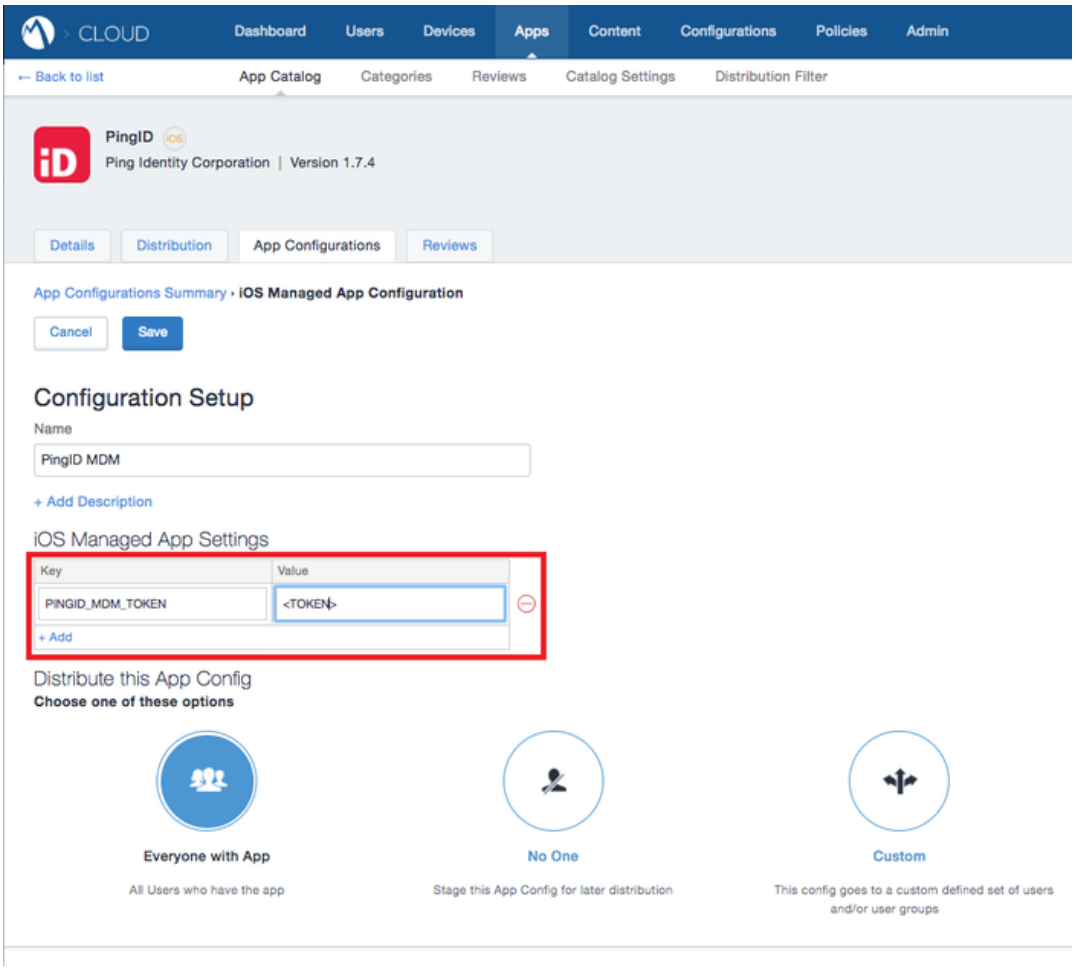


5. Click **Add**.

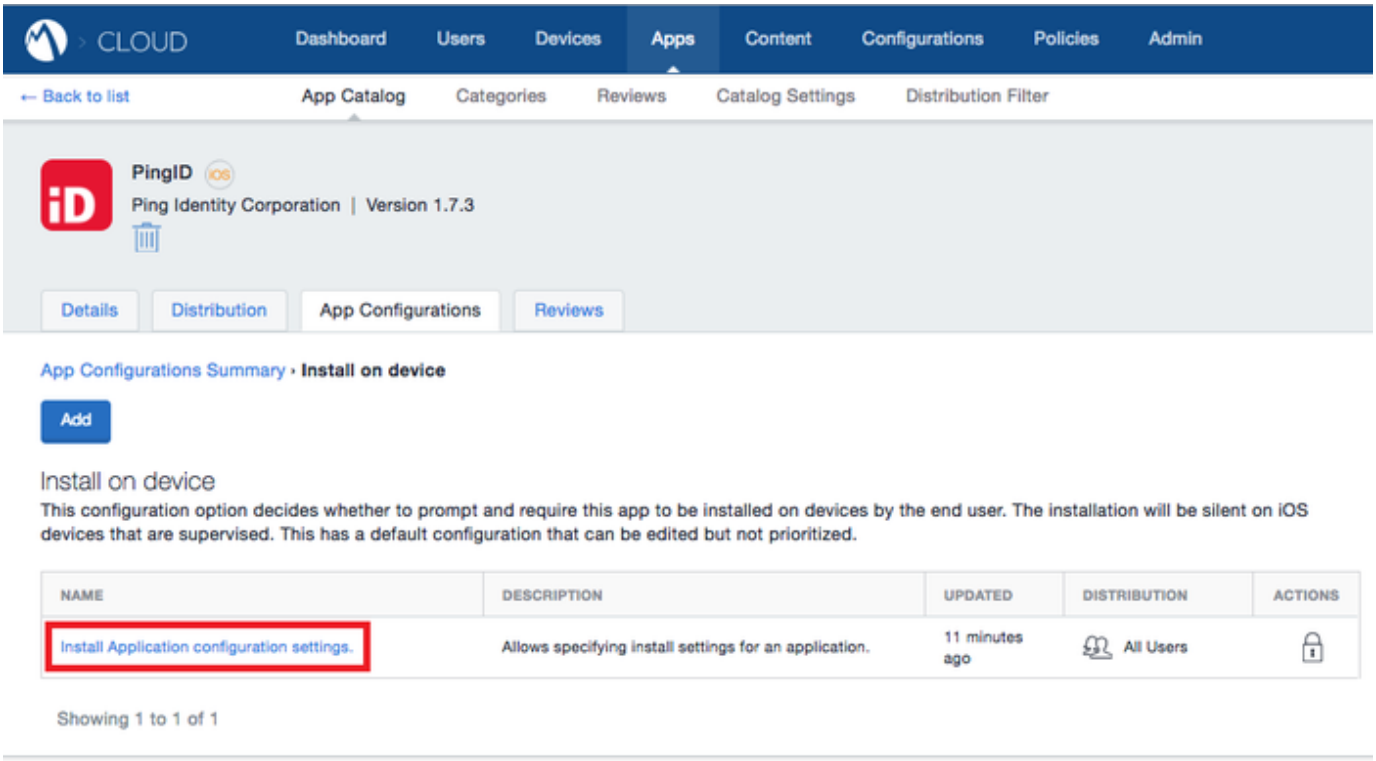


6. Enter the **Configuration Setup** parameter values.

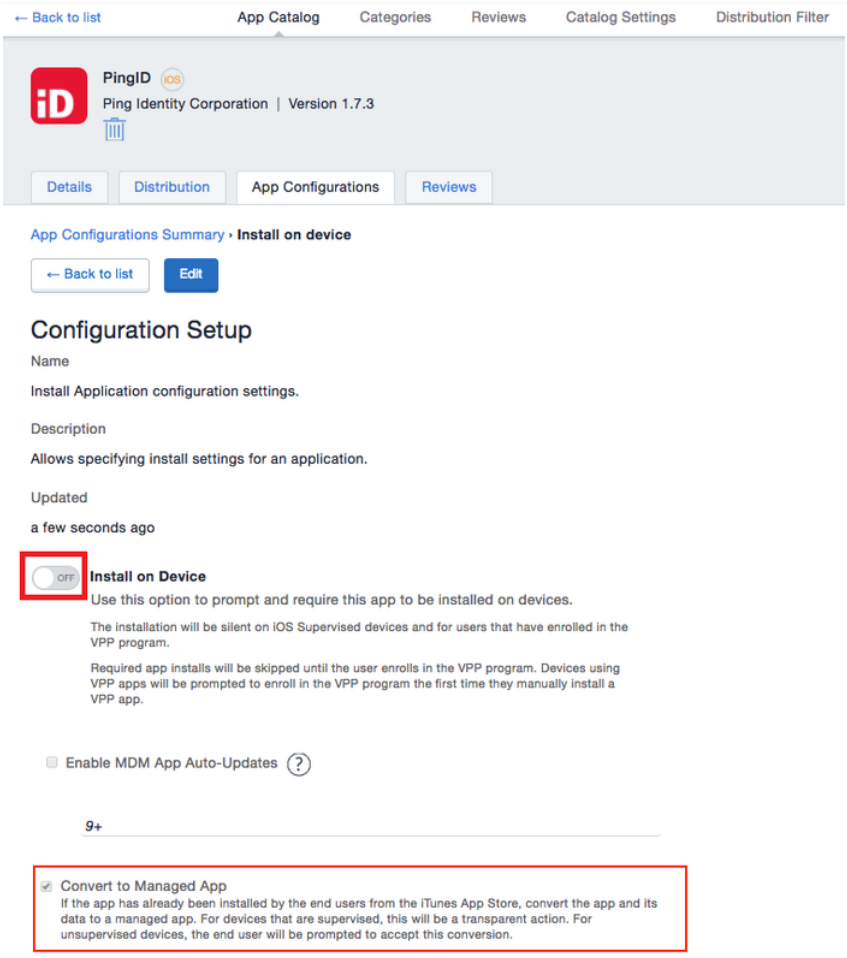
Parameter	Value
Name	`PINGID_MDM_TOKEN`
Token value	The token string value for MDM, as generated in the PingID admin web configuration page.



7. Click **Save**.
8. Click **Application Configurations Summary**.
9. Click **Install on device**.
10. Click **Install Application configuration settings**.



11. For iOS 9 and later, set the **Install on device** switch to **ON**.
12. Select the **Convert to Managed App** check box.



Note

This option transitions a non-managed app downloaded from the app store to a managed app. The user must approve it on their device.

Important

For Apple devices earlier than iOS 9, and Android devices

Users must execute the following steps:

1. Unpair the PingID mobile app on the iOS device.
2. Uninstall the PingID mobile app from the iOS device.
3. Reinstall the PingID mobile app, from the MDM's app catalog.
4. Pair the newly installed, MDM managed PingID mobile app.

For Apple devices with iOS 9 and later

The user receives a notification on their device to approve the transition to MDM management. After user approval, the PingID mobile app installed on the iOS device is managed by the MDM.

13. Click **Save/Update**.
    - When creating a new managed app entry, the button is marked **Save**.
    - When editing an existing entry, the button is marked **Update**.

> **Important**
>
> Repeat the entire configuration process for Android. The admin accesses the **Android for Work** options instead of**iOS Managed App Configuration**. The prerequisite to the Android app configuration is Configuring Android for Work for MobileIron.

Updating a PingID token in MobileIron

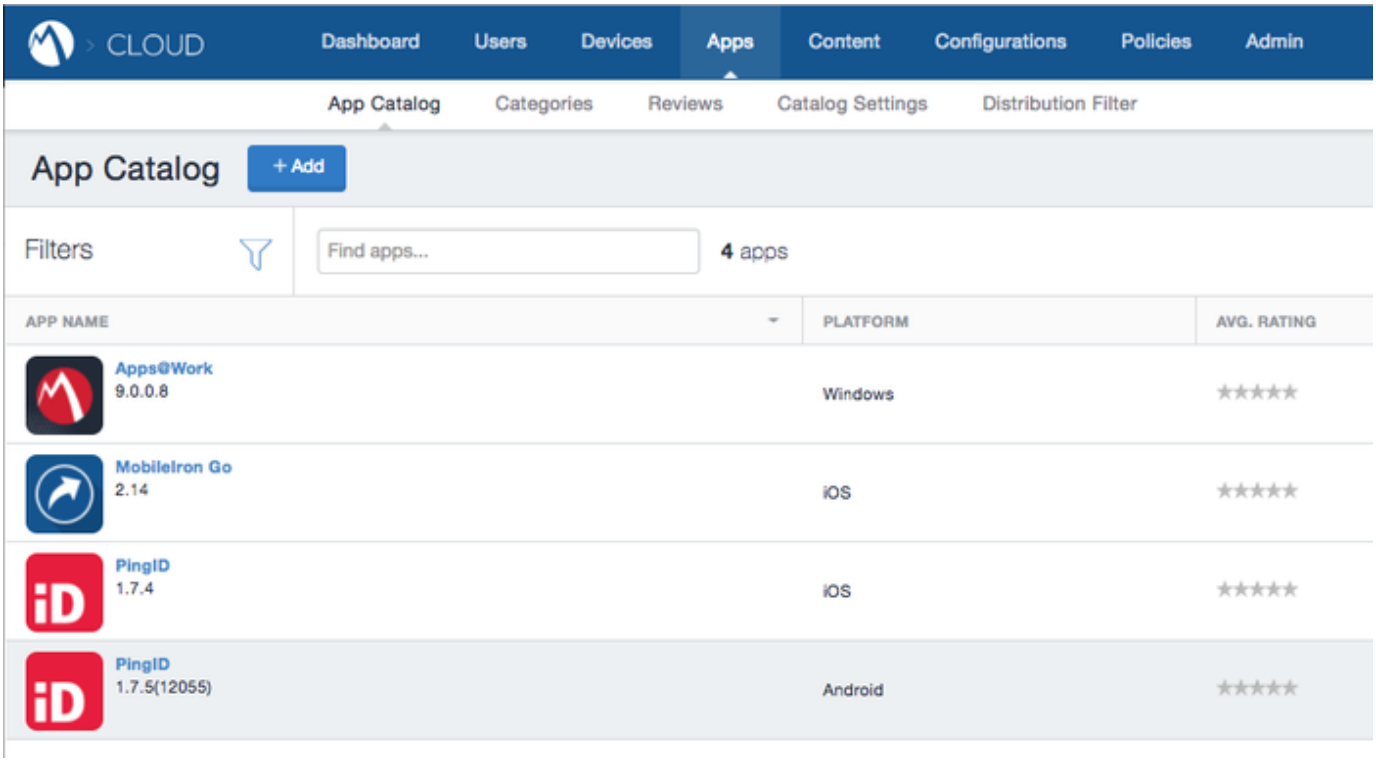
Update a PingID token in MobileIron.

About this task

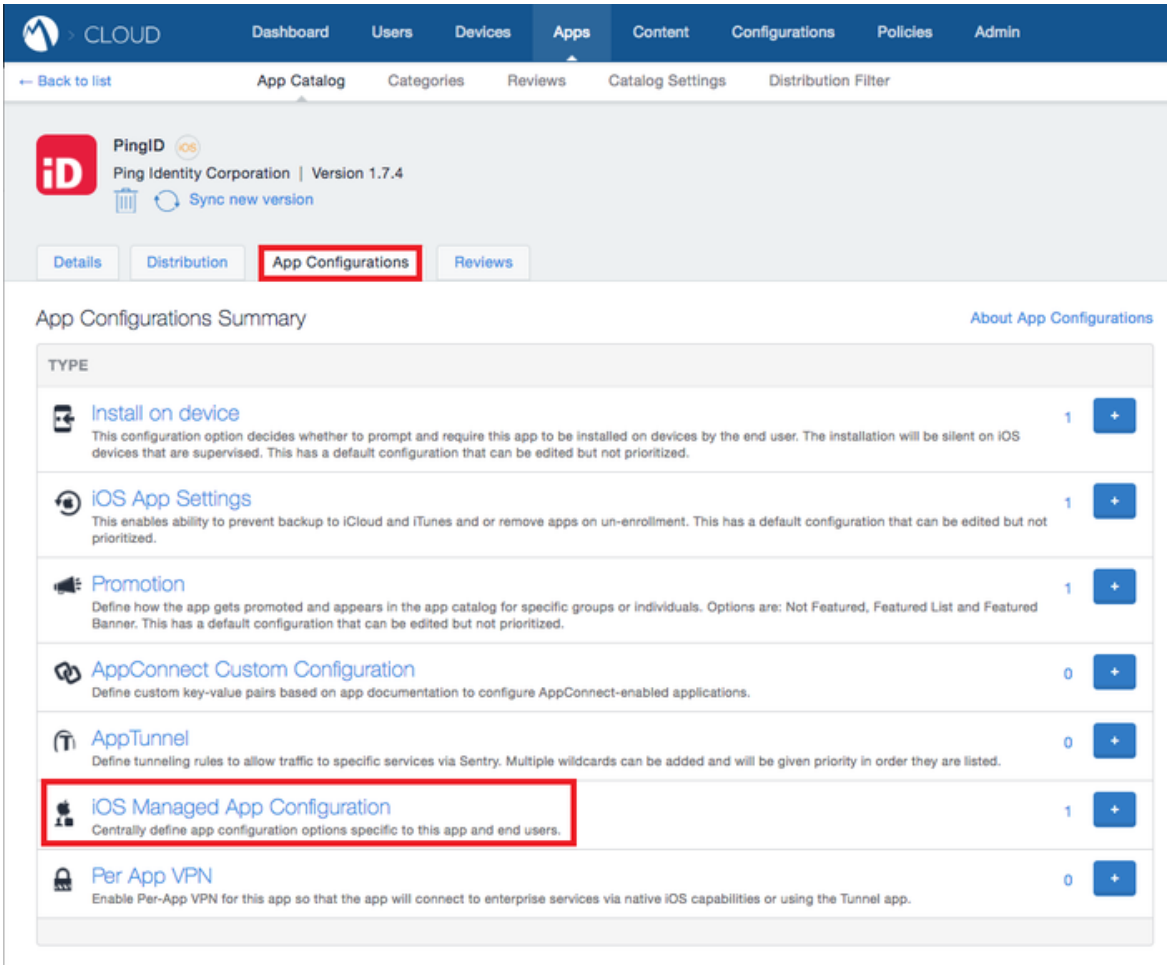
> **Important**
>
> The procedure detailed here is the iOS example for updating the token PingID managed app in MobileIron. The procedure for Android is identical. If the organization's mobile device management (MDM) manages both iOS and Android devices, configure and save the entire procedure separately for each platform.

Steps

1. In the MobileIron admin console, go to **Apps → App Catalog**.
2. Select the PingID mobile app for iOS.

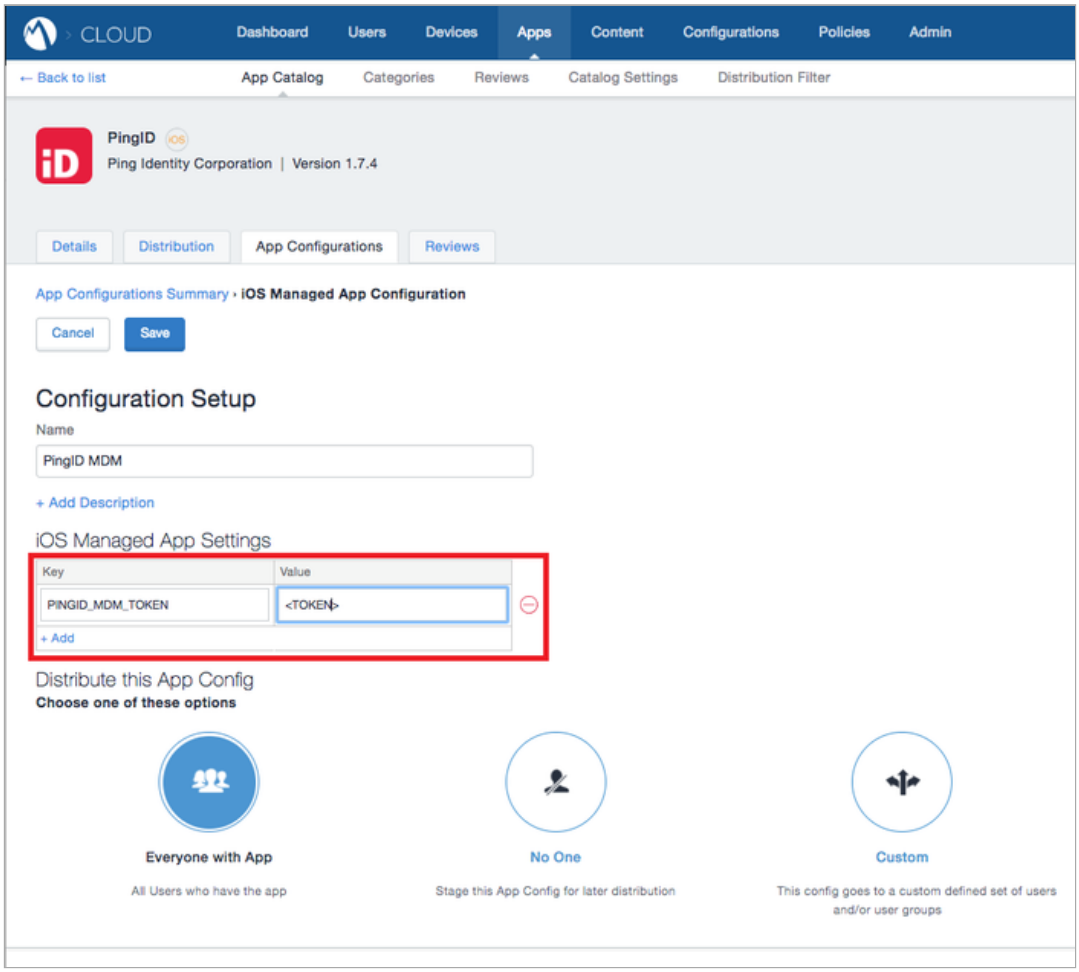


3. On the **App Configurations** tab, select **iOS Managed App Configuration**.



4. Update the **Configuration Setup** parameter values.

Parameter	Value
Name	`PINGID_MDM_TOKEN`.
Token value	The token string value for MDM, as generated in the PingID admin web configuration page.



5. Click **Save**.

> **Important**
>
> Repeat the entire process for Android.

Configuring Microsoft Intune for PingID

Manage the PingID app using Microsoft Intune.

> **Note**
>
> The following steps are for use cases where PingID MFA authenticating devices are managed by Microsoft Intune mobile device management (MDM). In cases where PingFederate is used to apply policies on accessing devices managed by Microsoft Intune, see Intune Integration Kit.

1. In Microsoft Intune, install an Apple Push Notification service (APNs) certificate for iOS. For more information, see Installing an APNs certificate for iOS in Microsoft Intune.

2. If your organization has iOS devices, add the PingID app for iOS. For more information, see Adding the PingID app for iOS in Microsoft Intune.
3. If your organization has Android devices, add the PingID app for Android. For more information, see Adding the PingID app for Android in Microsoft Intune.
4. Configure PingID configuration policies for Microsoft Intune. For more information, see Setting PingID app configuration policies for Microsoft Intune.

MDM maintenance:

As part of MDM maintenance activities for the PingID app, you can generate new tokens and revoke old tokens. For more information, see the following:

- In PingID:
  - Configuring Mobile Device Management (MDM)
  - Setting up MDM configuration in PingID for the first time
  - Adding a new MDM token
  - Revoking an MDM token
  - Rotating MDM tokens
- In Microsoft Intune:
  - Updating a PingID token in Microsoft Intune

Installing an APNs certificate for iOS in Microsoft Intune

To ensure that PingID app configurations can be pushed to iOS devices, install an Apple Push Notification service (APNs) certificate in Microsoft Intune.

Before you begin

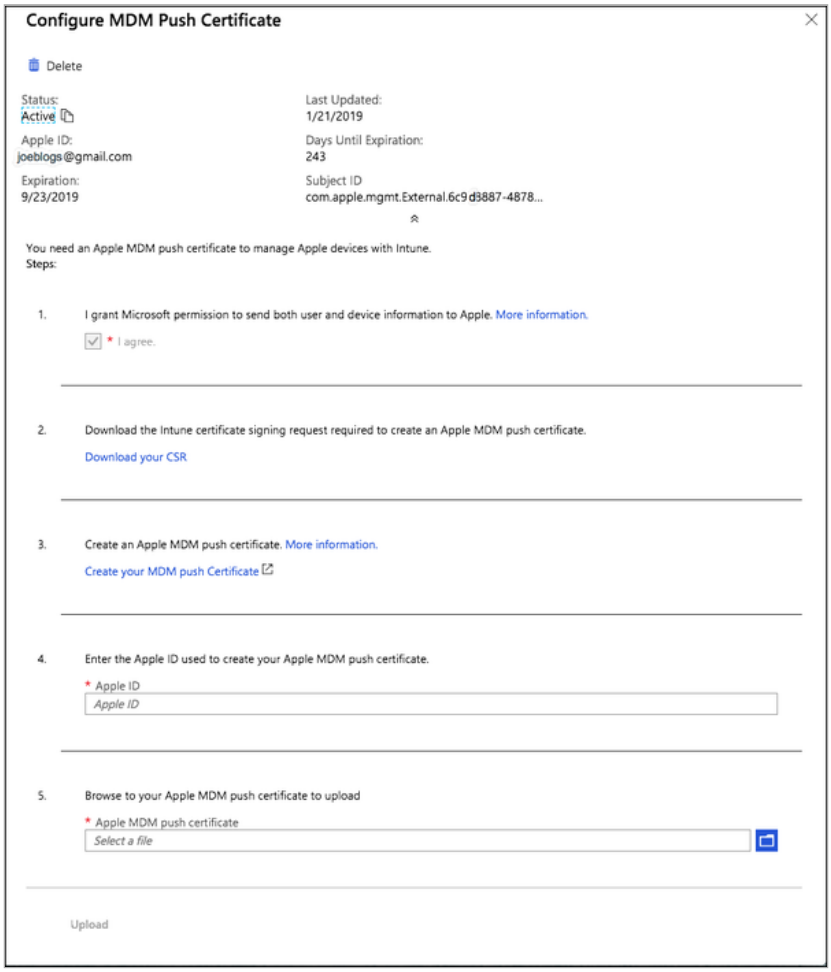
You will need your Apple ID for this procedure.

Steps

1. As a Global Administrator in the Microsoft Azure portal, go to **Intune → Device Enrollment → Apple Enrollment**, and then click **Apple MDM Push Certificate**.

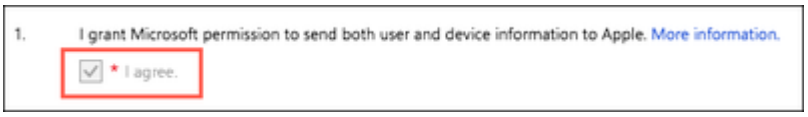
   Result:

   The **Configure MDM Push Certificate** window is displayed.

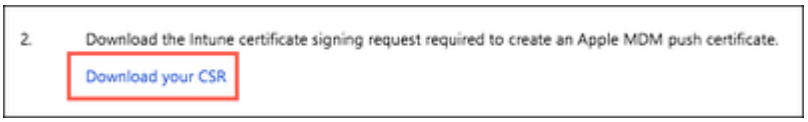


2. In the **Configure MDM Push Certificate** window, complete the following fields.

    1. In section **1**, select the **I Agree** check box.

    2. In section **2**, click **Download Your CSR**.

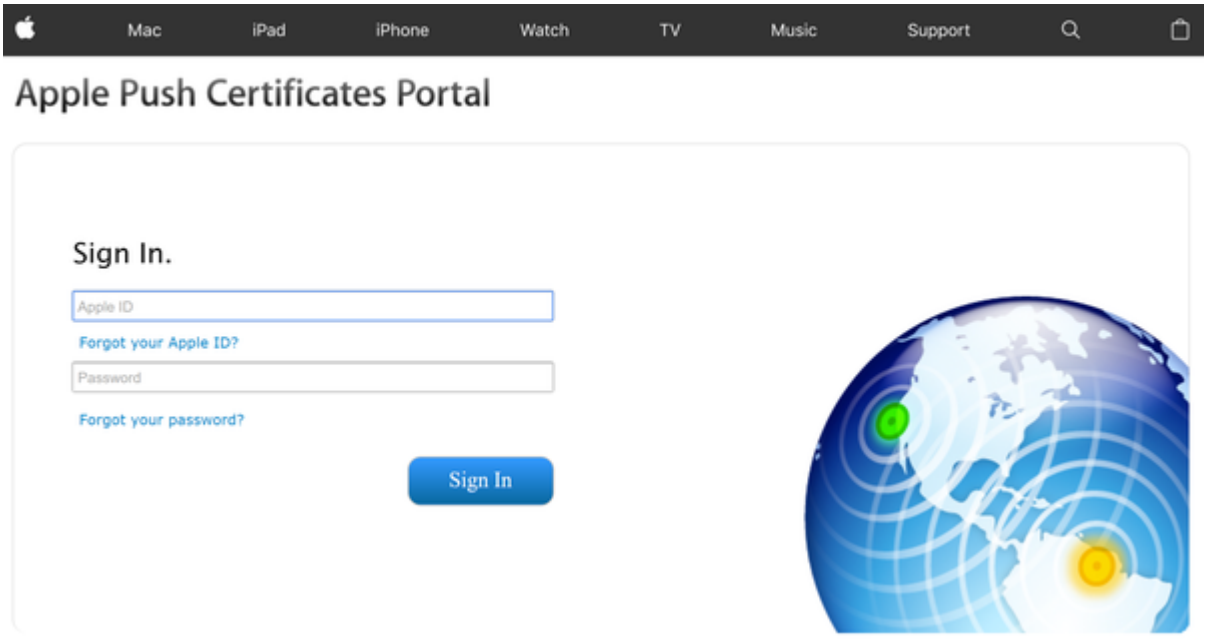
    3. In section **3**, click **Create Your MDM Push Certificate**.

    Result:

    The **Apple Push Certificates Portal** window opens in your browser.

3. Sign on to the Apple Push Certificates Portal.

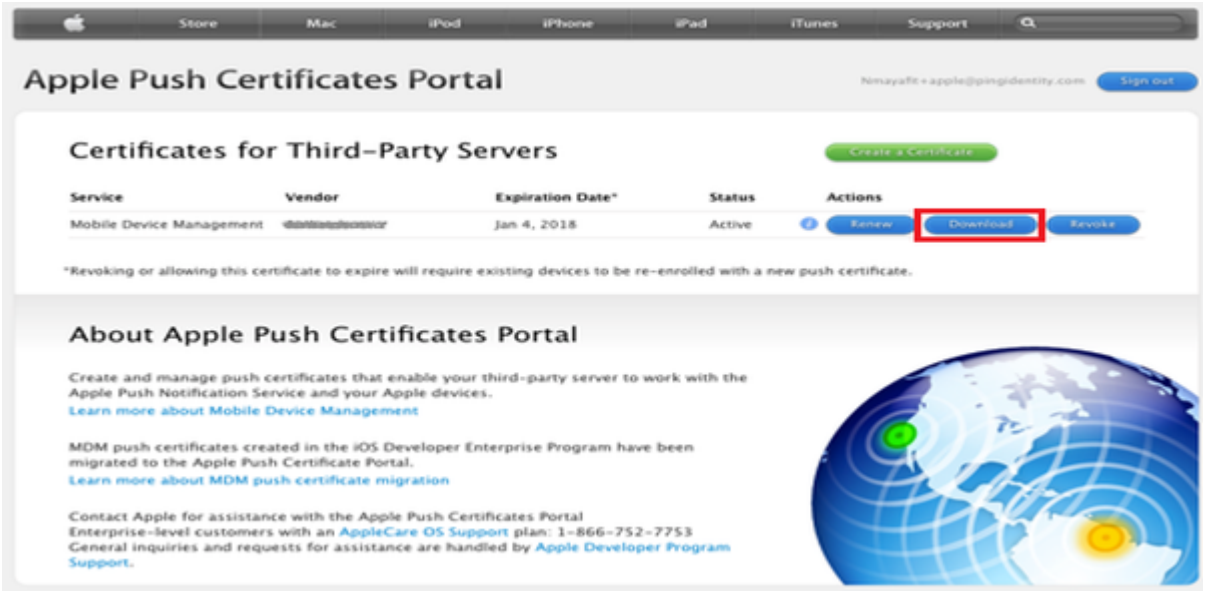


4. In either the **Get Started** section or the **Certificates for Third-Party Servers** section, click **Create a Certificate**.

> **Note**
>
> If your organization does not yet have any Apple Push certificates, the **Get Started** section is displayed. Otherwise, the **Certificates** list is displayed.

5. Click **Choose File** and browse for the certificate signing request (CSR) file you created previously, and then click **Upload**.

6. In the row of the new APNs certificate, click **Download**.



7. Return to the **Configure MDM Push Certificate** window and complete the following fields.

    1. In section **4**, enter your Apple ID.

    2. In section **5**, from the **Apple MDM Push Certificate** list, select your APNs certificate.

3. Click **Upload**, and then save your configuration.

Next steps

Add the PingID app for iOS. For more information, see Adding the PingID app for iOS in Microsoft Intune.

Configuring Android for Work for Microsoft Intune

To ensure that PingID app configurations can be pushed to Android devices, configure Android for Work for the organization's mobile device management (MDM).

Before you begin

In the Intune dashboard, configure Android work profile devices. For more information, see https://docs.microsoft.com/en-us/intune/android-enterprise-overview.

About this task

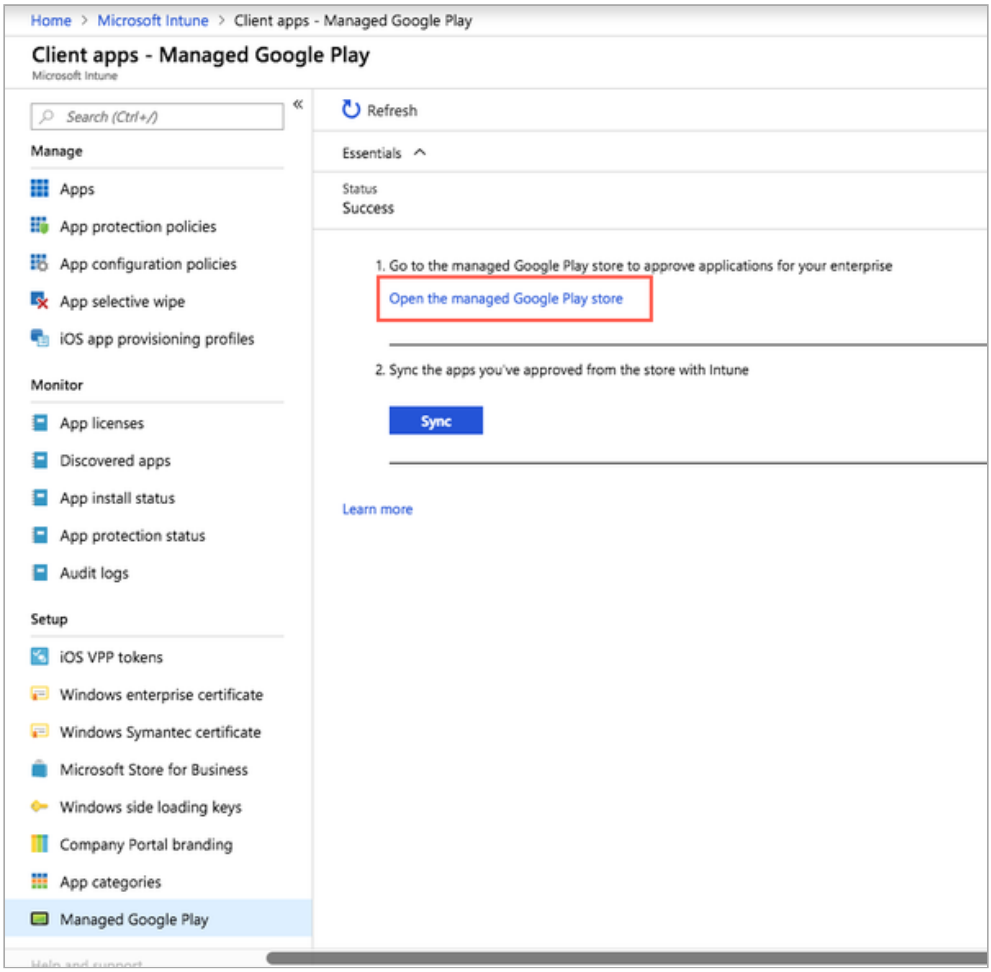
This is an example configuration of Android for Work without G Suite. You can configure Android for Work for MDM with G Suite.

Steps

1. Go to the Microsoft Azure portal at https://portal.azure.com.
2. Go to **Intune → Home → Client Apps → Managed Google Play**.

   Result:

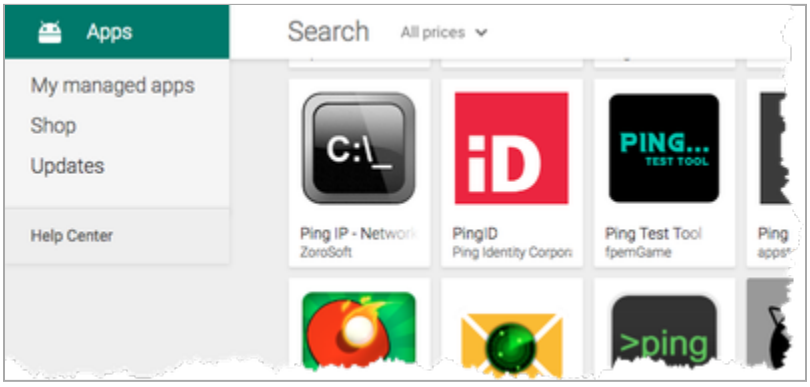
   The **Managed Google Play** window opens.
3. Click **Open the Managed Google Play Store**.



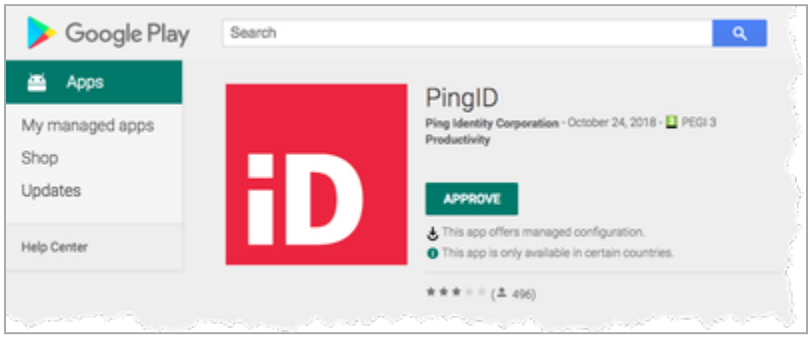
Result:

Google Play opens in a new browser tab or window.

4. Search for the PingID app and select it.



5. Click **Approve**.

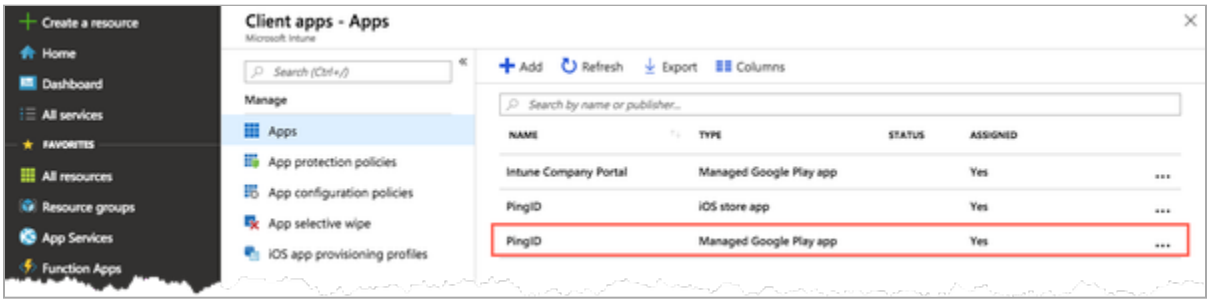


> **Note**
>
> You might be prompted to sign on as a managed Google Play administrator. Do so.

Result:

The **Client Apps - Apps** window is displayed.

6. From the **Apps** list, click the PingID Google Play entry, and then from the left-hand menu, click **Assignments**.

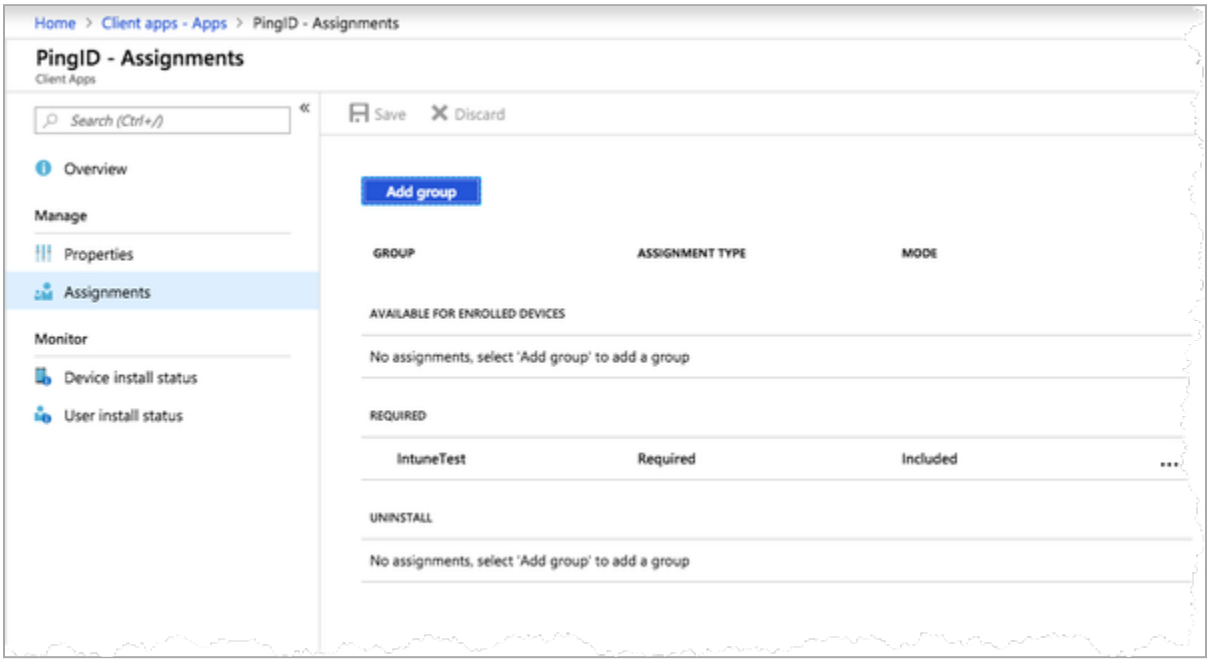


Result:

The **PingID - Assignments** window is displayed.

7. In the **PingID - Assignments** window, assign the PingID Android app to user groups.

   To create, manage and assign apps to groups, see the relevant Intune documentation.

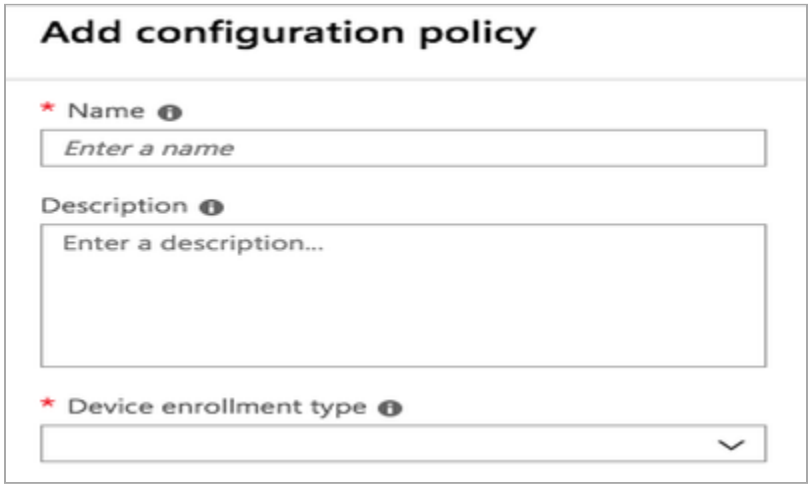


8. Go to **Intune → Client Apps → App Configuration Policies**, and then click **Add**.

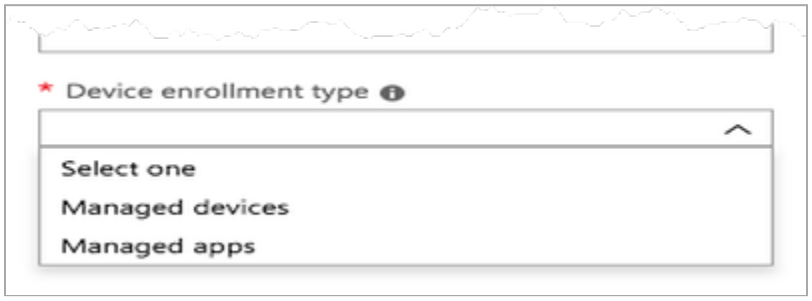
   Result:

   The **Add Configuration Policy** window is displayed.

9. In the **Name** field, enter a name for the policy.
10. In the **Description** field, add a description.



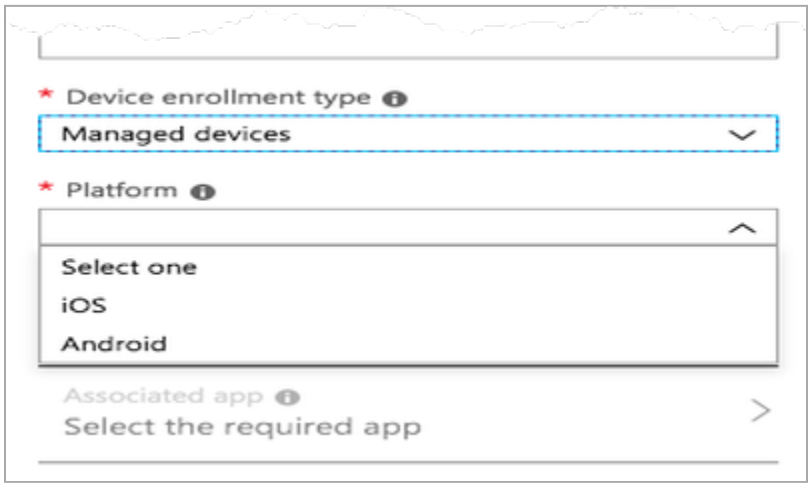
11. From the **Device Enrollment Type** list, select **Managed Devices**.



Result:

The **Platform** list is displayed.

12. From the **Platform** list, choose **Android**.

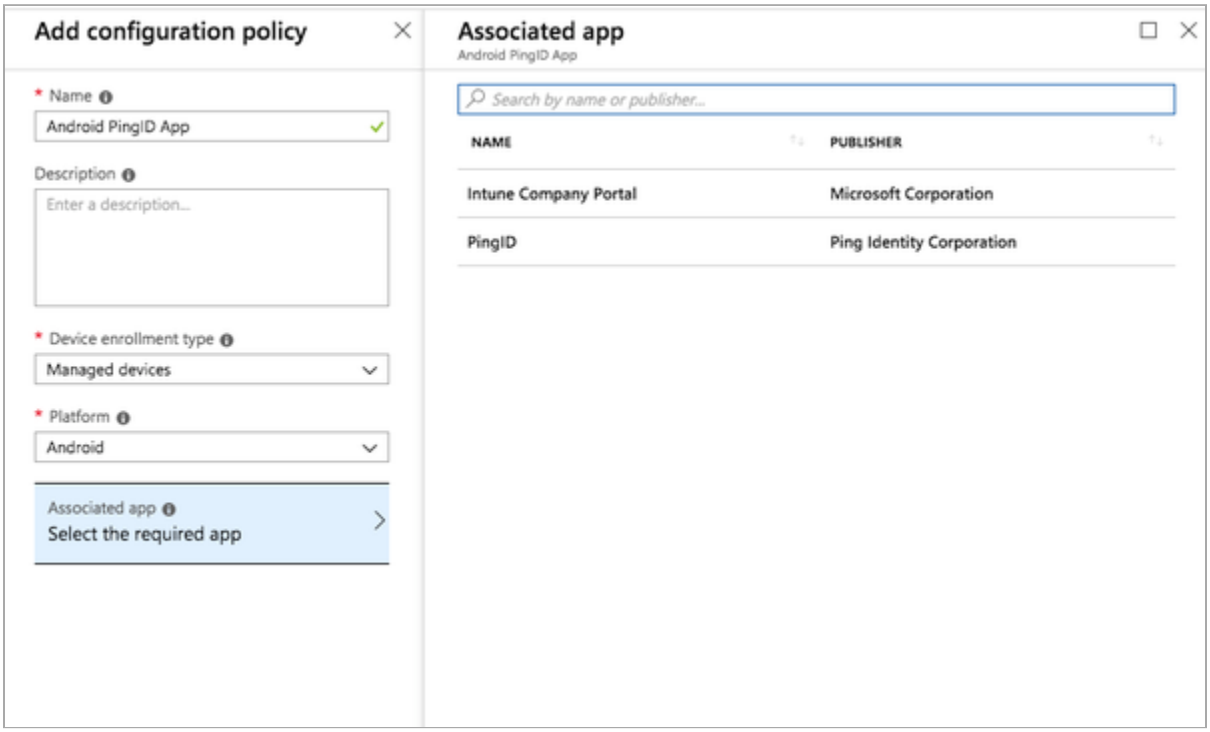


13. At the bottom of the window, click **Add**.

Result:

The **Associated App** tab is displayed.

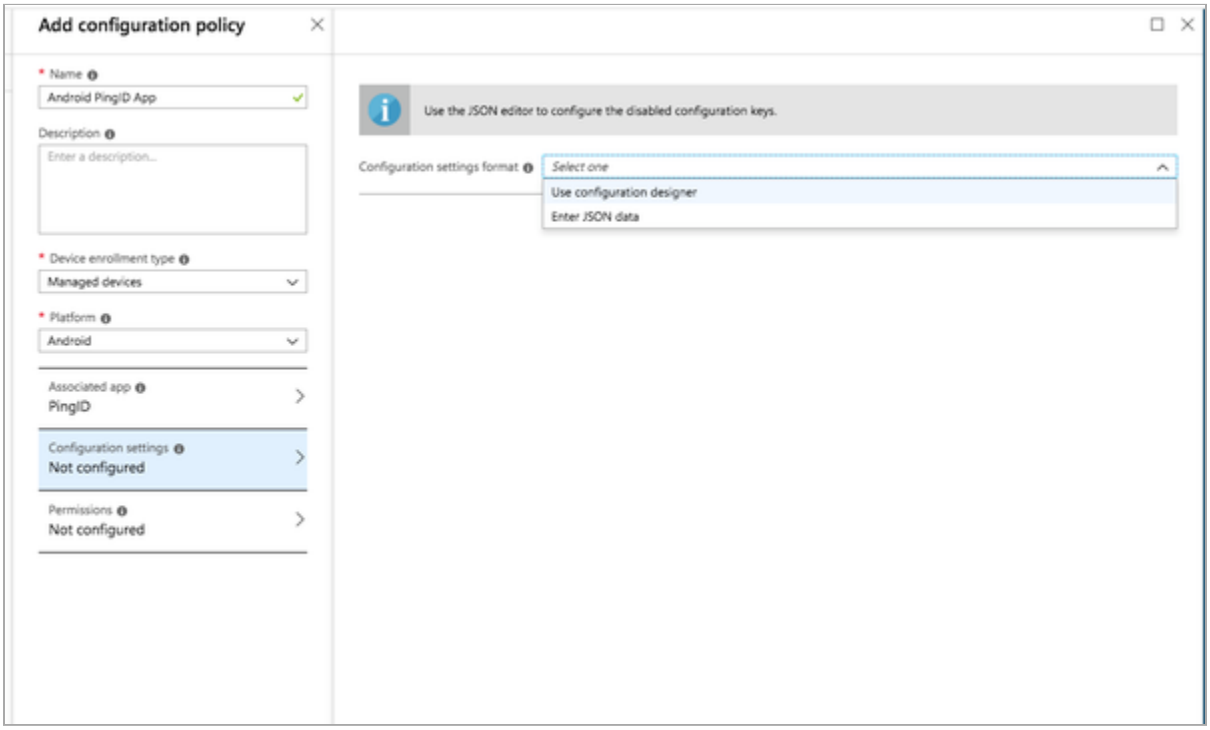
14. On the **Associated App** tab, click **PingID**.



Result:

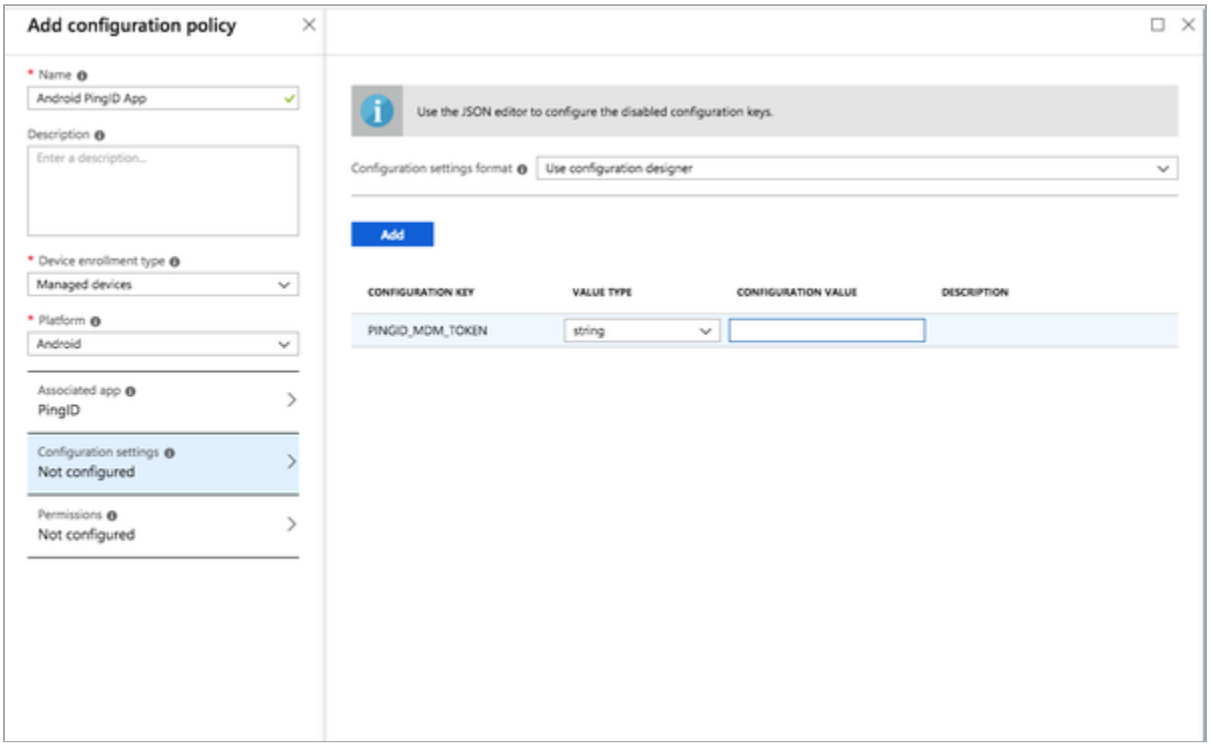
The **Configuration Settings** tab is displayed.

15. From the **Configuration Settings Format** list, select **Use Configuration Designer**.



16. In the **Configuration Value** field, enter the PingID MDM token, and then click **Add**.

For more information, see Setting up MDM configuration in PingID for the first time.



Next steps

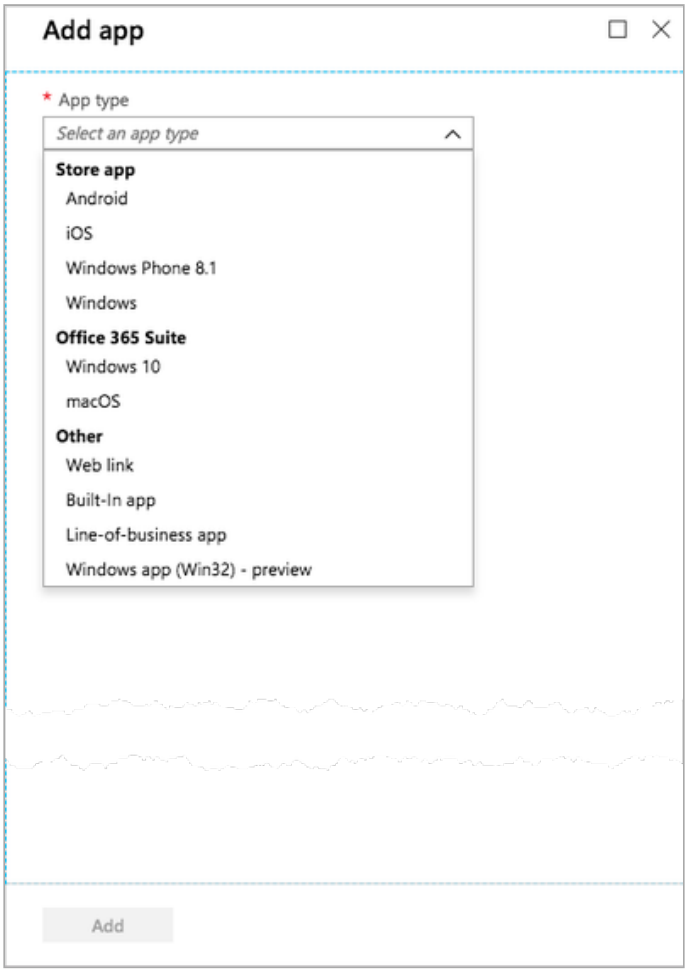
See Adding the PingID app for Android in Microsoft Intune.

Adding the PingID app for iOS in Microsoft Intune

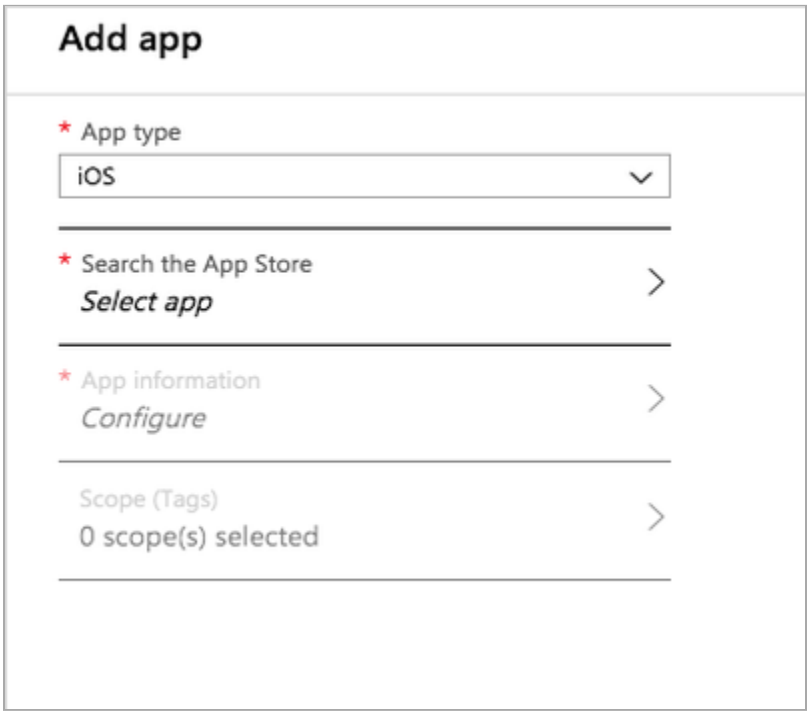
Configure PingID as an MDM-managed app for iOS devices in Microsoft Intune.

Steps

1. Go to the Microsoft Azure portal at https://portal.azure.com.
2. Go to **Intune → Client Apps → Apps → +Add → Add App**.
3. From the **App Type** list, select **iOS**.

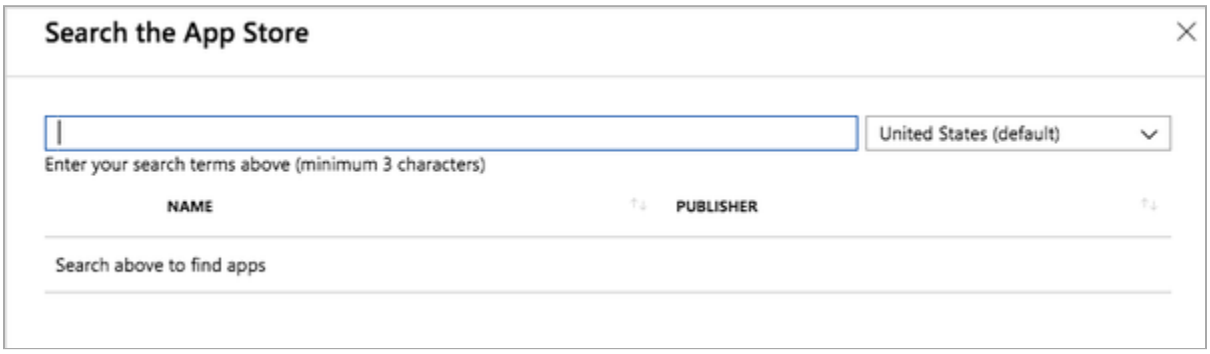


4. In the **Search the App Store** section, click **Select App**.



Result:

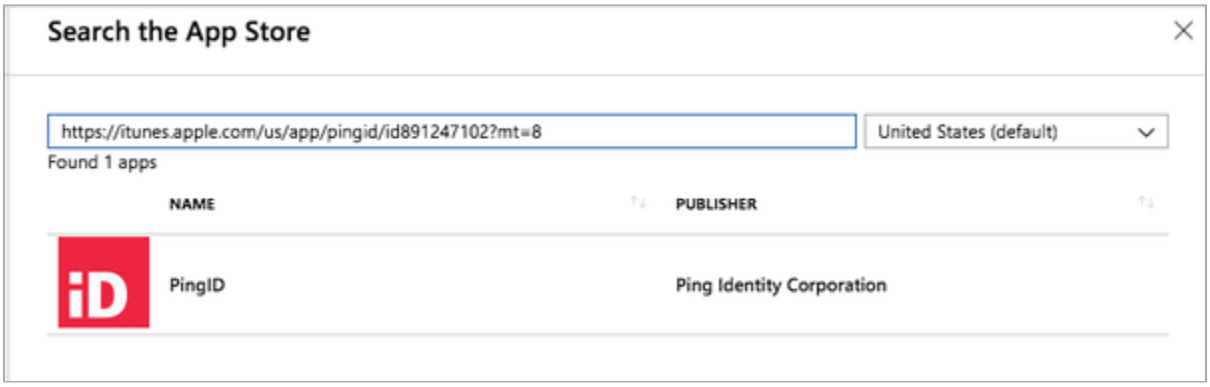
The **Search the App Store** window opens.



5. In the search field, enter th e PingID mobile app's iTunes App Store URL: https://itunes.apple.com/us/app/pingid/id891247102?mt=8.

   Result:

   The PingID app is displayed.

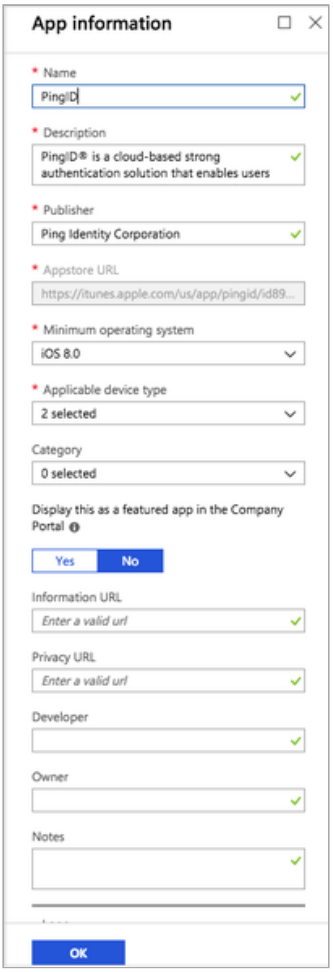


6. Click the PingID app.

   Result:

   You are returned to the **Add App** window with the **Configure** option enabled.

7. To open the **App Information** window, click **Configure**.
8. In the **App Information** window, make any required changes, and then click **OK**.



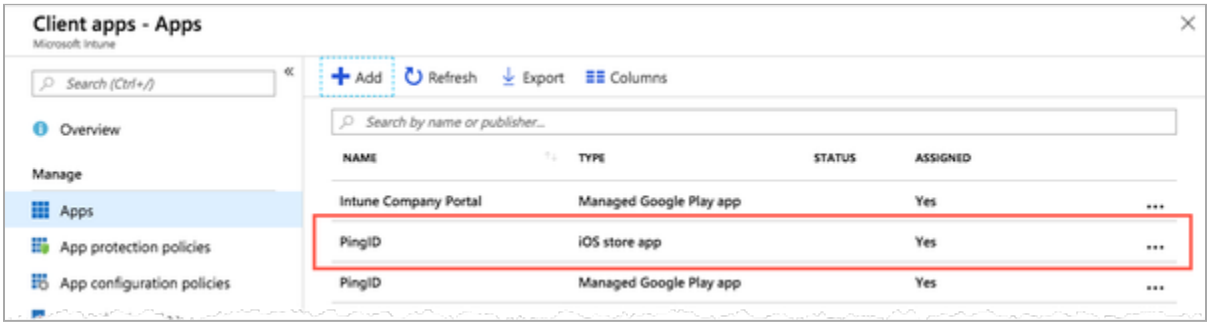
Result:

In the **Add App** window, the **Add** button is enabled.

9. In the **Add App** window, click **Add**.

Result:

Your app appears in the list of client apps.



Next steps

See Setting PingID app configuration policies for Microsoft Intune.

Adding the PingID app for Android in Microsoft Intune

To ensure that PingID app configurations can be pushed to Android devices, configure Android for Work for the organization's mobile device management (MDM).

Before you begin

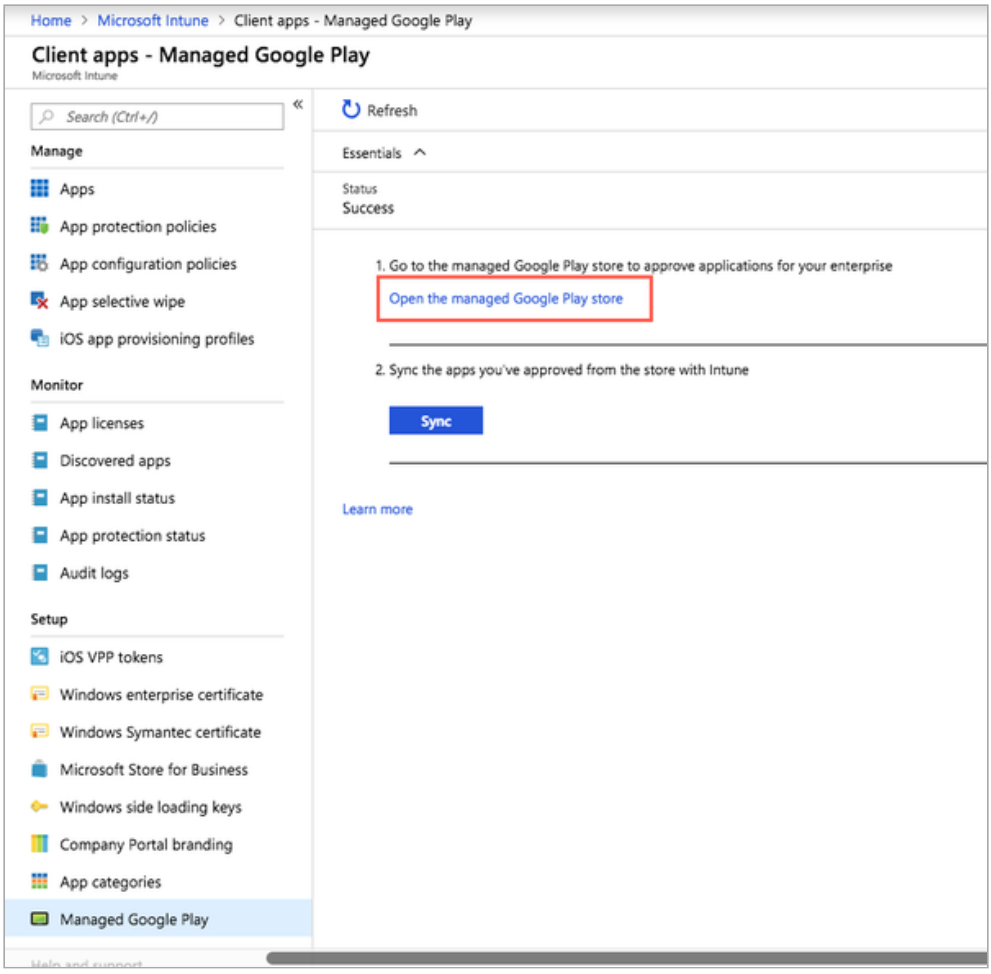
In the Intune dashboard, configure Android work profile devices. For more information, see https://docs.microsoft.com/en-us/intune/android-enterprise-overview.

About this task

This is an example configuration of Android for Work without G Suite. You can configure Android for Work for MDM with G Suite.

Steps

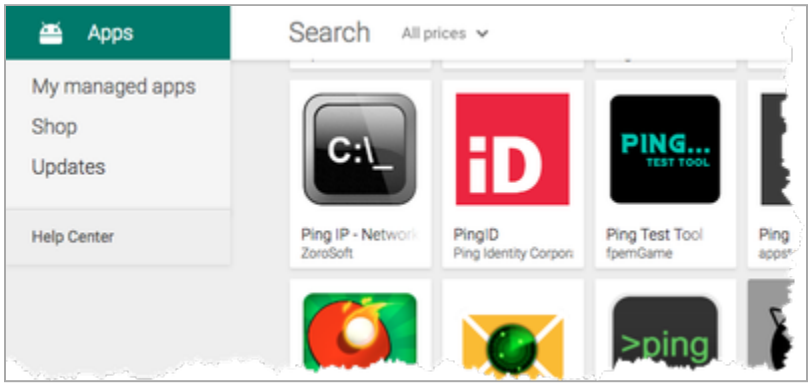
1. Go to the Microsoft Azure portal at https://portal.azure.com.
2. Go to **Intune → Home → Client Apps → Managed Google Play**.
3. In the **Client Apps - Managed Google Play** window, click **Open the Managed Google Play Store**.



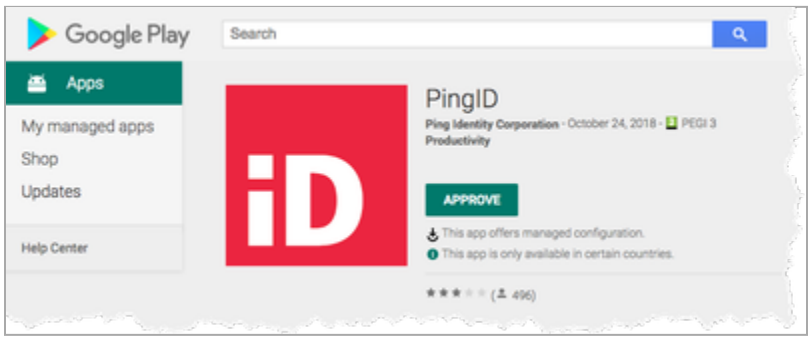
Result:

Google Play opens in a new browser tab or window.

4. Search for the PingID app and select it.



5. Click **Approve**.

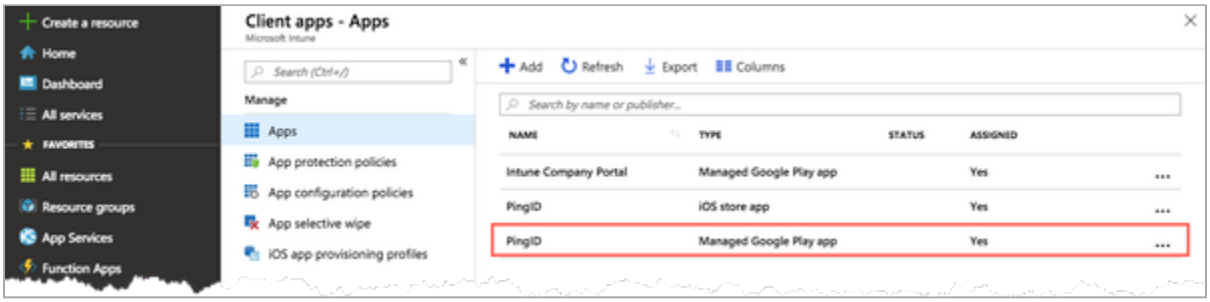


> **Note**
>
> You might be asked to sign on as a managed Google Play administrator.

Result:

The **Client Apps - Apps** window is displayed.

6. From the **Apps** list, select the PingID Managed Google Play app, and then from the left-hand menu, click **Assignments**.

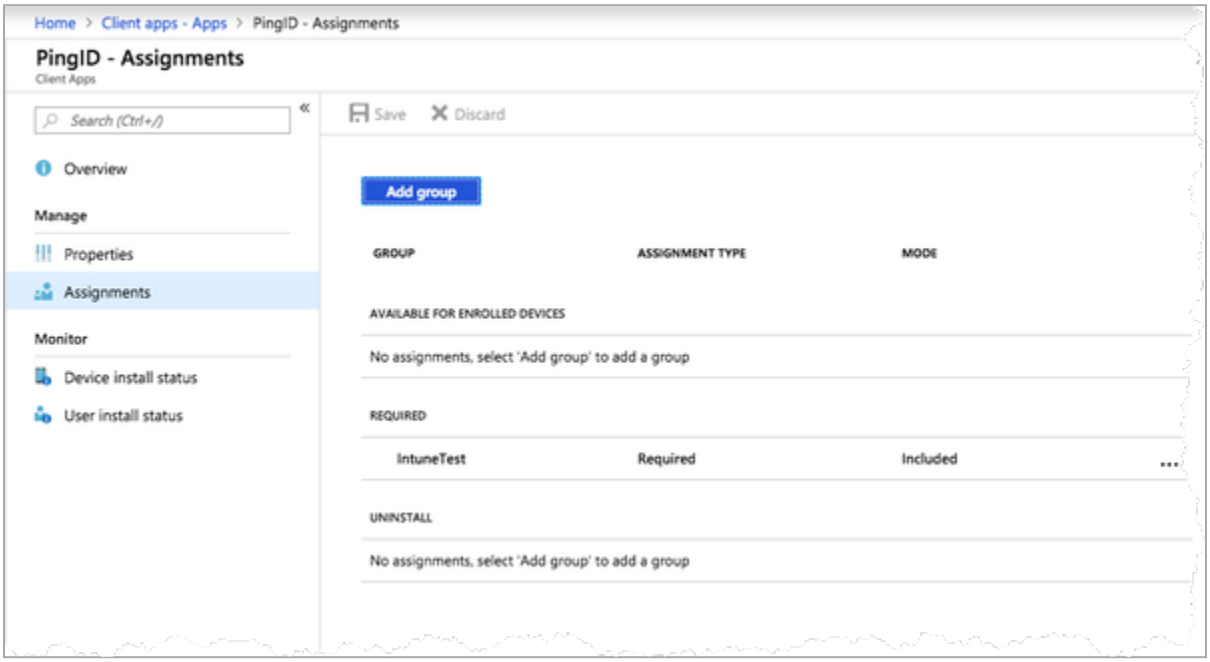


Result:

The **PingID - Assignments** window is displayed.

7. In the **PingID - Assignments** window, assign the PingID Android app to user groups.

   To create, manage and assign apps to groups, consult the relevant Intune documentation.



Next steps

See Setting PingID app configuration policies for Microsoft Intune.

Setting PingID app configuration policies for Microsoft Intune

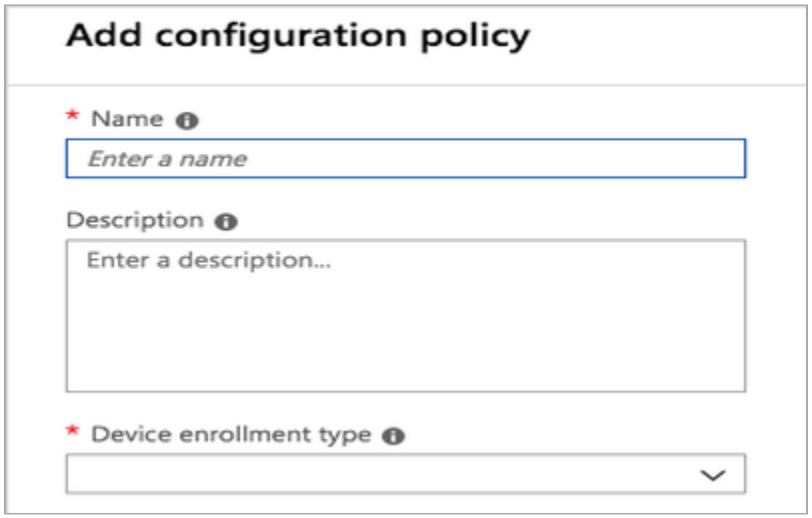
Configure the following procedure separately for iOS and Android.

Steps

1. Go to the Microsoft Azure portal at https://portal.azure.com.
2. Go to **Intune → Client Apps → App Configuration Policies → +Add**.

   Result:

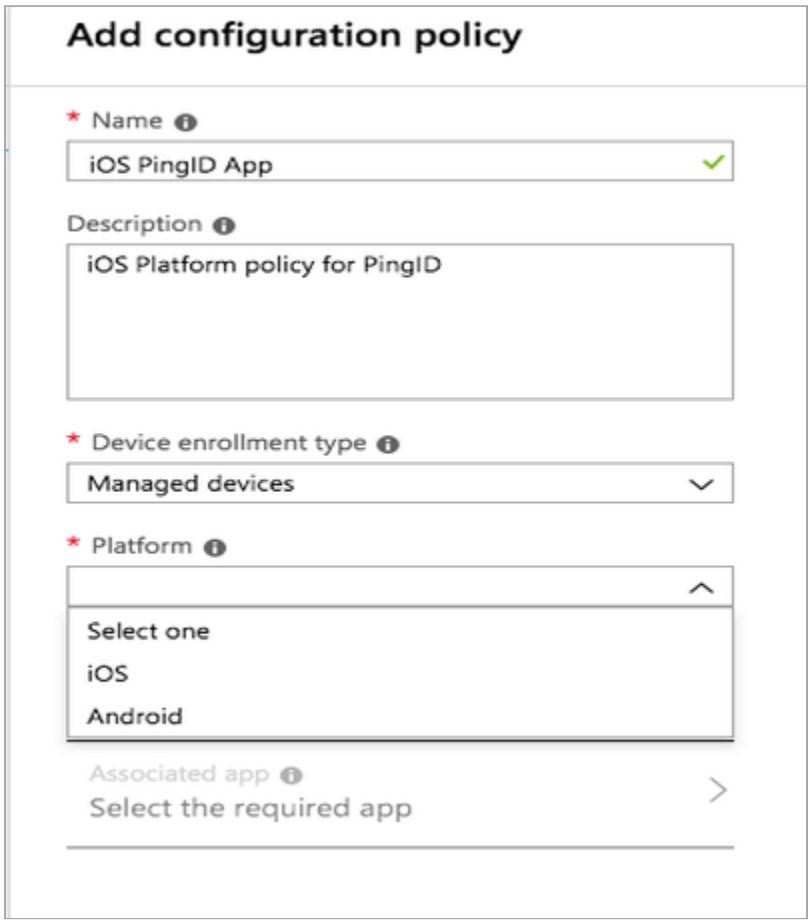
   The **Add Configuration Policy** window is displayed.



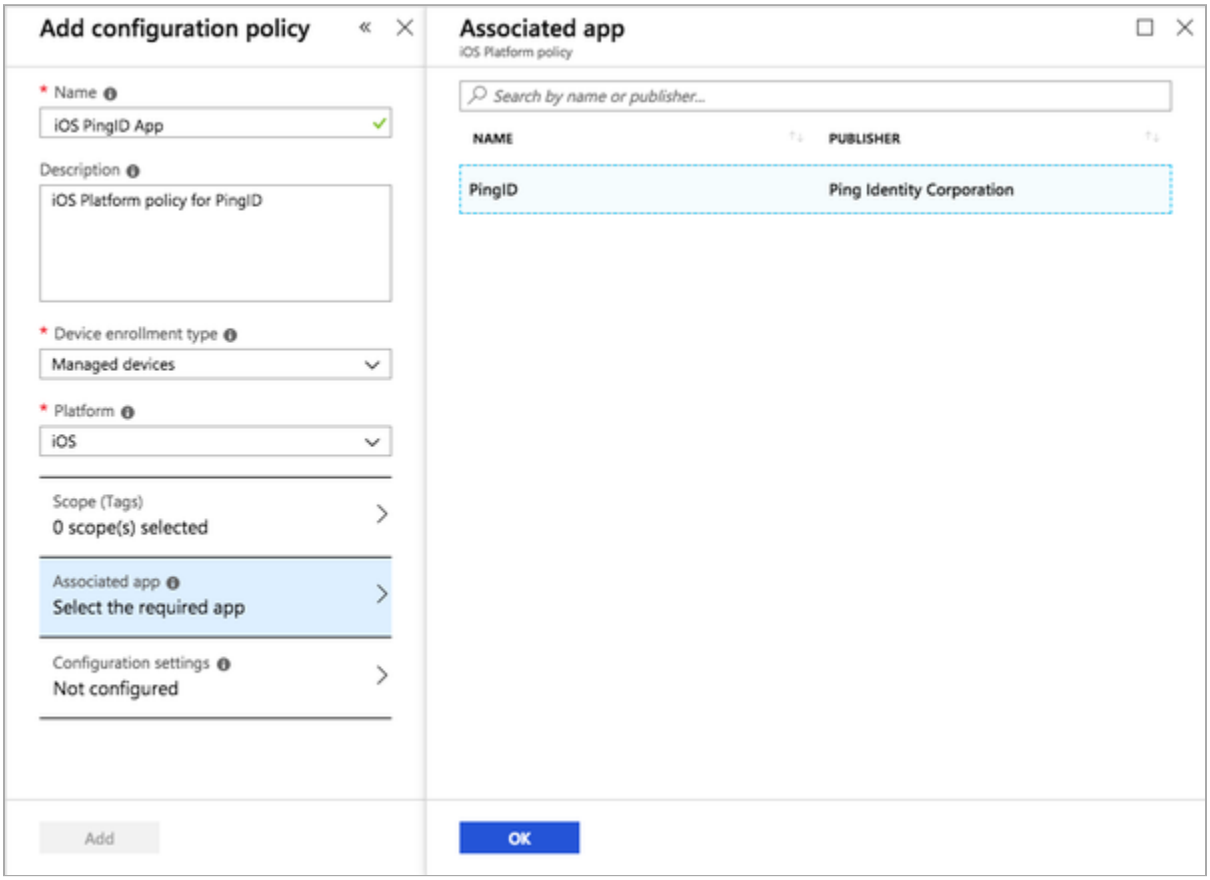
3. In the **Name** field, enter a policy name. In the **Description** field, enter a description.

4. From the **Device Enrollment Type** list, select **Managed Devices**.

5. From the **Platform** list, select the relevant platform.

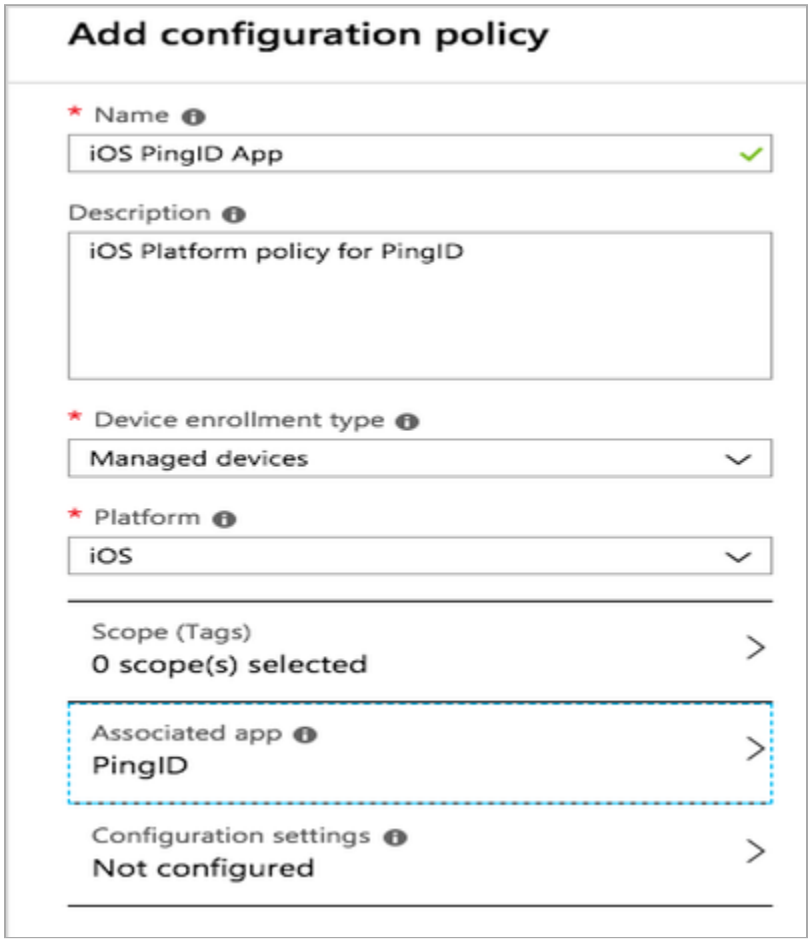


6. Click the **Associated App** section, and then in the **Associated App** pane, select **PingID**.

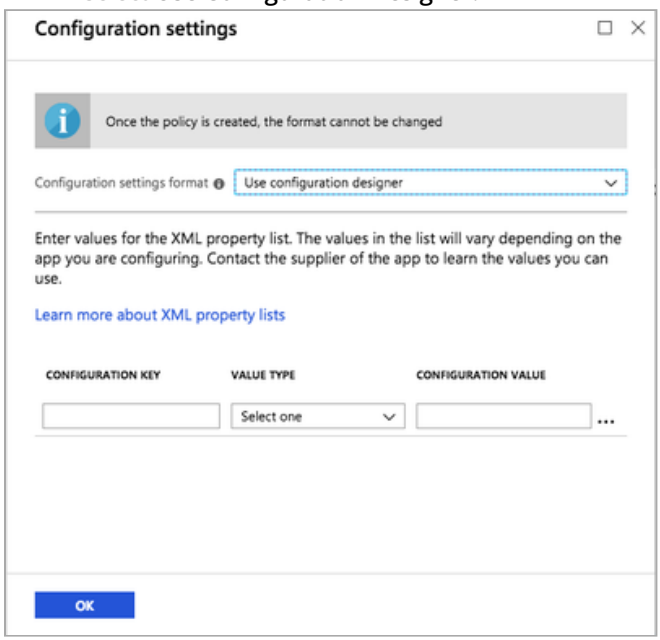
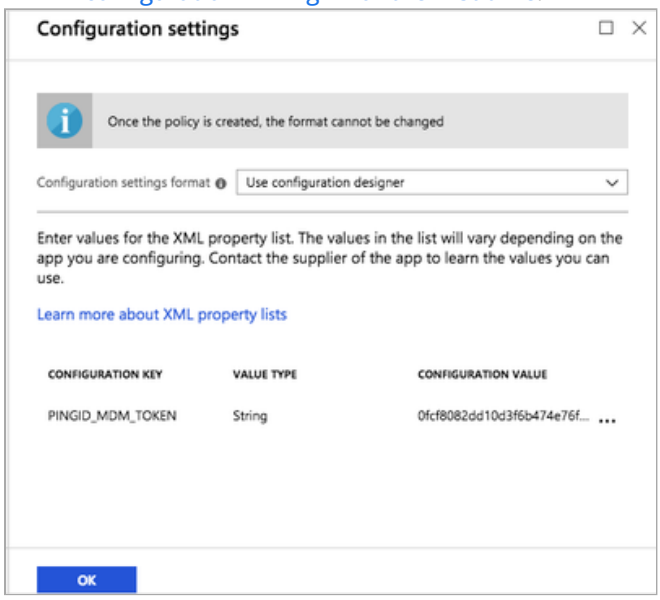


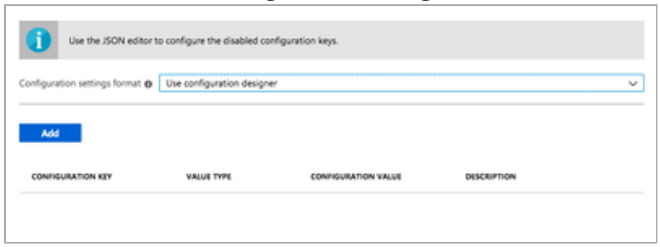
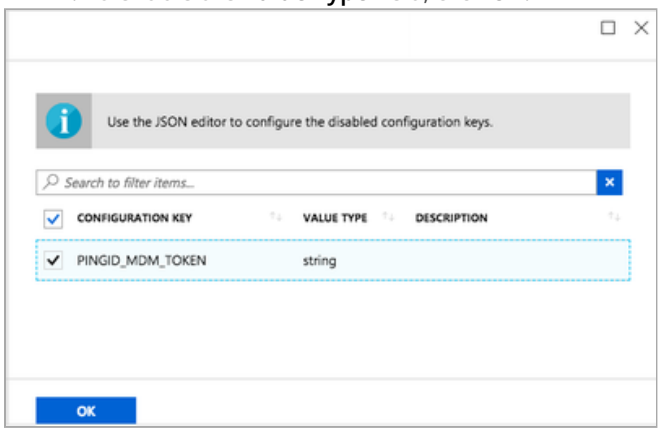
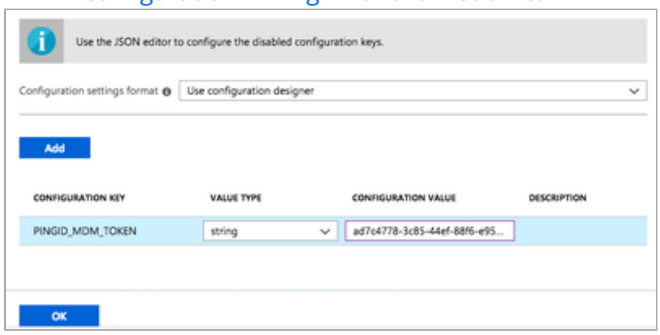
Result:

The **Associated App** section shows **PingID**.



7. Click the **Configuration Settings** section, and then follow the steps according to the relevant operating system.

Operating System	Steps
iOS	1. From the **Configuration Settings Format** list, select **Use Configuration Designer**.  1. In the **Configuration Key** field, enter `PING_MDM_TOKEN`. 2. From the **Value Type** list, select **String**. 3. In the **Configuration Value** field, enter your MDM string generated in the PingID admin portal. For more information, see Setting up MDM configuration in PingID for the first time. 

Operating System	Steps
Android	1. From the **Configuration Settings Format** list, select **Use Configuration Designer**.  1. Click **Add**. 2. To enable the **Value Type** field, click **OK**.  1. From the **Value Type** list, select **String**. 2. In the **Configuration Value** field, enter your MDM string generated in the PingID admin portal. For more information, see Setting up MDM configuration in PingID for the first time. 

8. Click **OK**.

   Result:

   You are returned to the **Add Configuration Policy** window.

Updating a PingID token in Microsoft Intune

Configure the following procedure separately for iOS and Android.

Before you begin

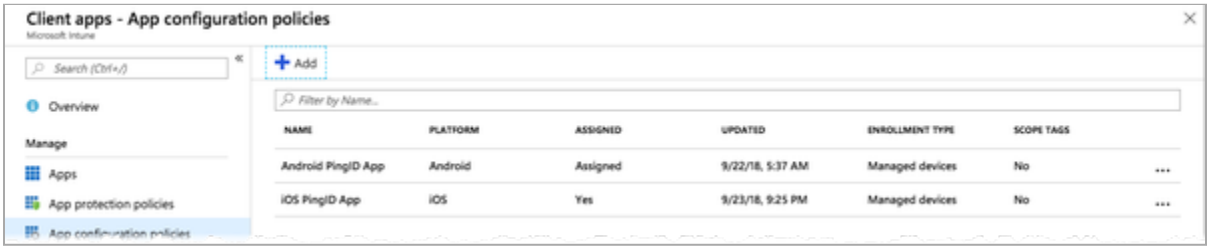
The PingID app is configured for both iOS and Android.

Steps

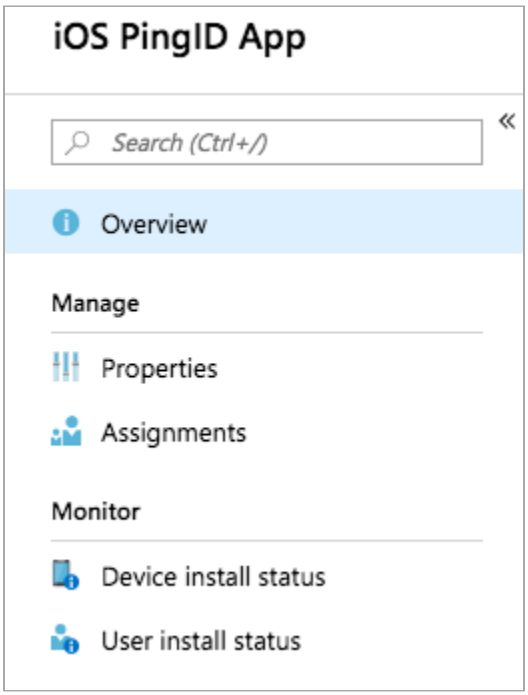
1. Go to the Microsoft Azure portal at https://portal.azure.com.
2. Go to **Intune → Client Apps → App Configuration Policies**.

   Result:

   The **Client Apps - App Configuration Policies** window is displayed.



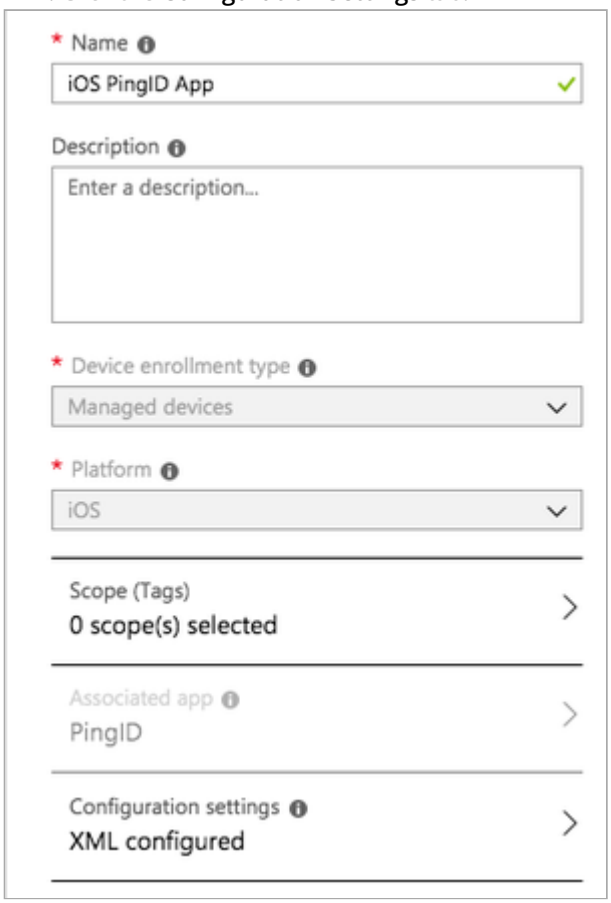
3. Click the relevant **Android PingID App** or **iOS PingID App** entry.
4. Click **Properties**.



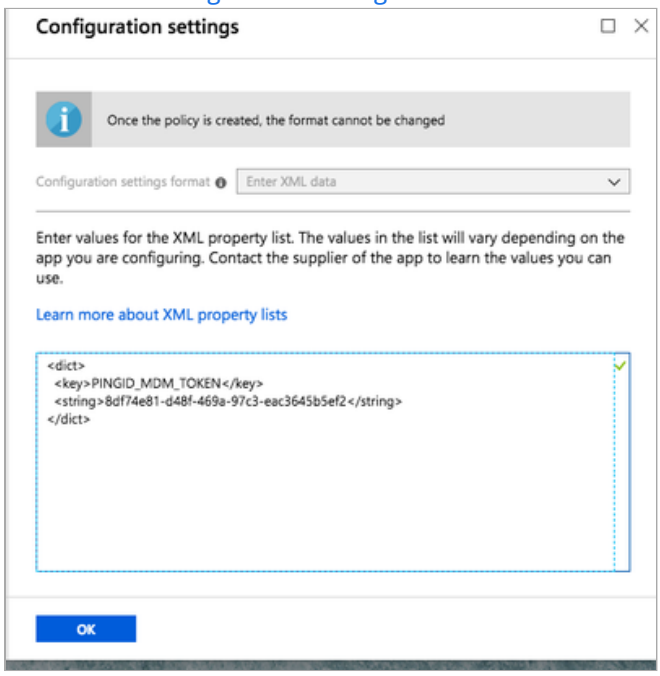
5. Follow the steps according to the relevant operating system.

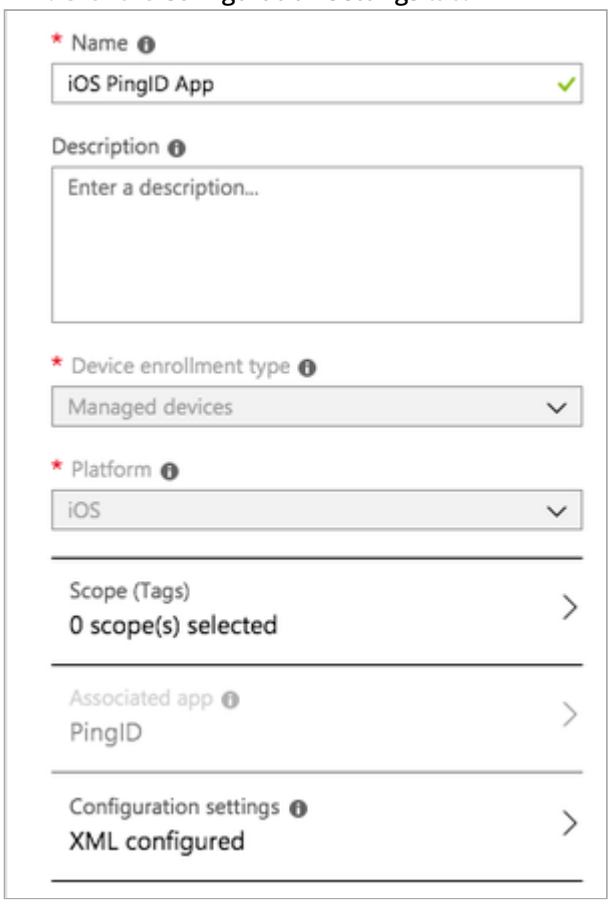
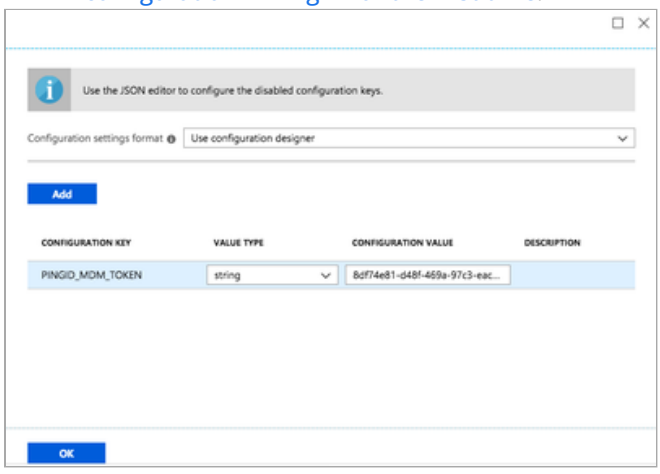
iOS

1. Click the **Configuration Settings** tab.



1. Enter your MDM string between `<string>` and `</string>`. For more information, see Setting up MDM configuration in PingID for the first time.



Operating System	Steps
Android	1. Click the **Configuration Settings** tab.  1. From the **Value Type** list, select **String**. In the **Configuration Value** field, enter your MDM string. For more information, see Setting up MDM configuration in PingID for the first time. 

6. Click **OK**.

Result:

You are returned to the app dashboard window.

7. Click **Save**.

Configuring pairing conditions

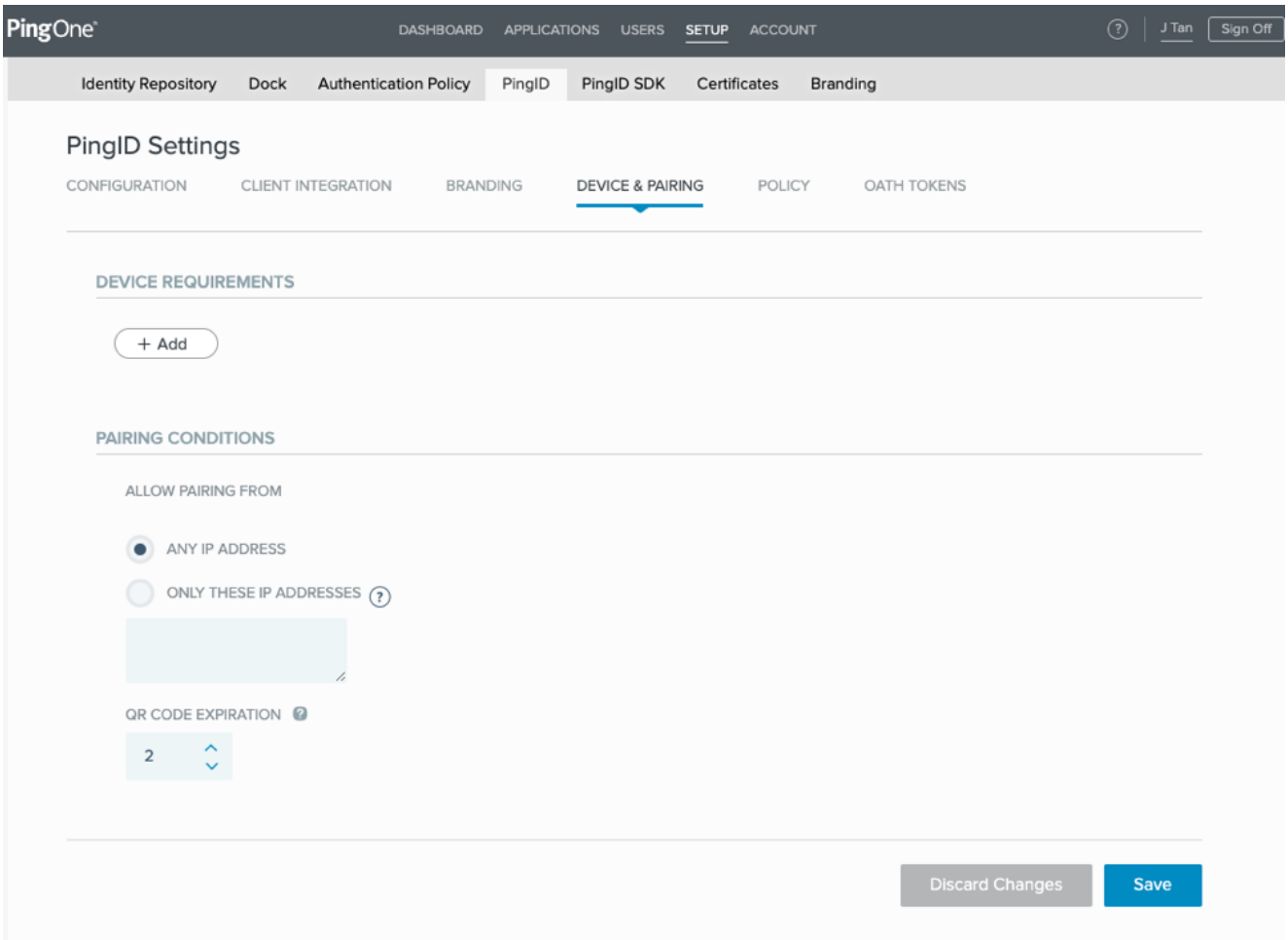
Configure pairing conditions for the PingID mobile app. Define the IP ranges of devices from which pairing is allowed. Set the duration of the time period for which a QR code and pairing code are valid.

About this task

> **Note**
>
> Pairing conditions apply to PingID mobile app pairing events only. They are not applied to any other authentication method.

Steps

1. In the PingOne admin console, go to **Setup → PingID Configuration → Device & Pairing**.



2. In the **Allow Pairing From** section, define the IP addresses permitted for the authenticating mobile device, such as the device on which PingID mobile app is installed. Click one of the following:

Choose from:

- **Any IP Address**: Allow pairing from mobile device with any IP address.
- **Only These IP Addresses**: Enter a list of allowed IP addresses or ranges. Only pairing requests from mobile devices with IP address in the permitted range are allowed.

> **Note**
>
> Enter the IP addresses or ranges using CIDR notation, each entry on its own line.

3. In the **QR Code Expiration** field, enter the number of hours for which the QR code will remain valid (1-48 hours; default is 48 hours).
4. Click **Save**.

Authentication policy

You can define policies per application or per group of applications for any application defined in PingFederate. You can also apply a policy to one or more user groups.

Define your PingID authentication policy in the **PingID → POLICY** tab, according to your unique security needs.

You can define a policy for high security applications and a separate policy for low security applications. You can apply a separate policy to your HR user group, IT user group, or Finance group.

Allowed authentication methods:

- Define or limit the authentication methods that can be used per policy. For more information, see Policy and rule authentication methods. For example, define stronger authentication methods, such as fingerprint authentication, for high security apps and a wider range of allowed authentication methods for less sensitive apps.

Different subsets of rules can be configured, depending on whether the protected application is accessed through the web or a VPN or SSH.

The VPN and SSH policy can be applied globally by configuring one or more rules in the default policy. For more information, see VPN and SSH policy.

The web authentication policy can be applied either:

- Globally using the default policy: The global (default) policy is only applied if no other web policy is defined or if no other web policy is applied during the authentication session. For more information, see Globally using the default policy.
- Per application or group: for PingFederate applications, you can apply a policy to one or more applications or to one or more user groups or both. If more than one policy exists for an application or user group, the policies are applied in the order that they appear in the **POLICY** list, as outlined in the policy rules. For more information, see Per application or group.

For more information, see Web authentication policy.

Policy implementation requirements

The PingID Policy service evaluates policies and rules according to the order in which they are listed. For more information, see Viewing and reordering authentication policies.

If an application or group appears in more than one policy, only the rules in the first applicable policy listed are applied.

Allowed authentication methods are defined per policy and affect the rule actions that can be selected. For detailed information about the allowed authentication methods and their implementation, see Policy and rule authentication methods.

For web application policies:

- PingFederate groups:
  - Use of PingFederate groups is only supported by PingID Adapter 2.1 or later.
  - To use PingFederate groups, enable the PingID **Adapter Query Directory** flag.
  - To ensure that no conflicts arise between policies, create and order policies carefully. This is of particular importance where users appear in more than one group. If a user or application appears in more than one policy, only the rules in the first applicable policy listed are applied.
  - PingFederate groups support LDAP groups, including OU's and CN's nested under OU's.
  - PingFederate groups only support the use of a single LDAP domain per organization.
  - PingID policy supports authentication of users with a maximum of 1000 LDAP groups using the `MemberOf` attribute. If a user is included in more than 1000 LDAP groups, rules that relate to groups are not applied when authenticating that user. When authenticating a user with more than 1000 groups, PingID still considers rules that do not include groups. If no other rule applies, the default rule is applied.
- PingFederate apps:
  - Using PingFederate apps requires the use of the PingID integration kit.
  - PingFederate apps are not included in the list automatically. You can add PingFederate applications to the applications list while creating a new policy. For more information, see Adding a PingFederate application.
- PingOne for Enterprise applications through PingID:

  To require users to authenticate using PingID when signing on to a PingOne for Enterprise application:
  - On the details page for the application, ensure that the **Force MFA** option is selected. For more information, see Add or update a SAML application.
  - In the **Policy** section on the PingID tab, apply the relevant authentication policy to the application.

When the organization requires biometrics authentication:

- In the PingID Admin portal, go to **Setup → PingID → Configuration**, and in the **Mobile App Authentication → Device Biometrics** section, if **Require** is chosen, and the policy is different, then the policy settings override the general admin configuration settings.

Policy evaluation

The PingID policy service evaluates the policies and then the rules within the selected policy.

Policy Evaluation

Policies are evaluated in the order in which they appear in the list on the **Policy** page as follows:

- The PingID policy service evaluates the first policy in the list on the **Policy** page and verifies whether the policy conditions are met. For example, if the user is trying to access one of the apps or is a member of one of the groups specified in the policy.
    - If the policy conditions are met, the PingID policy service does not evaluate any further policies and starts to evaluate the rules within the policy, as described in the next section.
    - If the policy conditions are not met, the PingID policy service evaluates the next policy that appears in the policy list.
    - If none of the policies were met, the default policy is applied.

> **Note**
>
> If prompt user to select is enabled, there are some situations in which the user will be able to select a device with which to authenticate, but the policy applied to the organization will prevent the user from authenticating with the selected device, causing the user to be blocked.

Rule Evaluation

Once the policy conditions are met, the PingID policy service evaluates policy rules as follows:

- The PingID policy service evaluates the first rule in the policy and verifies whether the rule conditions are met. For example, for the Specific Countries rule, is the user signing on from one of the defined locations?
    - If the rule conditions are met, the PingID policy service does not evaluate any further rules, and the rule action is applied.
    - If the rule conditions are not met, or the information required is not available, such as the location, the PingID policy service evaluates the next rule in the policy rule list.
    - If none of the rule conditions are met or the information required is not available, such as the location, the default action is applied.

Consideration for users with multiple devices

If a user has more than one device paired with their account:

- If the primary device is disallowed by a rule action, the user is only allowed to authenticate if their secondary device is permitted in the rule action.
- If the user's primary device is allowed by the policy and:
    - Rule action permits the primary device: the user is prompted to authenticate using the primary device.
    - Rule action requires a different device: the user is prompted to authenticate using the device specified. If the device required is not paired then the user is denied access.

- If the user's primary device is not allowed by the policy, and they have only one secondary device:
  - If the secondary device is allowed by the policy and rule action, the secondary device is selected automatically.
  - If the secondary device is not allowed either at policy or rule level, authentication is denied.

Considerations for users working on a shared accessing device

The PingID policy supports multiple users working on the same accessing device. Policy information is stored on the device per user. This enables PingID to evaluate users more accurately for policies, such as **Recent authentication**, per user for that device.

Example

For example:

If User A signs on at 9a.m., and User B signs on to the same device at 11a.m., and the organization employs a recent authentication rule that does not require authentication within 6 hours of authentication, the recent authentication is calculated from 9am for User A, and from 11am for User B.

> **Note**
>
> For Windows login, the PingID policy supports multiple users accessing the same device on a Windows login machine, however, the policy information is overridden each time the user signs on successfully.

Considerations for users working with more than one organization

The PingID policy supports a single user with multiple organizations and can distinguish between a user that is accessing more than one organization from the same accessing device. Policy information is stored on the device per user. This enables the PingID policy to evaluate users more accurately and consider users more accurately for policies, such as **Recent authentication**, per organization.

Example

For example:

If a user signs on to Organization Y at 9a.m. and Organization Z at 11a.m., and the organizations employ different recent authentication policies as follows:

- Organization Y: Recent authentication within the last 30 minutes.
- Organization Z: Recent authentication within the last 12 hours.

The user will be subject to the recent authentication policy of the organization that they are currently logged in to. In this example, they will need to authenticate again as follows:

- Organization Y: If logging in, or accessing resources after 9.30am the same day.
- Organization Z: If logging in, or accessing resources after 11pm the same day.

> **Note**
>
> For Windows login, the PingID policy supports multiple users accessing the same device on a Windows login machine, however, the policy information is overridden each time the user signs on successfully.

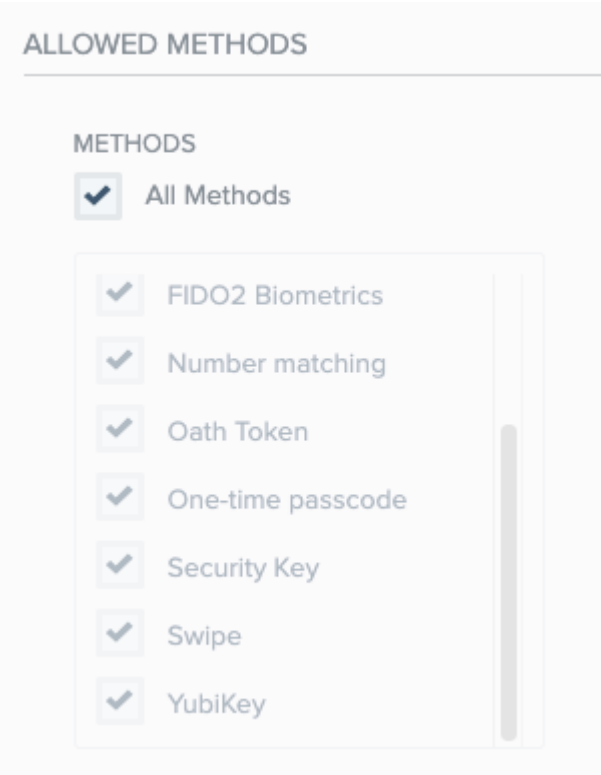
Policy and rule authentication methods

Define the authentication methods that you want to allow per policy and the authentication actions you want to enforce for each policy rule.

For examples of specific use cases and more detailed information about implementation, see Authentication method selection and priority - use cases.

Authentication methods are configured:

- Per policy: Select the authentication methods that you want to allow in the policy.

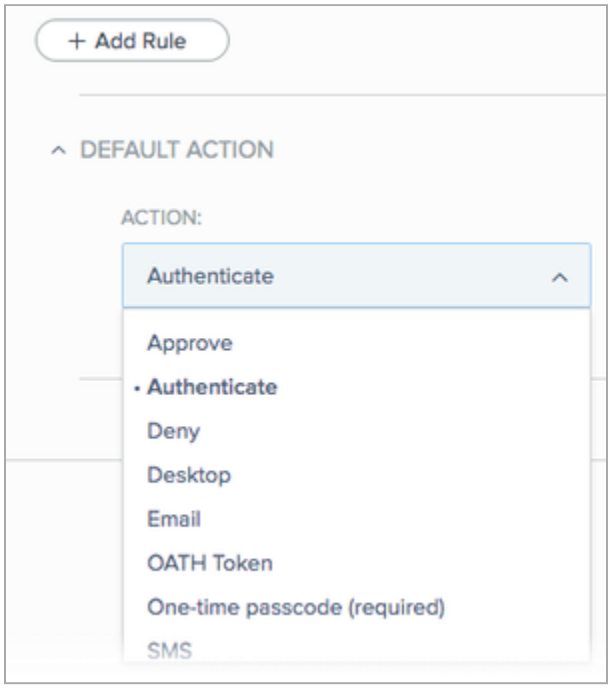


  - The authentication methods selected are the only authentication methods the user is allowed to authenticate with if this policy is applied.
  - The methods selected in the **Allowed Authentication Methods** section determine the actions available in all rules related to this policy.

    For a definition of the allowed authentication methods, see Allowed authentication methods.

    > **Note**
    >
    > Only authentication methods that are enabled at the organization level are available at the policy level. For details of how to configure authentication options at the organization level, see Configure the PingID service.

- Per rule: The Rule action determines how the user is authenticated in the event that the rule is applied. For a definition of the available rule authentication actions, see Rule authentication actions.



Allowed authentication methods

Define the authentication methods you want to make available for the policy in the **Allowed Authentication Methods** section. Only the selected allowed authentication methods are listed as options in the authentication rule **Action** list.

> **Note**
>
> If a new authentication method is added as a PingID capability and the **All Methods** check box is not selected in the **Allowed Authentication Methods** section, you must edit each policy and select the check box of the new authentication method manually to include it in a policy.

A description of the allowed authentication methods is shown in the following table.

Authentication methods allowed per policy

Allowed Authentication Method	Description
All Methods	Permit the use of all authentication methods currently configured for the organization. When the **All methods** check box is selected: • All available authentication methods are permitted at the policy level. • If additional authentication methods are added to PingID in the future, they are automatically applied to the policy. • Within a policy rule, all available authentication methods are listed in the rule **Actions** list. • Deprecated authentication actions appear and can be selected in policy rule **Actions** list. See Deprecated authentication actions. If the **All methods** check box is not selected: • Only the specific authentication methods selected in the **Allowed Authentication Methods** list are available for the user to authenticate. • If additional authentication methods are added to PingID in the future, they are not applied to existing policies automatically. Existing policies must be edited individually and the new authentication method added manually in order to apply it to the policy. • Within a rule, only the selected authentication methods are listed in the authentication actions in addition to relevant default actions, such as **Approve**, **Deny**, and **Authenticate**. • Deprecated authentication actions are not available in the policy rule **Actions** list.
Authenticator app	Authentication using an authenticator app, such as Google authenticator, is permitted.
Backup Authentication	Authentication using a backup authentication method is permitted. This option is useful if a user forgets their device, or it is lost or stolen. The **Forgot your device?** link only appears if: • Either the **Authenticate** rule action, or a rule action that includes a mobile device authentication method such as **Mobile App Biometrics**, is configured. • At least one backup authentication method is defined. See Configuring backup authentication methods.
Desktop	Authentication by a desktop app is permitted.
Email	Authentication by email is permitted.
FIDO2 Biometrics	Authentication by a FIDO2 biometrics device is permitted for web-based policies only.
Mobile App Biometrics	Authentication by a supported biometrics devices is permitted and applied according to the configuration defined in the Admin portal.

Allowed Authentication Method	Description
Number matching	Authenticate by number matching is permitted. • Number matching has priority over **Mobile App Biometrics** and **Swipe** authentication methods. • If **Mobile app biometrics** is set to **Require** in the **Configuration** tab, the user must authenticate successfully using biometrics and then authenticate using number matching. • Number matching is only supported by apps that are using web-based authentication.
Oath Token	Authentication using an OATH Token is permitted.
One-time passcode	Authentication using a one-time passcode (OTP) obtained using PingID mobile app is permitted. **Important** If this option is not selected, fallback to a OTP and direct passcode usage are not allowed, even if it is enabled in the **Configuration** page.
SMS	Authentication using an OTP obtained through SMS is permitted.
Security Key	Authentication using a security key is permitted for web-based policies only.
Swipe	Authentication using swipe is permitted.
Voice	Authentication using an OTP obtained through voice message is permitted.
YubiKey	Authentication using a YubiKey is permitted.

Rule authentication actions

The list of authentication actions that you can choose to enforce within a policy rule is determined by the authentication methods allowed at the policy level.

Rule authentication actions and deprecated actions

Authentication Action		Description
Approve		Approves access without requiring PingID authentication. **Note** This rule action cannot be used in a PingFederate passwordless flow, because at least one factor authentication is required to use the **Approve** action.

Authentication Action		Description
Authenticate		Allows a user to authenticate using any of the authentication methods available to the user and allowed at the policy level. **Note** If a user has a mobile app with both biometrics and swipe capabilities, biometrics authentication is given priority.
Authenticator app		Allows a user to authenticate using an authenticator app only, such as Google authenticator.
Deny		Denies access.
Desktop		Allows a user to authenticate using a desktop app only.
Email		Allows a user to authenticate using an email app only.
FIDO2 Biometrics		Allows a user to authenticate using device built in biometrics on a FIDO2 biometrics device. This option is only available for web-based policies.
Mobile App Biometrics		Allows a user to authenticate with the PingID mobile app using biometrics authentication only. This action works according to the biometrics configuration defined in the admin portal. Swipe authentication is also permitted if the following conditions are met: • If **Device Biometrics** is configured as **Enabled**, and biometrics are not defined on the user's device. • If **Device Biometrics** is not configured as **Require** in the admin configuration page. • If biometrics are not supported on the user's device. **Note** A one-time passcode fallback is also permitted when selecting this option.
	DEPRECATED: **Fingerprint (with fallback)**	• If the primary or selected device is the PingID mobile app, fingerprint authentication is used according to the fingerprint configuration defined in the admin portal. Fingerprint is the preferred method, but it is also possible to authenticate using swipe or a one-time passcode (OTP). • If the primary or selected device is not the PingID mobile app, the user authenticates with that device.

Authentication Action		Description
Number matching		Authenticate by number matching is permitted. • Number matching has priority over **Mobile App Biometrics** and **Swipe** authentication methods. • If **Mobile app biometrics** is set to **Require** in the **Configuration** tab, the user must authenticate successfully using biometrics and then authenticate using number matching.
Oath Token		Allows a user to authenticate using an OATH token only.
One-time passcode	**One-time passcode (required)**	Allows a user to authenticate using a OTP obtained from the PingID mobile app only.
	DEPRECATED: **One-time passcode (with fallback)**	• If the primary or selected device is the PingID mobile app, the user must enter an OTP using the mobile app. **Note** Swipe or fingerprint authentication is not permitted in this case. • If the primary or selected device is not the PingID mobile app, the user authenticates with that device.
SMS		Allows a user to authenticate using a passcode obtained by SMS only.
Security Key		Allows a user to authenticate using a security key only. This option is only available for web-based policies.
Swipe	**Swipe (required)**	Allows a user to authenticate using the PingID mobile app swipe action only. **Note** A OTP fallback is also possible when selecting this option.
	DEPRECATED: **Swipe (with fallback)**	• If the primary or selected device is the PingID mobile app, swipe is always required. **Note** Even if the user has fingerprint authentication defined on their device, fingerprint is not required in this case. • If the primary or selected device is not the PingID mobile app, the user authenticates with that device.
Voice		Allows a user to authenticate using a passcode obtained by a voice message only.

Authentication Action		Description
YubiKey		Allows a user to authenticate using a YubiKey only.

Deprecated actions

Some of the authentication methods in the rule **Action** list are in the process of being deprecated and will be removed at a future date. Until they are decommissioned, existing policies that contain deprecated actions remain unchanged.

Deprecated (legacy) actions are available for backward compatibility although the names have been changed to reflect their legacy status. For the updated names, see Rule authentication actions.

Deprecated authentication actions are only available in the rule **Action** list if the **All Methods** check box is selected in the **Allowed Authentication Methods** section at the policy level. We recommend that you upgrade all existing policy rules to the new, more specific authentication actions.

Authentication method selection and priority - use cases

See the following table for detailed examples of use cases where the configuration at the organization level can affect the implementation of an authentication policy.

Authentication method selection by specific use cases

Use Case	User Paired Devices	Allowed Authentication Methods	Rule Action	Result	Reason
1	• SMS (primary) • Email	All methods	Email	User is requested to authenticate through email	Although the primary is SMS, the user is requested to authenticate using email as the rule action requires email.
2	• Desktop (primary) • Email • YubiKey	YubiKey	Authenticate	User is requested to authenticate with YubiKey	User is automatically prompted to authenticate using a YubiKey, regardless of whether the configuration is set to **Default to Primary** or **Prompt user to select**. This is because the user only has one allowed authentication method paired with their account.

Use Case	User Paired Devices	Allowed Authentication Methods	Rule Action	Result	Reason
3	• The PingID mobile app (primary) • SMS • Voice	SMS/ Voice/ Email	Authenticate	User is unable to authenticate	• **Default to Primary**: Even though the user's primary device is disallowed (PingID Mobile app), the user is prompted to authenticate with the device that was enrolled first out of the list of allowed secondary devices. • **Prompt user to select:** the user is presented with a list of secondary devices. The user selects the secondary device with which they want to authenticate.
4	• SMS (primary) • YubiKey • Email	Mobile App Biometrics/ Swipe / One-time passcode	Authenticate	Authentication denied	User does not have one of the allowed authentication methods paired with their account.
5	• The PingID mobile app (primary) • Desktop • Voice	All methods	SMS	Authentication denied	User does not have the required authentication method paired with their account.
6	The PingID mobile app (Swipe disabled)	Mobile App Biometrics/ Swipe	Authenticate	Authentication denied	Swipe is disabled in the PingID mobile app and the user is unable to receive a push notification. As a one-time passcode (OTP) is not included in the **Allowed Authentication Methods**, the user cannot use an OTP, even if OTP Fallback is enabled.

Use Case	User Paired Devices	Allowed Authentication Methods	Rule Action	Result	Reason
7	The PingID mobile app (Swipe disabled)	All methods	Mobile App Biometrics (required)	Authentication denied	Mobile App Biometrics (required) permits authentication with biometrics only, and does not allow use of an OTP. “Swipe disabled” prevents the user from receiving a push notification to their device, preventing the user from authenticating with biometrics.
8	The PingID mobile app where: • Device supports biometrics • Biometrics not defined on device	Mobile App Biometrics	Mobile App Biometrics (required)	The user is able to authenticate using swipe or their device passcode in the event that their device screen is locked.	If a device does not support biometrics, PingID allows the user to authenticate using swipe as an exception. If the device supports biometrics, but biometrics are not defined on the device, the user can use swipe. This is possible because biometrics is enabled (and not required) by the biometrics configuration
9	The PingID mobile app where: • Device does not support biometrics • Biometrics required at configuration level	Mobile App Biometrics	Mobile App Biometrics (required)	The user is able to authenticate using swipe or their device passcode in the event that their device screen is locked.	Although biometrics is required, because the user’s device does not support biometrics, the user is still able to authenticate with swipe (if device unlocked), or using their device passcode (if device is locked).

Use Case	User Paired Devices	Allowed Authentication Methods	Rule Action	Result	Reason
10	The PingID mobile app where: • Device supports biometrics • Biometrics not defined on device • Biometrics required at configuration level	Mobile App Biometrics	Mobile App Biometrics (required)	The user is not able to authenticate	Biometrics are required at the configuration level, and biometrics authentication is possible on the user's device. The user is not able to authenticate because they have not defined biometrics on the device.
11	The PingID mobile app where: • Device supports biometrics • Biometrics are defined on device • Biometrics required at configuration level	Mobile App Biometrics / Swipe	Authenticate	User is able to authenticate with biometrics	Biometrics have a higher priority over swipe, and the user is prompted to authenticate with biometrics.

Use Case	User Paired Devices	Allowed Authentication Methods	Rule Action	Result	Reason
12	• Security key (primary) • Email • SMS Where the browser used does not provide WebAuthn support required for security key.	All methods	Authenticate	User is able to authenticate with email or SMS	• **Default to Primary**: Even though the user's primary device is disallowed because the browser does not support WebAuthn, the user is prompted to authenticate with the secondary device that was enrolled first out of the list of allowed secondary devices. • **Prompt user to select:** A security key is not included in the list of devices, as the browser does not support WebAuthn. The user is presented with a list of secondary devices only. The user selects the secondary device with which they want to authenticate.
13	• Security key (primary) • Email • SMS Where the browser used does not provide WebAuthn support required for security key.	All methods	Security Key	User is unable to authenticate	Even though the user has a security key paired with their account, they are signing on using a browser that does not support WebAuthn.

Use Case	User Paired Devices	Allowed Authentication Methods	Rule Action	Result	Reason
14	• The PingID mobile app (primary) • Security key • Email Where the browser supports WebAuthn. Policy rule **authenticating from a new device** is applied and requires a security key.	All methods	Security key	User is able to authenticate with a Security key only. In the case of a phishing attack, the user is not able to authenticate with any device.	• If authenticating from a new device a security key is required. • If the user is subject to a phishing attack, PingID can distinguish between a known and a fraudulent copy of a web page. If fraudulent, PingID does not recognize the source and triggers the **accessing from new device** policy rule. Even though the user has other devices paired, they are prompted to authenticate using a security key only, and cannot change device due to the policy rule restrictions. This configuration guards all devices against a phishing attack.
15	• FIDO2 biometrics (primary) • Email • SMS Where the browser used does not provide WebAuthn Platform support.	All methods	FIDO2 Biometrics	User is unable to authenticate	Even though the user has a FIDO2 biometrics device paired with their account, they are signing on using a browser that does not support WebAuthn.

Use Case	User Paired Devices	Allowed Authentication Methods	Rule Action	Result	Reason
16	• The PingID mobile app (primary) • FIDO2 Biometrics • Email Where the browser supports a WebAuthn Platform. Policy rule **authenticating from a new device** is applied and requires a security key.	All methods	FIDO2	User is able to authenticate with FIDO2 only. In the case of a phishing attack, the user is not able to authenticate with any device.	• If authenticating from a new device, FIDO2 biometrics device is required. • If the user is subject to a phishing attack, PingID can distinguish between a known and a fraudulent copy of a web page. If fraudulent, PingID does not recognize the source and triggers the **accessing from new device** policy rule. Even though the user has other devices paired, they are prompted to authenticate using a FIDO2 biometrics device only and cannot change device due to the policy rule restrictions. This configuration guards all devices against a phishing attack.

Web authentication policy configuration

Create a policy, define the apps and groups to which the policy applies, define the authentication methods that are allowed in the policy, and add one or more rules to the policy.

The following rules can be configured:

- Access from the company network: Specify the IP addresses that define the company network, allow silent authentication for users within the company network, or specify the method of authentication you require when within the company network.
- Accessing from countries: Specify the authentication method required when within a specific country or countries, or deny access for specific countries.
- Authenticating from a new device: Specify the authentication method required when authenticating from a new device.
- Recently authenticating from office: Determine which authentication action should be performed if the previous authentication request was within the defined period of time, and from the same accessing device, and the authenticating device's mobile location is the office.
- Recent authentication: Specify which authentication action should be performed if the previous authentication request was within the defined period of time, and from the same accessing device.

- Mobile OS version: Specify which authentication action should be performed for the defined mobile OS versions. Deny access for versions that are below a specific version, or define a specific authentication method for versions above a specific version.
- Recent authentication from company network: Specify which authentication action should be performed when logging in from within the company network, if the previous authentication request was within the defined time period. Optionally specify that the user's mobile device's must be located in the office during authentication.
- IP reputation rule: Specify authentication method according to the risk score of the IP address of the accessing device. Determine which authentication action should be performed for accessing devices with low, medium, or high risk IP addresses.
- Geovelocity anomaly rule: Specify the authentication method or deny access, if travel between the current login location and previous login location is not possible in the time elapsed since the last login.
- Limit push notifications rule: Reduce the likelihood of a user acknowledging a malicious push notification as part of an MFA fatigue attack by limiting the number of push notifications the user can deny or ignore within a given time period, and specifying appropriate rule actions.

To provide a higher level of security against phishing attacks when using various MFA authentication methods, we suggest you add the **Authenticating from a new device** rule to your policy and configure the rule action to require **Security key**.

If this is configured, and a user accidentally enters a phishing site, because it is the first time a user has entered the site and no previous authentication has occurred from the site, PingID will apply a device blessing policy. Therefore, the **Authenticating from new device**rule will be triggered and the user will be prompted to authenticate using their security key. Authentication with security key will fail as there was no match between the phishing host name to the legitimate hostname that was stored for the security key during registration time. Any other paired authentication method cannot be used to authenticate due to the **Authenticating from new device** rule action, protecting the user from the malicious site.

Important

If you define more than one policy, the policies are executed in the order in which they are appear in the Policy list. If you include more than one rule in a policy, the rules are executed in the order in which they appear in the policy. If an application or group appears in more than one policy, only the rules in the first applicable policy listed are applied (see Policy evaluation and Policy implementation requirements for further details).

Note

If you are using PingOne DaVinci to orchestrate your PingID flows, the following rules are not evaluated:

- Limit push notifications rule
- Mobile OS version rule
- Recent authentication from office rule
- Accessing from company network rule: authenticating device in company offices section
- Recent authentication from company network rule: authenticating device in company offices section

Viewing and reordering authentication policies

View, reorder, and edit the list of existing authentication policies or rules within a policy.

About this task

PingID executes policies in the order in which they are listed. The order in which the policies are listed is significant. For example, if an application is included in more than one policy, only the first policy in the list is executed and applied when a user attempts to access the application.

If a policy includes more than one rule, the order in which the rules are listed within the policy is also important. Policy rules are executed in the order in which they are listed, and after a rule's conditions are met, subsequent rules listed are not evaluated.

You can change the order in which both policies and the rules within a policy are listed.

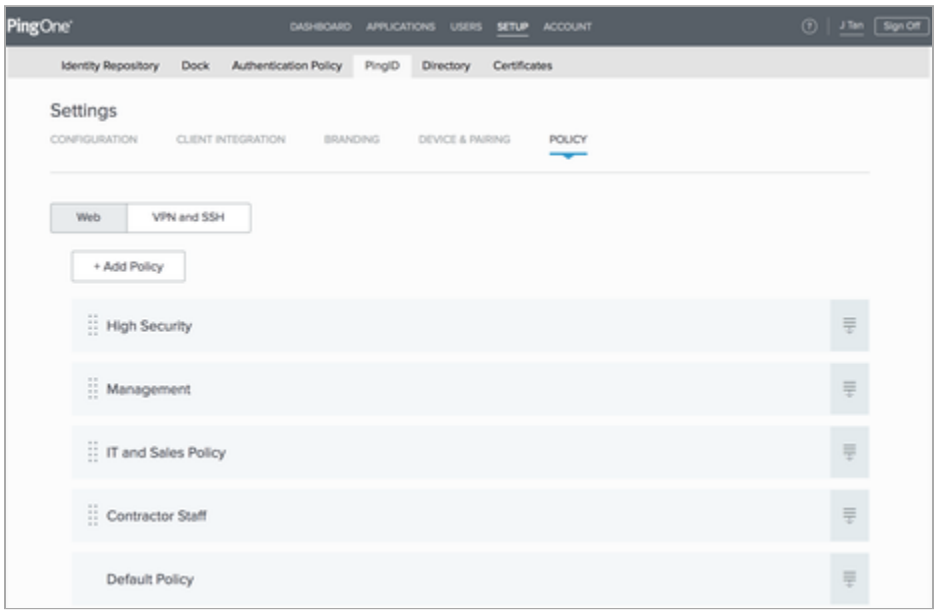
If more than one policy exists for an application or user group, the policies are applied in the order that they appear in the policy list as outlined in the policy rules.

Steps

1. Go to **Setup → PingID → Settings → Policy**, and click the **Web** tab.

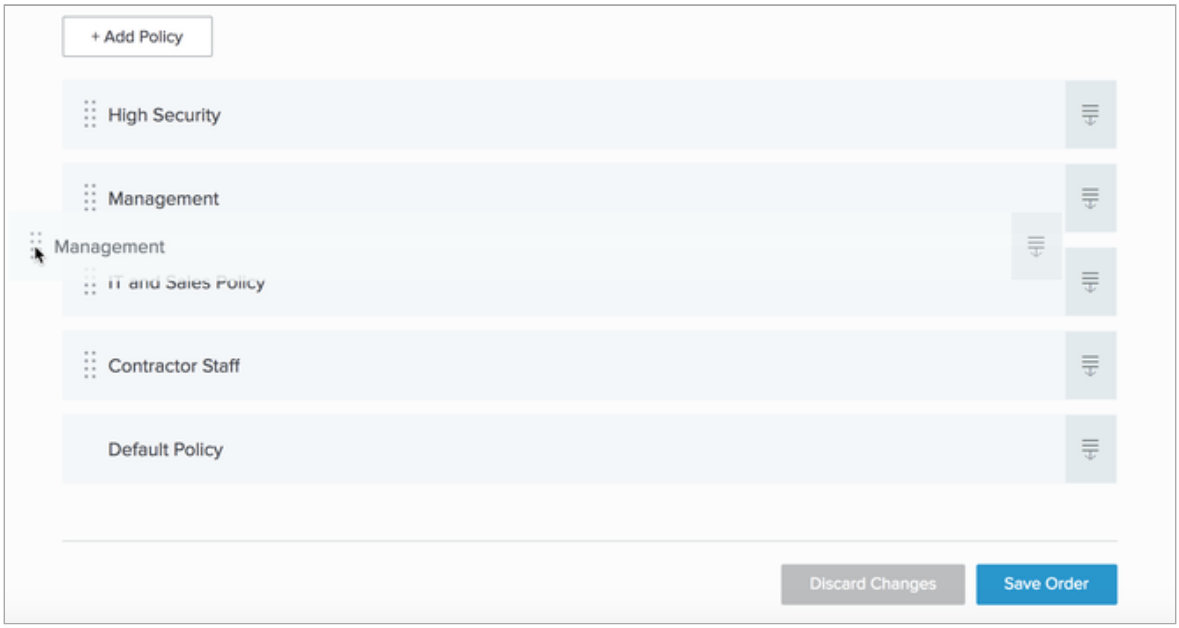
   Choose from:

   - To view the list of policies and the order in which they are executed, click the **Web** tab.

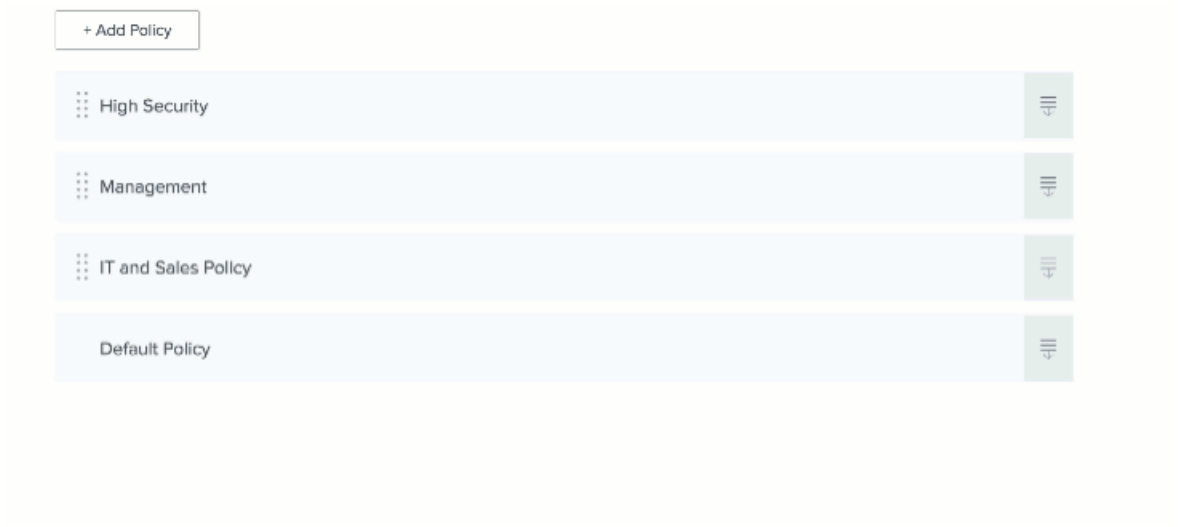


   - To reorder a policy:

     1. From the policies list, select the policy.
     2. Drag the policy to the position that you want it to be placed and release the mouse.



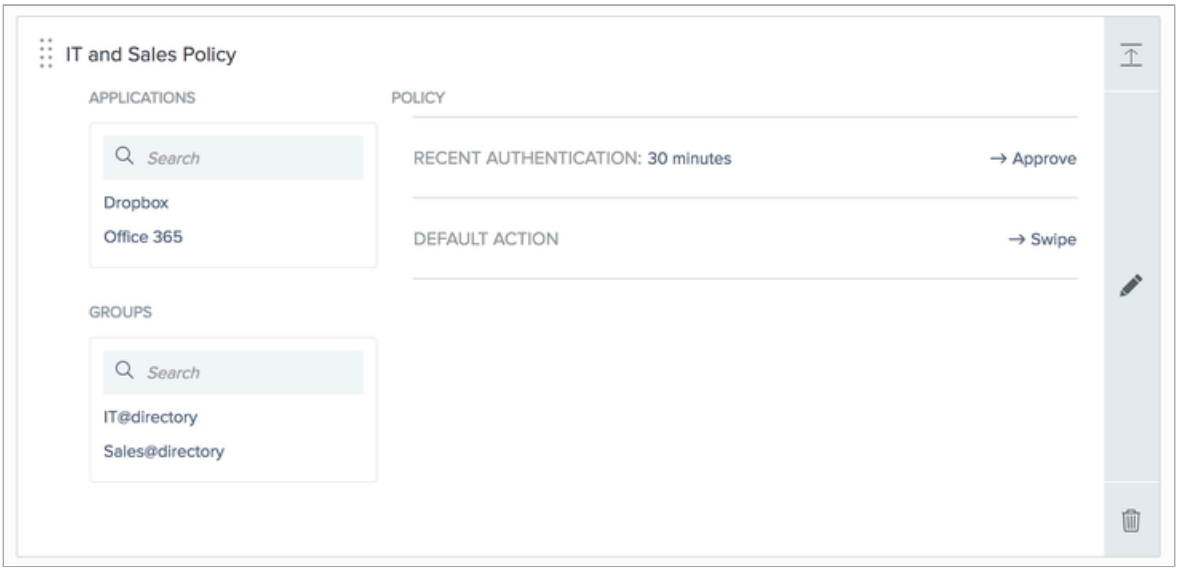
3. To secure the new order of the policies, click **Save Order**.



◦ To view or edit the policy details of a specific policy:

1. To expand an entry, click the **Expand** icon ( ).

> **Note**
>
> The applications and groups to which the policy applies are listed in the left column. The rules included in the policy and their configuration are listed in the right column.



- To edit a policy, click the **Pencil** icon ( ).

  You can edit the **Applications** and **Groups** to which the policy is applied, as well as the rules that are included in the policy. You can also rename the policy. For more information, see Editing a web authentication policy.

- To delete a policy, click the **Delete** icon.

Configuring a global authentication policy (default policy)

The default policy is a global policy that is applied to any application in your organization where no application-specific policy is defined. The default policy rules are applied when a user attempts to access the protected application through web access or sign on.

About this task

By default, the default policy includes a single default action **Authenticate** that is applied to a user access request. You can edit the default policy to modify the default action or to include additional rules.

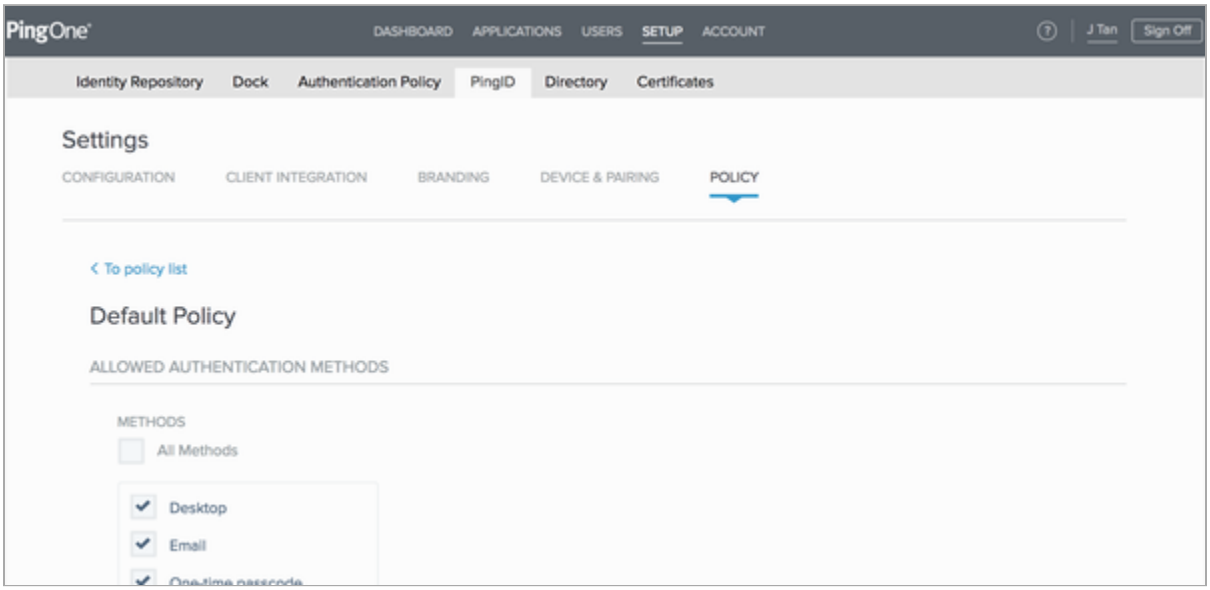
> **Note**
>
> An application- or group-specific policy always overrides the default policy configuration. To configure an application- or group-specific policy, see Configuring an app or group-specific authentication policy.

Steps

1. In the admin portal, go to **Setup → PingID → Settings → Policy → Web**.

   Result:

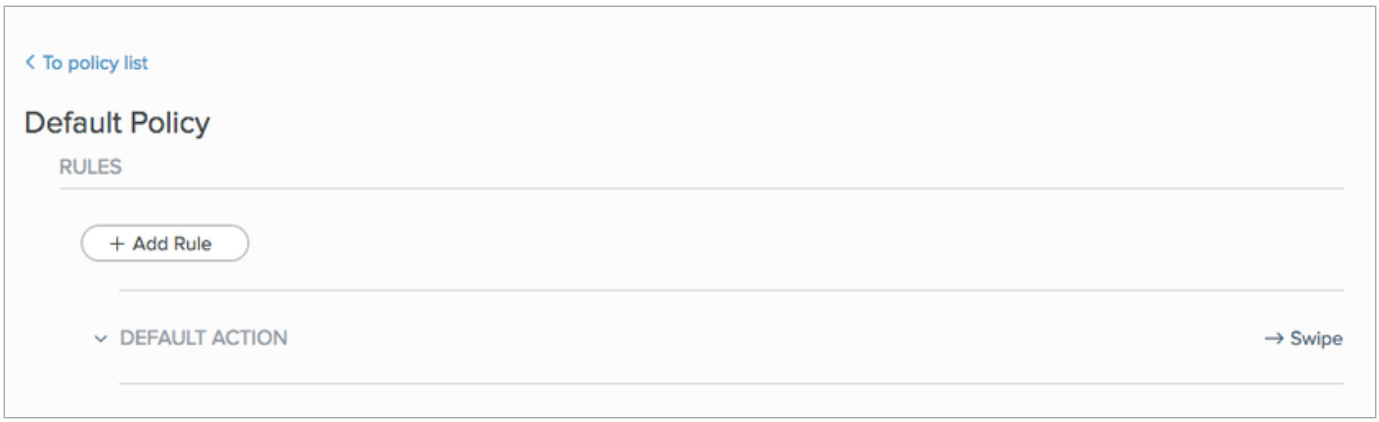
   The **Default Policy** is displayed.



2. Click the **Expand** icon ( ), and then click the **Pencil** icon ( ).

   Result:

   The **Default Policy** section displays showing the **Default Action** rule.



3. To edit the **Default Action** rule, click the **Arrow** icon to expand the rule.

> **Note**
>
> The **Default Action** rule determines which authentication action will be performed when no other default policy rule applies.

4. Select the action you want to apply:

   Choose from:

   - **Approve**: Approve access without requiring PingID authentication.
   - **Authenticate**: Allow the user to authenticate using any of the authentication methods available to the user, and allowed at the policy level.

- **Allowed Methods**: Click **Allowed Methods** to reveal a list of authentication methods allowed by this policy, and then select the check box of each authentication method that you want to allow for this rule. See Rule authentication actions for description per authentication type.
- **Deny**: Deny access.

5. From the **Allowed Authentication Methods** list, select a specific authentication method check box.

   The options listed are defined by those configured at policy level. For descriptions by authentication type, see Rule authentication actions.

6. To add and configure one or more rules to replace the **Default Action**:
   1. Click **+ Add Rule**.
   2. Configure one or more of the following rules:
      - Configure a company network access rule
      - Configure a rule for access from specific countries
      - Configure access rule from a new device
      - Configure recent authentication from office access rule
      - Configure recent authentication access rule
      - Configure mobile OS version access rule
      - Configuring a recent authentication from company network rule
      - Configuring an IP reputation rule (web policy)
      - Configuring a geovelocity anomaly rule (web policy)
      - Configuring a limit push notifications rule
7. Click **Save**.

Result

The **Default Policy** is saved and applied to all applications where an application-specific policy is not defined.

Configuring an app or group-specific authentication policy

Create a web authentication policy and apply it to one or more applications, one or more user groups, or both.

About this task

Configure various policies that are tailor made for your system. For example, you can configure a policy for your HR group that applies to several sensitive HR-related apps only. You could create three different policies for a high security app, giving different authentication policies to the Management group, the General User group, and the Contractor group.

If an app or group is included in more than one policy, only the first policy in which it is listed will be applied. If no policy exists for a specific application when a user signs on and attempts to access that application, the global policy (default policy) is applied.

> **Note**
>
> If you are interested in using the PingID API to create and update web authentication policies, see Web Authentication Policy API.

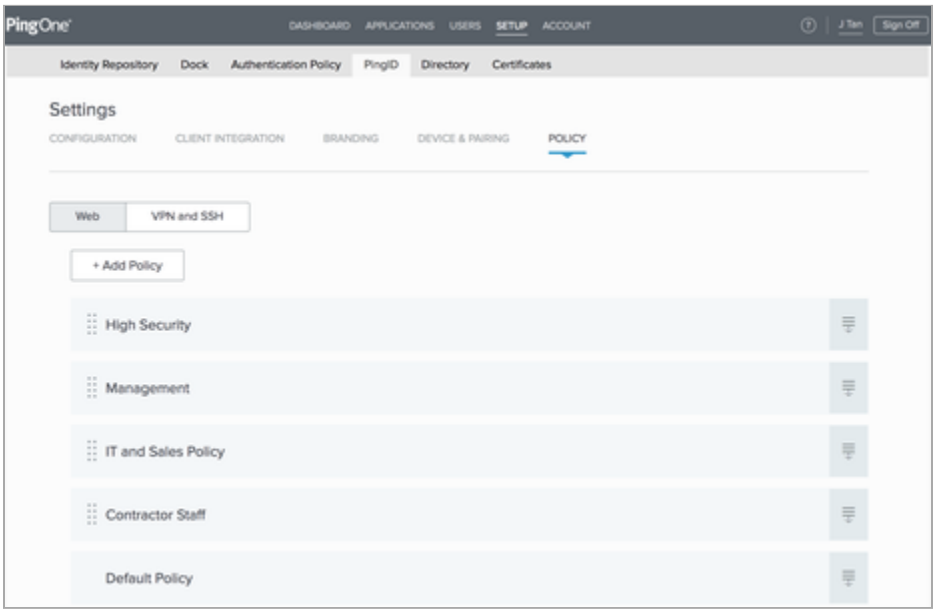
The following apps appear in the **Policy Apps** list by default:

- **AD FS**: Enables you to apply an authentication policy to users when Microsoft AD FS is the identity provider (IdP). For more information, see Integrate PingID with AD FS.
- **Admin Portal**: Enables you to apply an authentication policy to admins when accessing the admin portal.
- **Azure AD**: Enables you to apply an authentication policy to users when Microsoft Azure AD is the IdP. For more information, see Integrate PingID with Azure AD.
- **Device Management**: Enables you to apply an authentication policy to users when they authenticate to PingID's out of the box **Devices** page. The **Devices** page is used to add, remove, or change the devices a user has associated with their account. For more information, see Managing your devices.
- **Password Reset**: Enables you to apply an authentication policy to users requesting a password reset using the self-service password reset service from PingFederate. This service is accessed through the password reset link that appears on the sign on page when PingFederate is the IdP. For more information, see Configure self-service password reset.

> **Note**
>
> The default policy is a global policy that defines the rules that will be applied to any application in your organization where an application-specific policy is not defined. For more information, see Configure a global authentication policy.

Steps

1. In PingOne, go to **Setup → PingID → Settings → Policy**.

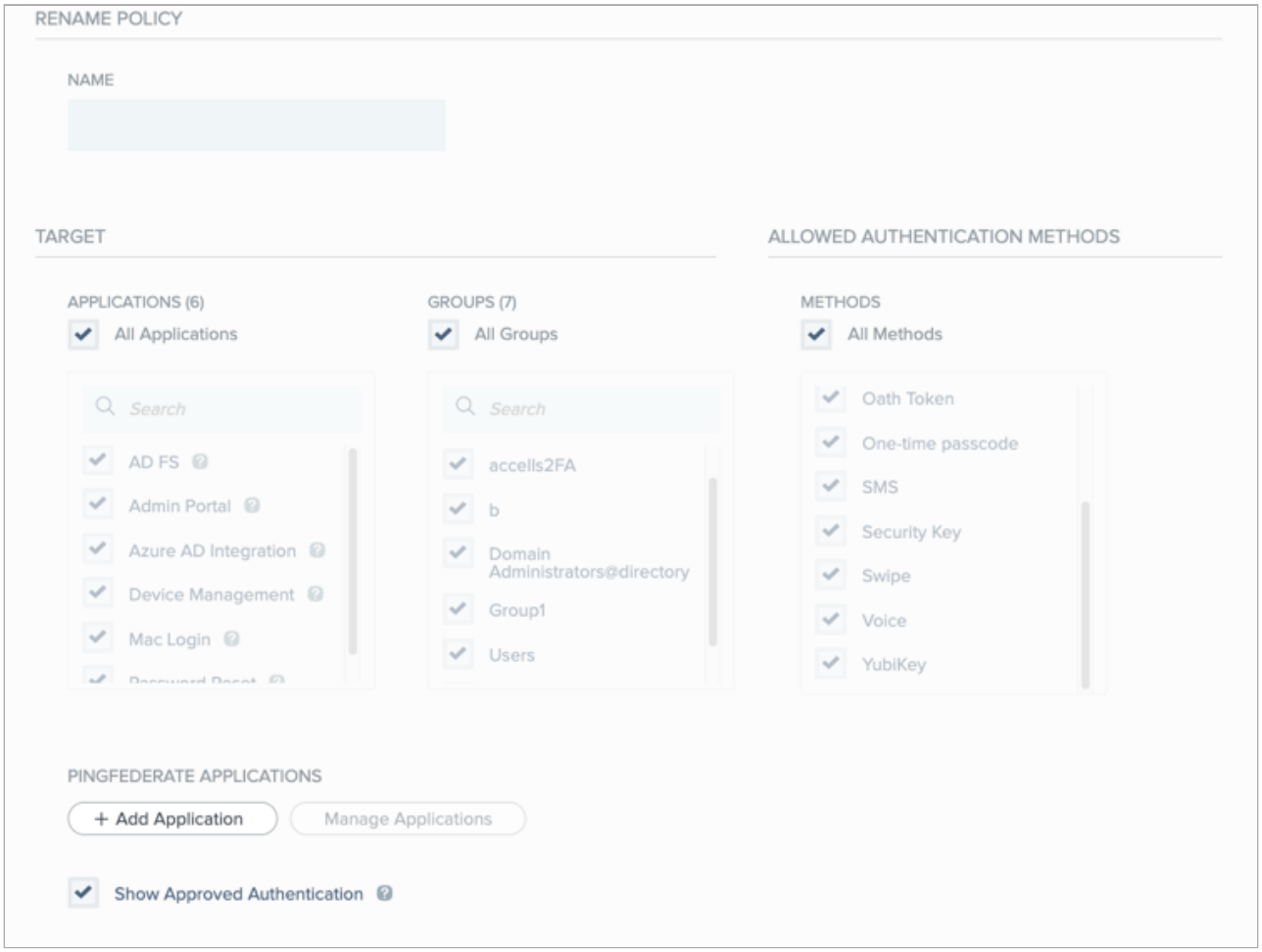


2. Click **+ Add Policy**.

Result:

The **New Policy** wizard opens.

3. In the **Name** field, enter a name for the policy.



4. In the **Applications** section, use the controls to select the applications to which the policy should apply. You must select at least one application. By default, the list shows the applications that you have defined in PingOne. To add PingFederate applications to the list, click the **Add Application** button. For more information, see Adding a PingFederate application.

> **Note**
>
> - List display items are limited to 300 for **Applications** and **Groups**. Use the search box to search for a specific application or group.
> - The **All Applications**/**Groups**/**Methods** check box selects all existing items and automatically applies any additional items that are added to PingID in the future.

> **Note**
>
> App-specific policies require the PingID Adapter 1.4 or later.

5. In the **Groups** section, select the check box for each group to which you want the policy to apply. You must select at least one group. If you want to apply the policy to all user groups, select the **All Groups** check box.

> **Note**
>
> If you are defining a policy that is also applicable to Windows login and want to make it applicable to only specific groups of users, keep the following points in mind:
> - The integration with Windows login must be through PingFederate.
> - You must be using version 2.4.2 or higher of the integration with Windows login.
> - You must have provided information for the **Group** attribute when configuring the PingID Adapter instance (see Configuring a PingID Adapter instance (Windows login)).

6. In the **Allowed Authentication Methods** section:

   Choose from:

   - Select one or more authentication methods that you want to make available for use in this policy.
   - Select the **All Methods** check box to permit the use of all existing configured authentication methods and automatically apply additional methods that are added to PingID in the future.

   > **Note**
   >
   > Only the methods selected are permitted for use in this policy and available in the rule **Actions** list.

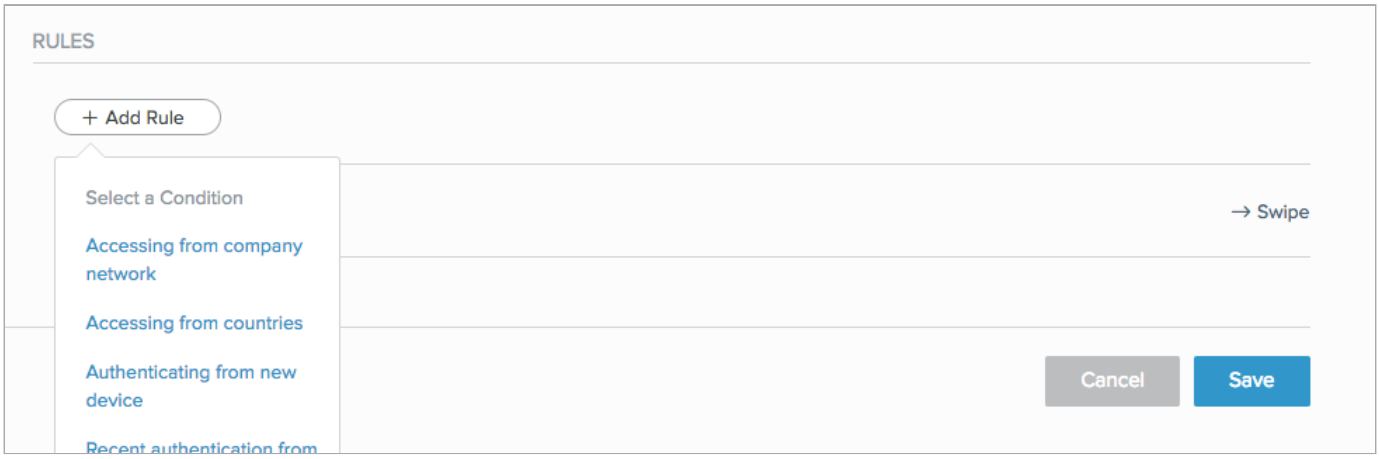
   > **Important**
   >
   > If you are configuring a rule that is based on the PingID mobile app, **Swipe**, **Mobile App Biometrics**, **Number matching** or **One-time passcode** must be included as an allowed authentication method.

7. To hide the authentication approval screen for PingID policy events in which the user is automatically approved and no challenge is sent to or requested from the user, clear the **Show Approved Authentication** check box.

   By default, this check box is selected.

> **Note**
>
> This option only applies to:
> - Relevant policy rules where the rule action **Approve** is selected.
> - PingID out of the box UI. It is not applicable to the PingID authentication API.

8. In the **Rules** section, click **+ Add Rule** for each rule that you want to add, and select the rule from the list.



9. Configure the rules that you want to include in the policy:
    - Configure a company network access rule
    - Configure a rule for access from specific countries
    - Configure authenticating from new device rule
    - Configure recent authentication from office access rule
    - Configure recent authentication access rule
    - Configure mobile OS version access rule
    - Configuring a recent authentication from company network rule
    - Configuring an IP reputation rule (web policy)
    - Configuring a geovelocity anomaly rule (web policy)
    - Configuring a risk level rule (web policy)
    - Configuring a limit push notifications rule
10. Within the policy, click and drag the rule to place it in the order you want it.

> **Important**
>
> If you have more than one rule in the policy, ensure that the rule appears in the order that you want it because this is the order that the rule will be executed.

11. After you have added and configured all the rules you want to add, click **Save**.
12. If more than one policy appears in the **Policy** list, click and drag the new policy and place it in the order that you want it to be considered. Click **Save Order**.

Next steps

To ensure the policy is applied to your organization, go to **PingID → Configuration** and ensure **Enforce Policy** is set to **Enabled**.

Configuring an accessing from company network rule (web policy)

About this task

Use this rule to define:

- The authentication action to prompt the user with if the web accessing device is within the company network, such as requiring a specific authentication method when within the company network, like **Mobile App Biometrics** or **Swipe**, or allowing silent authentication when within the company network.
- Optionally require the user's mobile authenticating device to be located within a defined office location during authentication with the **Authenticating Device in Company Offices** option. If this option is enabled, to sign on:
    - The user's authenticating device must be in a company office location.

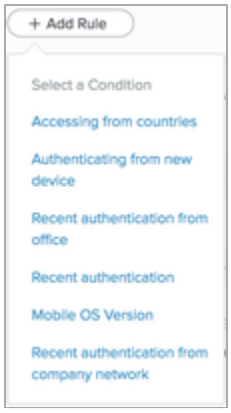
- The user's accessing device should originate from an IP address within the company network.

When creating this rule, you must specify the IP addresses that define the company network or define the geographic location of one or more offices around the world or both.

> **Note**
>
> If you are using PingOne DaVinci to orchestrate your PingID flows, the **authenticating device in company offices** section is not included in the policy evaluation.

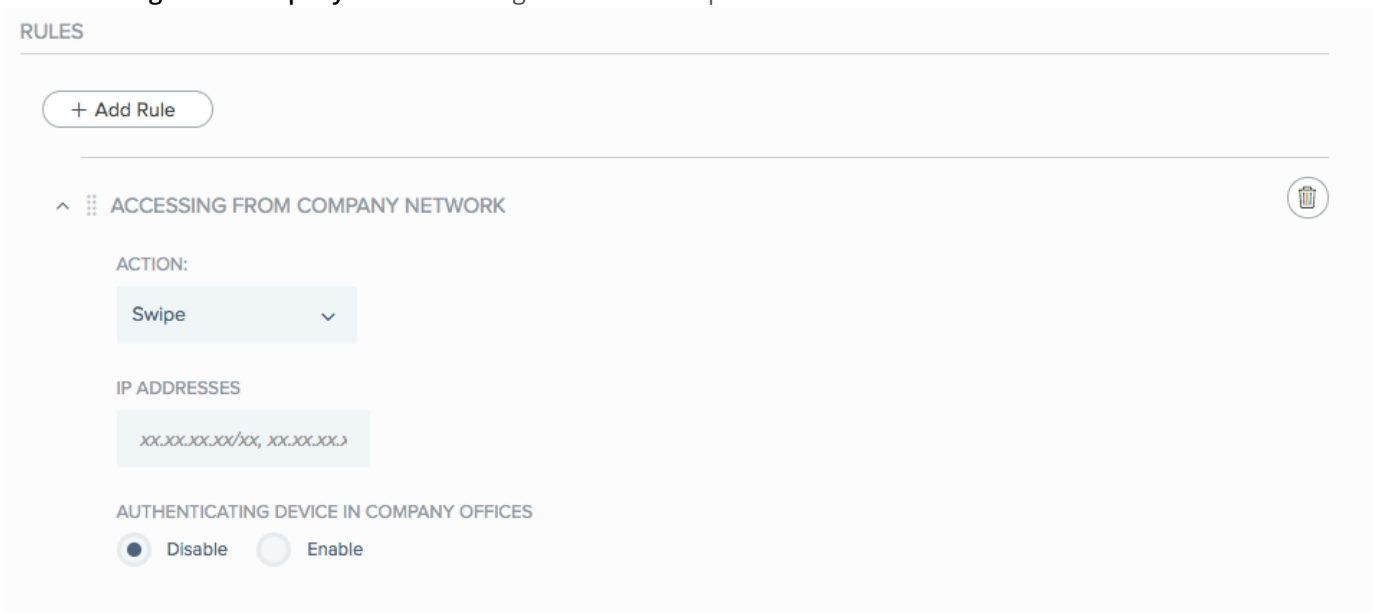
Steps

1. In PingOne, go to **Setup → PingID → Policy**.
2. From within the relevant policy, click **+ Add Rule**, and from the rule list, select **Accessing From Company Network**.



Result:

The **Accessing From Company Network** configuration wizard opens.



3. From the **Action** list, select the authentication action to be used if the rule conditions are met.

Choose from:

- **Approve**: Approve access without requiring PingID authentication.

- **Authenticate**: Allow the user to authenticate using any of the authentication methods available to the user, and allowed at the policy level.
- **Allowed Methods**: Click **Allowed Methods** to reveal a list of authentication methods allowed by this policy, and then select the check box of each authentication method that you want to allow for this rule. See Rule authentication actions for description per authentication type.

4. In the **IP Addresses** field, enter a list of external IP addresses or the IP range that belongs to the company network.

> **Note**
>
> Enter the IP addresses and ranges using CIDR notation with each entry on its own line.

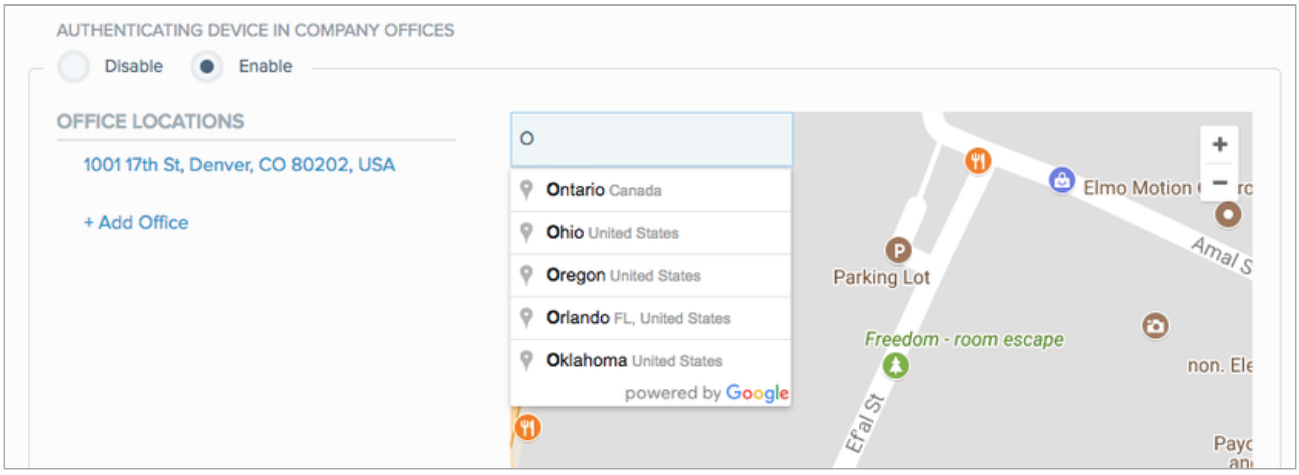
5. To require a user's authenticating device to be in the company offices when signing on from within the company network:
    1. Go to the **Authenticating Device In Company Offices** section.
    2. Click **Enable**.
    3. Define one or more company office locations.

       If the authenticating device is located within one of the defined areas, it is considered to be inside a company office.

       > **Note**
       >
       > If you are including a company office location in this rule, **Swipe**, **Mobile App Biometrics**, or a **One-time passcode** must be defined as an **Allowed Authentication Method** to ensure location-based information can be collected from the user.

       Result:

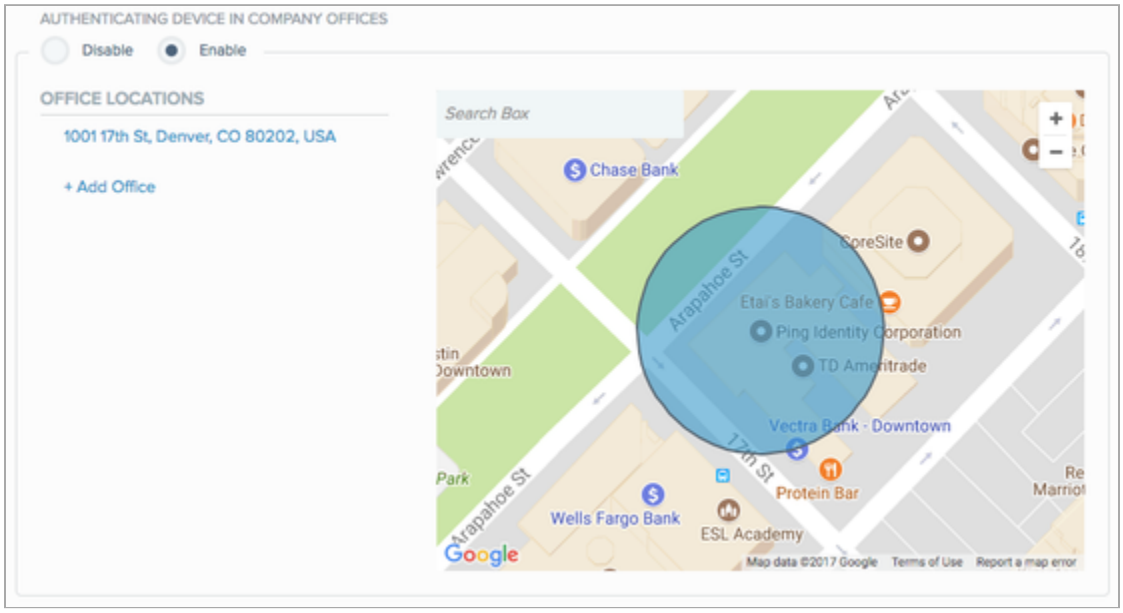
       The **Office Locations** wizard opens enabling you to define one or more office locations.



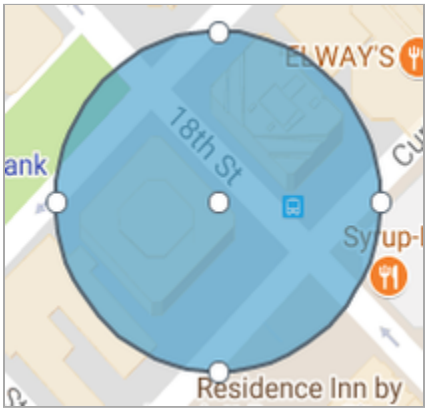
6. To define additional office locations:
    1. Click **+ Add Office** or enter an address in the search box.

       Result:

       A blue circle appears on the map defining the office area.



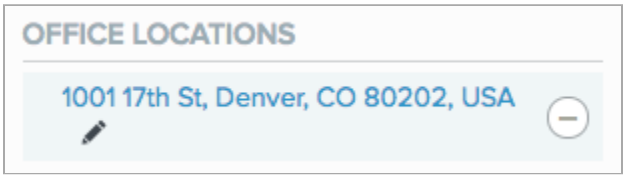
2. Use the white dots on the circle to fine-tune the geofence:



- To reposition the circle, click and drag the white dot at the circle's center to the desired location.
- To resize the circle, click and drag any white dot on the circle's rim.

1. To add another office location, click a location outside the circle. A new circle is added.
2. To edit an office location, click the **Pencil** icon ( ) and edit the name.

   By default, the location is named after its street address.

3. To delete an office address, click the **Minus** icon ( ).

> **Note**
>
> If you edit or delete offices in the **Office Locations** list, changes are applied to all rules that specify office locations.

7. To save the rule and apply it to the relevant policy, click **Save**.
8. To rearrange and save the new policy order, in the policy list, click and drag the new policy and place it in the order in which you want it to be considered. Click **Save Order**.

Next steps

To ensure the policy is applied to your organization, go to **PingID → Configuration** and ensure **Enforce Policy** is set to **Enabled**.

Configuring an access from specific countries rule (web policy)

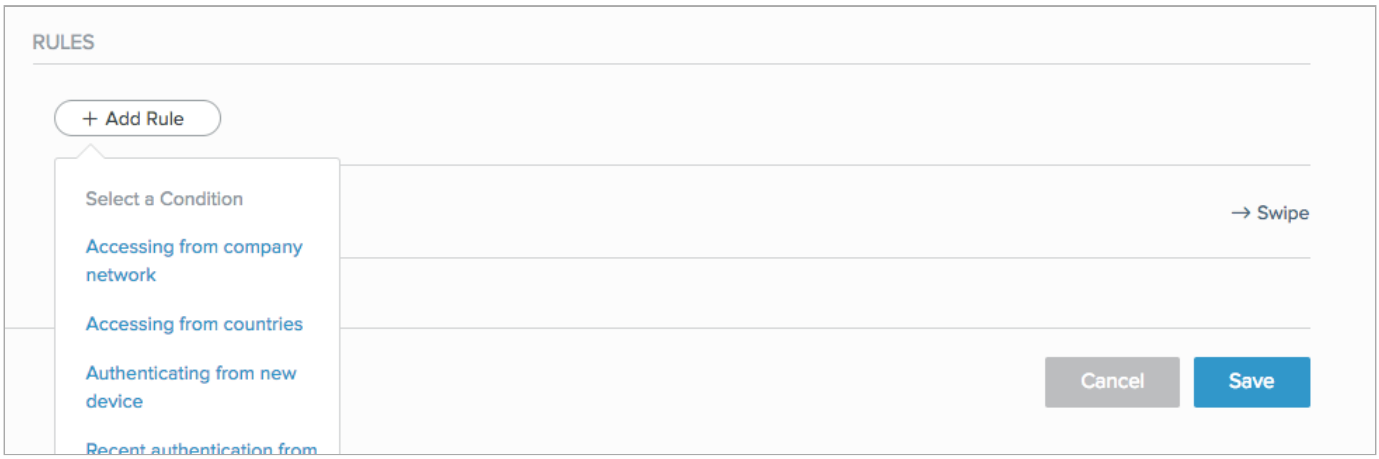
Define which authentication action to prompt the user with on the machine used for web access, according to country.

About this task

> **Note**
>
> The country is determined by the IP address of the accessing device and not by the authenticating device.

Steps

1. From within the relevant policy, click**+ Add Rule** and from the list, select **Accessing From Countries**.



Result:

The **Accessing From Countries** rule wizard opens.

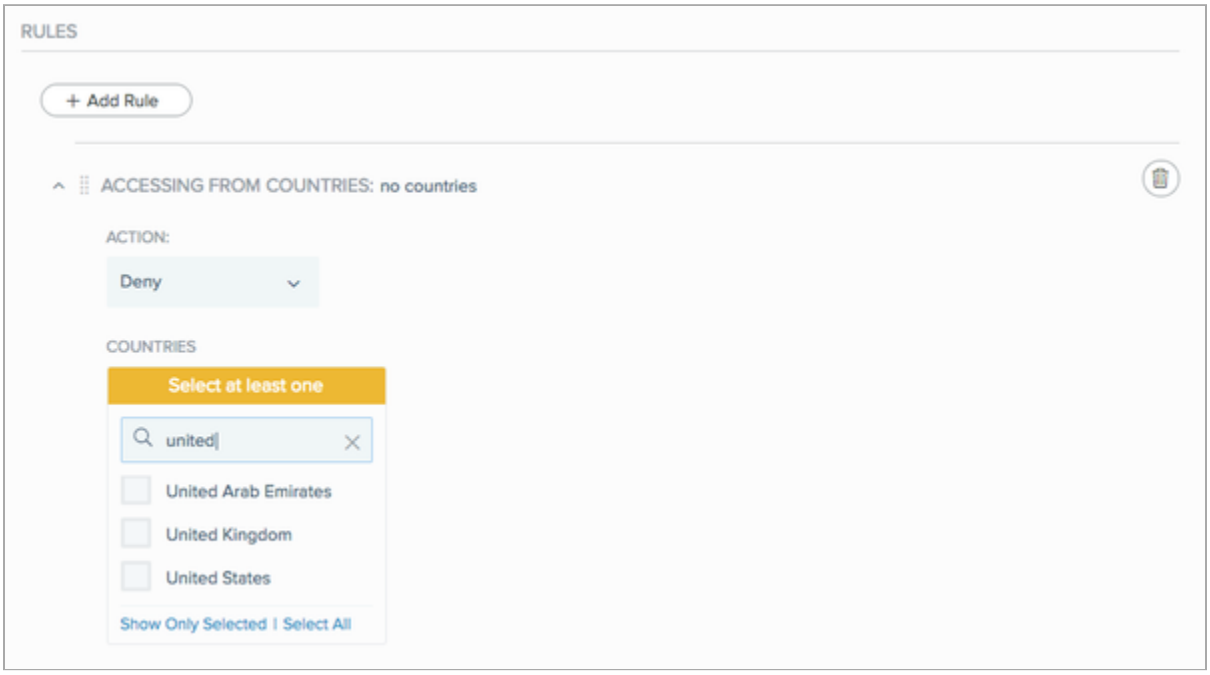
2. From the **Action** list, select the action to use when signing on in the selected countries.

Choose from:

- **Deny** (default): Deny access for authentication requests originating from the selected countries.
- **Authenticate**: Allow the user to authenticate using any of the authentication methods allowed at the policy level.

- **Allowed Methods**: Click **Allowed Methods** to reveal a list of authentication methods allowed by this policy, and then select the check box of each authentication method that you want to allow for this rule. See Rule authentication actions for description per authentication type.

3. From the **Countries** list, select the check box next to each country that you want to include in the rule.



Action	Description
Search by name	In the **Search** box, enter a string or part of a string to search for a specific country. **Note** The list of countries is filtered to display only countries containing the string.
View only the selected countries	Click **Show Only Selected**.
Select all countries in the list	Click **Select All**.
Clear all selections	Click **Unselect All**.

4. Click **Save**.

5. If you have more than one policy listed, in the **Policy** list, click and drag the new policy and place it in the order in which you want it to be considered. Click **Save Order**.

Next steps

To ensure the policy is applied to your organization, go to **PingID → Configuration** and ensure **Enforce Policy** is set to **Enabled**.

Configuring an authenticating from new device rule (web policy)

Define which authentication action to prompt the user with when a user signs on through the web and attempts to authenticate with a new device for the first time.

Steps

1. From within the relevant policy, click **+ Add Rule** and select **Authenticating From New Device**.

   Result:

   The **Authenticating From New Device** rule is added to the policy.

2. From the **Action** list, select the action to use when authenticating with a device for the first time.

   Choose from:

   - **Authenticate**: Allow the user to authenticate using any of the authentication methods allowed at the policy level.
   - **Allowed Methods**: Click **Allowed Methods** to reveal a list of authentication methods allowed by this policy, and then select the check box of each authentication method that you want to allow for this rule. See Rule authentication actions for description per authentication type.

3. Click **Save**.
4. In the **Policy** list, click and drag the new policy and place it in the order in which you want it to be considered. Click **Save Order**.

Next steps

To ensure the policy is applied to your organization, go to **PingID → Configuration** and ensure **Enforce Policy** is set to **Enabled**.

Configuring a recent authentication from office access rule (web policy)

Use this rule to waive PingID authentication if the last successful authentication request occurred in the office and within a given time period, such as within the last 30 minutes.

About this task

This rule defines which authentication action to prompt the user with if the previous authentication request:

- Occurred within the defined period of time.
- Originates from the same accessing device that was used for the previous authentication request.

- Used an authentication method that is one of the allowed authentication methods included in this policy.
- The authenticating device's mobile location is the office.

If the previous request was made at an office location, you might want to define less strict authentication requirements. For example, a user signed on from a specific office within the last 30 minutes using their mobile device.

Note

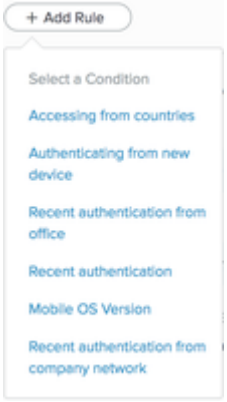
- If you are using PingOne DaVinci to orchestrate your PingID flows, this rule is not evaluated.
- Location services must be enabled on a user's devices for a location based policy to be applied to that device. For users with Android Q and later, the **Allow All The Time** option check box must be selected.

Note

To use this rule at least one of the mobile app authentication method must be selected in the **Allowed Authentication Method** section, such as **Swipe**, **Mobile App Biometrics**, or **One-time passcode**. If this rule does not appear in the **+ Add Rule** list, ensure at least one of these authentication methods check boxes is selected.

Steps

1. From within the relevant policy, click**+ Add Rule** and select **Recent authentication from office**.

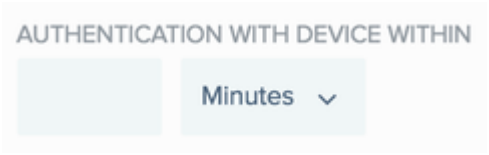


2. From the **Action** list, select which action to use if the previous authentication request was at an office location and within the time specified.

   Choose from:

   - **Deny** (default): Deny access for authentication requests originating from the selected countries.
   - **Approve**: Approve access without requiring PingID authentication.
   - **Authenticate**: Allow the user to authenticate using any of the authentication methods allowed at the policy level.
   - **Allowed Methods**: Click **Allowed Methods** to reveal a list of authentication methods allowed by this policy, and then select the check box of each authentication method that you want to allow for this rule. See Rule authentication actions for description per authentication type.

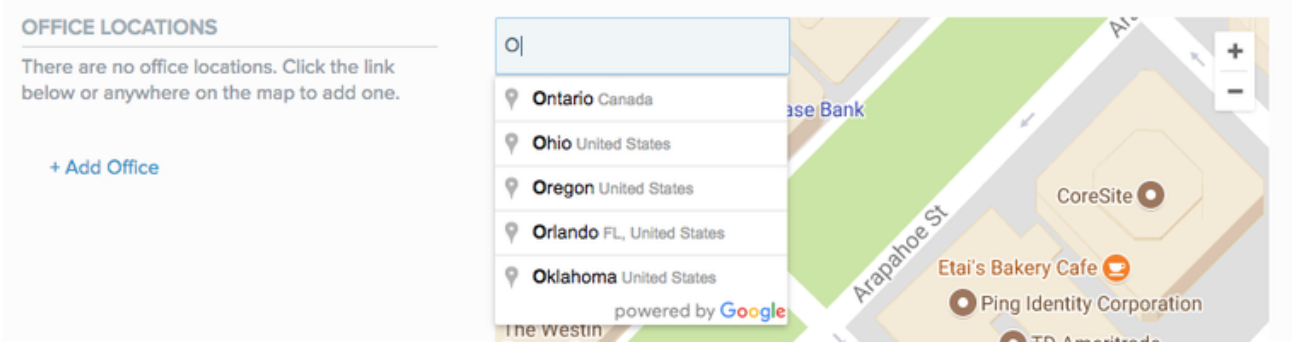
3. To define the time period that applies to the **Action** setting, from the **Authentication With Device Within** list, select the unit of time in **Minutes**, **Hours**, **Days**, or **Weeks**, and then enter the numerical value in the text box.



4. To define additional office locations:

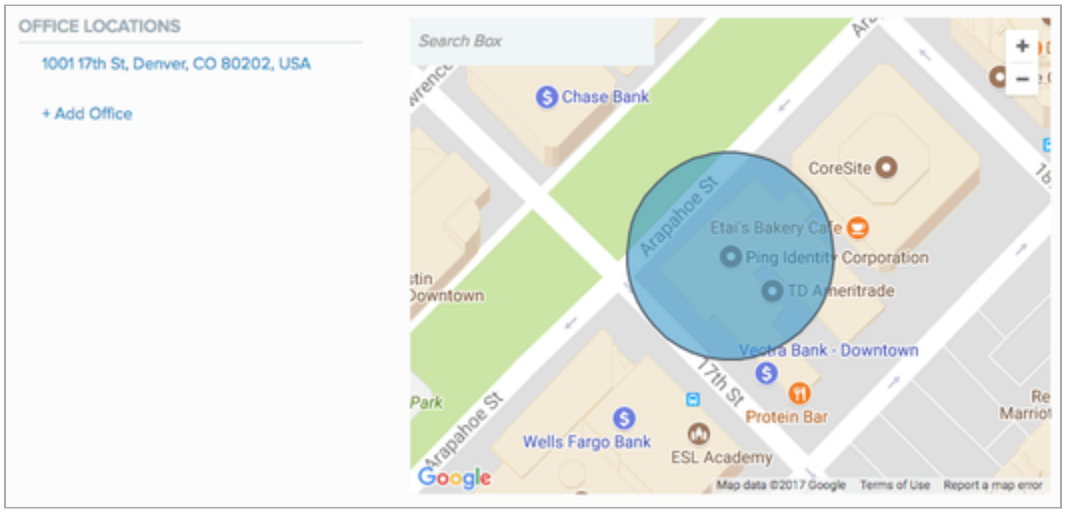
   The **Office Locations** wizard displays a list of the office locations currently defined. If the authenticating device is located within one of the defined areas, it is considered to be inside a company office.

   1. Click **+ Add office** or enter an address in the search box.

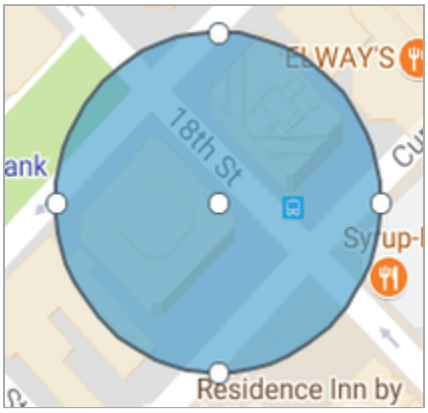


   Result:

   A blue circle appears on the map, defining the office area.



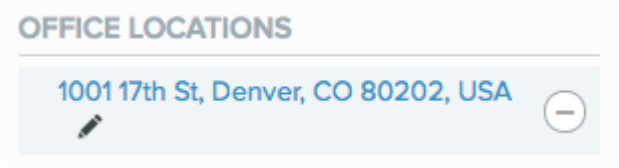
   2. Use the white dots on the circle to fine-tune the geofence:



- To reposition the circle, click and drag the white dot at the circle's center to the desired location.
- To resize the circle, click and drag any white dot on the circle's rim.

1. To add another office location, click a location outside the blue circle. A new circle is added.
2. To edit an office location, click the **Pencil** icon ( ) and edit the name.

   By default, the location is named after its street address.

3. To delete an office address, click the **Minus** icon ( ).

   > **Note**
   >
   > If you edit or delete offices in the **Office Locations** list, changes are applied to all rules that specify office locations.

5. Click **Save**.
6. In the **Policy** list, click and drag the new policy and place it in the order in which you want it to be considered. Click **Save Order**.

Next steps

To ensure the policy is applied to your organization, go to **PingID → Configuration** and ensure **Enforce Policy** is set to **Enabled**.

Configuring a recent authentication access rule (web policy)

Use this rule to waive PingID authentication if the last successful authentication request occurred within a given time period, such as within the last 30 minutes.

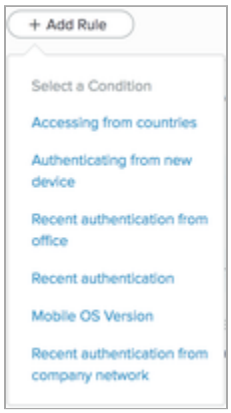
About this task

This rule defines which authentication action to prompt the user with if the previous authentication request:

- Occurs within the defined time period.
- Originates from the same accessing device that was used for the previous authentication request.
- Uses an authentication method that is one of the allowed authentication methods included in this policy.

Steps

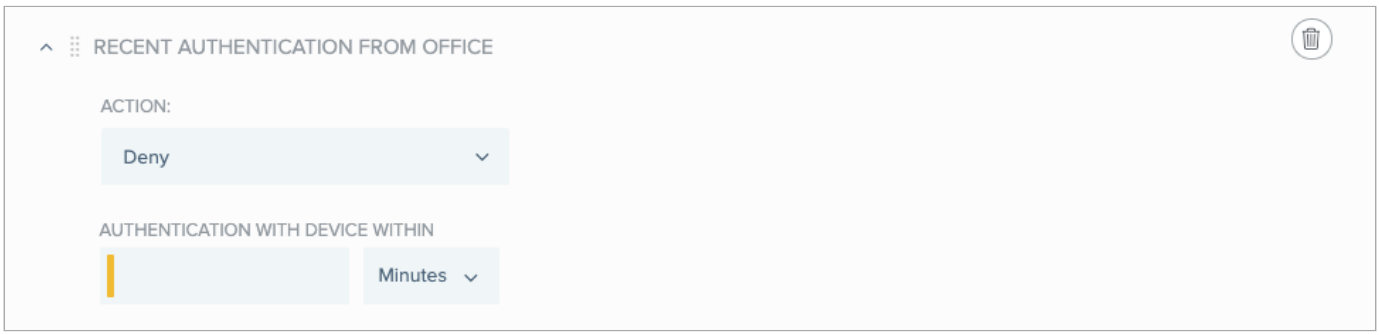
1. From within the relevant policy, click**+ Add Rule**, and select **Recent authentication**.



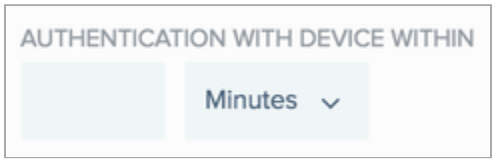
2. From the **Action** list, select the action to use if the previous authentication request was within the time specified.

   Choose from:

   - **Deny** (default): Deny access for authentication requests originating from the selected countries.
   - **Approve**: Approve access without requiring PingID authentication.
   - **Authenticate**: Allow the user to authenticate using any of the authentication methods allowed at the policy level.
   - **Allowed Methods**: Click **Allowed Methods** to reveal a list of authentication methods allowed by this policy, and then select the check box of each authentication method that you want to allow for this rule. See Rule authentication actions for description per authentication type.



3. To define the time period that applies to the **Action** setting, from the **Authentication With Device Within** list, select the unit of time in **Minutes**, **Hours**, **Days**, or **Weeks**, and then enter the numerical value in the text box.



4. Click **Save**.
5. In the **Policy** list, click and drag the new policy and place it in the order in which you want it to be considered. Click **Save Order**.

Next steps

To ensure the policy is applied to your organization, go to **PingID → Configuration** and ensure **Enforce Policy** is set to **Enabled**.

Configuring a mobile OS version access rule (web policy)

Use this rule to define which authentication action to prompt the user with for the defined mobile OS versions.

About this task

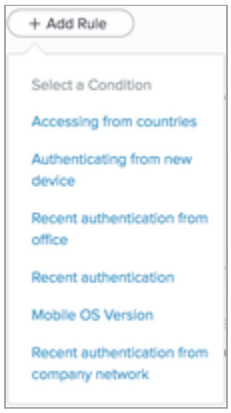
You might want to define stricter authentication requirements for older, more vulnerable OS versions.

> **Note**
>
> To use this rule, at least one mobile app authentication method must be selected in the **Allowed Authentication Method** section, such as **Swipe**, **Mobile App Biometrics**, or **One-time passcode**. If this rule does not appear in the **+ Add Rule** list, ensure at least one of these authentication methods is selected.

> **Note**
>
> If you are using PingOne DaVinci to orchestrate your PingID flows, this rule is not evaluated.

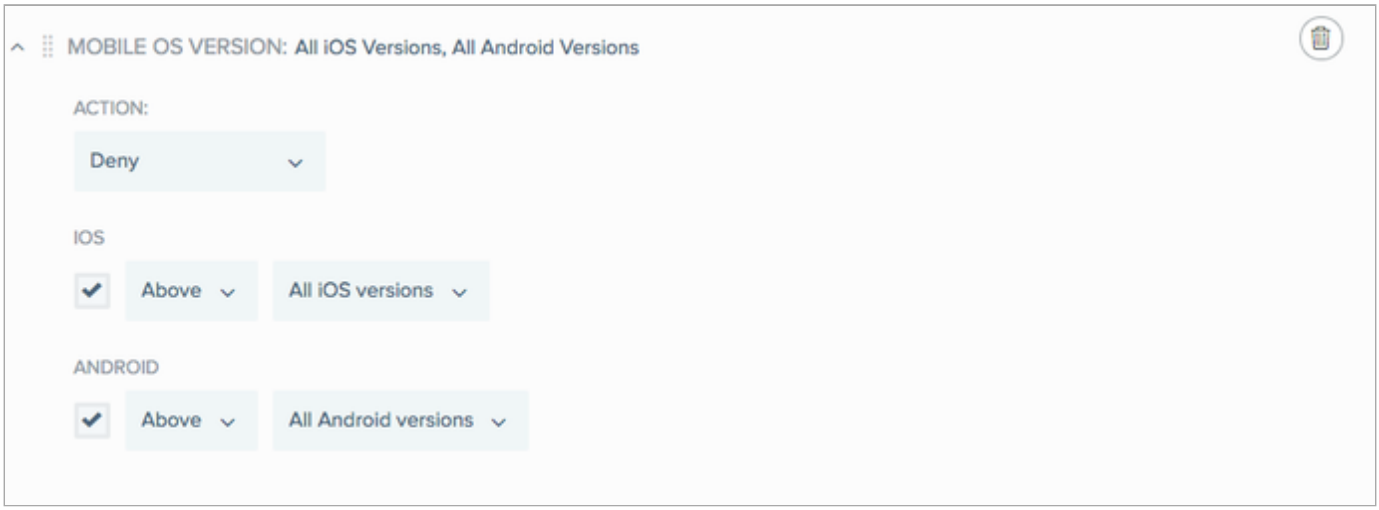
Steps

1. From within the relevant policy, click**+ Add Rule** and from the list, select **Mobile OS Version**.



Result:

The **Mobile OS Version** rule wizard opens.



2. From the **Action** list, select which authentication action to use for OS versions meeting the defined criteria.

   Choose from:

   - **Deny** (default): Deny access for authentication requests originating from the selected countries.
   - **Approve**: Approve access without requiring PingID authentication.
   - **Authenticate**: Allow the user to authenticate using any of the authentication methods allowed at the policy level.
   - **Allowed Methods**: Click **Allowed Methods** to reveal a list of authentication methods allowed by this policy, and then select the check box of each authentication method that you want to allow for this rule. See Rule authentication actions for description per authentication type.

3. To define the minimum or maximum permitted mobile operating system versions and associated action:

   1. Select the check boxes next to the OS that you want to include in the rule: iOS, Android, or both.
   2. For each OS that you want to include, select either:
      - **Above**, and then select the minimum permitted operating system version from the list.
      - **Below**, and then select the minimum permitted operating system version from the list.

4. Click **Save**.

5. In the **Policy** list, click and drag the new policy and place it in the order in which you want it to be considered, and then click **Save Order**.

Next steps

To ensure the policy is applied to your organization, go to **PingID → Configuration** and ensure **Enforce Policy** is set to **Enabled**.

Configuring a recent authentication from company network rule

Use this rule to waive PingID authentication if the last successful authentication request occurred within a specific IP range in the company network and within a given time period, such as within the last 30 minutes.

About this task

This rule defines which authentication action to prompt the user with if the previous authentication request:

- Occurs within the defined period of time.
- Originates from the same accessing device that was used for the previous authentication request.
- Uses an authentication method that is one of the allowed authentication methods included in this policy.
- The authenticating device's mobile location is within the specified IP range in the company network.
- Optional: You can require the user's mobile authenticating device to be located within a defined office location during authentication. See the **Authenticating Device In Company Offices** rule.

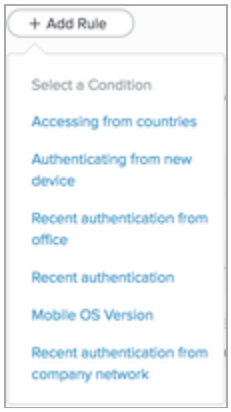
> **Note**
>
> If this option is enabled, to sign on:
> - The user's authenticating device must be in a company office location.
> - The user's accessing device should originate from an IP address within the company network.

When creating this rule, you must specify the IP addresses that define the company network and optionally define the geographic location of one or more offices around the world.

> **Note**
>
> - If you are using PingOne DaVinci to orchestrate your PingID flows, location-based policy rules are not evaluated.
> - Location services must be enabled on a user's devices in order for a location based policy to be applied to that device. For users with Android Q and later, the **Allow all the time** option must be selected.

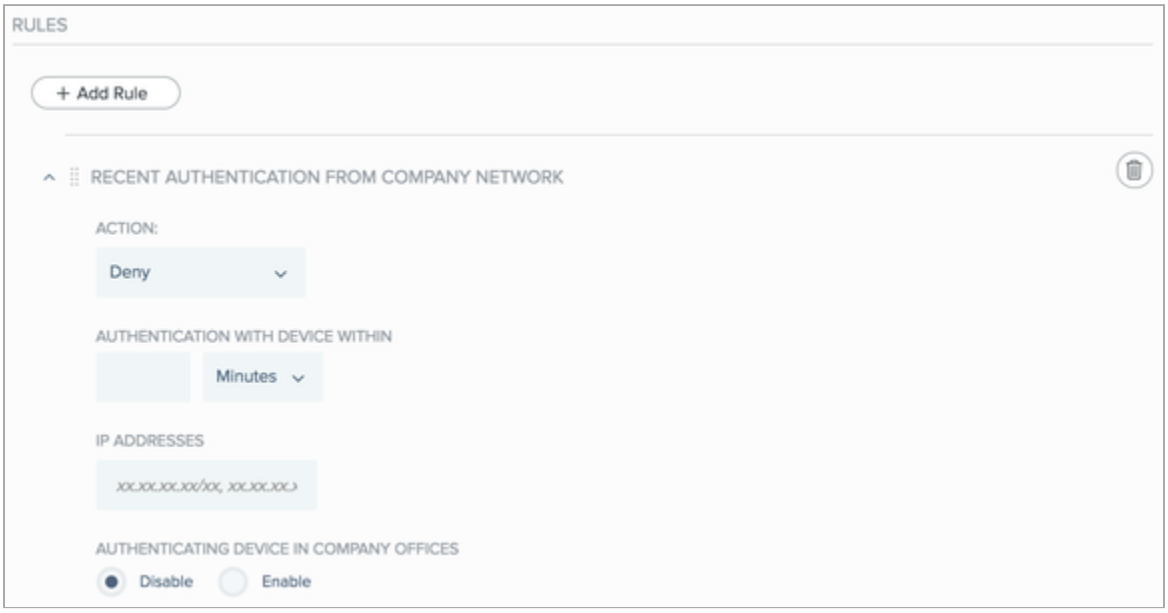
Steps

1. From within the relevant policy, click **+ Add Rule**, and from the list, select **Recent authentication from company network**.



Result:

The **Recent Authentication From Company Network** rule wizard opens.

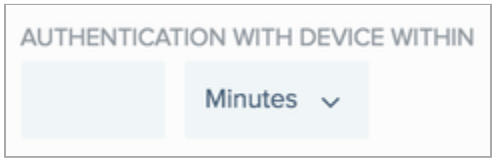


2. From the **Action** list, select the action that you want to apply when authenticating, if the rule conditions are met.

   Choose from:

   - **Deny** (default): Deny access for authentication requests originating from the selected countries.
   - **Approve**: Approve access without requiring PingID authentication.
   - **Authenticate**: Allow the user to authenticate using any of the authentication methods allowed at the policy level.
   - **Allowed Methods**: Click **Allowed Methods** to reveal a list of authentication methods allowed by this policy, and then select the check box of each authentication method that you want to allow for this rule. See Rule authentication actions for description per authentication type.

3. To define the time period that applies to the **Action** setting, from the **Authentication With Device Within** list, select the unit of time in **Minutes**, **Hours**, **Days**, or **Weeks**, and then enter the numerical value in the text box.



4. In the **IP Addresses** field, enter a list of external IP addresses or the IP range that belongs to the company network.

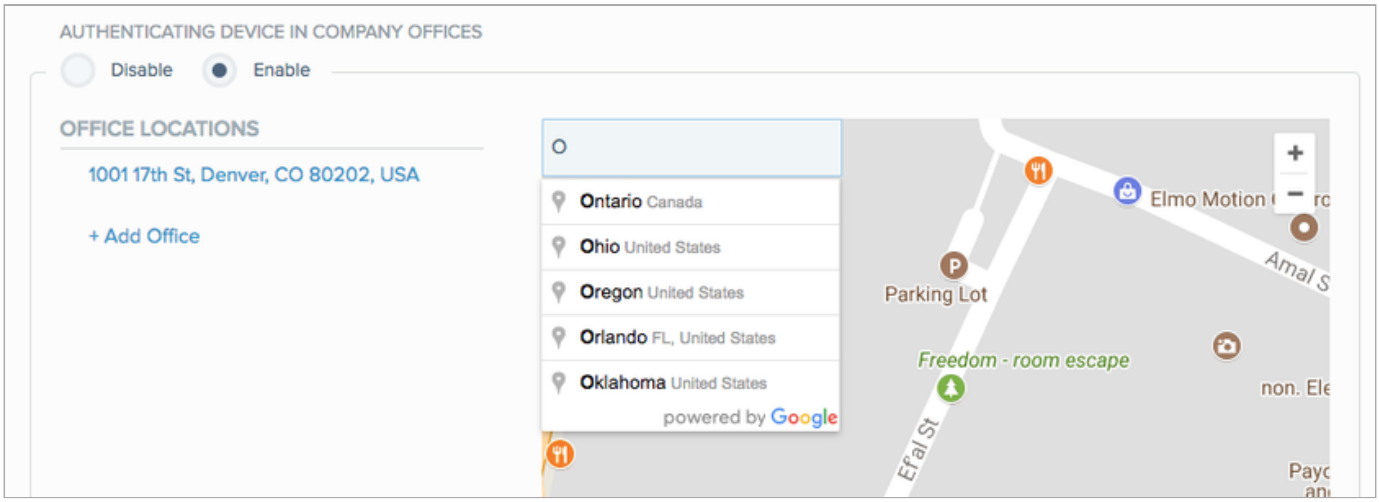
> **Note**
>
> Enter the IP addresses and ranges using CIDR notation with each entry on its own line.

5. To require a user's authenticating device to be in the company offices when signing on from within the company network, in the **Authenticating Device In Company Offices** section, click **Enable**.

> **Note**
>
> If you are defining a company office, in addition to an IP address, a mobile authentication method of **Swipe**, **Mobile App Biometrics**, or **One-time passcode** must be defined as an **Allowed Authentication Method** to apply this rule.

Result:

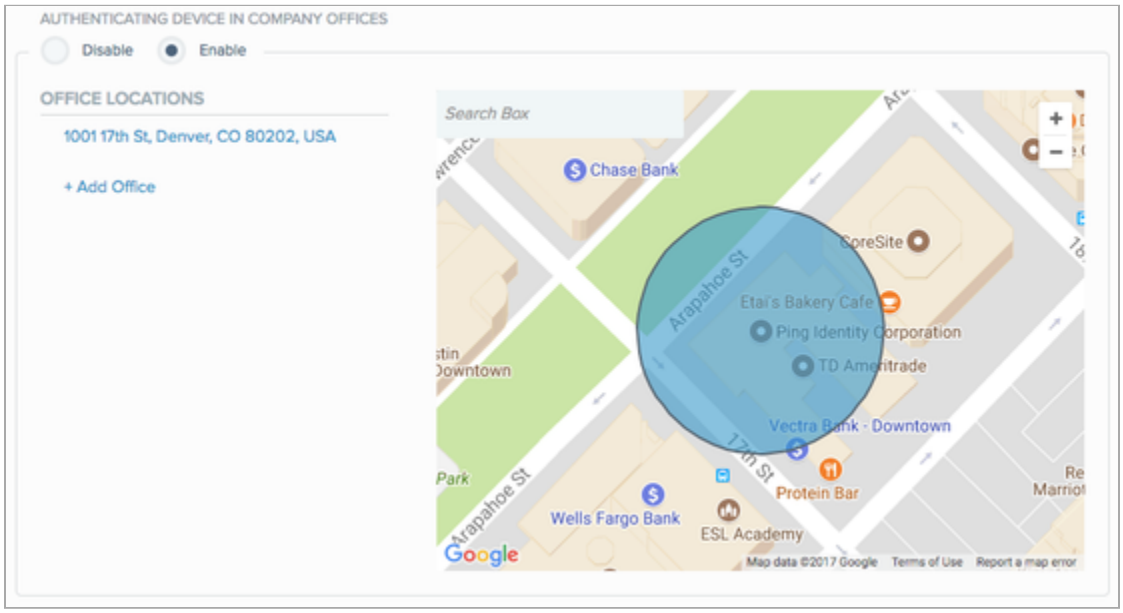
The **Office Locations** wizard opens, displaying a list of the office locations currently defined. If the authenticating device is located within one of the defined areas, it is considered to be inside a company office. Define one or more company office locations.



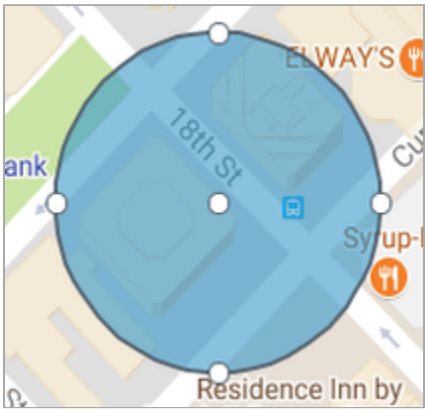
6. To define one or more office locations:

    1. Click **+ Add office** or enter an address in the search box.

        A blue circle appears on the map, defining the office area.



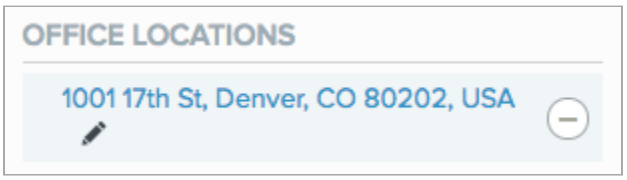
    2. Use the white dots on the circle to fine-tune the geofence:



- To reposition the circle, click and drag the white dot at the blue circle's center to the desired location.
- To resize the circle, click and drag any white dot on the circle's rim.

1. To add another office location, click a location outside the blue circle and a new circle is added.
2. To edit an office location, click the **Pencil** icon ( ) and edit the name.

   By default, the location is named after its street address.

3. To delete an office address, click the **Minus** icon ( ).

> **Note**
>
> If you edit or delete offices in the **Office Locations** list, changes are applied to all rules that specify office locations.

7. To save the rule and apply it to the relevant policy, click **Save**.
8. In the **Policy** list, click and drag the new policy and place it in the order in which you want it to be considered. Click **Save Order**.

Next steps

To ensure the policy is applied to your organization, go to **PingID → Configuration** and ensure **Enforce Policy** is set to **Enabled**.

Configuring an IP reputation rule (web policy)

Use this rule to determine which authentication action to prompt the user with, based on the risk score of the IP address of the user's accessing device.

About this task

PingID collects and analyzes IP address data from the user's accessing device and enables you to apply different authentication actions to IP addresses according to their risk scores. IP addresses are grouped into the following levels of risk:

- High: The IP address is considered high risk and might have recently been involved in numerous malicious activities, such as DDos attacks or spam activity.
- Medium: The IP address is considered medium risk and might have been involved in malicious activities, such as DDos attacks or spam activity.
- Low: The IP address is considered low risk.

You can define a different authentication for each risk group. Define more restrictive authentication for IP addresses in a higher risk group You can also define a whitelist of IP addresses that you want this rule to ignore.

{{{ Video removed }}}

> **Note**
>
> The IP reputation rule is not applied if there is insufficient data to determine the IP address' risk score.

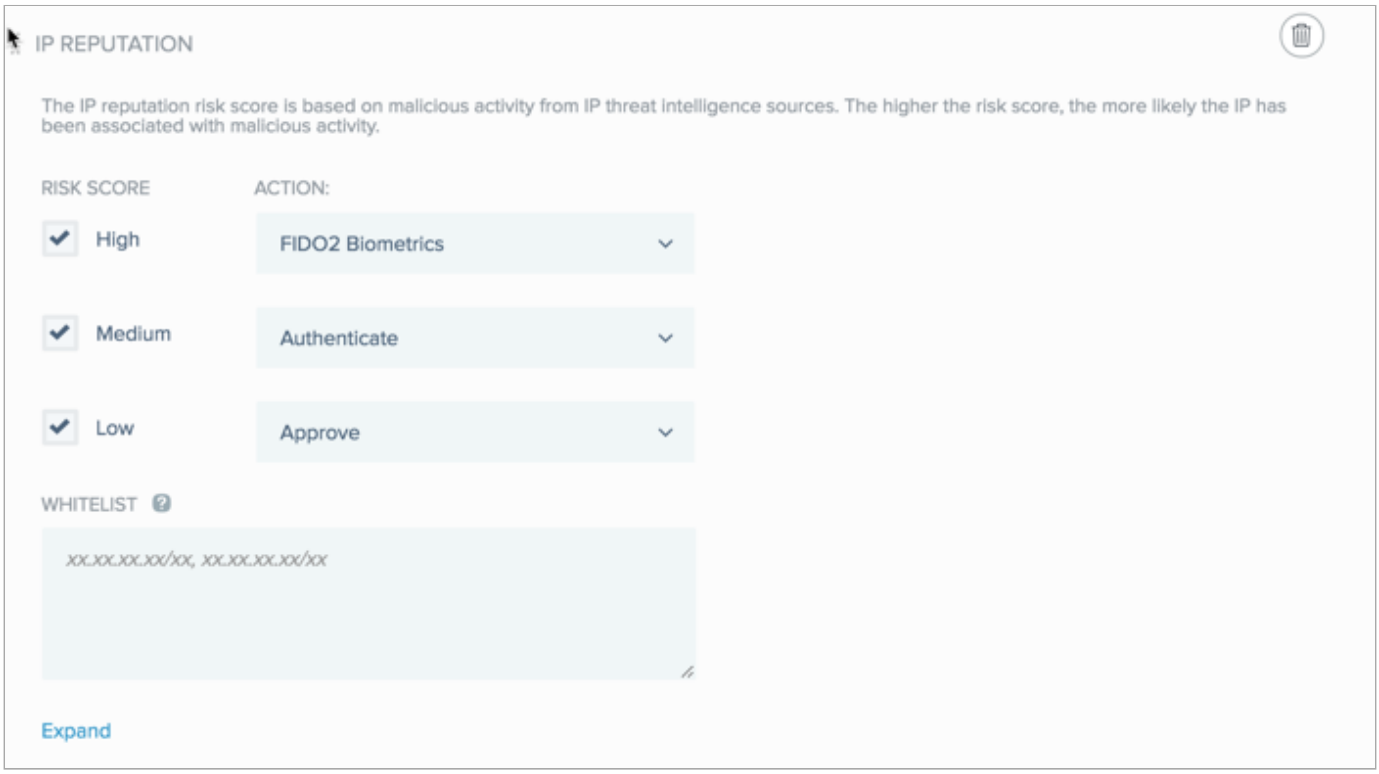
Steps

1. From within the relevant policy, click **+ Add Rule** and from the list, select **IP Reputation**.

   Result:

   The **IP Reputation** rule wizard opens.

2. Select the check box of each **Risk Score** group to which you want to apply a rule action, and from the **Action** list, select the action that you want to apply to that risk score group.



Choose from:

- **Deny**: Deny access for authentication requests originating from IP addresses in the selected risk score category. This option is selected for the High risk category, by default.
- **Approve**: Approve access without requiring PingID authentication for authentication requests originating from IP addresses in the selected risk score category.
- **Authenticate**: Allow the user to authenticate using any of the authentication methods allowed at the policy level.
- **Allowed Methods**: Click **Allowed Methods** to reveal a list of authentication methods allowed by this policy, and then select the check box of each authentication method that you want to allow for this rule. See Rule authentication actions for description per authentication type.

3. In the **Whitelist** field, specify one or more IP address ranges that you want the rule to ignore.

> **Note**
>
> Enter each IP address range in the format `XX.XX.XX.XX/XX` and separate each IP address range with a comma.

4. Click **Save**.
5. In the **Policy** list, click and drag the new policy and place it in the order in which you want it to be considered. Click **Save Order**.

Next steps

To ensure the policy is applied to your organization, go to **PingID → Configuration** and ensure **Enforce Policy** is set to **Enabled**.

Configuring a geovelocity anomaly rule (web policy)

PingID analyzes location data and allows you to specify an authentication rule when the travel time between a user's current sign on location and their previous sign on location is not possible in the time frame that has elapsed since the previous sign on. The location and resulting reputation classification are based on the user's accessing device.

About this task

{{{ Video removed }}}

For example, if a user signs on from New York, USA at 12:00 p.m. and then attempts to sign on from London, UK two hours later, a geovelocity anomaly is detected and a rule action, such as **Deny**, is applied.

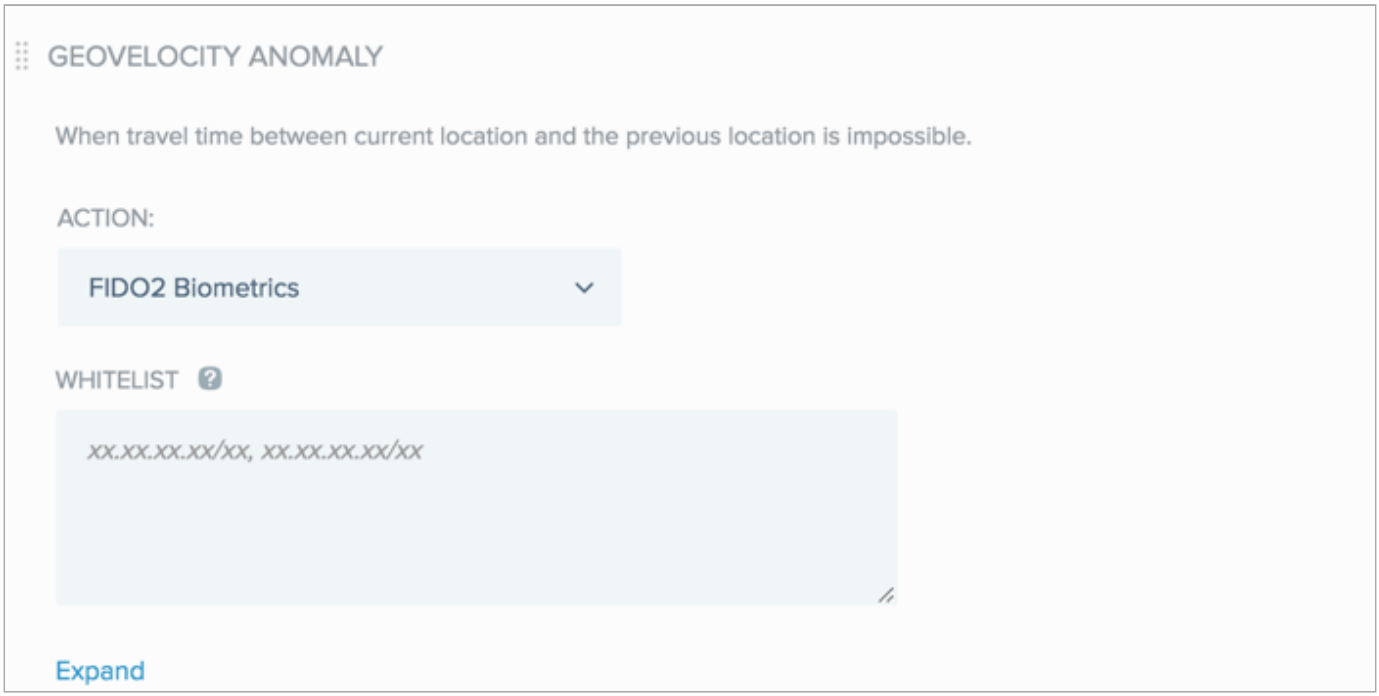
You can create a whitelist of IP addresses that you want this rule to ignore.

Steps

1. From within the relevant policy, click**+ Add Rule** and from the list, select **Geovelocity Anomaly**.

   Result:

   The **Geovelocity Anomaly** rule wizard opens.



2. From the **Action** list, select the authentication action that you want to apply in the event of a geovelocity anomaly.

   Choose from:

   - **Deny** (default): Deny access.
   - **Authenticate**: Allow the user to authenticate using any of the authentication methods allowed at the policy level.
   - **Allowed Methods**: Click **Allowed Methods** to reveal a list of authentication methods allowed by this policy, and then select the check box of each authentication method that you want to allow for this rule. See Rule authentication actions for description per authentication type.

3. in the **Whitelist** field, specify one or more IP address ranges that you want the rule to ignore.

   > **Note**
   >
   > Enter each IP address range in the format `XX.XX.XX.XX/XX`. Separate each IP address range with a comma.

4. Click **Save**.

5. In the **Policy** list, click and drag the new policy and place it in the order in which you want it to be considered. Click **Save Order**.

Next steps

To ensure the policy is applied to your organization, go to **PingID → Configuration** and ensure **Enforce Policy** is set to **Enabled**.

Configuring a risk level rule (web policy)

The PingOne Protect service combines a number of predictors such as user risk behavior, IP reputation, and geovelocity anomaly to calculate a single risk score. If you have a license for PingOne Protect, you can include the risk level that it calculates in your PingID policies. For more information on PingOne Protect, see Introduction to PingOne Protect.

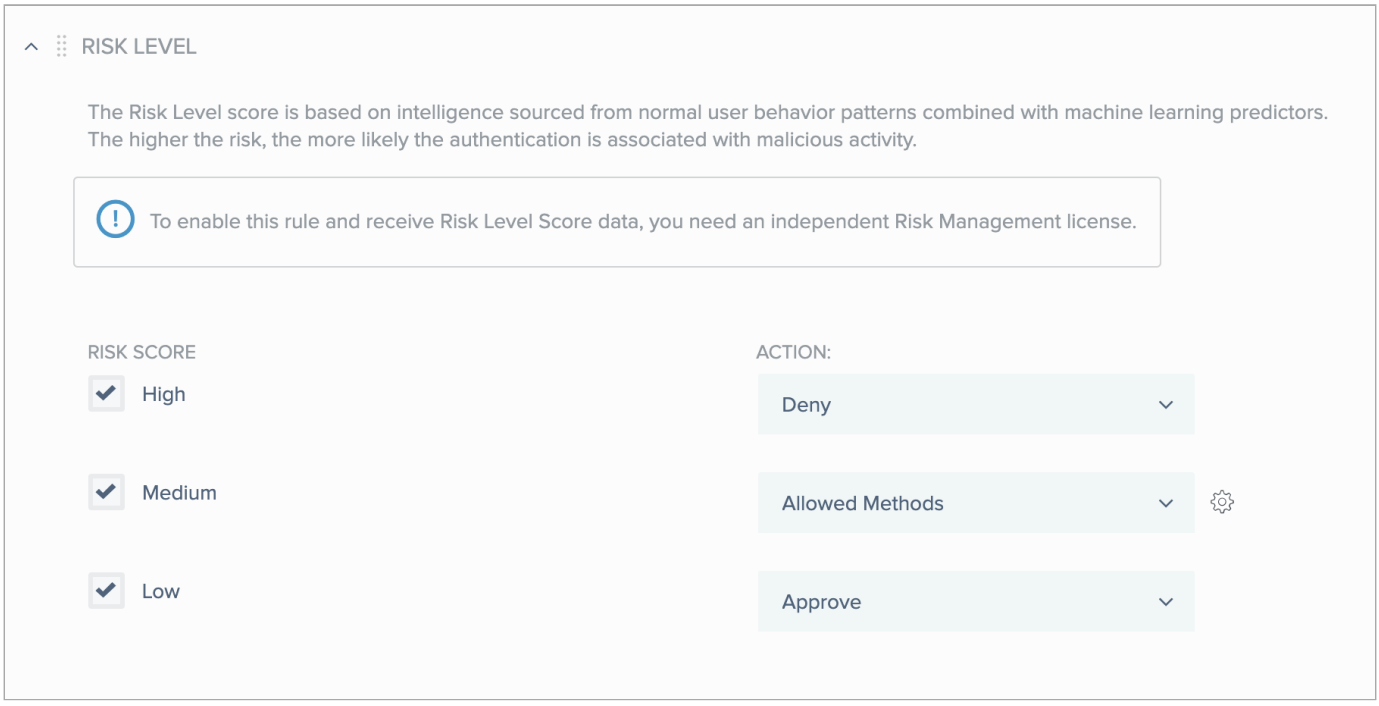
Before you begin

Before adding a risk level rule, make sure that you have provided a value for the **Resource ID** field in the definition of the PingID adapter for PingFederate. For more information, see Configuring a PingID Adapter instance. Version 2.11 or higher of the PingID adapter is required for this feature

> **Note**
>
> You can also add a rule that uses the risk level provided by a supported third-party risk service. If you are using a third-party service, make sure that you have provided a value for the **Risk Level** field in the definition of the PingID adapter for PingFederate.

Steps

1. Create a new policy, or open an existing policy for editing.
2. Click **Add Rule**.
3. Select **Risk Level** from the list of rules.
4. For each of the risk levels - high, medium, low - select the check box if you want to specify an MFA action for that level of risk.



5. For each risk level that you selected, use the list of actions to select the MFA action you want to use for that level of risk.

6. Click **Save**.
7. In the **Policy** list, click and drag the new policy and place it in the order in which you want it to be considered. Click **Save Order**.

Configuring a limit push notifications rule

Use this rule to reduce the likelihood of a user acknowledging a malicious push notification as part of an MFA fatigue attack by limiting the number of push notifications the user can deny or ignore within a 24-hour period.

About this task

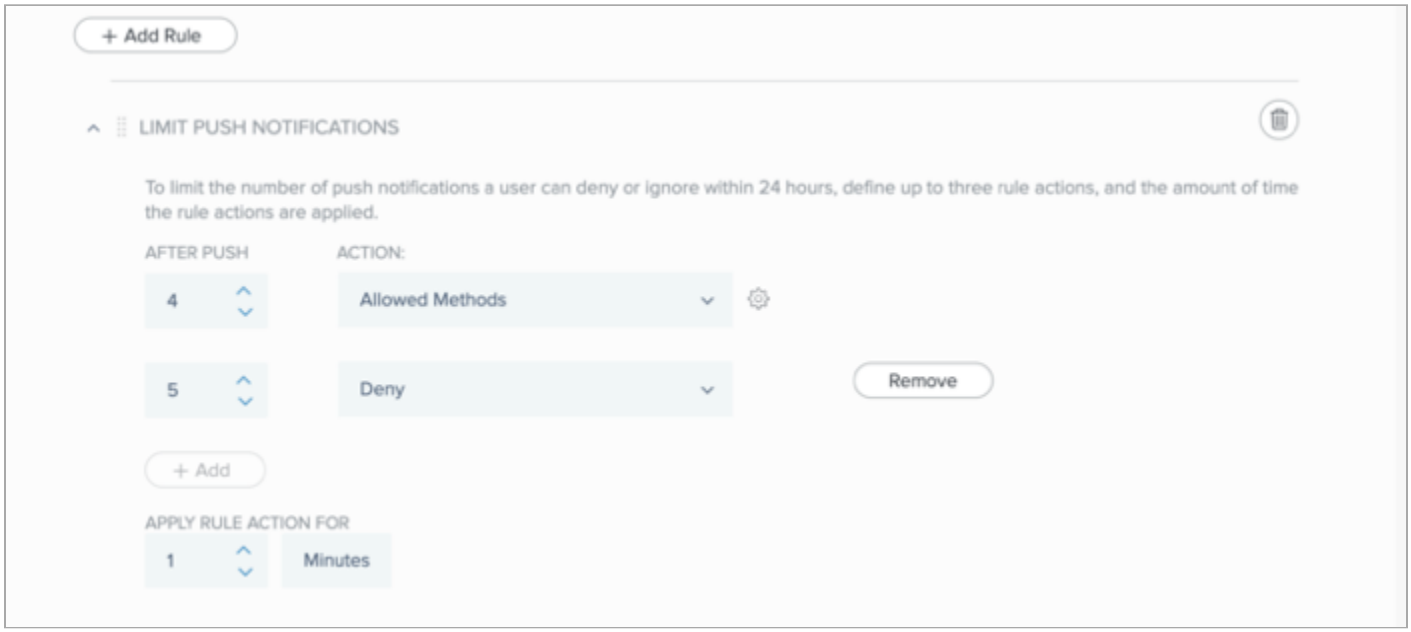
Specify an action from the list of allowed methods that are available, or choose to deny the user access. Then specify the time period for which the rule actions should be applied.

You can define an array of up to three push notification limits (subrules), and specify up to three actions that are triggered sequentially as the user reaches each limit. A rule defines the number of push notifications (ignored or denied) that must occur consecutively within a 24-hour period in order to trigger the rule action.

Each time the user authenticates successfully, the counter is reset.

For example, when applying the rule for 20 minutes:

- After 5 push notifications, the user must authenticate with a security key for a period of 20 mins.
- After 10 push notifications, the user must authenticate using biometrics, or number matching for a period of 20 mins.
- After 15 push notifications, the user is denied access for a period of 20 mins.



> **Note**
>
> - By default, only one limit is shown, however up to three limits can be defined. If you select **Deny** for the first or second limit action, no further actions can be specified.
> - If you are using PingOne DaVinci to orchestrate your PingID flows, this rule is not evaluated.

Steps

1. From within the relevant policy, click **+ Add Rule** and from the list, select **Limit push notifications**.

   Result:

   The **Limit Push Notifications** rule wizard open

2. To define a push notification limit:

   1. In the **After Push** field, select the number of push notifications after which the action is triggered, and then in the **Action** field, select the action that is triggered when the limit is reached. Choose from the following actions:

      - **Deny**: Deny access after the number of push notifications is reached.
      - **Allowed Methods**: Click **Allowed Methods** to reveal a list of authentication methods allowed by this policy, and then select the check box of each authentication method that you want to allow for this rule. See Rule authentication actions for description per authentication type.

   2. To add another push notification limit, click **Add** and repeat substep a.

3. In the **Apply Rule Action For** field, set a duration for the rule actions to be applied after they're triggered.
4. Click **Save**.
5. In the **Policy** list, click and drag the new policy and place it in the order in which you want it to be considered. Click **Save Order**.

Next steps

To ensure the policy is applied to your organization, go to **PingID → Configuration** and ensure **Enforce Policy** is set to **Enabled**.

Editing a web authentication policy

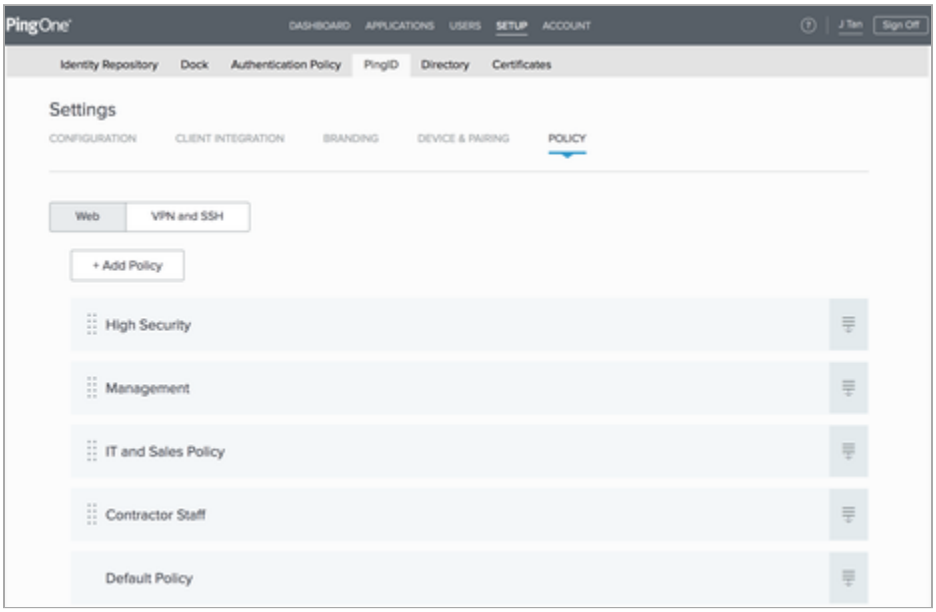
Within the policy, rename the policy, add, edit, or delete a rule, and modify the applications and groups to which the policy applies.

Steps

1. In the admin portal, go to **Setup → PingID → Policy**, and click the **Web** tab.

   Result:

   A list of policies is displayed.

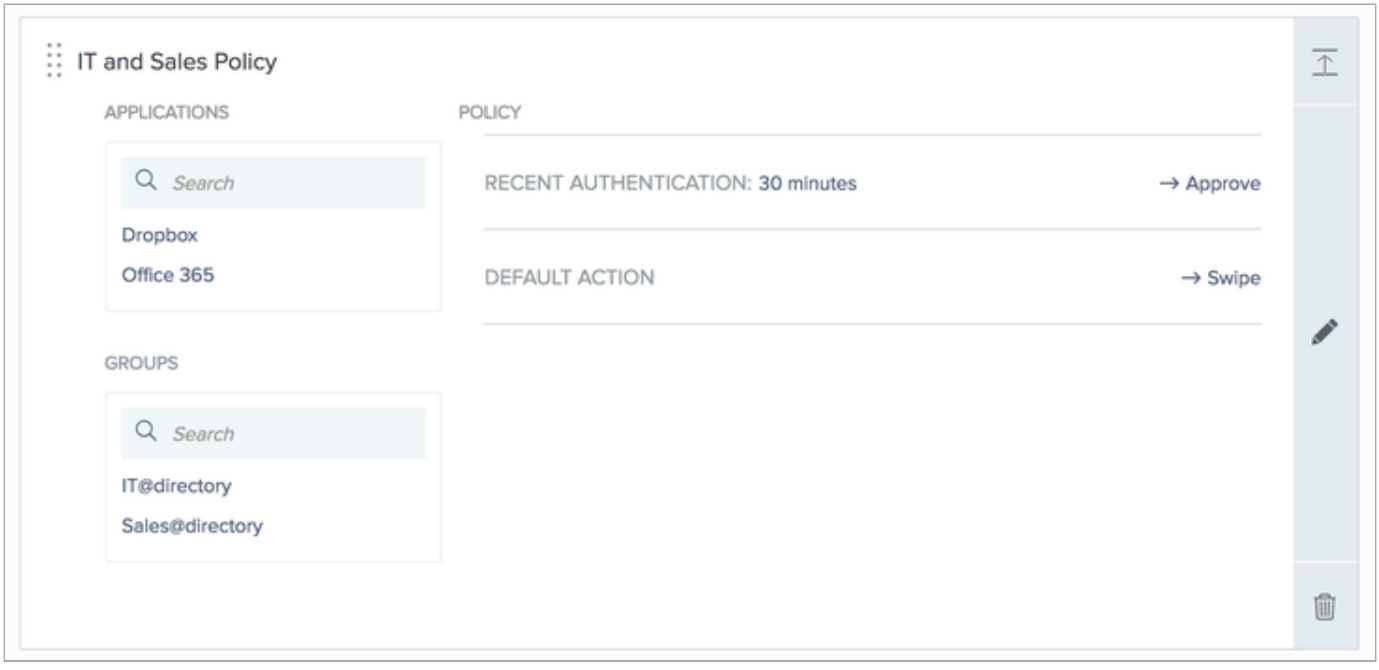


> **Note**
>
> To change the order in which the policy is applied, click and drag the policy entry up or down in the list.

2. Within the relevant policy you want to edit, click the **Expand** icon ( ).

   Result:

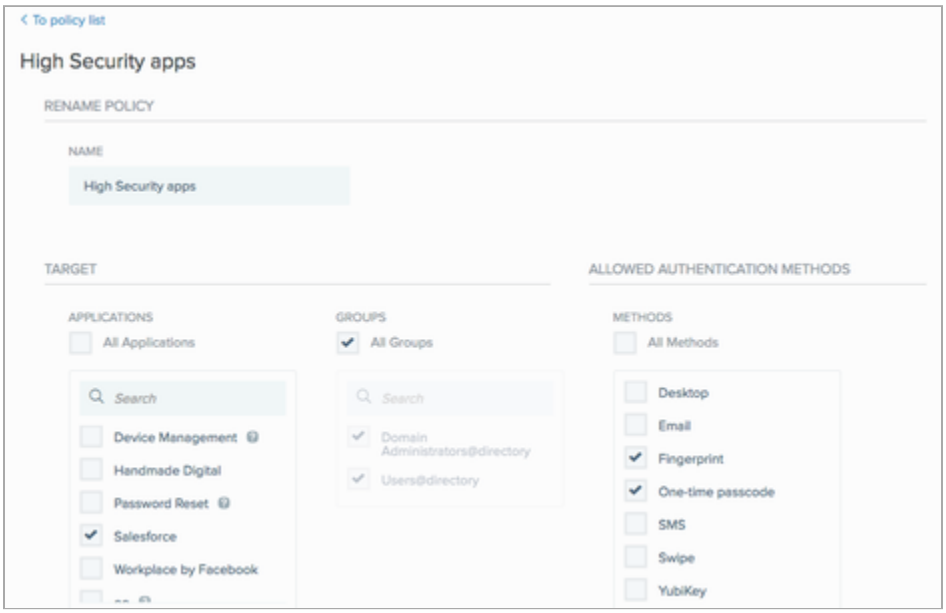
   The policy expands to show a summary of the policy configuration.



3. To edit the policy, click the **Pencil** icon ( ).

   Result:

The policy opens showing the **Applications**, **Groups**, **Rules**, and **Allowed Authentication Methods** to which the policy applies.



4. Edit the policy configuration:

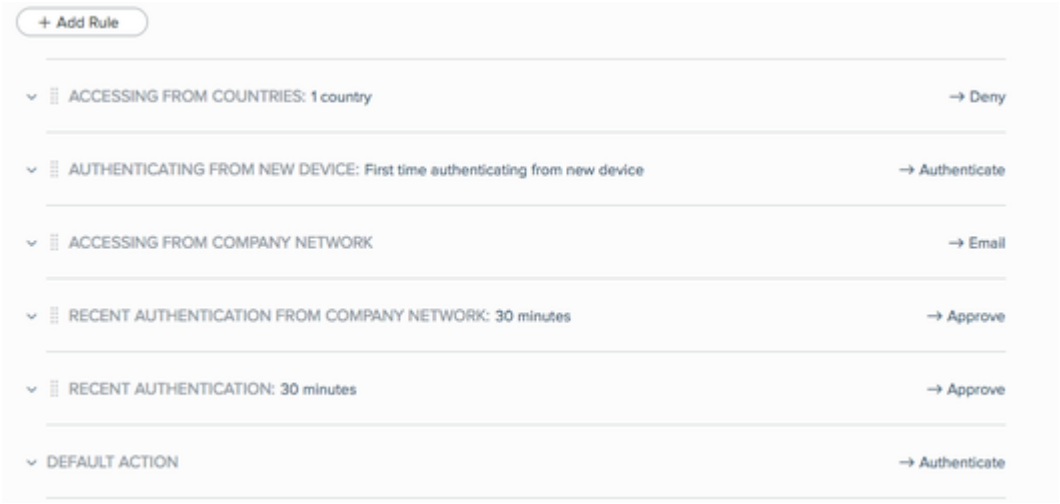
   Choose from:

   - **Name**: Rename the policy as required.
   - **Applications**: Select or clear an application check box to add or remove it from the list or:
   - Select the **All Applications** check box to include all applications currently listed and all applications that are added in the future.
   - Select the **Select All** check box to include all currently listed applications.

     > **Note**
     >
     > With this option, applications added to the list in the future will not be included in the policy.

   - **Groups**: select or clear a group's check box to add or remove it from the list, or select the **All Groups** check box to apply the policy to all groups.
   - **Allowed Authentication Methods**: select or clear an authentication method check box to add or remove it from the list, or select the **All Methods** check box to allow all current and future authentication methods.

5. Edit the policy rules as required:



Editing action	Description
Reorder rules within a policy	Click a rule, drag it to the desired position, and then release the mouse.
Edit existing rules	Click the arrow to the left of the rule you want to edit, and edit the fields that you want to change.
Add a rule	To add a rule, click **+ Add Rule**. Select and configure the relevant rule. **Note** For details of how to configure a specific rule, see the relevant rule as described in Configure an app or group-specific authentication policy.
Delete a rule	Click the rule that you want to delete and within the rule details, click the **Delete** icon ( ).

6. Click **Save**.
7. In the **Policy** list, click and drag the new policy and place it in the order in which you want it to be considered. Click **Save Order**.

Deleting a web authentication policy

Delete a policy from the policy list.

About this task

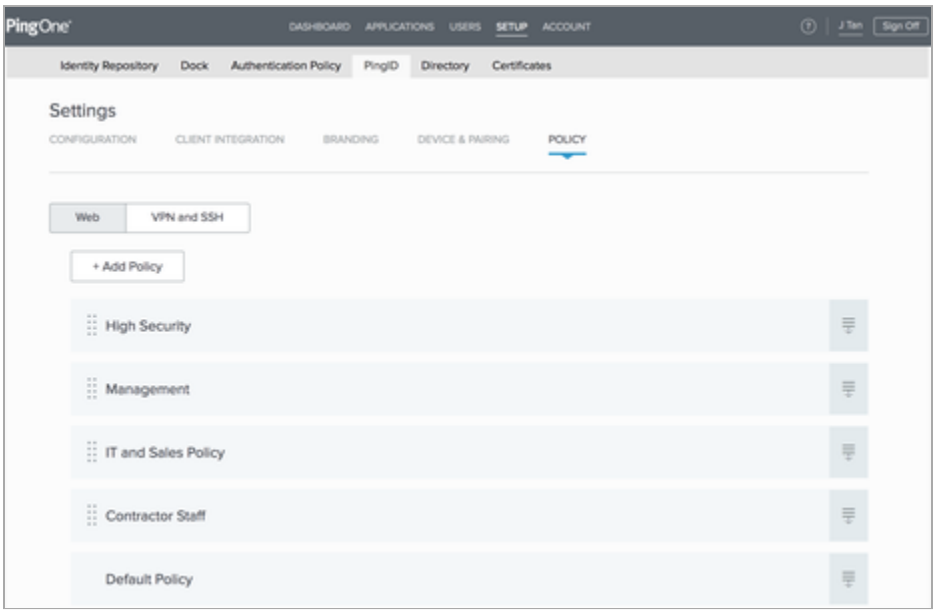
> **Note**
>
> If no other applications policies are configured after the policy is deleted, the default policy applies. The default policy cannot be deleted from the policy list.

Steps

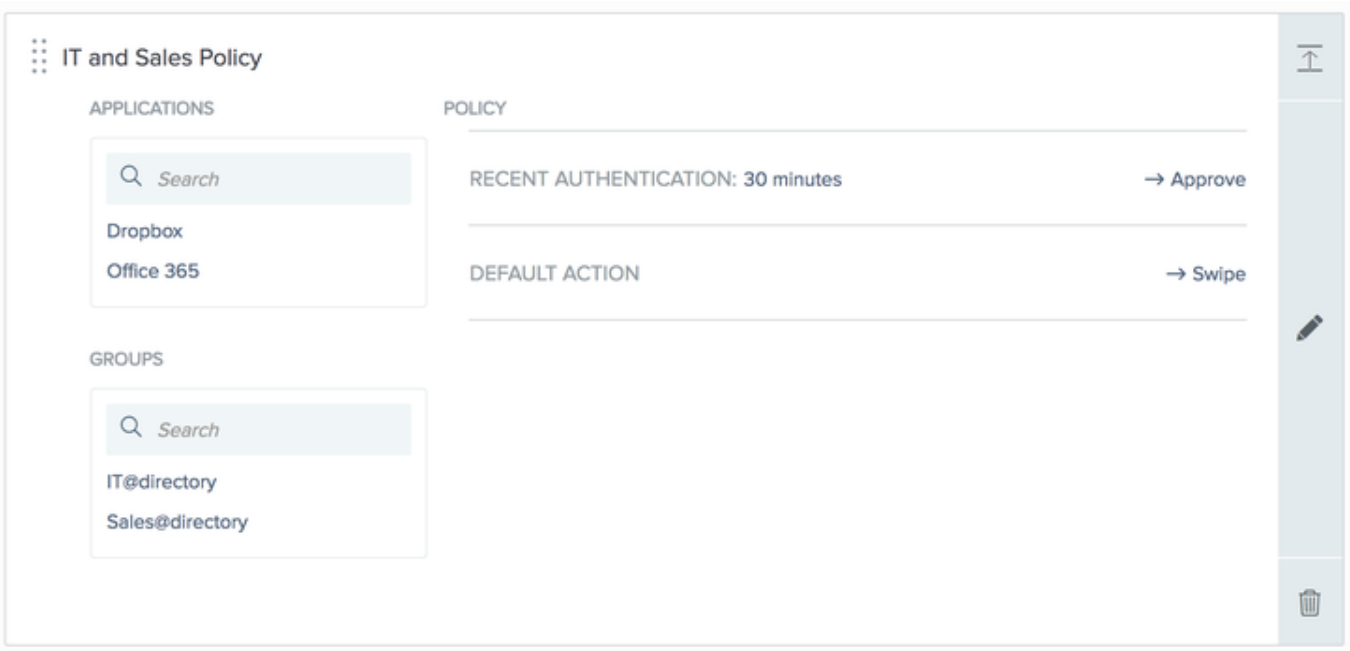
1. In the admin portal, go to **Setup → PingID → Policy**, and click the **Web** tab.

   Result:

   A list of policies is displayed.



2. Within the relevant the policy you want to edit, click the **Expand** icon ( ).



3. Click the **Delete** icon ().

> **Note**
>
> Ensure the remaining policies are listed in the order you want. This is the order in which they will be executed.

Result:

The policy is deleted from the list.

Managing app and group lists

You can apply a policy to any of the applications and groups that appear in the relevant list.

You can:

- Manually add applications to the applications list. See Adding a PingFederate application.
- Define a PingFederate application ID attribute. See Defining PingFederate application ID attributes.
- Edit the applications list. See Editing the applications list.
- Update the policy groups list. See Updating the policy groups list.

> **Note**
>
> - List display items are limited to 300 for **Applications** and **Groups**. Use the search box to search for a specific application or group.
> - The All **Applications**/**Groups** check box selects all existing items and automatically applies any additional items that are added to PingID in the future.

Adding a PingFederate application

You can add PingFederate applications to the applications list while creating a new policy.

About this task

By default, the applications list includes the following applications:

- **Device Management**: This application enables a user to manage their own devices, including adding, editing, or deleting multiple devices through the **Devices** page.
- **Password Reset**: This application enables users to reset their own password.

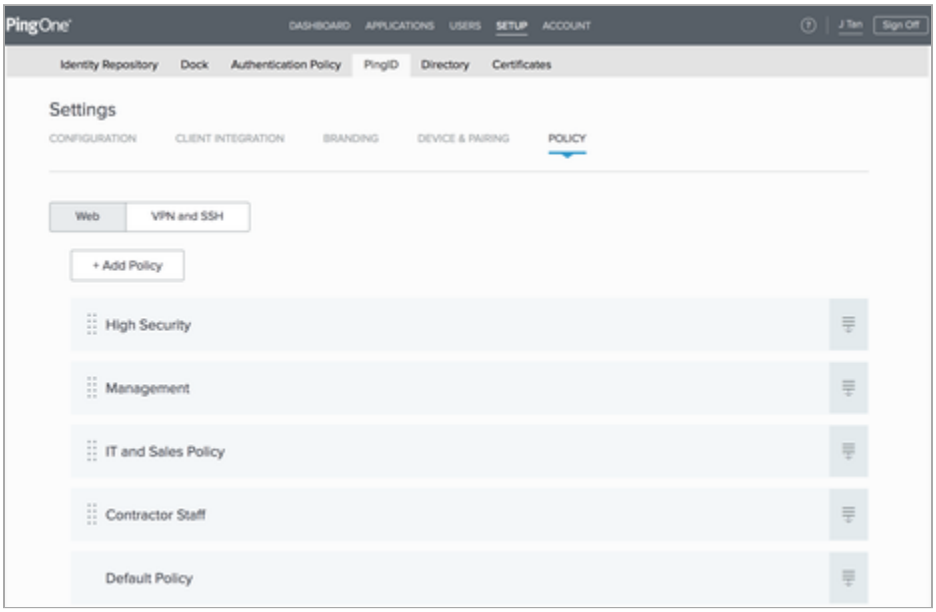
> **Note**
>
> App-specific policies require PingID Adapter 1.4 or later.

Steps

1. In the admin portal, go to **Setup → PingID → Policy**, and click the **Web** tab.

   Result:

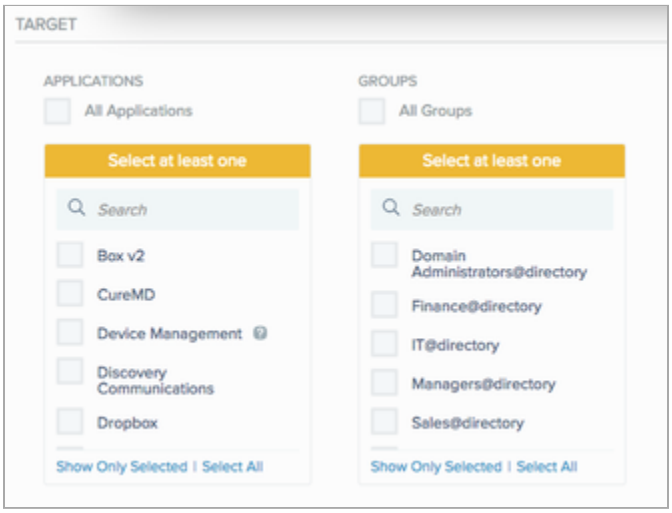
   A list of all the existing policies displays.



2. Click **+ Add Policy**.

   Result:

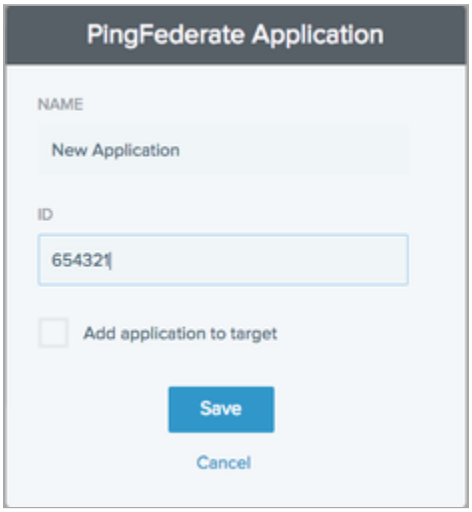
   The **New Policy** window displays with the **Applications** list.



3. In the **PingFederate Applications** section, click **+ Add Application**.

   Result:

   The **PingFederate Application** window appears.



4. In the **PingFederate Application** window, enter the following information:
    - **Name**: Enter the name of the application (max. 20 characters).
    - **ID**: Enter the application ID for the application. See unique application ID.
    - **Add application to target**: Select this check box to add the application to the new policy that you just created.
5. Click **Save**.

    Result:

    The new application is saved and appears in the **Applications** list.

Defining PingFederate application ID attributes

Define an application policy by adding the **Name** and **ID** attributes.

Each application that you define in the PingID **Policy** tab must include the following information:

- **Name**: The name of the application as it appears in the PingID policy application list. This attribute does not have to match the application name defined in PingFederate.
- **ID**: The unique ID for the relevant application in PingFederate. This attribute must match the relevant PingFederate Application ID attribute as defined in the following table.

> **Note**
>
> For more information from the administrator's guide, see PingFederate admin guide.

PingFederate application ID attribute mapping

Type of Target Application	Application Identifier
SAML or WS-Federation (service provider connection)	Partner Entity or Realm ID (Connection ID)
OAuth or OpenID Connect (OAuth Client)	OAuth Client ID
Custom	SP Adapter ID

Editing the applications list

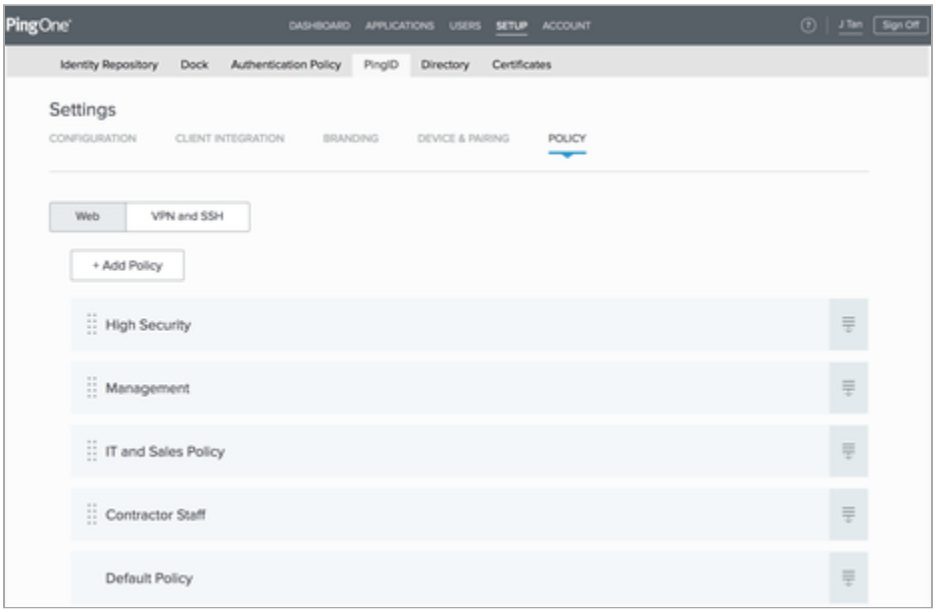
Rename a PingFederate application, change the unique ID, or delete an application.

About this task

Edit an application from the **New Policy** window.

Steps

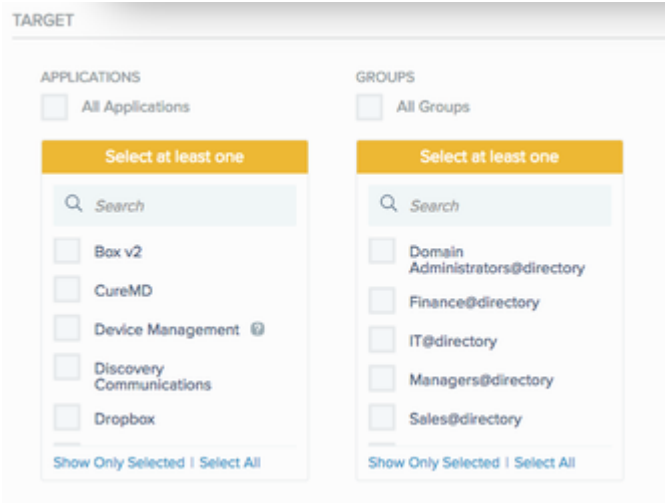
1. In the admin portal, go to **Setup → PingID → Policy**, click the **Web** tab.



2. Click **+ Add Policy**.

   Result:

   The **New Policy** window displays with the **Applications** list.



3. In the **Target** section, from the **Applications** list, select the check box of the applications that you want to edit.
4. In the **PingFederate Applications** section, click **Manage Applications**.

   Result:

   The **PingFederate Applications** window opens, enabling the editing of the applications you selected and their **Name** and **ID** fields.

5. To edit the application **Name** or **ID**, click the relevant field and enter the new name or ID.
6. To delete an application, in the application listing, click the **Delete** icon ( ).
7. Click **Save**.

   Result:

   Your changes are saved. The **Applications** list is updated.

Updating the policy groups list

When a group is created in Active Directory, it does not automatically appear in the policy groups list. At least one user that is assigned to the group must successfully authenticate using PingID for the groups list to be updated.

Before you begin

To ensure Active Directory groups are populated in the policy groups list, configure your system so that all user groups that appear in your directory are included in a PingOne single sign-on (SSO) assertion or PingID authentication, such as using the PingID Adapter attribute mapping. For more details, see Registering the PingID service.

About this task

For an organizational user group to appear in the policy groups list, update the policy groups list.

Steps

1. Create a new user group in your local Active Directory.
2. Assign users to the directory group.

   At least one user must be assigned to the group.
3. Ensure at least one of the users in the new group authenticates with PingID successfully or through SSO to PingOne.
4. In the PingOne admin portal, go to **Setup → PingID → Policy**. Refresh the **Policy** window.

   Result:

   The next time you create or edit a policy, the new group appears in the **Groups** list.

Enabling a Windows login and RDP authentication policy

Enable an authentication policy for Windows login and RDP.

Before you begin

Edit the relevant web policy authentication and ensure that the either the **Windows Login** or **Windows Remote Desktop** check box is selected. See Editing a web authentication policy.

About this task

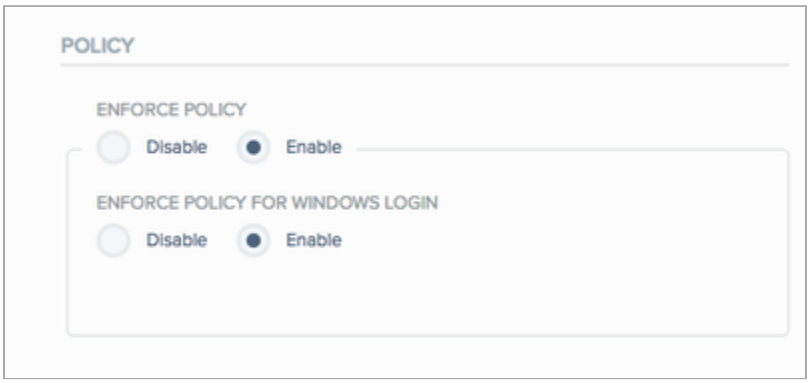
> **Note**
>
> You can apply an authentication policy to the PingID integration for Windows login 2.1+.

Steps

1. Go to **Setup → PingID → Configuration**.

> **Note**
>
> To manage both **Windows Login** and **Windows Remote Desktop** authentication policies, see Editing a web authentication policy and Deleting a web authentication policy.

2. In the **Policy** section, for both the **Enforce Policy** option and the **Enforce Policy For Windows Login** option, click **Enable**.



Configuring a RADIUS PCV and SSH access policy

Configure a policy for a user to access a protected application through a RADIUS PCV or SSH.

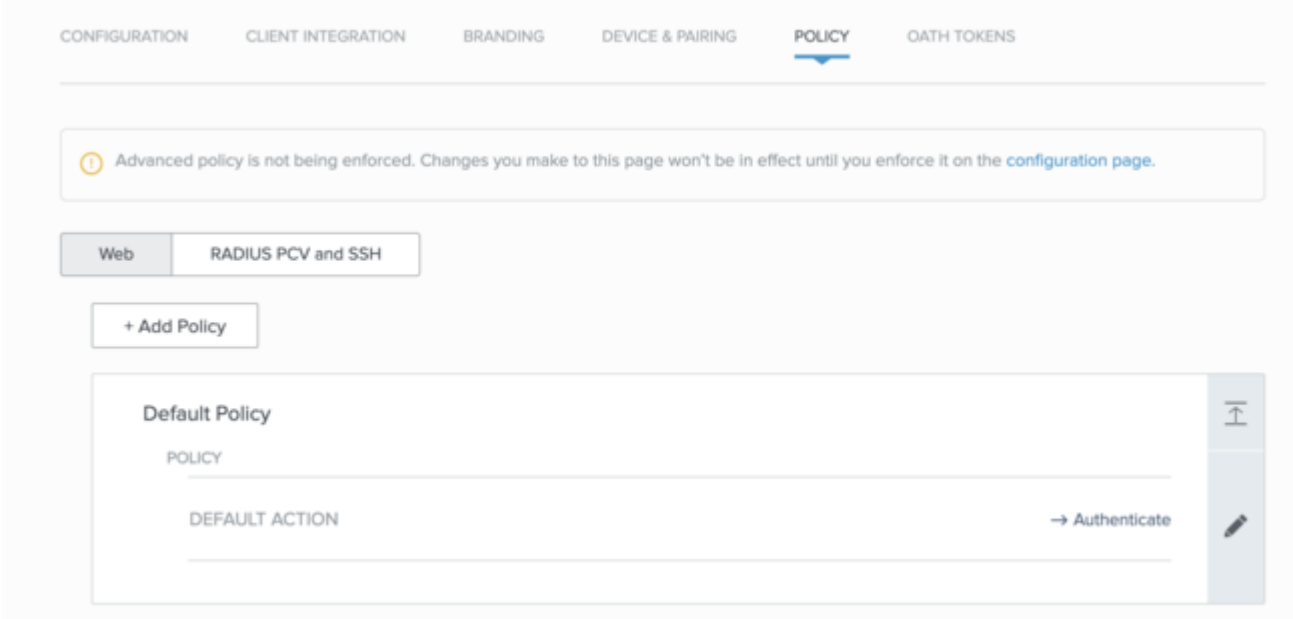
About this task

Edit the default policy and add one or more rules to the policy.

> **Note**
>
> To apply PingID policy features that require IP address information, the client IP address must be provided. For more information, see Prerequisites: Pingfederate RADIUS server.

Steps

1. In the admin portal, go to **Setup → PingID → Policy**, and click the **RADIUS PCV and SSH** tab.



2. In the **Allowed Methods** section, select the authentication methods to allow for this policy.

   Only the methods selected become available in the rule authentication **Actions** list.

> **Note**
>
> You must select at least one authentication method. To include all authentication methods, including **Deprecated** authentication actions, select the **All Methods** check box. For a detailed description of available authentication methods at the policy and rule level, see Policy and rule authentication methods.

3. In the **Rules** section, from the list, select and configure one or more policy rules.

   Choose from:

   - Configuring an accessing from company network rule (RADIUS PCV and SSH)
   - Configuring an accessing from countries rule (RADIUS PCV and SSH)

     Result:

     The chosen rule configuration section expands.

4. Complete the rule section configuration.

> **Note**
>
> From the **Action** list, the default action selected determines which authentication action is performed if no other policy rule applies.

5. Click **Save**.

Configuring an accessing from company network rule (RADIUS PCV and SSH)

Determine which authentication action to prompt the user with when accessing the RADIUS PCV or SSH, if the users device is within the company network.

About this task

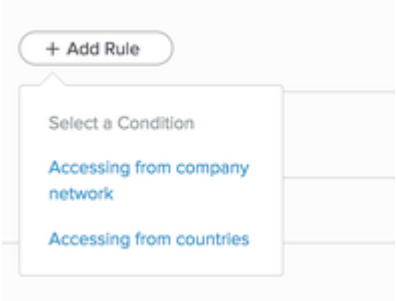
You can require a user's authenticating device to be in the company offices when signing on from within the company network. In addition, you can choose to silently authenticate the user without requiring active user intervention in the authentication process for in-network access.

> **Note**
>
> To apply the PingID policy features that require IP address information, the client's IP address must be provided first. For more information, see Prerequisites: Pingfederate RADIUS server.

> **Note**
>
> To ensure location-based policies are applied, you must also ensure location collection is enabled at the organization level (see Enabling or disabling location collection).

Steps

1. From within the relevant policy, click **+ Add Rule** and from the **Conditions** list, select **Accessing from company network**.



2. From the **Action** list:

   Choose from:

   - **Approve**: Approves access without requiring PingID authentication.
   - **Authenticate**: Allows a user to authenticate using any of the authentication methods allowed at the policy level.

     > **Note**
     >
     > If more than one authentication method is available, the method initiated by default is the method most recently paired by the user that is authenticating.

   - Select a specific authentication method. The options listed are defined by those configured at policy level. For a description of each authentication type, see Rule authentication actions.

3. In the **IP Addresses** field, enter a list of external IP addresses or ranges that belong to the company network.

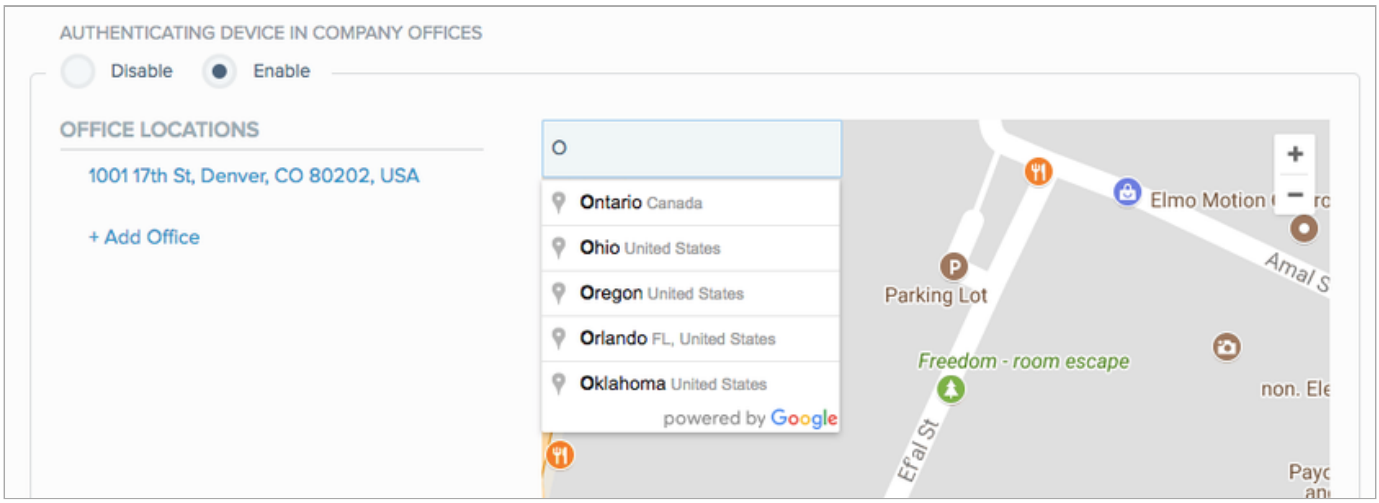
> **Note**
>
> Enter the IP addresses or ranges using CIDR notation with each entry on its own line.

4. To require a user's authenticating device to be in the company offices when signing on from within the company network, in the **Authenticating Device In Company Offices** field, click **Enable** and then define one or more company office locations.

> **Note**
>
> If you are defining a company office in addition to an IP address, in the **Allowed Authentication Method** section, select the **Swipe**, **Mobile App Biometrics**, or **One-time passcode** check box to define an authentication method to apply this rule.

Result:

The **Office Locations** wizard opens, enabling you to define one or more office locations. If the authenticating device is located within one of the defined areas, it is considered to be inside a company office.

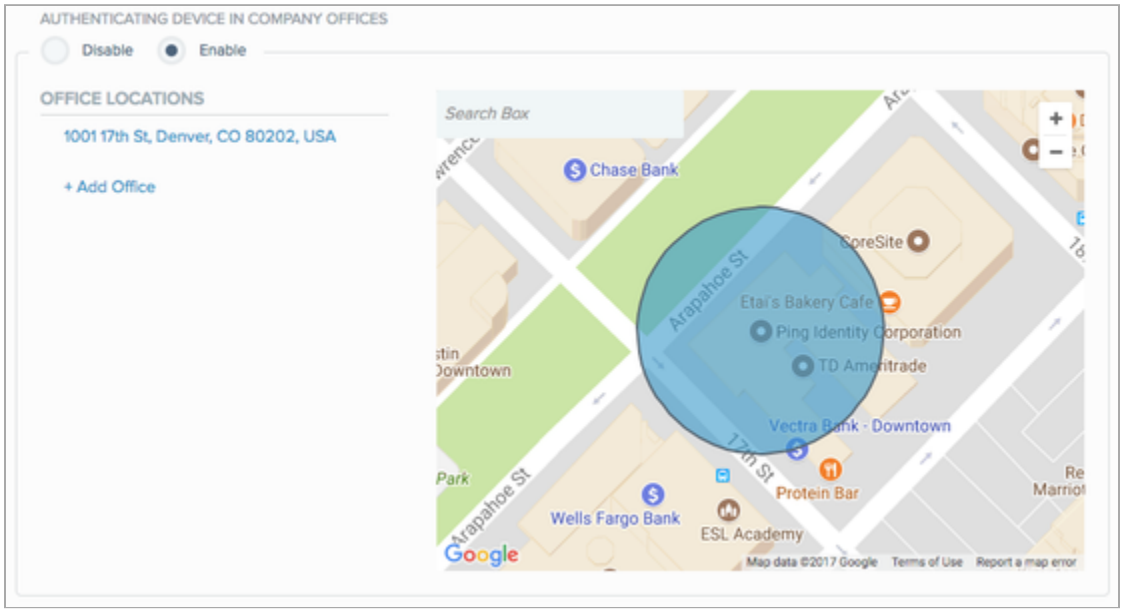


5. To define additional office locations:

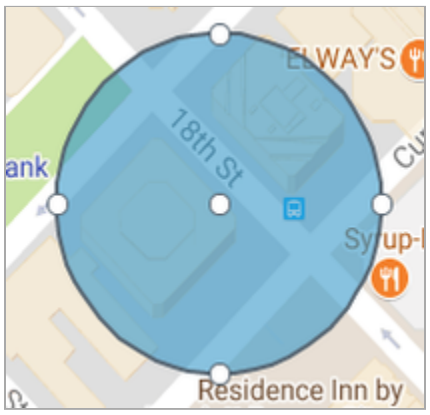
    1. Click **+ Add office** or enter an address in the search box.

        Result:

        A blue circle appears on the map, defining the office area.



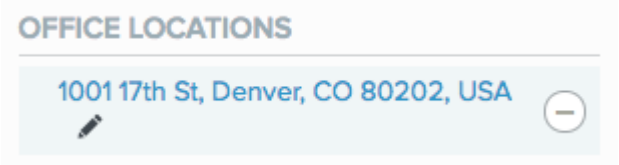
2. Click center of the circle to edit the coordinates.



- To reposition the circle, click and drag the white dot at the circle's center to the desired location.
- To resize the circle, click and drag any white dot on the circle's rim.
- To add another office location, click a location outside the circle. A new circle is added.

1. To edit an office location, click the **Pencil** icon ( ) and edit the name.

   By default, the location is named after its street address.

2. To delete an office address, click the **Minus** icon ( ).

> **Note**
>
> If you edit or delete offices in the **Office Locations** list, changes are applied to all rules that specify office locations.

6. In the **Policy** list, click and drag the new rule and place it in the order in which you want it to be considered. Click **Save Order**.
7. Click **Save**.

Next steps

To ensure the policy is applied to your organization, go to **PingID → Configuration** and ensure **Enforce Policy** is set to **Enabled**.

Configuring an accessing from countries rule (RADIUS PCV and SSH)

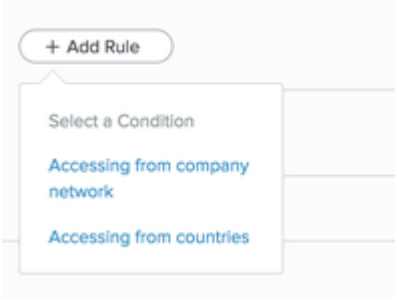
According to the country, determine which authentication action to prompt the user with on the machine that uses RADIUS PCV or SSH for access.

About this task

> **Note**
>
> The country location is determined by the IP address of the accessing device and not by the IP address of the authentication device.

Steps

1. From within the relevant policy, click**+ Add Rule** and from the **Conditions** list, select **Accessing from countries**.



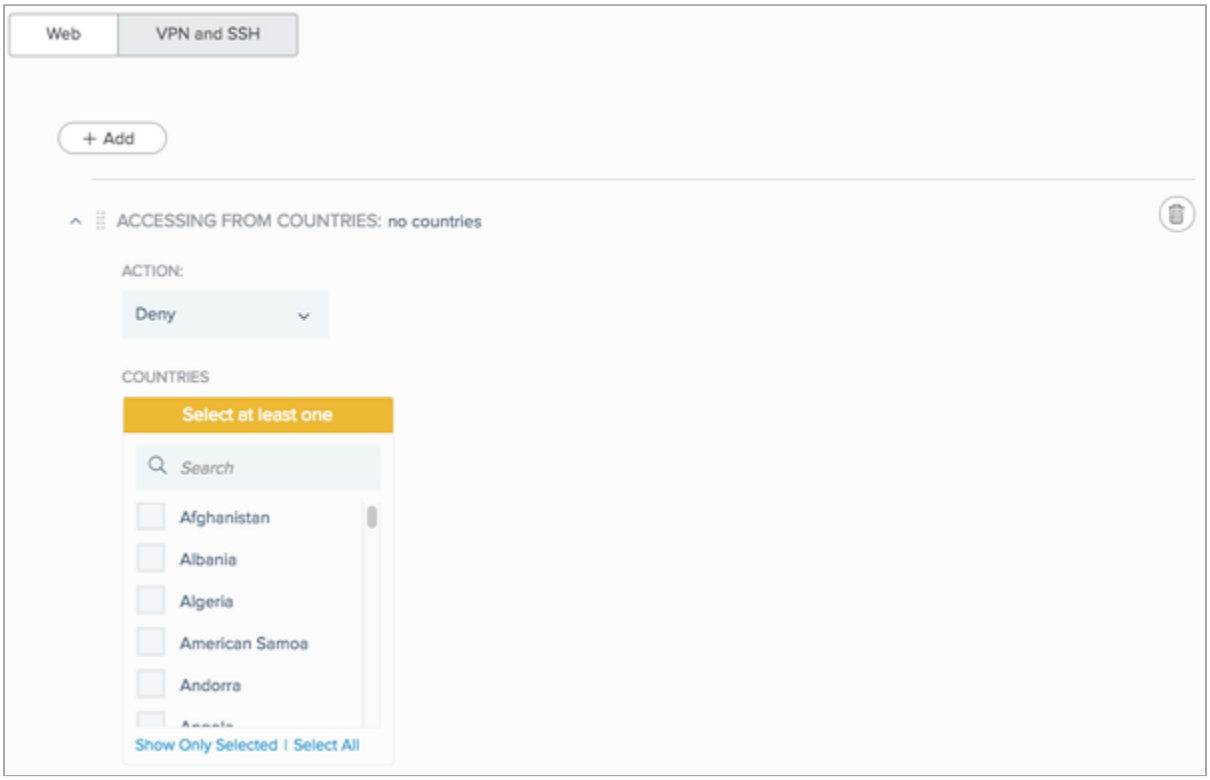
2. From the **Action** list:

   Choose from:

   - **Authenticate**: Allows a user to authenticate using any of the authentication methods allowed at the policy level.

     > **Note**
     >
     > If more than one authentication method is available, the method initiated by default is the method most recently paired by the user that is authenticating.

   - **Deny**: Denies access.
   - Select a specific authentication method. The options listed are defined by those configured at policy level. For a description of each authentication type, see Rule authentication actions.



3. From the **Countries** list, select the check box of each country to which you want the policy to apply.

Option	Description
Search bar	Use to search for a specific country, enter the country name or part of the name. Only countries whose name contains that string are displayed.
Show Only Selected	Use to show only the countries you have selected.
Select All	Use to select all countries.

4. If you have more than one rule listed, from the **Rules** list, click and drag the new rule and place it in the order you want it to be considered. Click **Save Order**.
5. Click **Save**.

Next steps

To ensure the policy is applied to your organization, go to **PingID → Configuration** and ensure **Enforce Policy** is set to **Enabled**.

Viewing policy events in the PingID report

Generate a PingID report to view a range of PingID events.

About this task

There are two types of policy events included in the PingID report:

`Pairing Details` *event*

Provides details of a user's pairing attempt, based on the Device & Pairing rules. For more information, see Device and pairing policy.

`Authentication Details` *event*

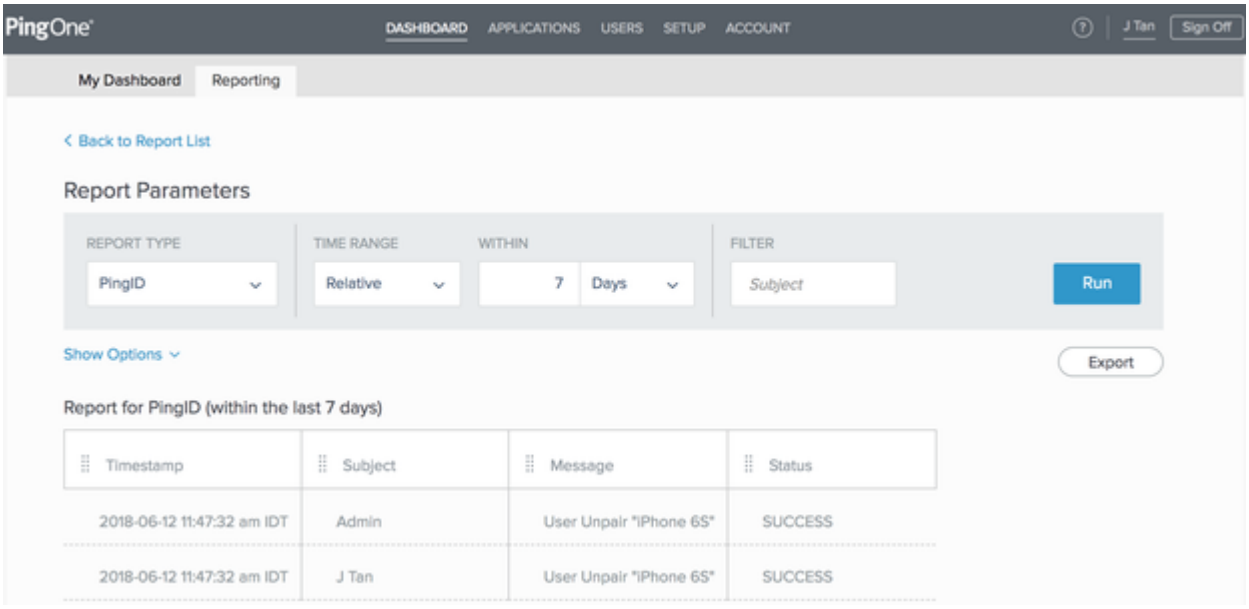
Provides details of a user's authentication attempt, based on the defined policy rules together with the Device & Pairing rules. For more information, see Configuring a global authentication policy (default policy), Configuring a RADIUS PCV and SSH access policy, and Device and pairing policy. The entry also indicates the apps and groups to which a policy is applied, if applicable.

> **Note**
>
> - Policy-related event data, such as `IP Address` and `Country`, is only included in report events when the accessing device is able to push the data as part of the authentication flow. For offline authentication events and authentication failure events, policy-related fields will therefore show results as `N/A`.
> - For an overview of running and filtering PingID reports, see Running the PingID activity report.

Steps

1. In the PingOne admin console, go to **Dashboard → Reporting**.
2. From the **Report Type** list, select **PingID**.
3. In the **Within** field, enter `7`, and then select **Days** from the list. Click **Run**.

> **Note**
>
> You can filter the results by changing the **Time Range** or entering a string in the **Filter** field and then running the report again.



Result

The PingID report displays, showing results for the past 7 days by default. Policy-related entries are identified by the following information:

Timestamp

The time at which the policy event occurred.

Subject

The user to whom the policy was applied.

Message

A list of policy-related fields providing detailed information about policy-related events. The first line of the **Message** field indicates whether the event is a `Pairing Details` event or an `Authentication Details` event.

Status

The status `POLICY` indicates that the event is a policy related event.

Each policy entry lists values for the relevant policy elements. The following table describes the elements that can be included in a policy event and their potential values. NOTE: The order of the elements in the table corresponds to the order of the elements in the displayed report.

Policy element	Value
Type of event	`Authentication Details` or `Pairing Details`.
IP Address	The IP address of the accessing device.
Previous Authentication IP	The IP address of the IP address of the accessing device used in the previous sign on.
Previous Authentication Time	The time of the last successful authentication.
IP Reputation Whitelist Met	Indicates whether the IP address of the accessing device appears in the IP reputation rule white list (`true` or `false`).
Geovelocity Whitelist Met	Indicates whether the IP address of the accessing device appears in the Geovelocity rule white list (`true` or `false`).
IP Risk Score	The risk score category of the IP address of the accessing device (`Low`, `Medium`, or `High`).
Country	The location from which the accessing device is communicating.
Previous Country	The location from which the accessing device communicated during the last sign on.
Ground Speed	The speed taken to travel between the current login location and the previous location, in the time that elapsed since the previous sign on (`km/h`). If the speed exceeds 1000 km/h, the rule is triggered.

Policy element	Value
Current VPN/Proxy login	Whether the accessing device for the current sign on is using a proxy or VPN. Possible values are `true` or `false`. If this value is true, the Geovelocity rule is ignored.
Previous VPN/Proxy login	Indicates the accessing device for the previous sign on was using a proxy or VPN. Possible values are `true` or `false`. If this value is `true`, the Geovelocity rule is ignored.
New Device	Whether the accessing device is new. Possible values are `true` or `false`.
Requested Application ID	The ID of the app the user is trying to access.
Requested Application Name	The name of the app the user is trying to access.
Password Reset	Indicates whether the user tried to reset the SSO password. Possible values are `true` or `false`.
Self Service Device Management	Whether the user tried to access the **Devices** page. Possible values are `true` or `false`.
Time since last Authentication	The amount of time that has passed since the last authentication. `In the last <number> minutes.`
Accessing Device UserAgent	The user agent string of the browser on the accessing device.
Accessing Device OS	The name and version of the OS on the accessing device, for example, `OS X 10,15`.
Accessing Device Browser	The browser used on the accessing device, for example, `Chrome 89.0`
Allowed Authentication Methods	The allowed authentication methods in the applied policy. This information is displayed in the event that a user attempts to authenticate with a device that is not allowed by this policy.
Time since last Authentication from Office	The last time the user authenticated from the office, in minutes. If no office is defined, the value is `N/A`.
Mobile OS Version	The OS name and version of the authenticating device. For example, `iOS 9.3.2`.
Device Model	The make and model of the authenticating device. For example, `iPhone 6S`.
Device Lock Enabled	Whether device lock is enabled on the mobile device. Possible values are `true` or `false`.
Device Rooted or Jailbroken	Whether the mobile device rooted or jailbroken. Possible values are `true` or `false`.

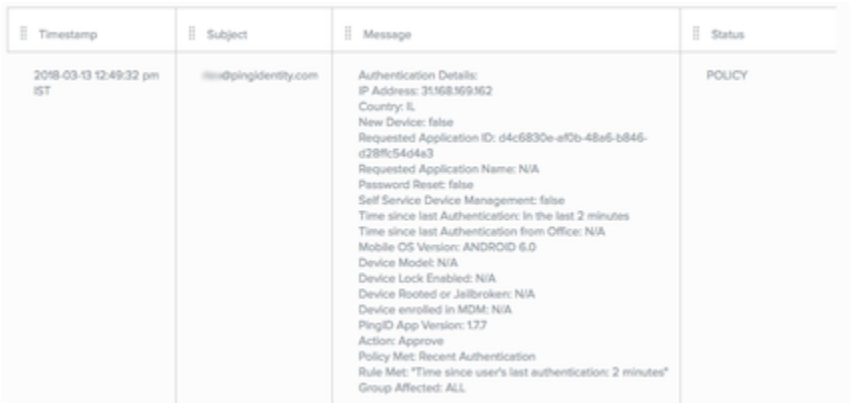
Policy element	Value
Device enrolled in MDM	Whether the mobile device is enrolled in mobile device management (MDM). Possible values are `true` or `false`.
PingID App version	The version of the PingID app on the user device. For example, `1.8.1`.
Action	The action defined for this policy: ***Approve*** Authentication is approved without any further action from the user. ***Deny*** Authentication is denied. ***Swipe*** A push notification is sent to the user requiring swipe to authenticate. ***Biometrics*** A push notification is sent to the user requiring the user to authenticate using their device biometrics. ***OTP*** The user is prompted to enter a one-time passcode to authenticate.
Policy/Policies not Met	The name of the policy/policies that were not met during the pairing or authentication action.
Policy/Policies Met	The name of the policy or policies with which the action complied.
Rule Met	The rule within the policy that was executed.
Group Affected	The groups to which the policy was applied.

Policy event examples

The following examples illustrate common policy event scenarios.

Authentication not requested because the user recently authenticated successfully

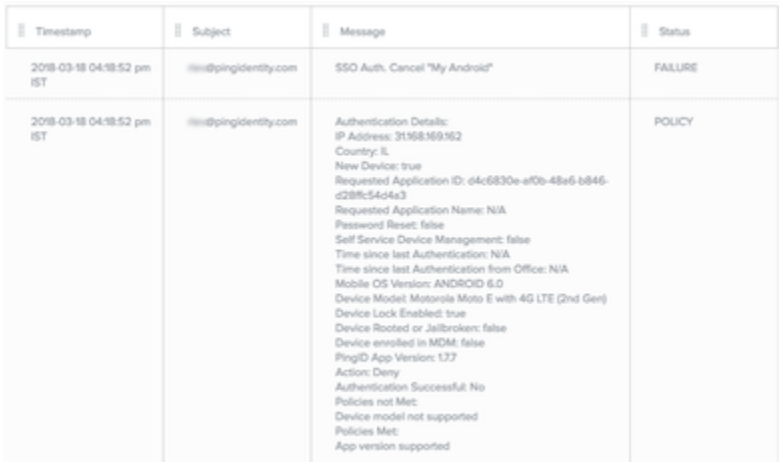
When performing an action that normally requires authentication, a user is not requested to authenticate (`Action: Approve`) because they already authenticated within the time stated in the policy (`Rule Met: "Time since user's last authentication: 2 minutes"`).



Timestamp	Subject	Message	Status
2018-03-13 12:49:32 pm IST	@pingidentity.com	Authentication Details: IP Address: 31.168.169.162 Country: IL New Device: false Requested Application ID: d4c6830e-af0b-48a6-b846-d28ffc54d4a3 Requested Application Name: N/A Password Reset: false Self Service Device Management: false Time since last Authentication: In the last 2 minutes Time since last Authentication from Office: N/A Mobile OS Version: ANDROID 6.0 Device Model: N/A Device Lock Enabled: N/A Device Rooted or Jailbroken: N/A Device enrolled in MDM: N/A PingID App Version: 1.7.7 Action: Approve Policy Met: Recent Authentication Rule Met: "Time since user's last authentication: 2 minutes" Group Affected: ALL	POLICY

Authentication unsuccessful

The policy does not support the specific mobile device. Authentication is denied to a user attempting to sign on using a device that is no longer supported (`Device Model: Moto E with 4G LTE (2nd Gen)` ; `Authentication Successful: No` ; `Policies not Met: Device model not supported`).



Timestamp	Subject	Message	Status
2018-03-18 04:18:52 pm IST	@pingidentity.com	SSO Auth. Cancel "My Android"	FAILURE
2018-03-18 04:18:52 pm IST	@pingidentity.com	Authentication Details: IP Address: 31.168.169.162 Country: IL New Device: true Requested Application ID: d4c6830e-af0b-48a6-b846-d28ffc54d4a3 Requested Application Name: N/A Password Reset: false Self Service Device Management: false Time since last Authentication: N/A Time since last Authentication from Office: N/A Mobile OS Version: ANDROID 6.0 Device Model: Motorola Moto E with 4G LTE (2nd Gen) Device Lock Enabled: true Device Rooted or Jailbroken: false Device enrolled in MDM: false PingID App Version: 1.7.7 Action: Deny Authentication Successful: No Policies not Met: Device model not supported Policies Met: App version supported	POLICY

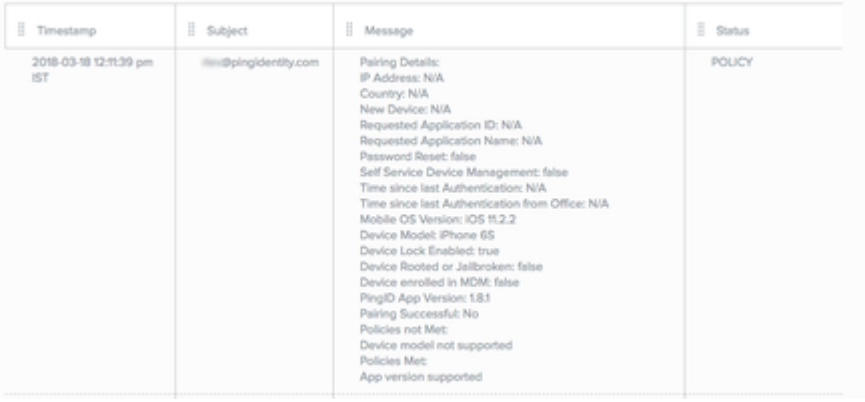
Pairing successful

When pairing a device, an authentication action policy event entry is displayed after the pairing attempt entry. Pairing event shows successful pairing of an iPhone 6S (`Device Paired "iPhone 6S"` `Status=SUCCESS` . Authentication event shows `New Device: true`).

2018-03-18 12:30:00 pm IST	@pingidentity.com	Authentication Details: IP Address: N/A Country: N/A New Device: true Requested Application ID: N/A Requested Application Name: N/A Password Reset: false Self Service Device Management: false Time since last Authentication: N/A Time since last Authentication from Office: N/A Mobile OS Version: iOS 11.2.2 Device Model: iPhone 6S Device Lock Enabled: true Device Rooted or Jailbroken: false Device enrolled in MDM: false PingID App Version: 1.8.1 Action: Swipe Policy Met: Default Policy Rule Met: "Default Action"	POLICY
2018-03-18 12:29:49 pm IST	@pingidentity.com	Device Paired "iPhone 6S"	SUCCESS

Pairing denied

A user's attempt to pair with an iPhone 6 fails, because the device is not supported. The event type (`Pairing Details`) indicates `Device Model: iPhone 6S` , `Policies not Met: Device model not supported` .



Troubleshoot PingID policy

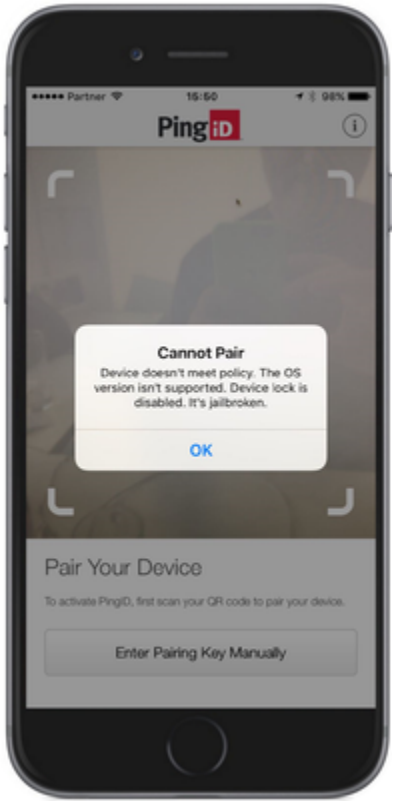
This section lists common issues that end users might encounter when using PingID.

The mobile app displays a Cannot Pair message, or the web screen displays a Blocked message

Cannot Pair

When attempting to pair a mobile device with PingID, the mobile app displays a **Cannot Pair** error, followed by text detailing the cause.

The description of the cause can comprise of one or more of the entries in the following table.

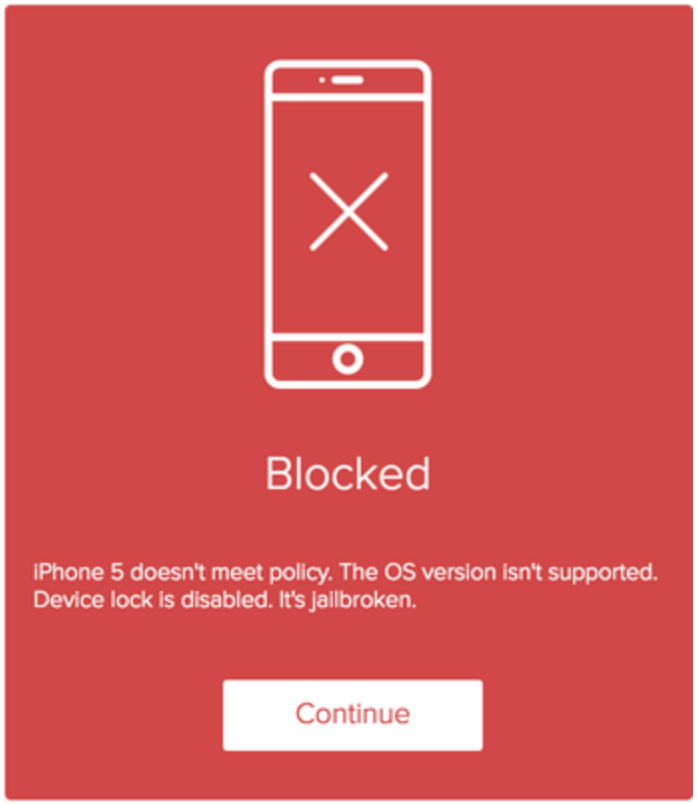


Blocked

When attempting to authenticate using a mobile device, the web screen returns a **Blocked** error , followed by:

- The name of the affected device
- The cause

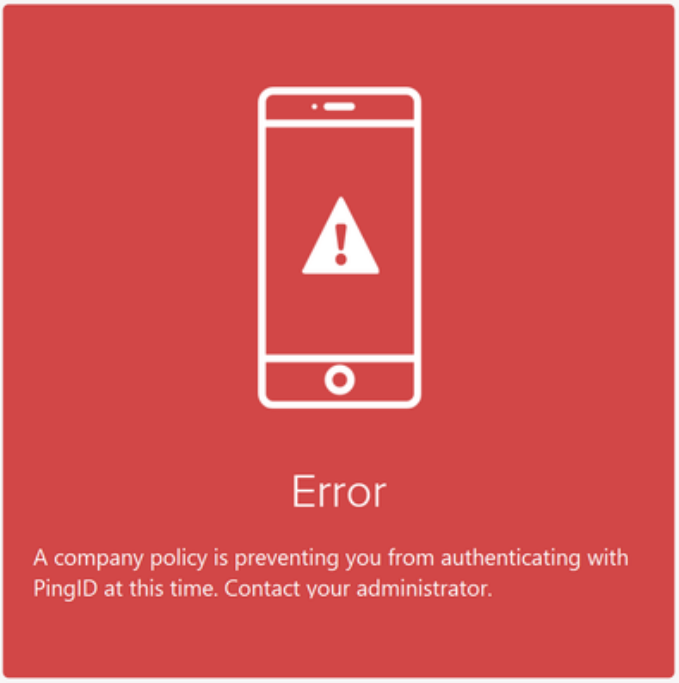
The description of the cause can comprise of one or more of the entries in the following table.



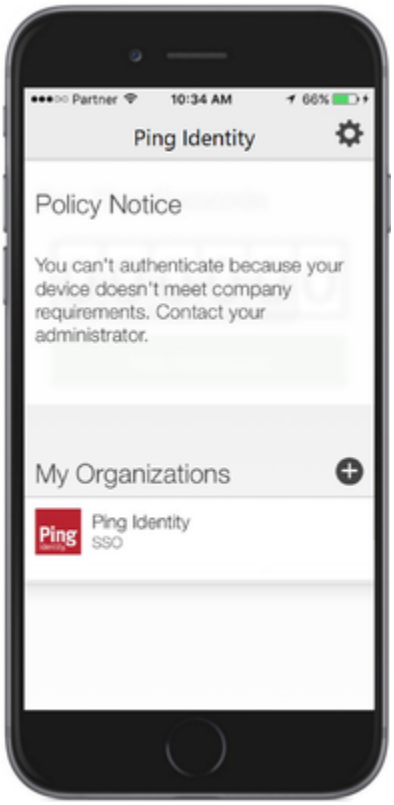
Message	Description and actions
Device is rooted. (Android) Device is jailbroken. (iOS)	Rooting and jailbreaking are ways of bypassing mobile device limitations and using the device in ways that manufacturers and carriers want to prevent. Removal of safeguards from the device through rooting or jailbreaking can leave it vulnerable to fraudulent attacks. Organizations that permit access to their networks using mobile apps want to ensure security. Only use an unrooted or unjailbroken device for authentication through PingID.
Device lock is disabled.	The organization's security policy requires that mobile devices accessing their network have device lock enabled. This enhances security and prevents unauthorized access if the mobile device is lost or stolen. Enable the mobile device lock to permit authentication through PingID.
Device type not supported.	Some organizations permit mobile device access to their networks only through preapproved brands and models. This message might also appear when the user's mobile device matches a brand and model disallowed by the organization's policy. Only use an approved device for authentication through PingID. Contact your administrator for the list of permitted or disallowed models.

Message	Description and actions
Device OS version not supported.	The organization's security policy permits access only when using devices that run a specific operating system version (or later) that complies with specific security prerequisites. To use your device for authentication with PingID, upgrade the operating system or replace it with a model running the minimum required (or later) version of the permitted mobile operating system. Contact your administrator for the minimum required OS version. **Note** This requirement can be reassessed periodically, and the required OS version might be updated in the future.
Device not enrolled in MDM.	The organization uses a mobile device management (MDM) system to enable the combination of effective mobile device use and to protect sensitive data from unauthorized access. To pair a mobile device for authentication through PingID, when prompted, the user must permit the MDM to operate as an administrator of the device.
A company policy is preventing you from pairing this device with PingID at this time. Contact your admin.	The mobile app displays a general message due to incompatibility with your organization's policy conditions, which are not covered by specific messages. Contact your administrator to assist in resolving the issue.

The web screen displays a general Error message

Error This is a general failure message due to incompatibility scenarios, not covered by specific messages. Contact your administrator to assist in resolving the issue.	

The mobile app displays a Policy Notice message

Policy Notice When the mobile device does not comply with the organization's device requirements policy, the **Policy Notice** screen appears on the mobile device and prevents the user from using the mobile app's OTP generator to complete authentication. Contact your administrator to assist in resolving the issue.	

Add your branding to PingID

You can customize PingID to include custom colors, logo, and background.

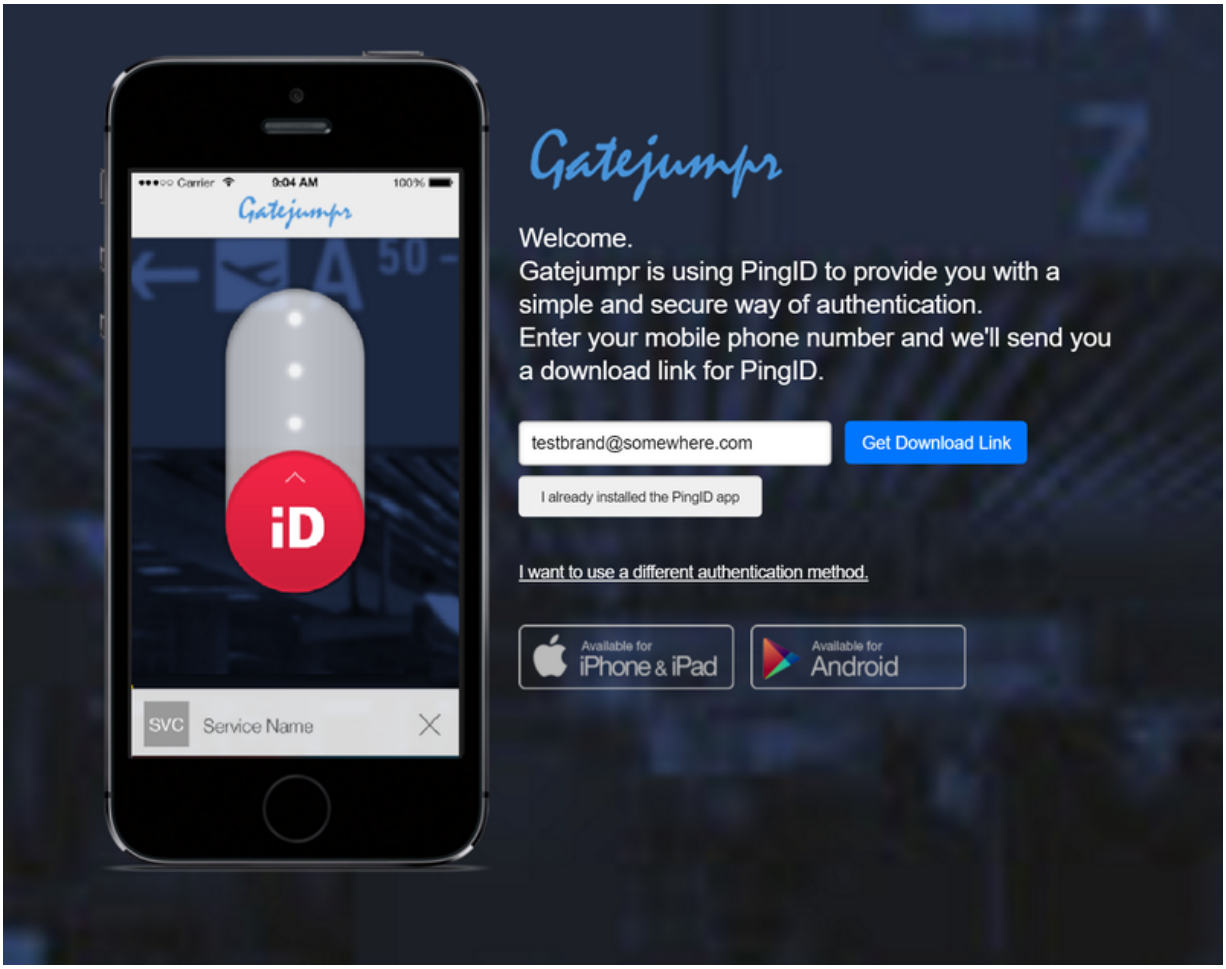
You can customize your end users' PingID experience to complement your organization's brand by applying your organizations branding elements to the PingID enrollment screens and selected mobile application elements. You can define your organization's custom colors, logo, and background.

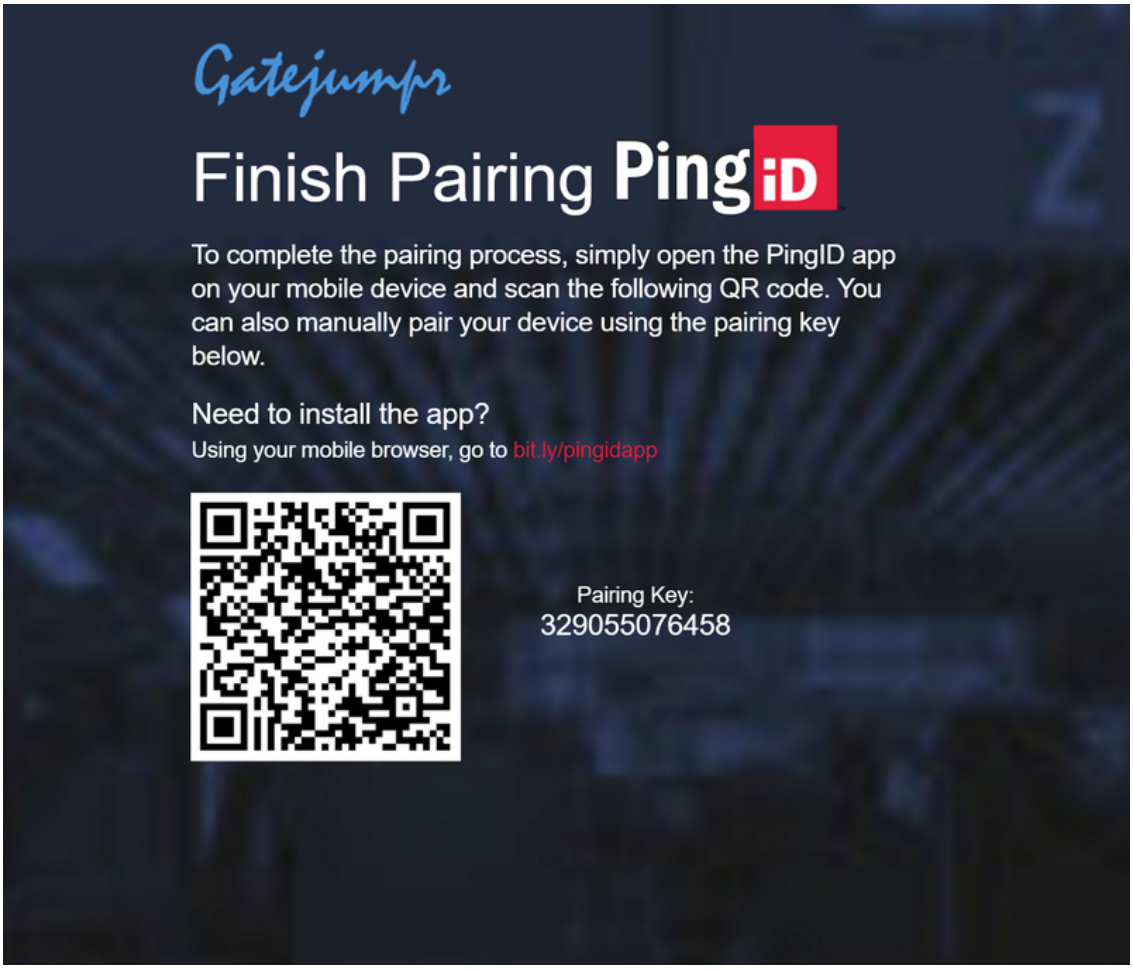
The benefits of customizing PingID with your branding include:

- Alignment with the organization's "look and feel"
- A customized and familiar end user experience
- Reduced end user confusion and suspicion

You can apply your organization's branding to the following elements:

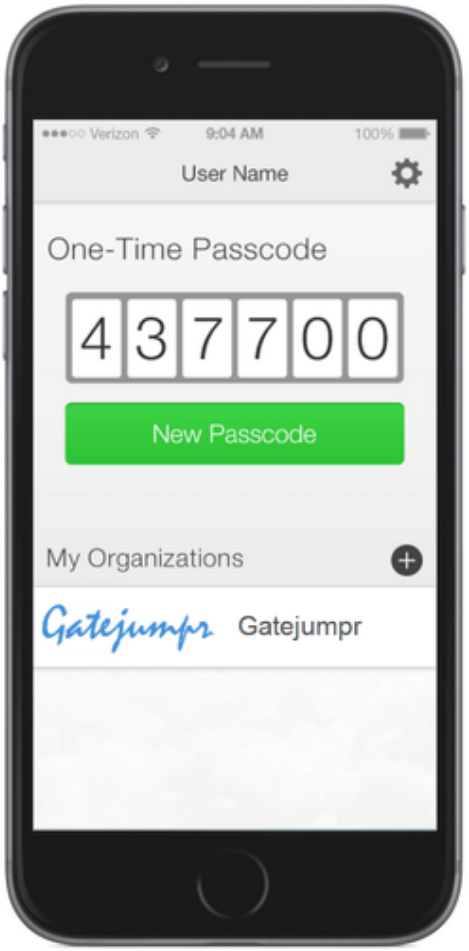
- Out-of-the-box user enrollment screens. For more information, see Customizing the PingID enrollment page (legacy).





- End user mobile authenticating devices', such as smart phones, swipe screen. For more information, see Customizing the PingID mobile app swipe screen.

• PingID App home screen. For more information, see Customizing the PingID mobile app home screen.

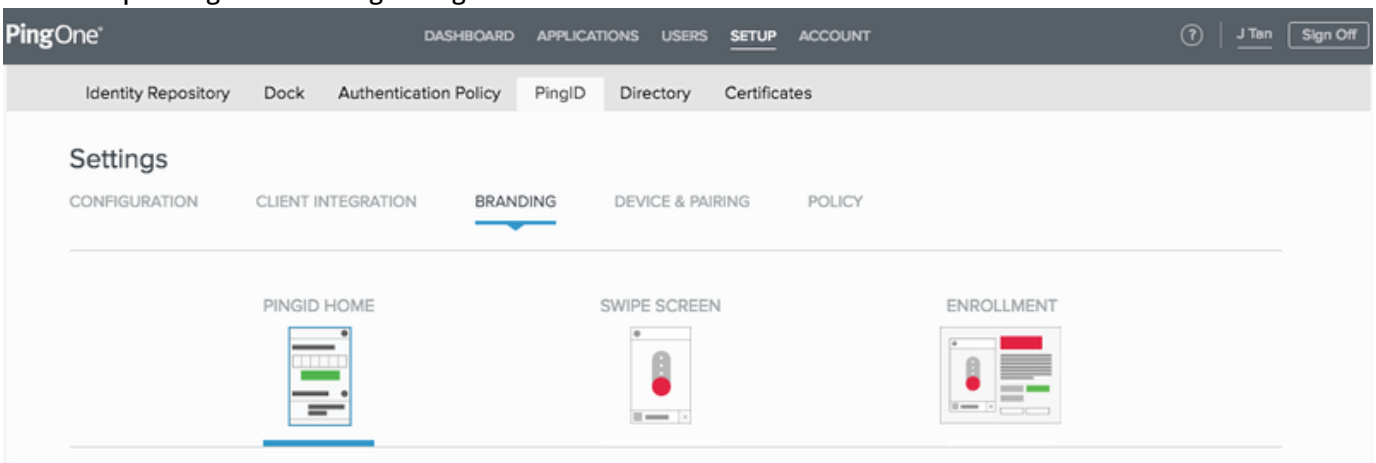


Customizing the PingID mobile app home screen

Customize the home screen of the PingID mobile app to make your corporate logo an integral part of your end users' authentication experience.

Steps

1. Go to **Setup → PingID → Branding → PingID Home**.



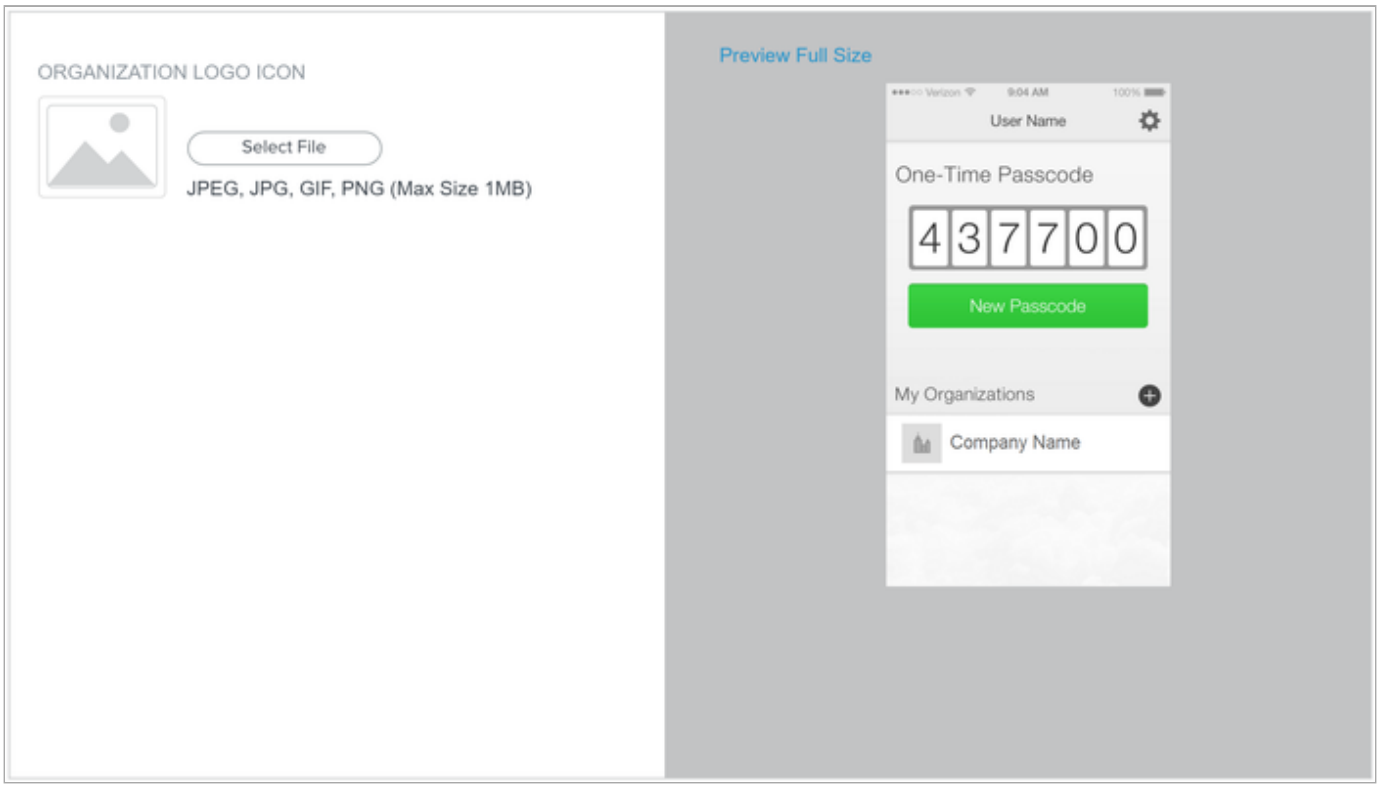
2. In the **Organization Logo Icon** section, click **Select File** and navigate to the image you want to use.

   Click **Preview Full Size** to view the proposed changes.

   > **Note**
   >
   > The icon can be a JPEG, JPG, GIF, or PNG file with a maximum size of 1MB.

   Result:

   The selected image appears in the **My Organizations** section of the PingID mobile app home screen, next to your **Company Name**.



   Click **Remove** to restore the original PingID default setting.

   Click **Save**.

> **Note**
>
> Clicking **Discard Changes** in the **PingID Home**, **Swipe Screen**, or **Enrollment** windows discards any changes made in all of the windows since the last save.

Customizing the PingID mobile app swipe screen

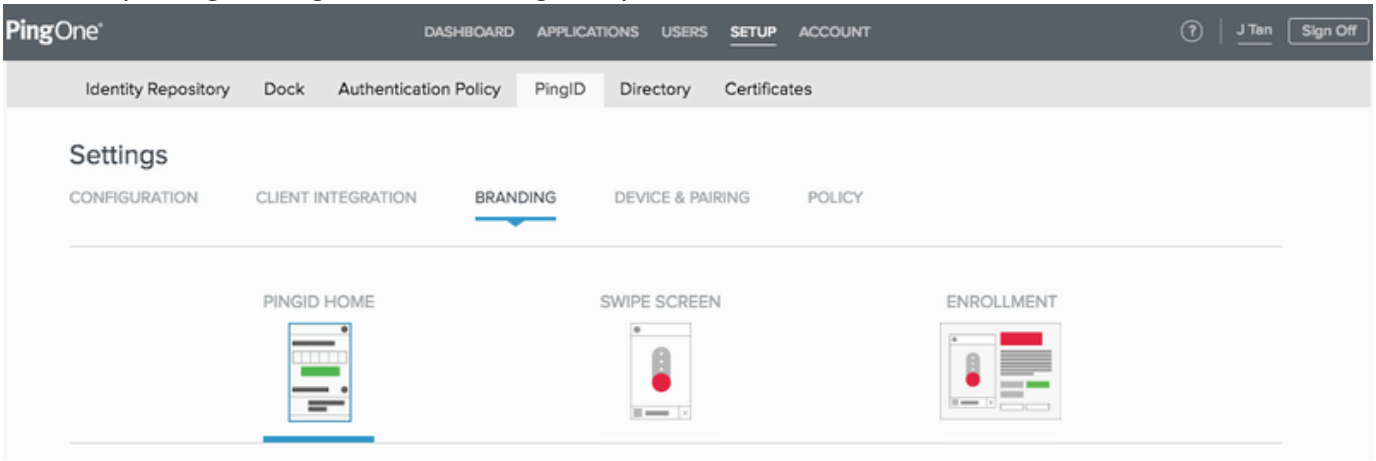
Customize the PingID mobile app swipe screen to fit the organization's logo, colors, and overall branding.

About this task

Add your organization's logo and change the background appearance by adding a background image or changing the color to fit the look and feel of your brand.

Steps

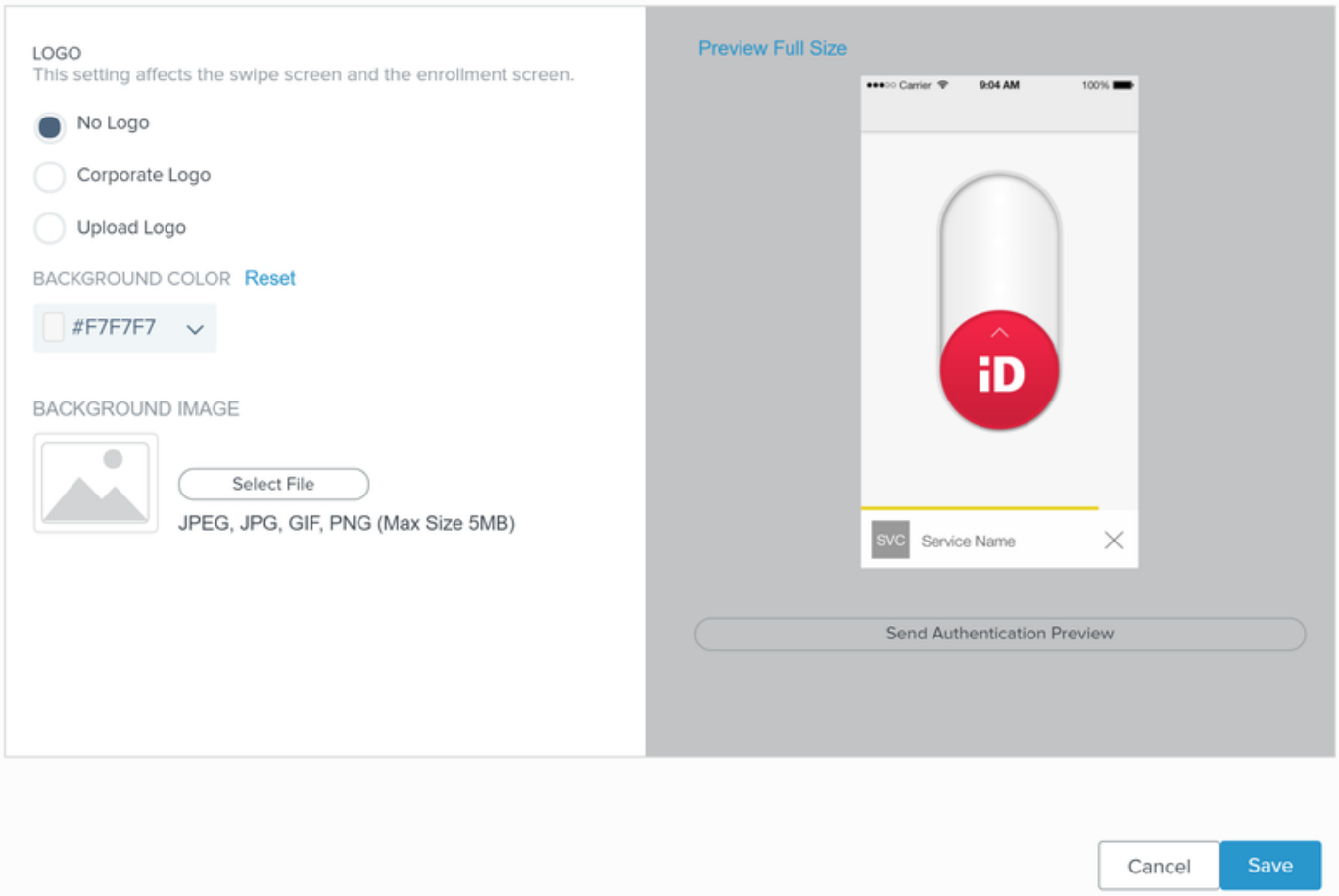
1. Go to **Setup → PingID Configuration → Branding → Swipe Screen**.

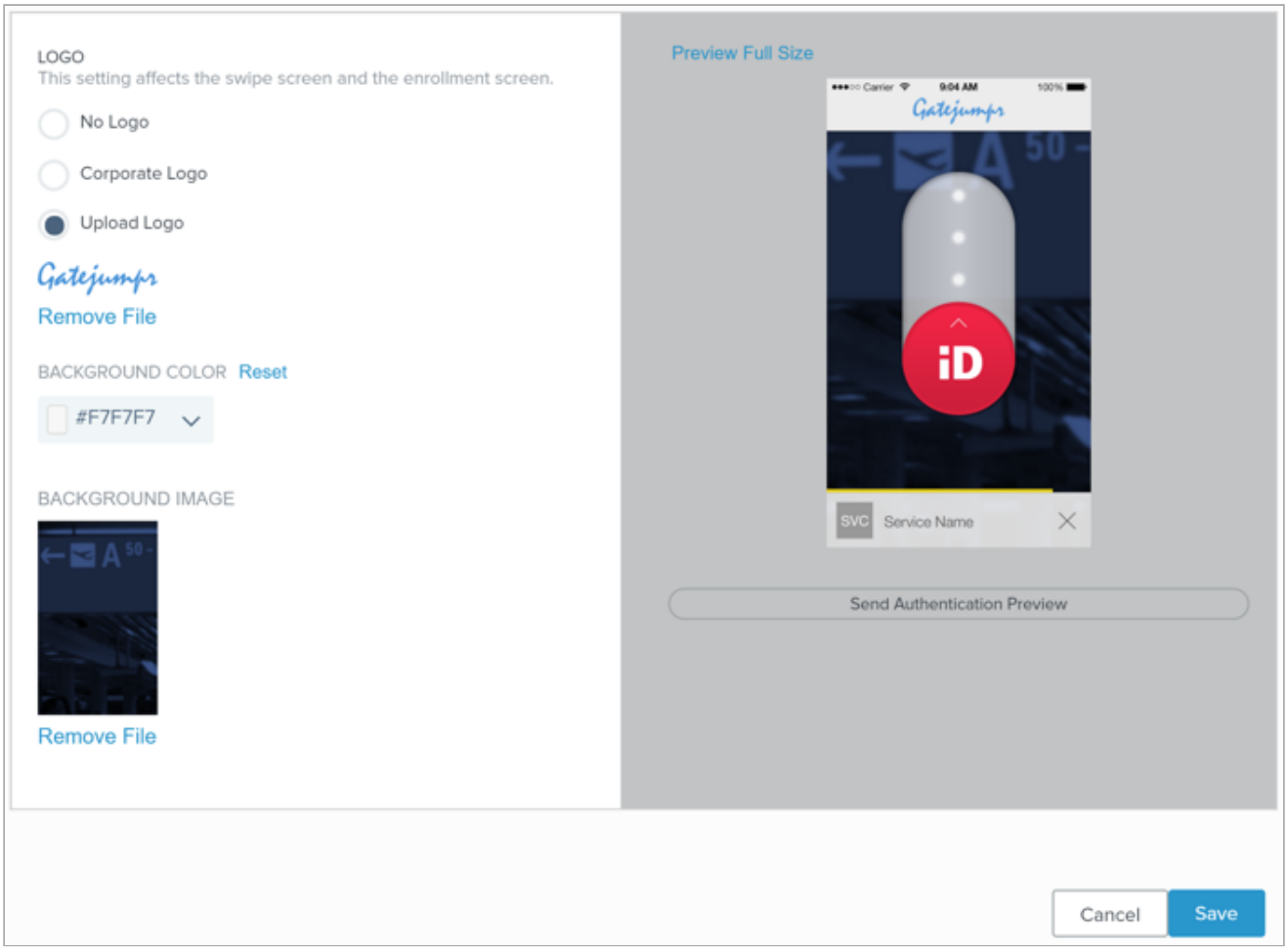


2. Customize one or more of the following elements:

Option	Description
Logo	Select the icon you want to apply to the swipe screen and enrollment page. ◦ **No Logo**: (default): do not apply a logo. ◦ **Corporate Logo**: Select to use the corporate logo configured in your PingOne dock settings. **Note** If you have not assigned a logo in the dock settings, this option is unavailable. In the PingOne Administration Guide, see Customize the Dock Settings. ◦ **Upload Logo**: To add a logo, click **Upload Logo**, navigate to the icon file you want to use, and then click **Open**. The logo can be a JPEG, JPG, GIF, or PNG file with a maximum size of 5 MB. **Important** The logo configuration applies to both the swipe screen and the enrollment screens.

Option	Description
Background Color	Customize the background color of the swipe screen. Click the **Background Color** color picker and select the background color or enter the relevant hex number. **Note** This option is only available if a background image is not selected. Click **Reset** to restore the default setting.
Background Image	Set a background image for the swipe screen. ◦ Click **Remove** to remove any existing image. ◦ Click **Select File** and navigate to the icon file you want to use. Click **Open**. **Note** The logo can be a JPEG, JPG, GIF, or PNG file with a maximum size of 5 MB.





3. To send a preview of the swipe screen to any user with PingID mobile app configured as their primary device:

    1. Click **Preview Full Size** to see your proposed changes.
    2. Click **Send Authentication Preview**.

        Result:

        The **Send Authentication Preview** modal appears.
    3. Enter the username, usually the administrator, of the user whose mobile phone will be used to display the live preview of the proposed branding configuration.
    4. Click **Send**.

        Result:

        The administrator can view the proposed changes on their mobile device.

        Click **Save**.

> **Note**
>
> Clicking **Discard Changes** in the **PingID Home**, **Swipe Screen**, or **Enrollment** windows discards any changes made in all of the windows since the last save.

Customizing the PingID Enrollment page

There are currently two versions of the PingID mobile app enrollment page - the enhanced enrollment page and the legacy enrollment page. The co-branding capabilities of the enhanced enrollment page provide administrators with additional advanced customizations of the enrollment process, including more control over text and style and a more flexible, configurable enrollment flow.

About this task

The legacy **Enrollment** page will remain available during a transition period.

> **Note**
>
> During the transition period, new organizations will see the **New Enrollment Page**. Enabling the **New Enrollment Page** disables the legacy page. To revert to the legacy **Enrollment** page, click the **Enable** toggle to off.
> The legacy enrollment page is now in maintenance mode, and only critical bugs related to the page will be handled.
> The option of using the legacy enrollment page will be removed completely on July 1, 2022, and any organizations still using the legacy enrollment page will automatically be migrated to the enhanced enrollment page. It is therefore recommended that you use the new enrollment page.
> For details on customizing the leagcy enrollment page, see Customizing the PingID enrollment page (legacy).

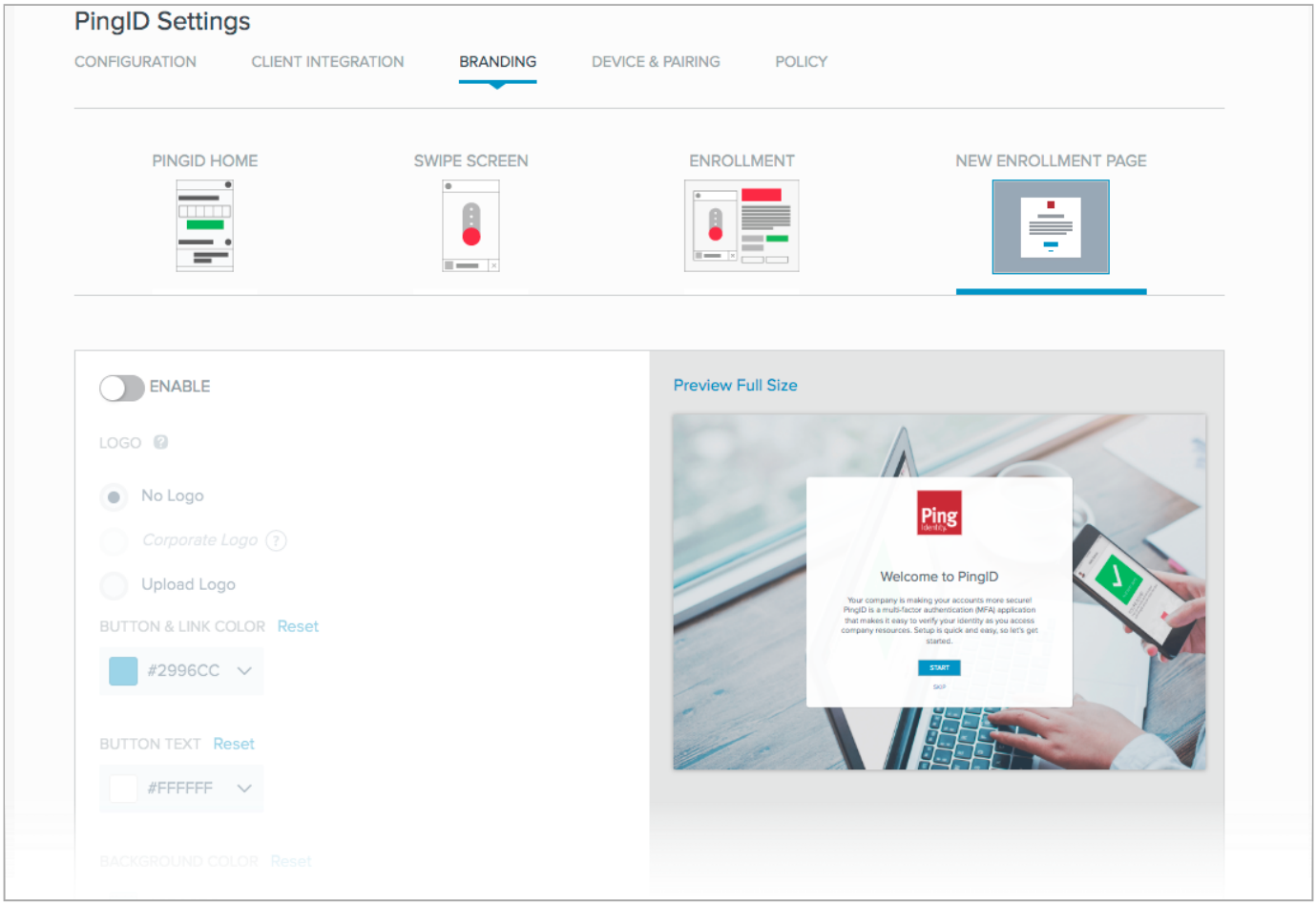
You can customize the look and feel of the PingID **Enrollment** page by:

- Adding your organization's logo
- Changing the background image or color
- Changing the enrollment **Start** button background color and text
- Changing the welcome text and color
- Changing the welcome text for multiple supported languages

To customize the PingID **Enrollment** page:

Steps

1. In the Admin console, go to **Setup → PingID → Branding → New Enrollment Page**.

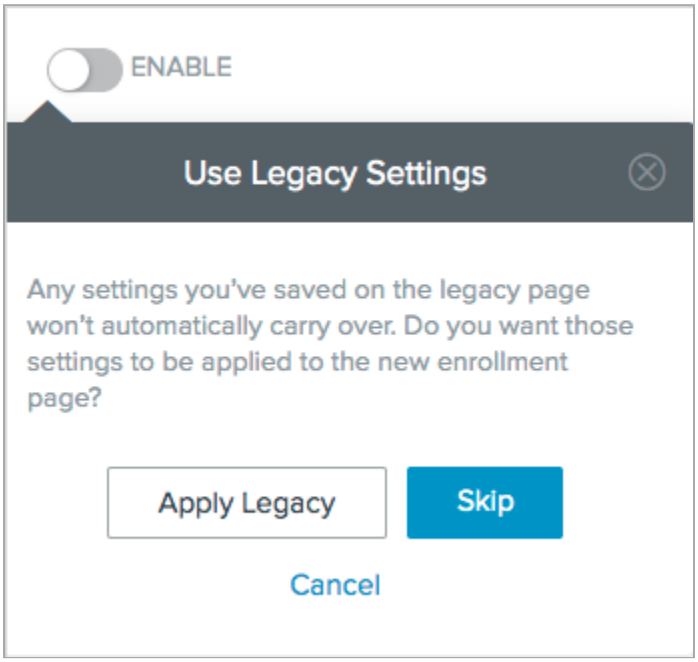


> **Note**
>
> For existing organizations, the **New Enrollment Page** is disabled with default or previous settings. For new organizations, during the transition period, it is enabled by default.

2. If you have an existing organization, click the **Enable** toggle to the on position.

   Choose from:

   - Click **Apply Legacy** to apply your relevant existing settings.
   - Click **Skip** to use the **New Enrollment Page** default settings.



3. Add your brand editing.

   For a description of the brand editing fields, see the Branding Fields section.

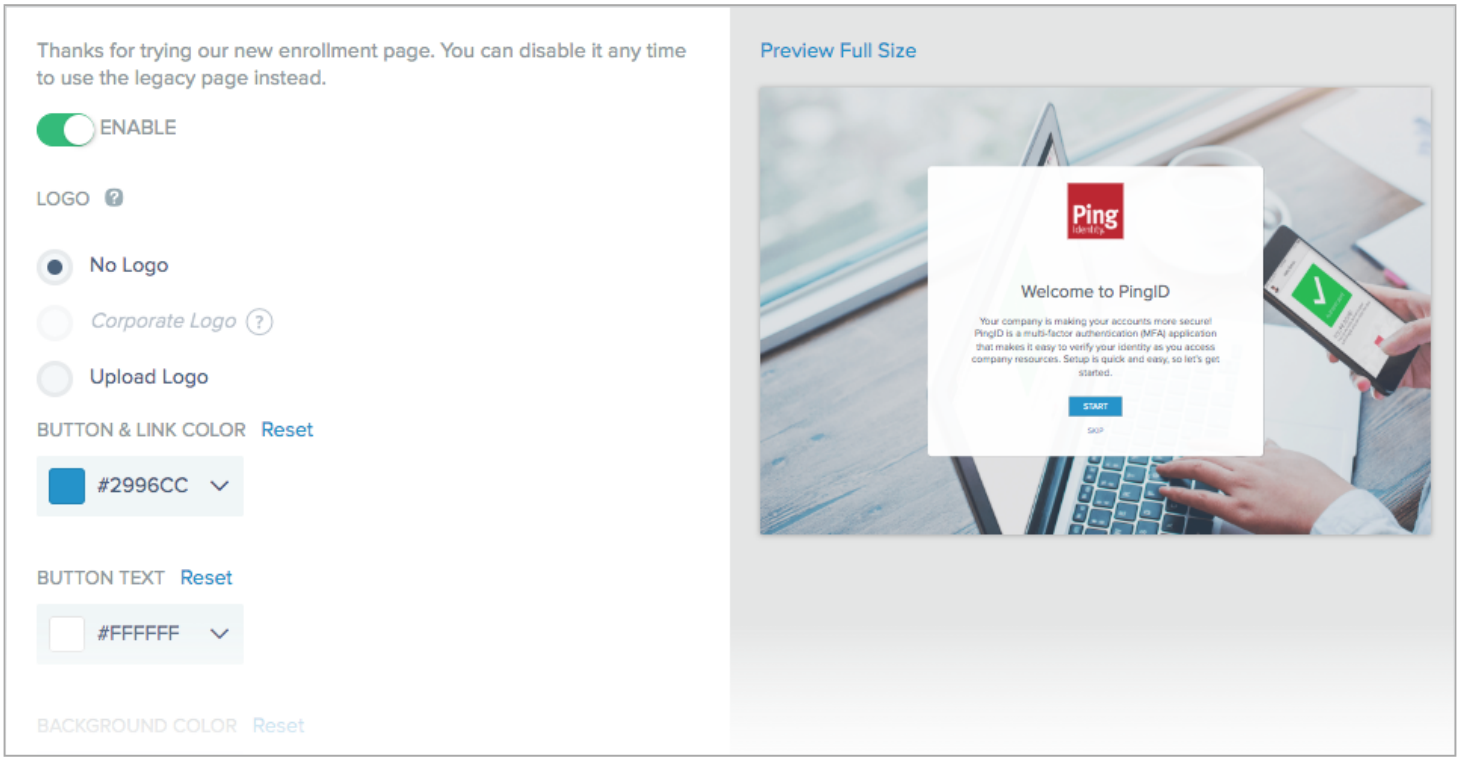
4. Click **Save**.

> **Note**
>
> To restore to the previous state, click **Discard Changes**.

Branding fields

Preview Image

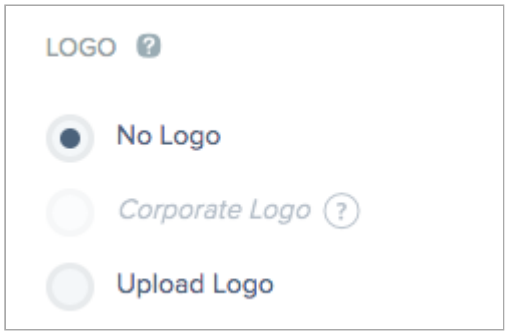
The branding fields are on the left of the page. On the right is the **Preview Full Size** image.



The **Preview Full Size** section reflects your current edits. To enlarge the preview, click anywhere inside the image. Click the image again to restore it to its original size.

> **Note**
>
> The branding fields can be entered all or in parts and in any order. Click **Save** to save your changes. Click **Discard Changes** to revert to the previous state.

Logo

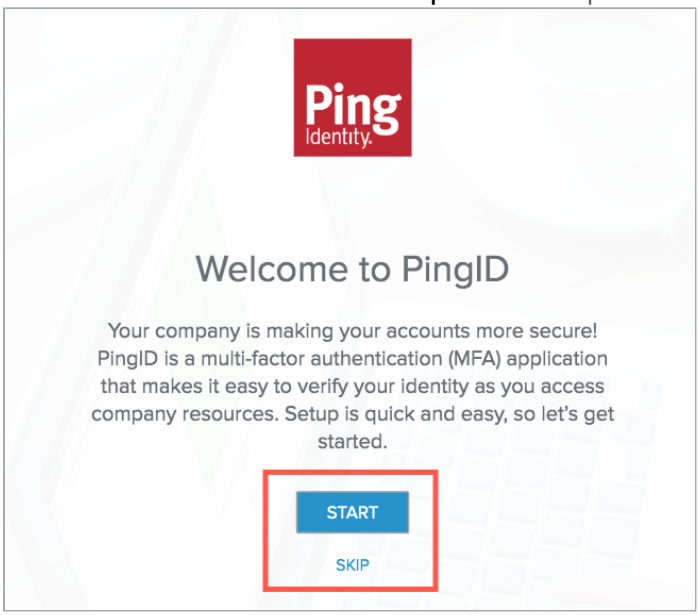


No Logo
This is the default.**Corporate Logo**
This option is available after the admin uploads the organization logo to the dock settings. For more information, see Assign branding and design in the PingOne for Enterprise Administration Guide.**Upload Logo**
When you select this option, the **Select File** button appears. Click **Select File** to select the logo image file.

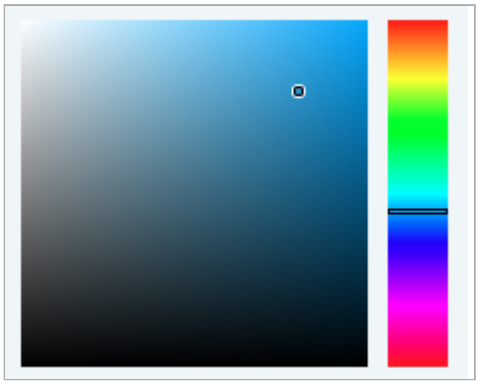
> **Note**
>
> - The logo can be a JPEG, JPG, GIF, or PNG file with a maximum size of 5 MB.
> - The logo is shared with **Swipe Screen**.

Button & Link Color, Button Text

These fields relate to the **Start** and **Skip** fields in the preview.



Click these and all subsequent color fields to open a standard color selector.



The color you select displays in hexadecimal format in the **Button & Link Color** and **Button Text** fields. You can also enter a hexadecimal number directly in the fields.

- The **Button & Link** color setting applies to the **Start** button background color and the **Skip** text color.
- The **Button Text** color applies to the **Start** button text color only.

Click **Reset** to revert to the default value.

Background Color

Click **Background Color** to open a standard color selector. Click **Reset** to restore the default setting.

> **Note**
>
> If you are using a background image, the background color does not display.

Background Image

In the **Background Image** section, click **Remove File** to remove the default image and reveal the **Select File** icon.

Click the **Select File** icon to select a background image. Click **Reset** to restore the default setting.

> **Note**
>
> If your image is truncated or distorted, you might need to physically re-size it before uploading. The PingID enrollment message background assumes a display aspect ratio of 16:9.

Text Color

Click **Text color** opens the standard color selector. This color applies to the text of the Welcome message. Click **Reset** to restore the default setting.

Customizing message texts

PingID provides customizable message texts for each of the supported languages. Currently supported languages are listed in PingOne for Enterprise language support.

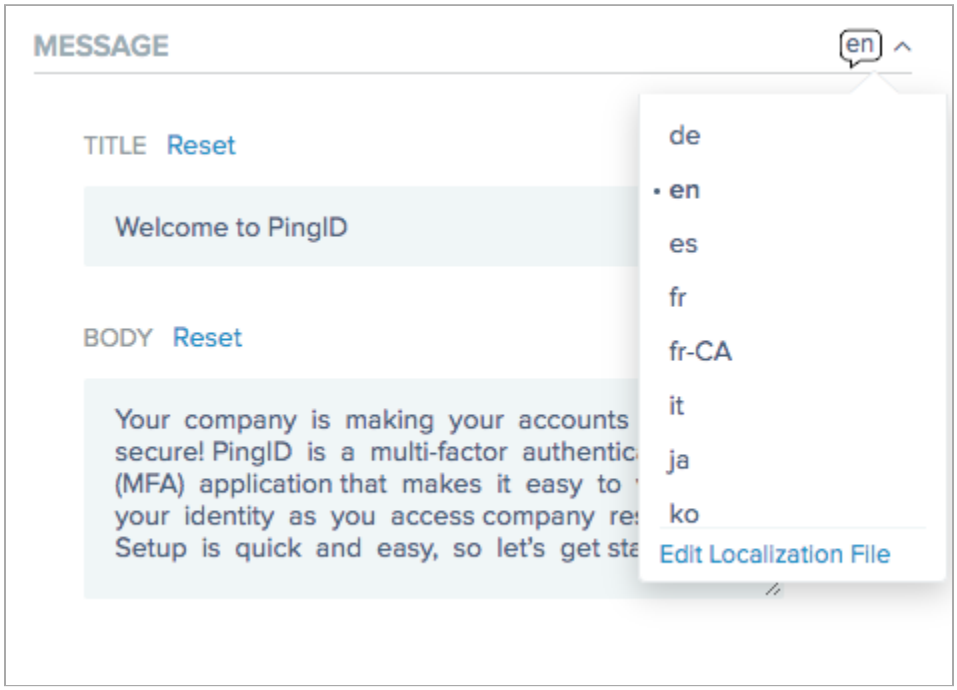
> **Note**
>
> When the end user's machine locale is set to one of the PingID supported languages, the user receives enrollment messages in the language of that locale. If the user's locale is not a PingID supported language, then the user receives enrollment messages in English.

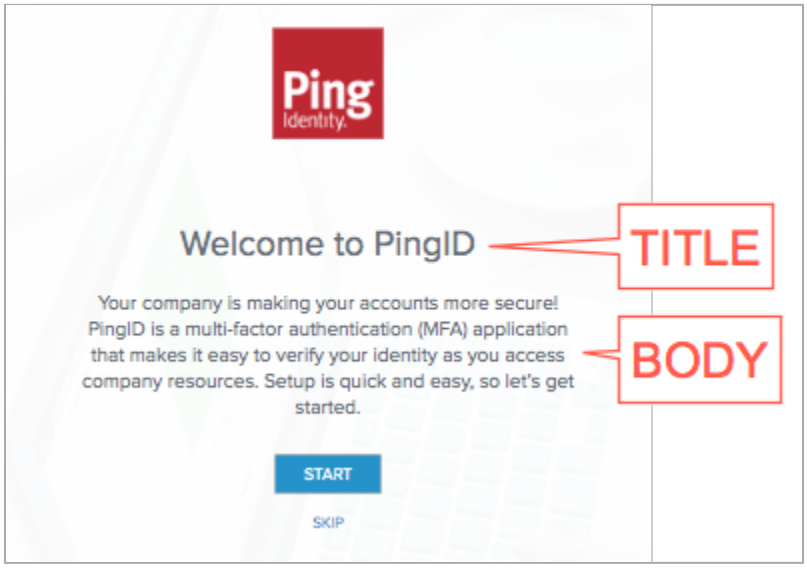
Customizing message texts online

Customize the title and body message text for your user's enrollment experience.

About this task

The **Message** section is the last item of the **New Enrollment Page**. The following image shows the **Message** section and the message preview.





Editable fields are:

Title

A short welcome message

Body

A paragraph-size message presented on the end user's device during enrollment regarding PingID's connection to the user's organization and its role in securing the user's identity. You can use regular text or HTML in this section.

To view or edit the **Title** and **Body** messages:

Steps

1. To choose a language other than English, in the **Message** section, click the language abbreviation icon, and then from the language selector list, select a language.

   Result:

   The **Title** and **Body** messages appear in the selected language.

2. Edit the text in the **Title** and **Body** fields.
3. Repeat step 2 for any other required languages.
4. Click **Save** to save your changes or **Discard Changes** to revert to the previous message.

> **Note**
>
> - There are no validation checks to verify that the entered message text is in the selected language.
> - To restore the default text for a locale, click **Reset** next to the **Title** and **Body** field headings to restore the default text.

Customizing message texts offline

You can download message text templates to edit offline for a later multi-locale upload.

About this task

> **Caution**
>
> Choose only one of either online or offline editing methods. To edit message texts online, see Customizing message texts online.

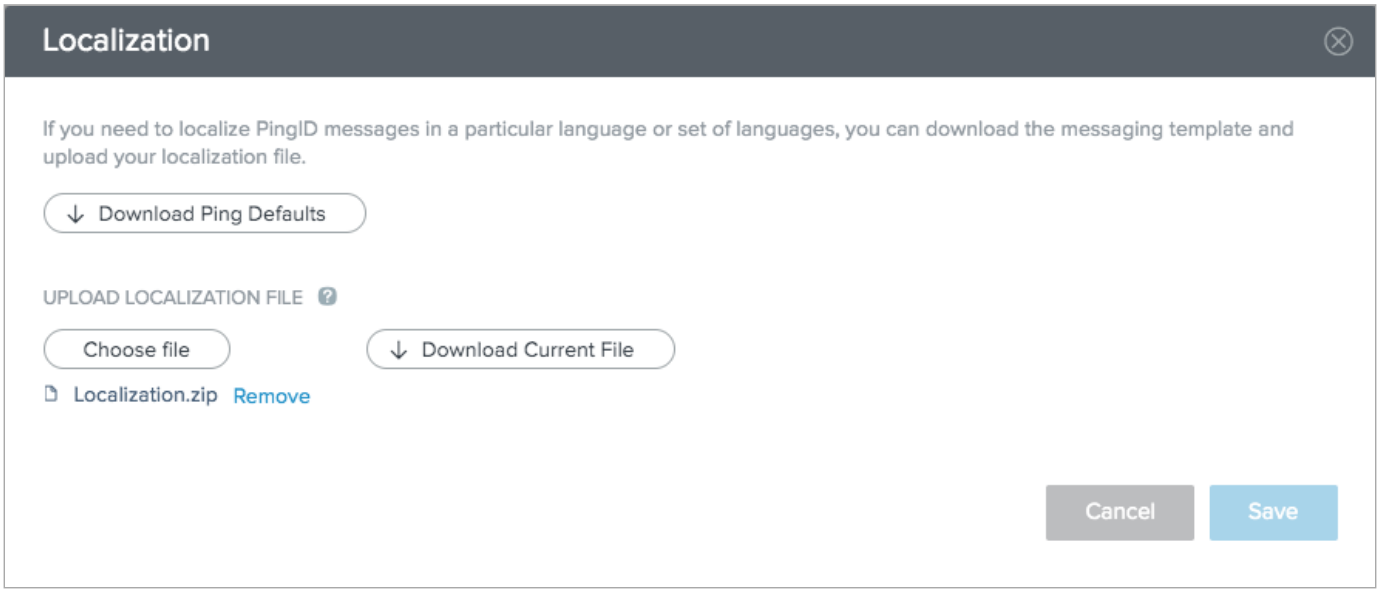
To prepare for customizing **Title** and **Body** messages offline:

Steps

1. In the languages list, select **Edit Localization File**.

   Result:

   The **Localization** dialog box opens.



2. Choose a localization file.

   Choose from:

   - Click **Download Ping Defaults** to download the PingID default message template for editing and customization.
   - Click **Download Current File** to download the current customized message texts template for further editing and customization.

     > **Note**
     >
     > The **Download Current File** button is not visible if customized message texts have not yet been uploaded or if the default PingID message texts were restored.

Result

After selecting **Download Ping Defaults**or **Download Current File**, a `.zip` file downloads containing a separate message localization file per supported language.

Creating customized messages

About this task

The localization files in the `.zip` file that you downloaded have the naming convention `Localization_<locale>.properties`.`__`

The following example shows the content of the `Localization_en.properties` file.

```
pingid.enrollment.content.body=Your  company  is  …  so let's get started.
pingid.enrollment.content.subject.line=Welcome to PingID
pingid.enrollment.content.description=Great news! … link to download PingID.
pingid.non.app.enrollment.text=I want to use a different authentication method.
```

The `pingid.enrollment.content.body` item is the **Body** text.

The `pingid.enrollment.content.subject.line` item is the **Title** text.

The remaining two lines refer to the legacy **Enrollment** page and are not relevant when using the **New Enrollment Page**.

To customize **Title** and **Body** messages offline:

Steps

1. Extract the downloaded `.zip` file.
2. Edit the `Localization_<locale>.properties` files to customize the message text.

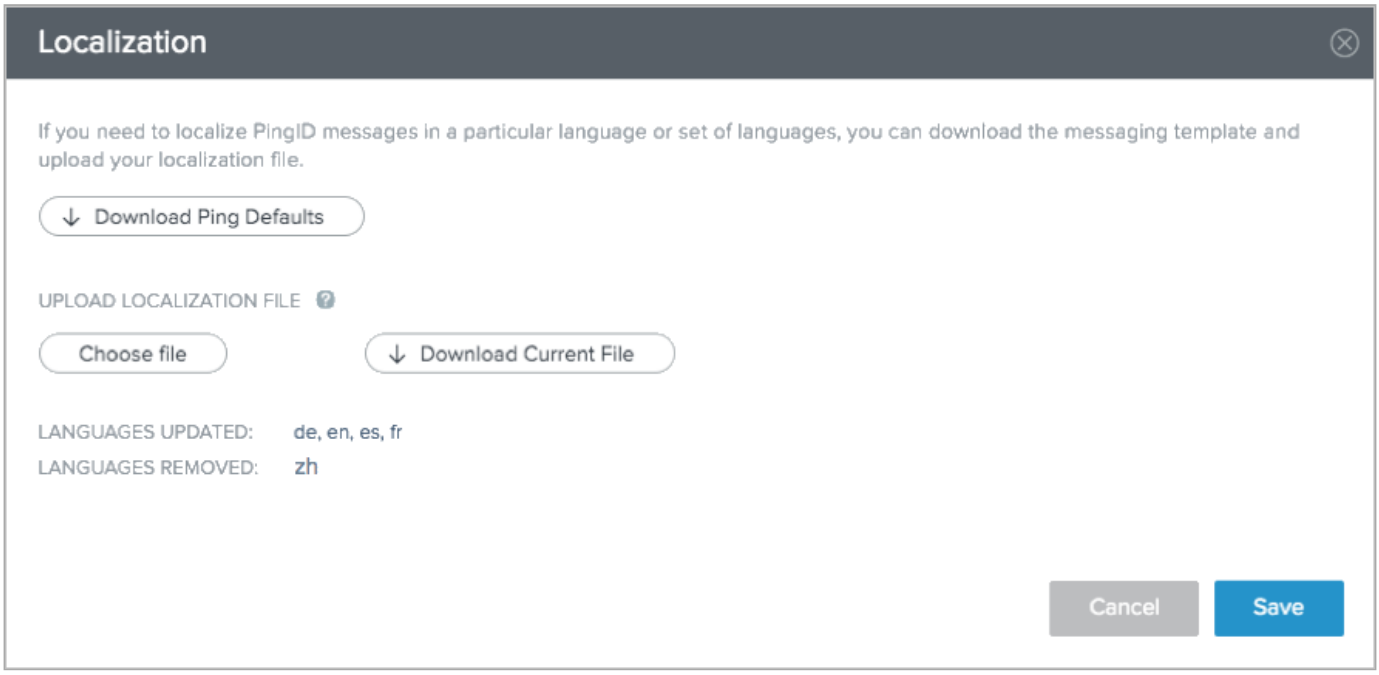
   > **Note**
   >
   > If there are errors in the field names `pingid.enrollment.content.body` and `pingid.enrollment.content.subject.line` strings, or those field names are not in the localization file, the affected message reverts to the default text for its locale.

3. Create a new `.zip` file containing your customized properties files. You can use any file name for the `.zip` file.

   > **Important**
   >
   > The `.zip` file must be a flat structure containing only the desired files.
   > - Uploading a `.zip` file with an invalid structure returns the error message `File doesn't contain any valid localizations`.
   > - Only files with file names complying with the `Localization_<locale>.properties` naming convention are uploaded.
   > - Files containing file names that do not comply with the `Localization_<locale>.properties` naming convention are ignored. This permits inclusion of instruction and maintenance files in the `.zip` file, such as `readme.txt`.
   > - Localization files for unsupported locales are ignored.

4. In the **Upload Localization File** section, click **Choose File**. In the file browser that opens, select the `.zip` file that you created in step 3.

   Result:



Languages Updated

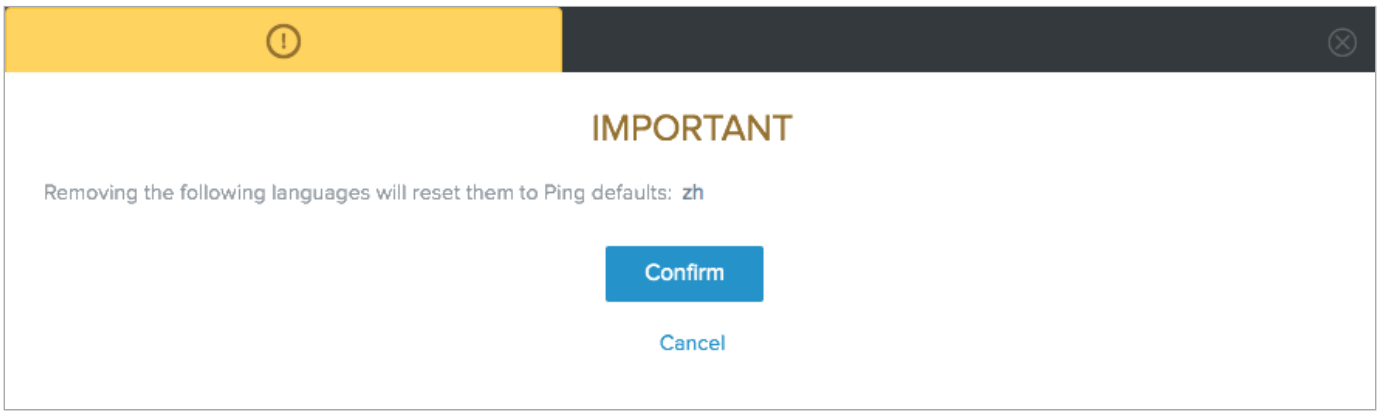
A list of the language locales whose messages change with this update.

Languages Removed

A list of the language locales whose messages restore to the default messages with this update.

5. Click **Save** to accept and upload the changes, or **Cancel** to abandon the upload.
6. If you have removed languages, click **Confirm** to complete the upload.

   Removed language messages are replaced by their defaults.



Note

- Uploading a `.zip` file of offline localization files resets online customizations for languages excluded from the `.zip` file. For example, if you make an online customization of English messages and then upload a `.zip` file that contains only a localization file for Spanish, only the Spanish messages update according to the uploaded customization. The English messages restore to the default message text.
- The system does not maintain a history of changes.

Restoring customized messages to defaults

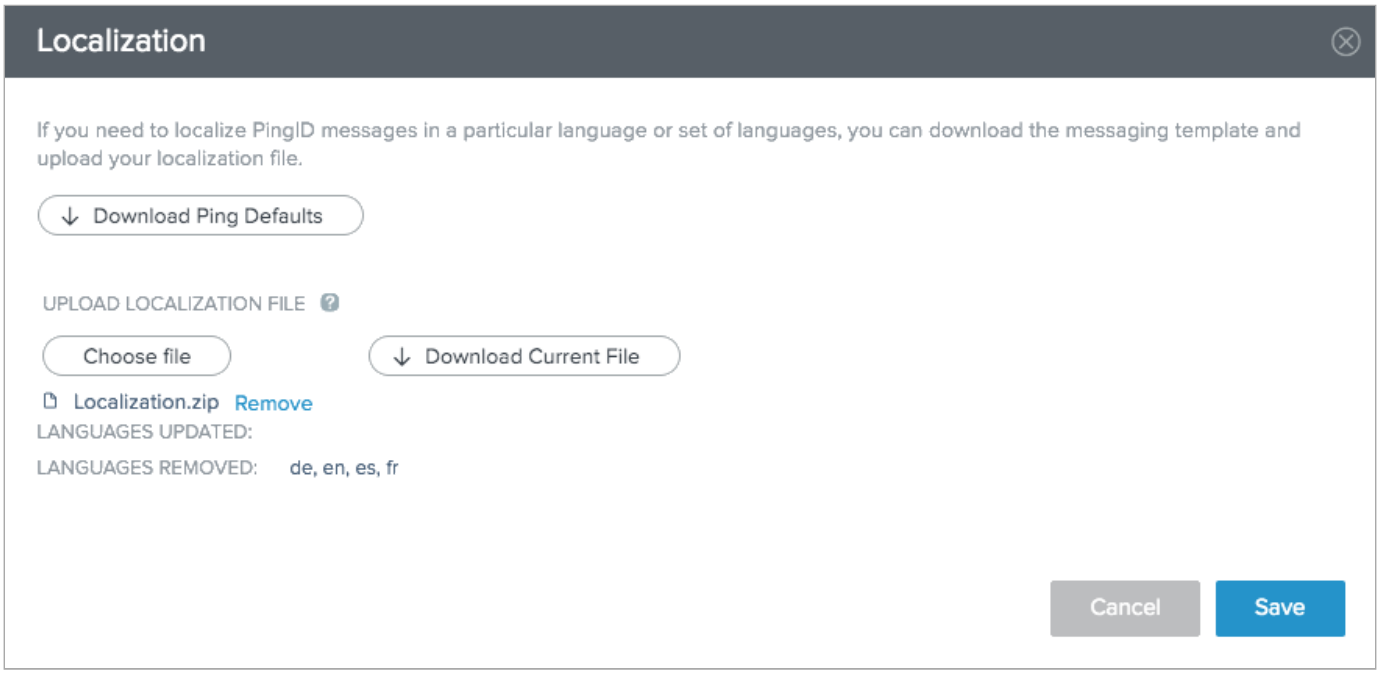
Remove current localization files to restore customized messages to defaults.

About this task

To restore customized messages to defaults:

Steps

1. Click **Remove** to restore the message texts to the original default text for all locales.



Result:

A list of the **Languages Removed**is displayed.

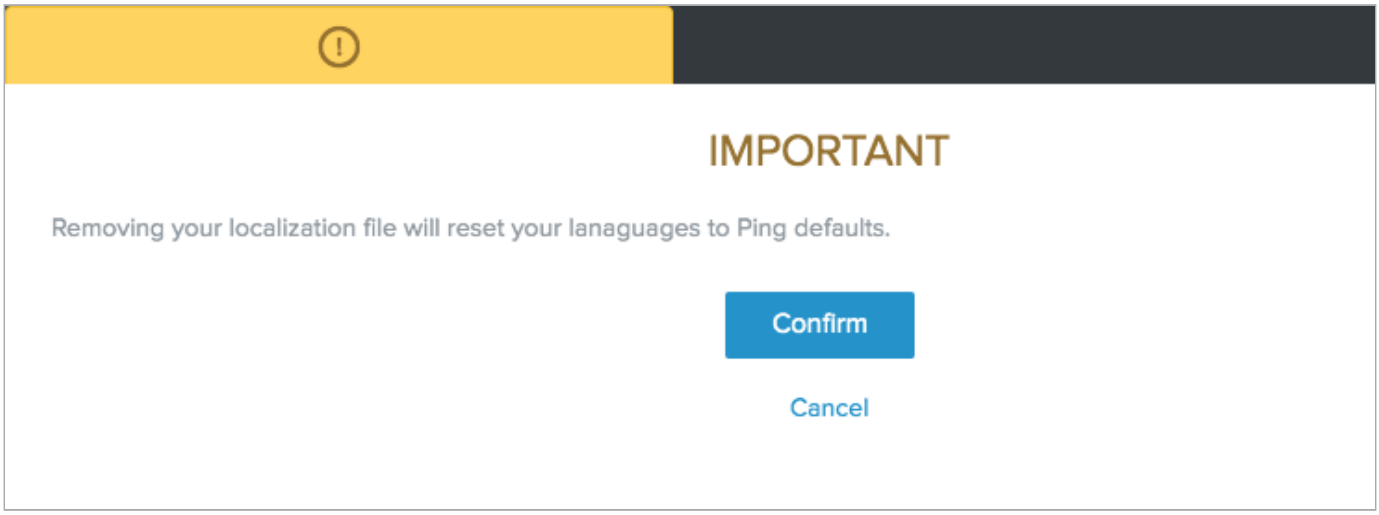
Languages Removed

A list of the language locales whose messages restore to the default messages with this update.

2. Click **Save**.

Result:

A confirmation dialog box warns that the removal of the customized localization file will restore the enrollment message text to the PingID default messages.



3. Click **Confirm**.

> **Note**
>
> You can click **Cancel** to abandon the **Remove** operation.

Reviewing customized messages

You can confirm your work by selecting each changed locale in turn and looking at the **Message** section and the **Preview** image.

Customizing the PingID enrollment page (legacy)

Customize the look and feel of the PingID mobile app enrollment page for the PingID user.

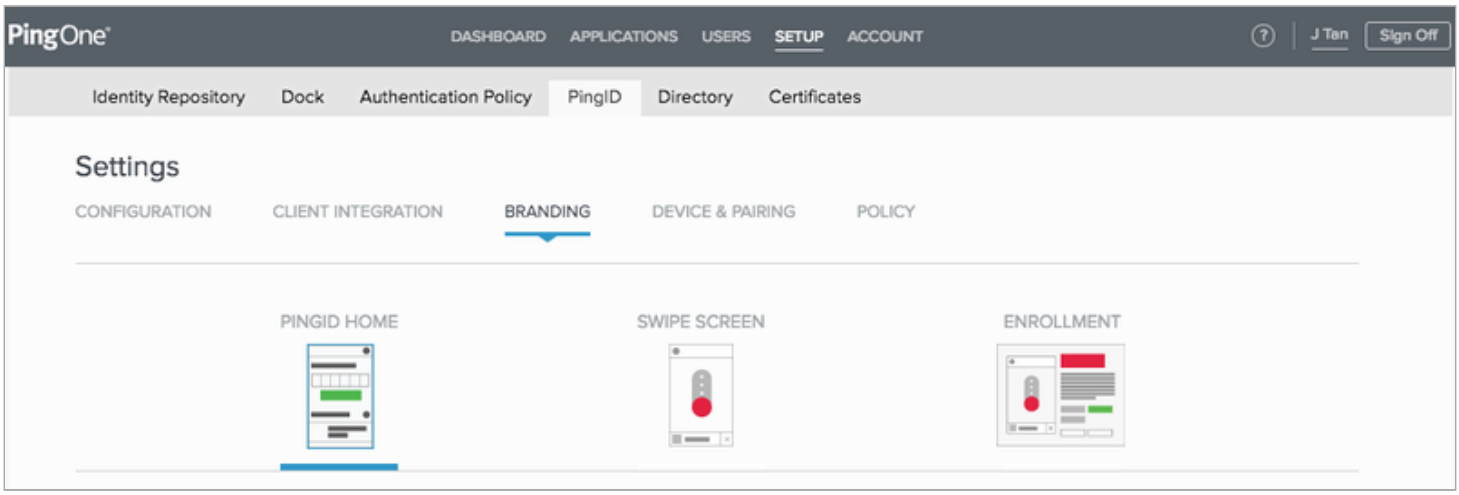
About this task

Configure the enrollment page by adding your organization's logo, changing the background appearance, and adding a background image or changing the color to reflect your organization's branding.

> **Note**
>
> - The legacy enrollment page is now in maintenance mode, and only critical bugs related to the page will be handled. The option of using the legacy enrollment page will be removed completely on July 1, 2022, and any organizations still using the legacy enrollment page will automatically be migrated to the enhanced enrollment page. It is therefore recommended that you use the new enrollment page. For details on customizing the new enrollment page, see Customizing the PingID Enrollment page.
> - PingID Authenticator supports Content Security Policy (CSP) to prevent unverified scripts from running in the PingID environment. CSP-supported browsers will not execute custom scripts defined in the enrollment page. To benefit from the latest security enhancements, always update your web browsers to include the latest security features and security patches.

Steps

1. Go to **Setup → PingID → Branding → Enrollment**.



1. Customize one or more of the following elements:

Option	Description
Logo	Select the icon you want to apply to the swipe screen and enrollment page. ◦ **No Logo**: (default): do not apply a logo. ◦ **Corporate Logo**: Use the corporate logo configured in your PingOne dock settings. If you have not assigned a logo in the dock settings, this option is unavailable. For more information, see Customize the Dock Settings in the PingOne Administration Guide. ◦ **Upload Logo**: To add a logo, click **Upload Logo**, navigate to the icon file you want to use, and then click **Open**. The logo can be a JPEG, JPG, GIF, or PNG file with a maximum size of 5 MB. **Important** The logo configuration applies to both the swipe screen and the enrollment page.
Download Link Button	Customize the look and feel of the **Get Download Link** button. ◦ To change the button background color, click the left color picker and select the background color or enter the relevant hex number. ◦ To change the button text color, click the right color picker and select the text color or enter the relevant hex number. ◦ Click **Reset** to restore the default values.

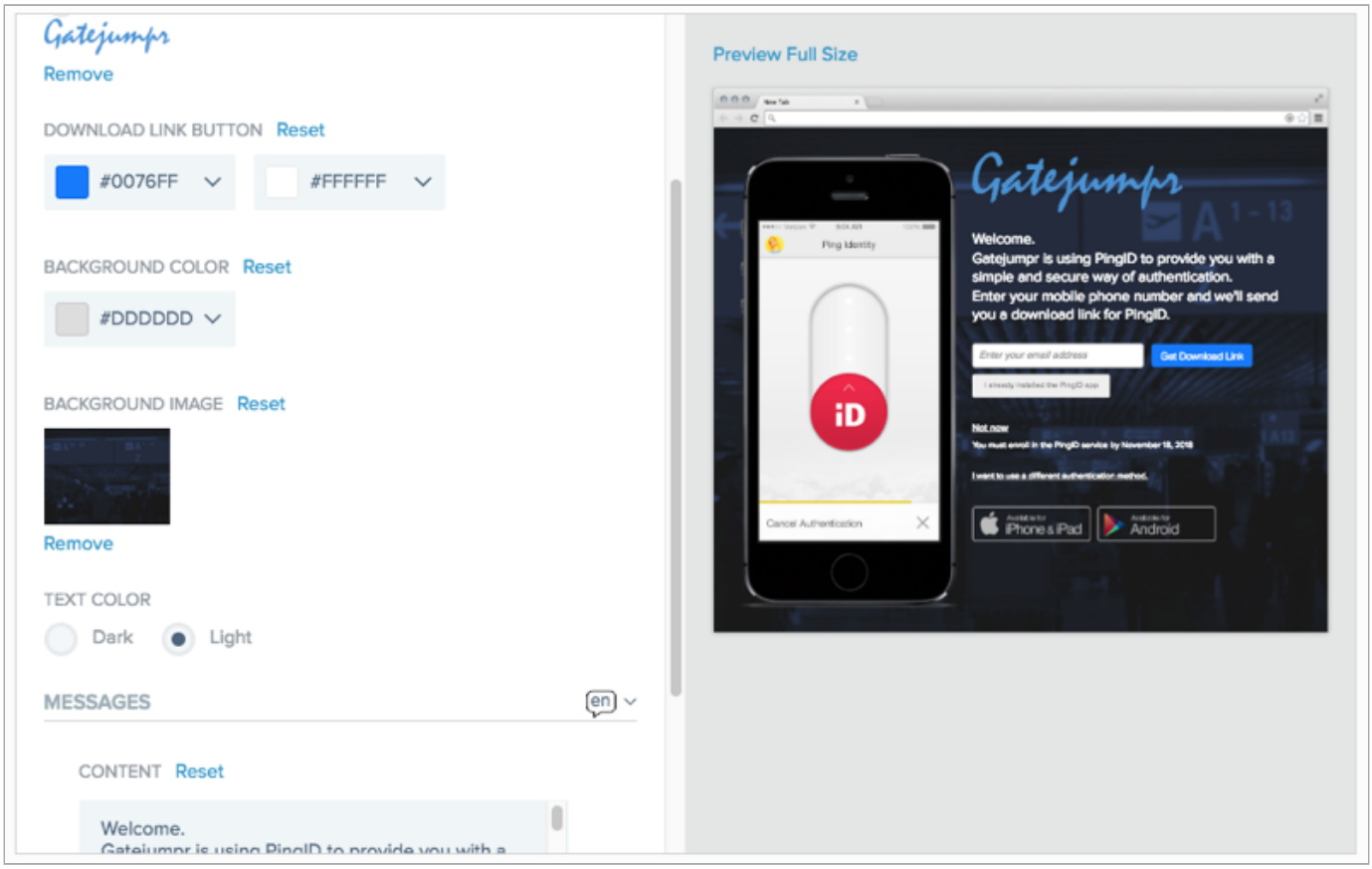
Option	Description
Background Color	Customize the background color of the enrollment page, click the**Background Color** color picker and, select the background color or enter the relevant hex number. **Note** This option is only available if a background image is not selected. Click **Reset** to restore the default setting.
Background Image	Set a background image for the enrollment page. 1. Click **Remove** to remove any existing image. 2. Click **Select File**, navigate to the icon file you want to use, and then click **Open**. **Note** The logo can be a JPEG, JPG, GIF, or PNG file with a maximum size of 5 MB. 3. **Text Color**: Select **Dark** or **Light** to customize the text color appearing in the Enrollment page.

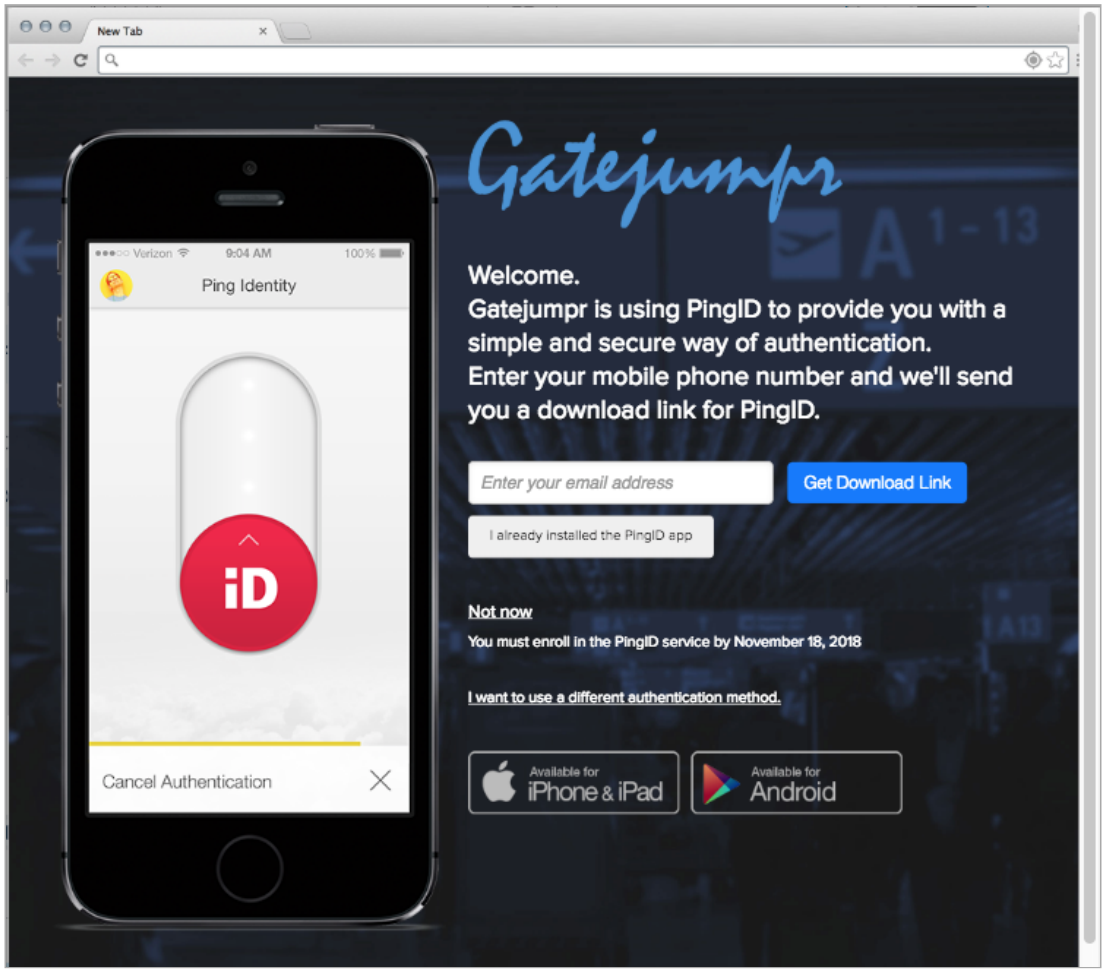
2. PingID provides customizable message texts for each of the supported languages. To customize messages on the enrollment page, see Customizing the enrollment page text by language locale.

Note

When the end user's machine's locale is set to one of PingID's supported languages, the user receives enrollment messages in that locale's language. If the user's locale is not a language supported by PingID, then the user receives enrollment messages in English.

3. Click **Preview Full Size** to preview the changes as they will appear on your organization's enrollment screen.





Click **Save**.

> **Note**
>
> Clicking **Discard Changes** in the **PingID Home**, **Swipe Screen**, or **Enrollment** windows discards any changes made in all of the windows since the last save.

Customizing the enrollment page text by language locale

When the end user's machine's locale is set to one of PingID's supported languages, the user receives enrollment messages in that locale's language. PingID provides default text for each of the supported languages. You can customize the enrollment message text per language.

About this task

Customize the text using one of the following methods:

- Using the Admin portal.
- Editing the Localization files for the languages that you want to include. See Customizing the registration language files.

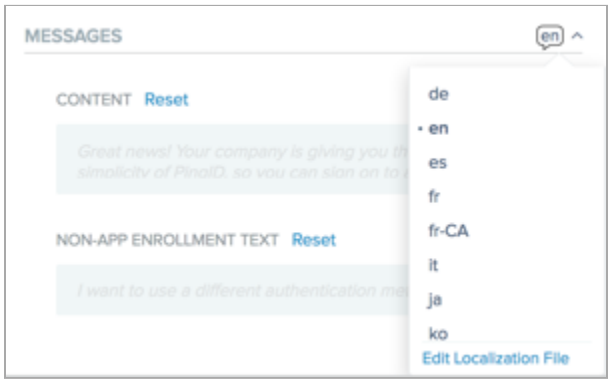
Use the same method every time you edit the language text. There are no text validation checks to verify that the text is in the selected language.

> **Note**
>
> If the user's locale is not a language supported by PingID, or no text is defined for a supported language, the enrollment page uses the English language text.

To customize the enrollment message text using the Admin portal:

Steps

1. Go to **Setup → PingID → BRANDING → ENROLLMENT**.
2. For each language that you want to edit:
    1. From the language selector list ( ), select the language you want to edit.



    2. Enter the customized text:

    CONTENT

    Customize the text you want to display in the main area of the Registration page Enrollment page.

    NON-APP ENROLLMENT TEXT

    Customize the text to display on the link presented to users who want to enroll to PingID using an authentication method other than the mobile app for an iOS or Android device. The text is updated in the preview page for the selected language.

3. Repeat step 2 for each language that you want to customize.
4. To see a preview of the text for each language, from the language selector list ( ), select the language you want to preview.

    The text updates automatically.

5. To restore the default text for a specific locale, select the locale and then next to the **Content** or **Non-App Enrollment Text** field, click **Reset**.
6. Click **Save**.

Customizing the registration language files

To localize the PingID registration messages in one or more languages, download the localization messaging template, customize the languages that you want to change, and then upload them through the Admin console enrollment configuration workflow.

About this task

When uploading a localization file:

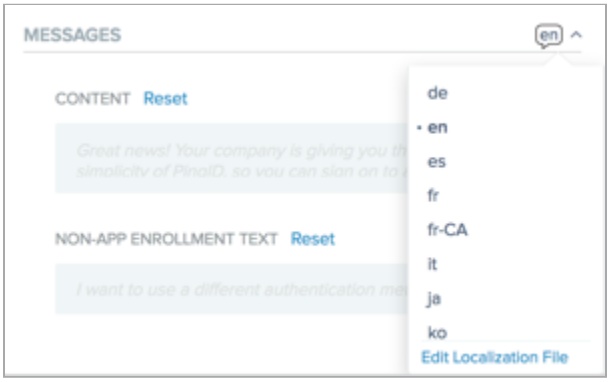
- Attempting to upload an invalid `.zip` file structure returns the error message `File doesn't contain any valid localizations`.
- If a localization file does not comply with the `Localization_<locale>.properties` naming convention, it is ignored.
- You can include instruction and maintenance files, such as `readme.txt`, in the `.zip` file.
- Localization files for unsupported locales are ignored.

Important

Customizations that you have implemented using the Admin portal Enrollment page are reset to the default text when you customize the localization `.zip` file. Uploading a localization `.zip` file updates all languages included in the `.zip` file. Any languages that are not included in the `.zip` file are reset to the default text.
For example, if you have an online customization for English messages, and you upload a `.zip` file that contains only a localization file for Spanish, then only the Spanish messages will be updated according to the uploaded customization. The English messages will revert to the default message text.

Steps

1. Go to **Setup → PingID → Branding → Enrollment**.
2. From the language selector list ( ), select **Edit Localization File**.



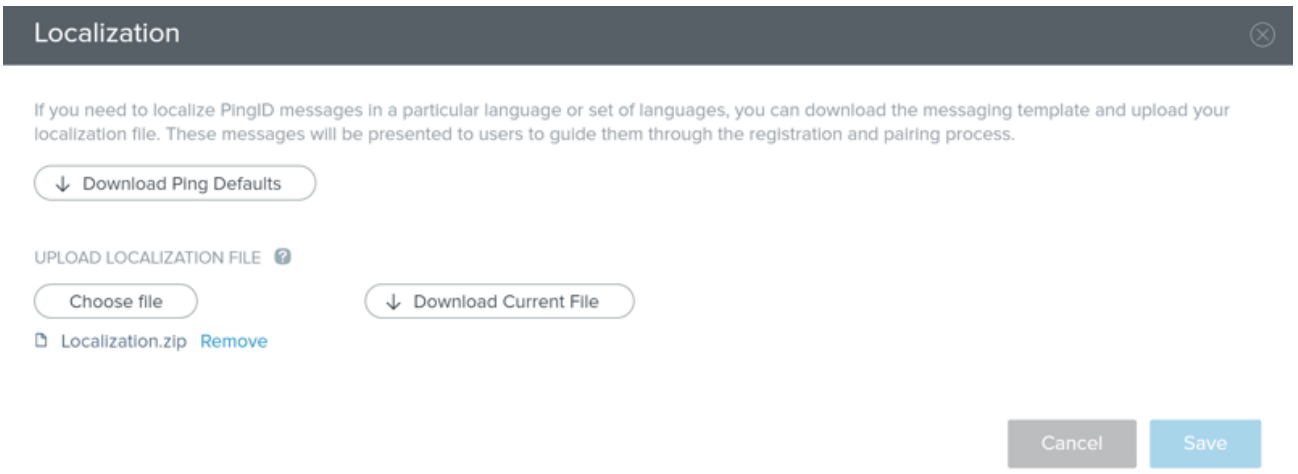
3. Choose a localization file to download:

   Choose from:

   - **Download Ping Defaults**: Download a `.zip` file of the default text templates for each of the supported languages.
   - **Download Current File**: Download the current version of the localization `.zip` file for further editing.

     Note

     This **Download Current File**option is not available if the default localization file has not been edited or the PingID localization message settings were restored to the default values.



4. Extract the localization template `.zip` file that you downloaded.

   The `.zip` file includes a separate text file for each locale.

5. For each language file that you want to edit, open the relevant properties file in a text editor and edit the following text content.

   - `pingid.enrollment.content.description=<CONTENT message text>`
   - `pingid.non.app.enrollment.text=<NON-APP ENROLLMENT TEXT link text>`

   > **Note**
   >
   > Errors in the leading `pingid.enrollment.content.description…` and `pingid.non.app.enrollment.text…` strings, or the absence of these leading strings in the localization file, causes the affected message to revert to the default text of its locale.

6. Create a `.zip` file including all of the custom localization properties files.

   > **Note**
   >
   > By default, files are named `Localization_<locale>.properties`. The `.zip` file must be a flat structure containing only the desired files, without any folder structures.
   > The `.zip` file must include files for all locales that do not contain the default text. If you do not include the file for a specific locale, the default text is used for that locale.

7. Upload the custom localization properties file:

   1. In the **Localization** window, in the **Upload Localization File** section, click **Choose File**. Select the `.zip` file that contains the custom `Localization_<locale>.properties` files.

      Result:

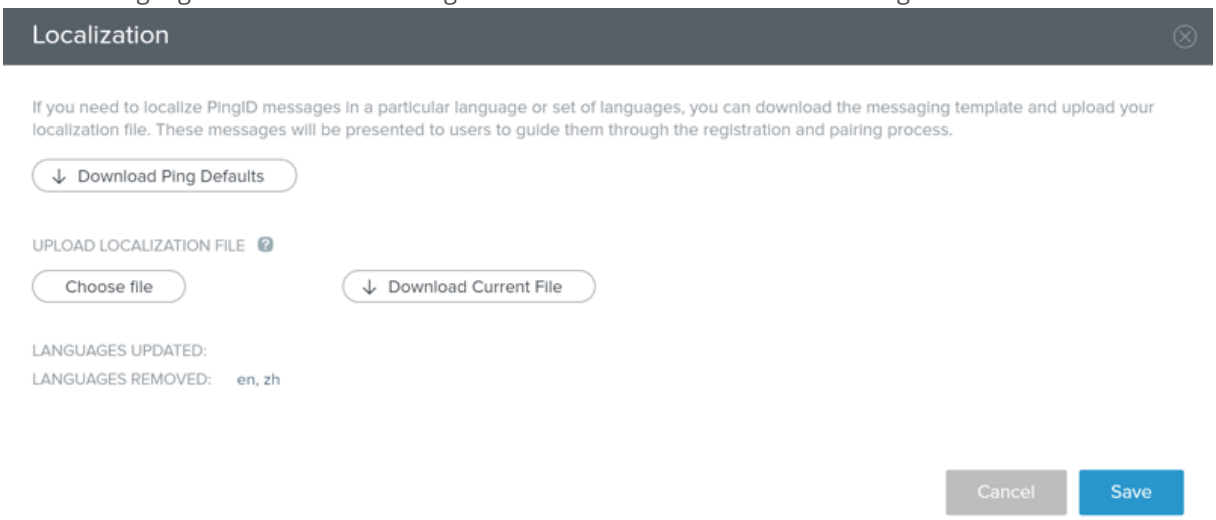
      A summary of the language files that will be modified shows the following:

      ### *Languages Updated*

      Lists the language locales whose messages will be changed

Languages Removed

Lists the language locales whose messages will be restored to the default messages



8. Click **Save**.

Restoring localization file message defaults

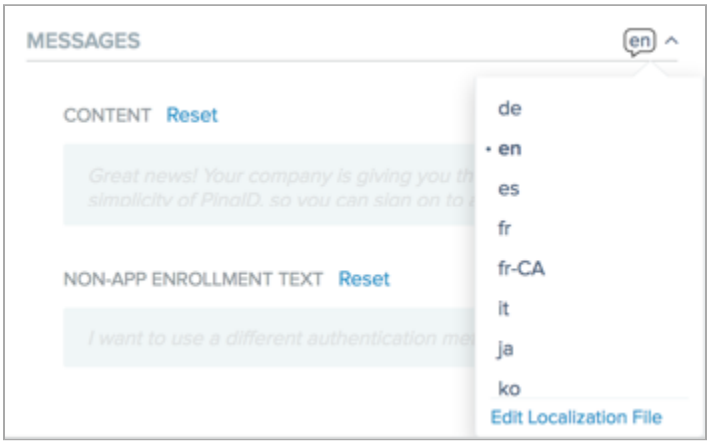
If you have customized the language for one or more locale by editing the localization file, you can restore the defaults by deleting the existing localization file for that language. Deleting the localization file restores the system defaults for all languages.

About this task

> **Note**
>
> You can also restore defaults per language from the **Enrollment** page. Select a specific language and click **Reset** next to the text you want to restore. Use only one method consistently, either through the localization file or using the Admin portal. The system does not maintain a history of changes.

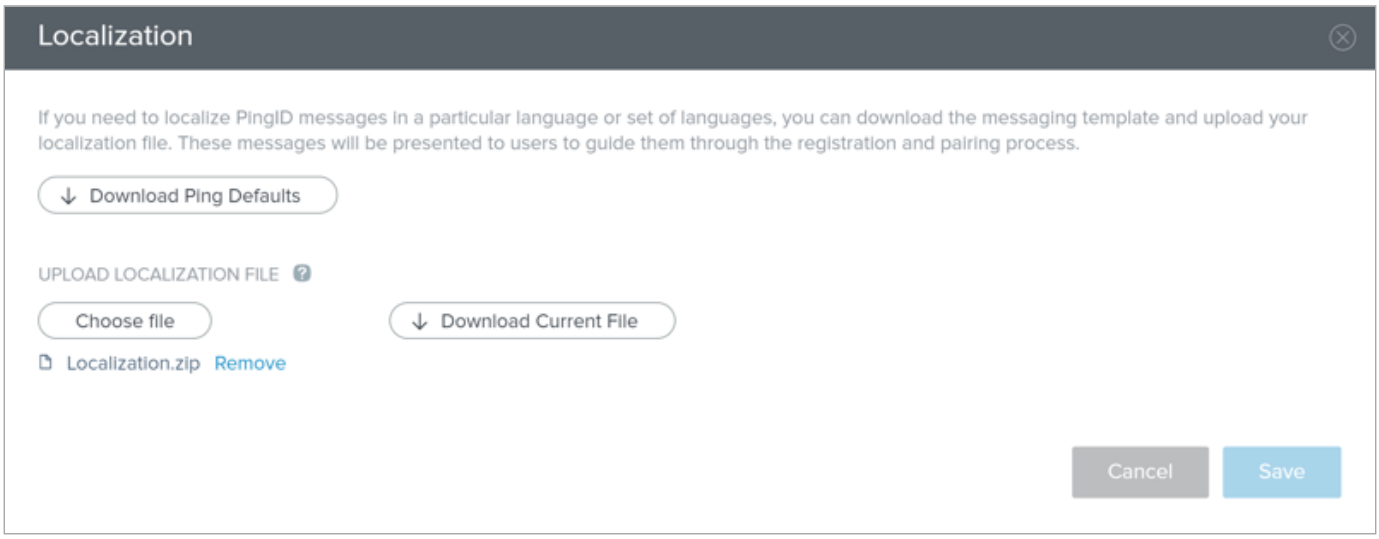
Steps

1. Go to **Setup → PingID → Branding → Enrollment**.
2. From the language selector list, select **Edit Localization File**.



Result:

The **Localization** window opens.



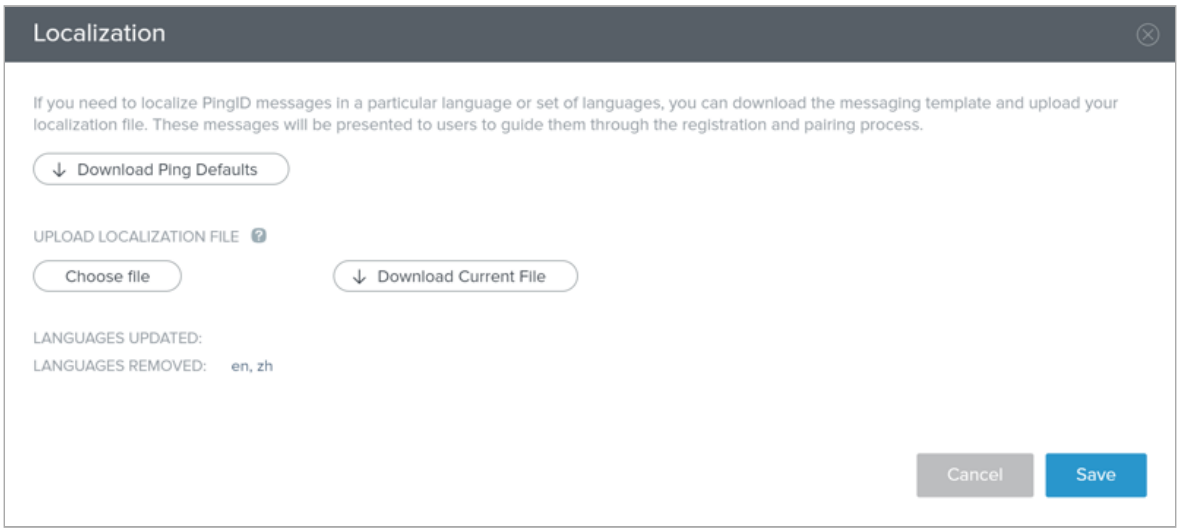
3. To restore messages text:

   Choose from:

   - To restore message text to the original for all locales, next to **Localization.zip**, click **Remove**.
   - To restore message text for one or more languages:

     1. Click **Download Current File** and extract the current localization template `.zip` file. A separate `Localization_<locale>.properties` file is included for each locale.
     2. Delete the files for the locales that you want to reset to default and then compress the remaining files.
     3. In the **Localization** window, next to **Localization.zip**, click **Remove**.
     4. Click **Choose file** and upload the new localization `.zip` file.

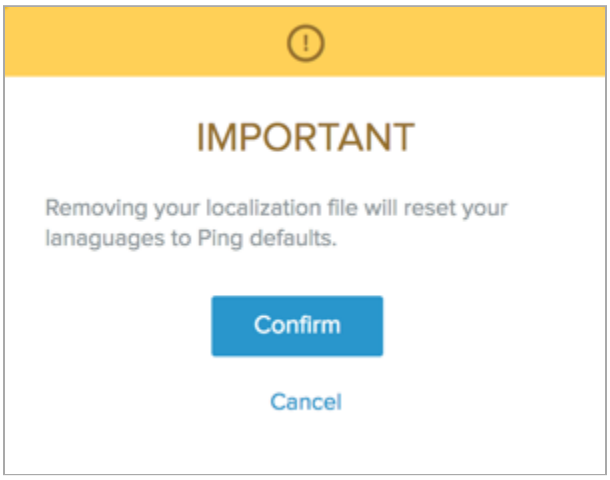
        The languages to be removed display in the **Languages Removed** section.



4. Click **Save**.
5. Click **Confirm**.

   Result:

   The following warning message displays.



Result

Your changes are applied and can be viewed in the relevant language selections in the **Enrollment** window.

PingID Reporting

You can view and run PingID Admin activity reports and user management reports.

Running the PingID Admin Activity Report

The PingID Admin Activity Report contains detailed information regarding admin-related activity.

About this task

To run the PingID Admin Activity Report:

Steps

1. In the PingOne admin console, go to **Dashboard → Reporting → Reports** to display the list of pre-defined reports.
2. On the **PingID Admin Activity of the last 7 Days** entry, click **Run**.

   Result:

   The report output is presented. See PingID Admin Activity Report fields for detailed descriptions of the report fields.

> **Note**
>
> - Customize the report output by adding optional field columns, removing default fields, and changing default runtime parameters. For more information, see Running a custom report.
> - You can stream PingID event information to Splunk or other third-party products. You can also view and analyze event information when you subscribe to PingID audit events through the PingOne subscription facility. For more information, see Subscriptions.

3. **Optional:** Click **Export** to download the report output in `.csv` format.

   Result:

   The report is saved in your browser's default downloads folder. The export process may take several minutes to complete, depending on the size of the report.

PingID Admin Activity Report fields

The PingID Admin Activity Report produces output with the following default and optional fields.

Customize the report output by adding optional field columns, removing default fields, and changing default runtime parameters. For more information, see https://docs.pingidentity.com/bundle/pingone/page/cwo1564020469709.html**Run a custom report**].

Field name	Description	Default/Optional
Timestamp	The date and time when the admin action event occurred, according to the current time zone.	Default
Admin	The email address, username, or LDAP name assigned to the administrator who performed the action.	Default
Admin Type	The type of administrator. This will be "user" unless the action was performed by a Ping Identity employee.	Default
Action	The type of resource and the action of the event. Possible values: • `account updated` • `report updated` • `user updated`	Default
Resource Name	The name of the resource on which the action was performed.	Default
Resource Type	The type of resource on which the action was performed. Possible values: • `account` • `account - authentication methods` • `report` • `user`	Default

Field name	Description	Default/Optional
Message	Detailed information regarding the action event, including the resource type, resource name, and nature of the admin action.	Default
Admin Id	The unique identifier assigned by PingOne to the administrator.	Optional
Browser Agent	The browser name and version used for PingOne SSO.	Optional
IP Address	The IP address of the host used to initiate the event.	Optional
Resource Id	The unique identifier assigned by PingOne to the resource.	Optional
Status	The status of the action. Possible values: • `SUCCESS` • `FAILURE`	Optional

Running the PingID activity report

The PingOne reporting menu allows you to run reports on PingID activity.

PingOne has two types of PingID reports:

- PingID activity report
- PingID SDK activity report

The reports provide detailed information regarding the status of PingID events, including:

- Full user life cycle management, including creating, editing, and deleting users
- Device life cycle management, including pairing and unpairing of devices
- Pairing and authentication actions. SMS and voice actions might also include price, delivery status, and carrier name.
- Sent emails include detailed delivery statuses

PingID can stream event information to Splunk. You can view and analyze this information when you subscribe to PingID audit events through the PingOne subscription facility. For more information, see Subscriptions in the PingOne for Enterprise Admin Guide.

Running a custom report

For greater flexibility than predefined reports, run a custom PingID activity report.

About this task

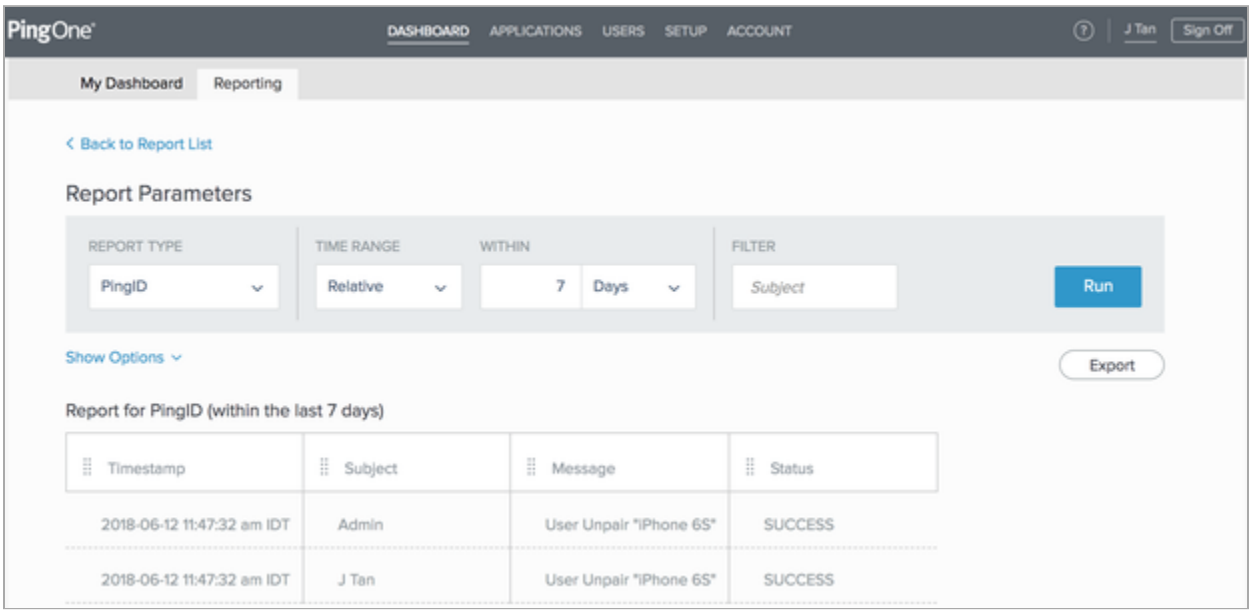
Unlike a predefined report, you must reset the specific parameters each time you run a custom report.

Steps

1. In the PingOne admin console, go to **Reporting → Reports** and click **Run New Report**.

   Result:

   The **Report Parameters** window opens.



2. In the **Report Type** list, select the type of report you want to run.
3. In the **Time Range** list, select either:

   Choose from:

   - **Specific Date**: Select or enter dates in the **Start** and **End** date pickers.
   - **Relative**: Enter a numerical value and select units in the **Within** field.

4. **Optional:** To filter the **Subject** field for the selected report type, in the **Filter** field, enter the subject in full.

> **Note**
>
> If the report includes more than one subject field, the report filter is applied to the **IdP Subject** field only.

5. **Optional:** To change the time zone for this report, click **Show Options** and in the **Time Zone** list, select a time zone.
6. **Optional:** To change the fields displayed, click **Show Options**, and then in the **Select Fields** list, select the check box for the event data you want to show in the results.

   All fields are selected by default.

7. For single sign-on reports, in the **Application Name** list, select a target application.
8. Click **Run**.
9. To modify the report, change any of the previous parameters and click **Run** to update the results.
10. To export the report in `.csv` format, click **Export**.

Result:

The report is saved in your default download folder.

> **Note**
>
> The amount of data that can be exported for a report is determined either by duration or quantity. The exported data is limited to either one week's data or 500,000 lines of data, whichever is smaller.

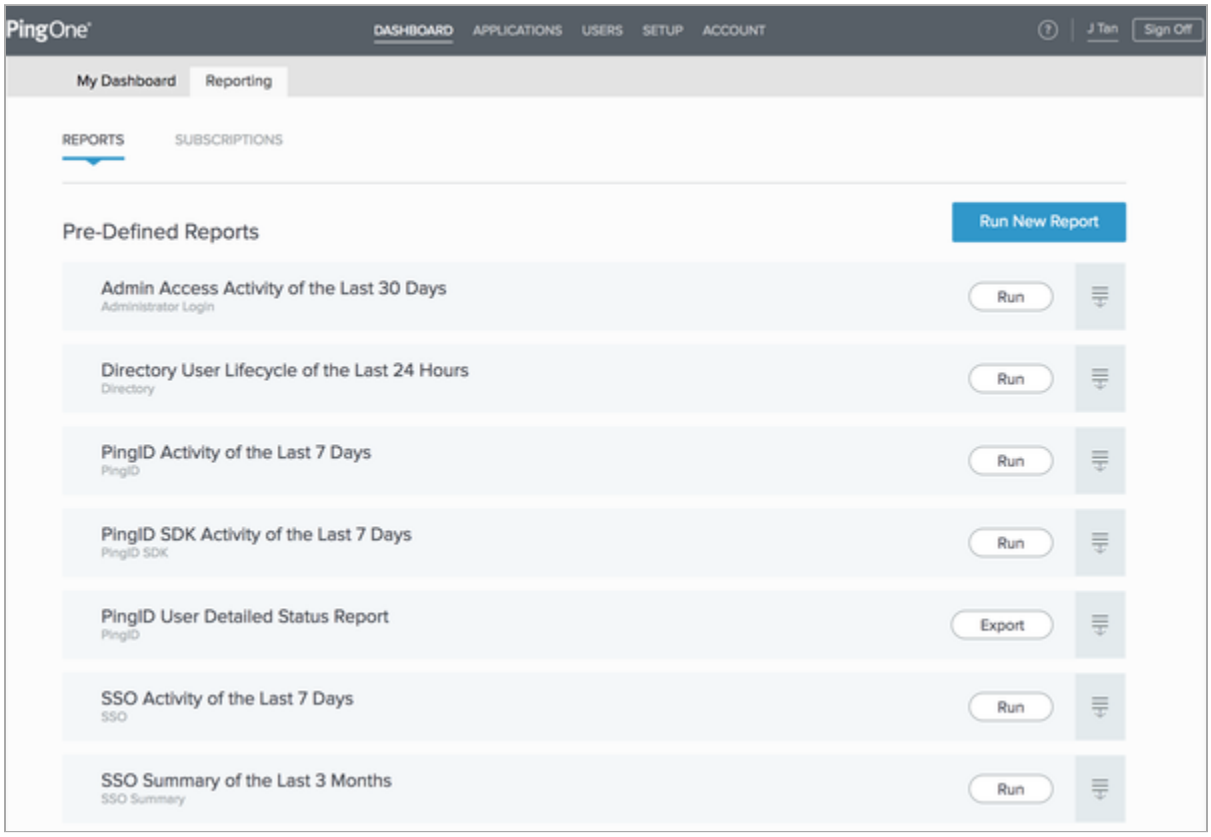
PingID report fields

The following table contains descriptions of the report fields available in PingID reports.

Field name	Description
Timestamp	Time at which the transaction occurred. Times are displayed in the time zone set in **User Settings**.
Subject	Username of the end user that authenticated using PingID.
Message	Detailed information regarding the status of the PingID transaction, including PingID registration, pairing, and authentication tasks. For successful authentication tasks, indicates the authentication method and the device used.
Status	Indicates the success or failure of the administrator or end user transaction.

Running the PingID User Detailed Status Report

The PingID User Detailed Status report provides detailed information regarding all users in the organization, details of their status and creation time, and their authentication devices.



Exporting the PingID User Detailed Status Report

About this task

The report extracts a single record per device per user in the organization. A user without any devices is listed in a single row, where the device columns are empty. All date and time values are reported according to the UTC time zone.

> **Note**
>
> For performance purposes, the report is cached for up to 2 hours. Rerunning the report within 2 hours will not produce updated results.

The PingID User Detailed Status Report cannot be customized in PingOne like other predefined reports.

Steps

1. From the Dashboard, click the **Reporting** tab.

   Result:

   You will see the PingID User Detailed Status Report in the predefined reports list.

2. Click **Export** and when prompted, save the file to the relevant location.

   The export process may take several minutes.

PingID User Detailed Status Report fields

PingID User Detailed Status Report field descriptions

Field name	Description	Type
username	The name of the user in PingID.	string
deviceId	The unique identifier of the specific device used to authenticate.	long
status	The status of the user account. The value will be identical on all rows that relate to that user. This value can be: • `ACTIVE`. The user's PingID account is created, and the user has completed registration and paired the account with a device. The user can perform any of the permitted PingID functions. • `NOT_ACTIVE`. The administrator created the user's PingID account but either the account is not yet activated, or an activation message and code was sent but the activation code has expired. • `PENDING ACTIVATION`. The user account was activated but has not been paired with a device. • `PENDING`. The user started the registration process but did not finish it, and has therefore not paired with a device. • `SUSPENDED`. The administrator suspended this user's ability to be authenticated by PingID. This may occur, for example, for security reasons if a user can't find the registered device.	string
userCreationTime	The date and time that the user was registered in PingID. If more than one row is shown per user, the value will be identical for all of the user's entries.	date and time (yyyy/MM/dd HH:mm:ss, timezone: UTC)
orgEmail	The user's contact email address. If a user has multiple devices, this email address will be identical on all rows.	string
deviceCount	The number of authentication devices registered to this user. This number should match the number of rows of devices for that user, and appear as an identical value on each of that user's device rows.	integer

Field name	Description	Type
deviceType	The type of authenticating device. The following device types are available: • Android • iPhone • SMS • Voice • YubiKey • Email • Desktop • Security Key • FIDO2 Biometrics • Hardware Token • Authenticator App	string
deviceRole	The role of the device. Possible values **Primary** or **Secondary**.	string
devicePairingDate	The date and time that the device was paired.	date and time (yyyy/MM/dd HH:mm:ss, timezone: UTC)
deviceModel	The model of the mobile device, tablet, or computer, on which the PingID App is installed.	string
osVersion	The version of the operating system of the mobile device, tablet or computer, on which the PingID App is installed.	string
appVersion	The PingID mobile app or desktop version installed on the user's mobile device, tablet, or computer.	string
countryCode	The international country dialing code for SMS or Voice authentication.	string
phoneNumber	The phone number for SMS or Voice authentication, excluding the international country dialing code.	string
yubikeySerialNumber	The serial number of the YubiKey paired with the user account.	string
deviceEmail	The email address for an email authentication device type.	string
lastTrxTime	The date and time of the most recent successful authentication activity of this user, irrespective of association with a particular authentication device. If a user has multiple devices, the date and time of the last activity will be identical on all rows. **Note**: When lastTrxTime is empty, either the user has never performed an authentication, or has last authenticated prior to October, 2018 and never since.	date and time (yyyy/MM/dd HH:mm:ss, timezone: UTC)

Field name	Description	Type
bypassUntil	For an active user, the entry in this column will be empty. If the admin has configured a user to be able to bypass PingID MFA, the date and time the bypass will expire, or has expired, is reported on each device row for that user.	date and time (yyyy/MM/dd HH:mm:ss, timezone: UTC)
lastDeviceTrxTime	The last device transaction time reflects the last time that a particular device was used for authentication. It is not necessarily the last time the user authenticated with any available device. **Note**: When lastDeviceTrxTime is empty, either the user has never performed an authentication on the specific device, or has last authenticated with the device prior to March, 2020 and never since.	date and time (yyyy/MM/dd HH:mm:ss, timezone: UTC)
fidoResidentKey	Indicates that when the security key was paired, the **Resident Key** field (in the Admin portal) was configured to **Required**. Values: `true` or `false`.This field only appears when the deviceType = Security Key.	boolean
fidoUserVerification	Indicates whether user verification has been performed successfully with the security key either during registration, or during at least one successful authentication attempt. Values: `true` or `false`.This field only appears when the deviceType = Security Key.	boolean
fidoBackupEligibility	Indicates whether the FIDO device (FIDO biometrics, or FIDO security key) supports credentials backup to the cloud.	boolean
fidoBackupState	Indicates whether the FIDO device credentials are backed up to the cloud.For devices that are already paired with PingID, these fields are updated on the fly.	boolean

Email customizations - general

Several PingID services send out emails to users.

The email sources are shown in the following table.

Email address source	Reference
RADIUS	See **Multiple Attribute Mapping Rules** in the General Parameters table of PingID RADIUS PCV parameters reference guide
PingID API	See the Add User section of PingID API - AddUser

Email address source	Reference
AD FS	See **Email Attribute** in step 4 of Configuring advanced settings
Azure AD	See step 4e of Configuring PingID MFA for Microsoft Azure AD Conditional Access
PingID for PingFed	See **Email Attribute** in step 5 of Configuring a PingID Adapter instance
PingOne SSO stand alone	https://docs.pingidentity.com/bundle/pingone/page/fml1564020492091-2.html**Connecting to an identity repository**]

Four email customizations are available:

1. Customize the email "From" address to change the default address of `noreply@pingidentity.com` to `noreply@yourdomain.com`.
2. Customize the email "Replyto" address to change the default address of `noreply@pingidentity.com` to `noreply@yourdomain.com`.
3. Customize the email "Subject" line.

> **Note**
>
> To change items 1 to 3 above, sign on to the Ping Identity Support Portal and open a case.

4. Customize the email message body. PingID supplies templates to customize the body of notification mails. To download the templates, see PingID email templates. Download the `.zip` file and extract it. The included `readme.txt` file contains a directory list of templates.

Email templates

The downloaded `.zip` file contains HTML templates for all PingID notification emails. You can view the files as-is in a web browser.

The HTML templates all use variables (replacement macros), some of which are mandatory and some are optional. The Templates variables and usage table lists each variable. NOTE: If you include images in any of the templates, they must be URL references to publicly available assets. Ping does not host the images used in templates.

After you finish editing your template, contact PingID Customer Support to upload the template.

About the table:

1. Variables are marked as follows:
    - M - mandatory
    - O - optional
    - Blank - irrelevant.

2. Variables all take the form `$[.parmname]`{variable_name}````. Mandatory variables must appear in your edited template.
3. The table shows the variables visible in the templates. All of the templates have undisplayed variables. The footnotes following the table list the undisplayed values.
4. The variable `${service-provider}` is optional for all files except `Download and Pair PinglD.html`. For `New Email Authentication Request.html`, it is also currently visible.

Templates variables and usage

Template File	Variables					Template usage		
${org-name}	${one-time-passcode}	${service-provider}	${activation-code}	${current-year}	User Paired New Device of Specific Type	Pairing	Remarks	
`webauthn_platform_android.html` (1)	M		O		O	Web: Android biometric		
`webauthn_platform_iphone.html` (1)	M		O		O	Web: iPhone FaceID		
`webauthn_platform_macintosh.html` (1)	M		O		O	Web: Mac Touch ID		
`webauthn_platform_windows.html` (1)	M		O		O	Web: Windows Hello		
`webauthn_platform.html` (1)	M		O		O	Web: Other biometric		
`webauthn.html` (1)	M		O		O	Web: Security key		
`android.html` (2)	M		O		O	Android device app		

Template File	Variables					Template usage		
`authenticatorAppEmailTemplate.html` (1)	M		O		O	Authenticator app		
`desktop.html` (3)	M		O		O	Desktop app		
`email.html` (3)	M		O		O	Authentication by email response		
`iphone.html` (2)	M		O		O	iPhone device app		
`oathTokenEmailTemplate.html` (1)	M		O		O	Authentication by OATH hardware token		
`sms.html` (3)	M		O		O	Authentication by SMS response		
`voice.html` (3)	M		O		O	Authentication by voice response		
`yubikey.html` (1)	M		O		O	Authentication using a YubiKey		
`Download and Pair PingID.html` (4)				M			When user clicks **Get Download Link** during registration	QR image required

Template File	Variables					Template usage		
`Email Authentication Pairing.html` (5)		M	O		O		Pairing code delivery is used when user clicks the **Receive passcodes via email** button during registration	One-time passcode sent by email
`New Email Authentication Request.html` (5)		M	O (Visible)		O		One-time passcode delivery during authentication	One-time passcode sent by the service provider

Notes to the table:

1. These files have the following additional optional undisplayed variables
    - `${cloudfront-url}` : Image
    - `${fraud-link}` : **Report fraud** button
2. These files have the following additional optional undisplayed variables
    - `${cloudfront-url}` : Image
    - `${device-name}`
    - `${device-details}`
    - `${fraud-link}` : **Report fraud** button
3. These files have the following additional optional undisplayed variables
    - `${cloudfront-url}` : Image
    - `${device-details}`
    - `${fraud-link}` : **Report fraud** button
4. The `Download and Pair PingID.html` file has the following additional optional undisplayed variables:
    - `${download-link-for-iphone-ipad}` : iOS download link
    - `${download-link-for-android}` : Android download link
    - `${no-scan-pairing-link}` : Link to **Finish Pairing PingID** button image
    - `${qrcode-image}` : Link to QR code image

5. These files have the following additional optional undisplayed variable:
    - `${download-link-for-android}`: Android download link

Troubleshoot PingID

This section lists common issues that end users may encounter.

Alternative authentication options not presented in "Add a New Device" dialog box

When **EMAIL** is set to **RESTRICT**, which references a `groups` attribute that has a unicode value, the alternative authentication options are not presented when the **Add a New Device** dialog box is opened from the Self Service management page.

As a workaround, the `groups` attribute should be removed from the mapping. For more information on attribute mapping, see Configuring LDAP attributes in PingFederate.

The phone number does not appear on the enrollment screen

The enrollment screen does not display pre-populated SMS or Voice phone numbers from the user directory, even though the **RESTRICT** and **PRE-POPULATE** settings are selected for **SMS** and **VOICE**, and the `phoneNumbers` attribute has been defined.

This is due to the google-libphonenumber validation method on the Self Service management page. The international country code is required, with a leading "+", unless it is a valid United States or Canadian number. When the number is set to **RESTRICT**, but flagged as invalid, this authentication option is not displayed.

> **Note**
>
> The **RESTRICT** feature only works with external identity providers.

For more information, see Configuring the phone number attribute in PingOne.

PingID Integrations

This section contains configuration details for PingID integrations.

Integrate with PingID for PingFederate SSO

Integrate PingID as an authentication solution with PingFederate either as a federation solution or as an identity bridge.

You can use PingID for PingFederate:

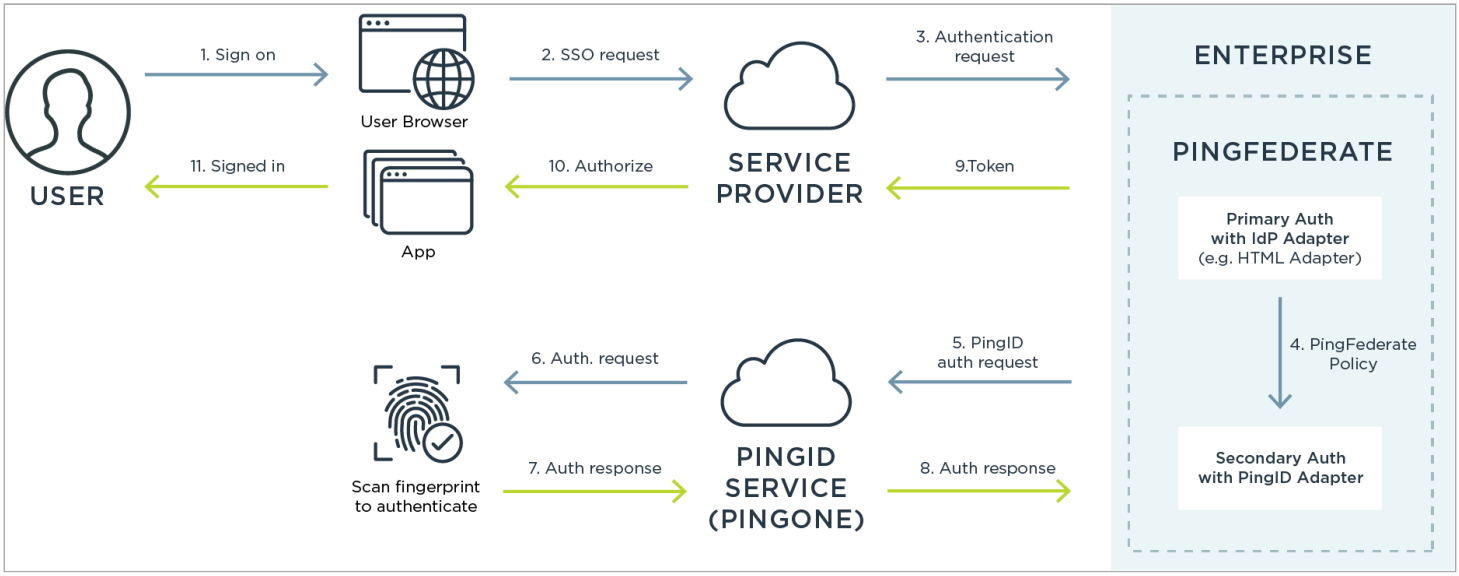
- As a secondary, or passwordless authentication solution for federated single sign-on (SSO).
- As a secondary or passwordless authentication solution when PingFederate is your PingOne identity bridge.

The process involves:

1. Registering the PingID service
2. Installing the PingID Integration Kit for PingFederate
3. Download the PingFederate properties file
4. Configuring an IdP adapter instance in PingFederate
5. Configuring a PingID Adapter instance
6. Creating a PingFederate policy contract, and creating a PingFederate policy for the relevant solution:
    - Configuring a PingFederate policy for secondary authentication
    - Configuring a PingFederate policy for passwordless authentication with FIDO2 passkeys
    - Configuring a PingFederate policy for passwordless authentication with legacy authentication methods

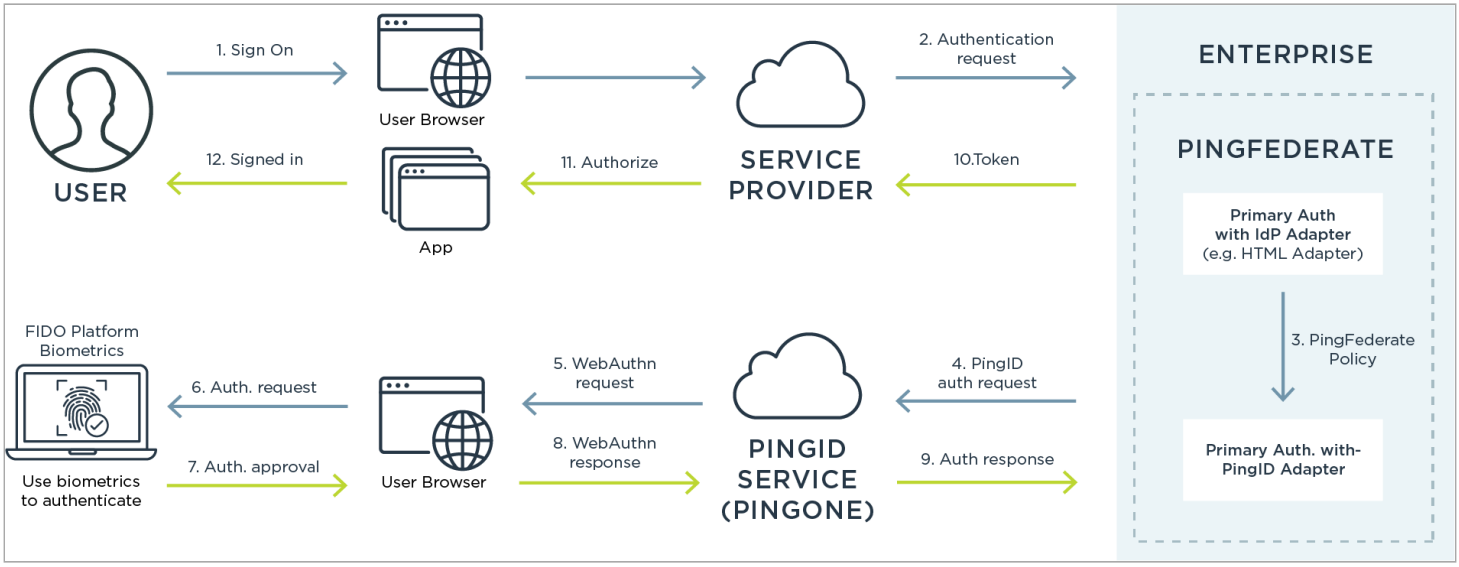
The following diagrams provide pictorial representation of secondardy and passwordless authentication solutions.

Secondary authentication



1. The user initiates the sign-on process at the user browser.
2. The user browser sends the SSO request to the SP.
3. The SP sends the authentication request to PingFederate.
4. PingFederate starts the authentication policy using an IdP adapter for primary authentication and PingID for secondary authentication with a PingID adapter.
5. PingFederate routes the authentication request to the PingID service.
6. The PingID service sends the authentication request to the PingID mobile app, and for example, the user scans their fingerprint to authenticate.
7. The PingID mobile app sends the authentication response to the PingID service.
8. The PingID service sends the authentication response to PingFederate.
9. PingFederate approves the authentication response and returns an access token to the SP.
10. The SP authorizes the app.
11. The app signs the user on.

Passwordless authentication



1. The user initiates the sign-on process in the browser at the SP.
2. The SP sends the authentication request to PingFederate.
3. PingFederate starts the authentication policy, which uses an IdP adapter for primary authentication. For more information, see Configuring a PingID Adapter instance.
4. PingFederate sends the authentication request to the PingID service (PingOne).
5. The PingID service (PingOne) sends the Web Authentication request to the user browser.
6. The user browser sends the authentication request to the FIDO platform on the user's FIDO-compatible device (for example Windows Hello, iOS and Android devices, and so on), and the user uses biometrics to authenticate.
7. The FIDO platform sends the authentication approval to the user browser.
8. The user browser sends the authentication approval response using Web Authentication protocol to the PingID service (PingOne).
9. The PingID service (PingOne) sends the authentication response to PingFederate.
10. PingFederate returns an access token to the SP.
11. The SP authorizes sign on to the app in the user browser.
12. The app signs the user on.

Managing users

Once you have PingID integrated with PingFederate, you will use the PingOne admin portal to manage users. For more information, see PingID User Life Cycle Management.

Registering the PingID service

Register for the PingID Enterprise service in PingOne, and then configure the PingID service.

About this task

If your organization is either:

- Using PingID solely as an authentication solution for federated single sign-on (SSO) with PingFederate.
- Integrating PingID for Windows login through PingFederate

you'll need to register for the PingID Enterprise service in PingOne, and then configure the PingID service. NOTE: If you're using PingFederate as your PingOne identity bridge, you already have a PingOne account and don't need to register for a PingID Enterprise account.

Steps

1. To get a registration key for the PingID Enterprise service, send an email request to sales@pingidentity.com.
2. When you've received your registration key, go to PingOne registration and in the dropdown list select **PingOne for Enterprise**, and then click **Next**.
3. Enter the following information and then click **Register** and accept the subsequent licensing agreement (see also Registering a PingOne account in the PingOne Admin guide).
    - **First Name**,**Last Name**, and**Company Name**.
    - **Data Center Region**: Select the regional data center in which you want your organization to be located.
    - **Email**: Enter your corporate email address.
    - **Registration Key**: Enter the registration key you received.
4. Configure the PingID service (See Configure the PingID service).
5. Once you have configured the PingID service, Installing the PingID Integration Kit for PingFederate

Installing the PingID Integration Kit for PingFederate

If your organization wants to use PingID as an authentication solution for federated single sign-on (SSO) with PingFederate, you must install the PingID Integration Kit.

Before you begin

> **Note**
>
> For instructions specific to the Windows Login Integration, see Installing PingID Integration Kit for PingFederate (Windows login).

PingID Integration Kit Requirements

Before you install the PingID Integration Kit:

- Register for the PingID Enterprise service on PingOne.

- Configure the PingID service and download the PingID properties file (see Managing the PingID properties file).
- Ensure you have installed the relevant PingFederate version as follows:
  - Beginning with PingID Integration Kit 2.11, PingFederate 10.0 or later is required
  - Beginning with PingID Integration Kit 2.10, PingFederate 9.3 or later is required
  - Beginning with PingID Integration Kit 2.6, PingFederate 9.2 or later is required
  - Beginning with PingID Integration Kit 1.4, PingFederate 8.4 or later is required
  - PingID Integration Kit 1.3 or earlier: requires PingFederate 8.3 or earlier (minimum supported version PingFederate 7.3)
- Ensure you have network access to your PingFederate installation.
- Ensure you have administrator permissions on PingFederate.
- Open ports:
  - 443 (outbound to Internet)
  - 1812 (UDP, to/from RADIUS clients)

> **Note**
>
> Port 1812 is required only if you plan on using the password credential validator (PCV) for RADIUS. This is the default port for RADIUS, but you also have the option of setting a different port number for the RADIUS client and RADIUS PCV. To change the port for the PCV, use the **RADIUS Server Authentication Port** option.

For further details about required web access, see PingID required domains, URLs, and ports.

About this task

If you are using PingFederate 8.2 or later, the PingID Integration Kit is bundled as part of the PingFederate installation.

If you're doing any of the following, you must install the integration kit manually:

- Updating your current version of the PingID Integration Kit to a newer version.
- Using a version of PingFederate earlier than 8.2.
- Installing the optional PingID Offline MFA feature. PingID offline MFA requires that device information be stored on the user directory for retrieval when PingID is offline. You must configure your organization's user directory to use this feature. For more information, see User directory for PingID offline MFA.

> **Note**
>
> Offline MFA requires the PingID Integration Kit 2.0 or later.

To install the integration kit to integrate PingID with your VPN, see Installing the PingID Integration Kit for VPN.

Steps

1. Download and extract the PingID Integration Kit package from the **Integrations** section of the PingID download page at https://www.pingidentity.com/en/resources/downloads/pingid.html.

2. **Optional:** If you are installing PingID offline MFA, set up the user directory by choosing one of the following methods to prepare the user directory for storage of the device information.

   For both of the following device storage methods, scripts are provided for setting up PingID offline MFA `bypass` or `block` state of the user in the directory. The **state** attribute is described in greater detail in User directory for PingID offline MFA.

   > **Note**
   >
   > Sample scripts for Active Directory are supplied in Integration Kit 2.0 and later. You can modify these scripts for specific implementations.

   Choose from:

   - Deployments where the device information is stored in an attribute on the user object class.

Setup with LDIF scripts (Active Directory only)	Manual directory setup for all directory types
Update the `<Your Location>` parameter in each of the following scripts to the location of your full DN for schemas and then run them. In the `ldif` folder: ■ `deviceAttribute.ldif` ■ `addDeviceToUser.ldif` **Note** If you are using Active Directory, run the supplied `ldif` scripts with the following command line instruction: `ldifde -i -f $<scriptname>`	1. Create a new User State attribute and link it to the user class as an optional attribute. **Note** The User State attribute can have any name. We recommend `pf-pingid-state`. ■ Attribute properties: ■ Type: `Unicode String` ■ Size: `0-64` ■ Object UID: `1.3.6.1.4.1.28867.9.2.37` 2. Create a new device list attribute in the directory named `pf-pingid-local-fallback` and link it to the user class as an optional attribute. **Note** The name of this device list attribute, `pf-pingid-local-fallback`, is mandatory. ■ Attribute properties: ■ Type: `Unicode String` ■ Size: `0-inf` (unlimited size). ■ Object UID: `1.3.6.1.4.1.28867.9.2.36`

- Deployments where device information is stored in an attribute on an object separate from that of the user. This is the same process whether the device information is in the same directory as the user object or in a separate directory.

Run the following scripts located in the `ldif` folder:

- `deviceAttribute.ldif`
- `createDeviceClass.ldif`

If you want to create a specific organizational unit (OU) to store users' device information, run the `deviceOrgUnit.ldif` script to create an OU with `CN=PingID-devices`.

Note

- You must specify in the plugin configuration where to save the new objects.
- You can either use an existing OU or create a new one.
- The name `PingID-Devices` is not mandatory. You can edit the script to change the name.
- If you are using Active Directory, execute the supplied `ldif` scripts with the following command line instruction: `ldifde -i -f ${scriptname}`

1. Create a new User State attribute and link it to the user class as an optional attribute.

   Note
   The User State attribute can have any name. We recommend `pf-pingid-state`.

   - Attribute properties:
     - Type: `Unicode String`
     - Size: `0-64`
     - Object UID: `1.3.6.1.4.1.28867.9.2.37`
2. Create a new device list attribute in the directory named `pf-pingid-local-fallback`.

   Note
   The name of this device list attribute, `pf-pingid-local-fallback`, is mandatory.

   - Attribute properties:
     - Type: `Unicode String`
     - Size: `0-inf` (unlimited size)
     - Object UID: `1.3.6.1.4.1.28867.9.2.36`
3. Create a new device class in the directory named `pf-pingid-device`.

   Note
   The name of this device list class, `pf-pingid-device`, is mandatory.

   - Class properties:
     - Object UID: `1.3.6.1.4.1.28867.9.1.3`
     - Possible superiors: `container, organizationalUnit`
     - Can contain the `pf-pingid-local-fallback` attribute.
     - In some cases to prevent a schema issue, you may need to add an identifying attribute to the `pf-pingid-device object` class, such as `cn`.
4. Device list container: Create a new OU in the directory and give it a descriptive name, such as `PingID-Devices`.

1. For Active Directory only, run the `stateAttribute.ldif` and `addStateToUser.ldif` scripts to create the `state` attribute and add the attribute to the user object class.

3. On the PingFederate host, stop the PingFederate server.
4. Remove the relevant files from the PingFederate directory, according to the version of the integration kit you are currently using:

   Choose from:

   - PingID Integration Kit 2.0 or later
   - In the `<pf_install>/server/default/deploy` directory, remove the `pf-pingid-idp-adapter-<version>.jar` and `pingid-web.war` files.
   - In the `<pf_install>/server/default/conf/template` directory, remove the `pingid-offline.auth.login.template.html` file.
   - In the `<pf_install>/server/default/conf/language-packs` directory, remove the `pingid-offline-auth-messages-<language>` files.
   - PingID Integration Kit 1.5-2.0
   - In the `<pf_install>/server/default/deploy` directory, remove the `pf-pingid-idp-adapter-<version>.jar` file.
   - PingID Integration Kit earlier than 1.5

     In the `<pf_install>/server/default/deploy` directory:

   - Remove the `pf-pingid-idp-adapter-<version>.jar` file.
   - Remove the `common-mfa-<version>.jar` file.
   - Remove the `gson-<version>.jar` file.
   - Remove the `jose4j-<version>.jar` file.
5. Copy the following files from the new `pf-pingid-integration-kit-<version>/pf-pingid-idp-adapter-<version>/dist` directory to the `<pf_install>/server/default/deploy` directory:
   - `pf-pingid-idp-adapter-<version>.jar`
   - `pingid-web.war`
6. **Optional:** If you are installing and configuring only for PingID offline MFA, before you restart the PingFederate Server:
   1. Copy the `pingid.offline.auth.login.template.html` file to the `<pf_install>/server/default/conf/template` directory.
   2. Configure the PingID offline MFA feature for language support:
      - Go to `<pf_install>/server/default/conf/language-packs`
      - For each required language:
        1. Copy the `pingfederate-messages.properties` file to the `pingfederate-messages_<language>_<region>.properties` directory according to the locales supported by Java. For example, `pingfederate-messages_fr_CA.properties`.

2. Append the content of the language file from the `dist/language-packs` directory to the appropriate properties file.

```
cat pingfederate-messages.properties pingid-offline-auth-
messages_fr_CA.properties >> pingfederate-messages_fr_CA.properties
```

> **Note**
>
> - A minimum of one language must be configured, including English.
> - Localization is supported for:
>   - English,
>   - French (EU)
>   - French (Canadian)
>   - German
>   - Japanese
>   - Chinese
>   - Dutch
>   - Italian
>   - Korean
>   - Portuguese
>   - Russian
>   - Spanish
>   - Thai

7. Restart the PingFederate server.

8. If PingFederate is deployed on clustered servers, repeat these steps for all PingFederate nodes.

Configuring a PingID Adapter instance

This topic describes how to configure a PingID Adapter instance.

Before you begin

To configure a PingID Adapter instance for integrating PingID with Windows login through PingFederate, see Configuring a PingID Adapter instance (Windows login).

About this task

- If an IdP adapter for primary authentication has not already been created, create one (see Configure an IdP adapter instance).
- (Optional)If you wish to override the default application name or application icon that the user sees when authenticating, do so in PingFederate. See Identify the target application.

Steps

1. In the PingFederate administrative console:
   - PingFederate 10.1 and higher: Click **Authentication**, and select **IdP Adapters**.
   - PingFederate 10 and lower: Under**Identity Provider** in the **INTEGRATION** area, click **Adapters**.

2. On the **IdP Adapter Instances** window, click **Create New Instance**.
3. On the **Type** tab, enter the following information, and then click **Next**:
    - **Instance Name**: The name you want to use to identify the adapter instance.
    - **Instance ID:** The adapter ID. This ID is for internal use and cannot contain spaces or non-alphanumeric characters.
    - **Type**: In the dropdown list, select the relevant PingID Adapter.
4. On the **IdP Adapter** tab, in the `PingID Properties` field, click **Choose File** and navigate to the PingID properties file you downloaded earlier (see PingFederate).

    See Configure the PingID service for instructions if you've not yet configured the PingID service.
5. If you're using LDAP to retrieve user information, click**Show Advanced Fields**, enter the information for the relevant fields, and then click **Save**.

    > **Note**
    >
    > This step enables the user email to be pre-populated in the mobile device registration page, and saves the user details, (including first name and last name), in the user listing for the PingID service.
    > - LDAP fields supply profile information to the PingID mobile device during registration (pairing a mobile device).
    > - LDAP attribute fields are case sensitive.

    - **LDAP Data Source** (Optional): Select a configured LDAP data store.

        > **Note**
        >
        > If you want greater flexibility, you can set the value of **LDAP Data Source** to "chained attributes". An example of where you can use this approach is to write OGNL expressions to define custom user groups that can be used in PingID policies (in addition to those groups defined in the directory). For more information, see Defining the IdP adapter contract.

    - **Query Directory** (Optional): The LDAP query for user information is done for every request. If this option isn't enabled, the query is only made when a PingID user cookie is not found.

        > **Note**
        >
        > If this flag is not enabled, features that rely on LDAP information may not work correctly.

    - **Base Domain**: The location that is used to search for the user, including subgroups. This attribute is equivalent to the `Search Base` attribute in Active Directory (e.g., `Base Domain: CN=Users,DC=domainname,DC=global`).

        > **Note**
        >
        > The `Base Domain` path must include at least one group, as well as the DC.

    - **Filter**: LDAP attribute used to find the LDAP entry for a specific user entity. If the**PingID User Attribute** is not defined, the attribute is also used to represent the username in PingID. For example, `userPrincipalName=${username}` ..

- **LDAP Search Scope**:
  - **OBJECT_SCOPE**: Limits the search to the base object.
  - **ONELEVEL_SCOPE**: Searches the immediate children of a base object, but excludes the base object itself.
  - **SUBTREE_SCOPE** (Default) : Searches all child objects as well as the base object.
- **Fname Attribute**: The attribute containing the user first name. For example, `givenName`.
- **Lname Attribute**: The attribute containing the user last name. For example, `sn`.
- **PingID User Attribute**: The LDAP attribute used to represent the username in PingID (for example, `User Principal Name (UPN)`, `sAMAccountName` or `objectGUID`). The value is taken from the user entity identified by the **Filter** attribute. If this field is blank, the **Filter** attribute is used.
- **Email Attribute**: The attribute containing the user email address. For example, `mail`. This email address is used during registration if users need to receive a link on their mobile device to download the PingID application.
- **Secondary Email Attribute**: An additional LDAP attribute that can be used for Email messages.
- **Group Attribute**: The LDAP attribute for group membership.
- **Phone Attribute**: The LDAP attribute of the phone number used for SMS messages, as well as voice calls if **Voice Number** attribute is left empty.

> **Note**
>
> This attribute must use the Google Library format, which dictates that all phone numbers must include '+', as well as the international country code.

- **Secondary Phone Attribute**: An additional LDAP attribute that can be used for SMS messages. If the **Secondary Voice Attribute** is undefined, this attribute is used for voice calls.
- **Yubikey Attribute**: The LDAP attribute for YubiKey (for future use).
- **Voice Number Attribute**: The LDAP attribute of the phone number used for voice calls. If left empty, the **Phone Attribute** is used for voice calls.

> **Note**
>
> This attribute must use the Google Library format, which dictates that all phone numbers must include '+', as well as the international country code.

- **Secondary Voice Attribute**: An additional LDAP attribute that can be used for Voice calls. If this attribute is undefined, the **Secondary Phone Attribute** is used for voice calls.
- **State Attribute**: The LDAP attribute that is preset in Active Directory, which is used to override how a specific user is authenticated during offline authentication.
- **PingID Heartbeat Timeout**: (Optional) Specify how many seconds to wait for a response when verifying the PingID and PingOne services. If not specified, the default is 30 seconds. If set to 0, the system default is used.

- **Authentication During Errors**: Determines how to handle user authentication requests when PingID services are unavailable. Options include:
  - **Bypass User**: Accept the user's first factor authentication, and bypass the PingID MFA flow when the PingID MFA service is unavailable.

    > **Caution**
    >
    > Requiring PingID registration while also allowing **Bypass User**may result in users being redirected to the next link in the PingFederate policy tree during a PingID service outage.

  - **Block User**: Reject and block the user's login attempt when the PingID MFA service is unavailable.
  - **Passive Offline Authentication**: Fallback to the PingID offline MFA flow when the PingID MFA service is unavailable. Users will be asked to scan a QR code with a mobile device previously registered with PingID to obtain an authentication code to authenticate.
  - **Enforce Offline Authentication**: Force PingID offline MFA flow regardless of the PingID MFA service availability.

    > **Note**
    >
    > In PingID Adapter versions older than v2.0 the **Authentication During Errors** property is called **Bypass PingID During Errors**, and if enabled, its meaning is the same as **Bypass User**.

- **Users without a paired device**: When PingID services are unavailable, choose to bypass or block users if they don't have a paired mobile device:
  - **Bypass**: bypass the PingID MFA flow when the PingID MFA service is unavailable and the user does not have a paired device.
  - **Block**: Reject and block the user's login attempt when the PingID MFA service is unavailable, and the user does not have a paired device.
- **LDAP Data Source for Devices**: The LDAP data source used for device attributes during offline authentication.
- **Encryption Key for Devices**: The Base64url encoded 256 bit key. Used to optionally encrypt the users devices list before saving to LDAP.
- **Distinguished Name Pattern**: The pattern the adapter uses to save device entries. This field is required only if the offline authentication is enabled and the offline authentication LDAP is different from the users LDAP. Example: `CN=${username},OU=PingID-Devices,DC=myDomain,DC=com`.
- **HTML Template**: The HTML template displayed to the user during offline authentication.
- **Cookie Duration**: The duration of the cookie (in days) before it expires. The default value is 1 day.
- `PingID Properties File Name`: Ensure the PingID Properties file is unique.

  > **Note**
  >
  > The PingID Properties file name must be unique for each adapter instance. This value is automatically assigned during the adapter configuration process, but when you create a hierarchical adapter configuration it doesn't reset automatically to a unique value.

- **Keep cookies at sign-off**: Prevents PingID cookies from being cleared during single logout of a user. Requires PID Adapter v2.7 or higher.

  > **Warning**
  >
  > This option prevents a full clean up of the user trace on the machine after SLO (single logout) and may expose your user accounts to additional security risks. This option should only be used with full understanding of the security implications.

- **Refresh UserId Cookie**: Refresh UserId cookie after a successful authentication. By default this option is unchecked.
- **Require PingID Registration**: (Optional) If the checkbox is selected, users that do not have at least one device paired with their account are blocked, until they successfully pair a device with their account.
- **Risk Level** (Optional): If you are using a third-party risk management service, set the value of this parameter to the name that was set in the adapter for the service.
- **Resource ID** (Optional): If you are using the PingOne Protect integration with PingFederate, this should be the name that you entered under **PingOne Risk API Response Mapping** or **PingOne Protect API Response Mapping**, on the relevant Adapter settings page.

6. (Optional) On the **Extended Contract** tab, to add attributes to the contract, for each attribute you want to add, in the**Extend the Contract** area, type the name of the attribute and click **Add**, and when finished, click **Next**.

   > **Note**
   >
   > For more information on using the**Extended Contract** screen, see Extend an IdP Adapter Contract.

7. On the**Adapter Attributes** tab in the **Pseudonym** column, select the checkbox for the subject attribute to be used as the expected identifier, then click **Next**.

   > **Note**
   >
   > On the**Adapter Attributes** tab you also have the option to mask attribute values in PingFederate log files. See Attribute masking for more information

8. On the **Adapter Contract Mapping** tab, click**Configure Adapter Contract**and then in the**Adapter Contract Mapping** window:

   1. Click **Next**, and then in the **Adapter Contract Fulfillment**tab, for each contract attribute, select the relevant **Source** value with which to fulfill your adapter contract.

9. Click **Next**, and then **Next** again to move to the **Summary** tab. Verify the information is correct and then click **Done**.
10. Click **Next** again, and then on the **Summary** tab, verify that the information is correct and click **Done** to return to the **Create Adapter Instance** screen.
11. Click **Next**, then **Done**, and then **Save**. The new adapter instance is saved.

Configuring a PingFederate policy for secondary authentication

PingID can serve as the secondary authentication source for PingFederate.

Before you begin

Before configuring PingID for secondary authentication:

- Install the PingID Integration Kit.
- Download the PingID properties file.
- Configure a PingID adapter instance.
- If an identity provider (IdP) adapter for primary authentication has not already been created, create one. For more information, see Configure an IdP adapter instance.
- If you want to configure the application name or application icon, do so in PingFederate. See Identifying the target application.

> **Note**
>
> If you want to implement a FIDO passwordless authentication flow, see (Legacy) Configuring a PingFederate policy for passwordless authentication with FIDO biometrics.

About this task

After you have created the relevant IdP and PingID adapters, create a PingFederate policy contract, and then create a PingFederate policy for secondary authentication.

> **Note**
>
> If you are running PingFederate 9.0 or earlier, you'll need to create a composite adapter rather than a PingFederate policy. See Configuring a composite adapter.

Steps

1. In PingFederate, create an Authentication Policy Contract.

   For more information, see Manage policy contracts.

   1. Go to **Authentication → Policies → Policy Contracts**.
   2. Click **Create New Contract**.
   3. In the **Contract Name** field, enter a name for the policy contract, and then click **Next**.
   4. On the **Contract Attributes** tab, for each attribute you want to add, type the name of the attribute and then click **Add**.

      For a list of PingID attributes, see PingID authentication attributes.

   5. To advance to the **Summary** tab and to review the contract, click **Next**. Click **Save**.

2. Create a PingFederate authentication policy.

   For more information, see Policies.

   1. Go to **Authentication → Policies → Policies**.
   2. Select the **IdP Authentication Policies** box, and then click **Add Policy**.

3. In the **Name** field, enter a meaningful name for the authentication policy.
4. From the **Policy** dropdown, select **IdP Adapters**, and then select your IdP Adapter from the list (for example, the HTML Form Adapter).

   Result:

   The IdP Adapter is added to the PingFederate policy tree.
5. In this new branch, perform the following.
   - From the **Fail** list, select **Done**.
   - From the **Success** list, select **IdP Adapters**, and then select your PingID Adapter instance.

     Result:

     A new PingID Adapter branch is created under the **Success** list.
6. Under the PingID Adapter branch field, click **Options**, and in the **Incoming User ID** window, perform the following.
   - From the **Source** list, select the IdP adapter.
   - From the **Attribute** list, select **username**.
   - Select the **User ID Authenticated** check box.
   - To close the window, click **Done**.
7. In the new PingID Adapter branch, perform the following.
   - From the **Fail** list, select **Done**.
   - From the **Success** list, select **Policy Contract**, and then select the policy contract you created earlier.
8. Under the PingID Adapter **Success** field, click **Contract Mapping**.
9. Complete the relevant contract mapping.

   For more information on contract mapping, see Configuring contract mapping. For a list of attributes that can be used upon successful authentication with PingID, see PingID authentication attributes.
10. To enable the policy, select the check box, and then click **Save**.

    Result:

    You return to the **Policy** window.
11. Click **Done**.

3. Add any further configurations, for example:

   Choose from:

   - Configure Browser SSO. For more information, see Configure IdP Browser SSO.
   - Configure OAuth settings. For more information, see OAuth configuration.

Configuring a PingFederate policy for passwordless authentication with FIDO2 passkeys

Configure a PingFederate policy for passwordless authentication with FIDO2 passkeys.

Before you begin

Before configuring PingID for passwordless authentication, make sure you:

- Install the PingID Integration Kit 2.7 or later.
- Download the PingID properties file.
- Configure an HTML form adapter instance.
- Configure a PingID Adapter instance.
- (Optional) If you wish to configure the application name or application icon, do so in PingFederate. Learn more in Identify the target application.
- Review the FIDO2 authentication requirements and limitations.

> **Note**
>
> The default policy's handling of null chain attributes optimizes the user authentication process by avoiding redundant LDAP queries and continuing straight to the PPM request stage. Therefore, the use of chained attributes is not permitted.

About this task

To use PingID as a passwordless authentication solution for federated single sign-on (SSO) with PingFederate, in PingFederate you'll need to:

- Create an authentication policy contract.
- Create a local identity profile and associate it with the HTML Form Adapter instance.
- Create an authentication policy.

Steps

1. Create a PingFederate authentication policy for passwordless authentication using a security key: (learn more in Policies).
    1. Go to Policies:
        - PingFederate 10.1 and higher: Click **Authentication**, and then click **Policies**.
        - PingFederate 10 and lower: In the**Identity Provider** tab, under **Authentication Policies**, click **Policies**.
    2. In the **Policies** tab, ensure the**IdP Authentication Policies** check box is selected, and then click **Add Policy**.
    3. In the **Name** field, enter a meaningful name for the authentication policy.
    4. In the **Policy** dropdown, select **IdP Adapters** and then select the**HTML Form Adapter**. A branch for the **HTML form Adapter** is added to the PingFederate policy tree, and **FAIL**/**SUCCESS** fields are added.

5. Directly under the **HTML form Adapter** field, click **Rules** and in the **Rules** popup window enter the following information, and then click **Done**:
   - **Attribute Name**: Select **policy.action**.
   - **Condition**: Select **equal to (case insensitive)**.
   - **Value**: Type **Security Key** as your authentication source.
   - **Result**: Type **Security Key** as your authentication source.
   - Select the **Default to success** check box.

   A Security Key branch is added to the PingFederate policy tree.
6. In the **HTML Form Adapter** branch **FAIL** field, click **Done**.
7. In the **HTML Form Adapter** branch **Security Key** field dropdown list, select **IdP Adapters**, and then select the PingID Adapter. **SUCCESS** and **FAIL** fields are added to the Security Key branch.
   1. Under the Security Key branch **FAIL** field, click **Done**.
   2. In the Security branch **SUCCESS** field dropdown list select the endpoint you require. For example:
      - **Policy Contracts**: Select the policy contract you created earlier and complete the relevant mapping (learn more in Configuring contract mapping).
      - **Local Identity Profiles**: Select the Local Identity Profile you created earlier and then complete the relevant mapping (learn more in Configuring local identity mapping).
8. In the **HTML Form Adapter** branch **SUCCESS** field dropdown list, select the action that you want to apply and configure it appropriately. For example:
   - If configuring the PingID Adapter (recommended), do the following:
     1. In the **SUCCESS** branch dropdown list, select **IdP Adapters** and then select**PingID Adapter**. **SUCCESS** and **FAIL** fields are added to the branch.
     2. Under the PingID Adapter **FAIL** field, click **Done**.
     3. In the PingID Adapter **SUCCESS** field, select the local identity profile you created earlier.
     4. Under the local identity profile click **Local Identity Mapping** and complete the relevant mapping with the PingID Adapter (learn more in Configuring contract mapping).

        > **Note**
        >
        > For a list of attributes that can be used upon successful authentication with PingID, see PingID authentication attributes.

     5. Under the **PingID Adapter** entry, click **Options** and specify the following fields:
        - **Source**: HTML Form Adapter
        - **Attribute**: Username
        - Make sure the **User ID Authenticated** check box is selected.

- If configuring a local identity profile:
    1. In the **SUCCESS** branch dropdown list, select the **Local Identity Profiles**, and then select the local identity profile that you created earlier.
    2. Directly under the**HTML Form Adapter** branch **SUCCESS** field click **Local Identity Mapping**, complete the relevant mapping from your source to the local identity contract, (learn more in Configuring local identity mapping), and then click **Done**.

2. Save the PingFederate policy.
3. Add any further configurations, for example:
    - Browser SSO: Configure IdP Browser SSO.
    - OAuth: OAuth configuration.

Customizing the HTML Form Adapter for passwordless authentication with a FIDO2 passkey

Customize the passwordless authentication flow by adding a passkey icon to the sign on window. You can also choose to show the passkey button when using webAuthn-compatible browsers only.

Before you begin

Before you start, create a PingFederate policy for passwordless authentication with a security key.

About this task

Add an HTML Form Adapter so that you can:

- Modify the icon to the passwordless flow button in the HTML Form Adapter to display a passkey icon.
- You can choose to show the passkey button only when the browser is WebAuthn compatible.

Steps

1. To add a passwordless authentication flow icon:
    1. Download the passkey image here and in the relevant PingFederate folder, save the icon to the `server/default/conf/template/assets/images` folder as `icon-passkey.png`.
    2. In the PingFederate folder, go to `server/default/conf/template/assets/css` and open the `main.css` file in a text editor.
    3. Add the following code to the `main.css` file, and then save the file.

```
body .button-container .social-media.SecurityKey, body .button-container .social-
media.Security.Key, body .button-container .social-media.securitykey, body .button-
container .social-media.security.key {
  background-image: url("../images/icon-passkey.png");
  background-position: left 10px center;
  background-size: 25px auto;
  font-size: 0;
  line-height: 0;
}
body .button-container .social-media.SecurityKey::after, body .button-container .social-
media.Security.Key::after, body .button-container .social-media.securitykey::after,
body .button-container .social-media.security.key::after {
  content: 'Passkey';
  font-size: 14px;
  line-height: 42px;
}
```

> **Note**
>
> The css styling can be modified in accordance with your organization's style guide.

4. (Optional) To modify the name of the passwordless authentication button that appears in the UI, in the main css file, modify the following line:

```
content: 'Passkey';
```

2. To hide the passkey button when a browser does not support WebAuthn:

   1. In the relevant PingFederate folder, go to `server/default/conf/template` and open `html.form.login.template.html` file in a text editor.

   2. In the html body add `isWebAuthnSupported();` to the `onload` attribute.

```
<body onload="setFocus();isWebAuthnSupported();isWebAuthnPlatformAuthenticatorAvailable();">
```

   3. In the `script` element, add a new function, and then save the file.

```
function isWebAuthnSupported() {
    var webauthnSupported = IsWebAuthnSupported();
    if (!webauthnSupported) {
        theElement = document.getElementById("securitykey-div");
        if (theElement) {
            theElement.style.display = "none";
        }
    }
}
```

Configuring a PingFederate policy for passwordless authentication with legacy authentication methods

Configure a PingFederate policy for passwordless authentication with FIDO biometrics or security key authentication methods.

The FIDO2 authentication method replaces the deprecated FIDO biometrics and security key authentication methods and offers expanded configuration options and support for a wide range of FIDO authentication devices, including cloud-synced FIDO devices.

- (Legacy) Configuring a PingFederate policy for passwordless authentication with FIDO biometrics
- (Legacy) Configuring a PingFederate policy for passwordless authentication with a security key

(Legacy) Configuring a PingFederate policy for passwordless authentication with FIDO biometrics

Configure a PingFederate policy for passwordless authentication with FIDO biometrics.

Before you begin

Before configuring PingID for passwordless authentication, make sure you:

- Install the PingID Integration Kit 2.7 or later.
- Download the PingID properties file.
- Configure an HTML form adapter instance.
- Configure a PingID Adapter instance.
- (Optional) If you wish to configure the application name or application icon, do so in PingFederate. See Identify the target application.
- Review the (Legacy) FIDO2 biometrics authentication requirements and limitations.

About this task

To use PingID as a passwordless authentication solution for federated single sign-on (SSO) with PingFederate, in PingFederate you'll need to:

- Create an authentication policy contract.
- Create a local identity profile and associate it with the HTML Form Adapter instance.
- Create an authentication policy.

Steps

1. In PingFederate, create an authentication policy contract: (see also Policy Contracts).
    1. In the **Identity Provider** tab, under **AUTHENTICATION POLICIES** area, click **Policy Contracts**.
    2. Click **Create New Contract**.
    3. In the**Contract Name** field, enter a name for the policy contract and click **Next**.
    4. In the **Contract Attributes** tab, for each attribute you want to add, in the **Extend the Contract** area, type the name of the attribute and then click **Add**. For a list of PingID attributes, see PingID authentication attributes.

5. Click **Next**, and then click **Done**.

2. Create a local identity profile for passwordless authentication:
    1. In the **Identity Provider** tab, click **Identity Profiles** and then click**Create New Profile**.
    2. In the **Profile Info** tab, enter the following information, and then click **Next**:
        - **Local Identity Profile Name**: Enter a meaningful name for the profile.
        - **Authentication Policy Contract**: Select your policy contract.
    3. In the**Authentication Sources** tab, in the **Authentication Source** field, enter **FIDO** as the name of your authentication source, click **Add**, and then click **Next**.
    4. Click **Done**, and then click **Save**. The local identity profile is saved.
3. In the **Identity Provider** tab, associate the HTML Form Adapter instance with the local identity profile:
    1. Click **Adapters**.
    2. Click the**HTML Form Adapter** and then click the **IdP Adapter** tab.
    3. Scroll down, and in the **Local Identity Profile** field, select the local identity profile that you created. Then click **Done**, and **Save**.
4. Create a PingFederate authentication policy for passwordless authentication. (See also Policies.)
    1. In the **Identity Provider** tab, under **Authentication Policies**, click **Policies**.
    2. In the **Policies** tab, ensure the **IdP Authentication Policies** checkbox is selected, and then click **Add Policy**.
    3. In the **Name** field, enter a meaningful name for the authentication policy.
    4. In the **Policy** dropdown, select **IdP Adapters**, and then select the **HTML Form Adapter**. A branch for the **HTML Form Adapter** is added to the PingFederate policy tree, and **FAIL**/**SUCCESS** fields are added.
    5. Directly under the **HTML Form Adapter** field, click **Rules**. In the **Rules** popup window, enter the following information, and then click **Done**:
        - **Attribute Name**: Select **policy.action**.
        - **Condition**: Select **equal to**.
        - **Value**: Enter **FIDO** as your authentication source.
        - **Result**: Enter **FIDO** as your authentication source.
        - **Default to success**: Ensure the checkbox is selected.
    6. In the **HTML Form Adapter** branch **FAIL** field, click **Done**.

7. In the **HTML Form Adapter** branch **SUCCESS** field dropdown list, select the action that you want to apply and configure it appropriately. For example:

   - If configuring the PingID Adapter (recommended), do the following:

     1. In the **SUCCESS** branch dropdown list, select **IdP Adapters**, and then select **PingID Adapter**. **SUCCESS**/**FAIL** fields are added to the branch.
     2. Under the PingID Adapter **FAIL** field, click **Done**.
     3. In the PingID Adapter **SUCCESS** field, select the local identity profile you created earlier.
     4. Under the local identity profile, click **Local Identity Mapping** and complete the relevant mapping. (See also Configuring contract mapping.)

        > **Note**
        >
        > For a list of attributes that can be used upon successful authentication with PingID, see PingID authentication attributes.

     5. Under the **PingID Adapter** entry, click **Options** and specify the following fields:

        - **Source**: HTML Form Adapter
        - **Attribute**: Username

   - If configuring a local identity profile:

     1. In the **SUCCESS** branch dropdown list, select the **Local Identity Profiles**, and then select the local identity profile that you created earlier.
     2. Directly under the **HTML Form Adapter** branch **SUCCESS** field, click **Local Identity Mapping**, complete the relevant mapping from your source to the local identity contract (see Configuring local identity mapping) and click **Done**.

        The **FIDO** policy branch is added to the policy tree.

8. In the **FIDO** branch:

   1. In the dropdown list, select **IdP Adapters**, and then select the **PingID Adapter**. **SUCCESS**/**FAIL** fields are added.
   2. In the **FAIL** field, click **Done**.
   3. In the **SUCCESS** field dropdown list, select the endpoint you require. For example:

      - **Policy Contracts**: Select the policy contract you created earlier and complete the relevant mapping. (See Policy Contracts.)
      - **Local Identity Profiles**: Select the Local Identity profile you created earlier and then complete the relevant mapping. (See Configuring local identity mapping.)

5. Save the PingFederate policy.
6. Add any further configurations, for example:

   - Browser SSO: Configure IdP Browser SSO

- OAuth: OAuth configuration

7. To complete the passwordless configuration, see (Legacy) Configuring FIDO2 passwordless authentication.

(Legacy) Configuring a PingFederate policy for passwordless authentication with a security key

Configure a PingFederate policy for passwordless authentication with a security key.

Before you begin

Before configuring PingID for passwordless authentication, make sure you do the following:

- In the PingID admin portal, configure security key for passwordless authentication.
- Install PingID Integration Kit 2.10 or later.
- Download the PingID properties file.
- Configure an HTML Form Adapter instance.
- For PingFederate 10.1 or earlier, optionally customize the HTML Form Adapter to:
  - Add a passwordless authentication flow icon for the HTML Form Adapter.
  - Only show the security key button when the browser supports WebAuthn.

  These options are automatically included in PingFederate 10.2 and later.
- Configure a PingID Adapter instance.
- Review the (Legacy) Security key authentication requirements and limitations.
- (Optional) If you wish to configure the application name or application icon, do so in PingFederate. See Identify the target application.

About this task

To use a security key with PingID as a passwordless authentication solution for federated single sign-on (SSO) with PingFederate, in PingFederate you'll need to:

- Create an authentication policy contract.
- Create a local identity profile and associate it with the HTML Form Adapter instance.
- Create an authentication policy.

Steps

1. In the PingFederate administrative console, create an authentication policy contract: (see also Policy Contracts).
   1. Got to Policy Contracts:
      - PingFederate 10.1 and higher: Click **Authentication → Policies**, and then click **Policy Contracts**.
      - PingFederate 10 and lower: In the **Identity Provider** tab, in the **Authentication Policies** area, click **Policy Contracts**.

2. Click **Create New Contract**.
3. In the**Contract Name** field, enter a name for the policy contract and click **Next**.
4. In the **Contract Attributes** tab, for each attribute you want to add, in the **Extend the Contract** area, type the name of the attribute and then click **Add**. For a list of PingID attributes, see PingID authentication attributes.
5. Click **Next**, and then click **Save**.

2. Create a local identity profile for passwordless authentication:
    1. Go to Local Identity Profiles:
        - PingFederate 10.1 and higher: Click **Authentication → Policies**, and then click **Local Identity Profiles**.
        - PingFederate 10 and lower: In the **Identity Provider** tab, click **Identity Profiles**.
    2. Click **Create New Profile**.
    3. In the**Profile Info** tab, enter the following information, and then click **Next**:
        - **Local Identity Profile Name**: enter a meaningful name for the profile.
        - **Authentication Policy Contract**: select your policy contract.
    4. In the **Authentication Sources** tab, in the **Authentication Source** field, enter **Security Key** as the name of your authentication source, click **Add**, and then click **Next**.
    5. In the **Summary** tab, click **Save** The local identity profile is saved.
3. Associate the HTML Adapter instance with the local identity profile:
    1. Go to IdP Adapters:
        - PingFederate 10.1 and higher: Click **Authentication**, and then click **IdP Adapters.**
        - PingFederate 10 and lower: In the **Security Identity Provider** tab, click **Adapters**.
    2. Click the **HTML Form Adapter**, and then click the **IdP Adapter** tab.
    3. Go to the **Local Identity Profile** field, and in the dropdown list select the local identity profile that you created.
    4. Click **Save**.
4. Create a PingFederate authentication policy for passwordless authentication using a security key: (see also Policies).
    1. Go to Policies:
        - PingFederate 10.1 and higher: Click **Authentication**, and then click **Policies**.
        - PingFederate 10 and lower: In the **Identity Provider** tab, under **Authentication Policies**, click **Policies**.
    2. In the **Policies** tab, ensure the **IdP Authentication Policies** check box is selected, and then click **Add Policy**.
    3. In the **Name** field, enter a meaningful name for the authentication policy.
    4. In the **Policy** dropdown, select **IdP Adapters** and then select the **HTML Form Adapter**. A branch for the **HTML form Adapter** is added to the PingFederate policy tree, and **FAIL**/**SUCCESS** fields are added.

5. Directly under the **HTML form Adapter** field, click **Rules** and in the **Rules** popup window enter the following information, and then click **Done**:
   - **Attribute Name**: Select **policy.action**.
   - **Condition**: Select **equal to (case insensitive)**.
   - **Value**: Type **Security Key** as your authentication source.
   - **Result**: Type **Security Key** as your authentication source.
   - Select the **Default to success** check box.

   A Security Key branch is added to the PingFederate policy tree.
6. In the **HTML Form Adapter** branch **FAIL** field, click **Done**.
7. In the **HTML Form Adapter** branch **Security Key** field dropdown list, select **IdP Adapters**, and then select the PingID Adapter. **SUCCESS** and **FAIL** fields are added to the Security Key branch.
   1. Under the Security Key branch **FAIL** field, click **Done**.
   2. In the Security branch **SUCCESS** field dropdown list select the endpoint you require. For example:
      - **Policy Contracts**: Select the policy contract you created earlier and complete the relevant mapping (see Configuring contract mapping).
      - **Local Identity Profiles**: Select the Local Identity Profile you created earlier and then complete the relevant mapping (see Configuring local identity mapping).
8. In the **HTML Form Adapter** branch **SUCCESS** field dropdown list, select the action that you want to apply and configure it appropriately. For example:
   - If configuring the PingID Adapter (recommended), do the following:
     1. In the **SUCCESS** branch dropdown list, select **IdP Adapters** and then select **PingID Adapter**. **SUCCESS** and **FAIL** fields are added to the branch.
     2. Under the PingID Adapter **FAIL** field, click **Done**.
     3. In the PingID Adapter **SUCCESS** field, select the local identity profile you created earlier.
     4. Under the local identity profile click **Local Identity Mapping** and complete the relevant mapping with the PingID Adapter (see also Configuring contract mapping).

        > **Note**
        >
        > For a list of attributes that can be used upon successful authentication with PingID, see PingID authentication attributes.

     5. Under the **PingID Adapter** entry, click **Options** and specify the following fields:
        - **Source**: HTML Form Adapter
        - **Attribute**: Username

- If configuring a local identity profile:

    1. In the **SUCCESS** branch dropdown list, select the **Local Identity Profiles**, and then select the local identity profile that you created earlier.

    2. Directly under the **HTML Form Adapter** branch **SUCCESS** field click **Local Identity Mapping**, complete the relevant mapping from your source to the local identity contract, (see Configuring local identity mapping), and then click **Done**.

5. Save the PingFederate policy.

6. Add any further configurations, for example:

    - Browser SSO: Configure IdP Browser SSO.
    - OAuth: OAuth configuration.

(Legacy) Customizing the HTML Form Adapter for passwordless authentication with a security key

Customize the passwordless authentication flow by adding a security key icon to the passwordless flow button. You can also choose to show the security key button when using webAuthn-compatible browsers only.

Before you begin

Before you start, create a PingFederate policy for passwordless authentication with a security key.

About this task

PingFederate 10.2 and later automatically includes a passwordless security key icon with the HTML Form Adapter, and automatically hides the security key button when the browser is not compatible with WebAuthn. For PingFederate 10.1 and lower, manually customize the HTML Form Adapter to:

- Add an icon to the passwordless flow button in the HTML Form Adapter. Add the security key icon provided by Ping Identity, or add your own custom icon.
- Choose to show the security key button only when the browser is webAuthn compatible.

Steps

1. To add a passwordless authentication flow icon:

    1. Download the security key image here, and in the relevant PingFederate folder, save the icon to the `server/default/conf/template/assets/images` folder as `icon-securitykey.png`.

    2. In the PingFederate folder, go to `server/default/conf/template/assets/css` and open the `main.css` file in a text editor.

    3. Add the following code to the `main.css` file, and then save the file.

```
body .button-container .social-media.securitykey {
  background-image: url("../images/icon-securitykey.png");
  background-size: auto 10px;
  background-position: left 10px center
}
```

2. To hide the security key button when a browser does not support WebAuthn:

    1. In the relevant PingFederate folder, go to `server/default/conf/template` and open `html.form.login.template.html` file in a text editor.

    2. In the html body add `isSecurityKeyAvailable();` to the `onload` attribute.

    ```
    <body
    onload="setFocus();isSecurityKeyAvailable();isWebAuthnPlatformAuthenticatorAvailable();">
    ```

    3. In the `script` element, add a new function, and then save the file.

    ```
    function isSecurityKeyAvailable() {
        var webauthnSupported = IsWebAuthnSupported();
        if (!webauthnSupported) {
            theElement = document.getElementById("securitykey-div");
            if (theElement) {
                theElement.style.display = "none";
            }
        }
    }
    ```

PingID authentication attributes

The following table lists the PingID attributes that can be used to evaluate PingFederate policy upon successful authentication with PingID.

These attributes can be applied to a range of use cases. For example, they can be used to verify authentication assurance levels.

> **Note**
>
> If the **Type** is `Bypass` or `Policy Approve`, all other authenticating device fields will not return a value.

`Attribute`	`Description`
`Authenticating Device`: Device used to authenticate, regardless of PingID policy	
`pingid.authentication.type`	Authentication action type. Options include: • `POLICY_APPROVE`: User automatically approved No authentication action is required by the user. * `MOBILE_APP_BIOMETRICS`: PingID Mobile App biometrics, e.g., FaceID, or Fingerprint * `MOBILE_APP_SWIPE`: PingID Mobile app swipe authentication * `MOBILE_APP_OTP`: PingID Mobile app one-time passcode (OTP) * `SMS` * `VOICE` * `DESKTOP_OTP`: PingID Desktop app OTP * `YUBIKEY` * `SECURITY_KEY` * `FIDO2_BIOMETRICS` * `OATH_TOKEN` * `AUTHENTICATOR_APP`: External authentication app, such as Google authenticator * `BYPASS`: Authentication bypassed

`pingid.authentication.authenticating.device.id`	The unique ID of the device from which the user is authenticating.
`pingid.eamAmr`	The authentication method the user is using to verify their identity. Use this attribute to facilitate integration with Microsoft Entra ID as an External Authentication Method (EAM).
`pingid.authentication.authenticating.device.longitude`	Longitude of the authenticating device from which the user is authenticating. Relevant for online authentication only.
`pingid.authentication.authenticating.device.latitude`	Latitude of the authenticating device from which the user is authenticating. Relevant for online authentication only.
`pingid.authentication.authenticating.device.altitude`	Altitude of the authenticating device from which the user is authenticating. Relevant for online authentication only.
`pingid.authentication.authenticating.device.accuracy`	GPS location accuracy of the authenticating device from which the user is authenticating. Relevant for online authentication only.
`pingid.authentication.authenticating.device.ip`	IP address of the device from which the user is authenticating.
`pingid.authentication.authenticating.device.app.version`	App version running on the authenticating device. Relevant for devices running on PingID mobile app.
`pingid.authentication.authenticating.device.model`	Model of the device from which the user is authenticating. Relevant for authenticating devices running PingID mobile app.
`pingid.authentication.authenticating.device.os.version`	OS version installed on the device with which the user is authenticating. Relevant for authenticating devices running PingID mobile app.
`pingid.authentication.authenticating.device.is.rooted`	Indicates whether the device is rooted or jailbroken. Relevant for authentication devices running PingID mobile app.
`pingid.authentication.authenticating.device.is.locked`	Indicates whether the authenticating device has a lock screen configured that requires a passcode. Relevant for authenticating devices running PingID mobile app.
`pingid.authentication.authenticating.device.is.mdm`	Indicates whether mobile device management (MDM) is installed on the authenticating device.
`Accessing device` : Device used to access the user's account or app	
`pingid.authentication.accessing.device.ip`	IP address of the accessing device.
`pingid.authentication.accessing.device.country`	Country in which the accessing device from which the user is authenticating is located. Based on the IP address of the accessing device.

`pingid.authentication.accessing.device.ip.reputation`	IP reputation of the accessing device from which the user is authenticating. Possible values **Low**, **Medium**, or **High**, or **Null**, according to the values defined in the IP reputation rule in PingID Policy.

Configuring offline MFA (PingID Adapter)

Offline multi-factor authentication (MFA) allows users to authenticate when the PingID server is inaccessible.

Before you begin

Offline MFA allows users to authenticate when the PingID server is inaccessible. If your organization is using PingID as a primary or secondary mode of authentication for federated single sign-on (SSO), you can implement the offline MFA feature of the PingID adapter, so you can circumvent unforeseen outages or network issues preventing users from logging in to access their applications.

Before you configure offline MFA, make sure that you have the following:

- PingID Adapter 2.0+ installed.
- A user directory to store the user's device information from PingID. For more information, see User directory for PingID offline MFA.
- Unlimited Strength Java Cryptography Extension (JCE), which is required for supporting the 256 byte key size for cryptographic algorithms. Without it, the feature will return an exception related to the missing library and will not function.

About this task

Sign on to the PingFederate admin console and configure the PingID Adapter for offline authentication. The configuration includes settings that support different user directory deployment implementations, such as storing the user device lists on the user object, on a separate devices object, or in a different directory, separate from the user's directory.

Steps

1. Sign on to the PingFederate admin console.
2. Click **IdP Configuration**.
3. Click **Adapters** in the **APPLICATION INTEGRATION** section.

   The **Manage IdP Adapter Instances** screen is displayed.
4. Click **PingID Adapter** (the adapter you previously installed, bundled with the PingID integration kit).

   The **PingID Adapter** summary screen is displayed.
5. Click the **IdP Adapter** tab.

   The **PingID Adapter** configuration screen is displayed.
6. Click **Show Advanced Fields**.

   The **PingID Adapter** advanced configuration options are displayed.

7. Configure the PingID offline MFA options.

Parameter	Description
`LDAP SEARCH SCOPE`	The options for determining the width and depth of the search, when the device list is stored on the user's object in the user directory: ◦ `OBJECT_SCOPE` : Search only in the base object. ◦ `ONE_LEVEL_SCOPE` : Search in the immediate children of the base object, but exclude the base object itself. ◦ `SUBTREE_SCOPE` : Search the base object and all of it children.
`STATE ATTRIBUTE`	The `STATE ATTRIBUTE` is used to override how a specific user is authenticated during offline authentication. The value of this field is the name of the attribute configured in the directory. If the PingID services are unreachable, the value of `STATE ATTRIBUTE` is evaluated: ◦ **Bypass**: The user bypasses PingID MFA. ◦ **Block**: (Case insensitive) The user will be blocked from performing the PingID offline MFA flow and denied access. **Note** If this parameter is not populated, the behavior of the offline authentication for the user will be taken from the **AUTHENTICATION DURING ERRORS** block in the PingID Adapter configuration.
`PINGID HEARTBEAT TIMEOUT`	The duration of time in seconds that the adapter will wait for the heartbeat calls to the PingID service, before falling back to the **AUTHENTICATING DURING ERRORS** feature. If left empty, the default is 30 seconds.
`AUTHENTICATION DURING ERRORS`	Determines how to handle user authentication requests when PingID services are unavailable. ◦ **Bypass User**: Accept the user's first factor authentication, and bypass the PingID MFA flow when the PingID MFA service is unavailable. ◦ **Block User**: Reject and block the user's login attempt when the PingID MFA service is unavailable. ◦ **Passive Offline Authentication**: Fallback to the PingID offline MFA flow when the PingID MFA service is unavailable. Users will be asked to scan a QR code with a mobile device previously registered with PingID to obtain an authentication code to authenticate. ◦ **Enforce Offline Authentication**: Force PingID offline MFA flow regardless of the PingID MFA service availability. **Note** User devices are updated in the directory for bypass, block, and passive offline modes.

Parameter	Description
`USERS WITHOUT A PAIRED DEVICE`	When PingID services are unavailable, you can choose to bypass or block users who have no paired mobile device (**pf-pingid-local-fallback** attribute in user's device list in the user directory). ◦ **Bypass User** indicates users without paired mobile devices will bypass the PingID adapter in an authentication attempt. ◦ **Block User** indicates users without paired mobile devices will have PingID block their authentication attempt. A user's individual block or bypass **State** attribute in the user directory will override the `USERS WITHOUT A PAIRED DEVICE` definition. **Note** This configuration is only relevant if **Passive offline authentication** or **Enforce offline authentication** were chosen in the `AUTHENTICATION DURING ERRORS` field. See User directory for PingID offline MFA for more details.
`LDAP DATA SOURCE FOR DEVICES`	The user directory data source used for retrieving additional user attributes for PingID offline MFA. This is the datastore in which the users device list (**pf-pingid-local-fallback** attribute) is stored.
`CREATE ENTRY FOR DEVICES`	Create the device list entry in the data source if it does not exist. This is the configuration setting for how and when PingFederate will create PingID device entries of type **pf-pingid-device**. **Note** Applicable only when **pf-pingid-local-fallback** is added to **pf-pingid-device**. ◦ **Checked**: **PingID Adapter** will create objects of type **pf-pingid-device** per user, and add the device list information in its **pf-pingid-local-fallback** attribute. ◦ **Unchecked**: PingFederate will assume that the **pf-pingid-device** objects per user are being created by an external system, and will only modify the **pf-pingid-local-fallback** attribute attached to them when needed.
`ENCRYPTION KEY FOR DEVICES`	This field contains the base64url encoded HMAC256 encryption key to encrypt the users devices list before saving to the user directory. This field is optional. If this field is empty, the devices lists will be kept unencrypted and will be stored as plain text. **Note** If the admin changes the encryption key, all users will have to authenticate online at least once, in order for new device details to be kept locally, or else the behavior in an offline scenario will follow the **USERS WITHOUT A PAIRED DEVICE** setting.

Parameter	Description
`DISTINGUISHED NAME PATTERN`	The pattern used to save device entries. It points to the location in the directory in which the **pf-pingid-device** objects reside. **Important** ◦ `DISTIGUISHED NAME PATTERN` must be used in either of the following scenarios: ■ When using more than one PCV or PingID Adapter instance with more than one configured PingID tenant. ■ When both the PCV and PingID Adapter are configured with more than one tenant. ◦ This parameter is required only if offline authentication is enabled when the **pf-pingid-local-fallback** attribute is saved separately from the user object.
`HTML TEMPLATE`	The template to which the adapter redirects users when the PingID offline MFA flow is triggered. The default value is `pingid.offline.auth.login.template.html`. Templates are located at `/server/default/conf/template`.

Choose one of the following methods to configure the `LDAP DATA SOURCE FOR DEVICES` to be used for offline authentication.

Method	Instructions
Deployments where the device information is stored in an attribute on the user object class	1. Set the `LDAP DATA SOURCE FOR DEVICES` field to the same data store as set in your `LDAP DATA SOURCE`. 2. Leave the `DISTINGUISHED NAME PATTERN` field empty. 3. Configure the remaining fields as necessary to comply with your organization's policy decisions.
Deployments where device information is stored in an attribute on an object separate from that of the user. This is the same process whether the device information is in the same directory as the user object, or in a separate directory.	1. Populate the `LDAP DATA SOURCE FOR DEVICES` field: ■ If the devices object is in the SAME directory as the user object, set the `LDAP DATA SOURCE FOR DEVICES` field to the SAME data store as set in your `LDAP DATA SOURCE`. ■ If the devices object is in a DIFFERENT directory from the user object, set the `LDAP DATA SOURCE FOR DEVICES` field to a DIFFERENT data store than that selected in `LDAP DATA SOURCE`. 2. Populate the `DISTINGUISHED NAME PATTERN` field with an appropriate pattern to specify where the device information is stored (for example: `CN={username},OU=PingID-Devices,DC=myDomain,DC=com`). 3. Select `CREATE ENTRY FOR DEVICES` if you want the adapter to create NEW records for users' devices, if they don't already exist.

> **Note**
>
> The `pingid_state` attribute is included in the core contract of the PingID adapter. The attribute value can be used in the Authentication Policy to make policy decisions based on the following criteria:
>
> | Criteria | pingid_statevalue |
> |---|---|
> | Success | [.codeph]``service_available`` |
> | {pingid} down, bypass | [.codeph]``service_unavailable`` |
> | Offline authentication success | [.codeph]``offline_auth`` |
> | Offline authentication success, state attribute bypass | [.codeph]``offline_auth_state`` |
> | Offline authentication success, users with unpaired device bypass | [.codeph]``offline_auth_unpaired`` |
> | Offline authentication success, user device data read error | [.codeph]``offline_auth_unknown`` |

8. Click **Done**.

   The **Manage IdP Adapter Instances** screen is displayed.

9. Click **Save** to persist the updated configuration.

10. To use OAEP padding together with RSA encryption during offline authentication:

    1. In PingFederate, go to **Authentication → PingID Adapter**.
    2. Click the **IdP Adapter** tab and then click **Show advanced Fields**.
    3. In the **Offline Authentication Encryption** drop-down list, select the relevant value, and then click **Save**.

       Possible values are **OAEP** (default) or **None**.

       > **Note**
       >
       > - The Offline Authentication Encryption configuration settings are backward compatible. If Offline Authentication Encryption is configured in the PingID Adapter v2.12 or later, no update is required in the UI. If upgrading from an older PingID Adapter version although the configuration is saved during the upgrade, the UI OAEP padding value is not automatically updated. An error message appears in the UI until you update it manually.
       > - If you are using a PingFederate cluster, you must carry out these steps on each server in order to use OAEP padding.

Testing PingID offline configuration

About this task

Conducting preliminary tests of the PingID offline configuration ensures the selected offline flow works in case of a PingID service failure.

To test PingID offline configuration:

Steps

1. Change the PingID properties file to break the connection to the PingID server by opening the **PingID Adapter configuration** and changing the values in the PingID properties file.

   Make sure to keep a copy of the original file.

   > **Note**
   >
   > You can alternately test the flow by setting the `Enforce Offline MFA` option without making changes to the properties file.

   1. Change the `idp_url` and `authenticator_url`.

      The original arguments are:

      - `idp_url` = `https://idpxnyl3m.pingidentity.com/pingid`
      - `authenticator_url` = `https://authenticator.pingone.com/pingid/ppm`

        Example:

   The following are examples of changes you can make to the arguments to test the offline configuration:

   - `Error 503`:
     - `idp_url` = `https://httpstat.us/503?`
     - `authenticator_url` = `https://httpstat.us/503?`
   - `Sleep=10000`:
     - `idp_url` = `https://httpstat.us/200?sleep=10000&`
     - `authenticator_url` = `https://httpstat.us/200?sleep=10000&`

       Result:
   - Replacing the PingID valid heartbeat page with a page that returns `error 503` (service unavailable) simulates an outage.
   - To test timeout configuration in PingFederate using `sleep=10000` simulates 10 seconds of latency on the demo webpage. If the timeout is less than 10 seconds, offline authentication is triggered.

2. Start an online authentication.

   > **Note**
   >
   > If the RADIUS password credential validator (PCV) is enabled, block all HTTP traffic to idpxnyl3m.pingidentity.com and authenticator.pingone.com on destination port 443 using your firewall or proxy server.

Result:

The selected MFA offline flow is triggered.

Configuring when using PingFederate 9.0 or earlier

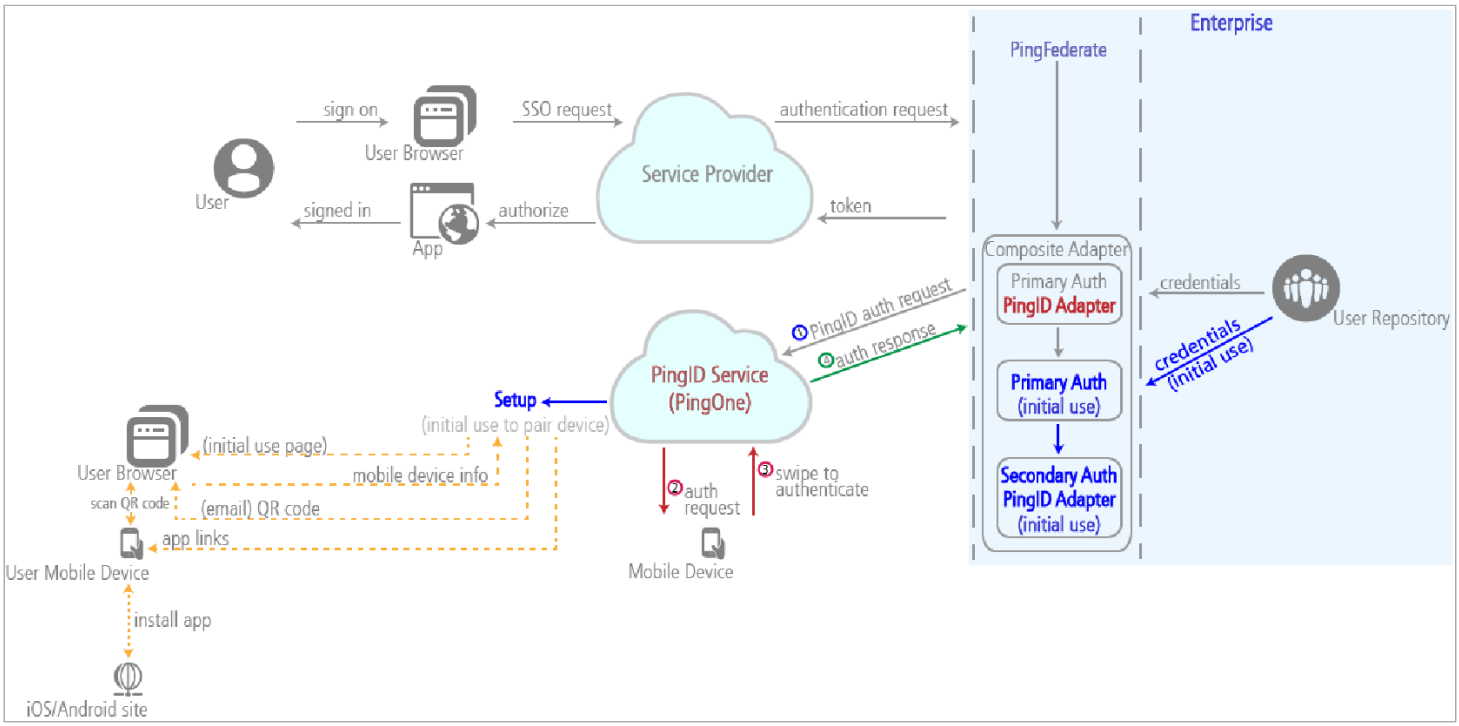
PingID can serve as a secondary authentication source for earlier PingFederate versions.

If you are using PingFederate 9.0 or earlier, you can use PingID for PingFederate:

- As a secondary authentication solution for federated single sign-on (SSO).
- As a secondary authentication solution when PingFederate is your PingOne identity bridge.

> **Note**
>
> Passwordless authentication is not supported if you are using PingFederate 9.0 or earlier. (It requires PingFederate v9.3 or higher.)

How It Works: Secondary Authentication



To use PingID for secondary authentication with PingFederate 9.0 or earlier, you must use a composite adapter. For more information, see Configuring a composite adapter.

Configuring a composite adapter

If you are using PingFederate 9.0 or earlier, you must create a composite adapter to enable secondary authentication.

About this task

This is part of the flow mentioned in Configuring a PingFederate policy for secondary authentication.

> **Note**
>
> Although it is possible to configure a composite adapter when running PingFederate 9.1 or higher, it is not recommended.

Steps

1. Go to **Identity Provider → Adapters → Manage IdP Adapters**.
2. Click **Create New Instance**.
3. For general instructions on creating a composite adapter instance for PingFederate 9.0 or earlier, see Configure the composite adapter.
4. On the **Type** tab, select **Composite Adapter** from the **Type** list.
5. On the **IdP Adapter** tab, select the IdP adapter instance you're using for the initial primary authentication and the PingID adapter you've configured, and add them to the composite adapter. For more information, see Configuring a PingID Adapter instance.
6. Click **Next** to continue configuring the adapter instance.

Supporting multiple access mode

Use multiple access mode to extend authentication sessions for low-risk devices and reduce security risks for multi-user devices.

> **Note**
>
> Multiple access mode requires:
>
> - PingFederate 9.2 or later
> - PingID Integration Kit 2.6 (PingID Adapter 2.5)
>
> This topic describes some sample configurations. Administrators should determine actual organization requirements. For more information, see the PingFederate documentation.

Some organizations want to offer their users an option for the system to retain successful authentication for a long period of time (long-lived session). For example, an organization whose policy challenges the user with the HTML Form Adapter followed by PingID multi-factor authentication (MFA) might require users authenticate only once every seven days.

Organizations typically have one or more of the following use cases:

- An organization-owned single-user device, for example, an employee's laptop or desktop computer. This is the predominant use case.
- An organization-owned multiple-users device, such as a kiosk or shared tablet.
- A device not owned by the organization that is used by single or multiple users, such as an internet cafe device or a home computer.

In a long-lived session scenario, an organization-owned accessing device allocated to an individual user for their sole use might be considered a low-risk scenario. However, secure long-lived sessions pose a challenge for organizations with teams whose users share an accessing device, or for users who might invoke authentication from a home computer or public computer.

In addition to organization-owned, single-user machine scenarios, admins can configure single sign-on (SSO) with MFA, supporting the following features:

- Indicate that a browser is running on a public device, such as on an organization-owned kiosk machine. User information will not be saved on that device.
- Allow users to indicate that the browser used for access is running on a public device, or on a device not regularly used for secure access, and assure users that they can securely sign on without concern about user information being kept on that device.
- Allow users the option to be deleted from a certain accessing device in order to avoid cases of other users later signing on to the same machine and being authenticated based on the long-lived session policy applied to a previous user's recent authentication.
- In terms of security compliance, ensure that when a user logs out, both first factor and MFA cookies are deleted and recent authentication policies will no longer apply.

Note

The PingID recent authentication policy rules are relevant only for private devices. Session information is not retained on termination of sessions on shared devices. For more information regarding the recent authentication access policy, refer to the following topics in the PingID admin guide:

- Configuring a recent authentication from office access rule (web policy)
- Configuring a recent authentication access rule (web policy)

When multiple access mode is configured, and a user attempts to access a protected resource, PingFederate analyzes parameters returned from the access request and determines whether the accessing device is private or shared. Based on the results, the process functions according to the following use case scenarios:

Private accessing device

- User information, including first factor and recent MFA information, is stored on the accessing device.
- PingID checks the recent MFA, and the user is not required to reauthenticate until the time limit expires on the recent authentication policy.

Note

When PingFederate is configured for single logout (SLO), and a signed-on user signs out from any accessed resource protected by PingFederate and PingID MFA on a private device:

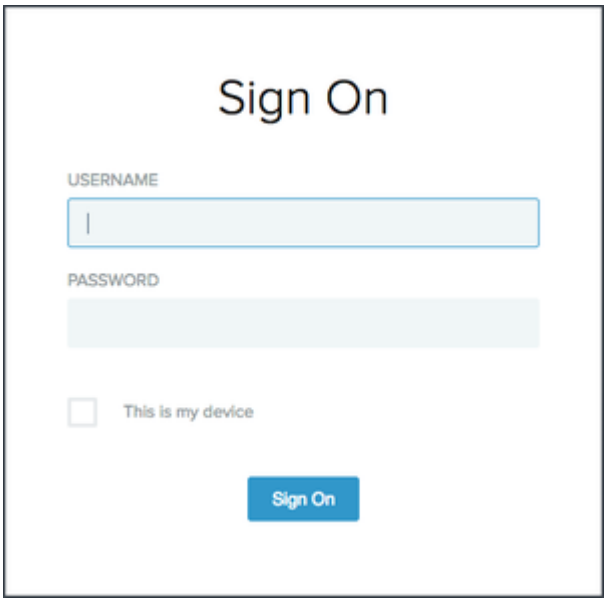
- An SLO is invoked, triggering user sign out from all protected resources accessed by the SSO.
- User and MFA session information is deleted from the accessing device.
- If PingID is configured to apply the recent authentication policy, there is no relevance to it once SLO has been invoked.

Shared accessing device

- No user information is stored on the accessing device.
- Because session information is not stored on shared devices, there is no relevance to the recent authentication policy.

Unknown accessing device

When the system is unable to determine whether the accessing device is private or shared, the HTML sign on form displays the **This is my device** check box, prompting the user to indicate the device status at sign on.



This is my device check box:

- Unchecked (default): Regards the accessing device as a shared device.
- Checked: Regards the accessing device as a private device.

Configuring multiple access mode

Enter these setting in PingFederate to configure multiple access mode.

Before you begin

Multiple access mode is supported from the following software versions:

- PingFederate 9.2 or later
- PingID Integration Kit 2.6 (PingID Adapter 2.5)

Steps

1. Configure PingFederate to determine whether the accessing device is organization-owned, and whether it is a private or shared device. Choose from the following methods to obtain this information.

   Choose from:

   - Reference the source IP address. For more information, see Configure the CIDR Authentication Selector.
   - Inspect the global HTTP header. For more information, see Configure the HTTP Header Authentication Selector.
   - Information returned by a mobile device management (MDM) system. Refer to the documentation for the following MDM Integration Kits available for PingFederate:

- MobileIron: Configuring MobileIron for PingID MDM integration
- Workspace ONE UEM (formerly known as AirWatch): Configuring Workspace ONE UEM for PingID MDM integration
- Inspect the distinguished name (DN) of the accessing device.

2. Configure multiple access mode.
    1. Download the PingID properties file. For more information, see Managing the PingID properties file for PingFederate.
    2. Create an HTML form adapter instance. Refer to HTML Form Adapter and Configure an HTML Form Adapter instance in the PingFederate admin guide. Make sure that:
        - **Session State** is set to **None**.
        - **Enable 'This is my device'** box is selected.
    3. Configure authentication sessions for the HTML Form Adapter. For more information, see Configure authentication sessions.
    4. Create a PingID adapter instance. For more information, see Configuring a PingFederate policy for secondary authentication. Make sure that:
        - **Type** is set to **PingID Adapter 2.5** or later, to support multiple access mode.

> **Important**
>
> The multiple access mode capability requires PingFederate Authentication Policies rather than the Composite adapter:
> - Create an Authentication Policy Contract (APC). For more information, see Policy contracts.
> - Create an authentication policy for the PingID adapter. For more information, see Policies.

Result

The following table summarizes the main flows, based on the attributes of the accessing device. These attributes are assessed to determine the use case, and whether the device is organization-owned, single or multi-user, or whether these attributes are unknown:

Accessing device attributes			Process flow	
Use case scenario	**Organization-owned device**	**Single/Multiple user device**	**HTML login form presents 'This is my device' checkbox**	**Session information saved**
`Private accessing device`: Each access device is organization-owned, and assigned to only one user.	Yes	Single user	No	Yes

Accessing device attributes			Process flow	
`Shared accessing device`: Access devices are organization-owned, and each device is identifiable before login at access time, as a multiple-user shared device.	Yes	Multiple users	No	No
`Unknown accessing device`: Access is permissible from devices whose status as a single-user or multi-user device is not identifiable before login at access time. These devices may also be either organization-owned privately owned. Since PingFederate cannot determine whether the access device is private or shared, the user is prompted at login to indicate the device status.	In this use case, the behavior is identical regardless of whether or not the access device is organization-owned.	Unknown whether single or multiple user device, when PingFederate presents the HTML login form	Yes	Depends on the user's response: • Yes: If the user checks **'This is my device'**. • No: If the user leaves **'This is my device'** unchecked.

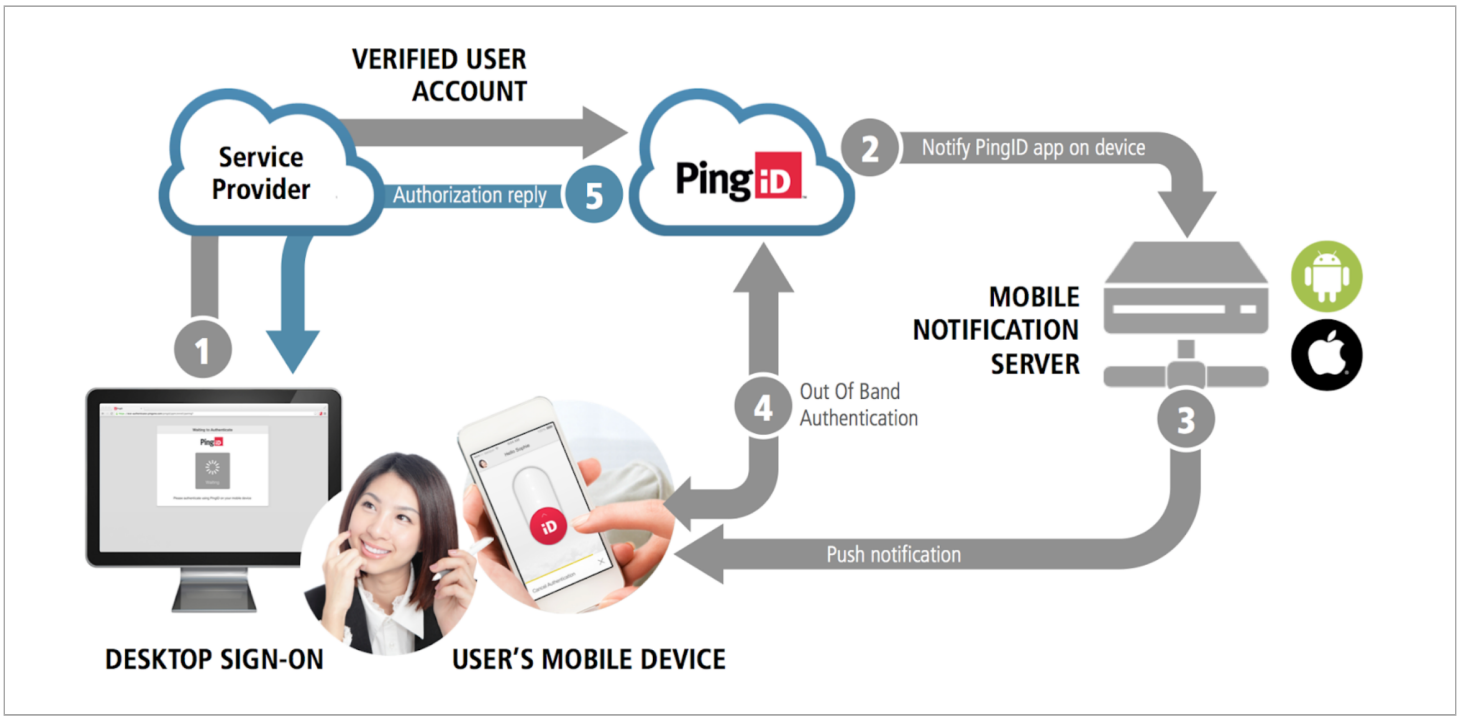
Integrate with PingID for PingOne SSO

If you have an existing legacy PingOne for Enterprise account, you can use an authentication policy to enable PingID as a secondary authentication solution for PingOne SSO.

> **Important**
>
> This integration is for PingID accounts that are using PingID with PingOne for Enterprise (legacy). If you are using PingID with the current PingOne platform, follow the instructions here

Configure and manage the PingID service using the PingOne for Enterprise admin portal. For more information, see Configure the PingID service.

How it works: PingOne secondary authentication with PingID



1. A user with PingOne as their identity provider (IdP) signs on to a service provider's (SP) resource. After PingOne successfully validates the user's credentials, it sends a request to the PingID server to authenticate the user.
2. PingID sends a request through the notification server to the PingID app installed on the user's mobile device.
3. The mobile notification server sends a notification to the PingID mobile app, and the user approves the sign-on request using the PingID mobile app.
4. PingID initiates an out-of-band authentication (OOBA) of the user.
5. The PingID server sends an authorization reply to the SP, which completes the sign-on process.

Creating or updating an authentication policy

An authentication policy allows you to use PingID to provide multi-factor authentication (MFA) to the single sign-on (SSO) process for your users or for subsets of your users.

About this task

By default, the policy is applied to all users and all applications, but you can select a filter to define the scope of the policy and assign the applications to include in the policy.

The authentication policy is applied to any new SSO sessions for Security Assertion Markup Language (SAML) or OpenID Connect (OIDC) applications.

> **Note**
>
> Applications that have been added to PingOne that use basic SSO or an SSO URL cannot be included in the authentication context for the policy.

After you enable your PingOne authentication policy, it works in conjunction with any PingID policies you want to configure. For more information, see PingID policy settings.

> **Note**
>
> If you change the identity bridge you're using, this can break any group filtering you include in your authentication policy. In this case, you must update your group assignments on the User Groups page and change the group filtering for your policy. For more information, see Authorize group access to applications.

Steps

1. Go to **Setup → Authentication Policy**.
2. Select **Enable Authentication Policy**.
3. **Required:** Select PingID as the authentication provider to use for the policy.

   If you don't select PingID, no PingID policies are applied for PingOne SSO.
4. In the **Authentication Filter** section, select one of the **Apply policy to** options:

   Choose from:

   - Click **All cases** to apply the policy to all users.
   - Click **Selected groups** to apply the authentication policy only to users who are members of the selected groups.

     > **Note**
     >
     > Do not use the underscore (_) or percent (%) characters in your search filter entry.

   - Click **All IPs except** to apply the authentication policy to all users except those whose IP address is in the list or block of IP addresses that you specify. The addresses must be IPv4 addresses in dot-decimal format (123.123.123.123) or an IPv4 address block in CIDR format (123.123.123.0/24).
5. In the **PingOne Admin Portal Configuration** section, select whether you want the policy to be applied to the PingOne admin portal.

   > **Note**
   >
   > This option is displayed only if you've upgraded to the new PingOne dock. Go to **Setup → Dock** to upgrade the dock.

   If you choose to apply the policy to the admin portal, you can also select the email address of a PingOne administrator for whom the policy does not apply.

   This administrator can bypass any authentication policy applied to the admin portal. Sign-on credentials for the admin portal are required for the administrator.
6. In the **Authentication Policy Context** section, specify the context where the policy will be applied.

Choose from:

- If you want to prompt MFA for all user attempts to SSO to SAML applications, select the **Apply to all sign-on attempts** option.
- If you want to prompt MFA only for specific applications, clear the **Apply to all sign-on attempts** option, and then under **Apply on application launch**, select the applications for which MFA should be triggered. If you have many applications, you can use the filter box to reduce the number of applications that are displayed in the list. The policy will only be applied to the applications that you select and to those you add with the **Force MFA** setting enabled. For more information, see Managing applications.

7. Click **Save**.

Result

The authentication policy is applied to all new user SSO sessions.

Next steps

- You can configure PingID policies to further refine your secondary level of authentication. For more information, see Web authentication policy configuration.
- If you're applying the authentication policy to the admin portal, see SSO to the PingOne admin portal with multi-factor authentication for further instructions.
- If you're using the PingFederate identity bridge, see SSO to the PingOne admin portal from PingFederate bridge

Disabling an authentication policy

Learn how to disable an authentication policy to revert to authenticating users through your identity bridge.

About this task

To disable an authentication policy:

Steps

1. Go to **Setup → Authentication Policy**.
2. Clear the **Enable Authentication Policy** check box.
3. Click **Save** and either:

   Choose from:

   - Disable the authentication policy and save the settings by clicking **Disable & keep data**.
   - Disable the authentication policy and delete the policy settings by clicking **Disable & wipe data**.

Result

The policy is disabled, and the authentication policy change is applied to all new user SSO sessions.

Integrating PingID with your VPN/Remote access system

PingID authentication can be integrated with your VPN or Remote access system using a RADIUS server, or directly to devices that support the PingID API.

For integrations with devices using a RADIUS server, see Integration for devices using a RADIUS server.

Currently supported devices are covered as follows:

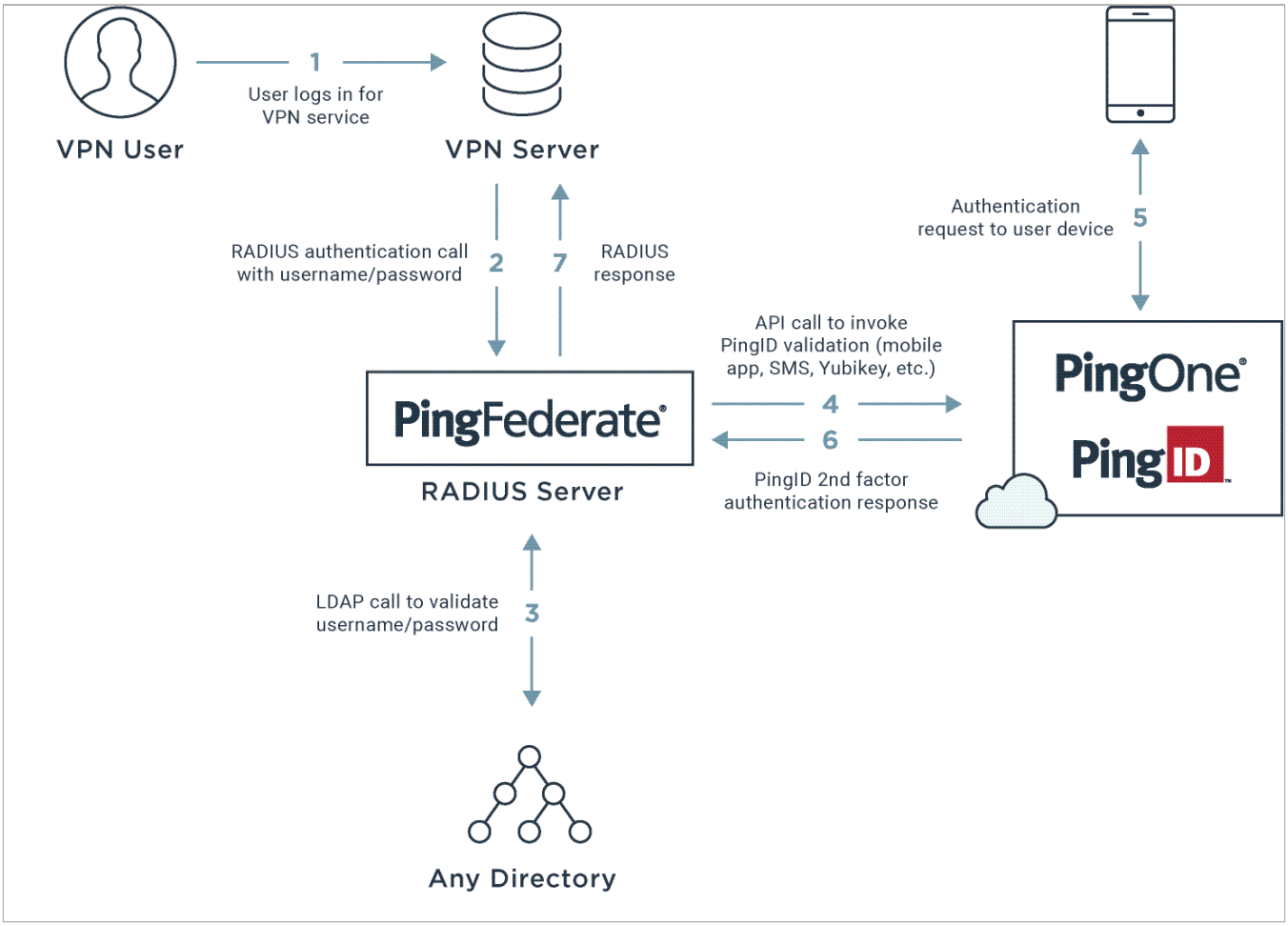
- Overview of Cisco ASA for PingID MFA
- Configuring Check Point VPN for PingID multi-factor authentication
- Configuring Juniper for PingID multi-factor authentication
- Configuring Palo Alto Global Protect for PingID multi-factor authentication
- Configuring Palo Alto Authentication Portal for PingID

Integration for devices using a RADIUS server

You can integrate PingID multi-factor authentication (MFA) into your VPN or remote access system.

About this task

The following diagram shows a general authentication flow. The actual configuration varies depending on your organizational infrastructure considerations and policies.



1. A user opens their IPSec or SSL VPN sign on window and enters a user name and password.
2. The VPN RADIUS client sends their details to the RADIUS Server on PingFederate.
3. PingFederate authenticates the user's credentials using the LDAP server as first-factor authentication.
4. After LDAP authentication approval, the RADIUS server initiates a second authentication using PingID, and the user receives a push notification to the relevant device, such as the PingID mobile app or a YubiKey.
5. The user approves the push notification or responds by entering a one-time passcode (OTP).
6. The PingID cloud service verifies the response and sends it back to the RADIUS server.
7. The RADIUS server returns a response to the VPN. If authentication is denied or an error occurs, the user receives an error message on their VPN window.

To configure PingID VPN integration, complete the following:

Steps

1. Install the PingID Integration Kit in PingFederate.

   For more information, see Installing the PingID Integration Kit for PingFederate.

2. Configure the RADIUS server settings in PingFederate.

For more information, see Configuring a RADIUS server on PingFederate.

3. Configure your VPN client settings.

   For more information, see one of the following sections:

   - Configure Cisco ASA for PingID MFA.
   - Configuring Check Point VPN for PingID multi-factor authentication.
   - Configuring Juniper for PingID multi-factor authentication.
   - Configuring Palo Alto Global Protect for PingID multi-factor authentication

Prerequisites: PingFederate RADIUS server

Before you begin, complete the following tasks:

- Your organization has installed and configured PingFederate. For more information, see Installation.
- PingFederate is configured with an LDAP Password Credential Validator (PCV). For more information, see Managing Password Credential Validator instances.

> **Note**
>
> PingID RADIUS PCV version 2.5.0 is incompatible with PingFederate version 11.2 and later. When upgrading to 11.2 or later, you must also upgrade the PCV version if you're currently using PCV version 2.5.0.

- You have administrator credentials for the PingFederate administrative console.
- Your VPN is configured to use the Password Authentication Protocol (PAP), MS-CHAP v2, or MS-CHAP v2 (EAP).

> **Note**
>
> CHAP is not supported by the PingFederate RADIUS server.

- To apply PingID policy features that require IP address information, the client IP address must be provided. The client IP must be sent using the RADIUS attribute `66:Tunnel-Client-Endpoint`. For more information, see Configuring a RADIUS PCV and SSH access policy.

> **Note**
>
> If the client IP attribute is not included:
> - IP-based policies will not work.
> - Entries in the PingOne report **IP address** field will show a value of `N/A`.

Integration for devices using a RADIUS server is a two-stage process

The first stage consists of installing the PingID integration kit for VPN and then configuring the RADIUS server on PingFederate. See Installing the PingID Integration Kit for VPN and Configuring a RADIUS server on PingFederate. You should also look at PingID RADIUS PCV parameters reference guide.

The second stage is configuration of your VPN device. Currently, supported devices are covered as follows:

- Overview of Cisco ASA for PingID MFA
- Configuring Check Point VPN for PingID multi-factor authentication
- Configuring Juniper for PingID multi-factor authentication
- Configuring Palo Alto Global Protect for PingID multi-factor authentication

Installing the PingID Integration Kit for VPN

To use PingID multi-factor authentication (MFA) for VPN authentication, you must install the PingID Integration Kit.

Before you begin

> **Note**
>
> For instructions specific to Windows Login Integration, see Installing PingID Integration Kit for PingFederate (Windows login).

PingID Integration Kit Requirements

Before you install the PingID Integration Kit:

- Register for the PingID Enterprise service on PingOne.
- Configure the PingID service and download the PingID properties file (see Managing the PingID properties file).
- Ensure you have installed the relevant PingFederate version as follows:
  - Beginning with PingID Integration Kit 2.11, PingFederate 10.0 or later is required
  - Beginning with PingID Integration Kit 2.10, PingFederate 9.3 or later is required
  - Beginning with PingID Integration Kit 2.6, PingFederate 9.2 or later is required
  - Beginning with PingID Integration Kit 1.4, PingFederate 8.4 or later is required
  - PingID Integration Kit 1.3 or earlier: requires PingFederate 8.3 or earlier (minimum supported version PingFederate 7.3)
- Ensure you have network access to your PingFederate installation.
- Ensure you have administrator permissions on PingFederate.
- Open ports:
  - 443 (outbound to Internet)
  - 1812 (UDP, to/from RADIUS clients)

> **Note**
>
> Port 1812 is required only if you plan on using the password credential validator (PCV) for RADIUS. This is the default port for RADIUS, but you also have the option of setting a different port number for the RADIUS client and RADIUS PCV. To change the port for the PCV, use the **RADIUS Server Authentication Port** option.

For further details about required web access, see PingID required domains, URLs, and ports.

About this task

The PingID Integration Kit is bundled as part of PingFederate 8.2 and later. If you have installed a recent version of PingFederate, no further action is required.

If you are doing any of the following, you'll need to install the integration kit manually:

- Using an earlier version of PingFederate.
- Updating the PingID Integration Kit.
- Installing the optional PingID offline MFA feature. PingID offline MFA requires that device information be stored on the user directory for retrieval when PingID cloud service is offline. If your organization requires the PingID offline MFA feature, configure the user directory. For more information, see User directory for PingID offline MFA.

> **Note**
>
> - PingID Integration Kit 2.0 and later is required for PingID offline MFA.
> - The setup of the prerequisite user directory for PingID offline MFA should be implemented before you stop the PingFederate server for deployment of the upgrade.

For more information about offline MFA, see PingID Offline MFA.

Steps

1. Download and extract the PingID Integration Kit package from https://www.pingidentity.com/en/resources/downloads/pingid.html.
2. **Optional:** If you are installing PingID offline MFA, set up the user directory. Sample scripts for Active Directory are supplied in Integration Kit 2.0 and later. You can modify these scripts for specific implementations. Choose one of the following methods to prepare the user directory for storage of the device information.

Method	Setup with ldif scripts (Active Directory only)	Manual directory setup for all types of directories
Deployments where the device information is stored in an attribute on the user object class.	Update the `<Your Location>` parameter to the location of your full DN for schemas, and then run them. In the `ldif` folder: ◦ `deviceAttribute.ldif` ◦ `addDevicesToUser.ldif` **Note** If you are using Active Directory, execute the supplied `ldif` scripts with the following command line instruction: `ldifde -i -f ${scriptname}`	1. Create a new user state attribute, and link it to the user class as an optional attribute: ■ The User State attribute name is optional. We recommend `pf-pingid-state`. ■ Attribute properties: ■ **Type**: Unicode String ■ **Size**: 0-64. ■ **Object UID**: 1.3.6.1.4.1.28867.9.2.37 2. Create a new device list attribute in the directory called `pf-pingid-local-fallback`, and link it to the user class as an optional attribute: ■ The name of this device list attribute (`pf-pingid-local-fallback`) is mandatory. ■ Attribute properties: ■ **Type**: Unicode String ■ **Size**: 0-inf (unlimited size). ■ **Object UID**: 1.3.6.1.4.1.28867.9.2.36

Deployments where device information is stored in an attribute on an object separate from that of the user. This is the same process whether the device information is in the same directory as the user object, or in a separate directory.	Run the following scripts located in the `ldif` folder: ◦ `deviceAttribute.ldif` ◦ `createDeviceClass.ldif` To create a specific organizational unit (OU) to store users' device information, run the `deviceOrgUnit.ldif script` to create an OU with `CN=PingID-devices`. **Note** ◦ You must specify where to save new objects in the plugin configuration. ◦ You can either use an existing OU or create a new one. ◦ The name `PingID-Devices` is not mandatory. The script may be edited to change the name. ◦ If you are using Active Directory, execute the supplied `ldif` scripts with the following command line instruction: `ldifde -i -f ${scriptname}`	1. Create a new User State attribute, and link it to the user class as an optional attribute: ■ The User State attribute name is optional. We recommend `pf-pingid-state`. ■ Attribute properties: ■ **Type**: Unicode String ■ **Size**: 0-64. ■ **Object UID**: 1.3.6.1.4.1.28867.9.2.37 2. Create a new device list attribute in the directory called `pf-pingid-local-fallback`: ■ The name of this device list attribute (`pf-pingid-local-fallback`) is mandatory. ■ Attribute properties: ■ **Type**: Unicode String ■ **Size**: 0-inf (unlimited size). ■ **Object UID**: 1.3.6.1.4.1.28867.9.2.36 3. Create a new device class in the directory called `pf-pingid-device`: ■ The name of this device list class (`pf-pingid-device`) is mandatory. ■ Class properties: ■ **Object UID**: 1.3.6.1.4.1.28867.9.1.3 ■ **Possible superiors**: container, organizationalUnit ■ May contain the `pf-pingid-local-fallback` attribute. ■ In some cases to prevent a schema issue, you may need to add an identifying attribute to the `pf-pingid-device` object class, such as `cn`. 4. **Device list container**: Create a new OU in the directory. The OU can have any name. We recommend `PingID-Devices`.

Active Directory only:

> **Note**
>
> For both of the above storage methods, scripts are provided for setting up PingID offline MFA `bypass` or `block` state of the user in the directory. For more information on the **state** attribute, see User directory for PingID offline MFA.
>
> - To create the **state** attribute and add the attribute to the user object class, run the `stateAttribute.ldif` and `addStateToUser.ldif` scripts.

3. On the PingFederate host, stop the PingFederate server.
4. Navigate to the `<pf_install>/server/default/deploy` directory and remove the `PingIDRadiusPCV-<version>.jar` file.

> **Note**
>
> If you are running PingID Integration Kit earlier than 1.5, remove the following files:
>
> - `pf-pingid-idp-adapter-<version>.jar`
> - `common-mfa-<version>.jar`
> - `gson-<version>.jar`
> - `jose4j-<version>.jar`

5. Copy the `PingIDRadiusPCV-<version>.jar` from the new `pf-pingid-integration-kit-<version>/pf-pingid-pcv-<version>/dist` directory to the `<pf_install>/server/default/deploy` directory.
6. Restart the PingFederate server.
7. If PingFederate is deployed on clustered servers, repeat these steps for all PingFederate nodes.

Configuring a RADIUS server on PingFederate

For your VPN to perform multi-factor authentication (MFA) using the PingID cloud service, you must create and configure a RADIUS server password credential validator (PCV) on PingFederate.

Before you begin

If the following conditions exist in your configuration, configure the relevant additional parameters:

- RADIUS clients that:
  - Handle first-factor authentication (and therefore does not send passwords to the RADIUS server),
  - and do not support RADIUS challenges

do not configure any delegate PCVs, and make sure to configure the following fields:

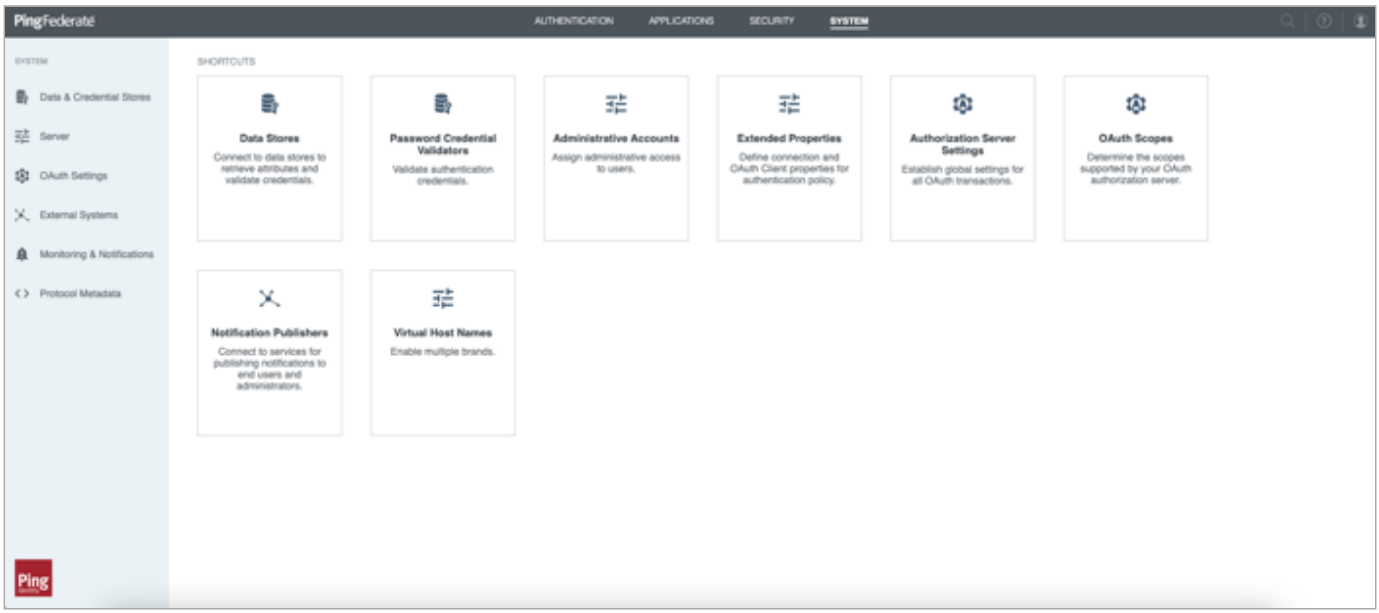
- `RADIUS Client Password Validation` : set this field to `enabled`.
- `Direct OTP validation` : For RADIUS clients running 3.0.4 or later, set this field to `enabled`.
- `OTP in Password Separator` :For RADIUS clients running 3.0.3 and earlier only, set this field to `Comma`
  - RADIUS clients that do not support RADIUS challenges: set the `RADIUS Client Doesn't Support Challenge` field to `enabled`.

If a RADIUS client requires additional attributes as part of the `Access-Accept` response, configure the relevant fields:

- `Multiple Attributes Mapping Rules`: Use this option to map attributes from a delegate PCV to any RADIUS attribute. This option supports the mapping of any vendor-specific attribute defined under `RADIUS Vendor-specific Attributes`.
- `User-Specific Groups to RADIUS client`: Use this option to add a single group name to any default RADIUS attribute. This option does not support vendor-specific attributes.

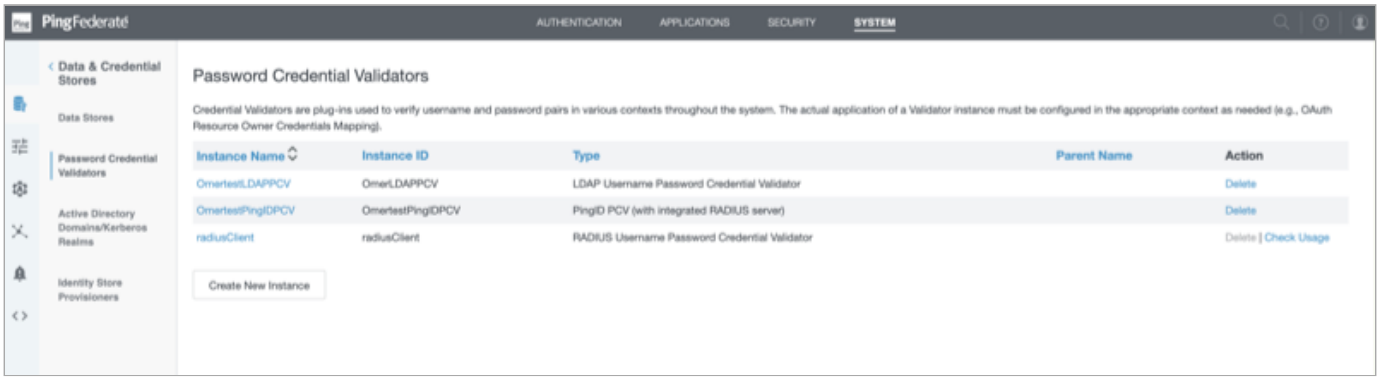
Steps

1. Open the PingFederate administrative console.
2. Click **System → Password Credential Validators**.



Result:

A list of credential validator instances is displayed.



3. In the**Instance Name** column, click **ldapPCV**.

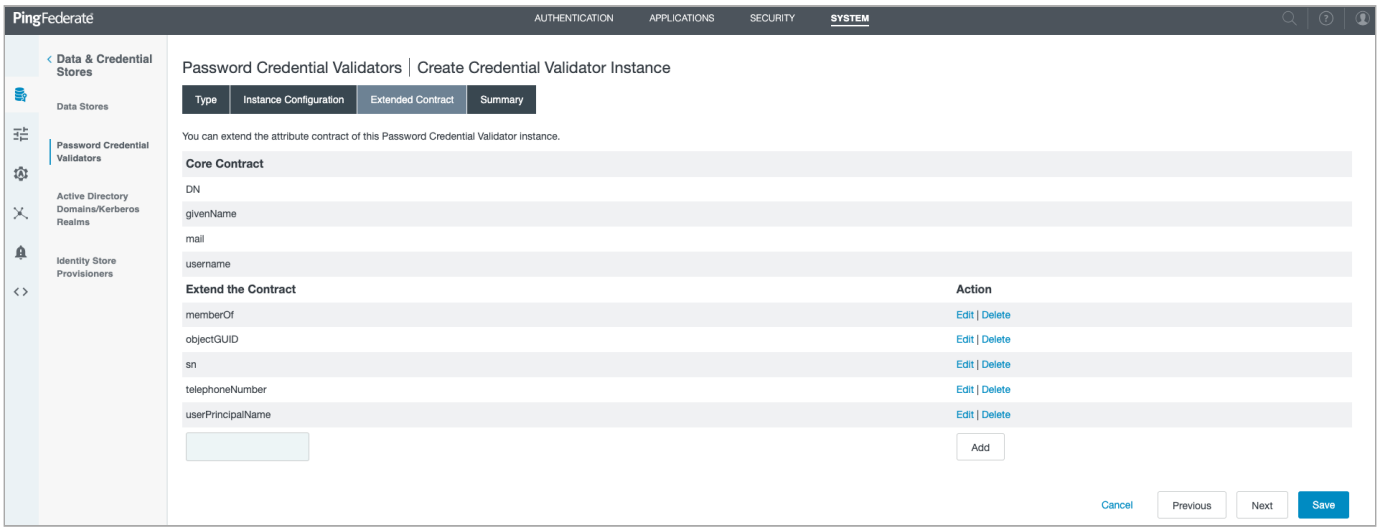
Result:

The **Create Credential Validator Instance** window opens.

4. Add the LDAP attributes that you want PingID to map and send to the PingID server.

    1. In the **Extend the Contract** field, enter an LDAP attribute, and then click **Add**. Repeat this step to add multiple attributes.

    > **Note**
    >
    > Some steps in RADIUS PCV configuration require use of LDAP user groups. To enable use of LDAP user groups, add the **memberOf** attribute to the LDAP Extended Contract mapping.



    1. Click **Done**, and then click **Save**.

        Result:

        The **Manage Credential Validator Instances** window opens.

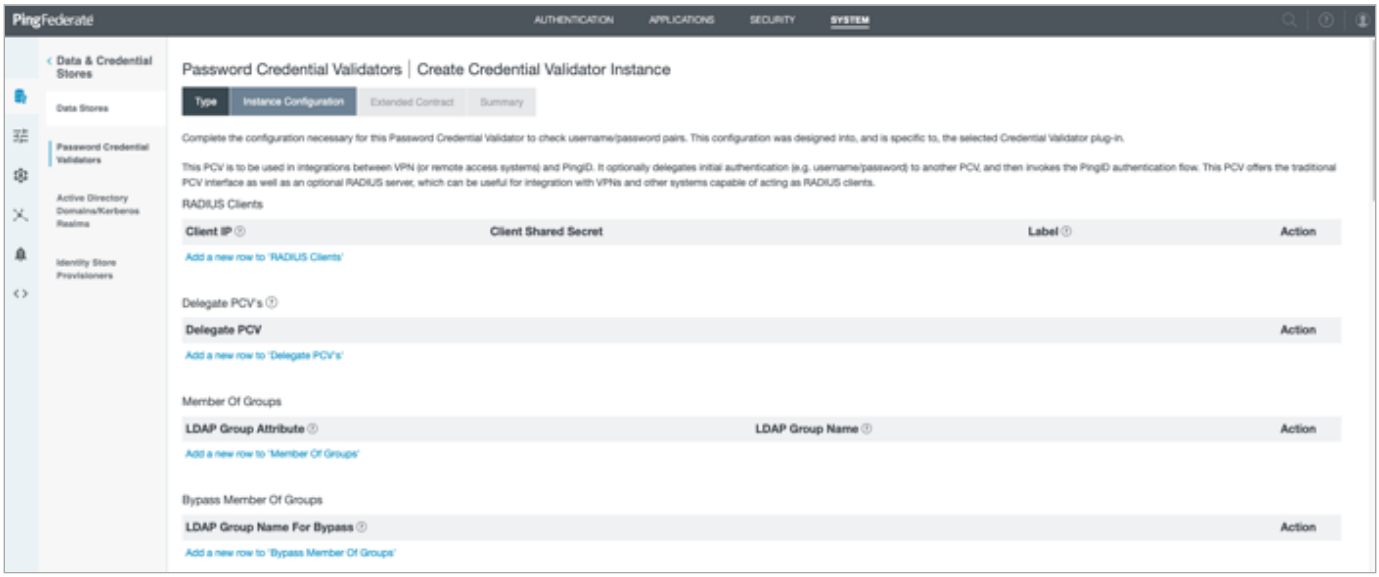
    2. Repeat this step for each LDAP PCV instance that you want to connect to the RADIUS server as a delegate PCV.

5. To create the RADIUS server instance, click **Create New Instance**.

6. In the **Instance Name** and **Instance ID** fields, enter a meaningful instance name and instance ID.

7. From the **Type** list, select **PingID PCV (with integrated RADIUS server)**.

8. Click **Next**.



9. To provide the necessary permissions for client to connect to the RADIUS server, create an approved RADIUS client:
    1. In the **RADIUS Clients** section, click **Add a New Row to RADIUS Clients**.

        > **Note**
        >
        > The IP address of the VPN server/remote access system is required here.

    2. Enter the RADIUS client's IP address and its shared secret. Optionally, you can add a label for each client to help distinguish between them when reviewing the list. Click **Update**.
10. Repeat the procedure from step 3 for all additional RADIUS clients that you want to add.
11. To add a Delegate PCV for the initial user authentication:
    1. Click **Add a New Row to Delegate PCV**.
    2. From the **Delegate PCV** list, select the LDAP PCV that you created when you set up PingFederate, and then click **Update**.

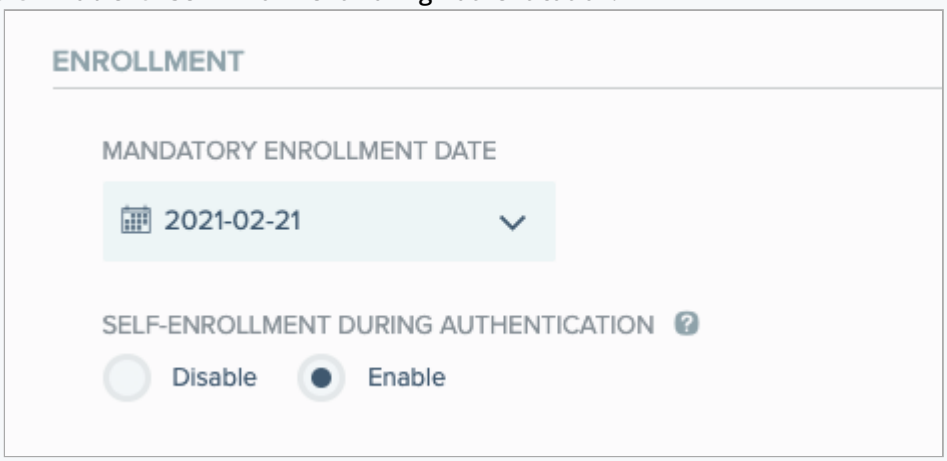
        > **Note**
        >
        > If you do not add a Delegate PCV, the RADIUS server assumes first-factor authentication has been performed by an external service. The RADIUS server will not authenticate against the LDAP directory and only PingID MFA will be used.

12. **Optional:** To define different authentication behavior per LDAP group, see Configuring LDAP group behavior in RADIUS Server.
13. In the **If the User Is Not Activated on PingID** list, select one of the following options:

    Choose from:

    - **Register the user**: If the user does not have a PingID cloud service account, initiate "on the fly registration" using the Challenge Page on the VPN clientless SSL. This is the default setting.

> **Note**
>
> The **Mandatory Enrollment Date** set in the PingID admin web portal determines when it is mandatory for the user to register. Before this date, "on the fly registration" is optional. To allow users to self-register, click **Enable** for **Self-Enrollment During Authentication**.

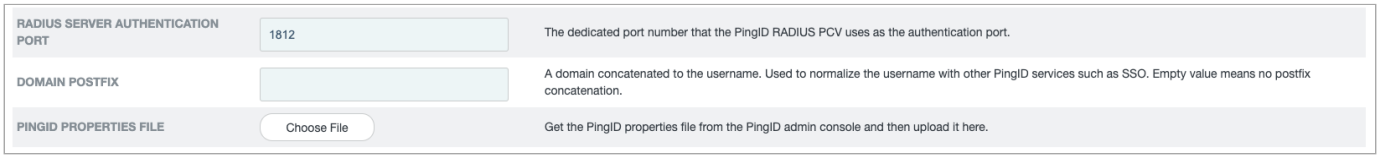


- **Always fail the login**: If the user does not have a PingID cloud service account, access is denied.
- **Fail login unless in grace period**: If the user does not have a PingID cloud service account by the mandatory enrollment date, access is denied.
- **Let the user in without PingID**: If the user is registered, authenticate with both LDAP and PingID MFA. If the user is not registered with PingID, authenticate with LDAP single-factor authentication only.

14. In the **RADIUS Server Authentication Port** field, enter the port number. The default port is 1812.

> **Note**
>
> The port number must match the port number you define on the VPN client.

15. To define the communication settings between RADIUS server and the PingID cloud service:
    1. In the PingOne for Enterprise admin portal, go to **Setup → PingID → Client Integration**.
    2. In the **Integrate with PingFederate and Other Clients** section, click **Download** to save a copy of the `pingid.properties` file. For more information, see Managing the PingID properties file.
    3. On the **Password Credentials Validators** tab, in the **PingID Properties** field, click **Choose File** and navigate to the PingID properties file you downloaded earlier. For more information, see Managing the PingID properties file.



16. **Optional:** Configure any additional RADIUS PCV parameters that you want to include. For a list of options, see PingID RADIUS PCV parameters reference guide.
17. Click **Next** twice, and then click **Done**.
18. Click **Save**.

> **Note**
>
> To perform a health-check on the RADIUS PCV server, use the heartbeat on /pf/heartbeat.ping. The PingID RadiusPCV does not expose its own heartbeat endpoint. For more information, see Enabling Heartbeat in PingFederate 7.3 and later.

PingFederate

You can download the PingID for PingFederate properties file for use when integrating PingID with PingFederate.

About this task

The Integrate with PingFederate Bridge properties file provides full permission to perform enrollment, device management, and authentication actions. You can rotate or revoke generated properties files with minimal downtime.

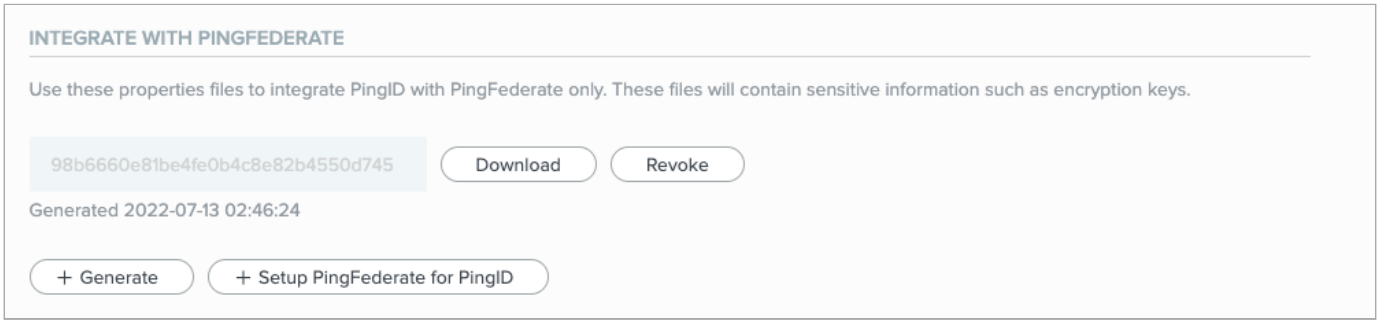
> **Note**
>
> For Window login, Mac login, and SSH integrations, you should download the version of the properties file that restricts user permissions to authentication only. For more information, see the relevant tabs on this page.

The PingID properties file contains sensitive information including the secret encryption key. It should only be handled by administrators and should not be distributed more than is necessary.

> **Warning**
>
> To ensure minimal downtime when rotating a PingID properties file (key rotation), first generate the PingID properties file and link it to the relevant client, and then revoke the old properties file.

Steps

1. In the PingOne admin portal, go to **Setup → PingID → Client Integration**.



Result:

The **Integrate with PingFederate and Other Clients** section is displayed, listing any PingID properties files that are already defined.

2. To generate a new PingID properties file, click **+ Generate**, and then click **Save**.

> **Note**
>
> You can have a maximum of five active PingID properties files. If you have five active files and want to generate a new one, you must first revoke one of your existing files.

Result:

A new entry is added to the properties file list, showing the new PingID properties file.

3. In the relevant row, click **Download**, and then save the file to the desired location with a meaningful name.
4. To revoke an old PingID properties file:
    1. Download and open the PingID properties file you want to revoke, and ensure the token matches the token listed in the web portal.
    2. In the relevant row of the properties file list, click **Revoke**, and then click **Save**.

       Result:

       The selected file is removed from the PingID server and can no longer be used for authentication.

Configuring LDAP group behavior in RADIUS Server

About this task

You can use groups for a number of administrative purposes, for example:

- Defining and restricting who can sign on to PingFederate.
- Gradually introducing PingID multi-factor authentication (MFA) into your organization.
- Creating user groups that are exempt from PingID MFA.

Steps

1. Add an LDAP user group.

Option	Steps
Add an LDAP user group that will require members to authenticate using PingID MFA	1. In the **LDAP Group Name** section, click **Add a new row to 'Member of Groups'**. 2. Enter the CN value of the relevant LDAP group name, and click **Update**. **Note** Do not enter the full DN. For example, if the full DN is `DN=CN=Android Users,OU=PingGroups,DC=intheory,DC=com`, enter only the CN value of `Android Users`. 1. Repeat the previous steps for all relevant LDAP groups. **Note** If no groups are defined in the RADIUS Server, group configuration is disregarded during authentication, even if the **Check Groups** option is enabled.
Add an LDAP group for users that you want to bypass MFA	1. In the **LDAP Group Name for Bypass** section, click **Add a new row to 'Bypass Member of Groups'**. 2. Enter the relevant LDAP group name's CN, then click **Update**. 3. Repeat the previous steps for all relevant LDAP groups. **Note** Users included in a Bypass MFA LDAP group will not be prompted to authenticate using PingID, even if they are included in an LDAP group, or the company policy requires MFA.

2. Configure the groups by enabling or disabling the following options:

   - **Check Groups** (cleared by default): If selected, MFA is only performed if the user is a member of one of the groups defined in the **Member of Groups** section. If cleared, group configuration is ignored during authentication.
   - **Check Bypass Groups** (cleared by default): If selected, MFA is bypassed if the user is a member of one of the defined groups in the **Member of Bypass Groups** section. If cleared, Bypass groups are ignored, and the user is required to authenticate.
   - **Fail Login if the User is Not Member of the LDAP Group:** If selected, users that are not LDAP group members cannot sign on. LDAP group members are always authenticated using PingID MFA. If cleared, only users that are members of a specified group are authenticated using PingID MFA. All other users are validated using LDAP authentication only.

Configuring RADIUS PCV for MS-CHAPv2

To use MS-CHAPv2 encryption with the RADIUS protocol, you need to enable PingID Password Credential Validator (PCV) to work with the relevant Network Policy Service (NPS). The PingID password credential validator (PCV) implements PingID as the second factor in the flow between the client and the network policy service (NPS).

Before you begin *Install the PingID Integration Kit.*

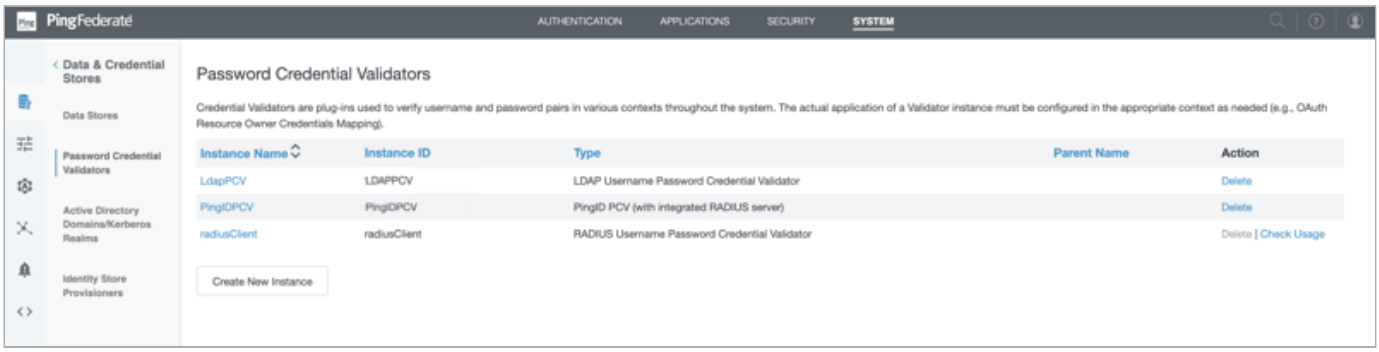
> **Note**
>
> Use of PingID as the second factor between the RADIUS client and an NPS is only supported when using either MS-CHAPv2 or EAP-MSCHAPv2 encryption.

Steps

1. In PingFederate, go to **Password Credential Validators**.

   Result:

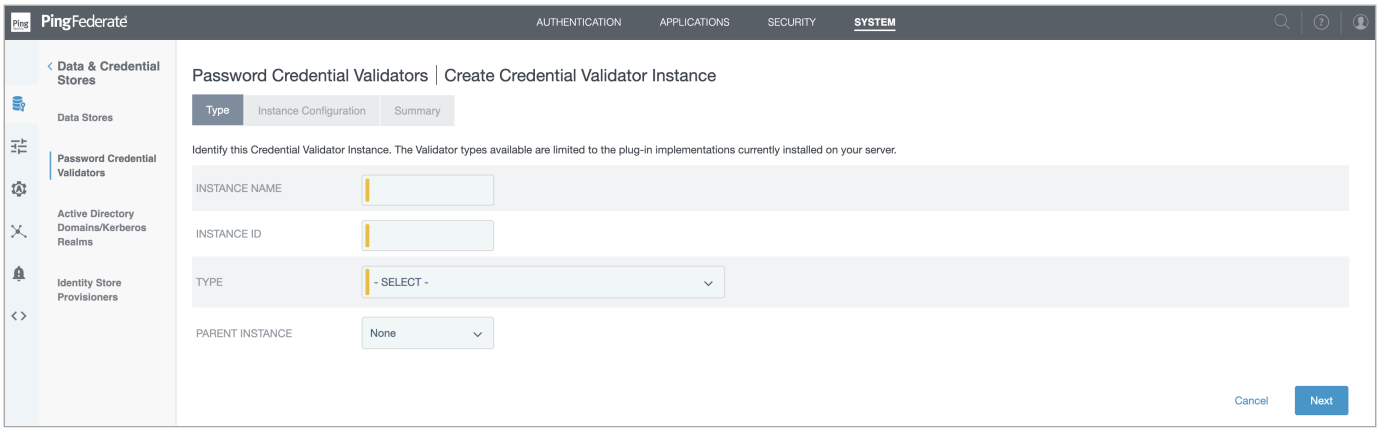
   A list of credential validator instances is displayed.



2. Click **Create New Instance**.

   Result:

   The **Create Credential Validator Instance** window opens.



3. In the**Instance Name** and **Instance ID** fields, enter a meaningful instance name and instance ID.

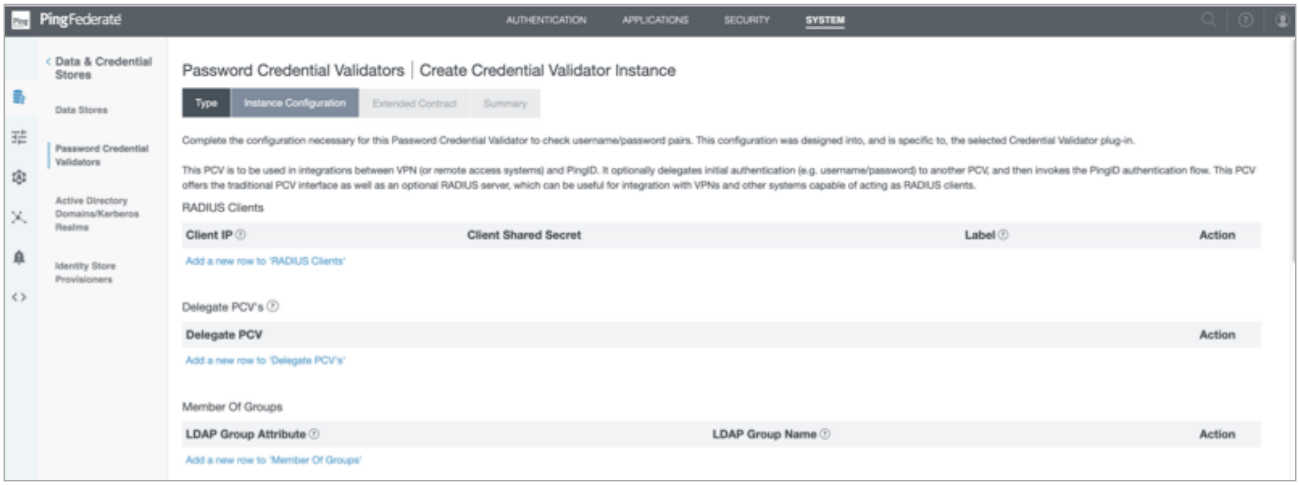
4. In the **Type** list, select **PingID PCV (with integrated RADIUS server)**. Click **Next**.

5. To specify an LDAP as the attribute source:

    1. Configure an LDAP connection.

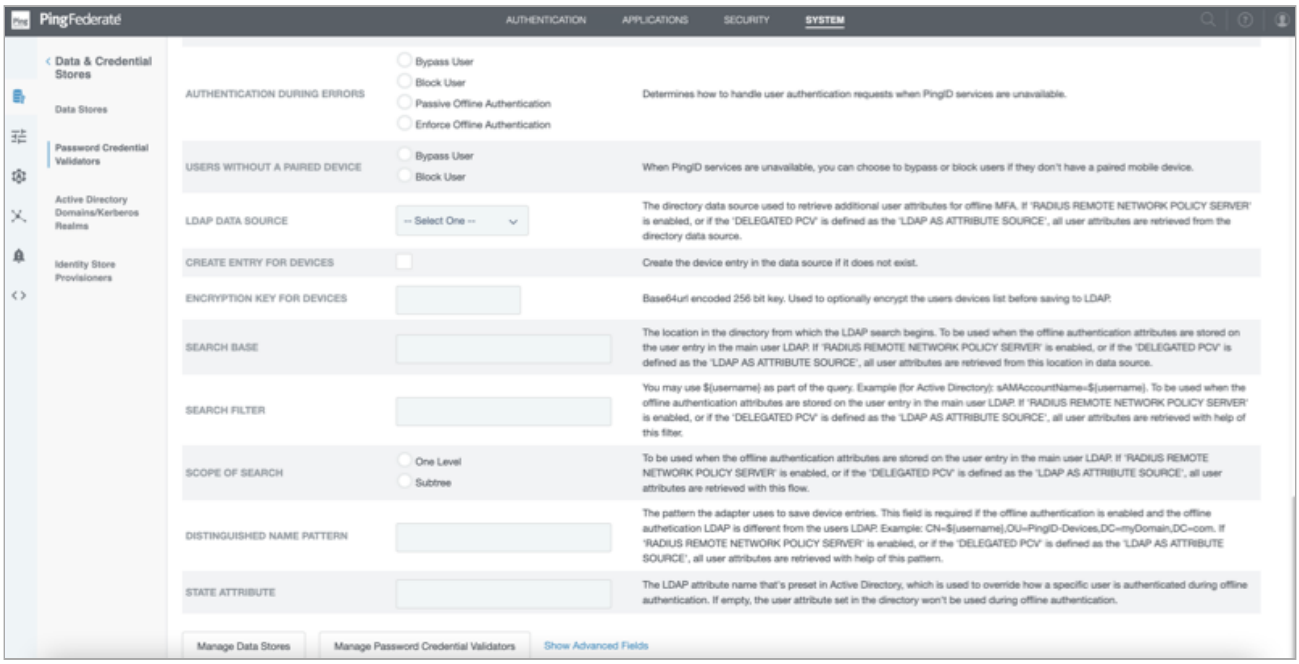
    2. In the **Delegate PCV**field, click **Add a new row to Delegate PCVs**.

    3. In the **Delegate PCV** list, select **LDAP as attribute source**.



    4. In the **LDAP Data Source** field, select the LDAP connection that you configured.

    5. Configure either the **Search Base** and **Search Filter** fields, or the **Distinguished Name Pattern**field.



6. To provide the necessary permissions for client to connect to the PingID RADIUS PCV, create an approved RADIUS client:

    1. In the **RADIUS Clients** section, click **Add a New Row to RADIUS Clients**.

    2. Enter the RADIUS client's IP address and shared secret. Optionally, you can add a label for each client to help distinguish between them when reviewing the list.

> **Note**
>
> Validation of the client IP shared secret is performed on the PCV side and the NPS side. Therefore you must make sure the shared secret on the client matches the shared secret on the endpoint NPS.

3. Click **Update**.

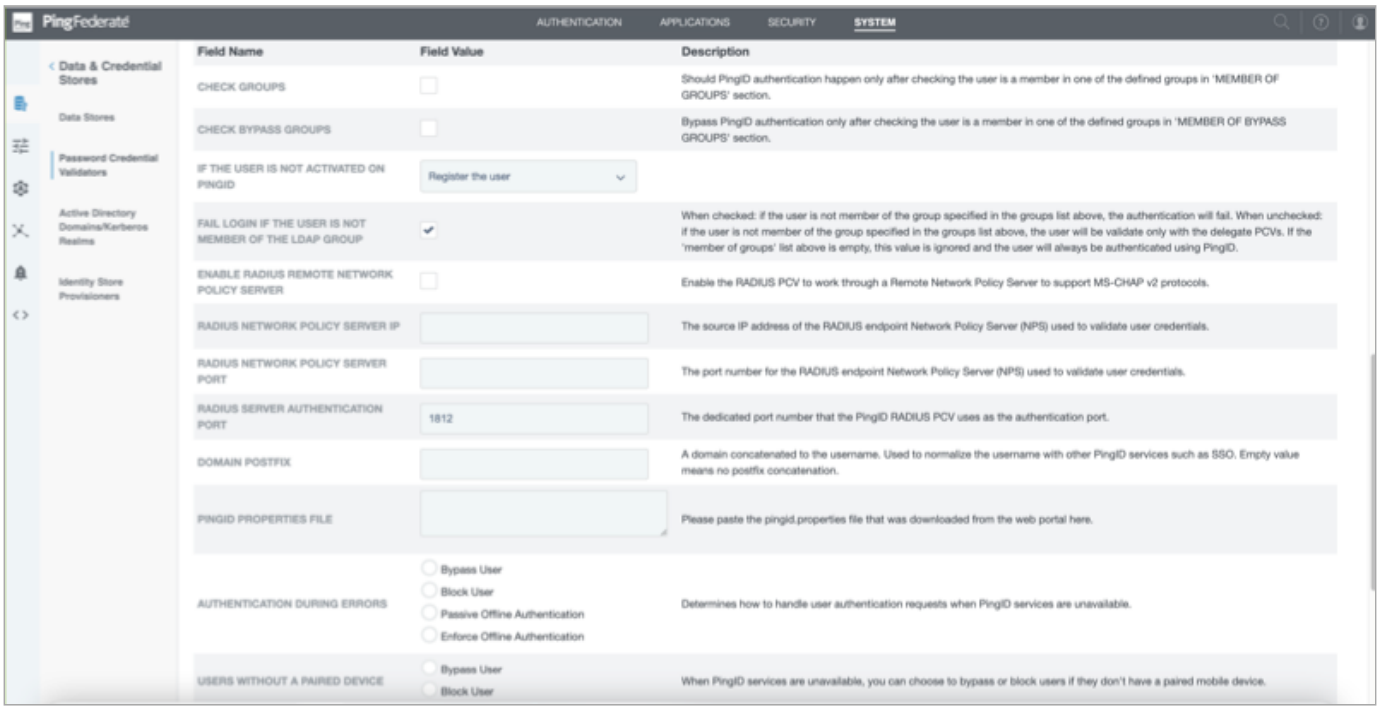
7. **Optional:** To define different authentication behavior per LDAP group, see Configuring LDAP group behavior in RADIUS Server.

8. In the **If the User Is Not Activated on PingID** list, select one of the following options:

   Choose from:

   - **Always fail the login**: If the user does not have a PingID cloud service account, access is denied.
   - **Fail login unless in grace period**: If the user does not have a PingID cloud service account by the mandatory enrollment date, access is denied.
   - **Let the user in without PingID**: If the user is registered, authenticate with both LDAP and PingID MFA. If the user is not registered with PingID, authenticate with LDAP single-factor authentication only.

9. Select the **Enable RADIUS Remote Network Policy Server**check box.



10. In the **RADIUS Network Policy Server IP** field, enter the relevant IP address for your NPS.

11. In the **RADIUS Network Policy Server Port** field, configure the dedicated authentication port number of the remote NPS.

> **Note**
>
> Make sure the **RADIUS Server Authentication Port** number is unique and not used for any other PingID RADIUS PCV instance. The default port is 1812.

12. To define the communication settings between RADIUS Server and the PingID cloud service:
    1. In the PingOne admin portal, go to **Setup → PingID → Client Integration**.
    2. In the **Integrate with PingFederate and Other Clients** section, click **Download** to save a copy of the `pingid.properties` file.

       For more information, see Managing the PingID properties file.
    3. In a text editor, open the `pingid.properties` file, copy the file contents, and paste the contents into the **PingID Properties file** field in PingFederate.
13. **Optional:** Configure any additional RADIUS PCV parameters that you want to include.

    For a list of options, see PingID RADIUS PCV parameters reference guide.
14. Click **Next** twice, and then click **Done**.
15. Click **Save**.

> **Note**
>
> To perform a health-check on the RADIUS PCV server, use the heartbeat on /pf/heartbeat.ping. The PingID Radius PCV does not expose its own heartbeat endpoint. For more information, see Enabling Heartbeat in PingFederate 7.3 and later.

Enable users to enter an OTP with their username

The PingID RADIUS PCV with EAP-MSCHAPv2 only works in no-challenge mode. Your users can enter a one time passcode (OTP) with their username when signing on in no-challenge mode.

About this task

The following authentication methods are supported for this mode.

User experience:

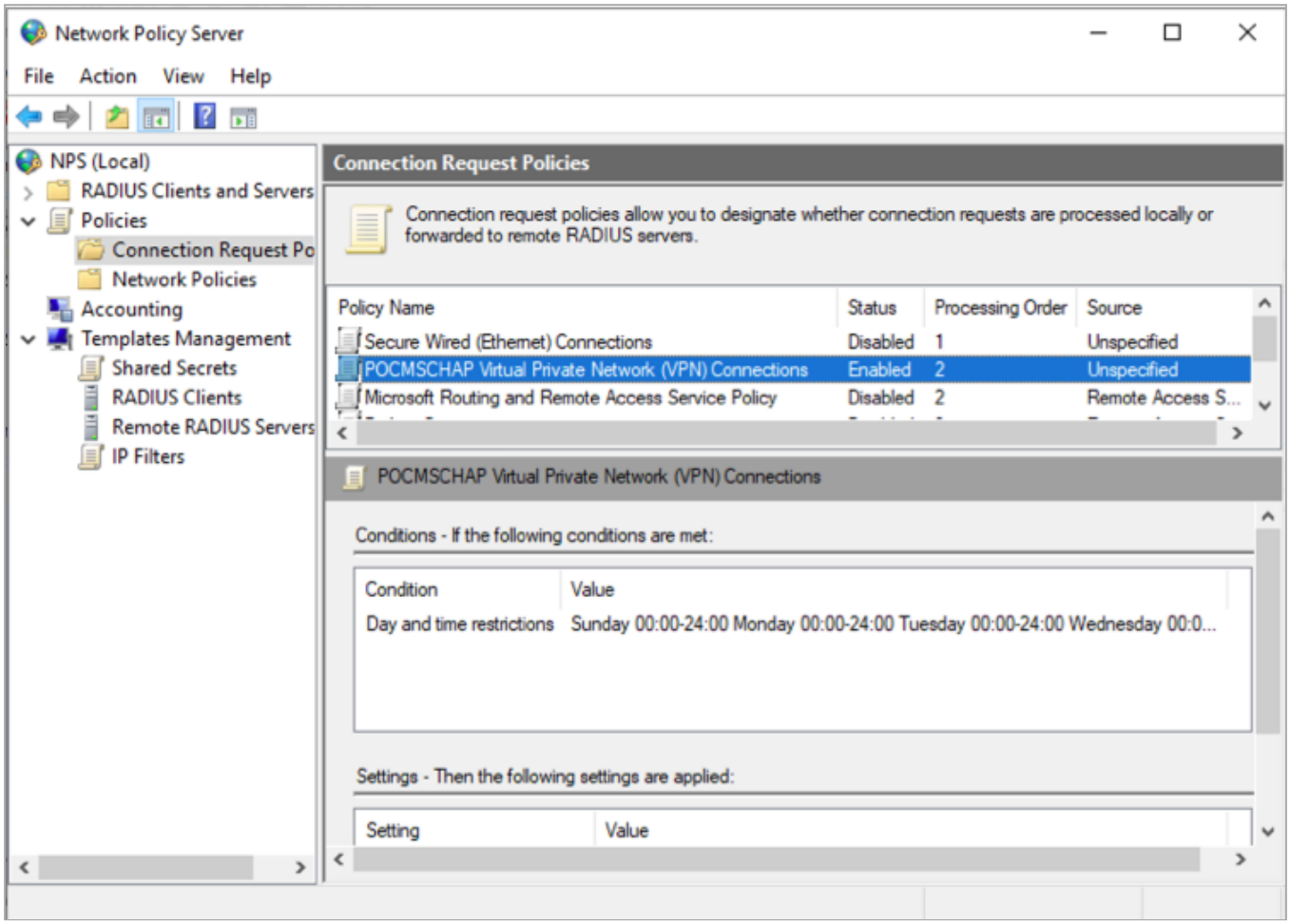
- If a mobile App user wants to authenticate using swipe or RADomS client username field.enter the OTP in the RADIUS client username field.
- When using a Desktop app or YubiKey, or if the user's mobile App is offline, then the user should add a comma after their username and then the OTP.

  For example, user John can enter the OTP 123456 as John,123456.
- If the user is registered with multiple devices supported by this mode, an OTP generated by any one of those devices will authenticate the user.
- This mode does not support on-the-fly registration.

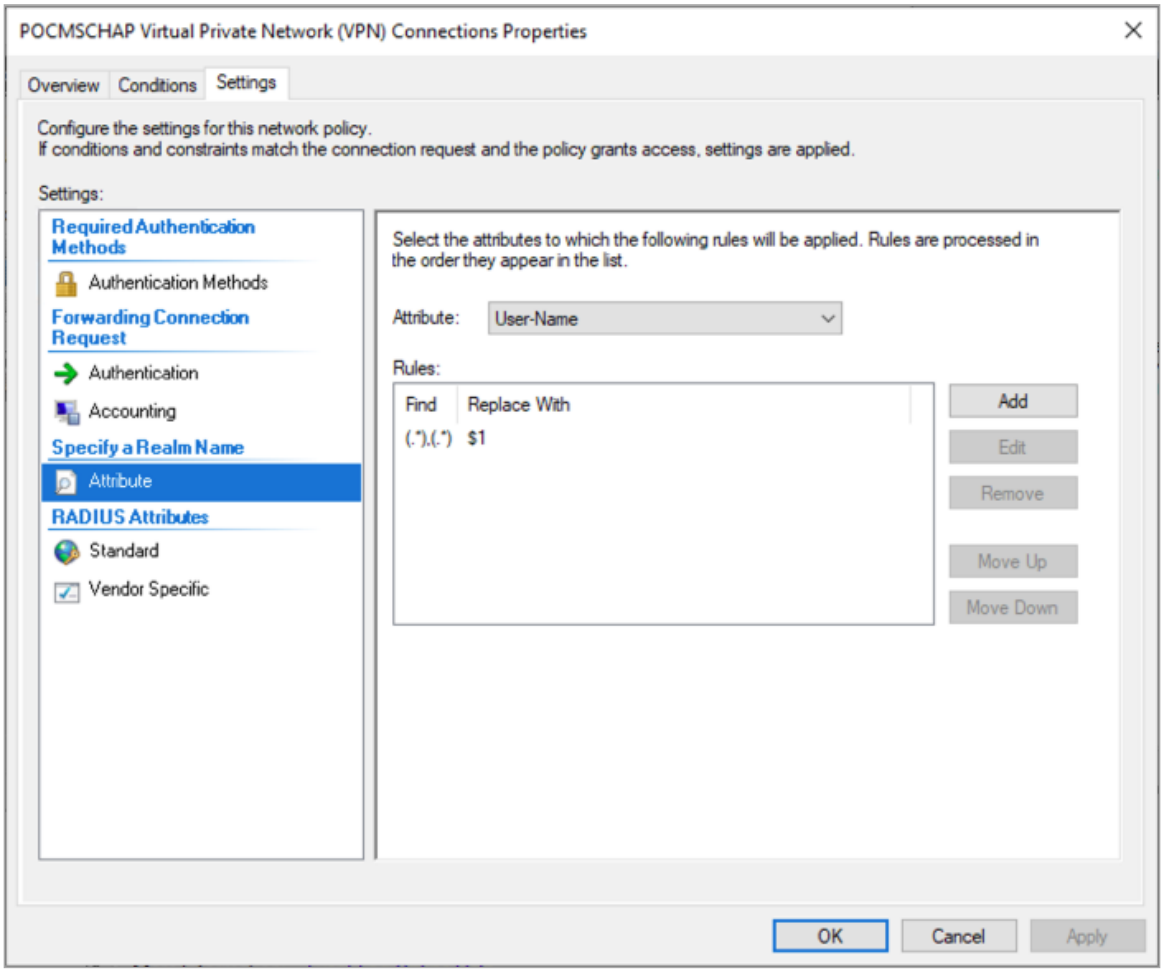
To configure the NPS to enable users to enter an OTP together with their username:

Steps

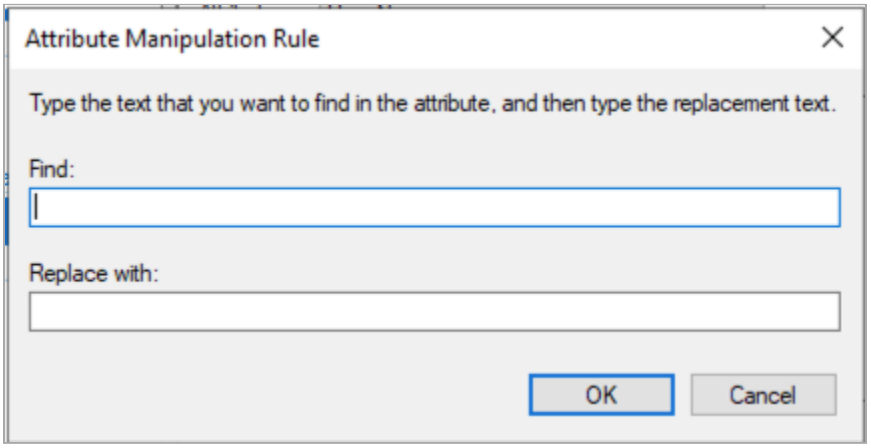
1. Sign on to the Windows server and open the **Network Policy Server** (NPS) configuration window.
2. In the **NPS** tree, under **Policies** click **Connection Request Policies**.



3. In the **Connection Request Policies** list, double-click your policy to view the policy properties.
4. Click the **Settings** tab, and in the **Specify a Realm Name** section, click **Attribute**.



5. In the **Attribute** field, select **User-Name**.
6. Click **Add**.
7. In the **Attribute Manipulation Rule** window, enter the following and then click **OK**:
    - **Find**: `(.),(.)`
    - **Replace with**: `$1`



> **Note**
>
> To add the OTP (or Yubikey OTP) the user should add a comma after their username and then enter the OTP.
> For example, user `John` can enter the OTP `123456` as `John,123456`.

PingID RADIUS PCV parameters reference guide

The following tables detail the PingID RADIUS password credential validator (PCV) configuration parameters available in PingFederate.

General Parameters

PingID RADIUS PCV Configuration General Parameters

Parameter	Description
RADIUS Clients	
Client IP	For the RADIUS **Client IP** address, use the IP address of the VPN server/remote access system.
Client Shared Secret	The RADIUS client shared secret. The shared secret is shared with the VPN.
Label (optional)	Add a label to a specific client.
Require Message-Authenticator (optional)	To mitigate the risk of a Blast-RADIUS attack, require this attribute in every RADIUS PCV client request and also include it as the first attribute in every RADIUS response. The default is **Disabled**. **Note** Learn more in the Ping Identity Knowledge Base article, RADIUS vulnerability CVE-2024-3596

Parameter	Description
Limit Proxy-State (optional)	Optional: To mitigate the risk of a Blast-RADIUS attack, RADIUS Gateway ignores requests that contain one or more Proxy-State attribute if they do not include the Message-Authenticator attribute. This option should only be used for legacy clients that don't support sending the Message-Authenticator attribute and aren't acting as proxy clients. The default is **Disabled**. **Note** Learn more in the Ping Identity Knowledge Base article, RADIUS vulnerability CVE-2024-3596
Delegate PCVs	
Delegate PCV	The instance name of the "LDAP PCV with Extended Attributes" PCV. If PingID RADIUS PCV is only required to receive user attributes from an LDAP data source, select **LDAP as Attribute Source**. This field should be left blank if: • The VPN client performs LDAP verification. • LDAP verification is not required from the RADIUS PCV. If **RADIUS Remote Network Policy Server** mode is enabled, either **LDAP as Attribute Source** must be selected, or the field should be left blank.
Member Of Groups	Enter one or more pairs of LDAP group attribute and LDAP group name. Users in the groups defined here can be authenticated using PingID MFA. The default value for the LDAP group attribute is *memberOf*. **Note** Do not enter the full DN. For example, if the full DN is: **DN=CN=Android Users,OU=PingGroups,DC=intheory,DC=com** enter only the CN value **Android Users**.
LDAP Group Name for Bypass	Enter one or more LDAP group names. Users in the groups defined here will not be authenticated using PingID MFA.
RADIUS Vendor-Specific Attributes	If you want to have vendor-specific attributes sent during authentication, add them to the **RADIUS Vendor-Specific attributes** section, and then refer to them when you complete the **Multiple attributes mapping rules** section. To add a vendor-specific attribute: 1. Click **Add a new row to 'RADIUS Vendor-Specific attributes'**. 2. Enter the ID of the vendor. 3. Enter a name for the attribute. Note that this is the field that has to be referred to in the **Multiple Attributes Mapping Rules** section. 4. Enter the number of the attribute.

Multiple Attributes Mapping Rules

Permits mapping definitions for LDAP attributes to return all values of the attribute to the RADIUS client or PingID, depending on the **Destination Selection**. LDAP attributes may contain more than one value (for example, a user may be a member of more than one group), in which case the values are separated by the semicolon (;) character.

> **Note**
>
> - Single value LDAP attributes may be mapped to either RADIUS client or PingID destination attributes.
> - Multiple value LDAP attributes may be mapped only to RADIUS client destination attributes.

Click **Add a new row to 'Multiple attributes mapping rules'**, and enter the following fields for each rule:

- **Source Selection**: `LDAP` (other values are reserved for future use).
- **Source Attribute**: The name of the LDAP attribute whose value will be passed to the RADIUS client or PingID, depending on the value of **Destination Selection**. The attribute selected here must be included in the extended contract of the Delegate PCV.
- **OGNL Expression**: Enter an OGNL expression if you want to fine-tune the mapping between the source and destination attributes. For more information on the use of OGNL expressions for this purpose, see Introduction to OGNL.
- **Destination Selection**: `RADIUS`, Vendor Specific (for vendor-specific RADIUS attributes), or `PingID`.
- **Destination Attribute**: the name of the RADIUS or PingID attribute which will receive the value from the LDAP **Source Attribute**. For vendor-specific attributes, use the name that you provided in the **RADIUS Attribute Name** column in the **RADIUS Vendor-Specific attributes** section of the page.

PingID destination attributes (when the value of **Destination Selection** is `PingID`):

- **fname**: The attribute containing the user first name. For example, `givenName`.
- **lname**: the name of the LDAP: The attribute containing the user last name. For example, `sn`.
- **email**: The attribute containing the user email address. For example, `mail`. This email address is used during registration if users need to receive a link on their mobile device to download the PingID application.

> **Note**
>
> - A PingID **Destination Attribute** may be mapped to only one LDAP **Source Attribute**.
> - If the value of one attribute is invalid, the mapping fails for all attributes.

- **RADIUS Attribute Type**: The type of the attribute

Parameter	Description
User Specific Groups to RADIUS Client	Permits mapping specific LDAP user groups in order to send their values to the RADIUS client. For each group listed in the table: • If the user is a member of the group, the LDAP group name (**Member Of**) is assigned to the **RADIUS Attribute**. • If the user is not a member of the group, the **Default Value** is assigned to the **RADIUS Attribute**. If the **Default Value** is not defined, the **RADIUS Attribute** will not be sent to the RADIUS client. Click **Add a new row to 'User Specific Groups to RADIUS Client'**, and enter the following fields: • **Member Of**: The LDAP group name. • **RADIUS Attribute**: the name of the RADIUS attribute which will receive either the LDAP group name from **Member Of**, or the **Default Value**, depending on whether the user is a member of the group or not. • **Default Value**: The value to assign to the named **RADIUS Attribute** when the user is not a member of the LDAP group listed in **Member Of**. If the **Default Value** is not defined, the **RADIUS Attribute** will not be sent to the RADIUS client.
Check Groups	Select this option to initiate PingID authentication only after users are confirmed as members of a group defined in **Member of Groups**. When selected, the RADIUS PCV filters groups according to the following configuration fields: • LDAP Group Name • Fail Login if the User is not Member of the LDAP Group
Check Bypass Groups	Select this option to bypass PingID authentication only after users are confirmed as a member of at least one of the groups defined in the '**Member Of Bypass Groups**' section.
If the User is not Activated on PingID	Defines how authentication requests are handled if a user is not registered in the PingID cloud service, or if the user's mobile device is unpaired. Select either: • **Register the user** (default): Initiate PingID registration for unregistered users and users without a paired mobile device. • **Always fail the login**: Fail authentication requests for unregistered users and users without a paired mobile device. • **Fail login unless in grace period**: If the user is not registered in PingID by the mandatory enrollment date, access is denied. • **Let the user in without pingid**. If the primary authentication (delegate PCV) is successful, allow authentication requests to proceed.

Parameter	Description
Fail Login on PingID Technical Error	If selected, authentication requests fail if the PingID cloud service is unavailable. When it is not selected, the PingID MFA process is bypassed. This option is enabled by default. **Note** This field is deprecated in PCV 2.0, and replaced by **AUTHENTICATION DURING ERRORS**.
Fail Login if the User is not member of the LDAP Group	Select or clear the checkbox. • Selected: Authentication fails if the user is not included in any of the groups defined in the **LDAP Group Name** field. • Cleared (default): If a user is not member of any of the groups listed in Member of Groups, authentication will proceed without using PingID. **Note** This option is ignored if **Let the user in without PingID** is selected. If no groups are listed in **Member of Groups**, this field is ignored and authentication requests are performed using both LDAP and PingID authentication.
Enable RADIUS remote network policy server	Enable the RADIUS PCV to work through a Remote Network Policy Server to support MS-CHAPv2 protocols.
RADIUS Network Policy Server IP	The source IP address of the RADIUS endpoint Network Policy Server (NPS) used to validate user credentials.
RADIUS Network Policy Server Port	The port number for the RADIUS endpoint Network Policy Server (NPS) used to validate user credentials.
RADIUS Server Authentication Port	The port number assigned to the PingID PCV RADIUS server. The RADIUS server listens for requests from RADIUS clients on this port. The default value is `1812`. **Note** If you are using more than one RADIUS PCV instance in the same PingFederate environment, this value must be unique for each RADIUS PCV instance.
Domain Postfix	A domain name postfix (including '@') that can be appended to the username standardize the PingID usernames throughout the various PingID services (e.g., SSO). This field is left blank by default.

Parameter	Description
PingID Properties File	The PingID properties file configures the trusted connection between the RADIUS PCV and the relevant tenant in the PingID service. From the PingID configuration window, download the PingID properties file and then upload it to the PingID RADIUS PCV instance in PingFederate. For information see Configuring a RADIUS server on PingFederate **Note** To ensure the properties file is encrypted, it must be uploaded to the PingID RADIUS PCV instance in PingFederate.
Authentication During Errors	Determines how to handle user authentication requests when PingID services are unavailable. • **Bypass User**: Accept the user's first factor authentication, and bypass the PingID MFA flow when the PingID MFA service is unavailable. • **Block User**: Reject and block the user's login attempt when the PingID MFA service is unavailable. • **Passive Offline Authentication**: Fallback to the PingID offline MFA flow when the PingID MFA service is unavailable. Users will be asked to access MFA offline manual authentication from the PingID mobile app using a mobile device previously registered with PingID, and enter a 12-digit authentication key to obtain an authentication code to authenticate. See also Configuring offline MFA (PingID Adapter). • **Enforce Offline Authentication**: Force PingID offline MFA flow regardless of the PingID MFA service availability. **Note** • This parameter replaces **Fail Login on PingID Technical Error**, which is deprecated in PCV 2.0.
Users Without a Paired Device	When PingID services are unavailable, you can choose to bypass or block users who have no paired mobile device (**pf-pingid-local-fallback** attribute in user's device list in the user directory). • **Bypass User** indicates users without paired mobile devices will bypass the PingID adapter in an authentication attempt. • **Block User** indicates users without paired mobile devices will have PingID block their authentication attempt. A user's individual block or bypass **State** attribute in the user directory will override the **USERS WITHOUT A PAIRED DEVICE** definition. **Note** This configuration is only relevant if **Passive offline authentication** or **Enforce offline authentication** were chosen in the `AUTHENTICATION DURING ERRORS` field. See User directory for PingID offline MFA for more details.

Parameter	Description
LDAP Data Source	The directory data source used to retrieve additional user attributes for offline MFA. This is the data store in which the users device list (pf-pingid-local-fallback attribute) is stored. If **RADIUS Remote Network Policy Server** mode is enabled, or if **Delegate PCV** is defined as **LDAP As Attribute Source**, all user attributes are retrieved from this directory data source.
Create Entry for Devices	Create the device list entry in the data source if it does not exist. This is the configuration setting for how and when PingFederate will create PingID device entries of type **pf-pingid-device**. **Note** Applicable only when **pf-pingid-local-fallback** is added to **pf-pingid-device**. • **Checked**: PingFederate will create objects of type **pf-pingid-device** per user, and add the device list information in its **pf-pingid-local-fallback** attribute. • **Unchecked**: PingFederate will assume that the **pf-pingid-device** objects per user are being created by an external system, and will only modify the **pf-pingid-local-fallback** attribute attached to them when needed.
Encryption Key for Devices	This field contains the base64url encoded HMAC256 encryption key to encrypt the users devices list before saving to the user directory. This field is optional. If this field is empty, the devices lists will be kept unencrypted and will be stored as plain text. **Note** • If the admin changes the encryption key, all users will have to authenticate online at least once, in order for new device details to be kept locally, or else the behavior in an offline scenario will follow the **USERS WITHOUT A PAIRED DEVICE** setting.
Search Base	The location in the directory from which the LDAP search begins. To be used when the offline authentication attributes are stored on the user entry in the main user LDAP. **Note** Applicable when **pf-pingid-local-fallback** is added to the user object. If **RADIUS Remote Network Policy Server** mode is enabled, or if the**Delegate PCV** is defined as the**LDAP as attribute source**, all user attributes are retrieved from this location in data source.

Parameter	Description
Search Filter	The basis of what to filter, when the device list is stored on the user's object in the user directory. The **Search Filter** parameter value must be identical to the **Search Base** field in the relevant **Password Validator Instance Configuration**. You may use `${username}` as part of the query. Example (for Active Directory): `sAMAccountName=${username}`. **Note** • Applicable only when **pf-pingid-local-fallback** is added to the user object. If **RADIUS Remote Network Policy Server** mode is enabled, or if **Delegate PCV** is defined as the LDAP**As Attribute Source**, all user attributes are retrieved with help of this filter.
Scope of Search	The options for determining the width and depth of the search, when the device list is stored on the user's object in the user directory: • **One level**: search only in the defined branch, and not in its subtrees. • **Subtree**: search in the defined branch, and all of its subtrees. **Note** • Applicable only when **pf-pingid-local-fallback** is added to the user object.
Distinguished Name Pattern	The pattern used to save device entries. It points to the location in the directory in which the **pf-pingid-device** objects reside. **Important** • You may use either this **DISTIGUISHED NAME PATTERN** setting, OR the set of the 3 SEARCH configuration settings (**SEARCH BASE**, **SEARCH FILTER** and **SCOPE OF SEARCH**) above. • **DISTIGUISHED NAME PATTERN** must be used in either of the following scenarios: ◦ When using more than one PCV or PingID Adapter instance with more than one configured PingID tenant. ◦ When both the PCV and PingID Adapter are configured with more than one tenant. • This parameter is required only if offline authentication is enabled when the **pf-pingid-local-fallback** attribute is saved separately from the user object. If **RADIUS Remote Network Policy Server** mode is enabled, or if **Delegate PCV** is defined as **LDAP As Attribute Source**, all user attributes are retrieved with the help of this pattern.

Parameter	Description
State Attribute	The **STATE ATTRIBUTE** is used to override how a specific user is authenticated during offline authentication. The value of this field is the name of the attribute configured in the directory. If the PingID services are unreachable, the value of **STATE ATTRIBUTE** is evaluated: • **Bypass**: the user bypasses PingID MFA. • **Block**: (case insensitive), the user will be blocked from performing the PingID offline MFA flow, and denied access. • Empty: the user attribute set in the directory won't be used during offline authentication. **Note** The exact name of the attribute configured in this field must also be added in the **Extended Contract** tab of the relevant Delegate PCV. This parameter is unrelated to the **State Encryption Key** parameter in the following table.

Advanced Parameters

PingID RADIUS PCV Configuration - Advanced Parameters

Parameter	Description
Server Threads	Enter a number to specify a fixed number of threads that can use a shared unbounded queue to service RADIUS requests. If no value is specified, new threads are created as required, and previously constructed threads are reused when available. **Note** Threads that have not been used for 60 seconds are terminated and removed from the pool.
Enable RADIUS Server	Select the checkbox to enable the integrated RADIUS Server. This option is enabled by default.
Default Shared Secret	Specify the default RADIUS shared secret. If specified, the RADIUS shared secret is used for any client that is not found in the RADIUS client configuration.
Application Name	Label to show on the PingID app's authentication screen instead of the default text ("vpn").

Parameter	Description
Application Icon	Icon to show on the PingID app's authentication screen instead of the default icon. The format of the graphic must be JPEG or PNG, and the graphic must be 100px x 100px or less, and 150 kB or less. The value of the parameter should be a valid URL that begins with *https*.
State Encryption Key	The base64 URL-encoded 256-bit key used to protect the integrity of the RADIUS state attribute. The RADIUS #24 State attribute is auto-generated by the PingID PCV and should not be modified. This parameter is unrelated to the **State Attribute** parameter in the previous table.
State Lifetime	The amount of time that the RADIUS server waits for a response before timeout (in seconds). The default value is `300`.
Radius Client Doesn't Support Challenge	The RADIUS client doesn't support the access-challenge message in the RADIUS protocol. This mode also supports RADIUS clients which send the user collected OTP to the RADIUS server using the password field, for example Amazon Workspaces. **Supported authentication methods for this mode**: Mobile App (Swipe, Biometrics, OTP), Desktop App, OATH tokens, Authenticator app and YubiKey. **Not supported:** SMS, Voice and Email. **User experience:** • If a mobile App user wishes to authenticate using swipe or biometrics, then OTP shouldn't be entered in the RADIUS client password field. • If a mobile App user's device is offline, then the user should enter the App generated OTP in the password field, after the password, using the separator defined in **OTP in Password Separator**. • If using the Desktop App or YubiKey, the user should enter the App or YubiKey generated OTP in the password field, after the password, using the separator defined in **OTP in Password Separator**. • If the user is registered with multiple devices supported by this mode, an OTP generated by any one of those devices will authenticate the user. • This mode does not support on-the-fly registration.
OTP in Password Separator	If the **Radius Client Doesn't Support Challenge** is activated, and OTP fallback is enabled: • **Comma**: At login, users must enter their password followed by a comma, and then the OTP. • **None**: At login, users must concatenate the OTP to the end of their login password (without spaces, commas or any other separator).
Radius Client Password Validation	When the RADIUS client validates the user password, the RADIUS PCV will not get the password at all, and as a result, will not validate it. If the RADIUS client does not support the RADIUS challenge, the user's OTP might be in the password field.

Parameter	Description
Direct OTP Validation	Perform OTP validation for RADIUS clients that do not support access-challenge or do not have a Delegate PCV configuration, as well as for clients opting to use LDAP as an Attribute Source within the Delegate PCV setup. This allows the LDAP as an attribute source in the Delegate PCV setup to be used to map the `username` with the `PingID Username Attribute`. For example, This allows a RADIUS request with username `jtan` to be sent to PingID server for OTP validation with the username `janetan@pingidentity.com`.
PingID Username Attribute	The name of the attribute from the delegate PCV's attribute contract that will be used as the PingID username for the RADIUS originated authentication.
PingID Heartbeat Timeout	The duration of time in seconds that the adapter will wait for the heartbeat calls to the PingID service, before falling back to the **AUTHENTICATING DURING ERRORS** feature. If left empty, the default is 30 seconds.
Newline Character	Select the line separation character that you want to use for RADIUS server challenge messages. Choose from: • None • Unix style ('\n') • Windows style ('\r\n") • HTML (' ')

Configuring offline MFA (RADIUS PCV)

Offline multi-factor authentication (MFA) allows users to authenticate if the PingID server is inaccessible. To circumvent unforeseen outages or network issues preventing users from signing on to access their applications, implement the offline MFA feature of the RADIUS Password Credential Validator (PCV).

Before you begin

- Install the latest version of the PingID Integration Kit.
- Have PingID RADIUS PCV 2.0 or later.
- Have a user directory to store user's device information from PingID. For more information, see User directory for PingID offline MFA.
- Have Unlimited Strength Java Cryptography Extension (JCE), which is required for supporting the 256-byte key size for cryptographic algorithms. Without it, the feature will return an exception related to the missing library and will not function.

About this task

To configure offline MFA, sign on to the PingFederate administrative console and configure the RADIUS PCV for offline authentication. This configuration includes settings to support different LDAP deployment implementations, such as storing the user device lists on the user object, on a separate devices object, or in a different directory, separate from the user directory.

Steps

1. Sign on to the PingFederate administrative console.
2. Click **Server Configuration**.
3. In the **Authentication** section, click **Password Credential Validators**.

   Result:

   The **Manage Credential Validator Instances** window displays.
4. Click **PingID PCV (with integrated RADIUS server)**.

   Result:

   The **RADIUS** instance summary window displays.
5. Click the **Instance Configuration** tab.
6. Click **Show Advanced Fields**.
7. Configure the offline authentication options.

Parameter	Description
Authentication During Errors	Determines how to handle user authentication requests when PingID services are unavailable. ◦ **Bypass User**: Accepts the user's first factor authentication and bypasses the PingID MFA flow when the PingID MFA service is unavailable. ◦ **Block User**: Rejects and blocks the user's login attempt when the PingID MFA service is unavailable. ◦ **Passive Offline Authentication**: Falls back to the PingID offline MFA flow when the PingID MFA service is unavailable. Users are asked to scan a QR code with a mobile device previously registered with PingID to obtain an authentication code to authenticate. ◦ **Enforce Offline Authentication**: Forces PingID offline MFA flow regardless of the PingID MFA service availability. **Note** ■ User devices are updated in the directory for bypass, block and passive offline modes. ■ This parameter replaces **Fail Login on PingID Technical Error**, which is deprecated in PCV 2.0.

Parameter	Description
Users Without a Paired Device	When PingID services are unavailable, you can bypass or block users who have no paired mobile device, defined by the `pf-pingid-local-fallback` attribute in user's device list in the user directory. ◦ **Bypass User**: Users without paired mobile devices will bypass the PingID adapter in an authentication attempt. ◦ **Block User**: PingID blocks authentication attempts from users without paired mobile devices. A user's individual block or bypass `State` attribute in the user directory will override the `Users Without a Paired Device` definition. **Note** This configuration is only relevant if you select **Passive Offline Authentication** or **Enforce Offline Authentication** in the **Authentication During Errors** section. For more information, see User directory for PingID offline MFA.
LDAP Data Source	The user directory data source used for retrieving additional user attributes for PingID offline MFA. This is the data store in which the users device list, defined by the **pf-pingid-local-fallback** attribute, is stored.
Create Entry for Devices	Creates the device list entry in the data source if it does not exist. This is the configuration setting for how and when PingFederate will create PingID device entries of type **pf-pingid-device**. If selected, PingFederate creates objects of type **pf-pingid-device** per user, and adds the device list information in its `pf-pingid-local-fallback` attribute. Otherwise, PingFederate will assume that the **pf-pingid-device** objects per user are being created by an external system and will only modify the `pf-pingid-local-fallback` attribute attached to them when needed. **Note** Applicable only when **pf-pingid-local-fallback** is added to **pf-pingid-device**.

Parameter	Description
Encryption Key for Devices	This optional field contains the base64url encoded HMAC256 encryption key to encrypt the users devices list before saving to the user directory. If this field is empty, the devices lists are kept unencrypted and are stored as plain text. **Note** If the admin changes the encryption key, all users must authenticate online at least once in order for new device details to be kept locally, or else the behavior in an offline scenario will follow the `Users Without a Paired Device` setting.
Search Base	The location in the directory from which the user directory search begins. Use when the offline authentication attributes are stored on the user entry in the main user directory. It contains the value of the **Search Base** field in the relevant **Password Validator Instance Configuration**, and the PCV `Search Base` parameter value must be identical to that. **Note** Applicable only when **pf-pingid-local-fallback** is added to the user object.
Search Filter	The basis of what to filter when the device list is stored on the user's object in the user directory. The **Search Filter** parameter value must be identical to the **Search Base** field in the relevant Password Validator Instance configuration. You can use `${username}` as part of the query. For example (for Active Directory), `sAMAccountName=${username}`. **Note** Applicable only when **pf-pingid-local-fallback** is added to the user object.

Parameter	Description
Scope of Search	The options for determining the width and depth of the search when the device list is stored on the user's object in the user directory: ◦ **One level**: search only in the defined branch and not in its subtrees. ◦ **Subtree**: search in the defined branch and all of its subtrees. **Note** Applicable only when **pf-pingid-local-fallback** is added to the user object.
Distinguished Name Pattern	The pattern used to save device entries. It points to the location in the directory in which the **pf-pingid-device** objects reside. **Important** ◦ You can use either the `Distinguished Name Pattern` setting or the set of the **Search Base**, **Search Filter** and **Scope of Search** configuration settings above. ◦ `Distinguished Name Pattern` must be used in either of the following scenarios: ■ When using more than one PCV or PingID Adapter instance with more than one configured PingID tenant. ■ When both the PCV and PingID Adapter are configured with more than one tenant. ◦ This parameter is required only if offline authentication is enabled when the **pf-pingid-local-fallback** attribute is saved separately from the user object.

Parameter	Description
State Attribute	`State Attribute` overrides how a specific user is authenticated during offline authentication. The value of this field is the name of the attribute configured in the directory. If the PingID services are unreachable, the value of `State Attribute` is evaluated: ◦ **Bypass**: the user bypasses PingID MFA. ◦ **Block**: (case insensitive), the user is blocked from performing the PingID offline MFA flow and denied access. ◦ Empty: the user attribute set in the directory won't be used during offline authentication. **Note** The exact name of the attribute configured in this field must also be added in the **Extended Contract** tab of the relevant Delegate PCV.
PingID Heartbeat Timeout	The duration of time in seconds that the adapter waits for the heartbeat calls to the PingID service, before falling back to the `Authenticating During Errors` feature. If left empty, the default value is 30 seconds.

8. Click **Done**.

   Result:

   The **Manage Credential Validator Instances** window is displayed.

9. Click **Save** to persist the updated configuration.

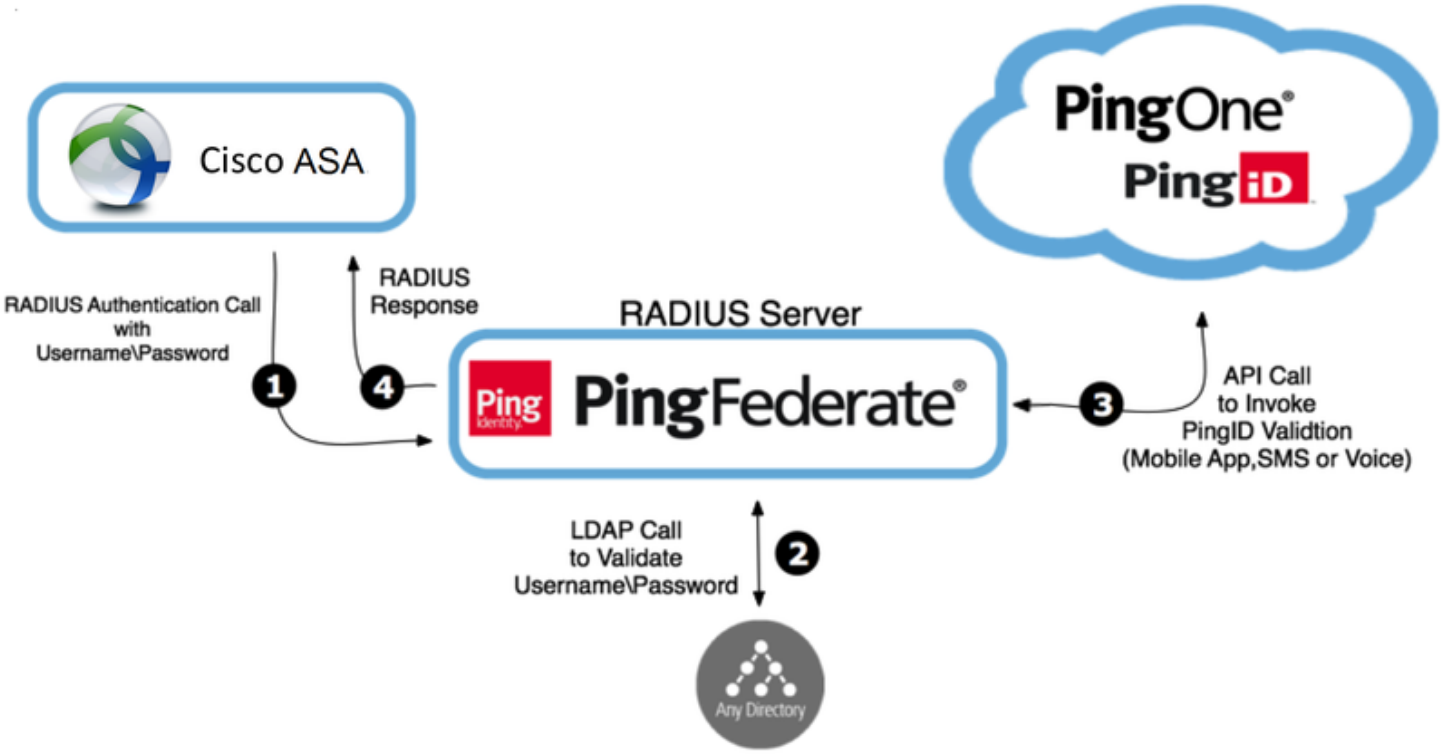
Configure Cisco ASA for PingID MFA

Overview of Cisco ASA for PingID MFA

This topic details the configuration required in your Cisco ASA VPN for integrating PingID multi-factor authentication (MFA).

How Multi-Factor VPN Authentication Works

The following image represents a general flow. Actual configuration varies according to company infrastructure considerations and policies.



Processing steps

1. When a user opens either their IPSec or SSL VPN sign-on window and enters a username and password, their details are sent to the RADIUS Server on PingFederate through the VPN.
2. PingFederate authenticates the user's credentials against the LDAP Server as first-factor authentication.
3. After LDAP authentication approval, the RADIUS server initiates second-factor authentication with PingID. If authentication is denied, the user's VPN window displays an error message.

Configuring Cisco ASA VPN for PingID MFA

Configure Cisco ASA VPN to work with PingID multi-factor authentication (MFA).

Before you begin

Configure the necessary settings in PingOne and PingFederate.

About this task

Configuring Cisco ASA for MFA involves the following steps:

- Adding an AAA server group
- Adding a Radius PCV server configuration

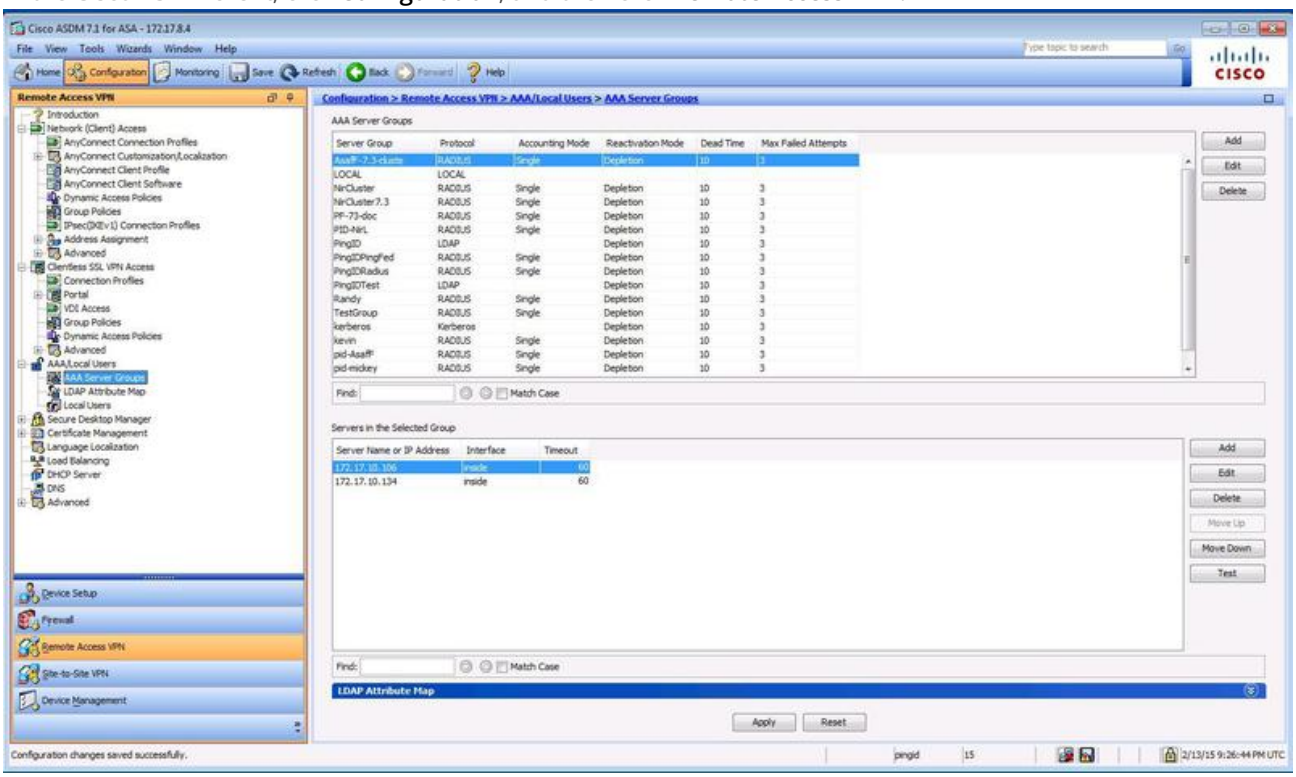
- One or both of the following steps:
  - Configuring a clientless SSL VPN
  - Configuring the network client profile

The following video describes the configuration process for your Cisco ASA VPN.

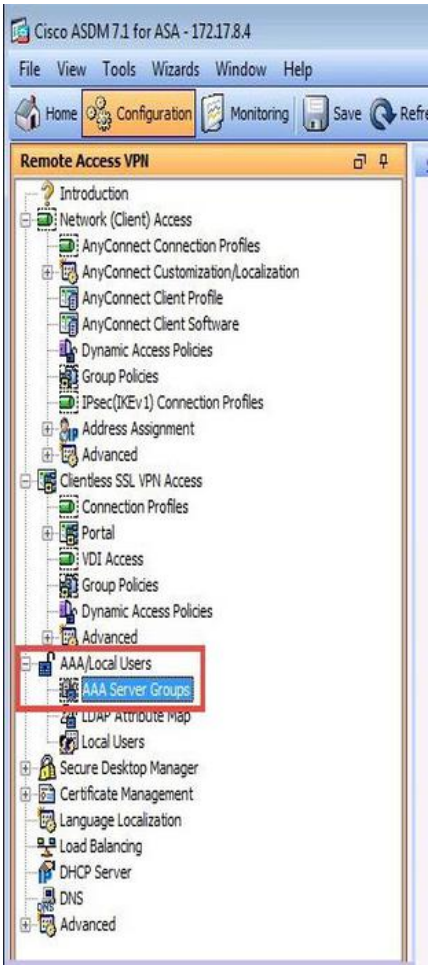
Your browser does not support the video tag.

Steps

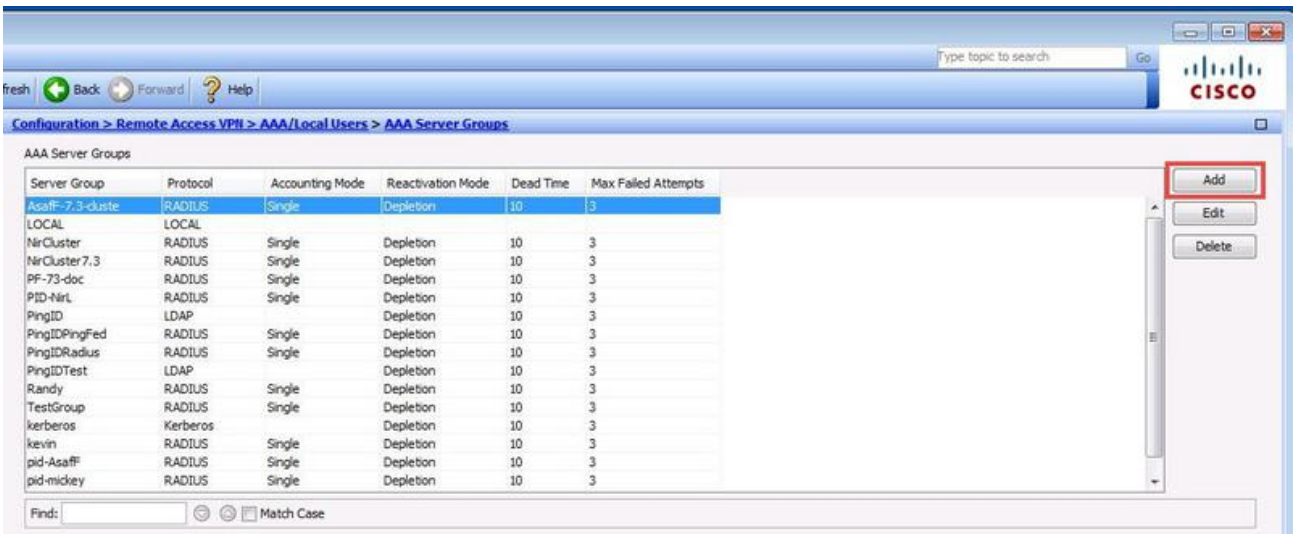
1. In the Cisco ASDM client, create an AAA Server Group to manage the security required for the RADIUS PCV Server configuration.
   1. In the Cisco ASDM client, click **Configuration**, and then click **Remote Access VPN**.



   2. In the **Remote Access VPN** navigation tree, go to **AAA/Local Users → AAA Server Groups**.

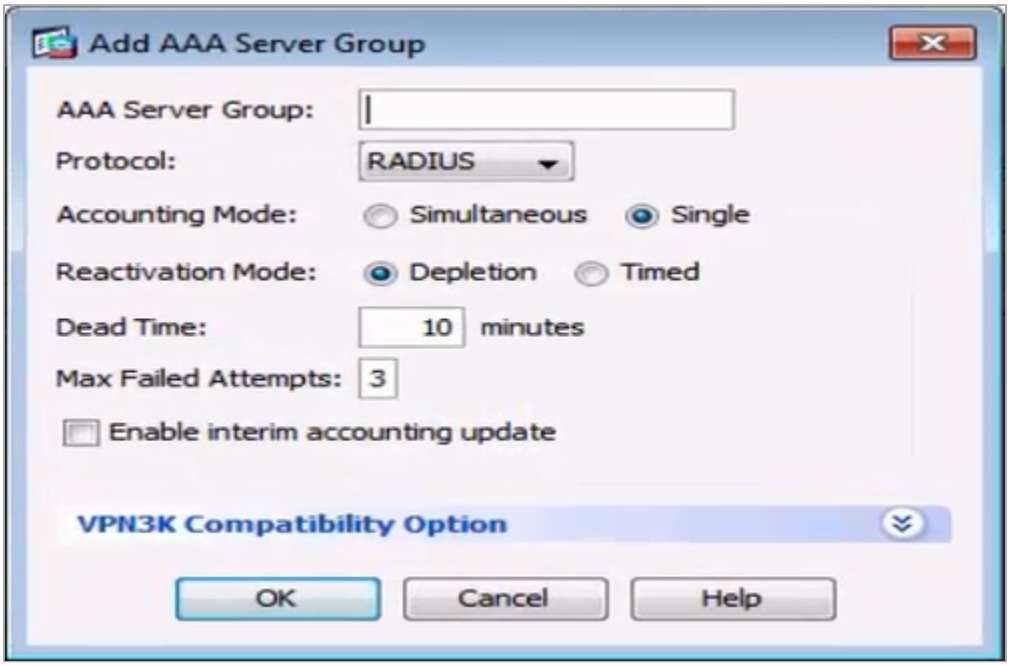


3. In the **AAA Server Groups** pane, click **Add**.



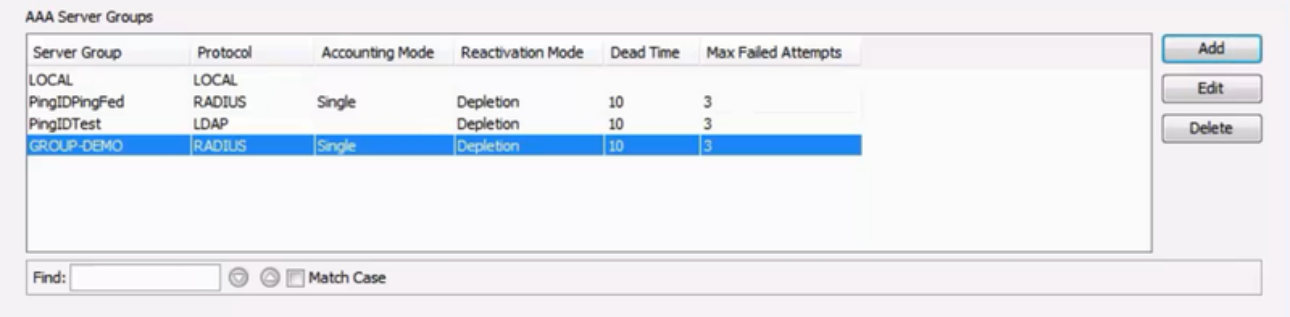
Result:

The **Add AAA Server Group** dialog box opens.

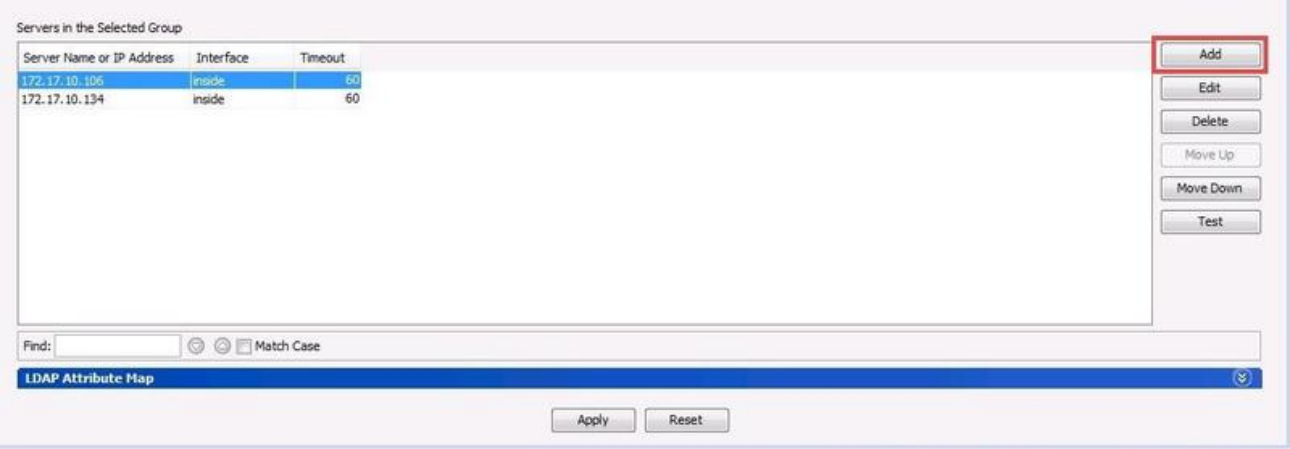


4. Enter values for the following parameters:
    - **AAA Server Group**: Enter the new server group name.
    - **Protocol**: Select the `RADIUS` protocol.
    - Accept the default values for all other fields, as shown in the **AAA Server Group** dialog box.
5. Click **OK**.

2. Add a new RADIUS PCV server configuration to the server group that you just created.
    1. In the **AAA Server Groups** pane, from the **Server Group** list, double-click the server group that you created in the previous step.

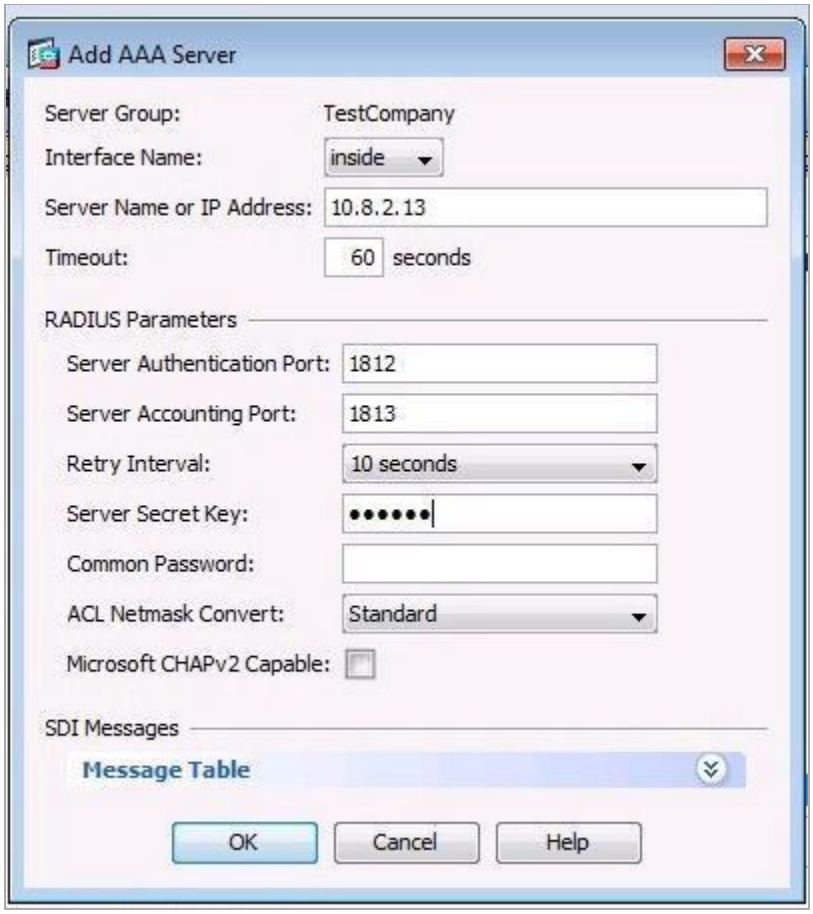


2. In the **Servers in the Selected Group** pane, click **Add**.



Result:

The **Add AAA Server** dialog box opens.



3. Enter values for the following parameters:

- **Server Name or IP Address:** Enter the IP address or server name of the PingFederate server that contains the RADIUS PCV server.
- **Timeout:** Change the timeout value to 60 seconds.

> **Note**
>
> This allows sufficient time for MFA to receive the necessary authentication approval.

- **Server Authentication Port:** Enter the port number configured in the RADIUS Server PCV. The default value is 1812.
- **Server Accounting Port:** Enter the port number configured in the RADIUS Server PCV.

> **Note**
>
> The **Server Accounting Port** number should be the next consecutive port following the port number configured for the **Server Authentication Port**. The default **Server Authentication Port** value is 1813.

- **Server Secret Key:** Enter the shared secret configured in the RADIUS Server PCV.

4. Click **OK**.

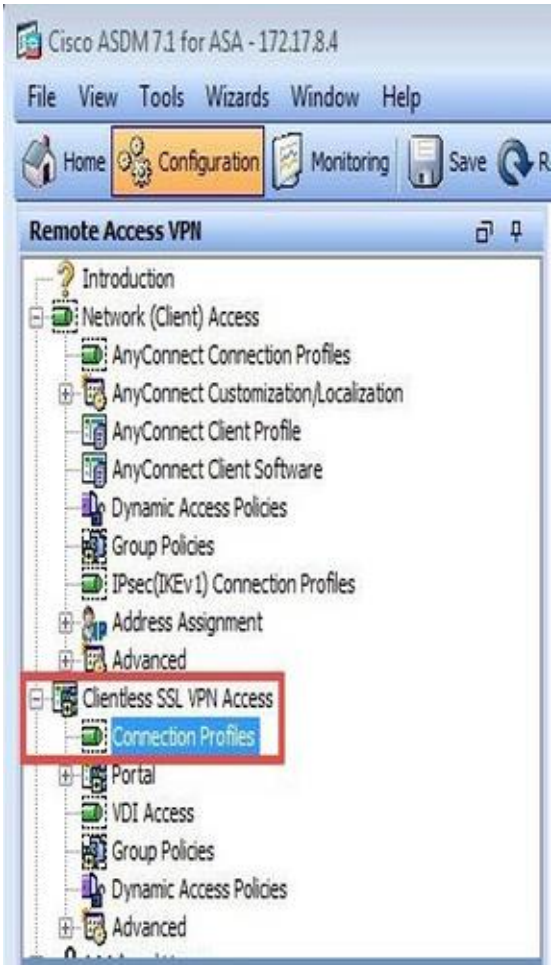
3. Configure a Clientless SSL VPN.

> **Note**
>
> If you do not plan on using a clientless SSL VPN, you can skip to the next section, which provides instructions on configuring the network client profile.

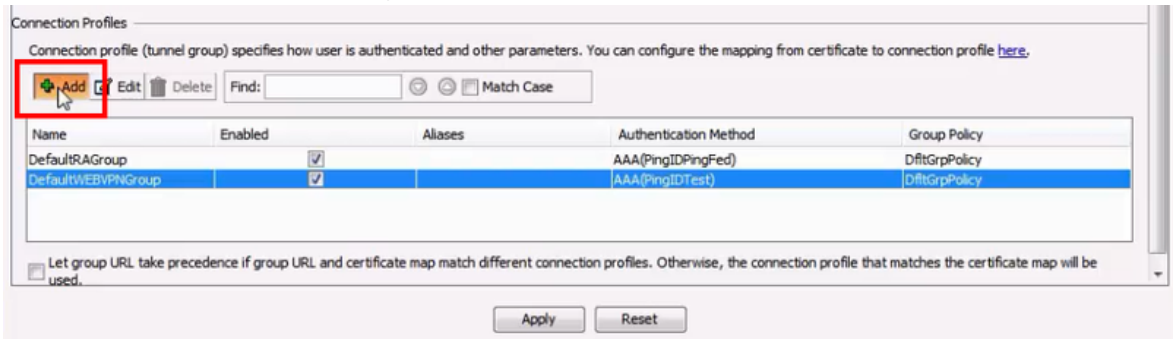
This includes the following steps:

- Configuring the connection profile by configuring the connection profile name, linking the AAA Server group to the Clientless SSL VPN profile, and selecting the related security policy.
- Configuring the connection alias.
- Configuring the group URL by defining the URL link that you provide to the user. The user enters the URL to sign on to the system through a browser.

1. In the **Remote Access VPN** navigation tree, go to **Clientless SSL VPN Access → Connection Profiles**.

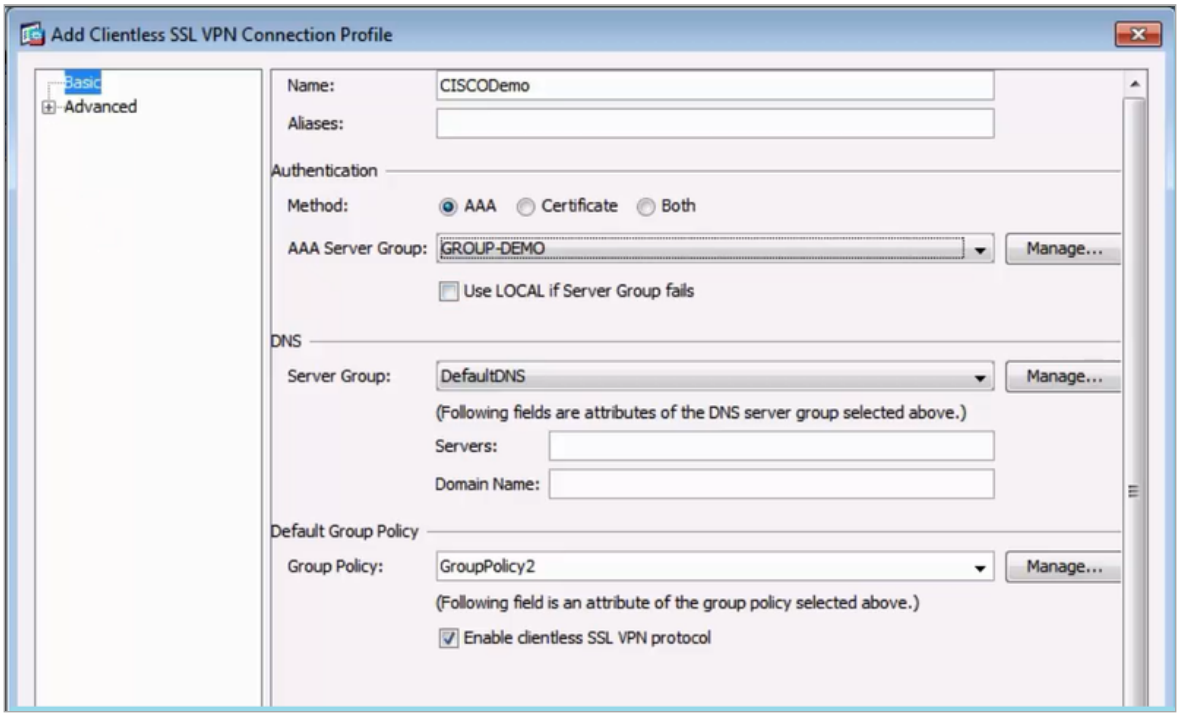


2. In the **Connection Profiles** section, click **Add**.

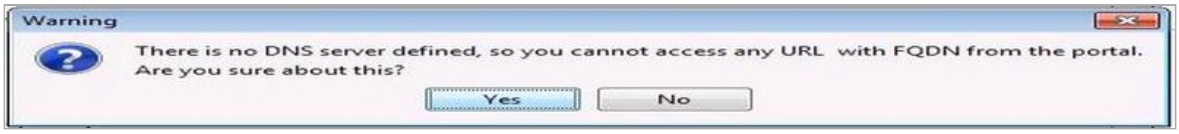


Result:

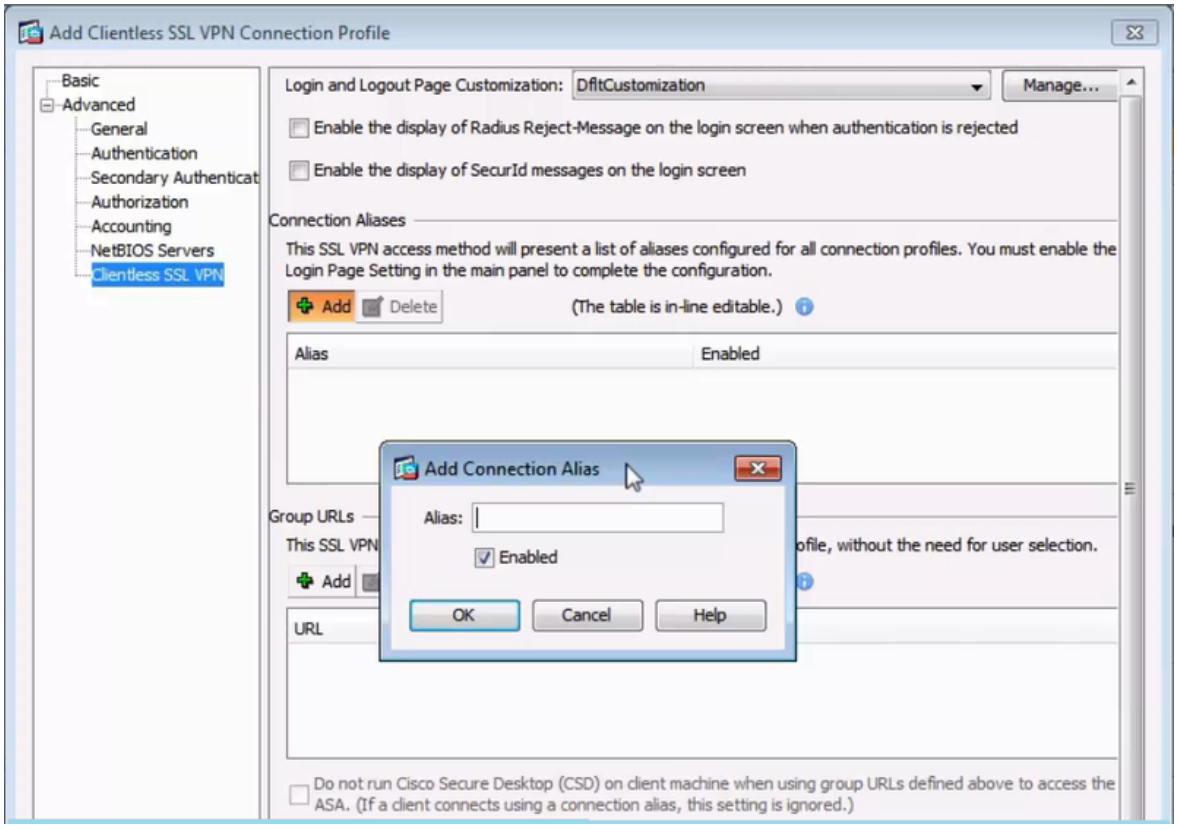
The **Add Clientless SSL VPN Connection Profile** dialog box opens.



3. Enter values for the following parameters:
    - **Name**: Enter the relevant server name.
    - **Authentication Method**: Select `AAA`.
    - **AAA Server Group**: Select the server group that you created in step 1.
4. In the left pane, go to **Advanced → Clientless SSL VPN**. If the following message appears, click **Yes**.



5. In the **Connection Aliases** section, click **Add**.



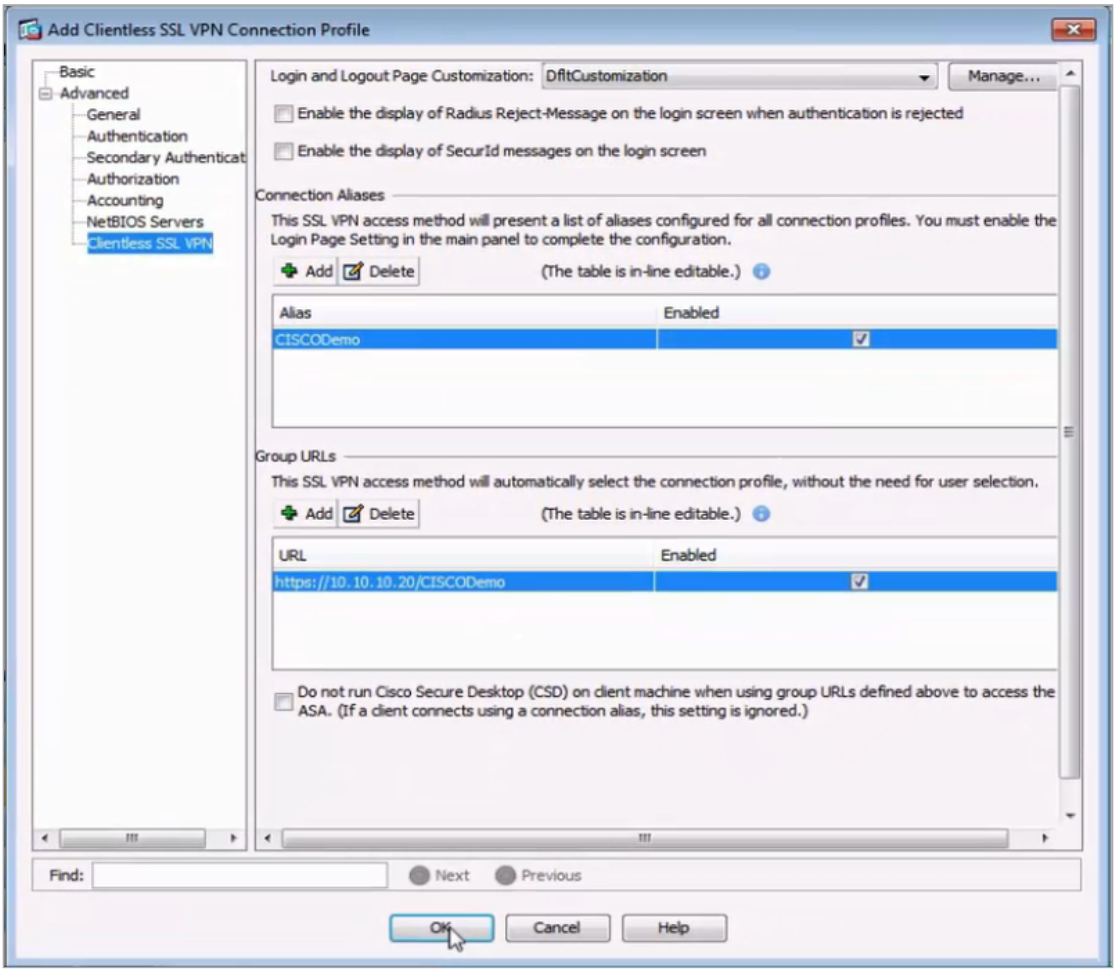
6. In the **Add Connection Alias** dialog box, enter a name in the **Alias** field.
7. Select the **Enabled** check box. Click **OK**.
8. In the **Group URLs** area, click **Add**.
9. In the **Add Group URL** dialog box, enter the server URL in the **URL** field.

> **Note**
>
> The group URL is the address you provide to the user to sign on to the Cisco VPN, and must have the format `https://<Cisco host name or IP address>/<Alias name>`.

10. Select the **Enabled** check box, and then click **OK**.

Result:

The URL is added to the Group URLs list.



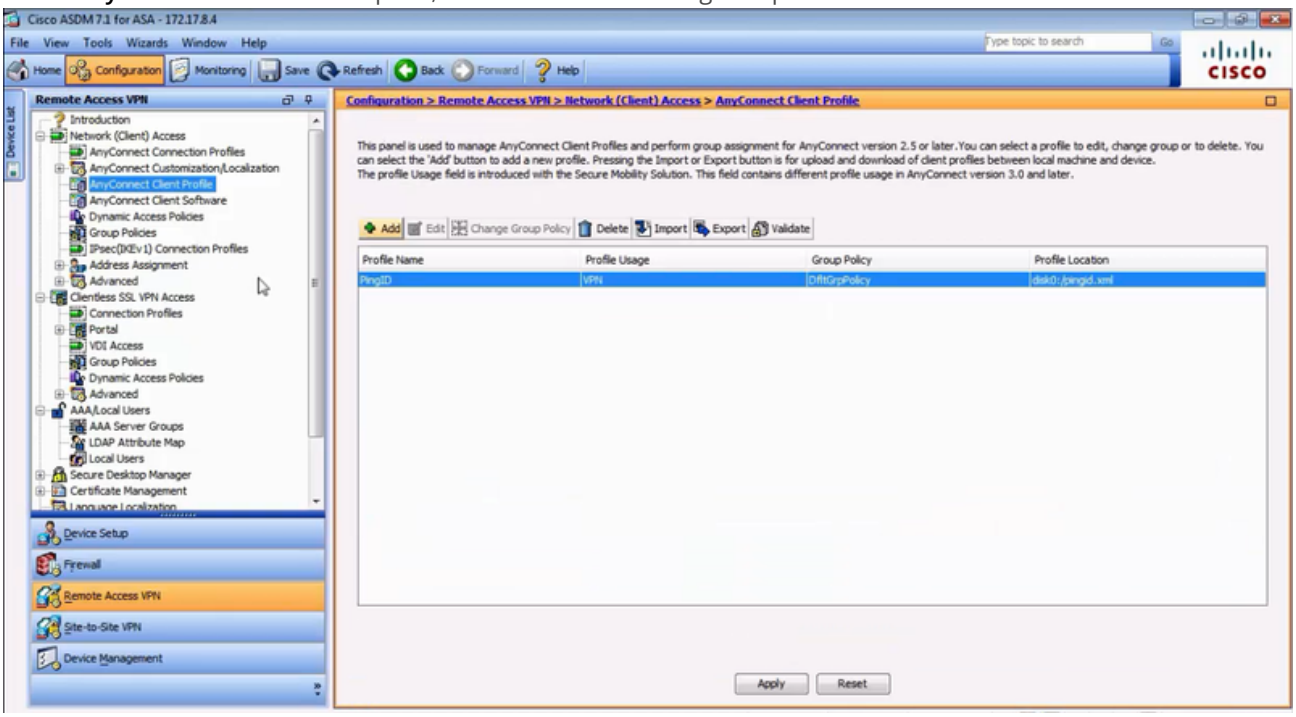
11. Click **OK**.

4. Configure the Network Client Profile to provide enough time for MFA to receive authentication approval.

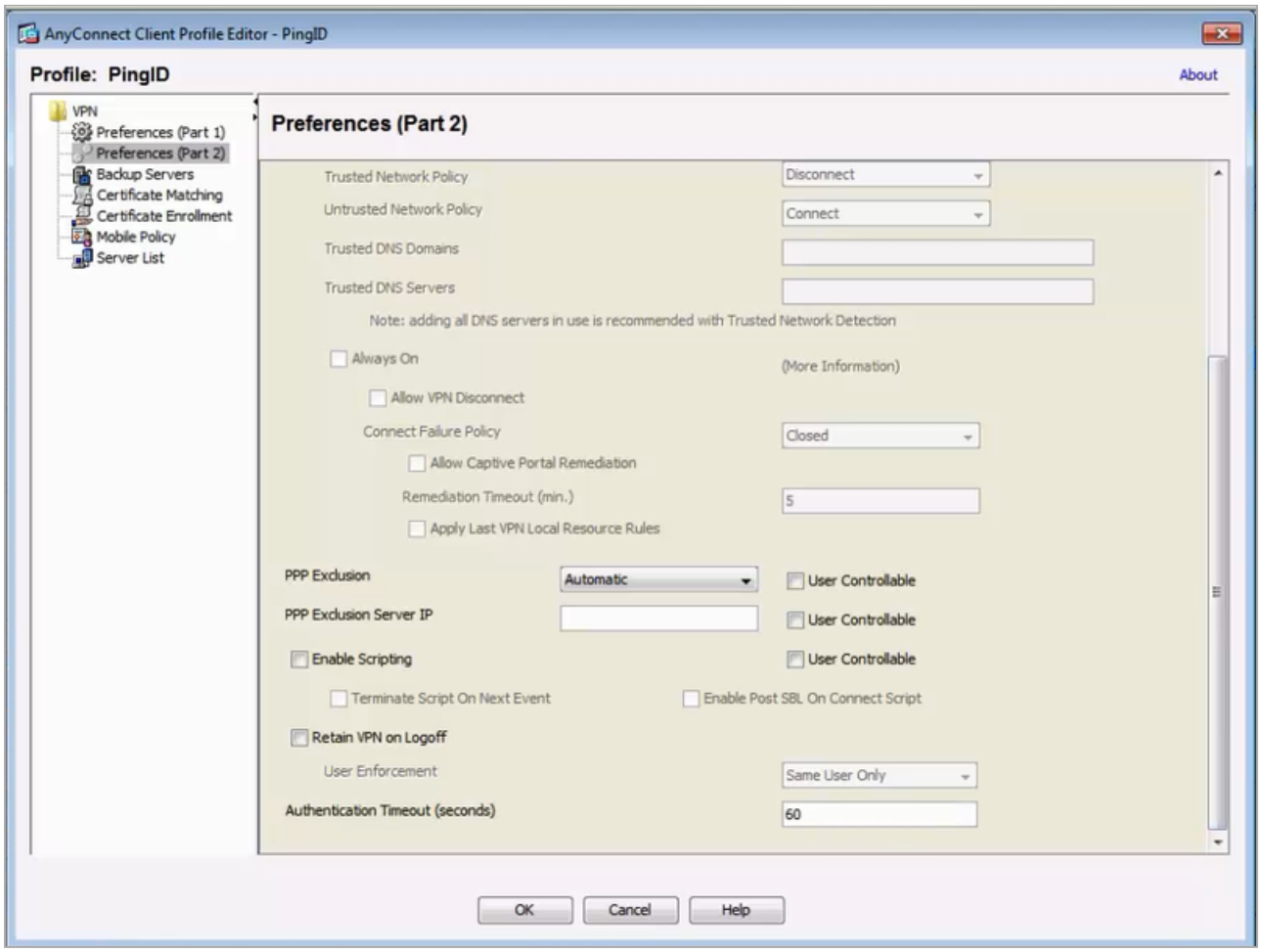
> **Note**
>
> If you carried out the steps in the previous section to configure a clientless SSL VPN, and do not plan on using a network client, you can skip the steps in this section.

1. In the **Remote Access VPN** navigation tree, go to **Network (Client) Access → AnyConnect Client Profile**.

2. In the **AnyConnect Client Profile** pane, double-click the existing VPN profile.



3. In the **Profile Tree**, select **Preferences (Part 2)**.



Result:

The **Any Connection Profile Editor – PingID** dialog box opens.

4. Set the **Authentication Timeout (seconds)** field to `60`. Click **OK**.

> **Note**
>
> This allows sufficient time for MFA to receive the necessary authentication approval when working with IPSec client.

5. In the **AnyConnect Client Profile** pane, click **Apply**.

Result:

The changes are applied and your configuration is complete.

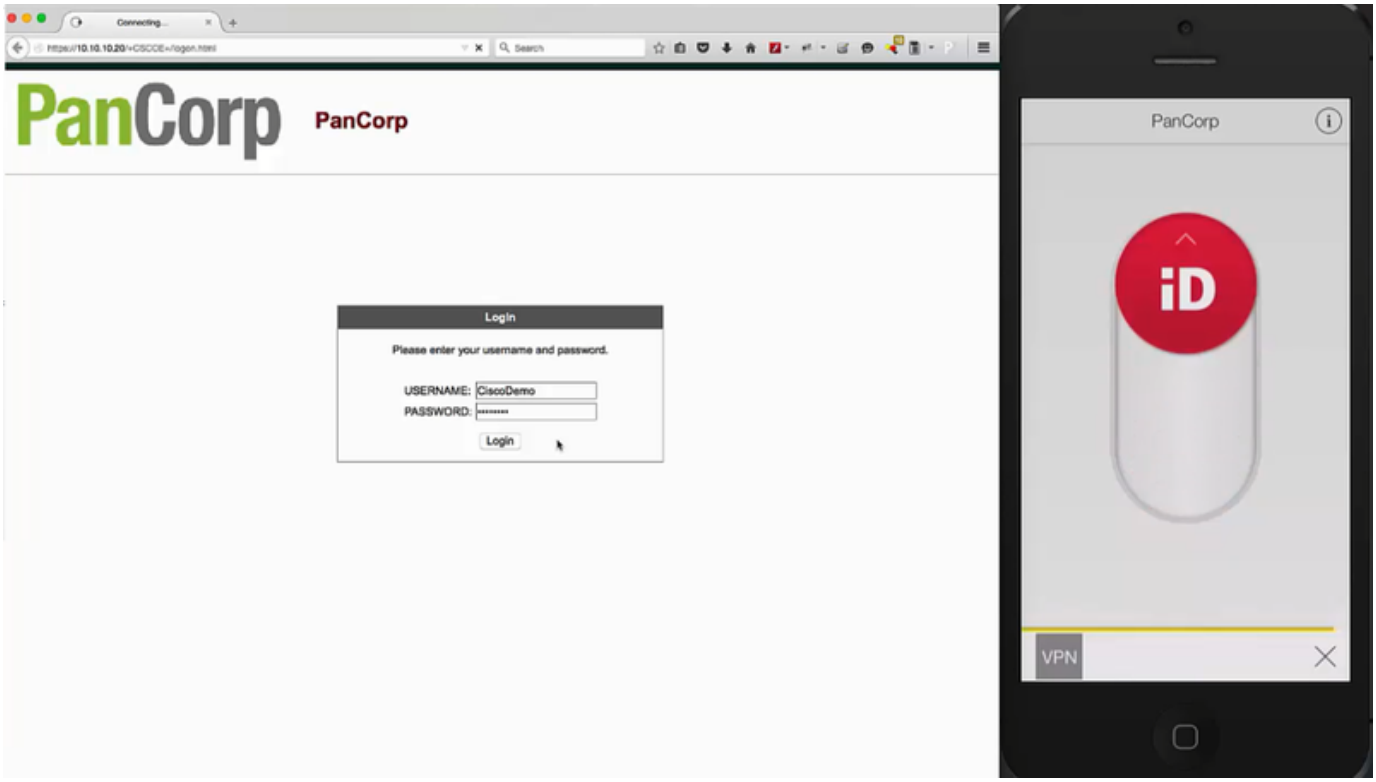
Signing on to the Cisco VPN using PingID as MFA

After Cisco ASA is configured for use with PingID, sign on to your Cisco VPN using PingID.

Steps

1. Open a browser and enter the group URL, as configured in Configuring Cisco ASA VPN for PingID MFA.
2. Enter your organization's username and password, and then click **Login**.
3. To complete the sign-on process using PingID as your MFA, follow the steps provided on the web browser page.

> **Note**
>
> When multi-factor authentication (MFA) is successful, you receive a push notification to your smartphone.



4. To approve the authentication request, swipe the slider up.

   Result:

   Authentication is complete, and your VPN connection is created.

Configuring Check Point VPN for PingID multi-factor authentication

This procedure details the configuration required in your Check Point VPN for integrating PingID multi-factor authentication (MFA).

Prerequisites

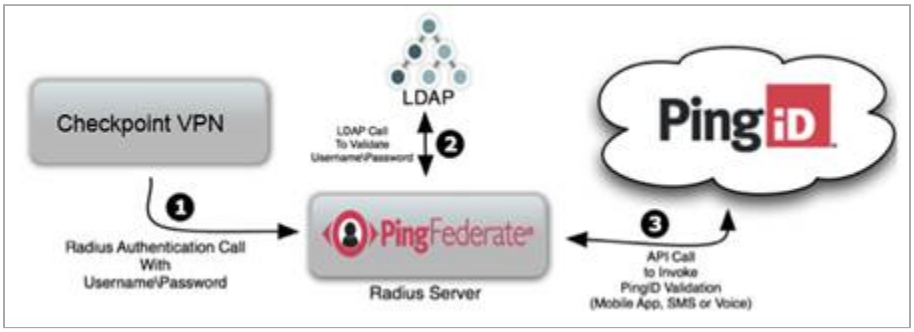
- You have installed Check Point VPN, including Check Point SmartConsole and SmartDomain Manager.
- You have configured the necessary settings in PingOne and PingFederate. For more information, see:
  - Configuring PingOne for Multi-Factor VPN Authentication
  - Configuring PingFederate for Multi-Factor VPN Authentication

About this task

The following video describes the Check Point VPN process.

{{{ Video removed }}}

The following image represents a general flow. Actual configuration will vary according to individual company infrastructure considerations and policies.



Processing steps

1. When a user opens their IPSec or SSL VPN login window and enters a user name and password, their details are sent to the RADIUS Server on PingFederate through the VPN.
2. PingFederate authenticates the user's credentials against the LDAP Server as first-factor authentication.
3. After LDAP authentication approval, the RADIUS server initiates second-factor authentication with PingID. If authentication is denied, the user's VPN window displays an error message.

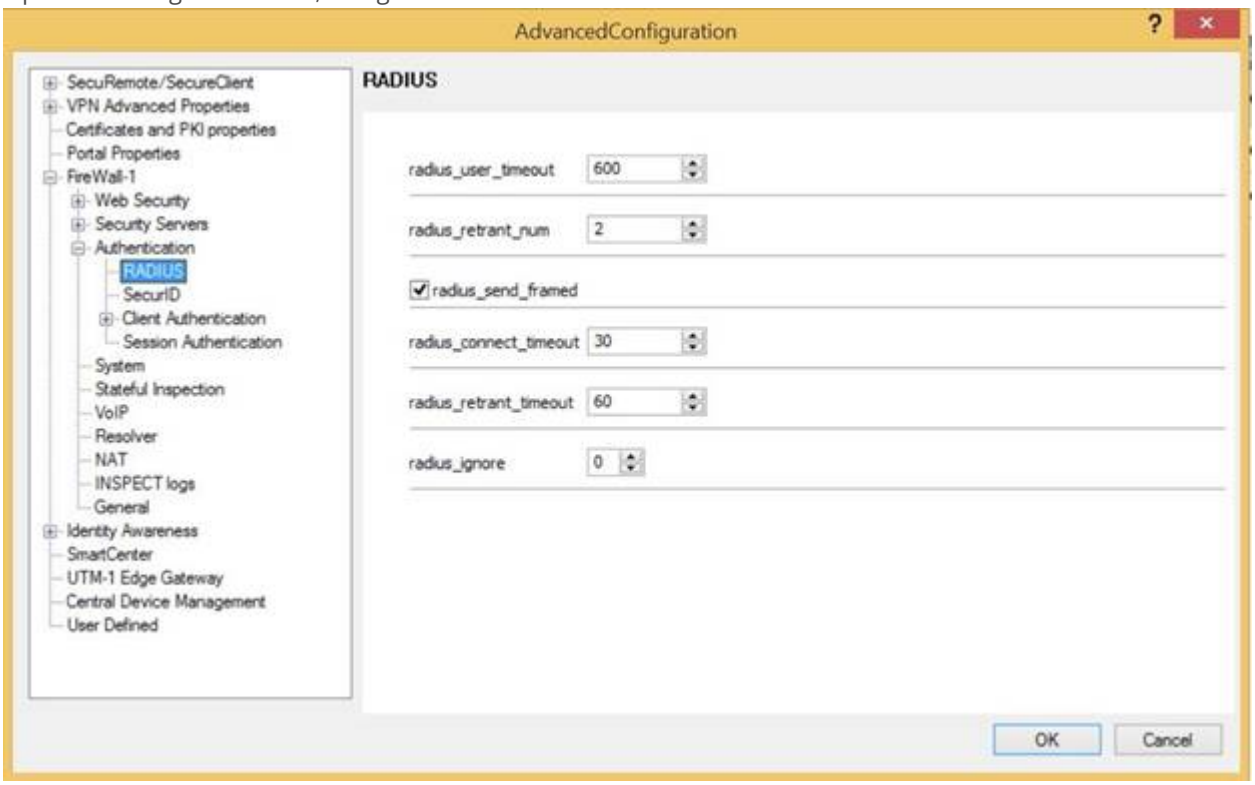
Configuring Global Properties

To configure Check Point VPN for PingID multi-factor authentication (MFA), you must configure Global Properties.

Steps

1. From the Windows **Start** menu, open the **Checkpoint SmartDashboard**.
2. Enter your username and password and click **Login**.
3. In the Check Point SmartDashboard, in the **Checkpoint** menu bar, click the **Menu** icon ( ). Go to **Policy → Global Properties**.
4. Click **Smart Dashboard Customization**.
5. Click **Configure**.

6. Open the configuration tree, and go to **FireWall-1 → Authentication → RADIUS**.



7. Configure the following settings:
    - **radius_user_timeout**: 600
    - **radius_retrant_num**: 2
    - **radius_send_frames**: Select the check box.
    - **radius_connection_timeout**: 30
    - **radius_retrant_timeout**: 60
    - **radius_ignore**: 0
8. Click **OK**.

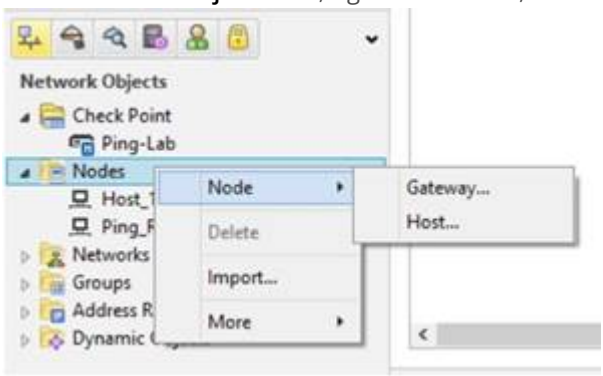
Configuring the RADIUS host

To configure Check Point VPN for MFA, you must configure the RADIUS host.

Steps

1. In the **Network Objects** toolbar, click the **Network Objects** tab ( ).

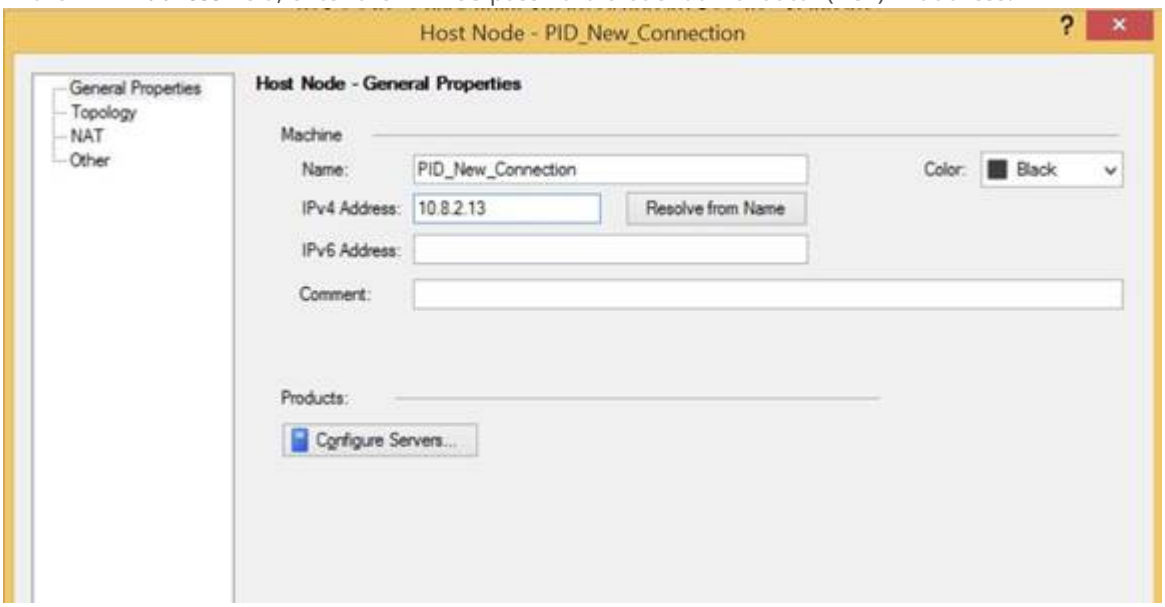
2. In the **Network Objects** tree, right-click **Nodes**, and then go to **Node → Host...**



3. In the **Host Node** dialog box, in the **Host Node** navigation tree, click **General Properties**.

4. In the **Name** field, enter the RADIUS host name.

5. In the **IPv4 Address** field, enter the RADIUS password credential validator (PCV) IP address.



6. Click **OK**.

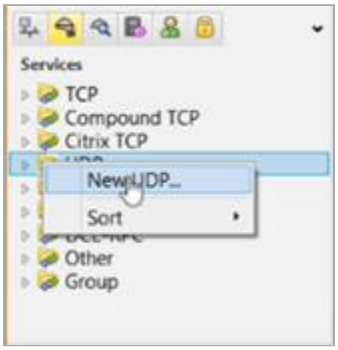
Creating a UDP entry

Create two UDP entries, one for the authentication port and one for the accounting port.

Steps

1. In the **Network Objects** toolbar, click the **Services** tab ().

2. In the **Network Objects** tree, right-click on **UDP** and select **New UDP...**



3. In the **UDP Service Properties - NEW-RADIUS** window, enter the following information:

   1. In the **Name** field, enter a name for the UDP service.
   2. In the **Port** field, enter the port number.

      The default port is 1812.

      > **Note**
      >
      > The port number must match the one defined in your RADIUS PCV configuration.

4. Click **OK**.
5. Repeat the process to create a UDP service for the RADIUS accounting port.

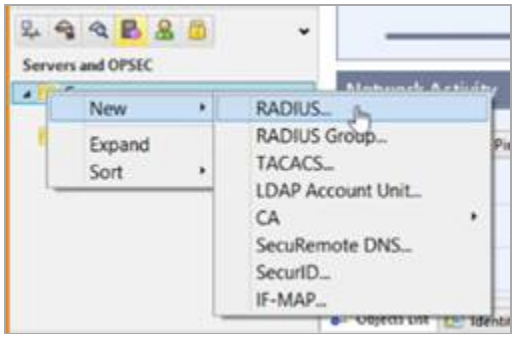
   > **Note**
   >
   > The RADIUS accounting port number should be the next consecutive number to the port number used for the authentication port.

Creating the VPN RADIUS server

To configure Check Point VPN for PingID MFA, you must create the VPN RADUS server.

Steps

1. In the **Network Objects** toolbar, click the **Servers and OPSEC** tab ( ).
2. In the **Network Objects** tree, right-click on **Servers** and go to **New → RADIUS...**.



The following window is displayed:

3. On the **General** tab, enter the following information.
    1. In the **Name** field, enter a RADIUS server name.
    2. From the **Host** list, select the RADIUS host that you created previously.

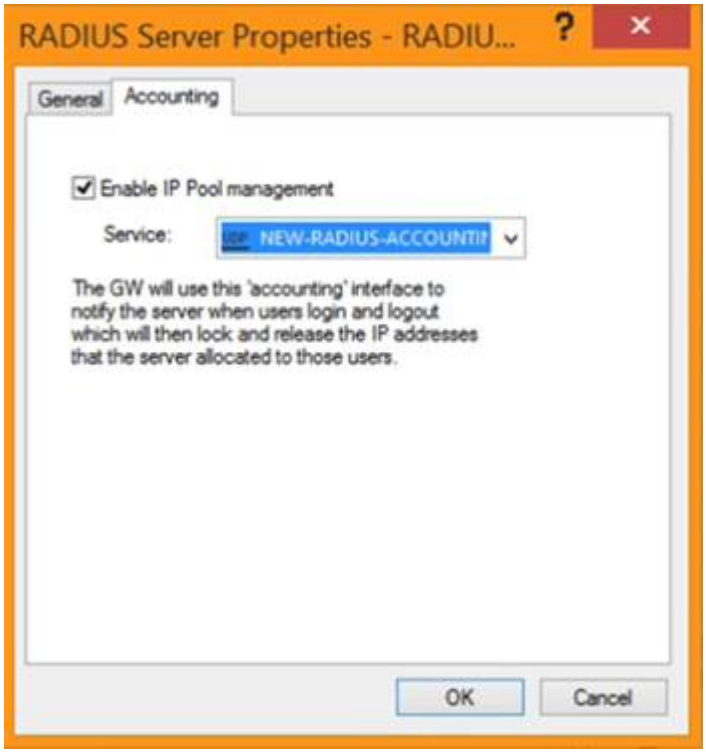
       For more information, see Configuring the RADIUS host.
    3. From the **Service** list, select the RADIUS service that you created previously.

For more information, see Create a UDP Entry.

1. In the **Shared Secret** field, enter the shared secret.

   > **Note**
   >
   > The shared secret must match the one configured in the RADIUS server PCV.

2. From the **Version** list, select **RADIUS Ver. 1.0 Compatible**.
3. From the **Protocol** list, select **PAP**.
4. Click the **Accounting** tab.



5. On the **Accounting** tab, enter the following information:
   1. Select the **Enable IP Pool Management** check box.
   2. From the **Service** drop-down menu, select the RADIUS accounting service you created earlier.

      For more information, see Create a UDP Entry.
6. Click **OK**.

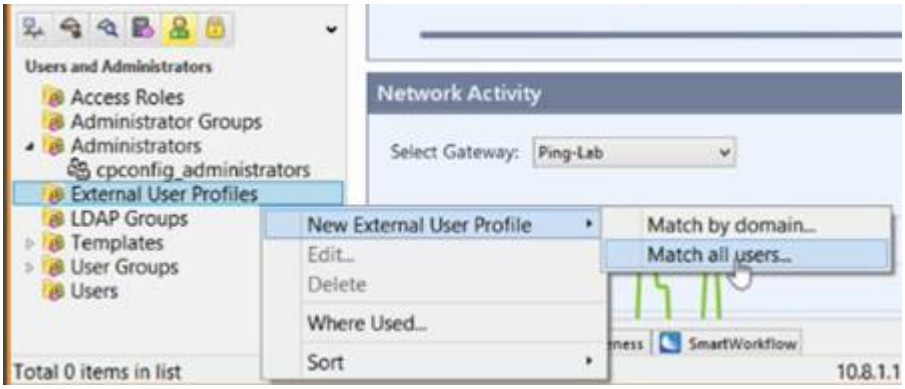
Configuring a RADIUS user profile

To configure Checkpoint VPN for PingID multi-factor authentication (MFA), you must configure a RADIUS user profile.

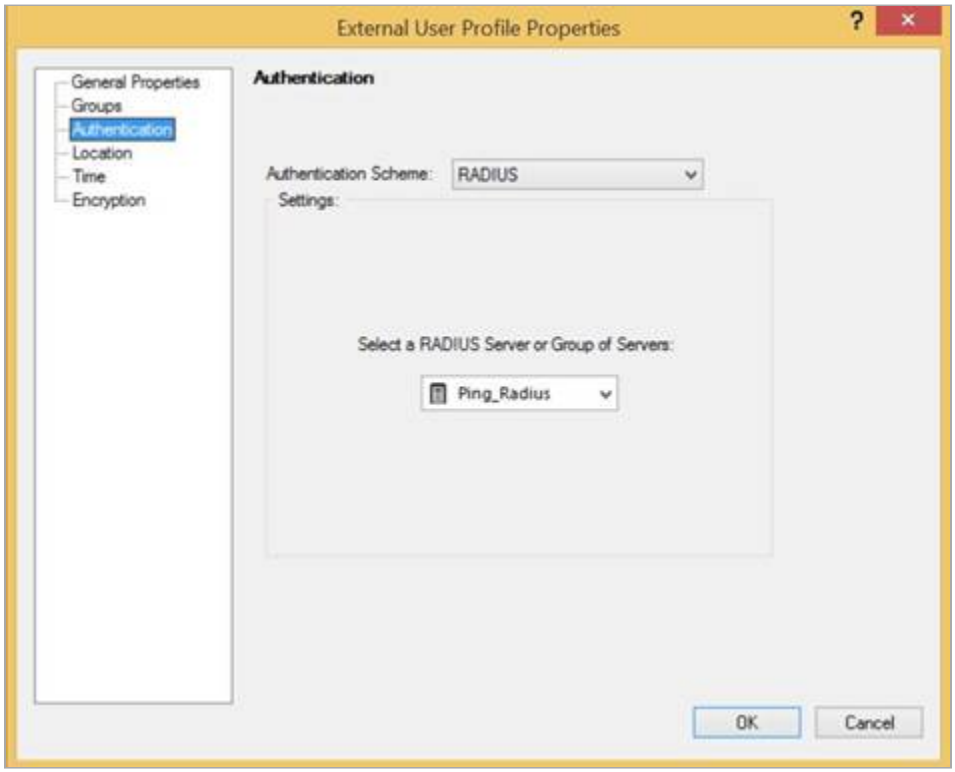
Steps

1. In the **Network Objects** toolbar, click  .
2. In the **Network Objects** tree, expand **External User Profiles**.
3. Double-click the **generic*** user profile.

> **Note**
>
> If the generic* user profile is not listed, right-click on **External User Profiles**, and select **New External User Profile → Match all users...**.

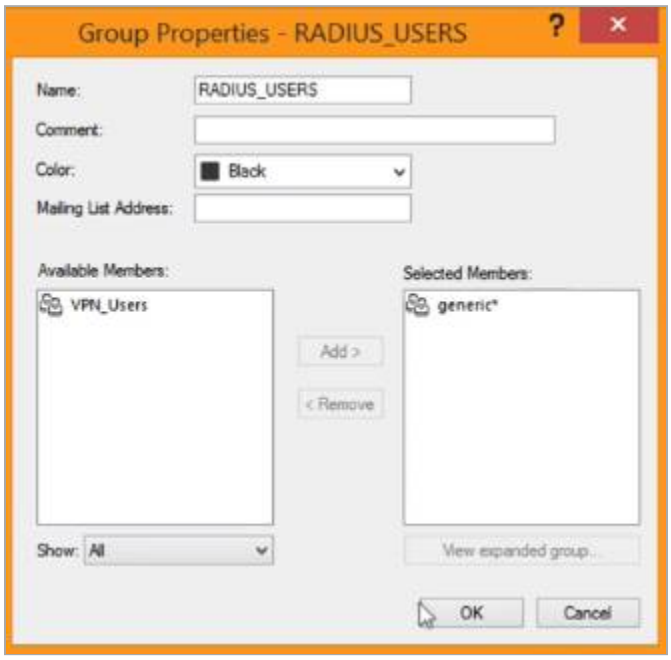


4. In the **External User Profile Properties** window, from the navigation tree, click **Authentication**.



5. In the **Authentication** window, enter the following information:
    1. From the **Authentication Scheme** list, select **RADIUS**.
    2. From the **Select a RADIUS Server or Group of Servers:** list, select the RADIUS server that you created previously.

       For more information, see Create the VPN RADIUS server.
6. Click **OK**.
7. In the **Network Objects** tree, right-click **User Groups**, and select **New Group...**.



8. In the **Group Properties - RADIUS_USERS** window, enter the following information:
    1. In the **Name** field, enter a name for the RADIUS group.
    2. From the **Available Members** pane, select **generic***. Click **Add**.

       Result:

       The generic member is added to the **Selected Members** list.
9. Click **OK**.

Setting the participating gateways

To configure Checkpoint VPN for PingID multi-factor authentication (MFA), you must set the participating gateways.

Steps

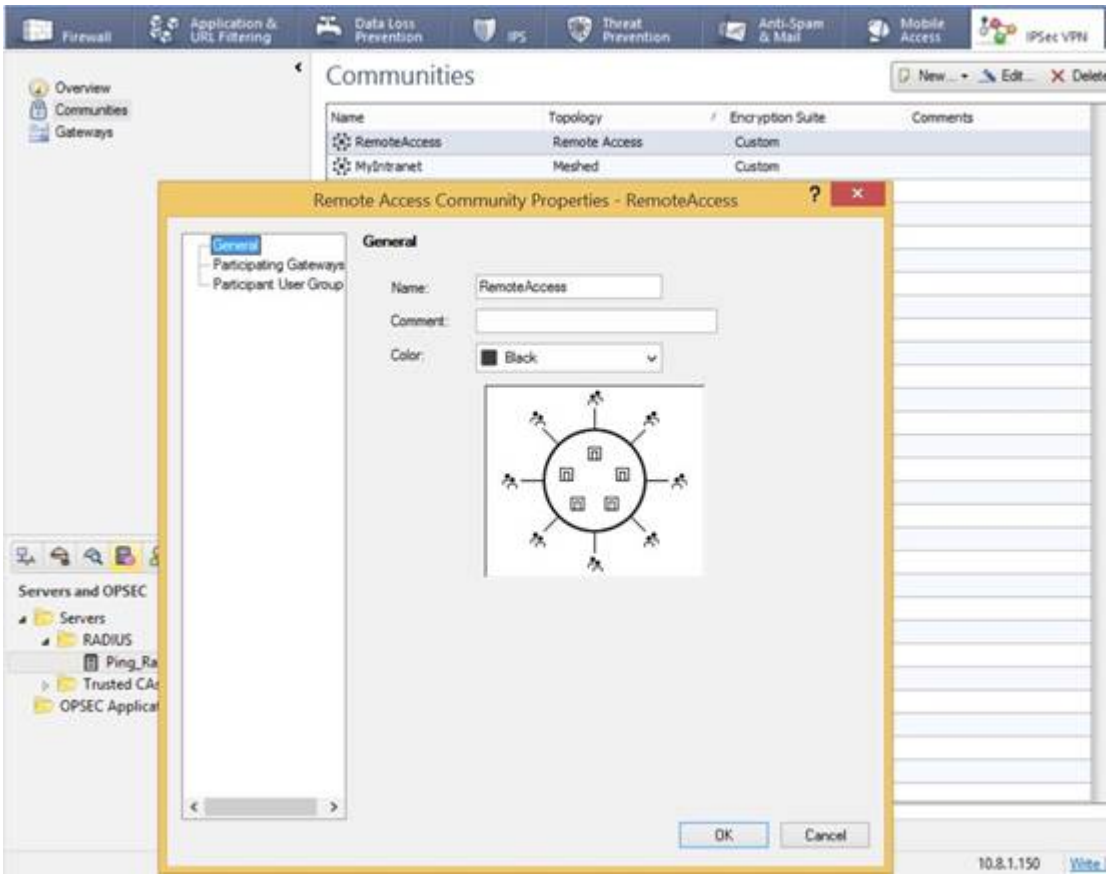
1. In the **Checkpoint** toolbar, click the **IPSec VPN** tab.

2. In the left navigation pane, click **Communities**.

   Result:

   The available communities are listed.

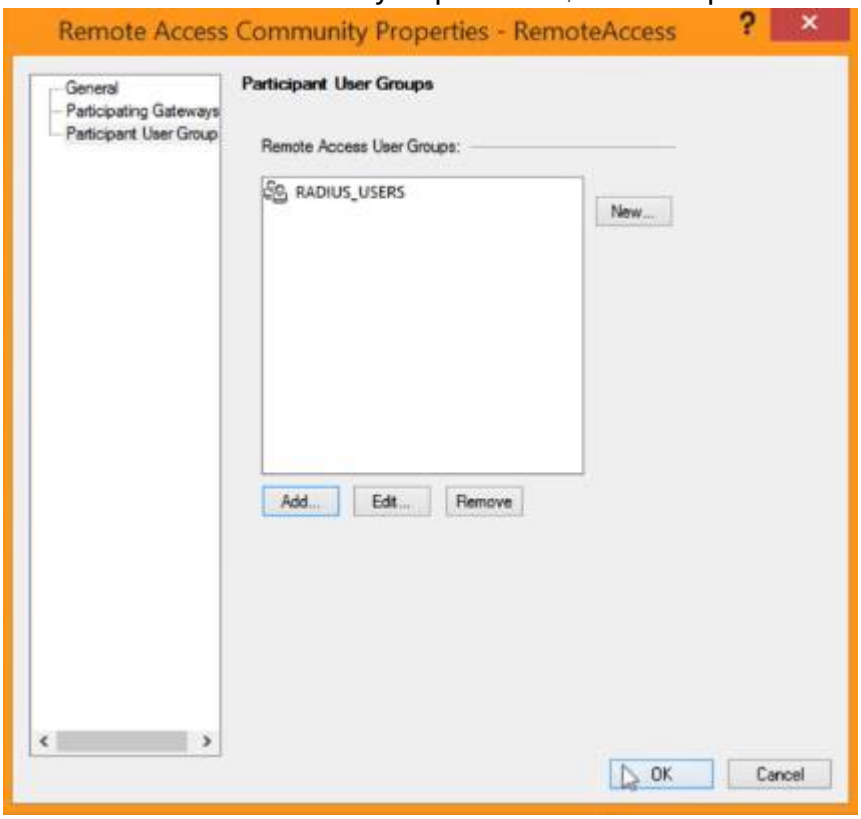
3. Double-click the **RemoteAccess** community.



4. In the **Remote Access Community Properties** window, in the navigation tree, click **Participating Gateways**.

5. If your checkpoint VPN gateway does not appear in the **Participant Gateway** list, click **Add**, and then select your VPN Gateway.

6. In the **Remote Access Community Properties** tree, click **Participant User Groups**.



7. If the user group you created is not listed, click **Add** and select the group from the list.
8. Click **OK**.

Adding a RADIUS rule

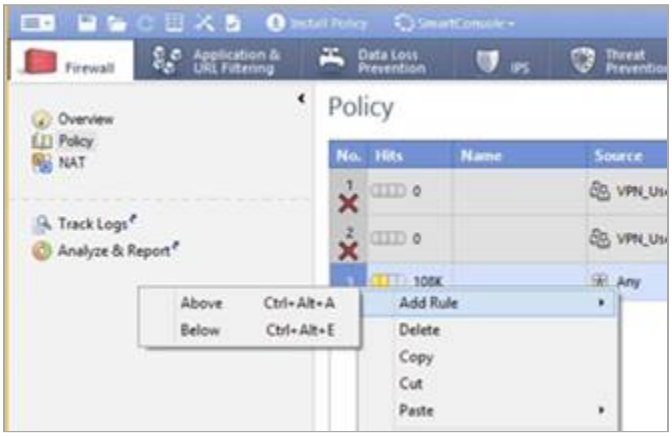
To configure Checkpoint VPN for PingID multi-factor authentication (MFA), you must add a RADIUS rule.

Steps

1. In the **Checkpoint** toolbar, click the **Firewall** tab.
2. In the upper left-hand tree, click **Policy**.

   Result:

   The rules of the existing policy are listed.
3. In the row for **Any**, in the **No.** column, right-click and select **Add Rule → Above**.



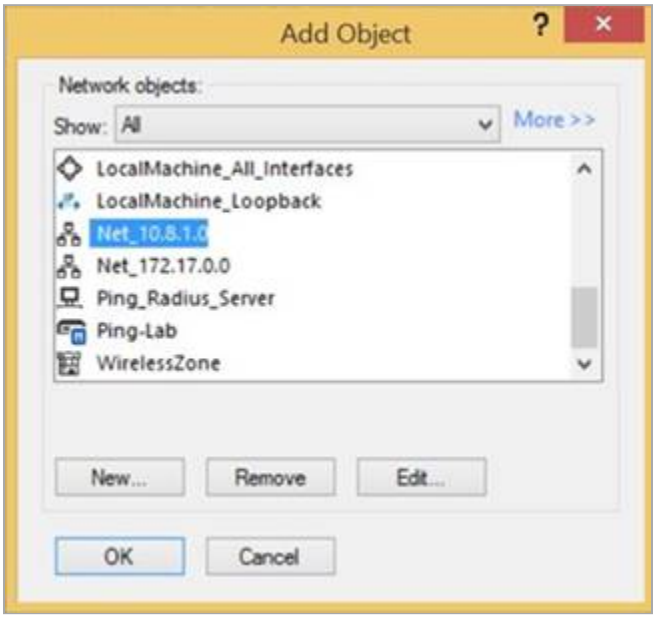
Result:

A new row is added to this policy.

4. In the new row, in the **Source** column, right-click **Any**, and then go to **Add Objects → Add Legacy User Access**.
5. In the **Legacy User Access** window, select the RADIUS user configured earlier. Click **OK**.

   For more information, see Configure a RADIUS user profile.

6. In the **Destination** column, right-click **Any** and select **Network Object**.
7. In the **Add Object** window, select the VPN network configured by your network administrator. Click **OK**.



8. In the **VPN** column, right-click **Any Traffic**, and then click **Edit Cell**.
9. In the **VPN Match Conditions** window, select **Only Connections Encrypted in Specific VPN Communities**.

10. Add the RemoteAccess community to the rule.
    1. In the **VPN Match Conditions** window, click **Add**.
    2. Select **RemoteAccess**. Click **OK**.
    3. To return to the main menu, click **OK**.
11. In the **Action** column of your RADIUS rule, right-click and select **Accept**.
12. In the **Track** column of your RADIUS rule, right-click **None**, and then select **Log**.

Defining a Mobile Access rule

The Mobile Access rule triggers when the authentication process approves a user's credentials. It defines the landing page that the user sees when they sign on.

Steps

1. In the **Checkpoint** toolbar, click the **Mobile Access** tab.
2. In the upper left-hand tree, click **Policy**.

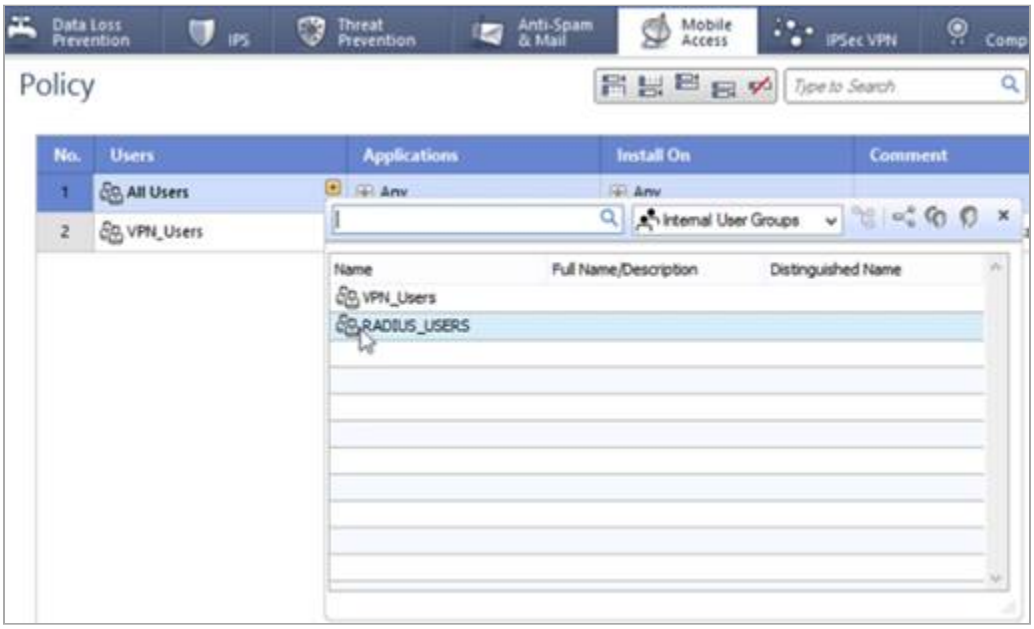
   Result:

   The existing policy is listed.
3. Right-click the **No.** column and select **New Rule**.

   Result:

   A new row is added to the list of rules.
4. In the **Users** column, click the **Plus** icon ( ) and select the Radius Users group that you previously created.

   For more information, see Configure a RADIUS user profile.

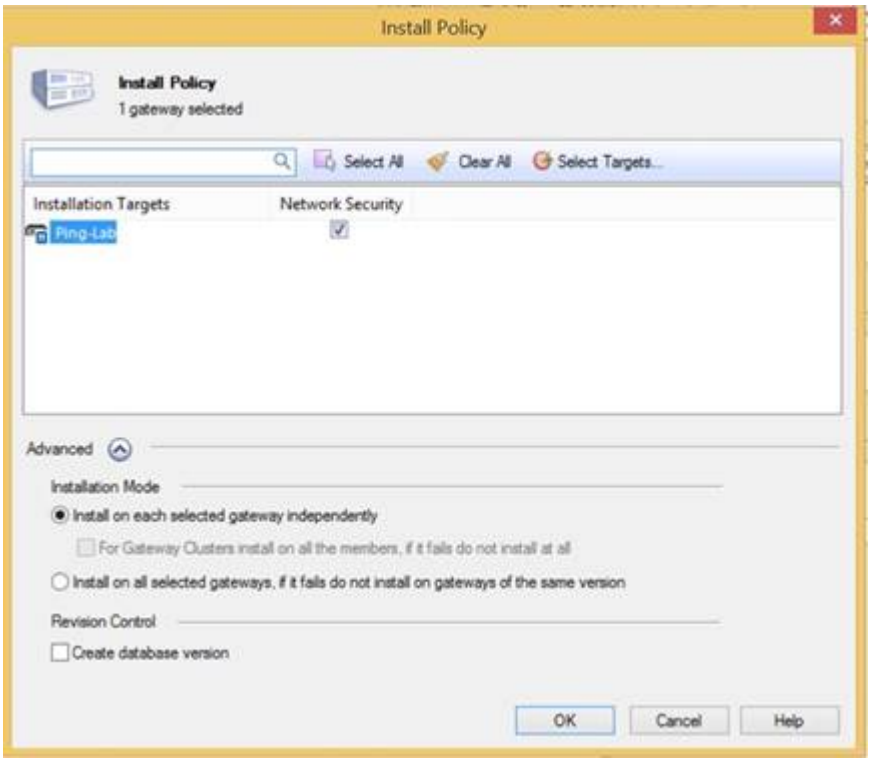


Committing the changes

To apply the configuration, commit the changes.

Steps

1. In the **Checkpoint** menu bar, click **Install Policy**.



2. Ensure that the **Install on Each Selected Gateway Independently** option is selected, and then click **OK**.

   Result:

   The configuration is verified and installed. A message appears when the policy installation is complete.

Signing on to the Check Point VPN for the end user

When the PingID RADIUS password credential validator (PCV) multi-factor authentication (MFA) configuration is complete, sign on to your Check Point VPN.

Steps

1. Open a browser and enter the URL of your Check Point external IP SSL VPN address, as configured in Configure the RADIUS host.

   > **Note**
   >
   > Enter the URL with a format of https://*<IP address or Check Point Hostname>*/sslvpn.
   > For example, https://PID_New_Connection/sslvpn or https://10.8.2.13/sslvpn.

2. Enter your organization's credentials and click **Sign In**.

   Result:

   You will receive a push notification to your mobile device.

3. To approve the authentication request, in the PingID mobile app, swipe the slider up.

> **Note**
>
> This might differ according to the organization's approved MFA devices.

Result:

PingID acknowledges the return notification from your mobile device, and access is granted.

Configuring Juniper for PingID multi-factor authentication

Configure Juniper VPN to work with PingID multi-factor authentication (MFA).

Configuring Juniper for MFA involves the following tasks:

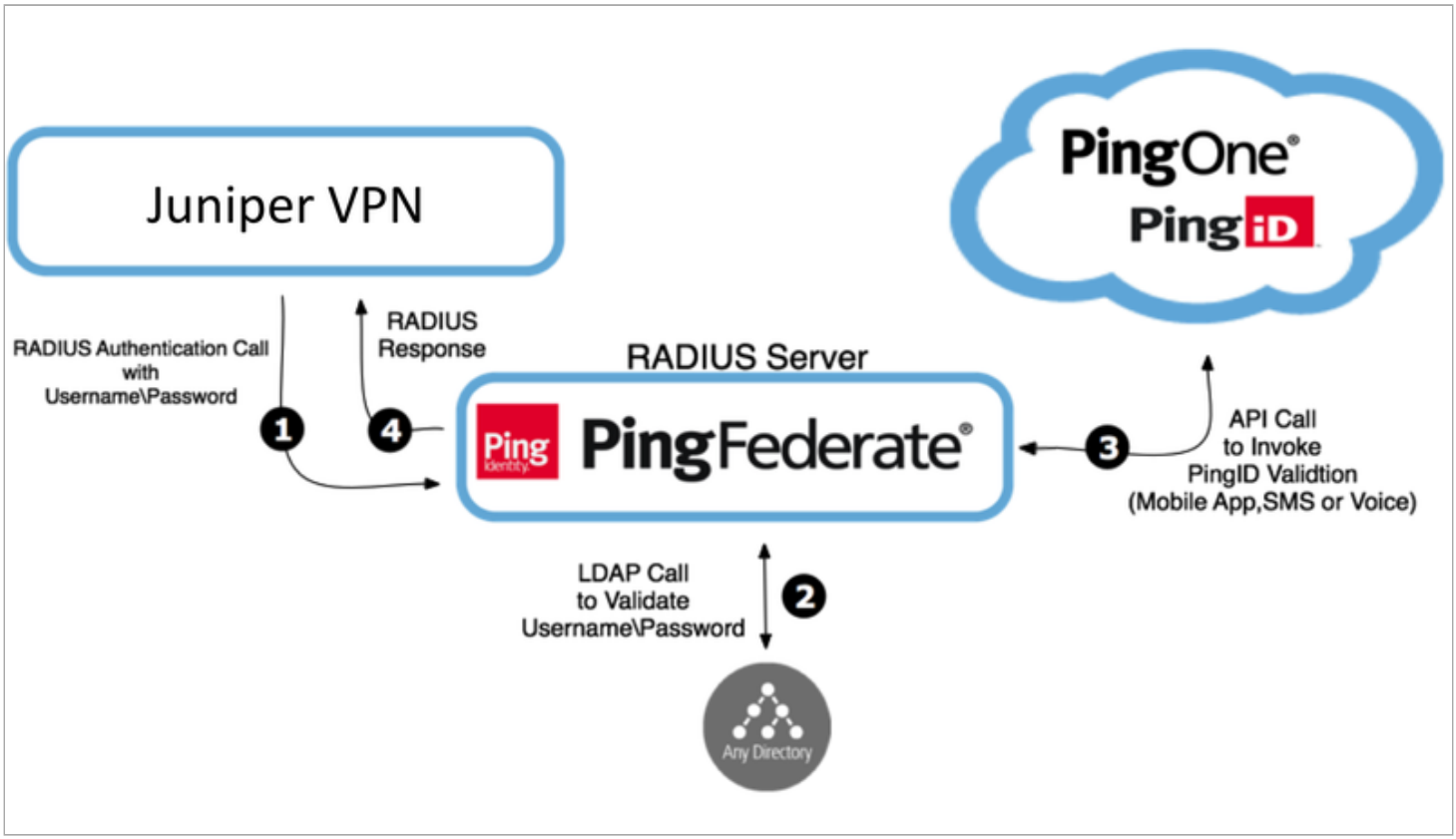
- Adding a RADIUS Server
- Adding a New Authentication Realm
- Configuring a Signing In Policy

The following video describes the Juniper VPN configuration process.

Your browser does not support the video tag.

How it works

The following image represents a general flow. The actual configuration varies depending on your organizational infrastructure considerations and policies.



Processing steps

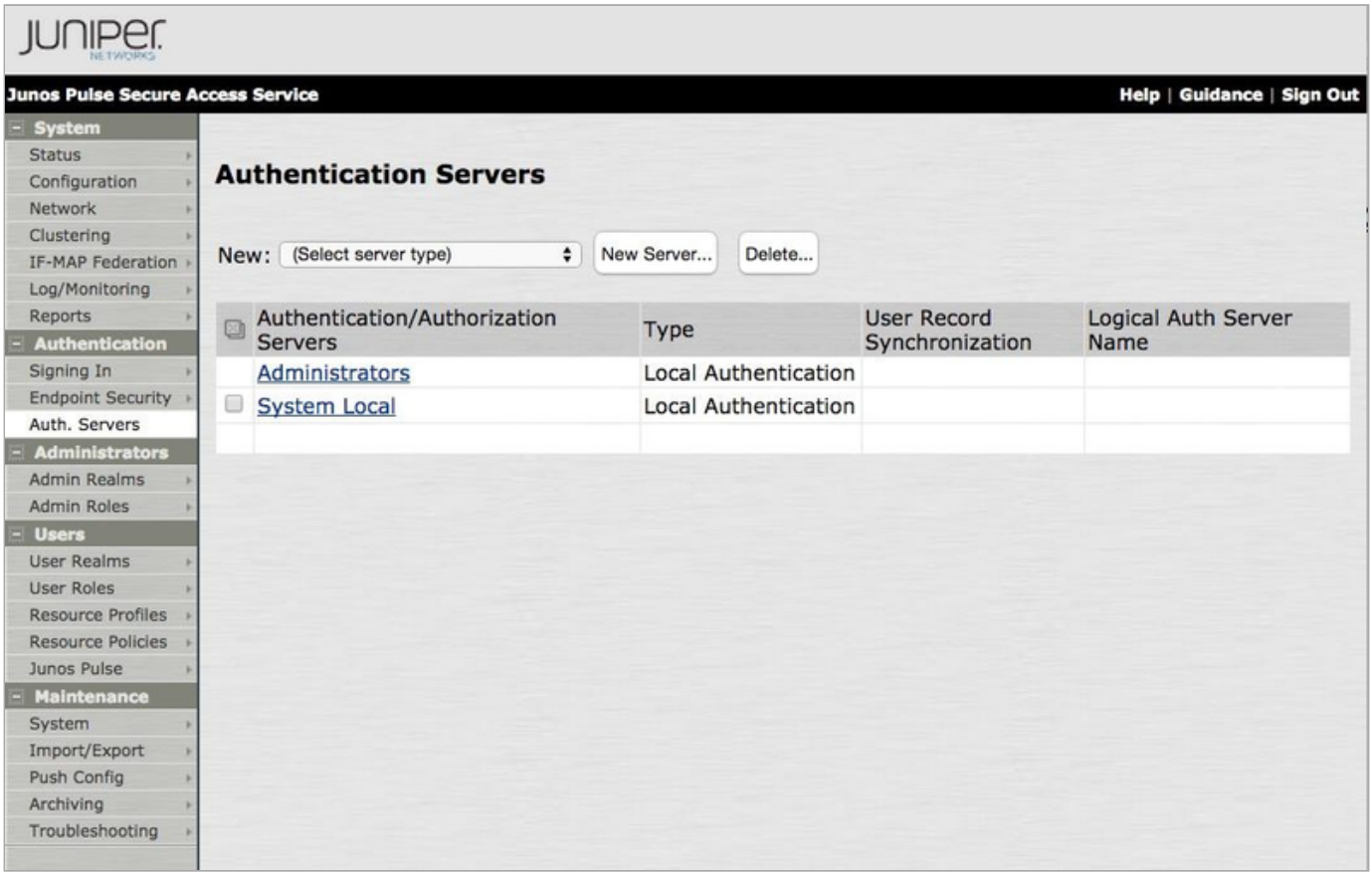
1. When a user opens their Juniper IPSec or SSL VPN sign-in window and enters a username and password, their details are sent to the RADIUS Server on PingFederate through the VPN RADIUS client.
2. PingFederate authenticates the user's credentials with the LDAP Server as first-factor authentication.
3. Upon LDAP authentication approval, the RADIUS server initiates second-factor authentication with PingID.
4. The RADIUS server returns a response to the Juniper VPN. If authentication is denied or an error occurs, the user's VPN window displays an error message.

Adding a RADIUS Server

To configure Juniper for PingID multi-factor authentication (MFA), you must add a RADIUS server.

Steps

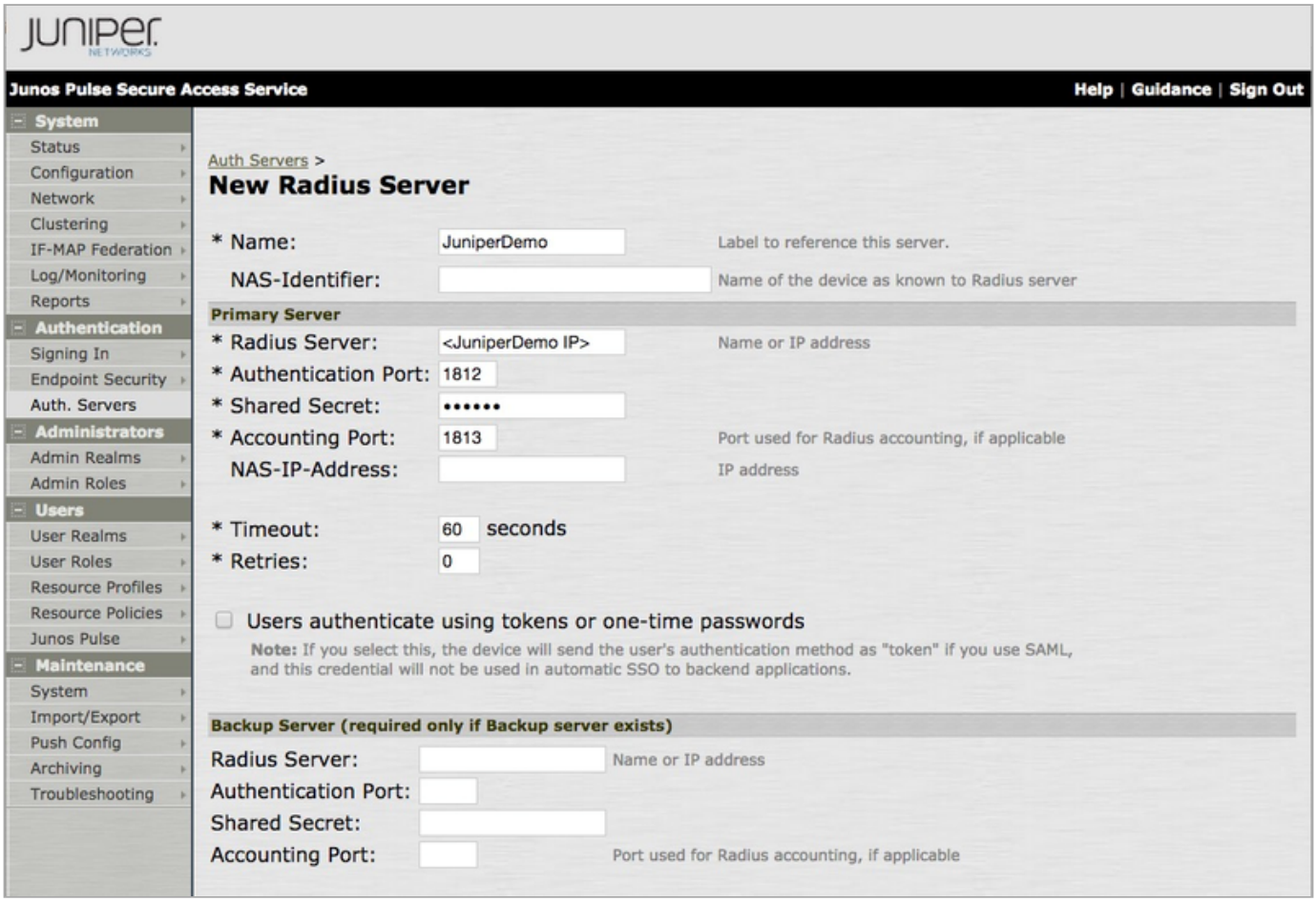
1. Sign on to Juniper with your administrator ID and password.
2. In the left-hand navigation pane, go to **Authentication → Auth. Servers**.



3. From the **New** list, select **RADIUS Server**, and then click **New Server**.

   Result:

   The**New Radius Server** window opens.



4. In the **New Radius Server** window, enter the following information:
    1. In the **Name** field, enter the RADIUS Server name.
    2. In the **NAS-Identifier** field, enter the name of the device as known to the RADIUS server.
    3. In the **Radius Server** field, enter the DNS name or IP address of the RADIUS server password credential validator (PCV).
    4. In the **Authentication Port** field, enter the port configured in the RADIUS server PCV. The default value is `1812`.
    5. In the **Shared Secret** field, enter the shared secret configured in the RADIUS server PCV.
    6. In the **Accounting Port** field, enter the port used for RADIUS accounting.

        > **Note**
        >
        > The default value is `1813` and should not be changed.

    7. In the **Timeout** field, enter `60`.

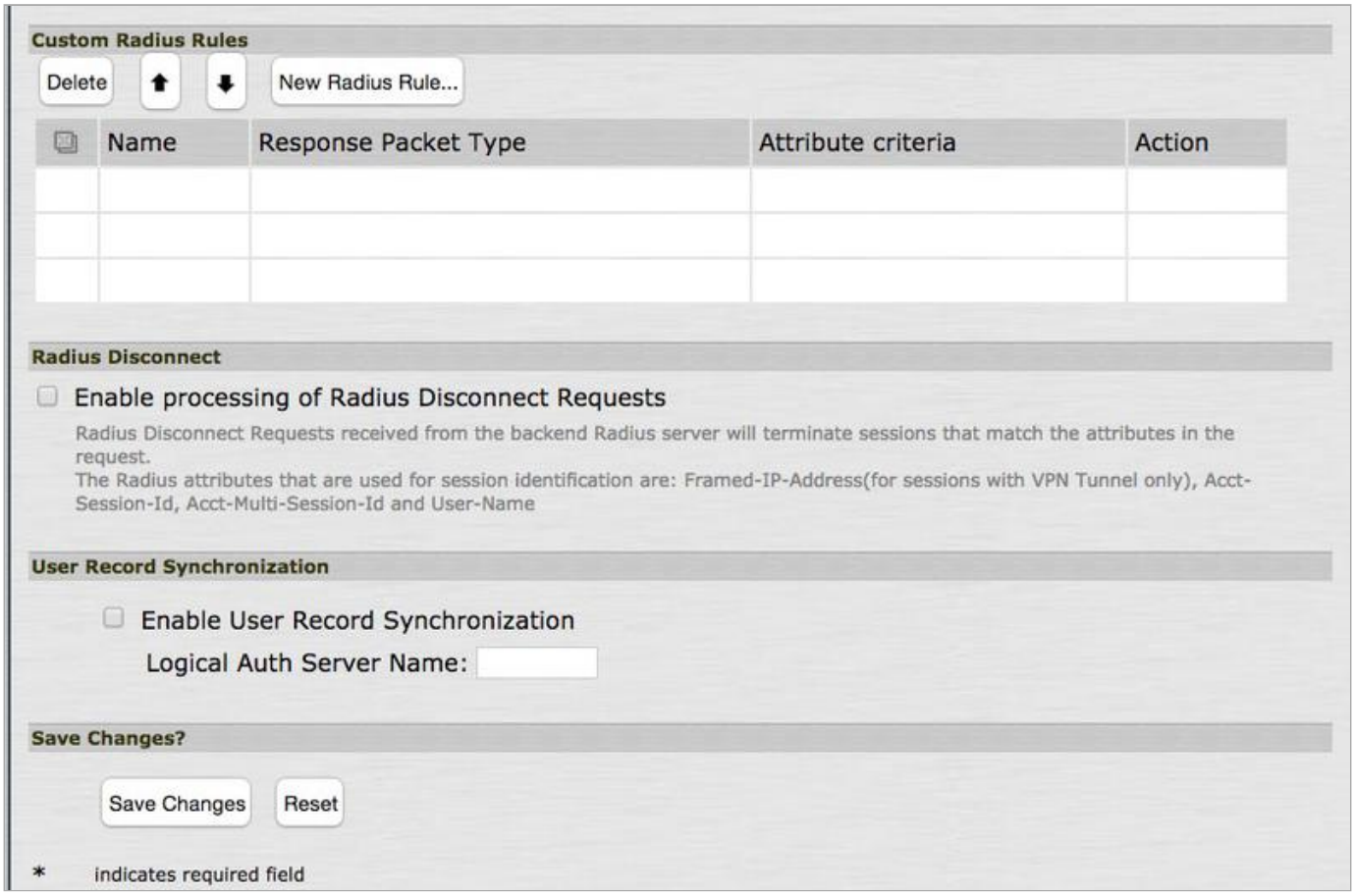
        The default value is `30`.

        > **Note**
        >
        > The **Timeout** field determines the amount of time in seconds before the connection is timed out.

5. Click **Save Changes**.

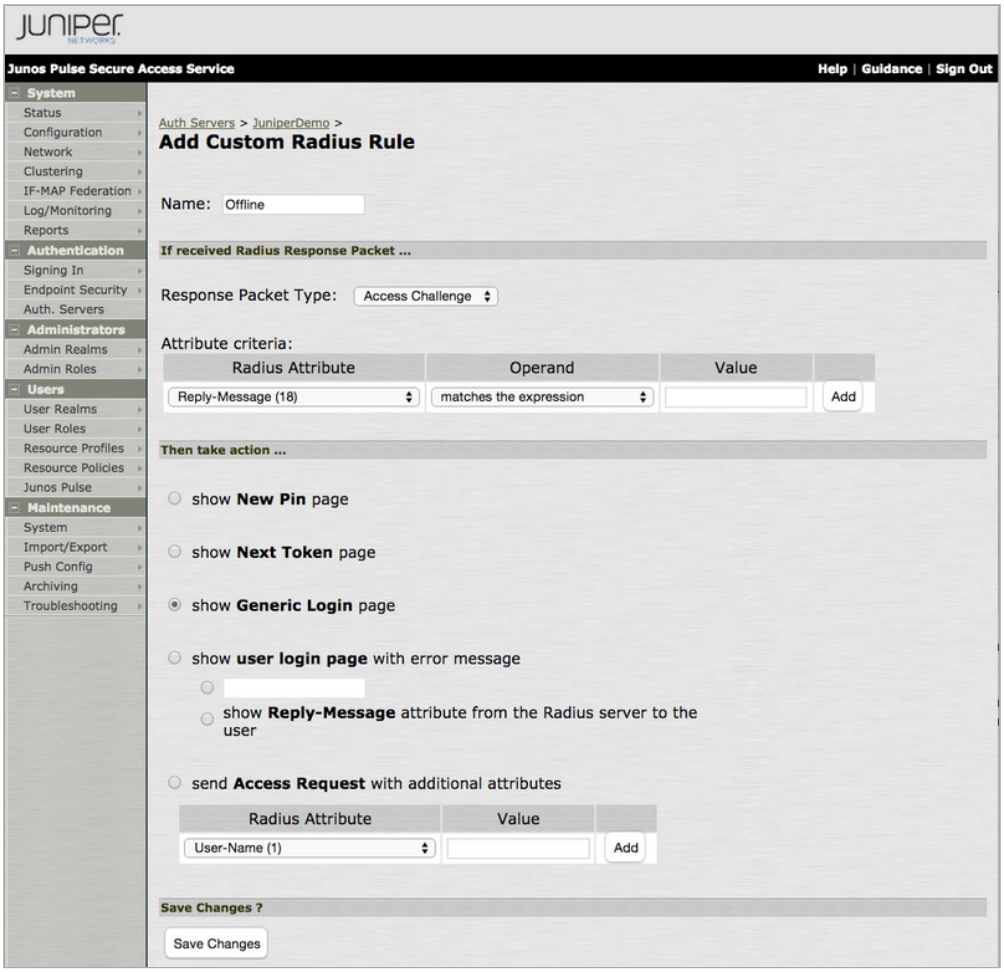
   Result:

   The Custom Radius Rules section is enabled.



6. Click **New Radius Rule**.

   The following window is didplayed:



7. In the **Add Custom Radius Rule** window, enter the following information:
    1. In the **Name** field, enter `Offline`.
    2. From the **Response Packet Type** list, select **Access Challenge**.

    This is the default value.
    1. Select the **Show Generic Login Page** check box.
8. Click **Save Changes**.

Adding a New Authentication Realm

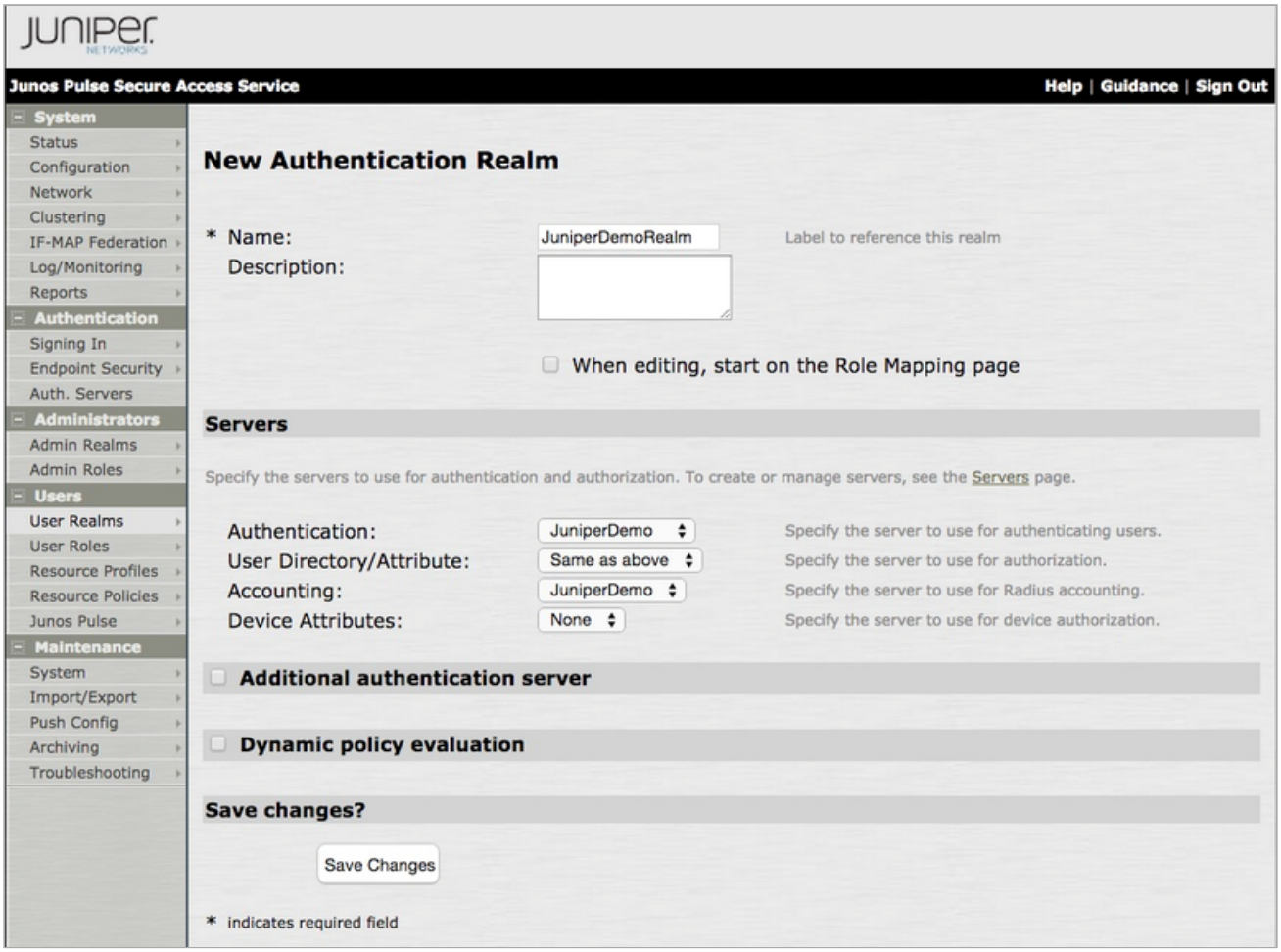
To configure Juniper for PingID multi-factor authentication (MFA), you must add a new authentication realm.

Steps

1. In the left-hand navigation pane, go to **Users → User Realms → New**.

    Result:

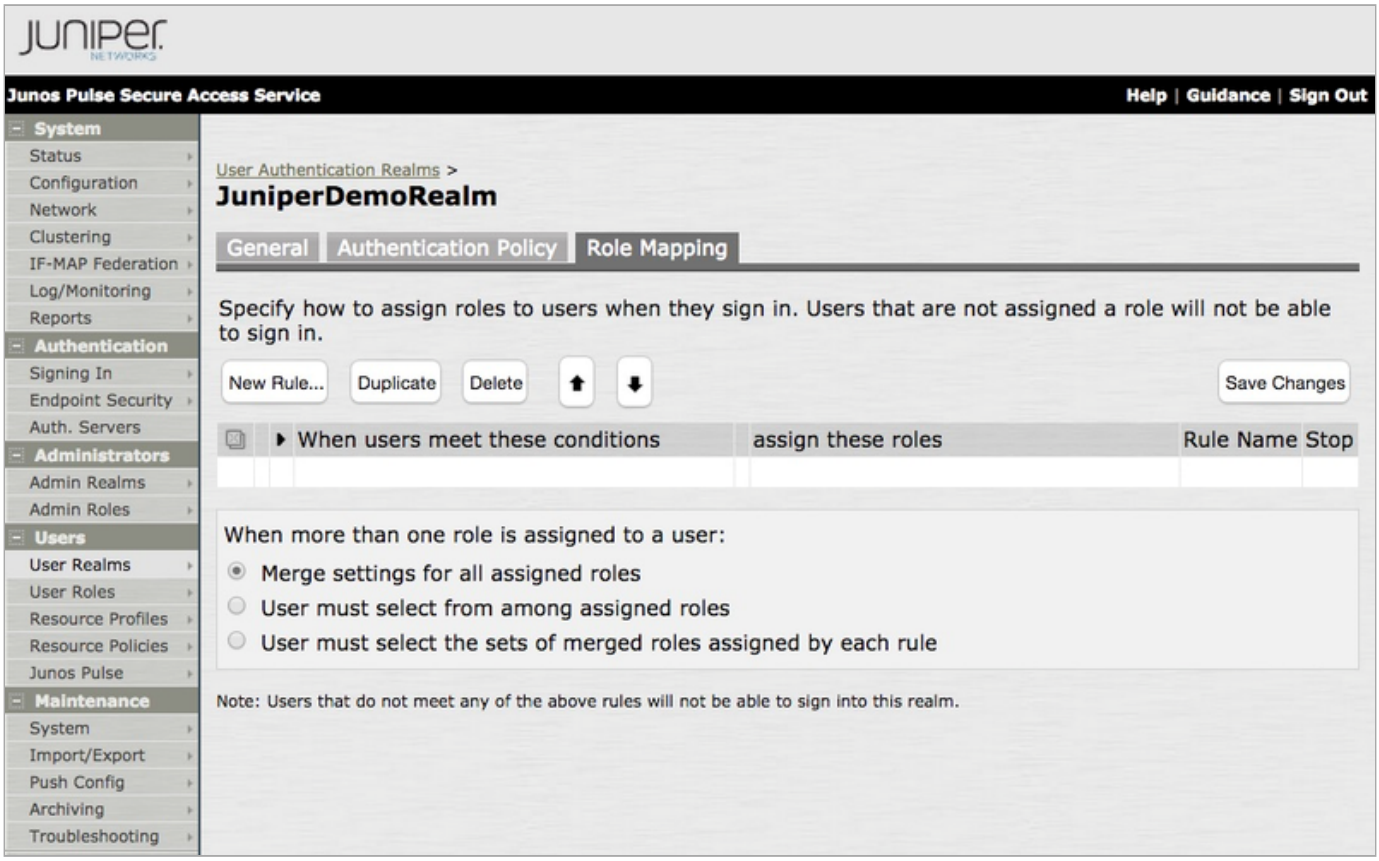
    The **New Authentication Realm** window opens.



2. In the **Name** field, enter a name for the Authentication Realm.
3. In the **Servers** section, enter the following information:
    1. From the **Authentication** list, select the name of the RADIUS server created in Adding a RADIUS Server.
    2. From the **User Directory/Attribute** list, select **Same as Above**.
    3. From the **Accounting** list, select the name of the RADIUS server created in Adding a RADIUS Server.
    4. From the **Device Attributes** list, select the default value of **None**.
4. Click **Save Changes**.

    Result:

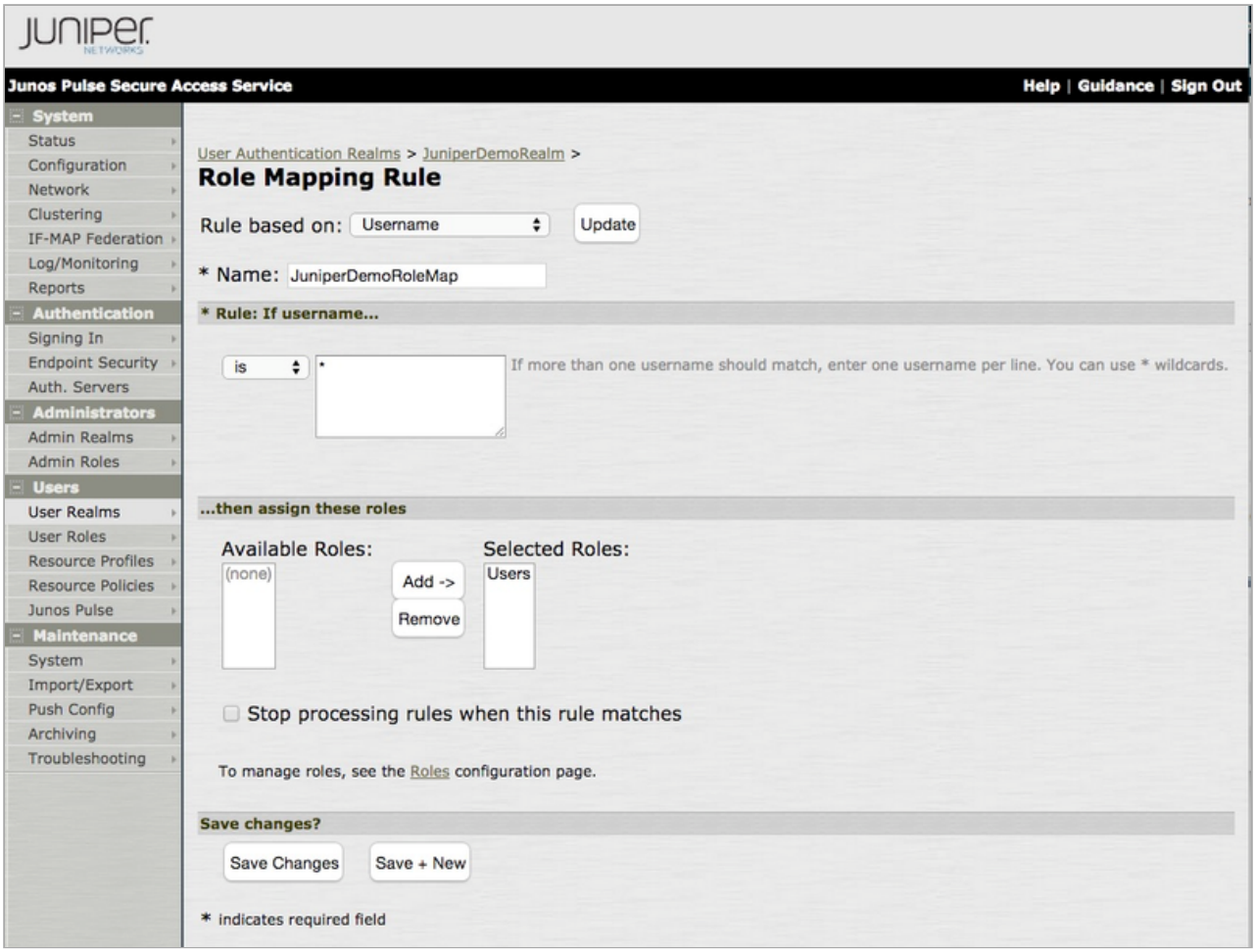
    The Authentication Realm is saved and three additional tabs appear.



5. On the **Role Mapping** tab, click **New Rule**.

   Result:

   The **Role Mapping Rule** window opens.



6. In the **Role Mapping Rule** window, enter the following information:

    1. From the **Rule Based On** list, select **Username**.

    This is the default value.

    1. In the **Name** field, enter a name for the rule.
    2. In the *** Rule: If Username...** section, select **is** from the list, and then enter `*` in the text box.
    3. In the **...Then Assign These Roles** section, select **Users** in the **Available Roles** list, and then click **Add**.

        Result:

        The **Users** role is added to the **Selected Roles** list.

7. Click **Save Changes**.

    Result:

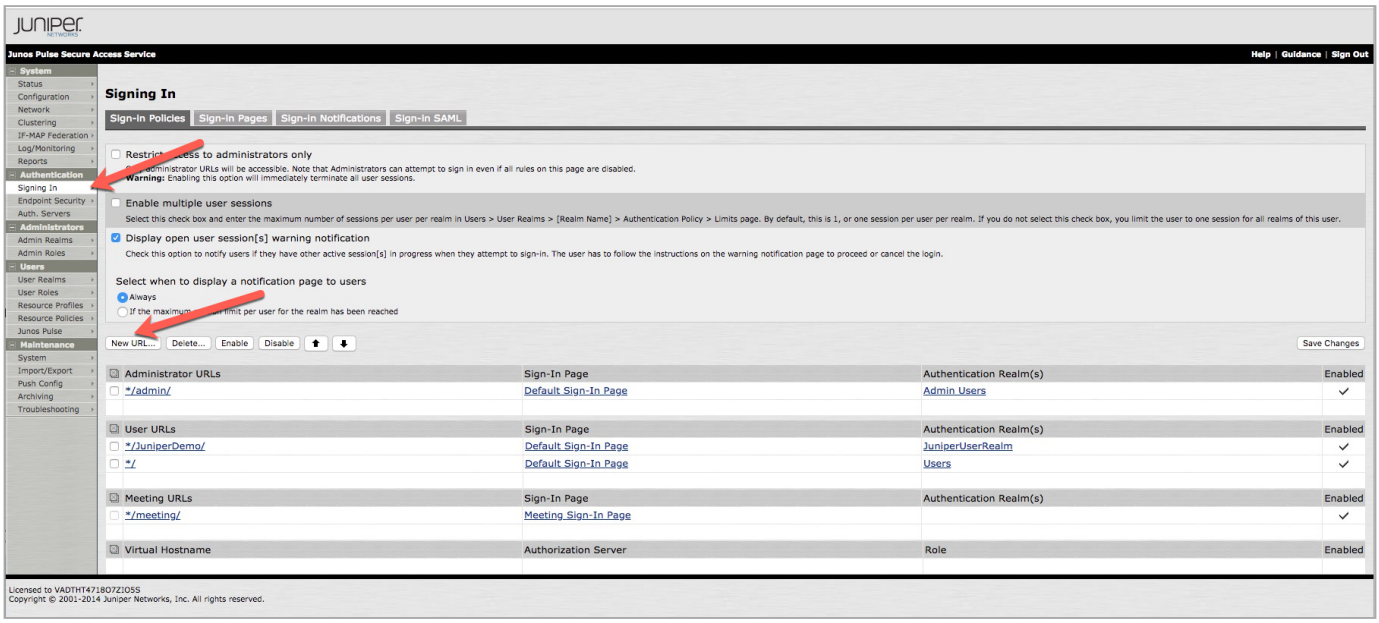
    The Authentication Realm is saved.

Configuring a Signing In Policy

To configure Juniper for PingID multi-factor authentication (MFA), you must configure a sign in policy.

Steps

1. In the left navigation pane, in the **Authentication** section, click **Signing In**.



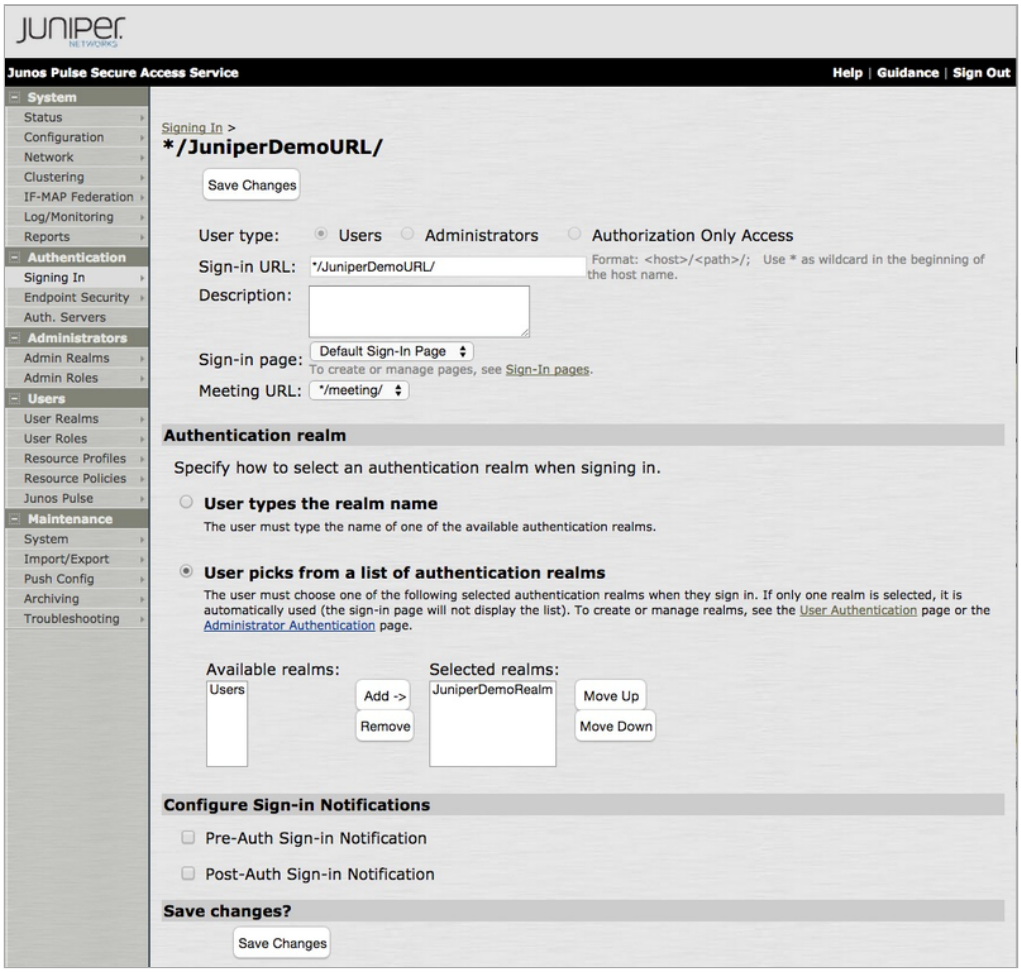
Result:

The **Signing In** window opens.

2. In the **Signing In** window, click **New URL...**.

Result:

The next section of the **Signing In** window opens.



3. In the **User Type** section, click **Users**.
4. In the **Sign-in URL** field, enter the sign-in URL in the format of `<host>/<path>/`.

   Example:`*/JuniperDemoURL/`

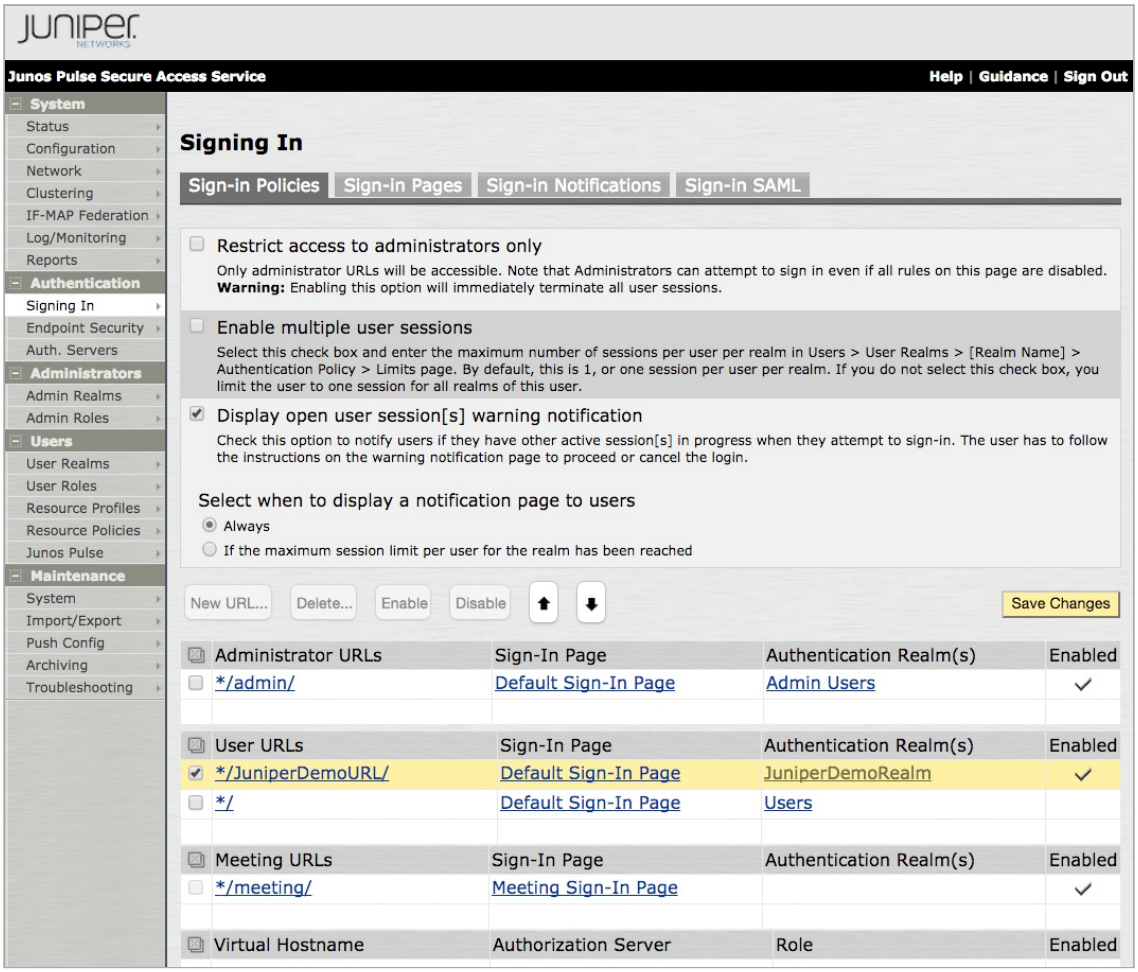
5. In the **Authentication Realm** section, enter the following information:

   1. Click **User Picks from a List of Authentication Realms**.
   2. From the **Available Realms** list, select the realm created in Adding a New Authentication Realm, and then click **Add**. The realm is added to the **Selected Realms** list.

      Result:

      The **Signing In** window is displayed, and the **User URL** list contains the new URL.

6. Click **Save Changes**.
7. From **User URLs** list, select the check box next to the URL you just created.
8. To move the URL to the top of the list, click the **Up Arrow**icon ( ).



9. Click **Save Changes**.

   Result:

   The Juniper VPN is now configured to use the PingFederate RADIUS password credential validator (PCV) server.

Signing on

Sign on to your user URL page.

Steps

1. In a web browser, enter the user URL you previously created in Configuring a Signing In Policy.
2. Authenticate with your username and password.
3. Perform your second-factor authentication using PingID.

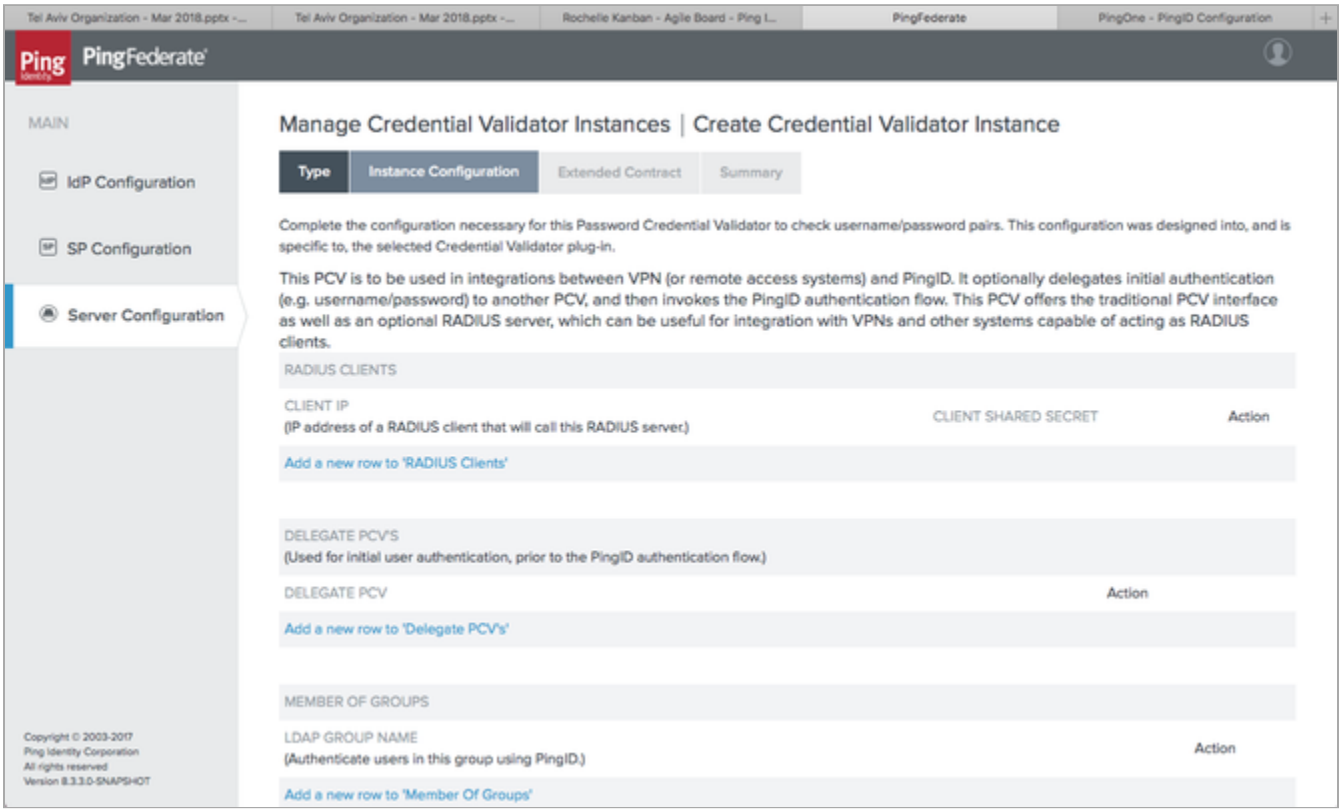
Configuring Juniper as first factor authentication

Configure Juniper 8.0 as the first-factor ID provider using LDAP and PingFederate with PingID RADIUS password credential validator (PCV) as the second factor.

Steps

1. Configure PingFederate with a PingID RADIUS PCV, and leave the **Delegate PCV** section empty.

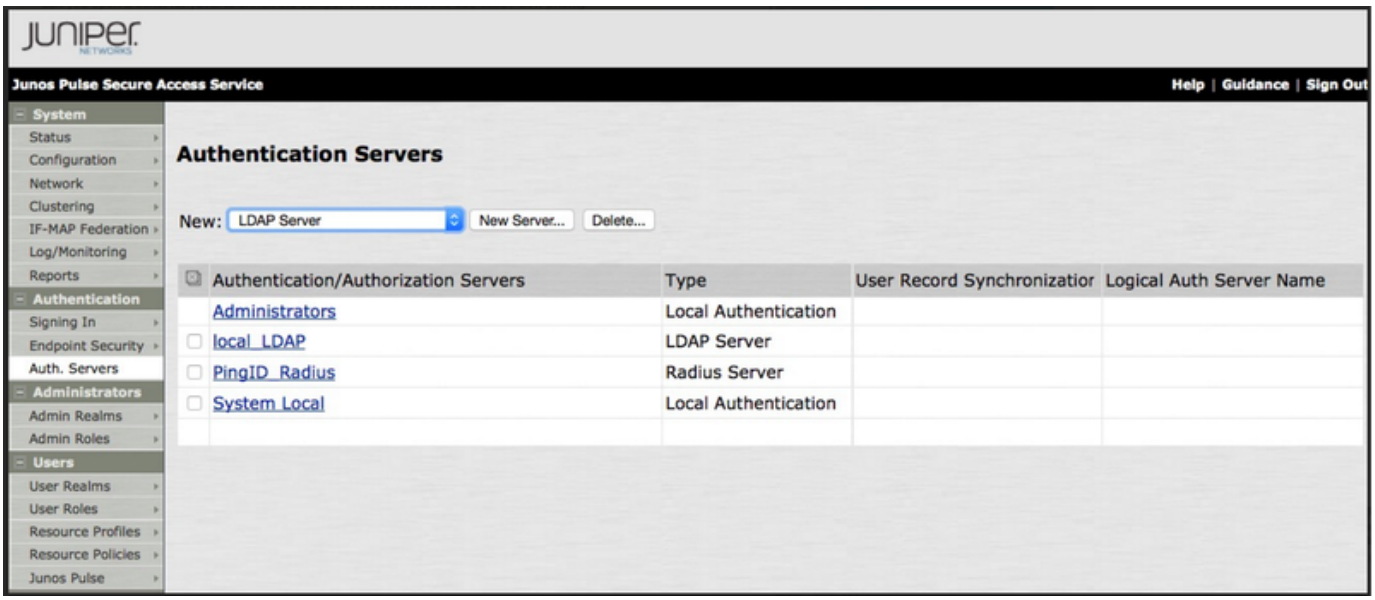
   For more information, see Integration for devices using a RADIUS server.



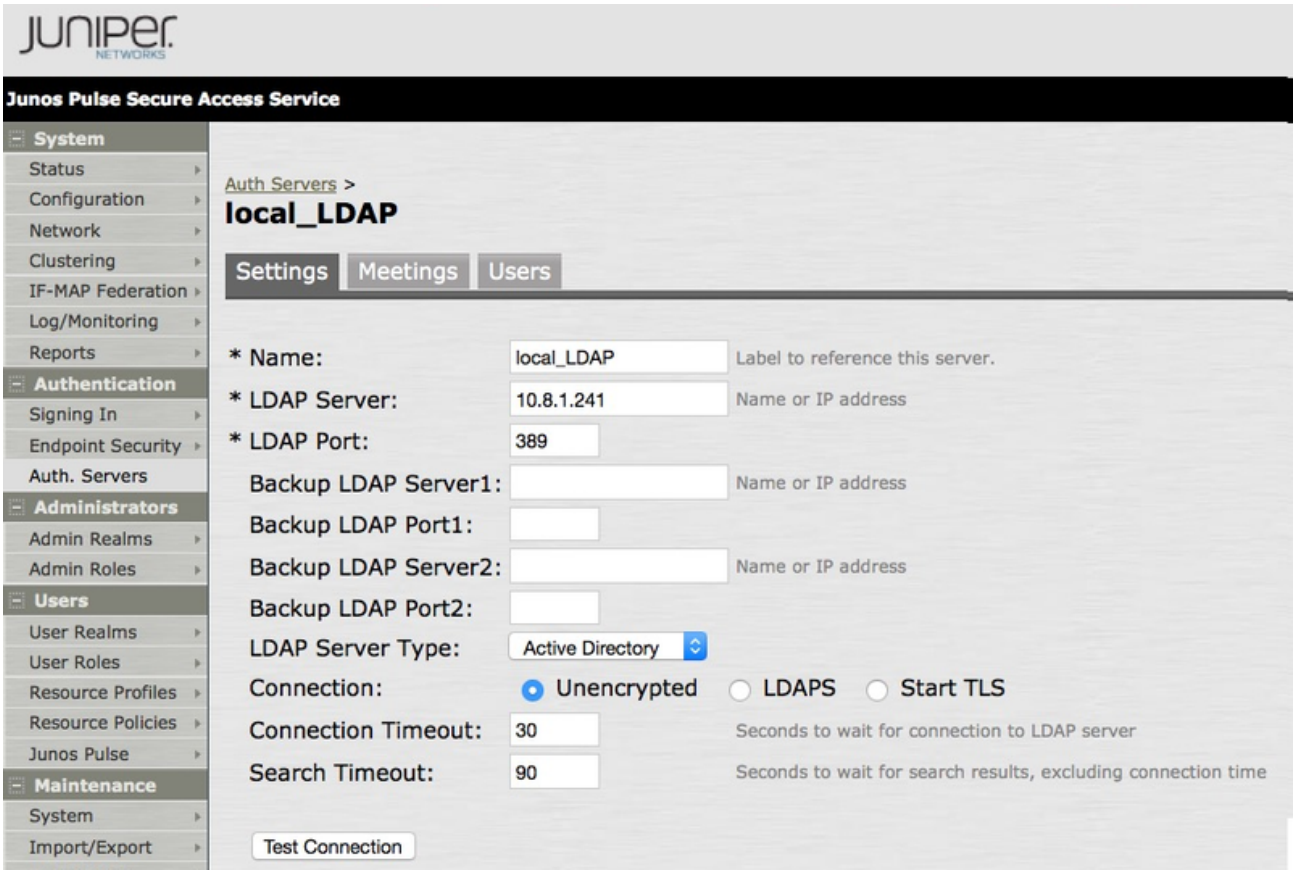
2. In the Juniper admin portal, create and configure the PingID RADIUS configuration.

   For more information, see Configuring Juniper for PingID multi-factor authentication.

3. Go to **Authentication → Authentication Servers**.



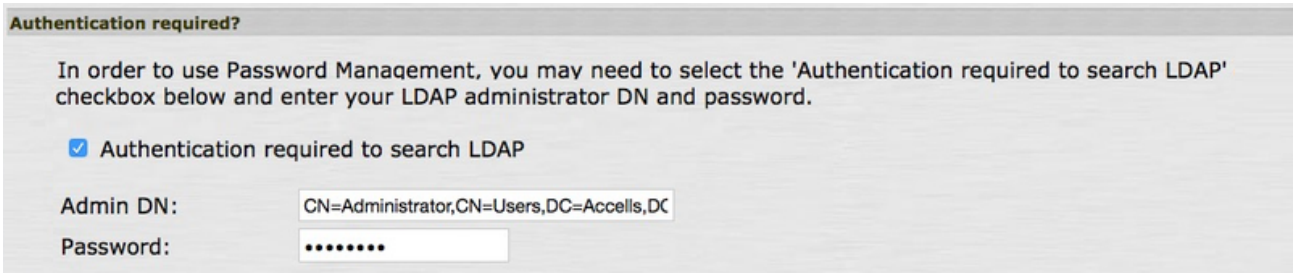
4. From the **New** drop-down list, select **LDAP Server**, and then click **New Server**.
5. In the **Settings** tab, complete the following fields:
    1. In the **Name** field, enter a name for the server.
    2. In the **LDAP Server** field, enter the IP address or hostname of the LDAP server.
    3. In the **LDAP Port** field, keep the default value of `389`, or change it according to the LDAP configuration.
    4. From the **LDAP Server Type** list, select **Active Directory**.
    5. From the **Connection** options, keep the default value of `Unencrypted`, or change it to match the LDAP configuration.
    6. In the **Connection Timeout** field, enter `30`.
    7. In the **Search Timeout** field, enter `90`.
    8. Leave all other fields empty.



6. To confirm that the connection is valid before continuing, click **Test Connection**.
7. In the **Authentication Required?** section, complete the following fields:
    1. Select the **Authentication Required to Search LDAP** check box.
    2. In the **Admin DN** field, enter the admin DN.

For example, `CN=Administrator, CN=Users, DC=Accells, DC=Lab`.

3. In the **Password** field, enter the admin password.

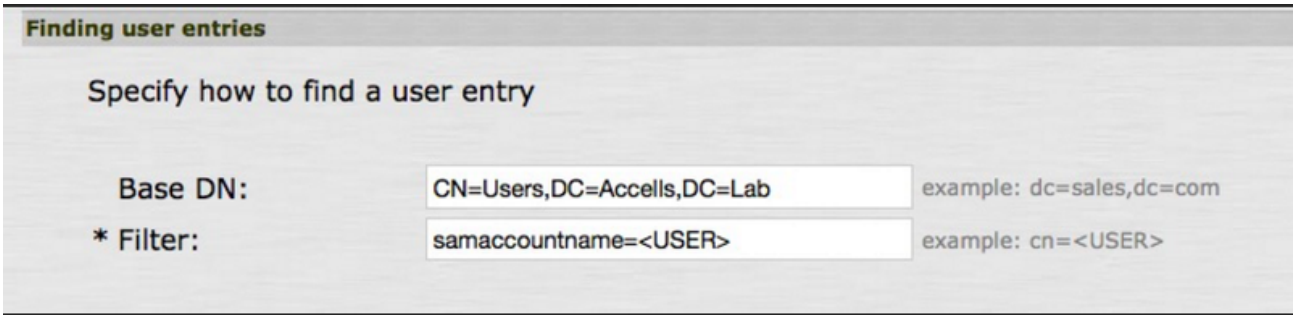


8. In the **Finding User Entries** section, complete the following fields:

1. In the **Base DN** field, enter the Base DN.

   For example, `CN=Users, DC=Accells, DC=Lab`.

2. In the **Filter** field, enter `samaccountname=<USER>`.



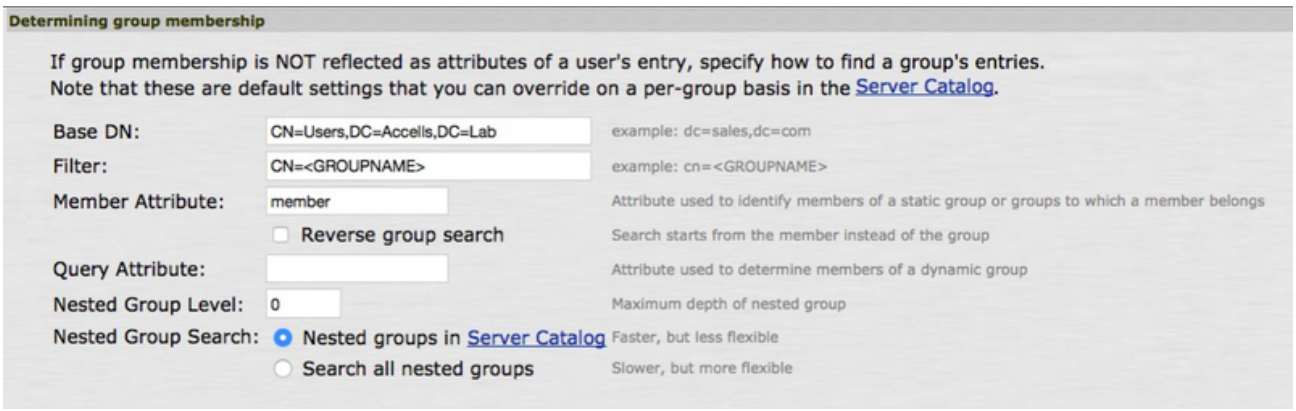
9. In the **Determining Group Membership** section, complete the following fields:

1. In the **Base DN** field, enter the Base DN.

For example, `CN=Users, DC=Accells, DC=Lab`.

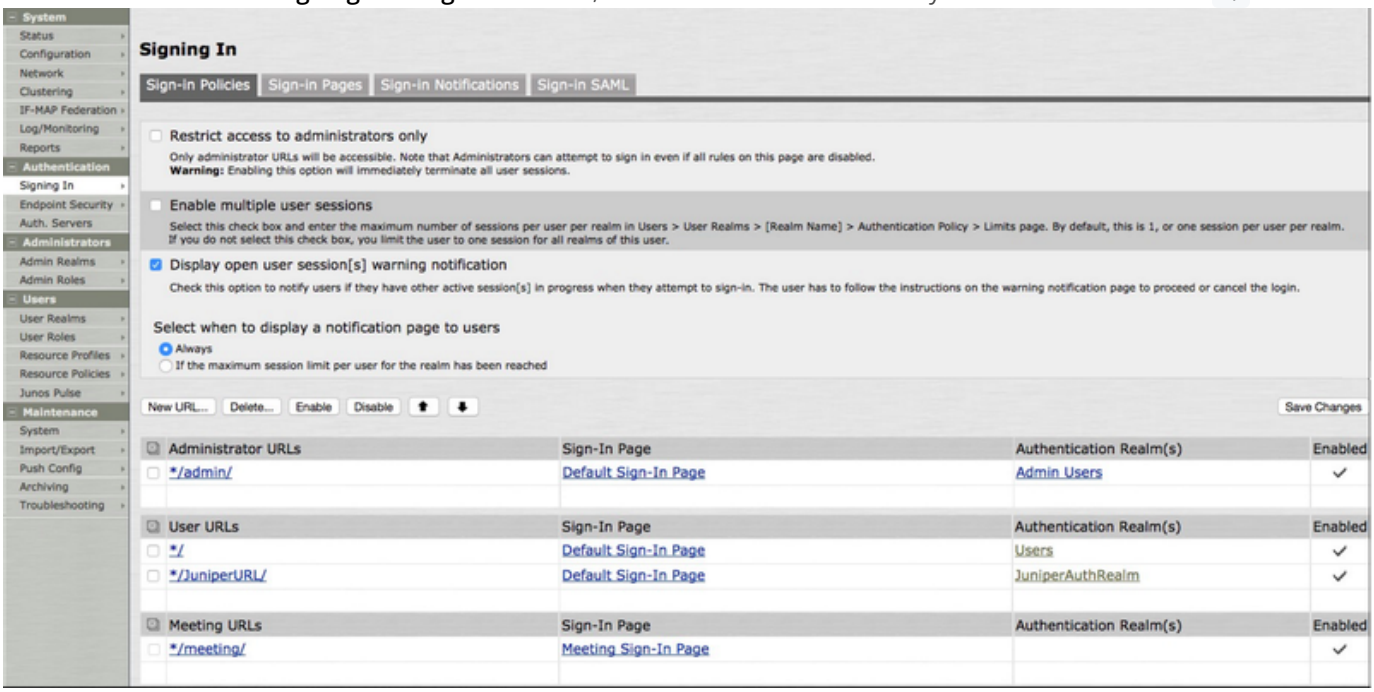
1. In the **Filter** field, enter `CN=<GROUPNAME>`

2. In the **Member Attribute** field, enter `member`.



10. Click **Save Changes**.

11. Go to **Authentication → Signing In → Sign-in Policies**, and ensure that the first entry on the **User URLs** list is `*/`.



> **Important**
>
> This differs from the instructions in the RADIUS PCV documentation.

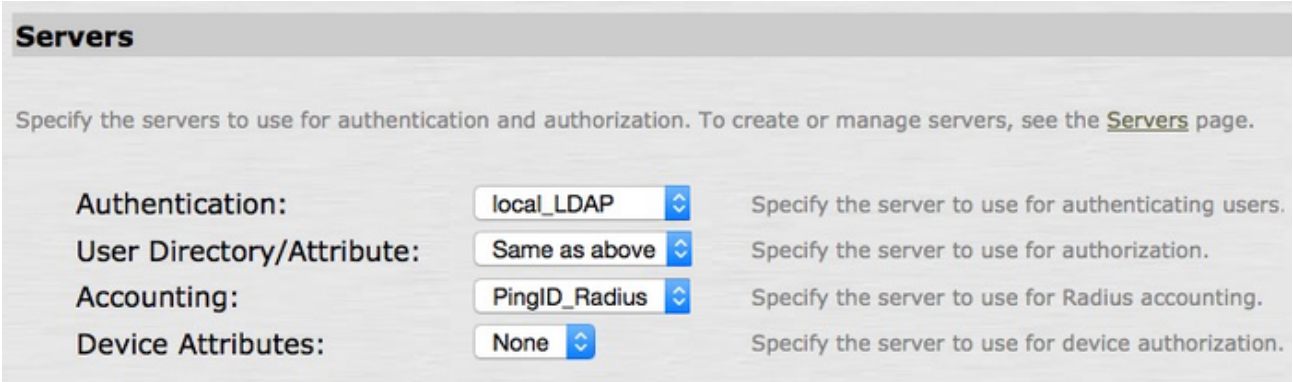
12. Go to **Users → User Realms → Users** and in the **Servers** section, complete the following fields:

    1. From the **Authentication** list, choose the LDAP authentication server created earlier.

    For example, **local_LDAP**.

    1. From the **User Directory/Attribute** list, select **Same as Above**.
    2. From the **Accounting** list, select the Juniper RADIUS authentication server created earlier.

       For example, **PingID_Radius**.

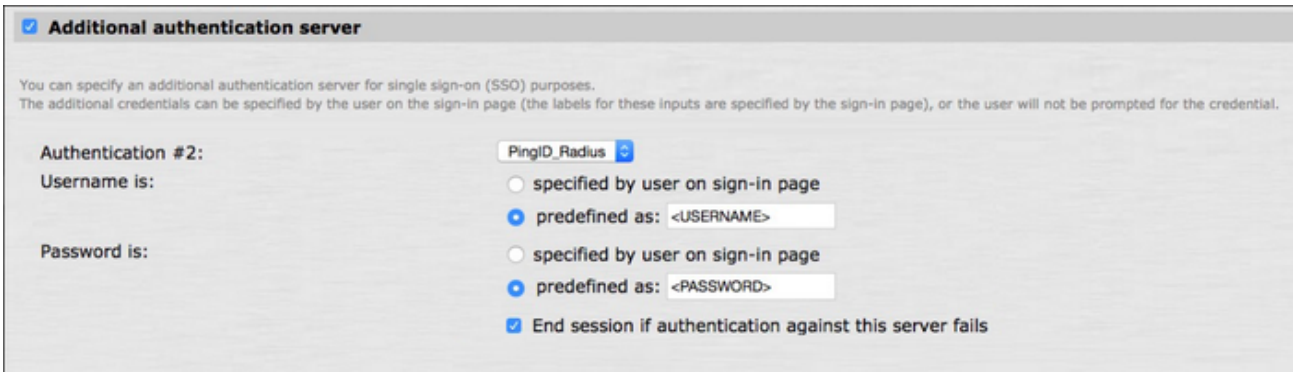


13. Select the **Additional Authentication Server** check box, and then complete the following fields:

    1. From the **Authentication #2** list, select the Juniper RADIUS authentication server created earlier.

For example, **PingID_RADIUS**.

1. In the **Username is:** section, click **Predefined as** and enter `<USERNAME>`.
2. In the **Password is:** section, click **Predefined as** and enter `<PASSWORD>`.
3. Select the **End Session if Authentication Against this Server Fails** check box.



14. Click **Save Changes**.
15. To sign on to Juniper while using the Juniper LDAP configuration as the first-factor for authentication, use the default user URL.

    Example:

    https://*<juniper IP>*, https://*<juniper hostname>*, or https://10.8.1.240/

Configuring Palo Alto Global Protect for PingID multi-factor authentication

In the following tasks, you will configure Palo Alto Global Protect to work with PingID multi-factor authentication (MFA).

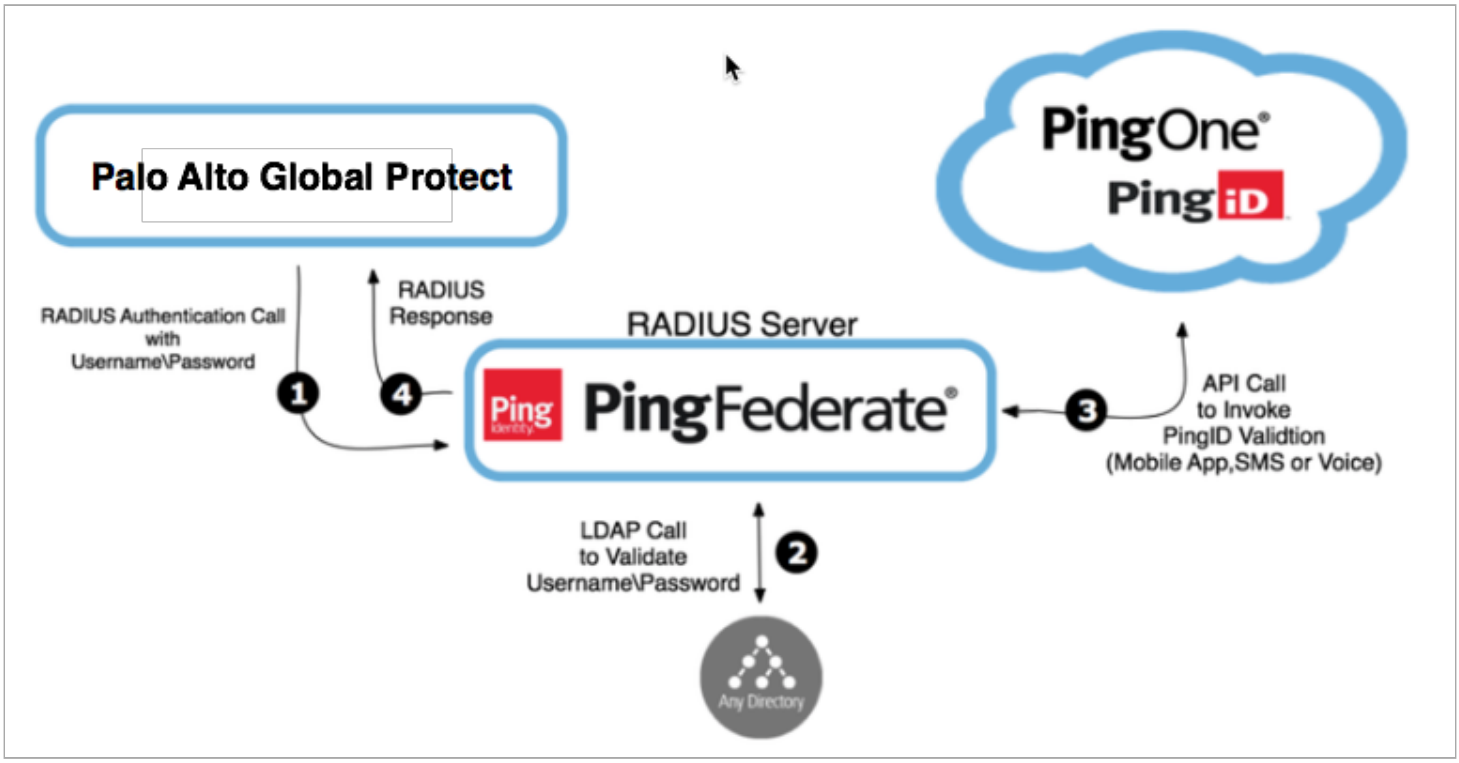
Prerequisites

To set up PingFederate or PingFederate Bridge as a RADIUS server, see Prerequisites: PingFederate RADIUS server.

> **Note**
>
> If your end users encounter the Javascript error "Assignment to read-only properties is not allowed in strict mode" when authenticating via PingID, they should upgrade to version 5.2.11 of the GlobalProtect app.

How it works

The following diagram illustrates a general flow. The actual configuration varies depending on your organizational infrastructure considerations and policies.



Processing Steps

1. When a user opens their Palo Alto Global Protect sign-on window and enters a username and password, their details are sent to the RADIUS server on PingFederate through the VPN RADIUS client.
2. PingFederate authenticates the user's credentials with the user repository, such as an LDAP server, as first-factor authentication.
3. Upon authentication approval from the user repository, the RADIUS server initiates a second authentication with PingID.
4. The RADIUS server returns a response to Palo Alto Global Protect. If authentication is denied or if an error occurs, the user's terminal displays an error message.

Setting up a RADIUS profile in the New Generation Firewall

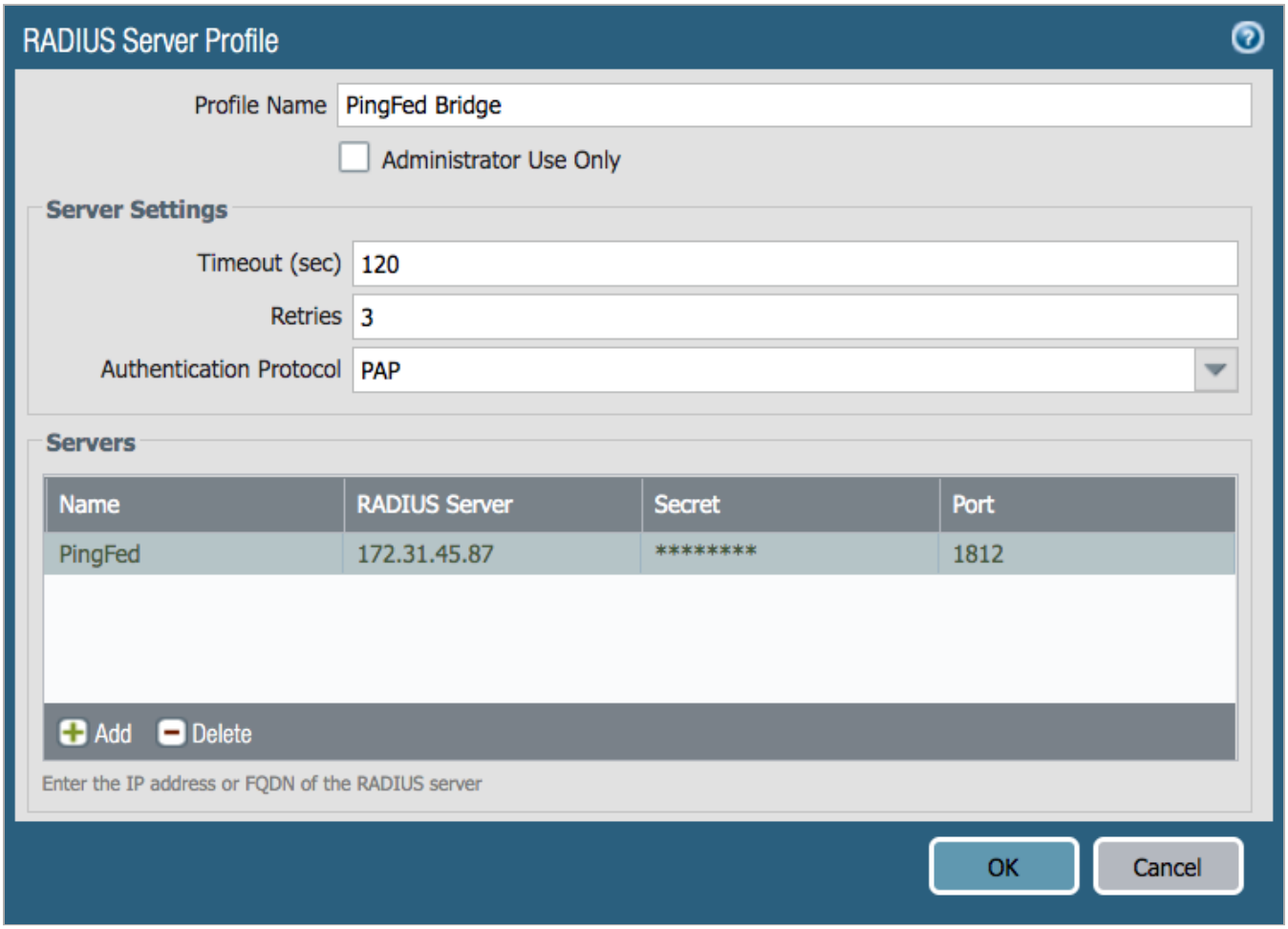
To configure Palo Alto Global Protect to work with PingID multi-factor authentication (MFA), you must set up a RADIUS profile.

Steps

1. Go to **Device → Server Profiles → RADIUS**, and click **Add**.

   Result:

   The following window is displayed.



2. In the **Profile Name** field, enter a name for the server.
3. In the **Server Settings** section, set the **Timeout** and **Retries**fields according to your policy.
4. From the **Authentication Protocol**list, select **PAP**.
5. In the **Servers** section, click **Add**, and then add the RADIUS server details.

Next steps

For further information about setting the RADIUS profile, see Configure RADIUS Authentication.

Creating an authentication profile

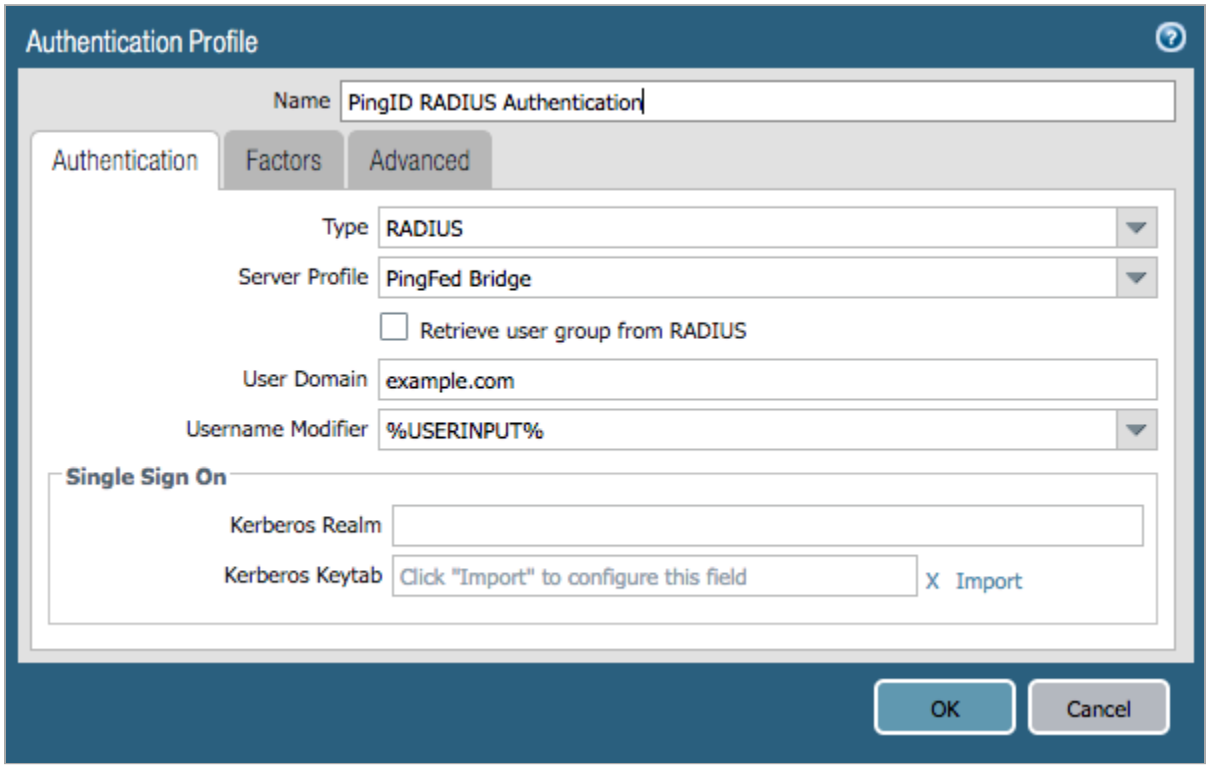
To configure Palo Alto Global Protect to work with PingID multi-factor authentication (MFA), you must create an authentication profile.

Steps

1. Go to **Device → Authentication Profile**, and then click **Add**.

   Result:

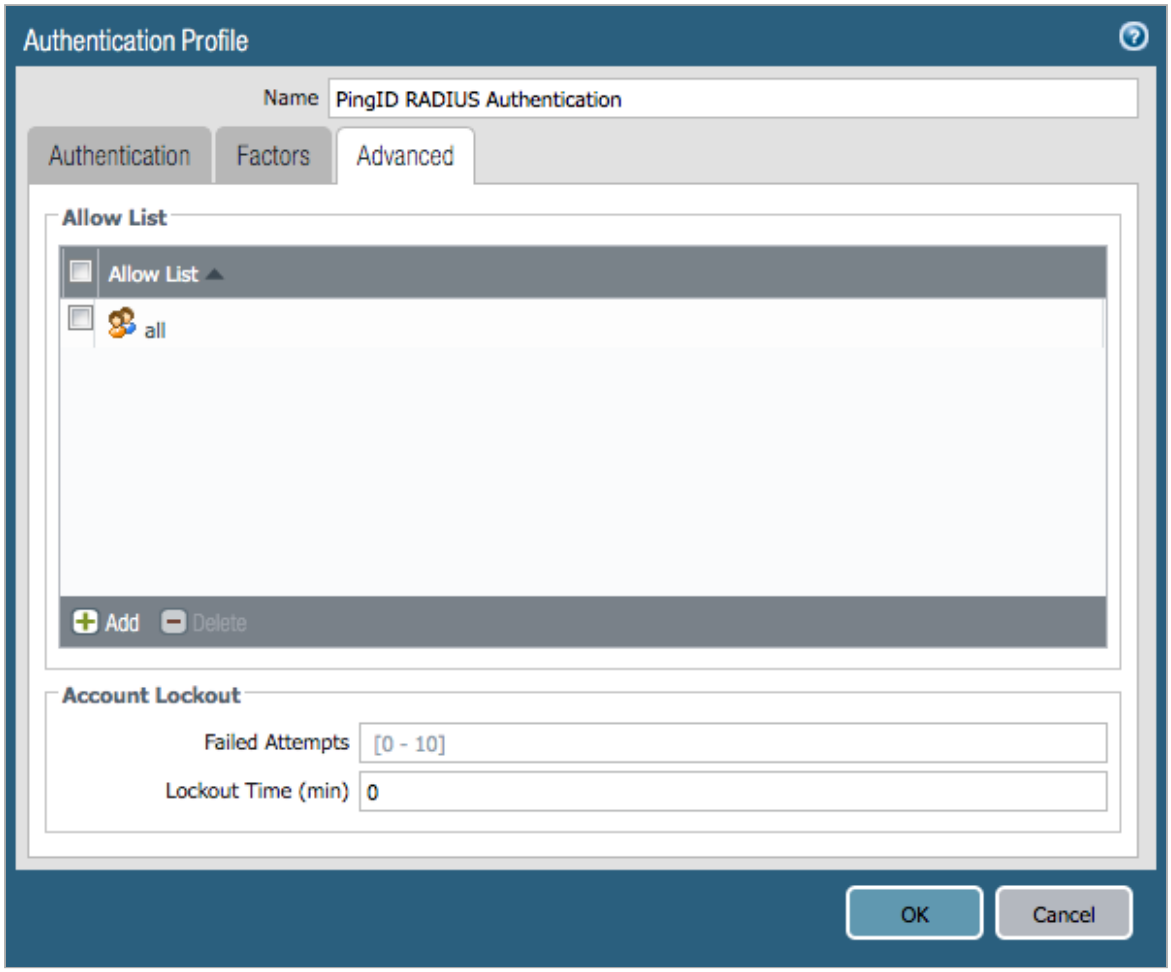
   The **Authentication** tab of the **Authentication Profile** window is displayed.



2. In the **Name** field, enter a name for the profile.
3. From the **Type** list, select **RADIUS**.
4. From the **Server Profile** list, select the RADIUS profile that you previously created.
5. In the **User Domain** field, enter your own domain name.
6. From the **Username Modifier** list, leave the default selection of **%USERINPUT%**.
7. Click **Advanced**.

   Result:

   The **Advanced** tab of the **Authentication Profile** window is displayed.



8. In the **Allow List** section, select the group to which this authentication profile will apply. Click **OK**.

Setting Global Protect Authentication with the new profile

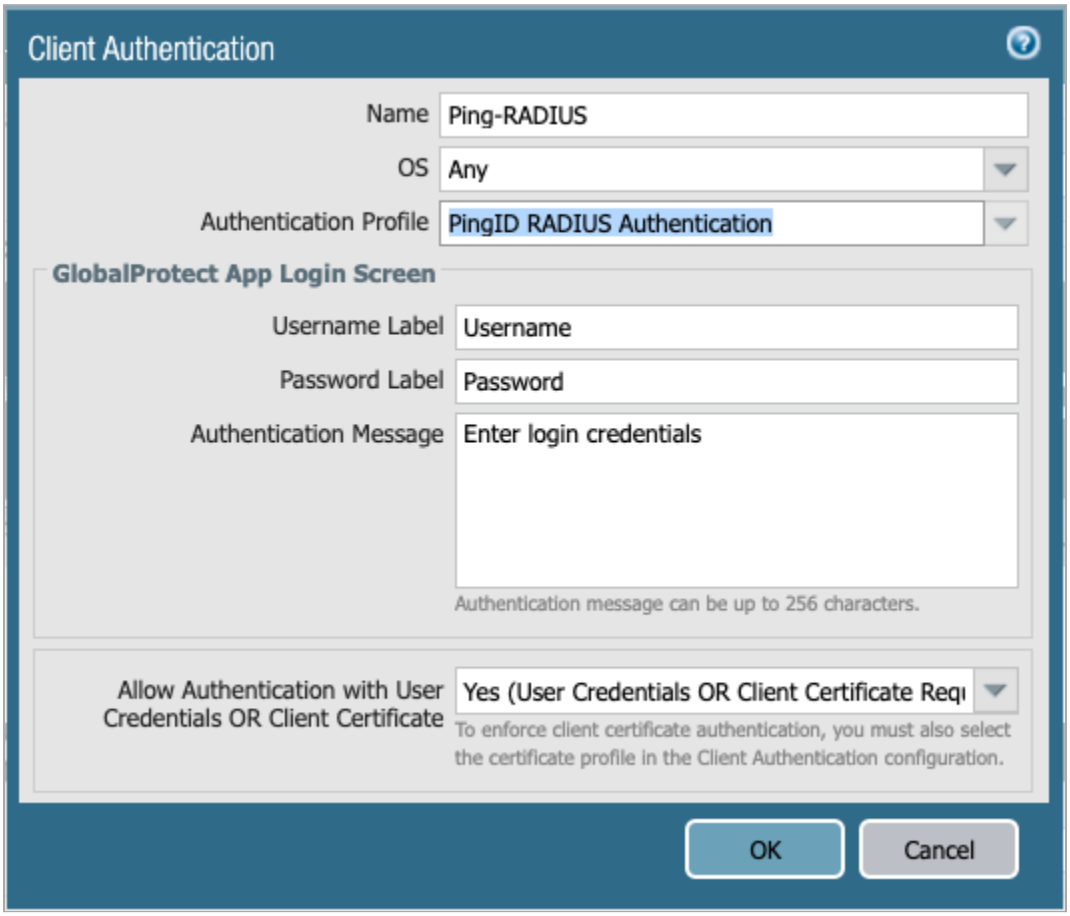
Add the authentication profile to the Global Protect Portal.

Before you begin

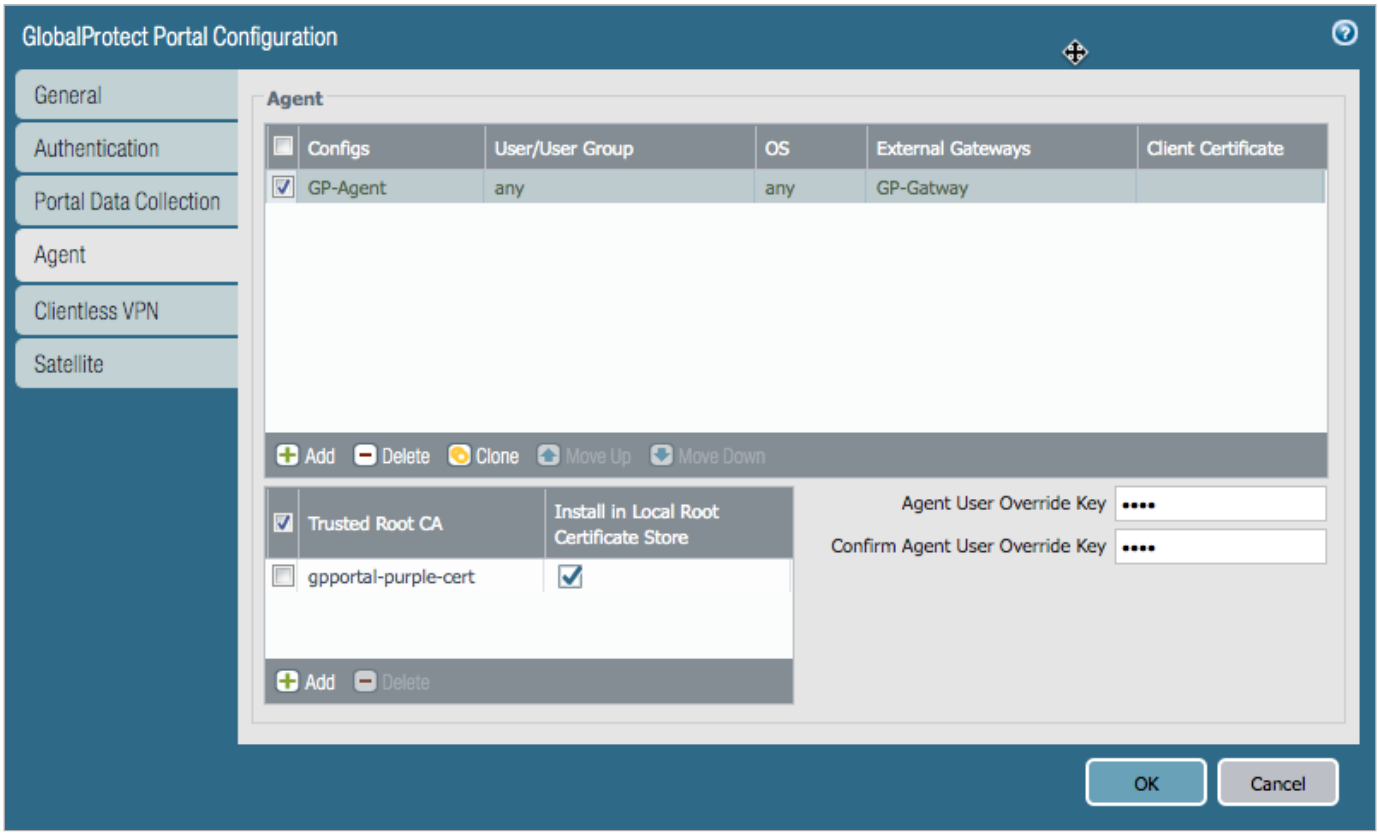
If you have not yet created a Global Protect Portal, see Set Up Access to the GlobalProtect Portal.

Steps

1. Go to **Network → Global Protect → Portals**, and open the portal you want to modify.
2. On the **Authentication** tab, choose the **SSL/TLS Service Profile** for the portal.
3. At the bottom left of **Client Authentication**, click **Add**.
4. In the **Client Authentication** window, enter a name in the **Name** field.
5. From the **Authentication Profile** list, select the authentication profile that you previously created.



6. **Optional:** From the **Allow Authentication with User Credentials or Client Certificate** list, select **Yes (User Credentials or Client Certificate Required)**.
7. Click **OK**.
8. Go to the **Agent** tab.
9. In the **Trusted Root CA** section, set the trusted root certificate authority (CA).



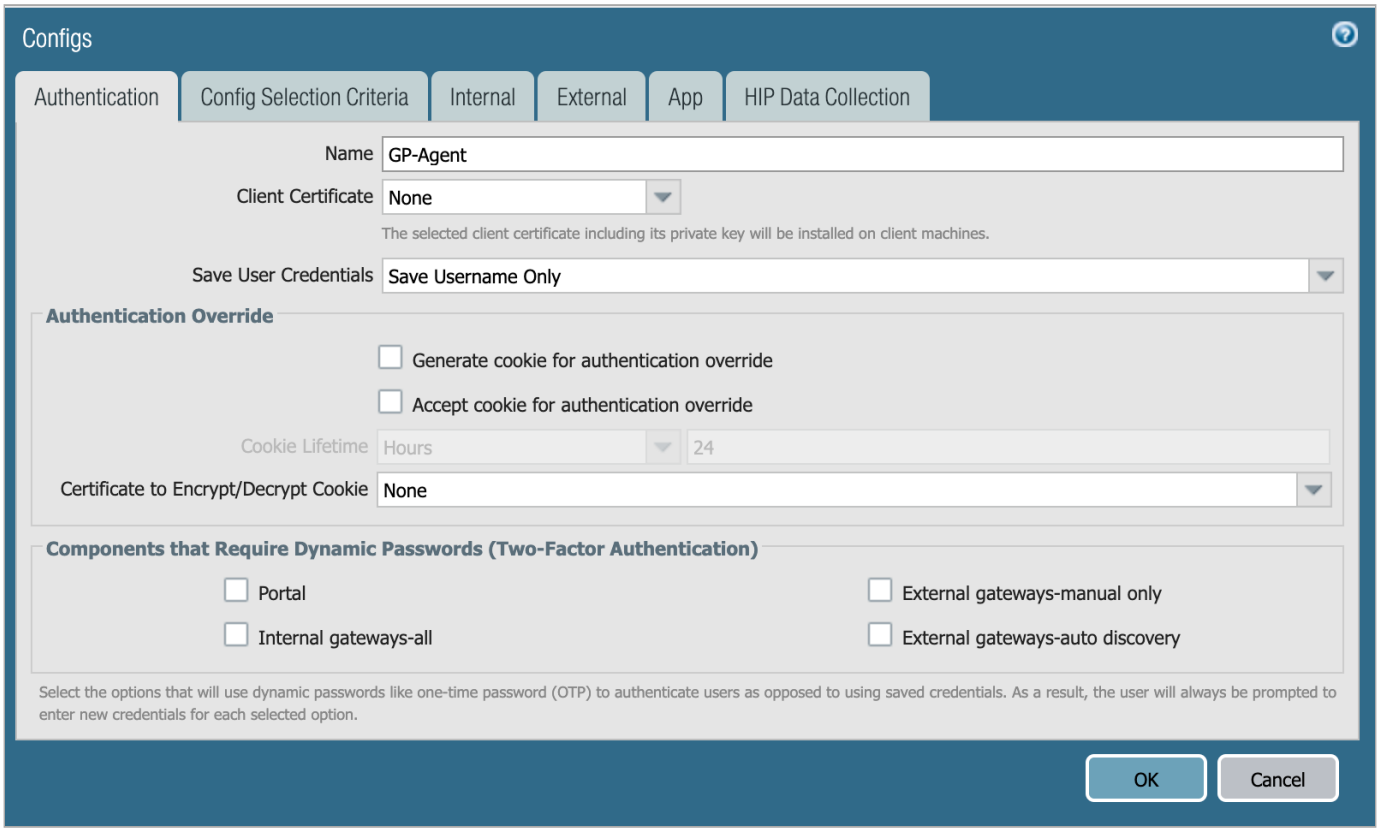
10. In the **Agent** section, click **Add**.

    Result:

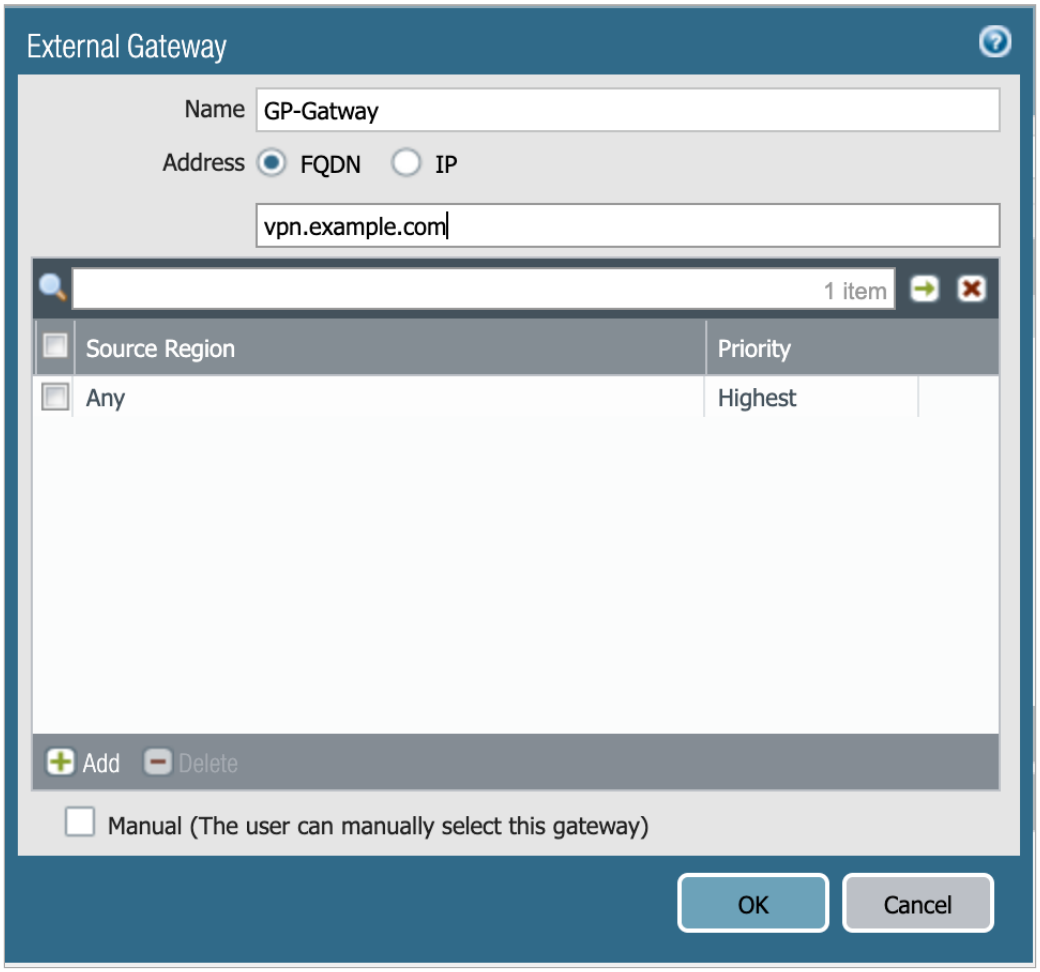
    The **Configs** window opens.

11. In the **Authentication** tab, in the **Name** field, enter a name.

12. From the **Save User Credentials** list, select **Save Username Only**.



13. Go to the **External** tab, and in the **External Gateways** section, click **Add**.
14. In the **Name** field, enter a name for the gateway.
15. In the **Address** field, enter the fully-qualified domain name (FQDN) or IP for the agent, and select the appropriate check box. Click **OK**.



16. Go to the **App** tab and review the **App Configurations**.
17. Make any necessary changes, and then click **OK**.

Next steps

Ensure that the Gateway is configured. For more information, see Configure a GlobalProtect Gateway.

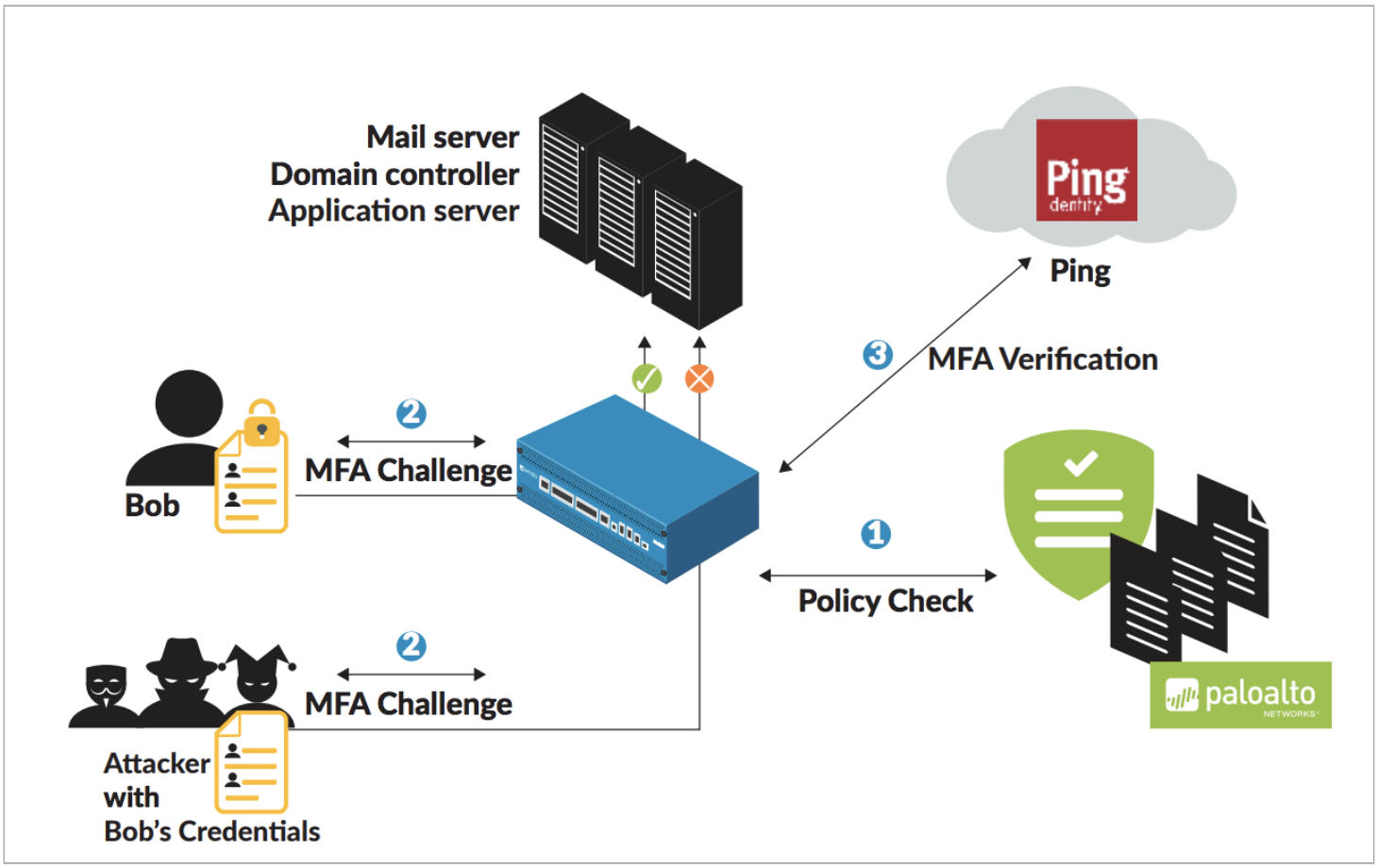
Configuring Palo Alto Authentication Portal for PingID

Palo Alto Networks Next-Generation Firewall (NGFW) Authentication Policy enables you to authenticate end users before they can access services and applications.

Overview

When a user requests a service or application, such as by visiting a web page, the firewall evaluates the authentication policy. Based on the matching authentication policy rule, the firewall then prompts the user to authenticate using one or more methods (factors). After the user authenticates for all factors, the firewall evaluates the Security Policy to determine whether to allow access to the service or application. To use multi-factor authentication (MFA) for protecting sensitive services and applications, you must configure an authentication policy to display a web form for the first authentication factor. For more information, see Multi-Factor Authentication.

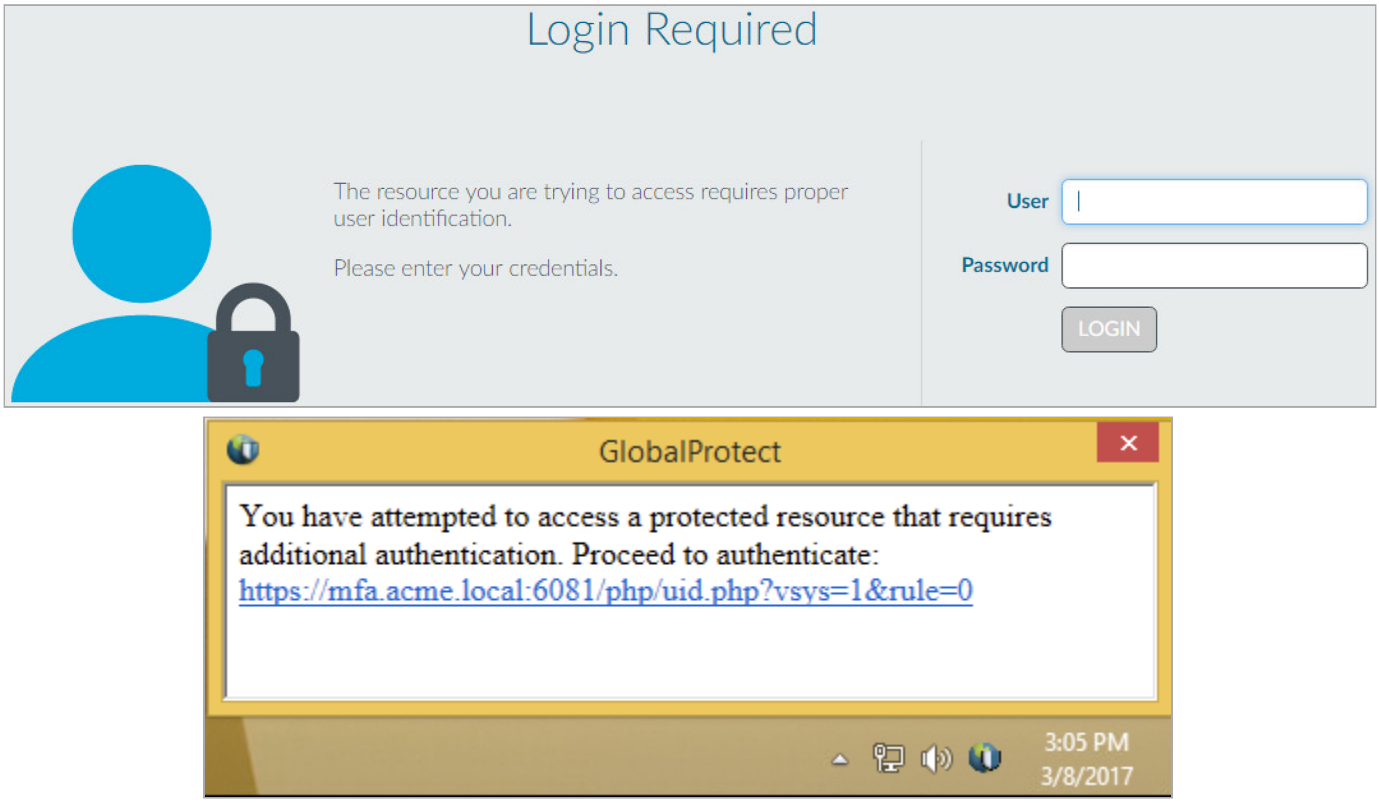
To facilitate MFA notifications for client-server applications (such as Perforce) on Windows or macOS endpoints, a VPN tunnel established through the GlobalProtect Client is required. When a session matches an authentication policy rule, the firewall sends a UDP notification to the GlobalProtect Client with an embedded URL link to the authentication portal page. The GlobalProtect Client then displays this message as a popup notification to the user.



Processing steps

Users generate traffic to a service or application, which triggers the authentication process as shown in the following figure. A user wishes to access a service or application protected by an authentication policy. The authentication portal located on NGFW requires a username and password.

1. The user's credentials are validated against LDAP or another authentication server type.
2. After the user submits credentials, the authentication server sends additional user data with its successful authentication message back to the authentication portal.
3. The authentication portal initiates MFA through PingID.



> **Note**
>
> You can achieve the same workflow for client-server applications also. For more information, see Configure GlobalProtect to Facilitate Multi-Factor Authentication Notifications.
> The following configuration steps only describe authentication for a browser-based application using the authentication portal.

4. PingID pushes an authentication request to the user's selected authentication method, such as mobile phone, email, or desktop application.
5. The user completes the authentication request.
6. PingID sends the authentication result to the authentication portal.
7. The authentication portal allows access to requested service

> **Note**
>
> In what follows, NGFW stands for New Generation Firewall

The following topics show how to secure an authentication portal sign-on with PingID. The example will add an LDAP and MFA authentication profile.

Preparing for configuration

Steps

1. In PingOne, download the PingID properties file.

For more information, see PingFederate.

2. In the Palo Alto NGFW admin portal, create a certificate profile for PingID.
    1. Go to **Device → Certificate Management → Certificate Profile → Add**.
    2. Create the certificate profile for PingID.

    For more information, see Configure a Certificate Profile in the Palo Alto documentation.

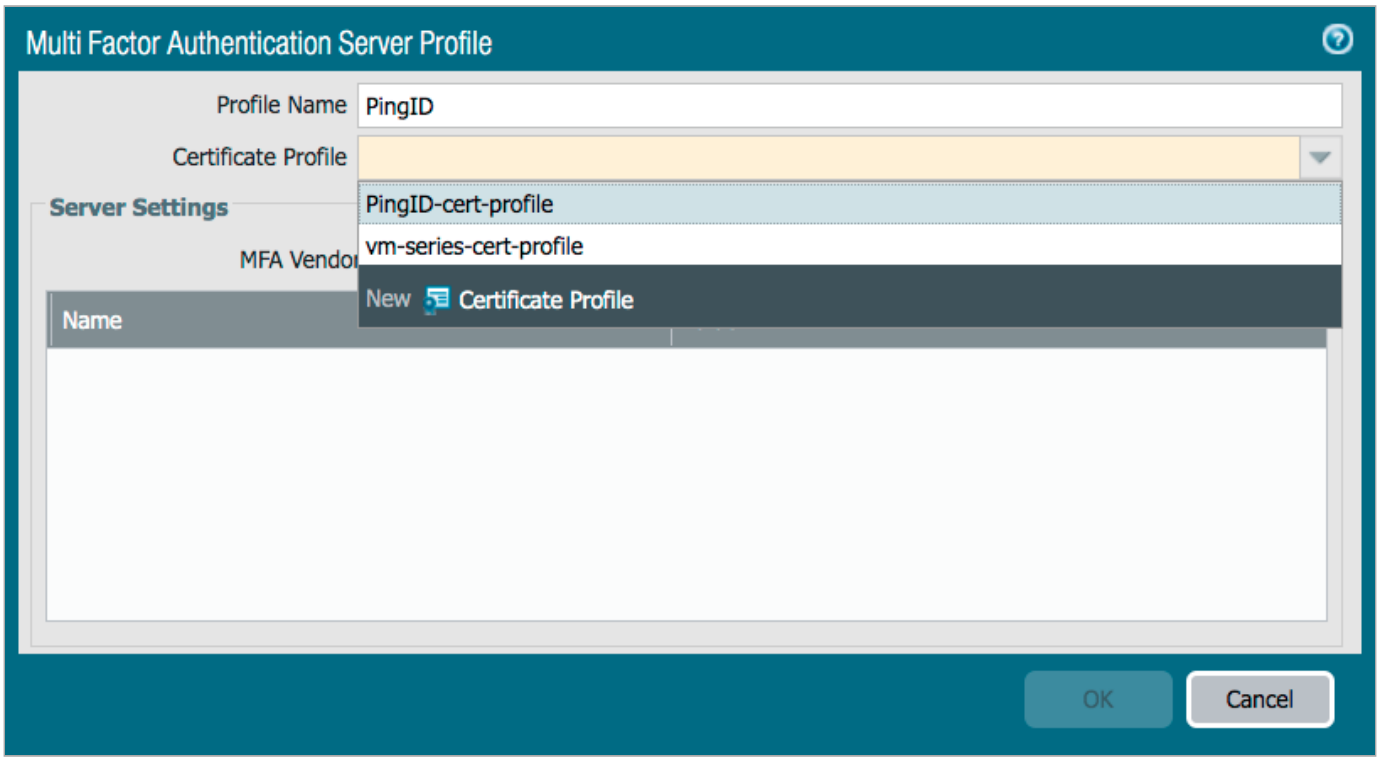
Adding PingID for MFA

Steps

1. In the NGFW admin portal, click the **Device** tab, and then go to **Server Profiles → Multi Factor Authentication**.
2. Click **+Add**.

    Result:

    The **Multi Factor Authentication Server Profile** window appears.



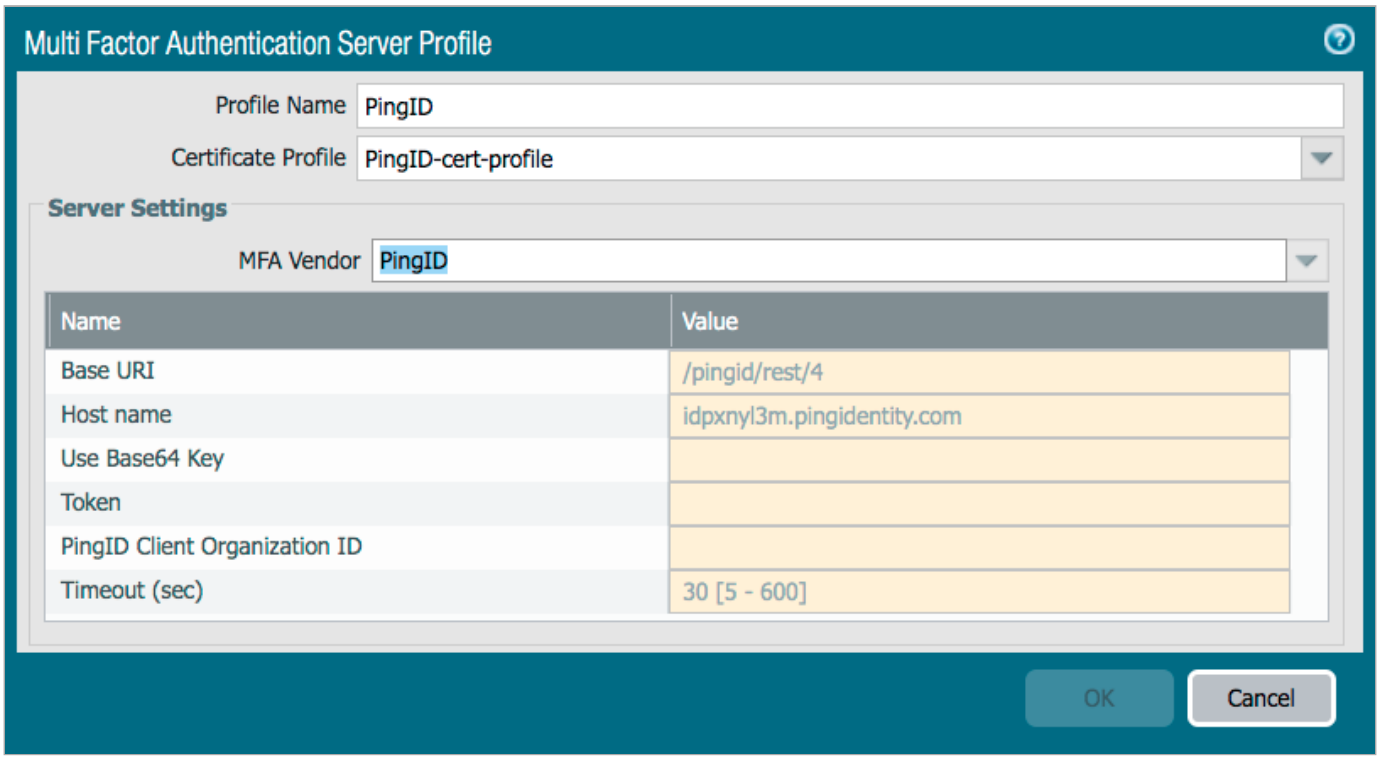
3. In the **Profile Name** field, enter a name for the profile. We will use **PingID**.
4. From the **Certificate Profile** list, select the certificate profile that you previously created.

    > **Note**
    >
    > If you have not yet created a certificate profile for PingID, see Configure a Certificate Profile in the Palo Alto documentation.

5. From the **MFA Vendor** list, select **PingID**.

Result:

Several fields populate automatically.

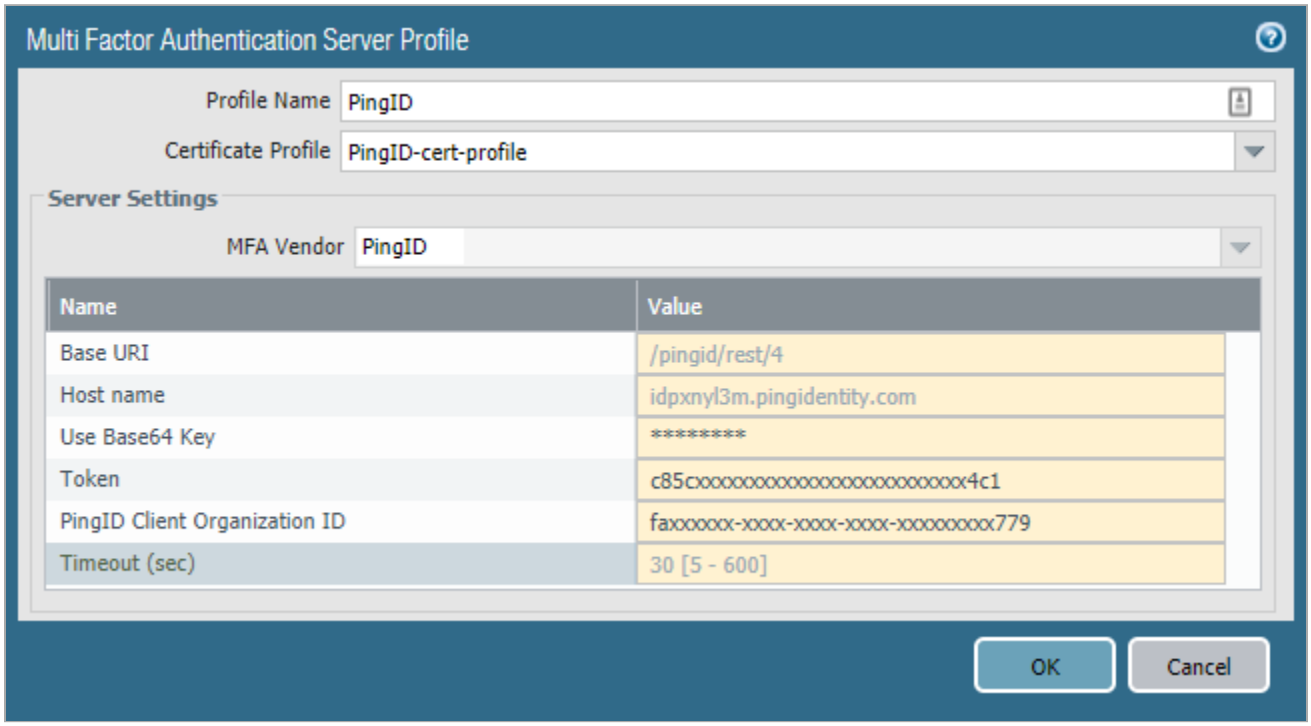


6. From the PingID properties file, complete the three fields listed in the following table.

   The relationships between the PingID properties fields and the fields listed in the **Multi Factor Authentication Server Profile** window are described in the following table.

Display Name	Certificate Field	Illustrative value
Use Base64 Key	`use_base64_key`	APIxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx7ct4z7LOM=
Token	`token`	c85cxxxxxxxxxxxxxxxxxxxxxxxxxx4c1
PingID Client Organization ID	`Org_alias`	faxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxx779

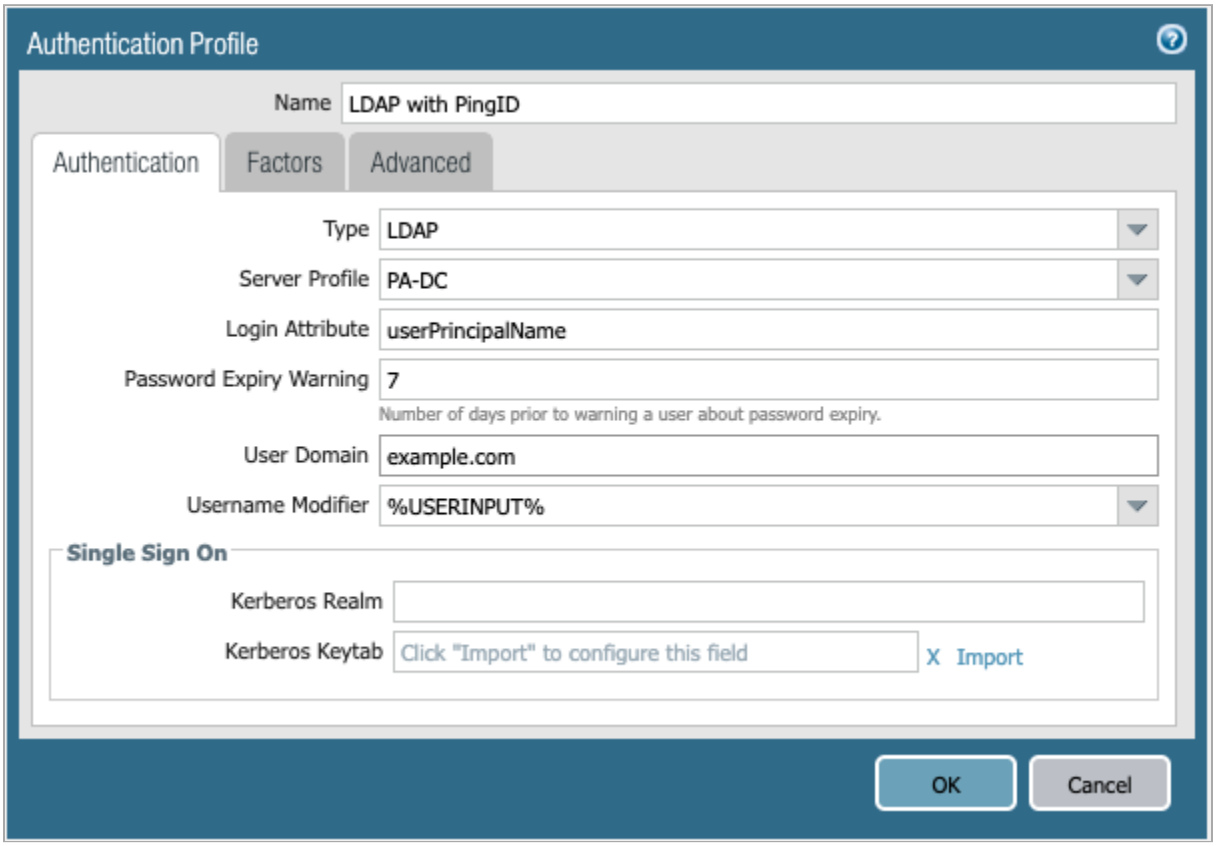
7. Ensure that the **Use Base64 Key**, **Token**, and **PingID Client Organization ID** fields are populated, and then click **OK**.



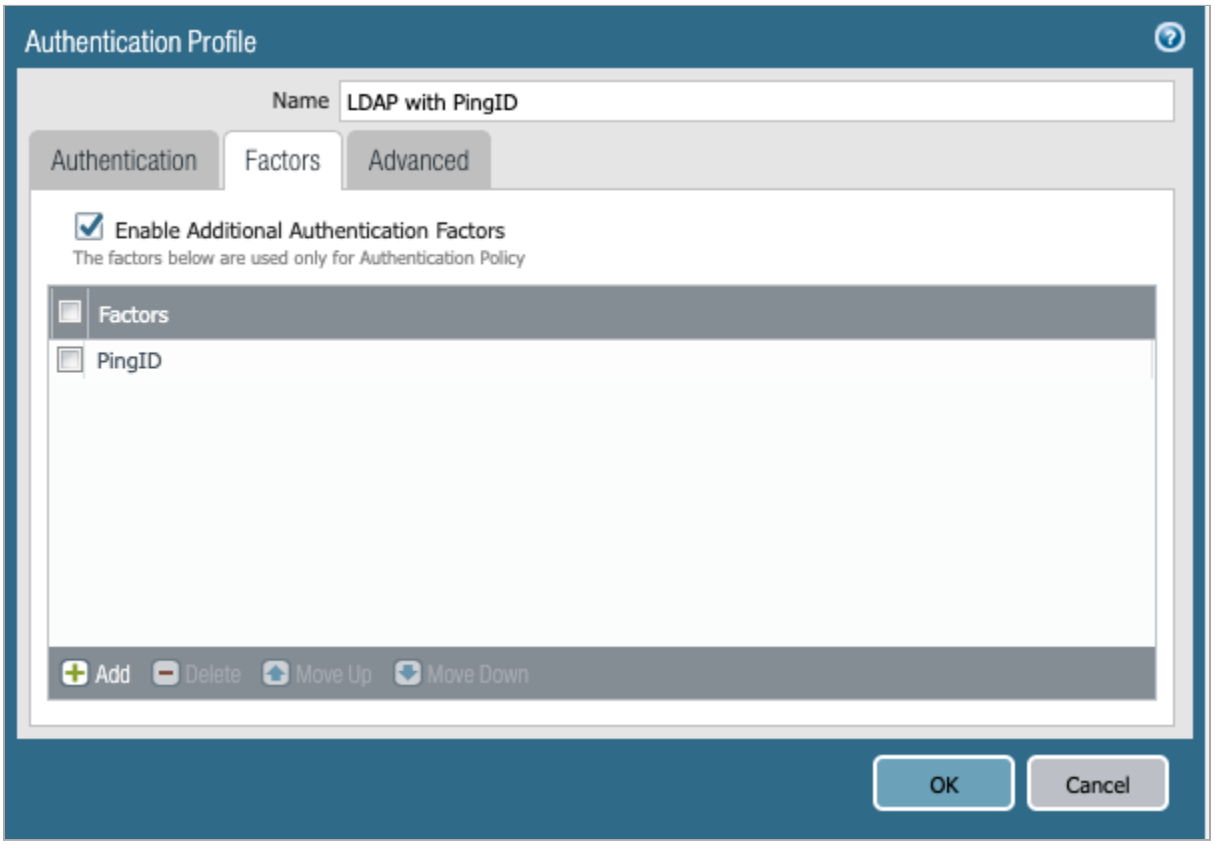
Configuring an authentication profile for MFA

Steps

1. In the Palo Alto NGFW admin portal, go to **Device → Authentication Profile**, and then click **Add**.
2. In the **Name** field, enter a name for the profile.
3. From the **Type** list, select **LDAP**.

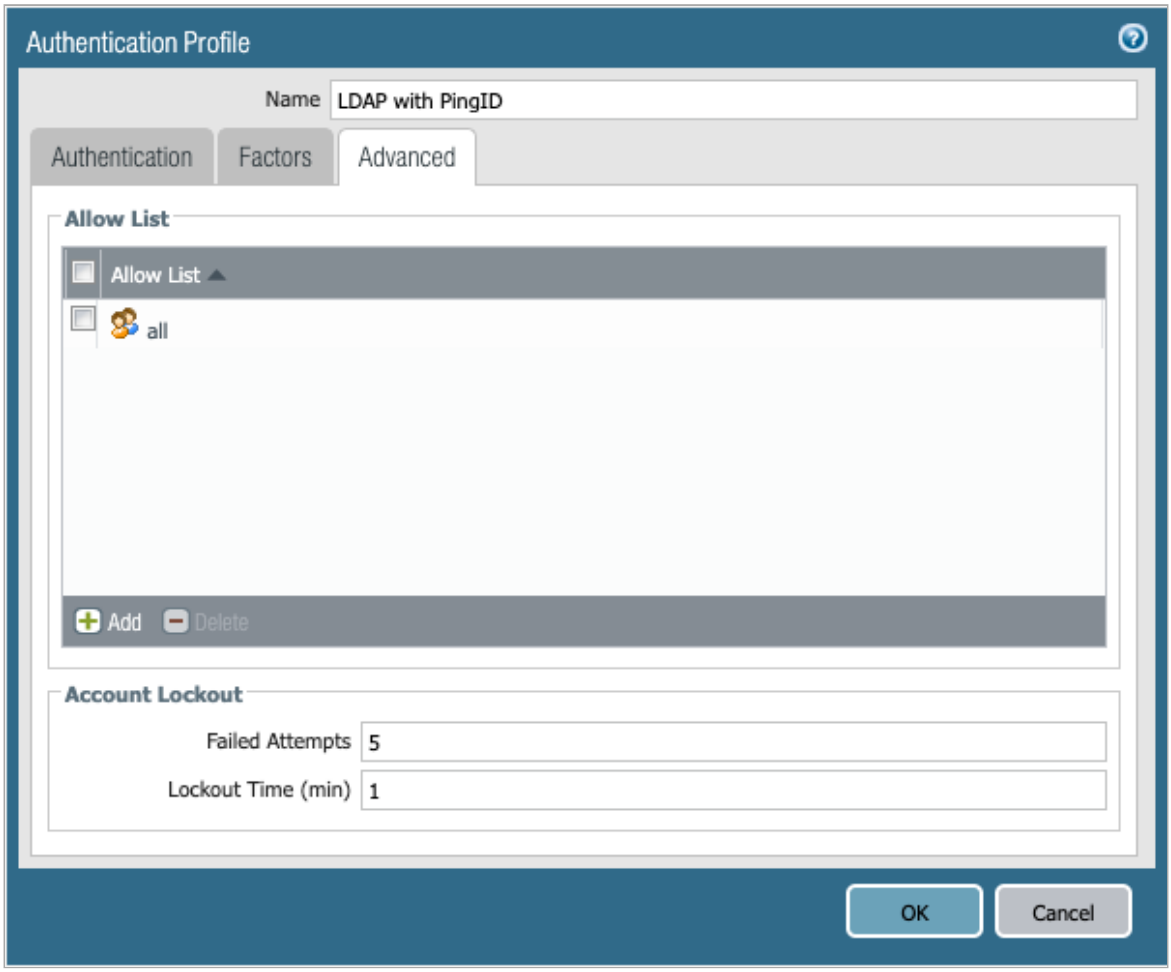


4. Go to the **Factors** tab and check **Enable Additional Authentication Factors**.



5. Click **Add**, and then select **PingID**.
6. Go to the **Advanced** tab, and in the **Allow List** section, click **Add** and select the relevant groups or users.

   In this example, we chose **all**.



7. **Optional:** Change the **Failed Attempts** and **Lockout Time** fields.
8. Click **OK**.

Configuring authentication enforcement

Create authentication enforcement to protect service and apps with the authentication portal.

Steps

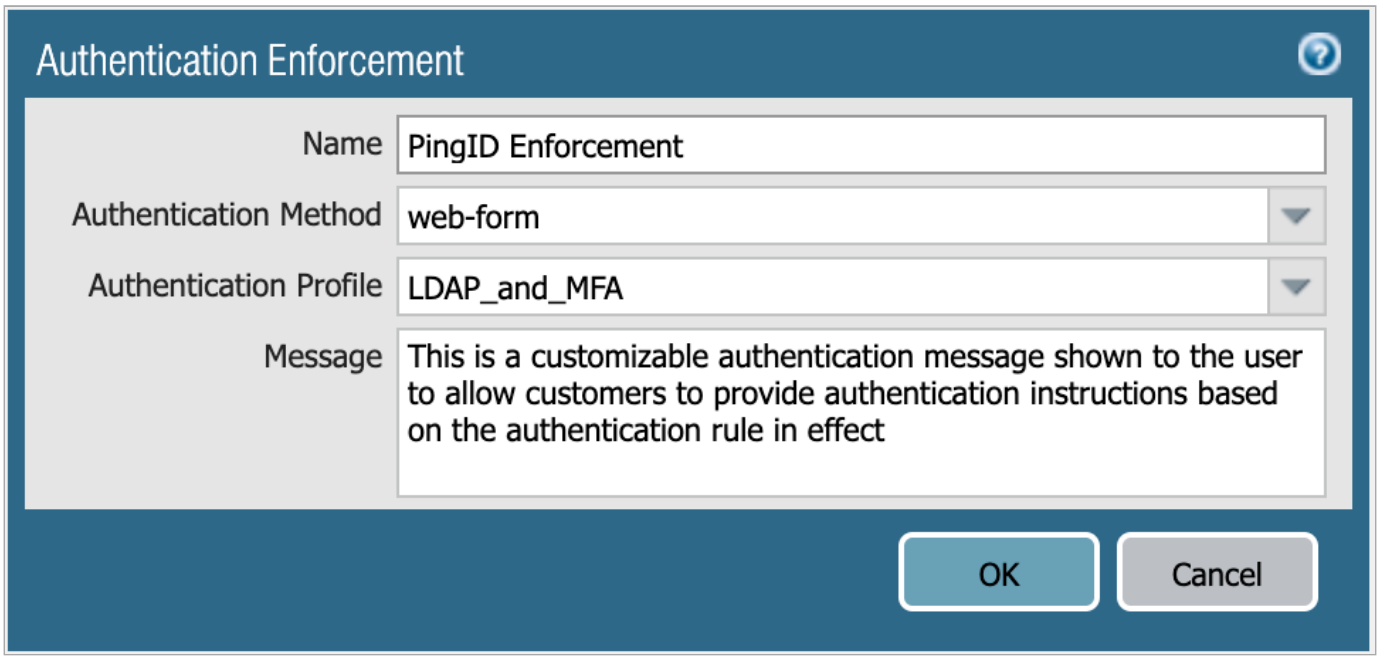
1. In the Palo Alto NGFW admin portal, go to **Objects → Authentication**, and then click **Add**.
2. In the **Name** field, enter a name for the authentication profile.
3. From the **Authentication Method** list, select **web-form**.

> **Note**
>
> This example configures authentication to a browser-based application using the authentication portal (**web-form**).

4. From the **Authentication Profile** list, select the appropriate certificate profile.

   For more information, see Preparing for configuration.

5. **Optional:** In the **Message** field, enter an instructional message for the user.



6. Click **OK**.

Next steps

For more information, see Authentication Enforcement in the Palo Alto documentation.

Configuring authentication policy

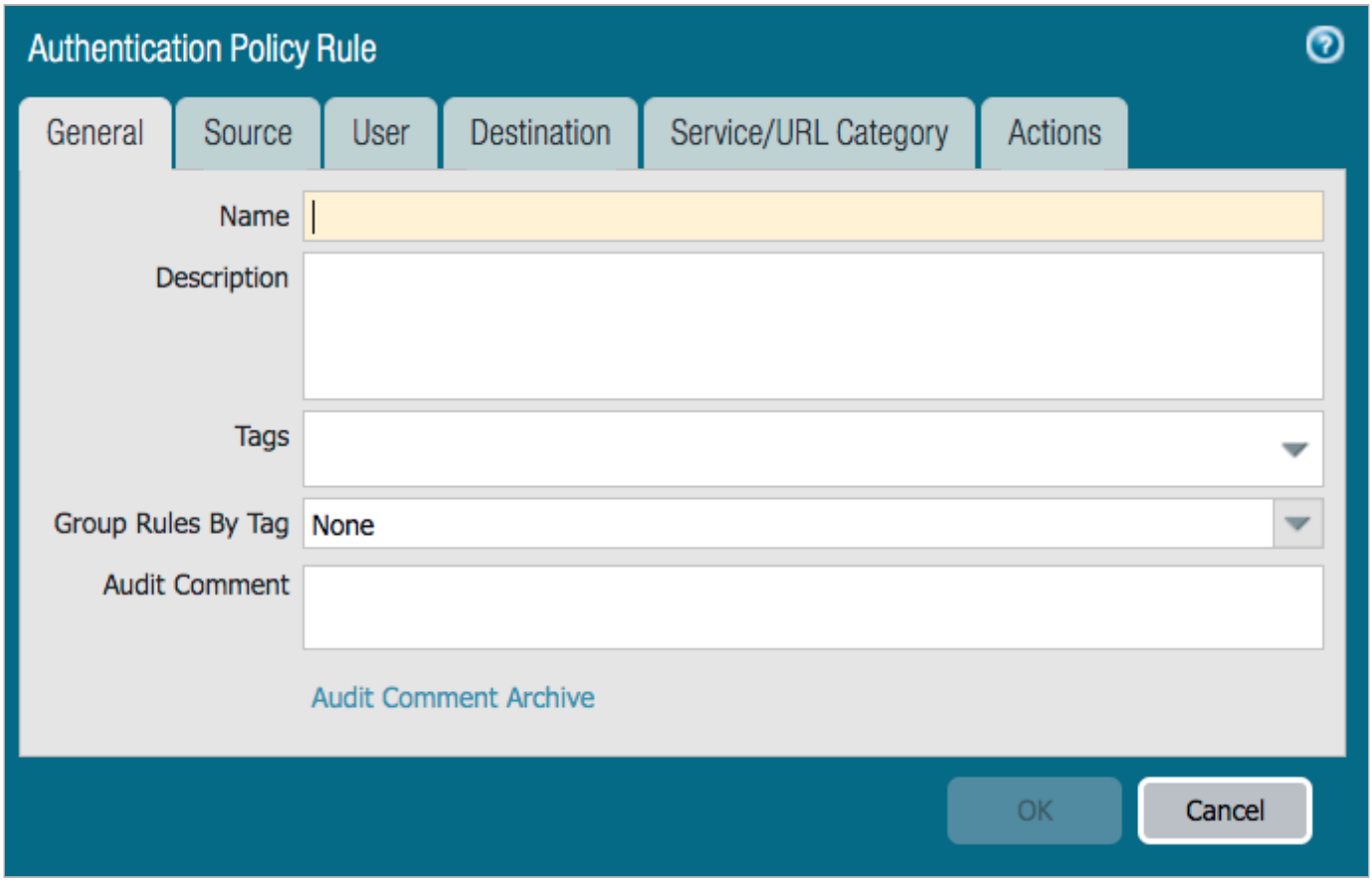
Create an authentication policy rule to protect chosen services or apps with the authentication portal.

Steps

1. In the Palo Alto NGFW admin portal, go to **Policies → Authentication**, and then click **Add**.

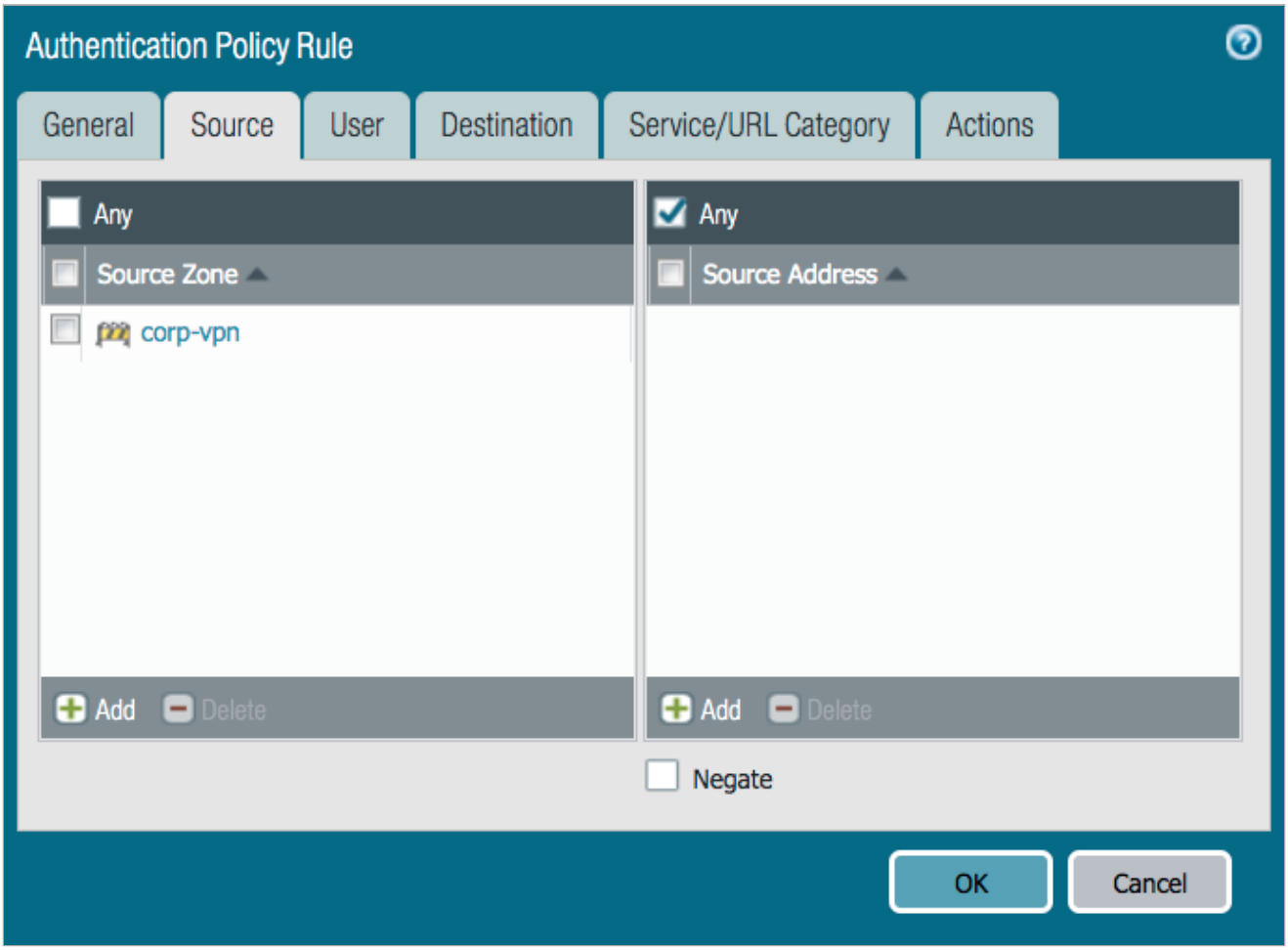
   Result:

   The **Authentication Policy Rule** window is displayed.

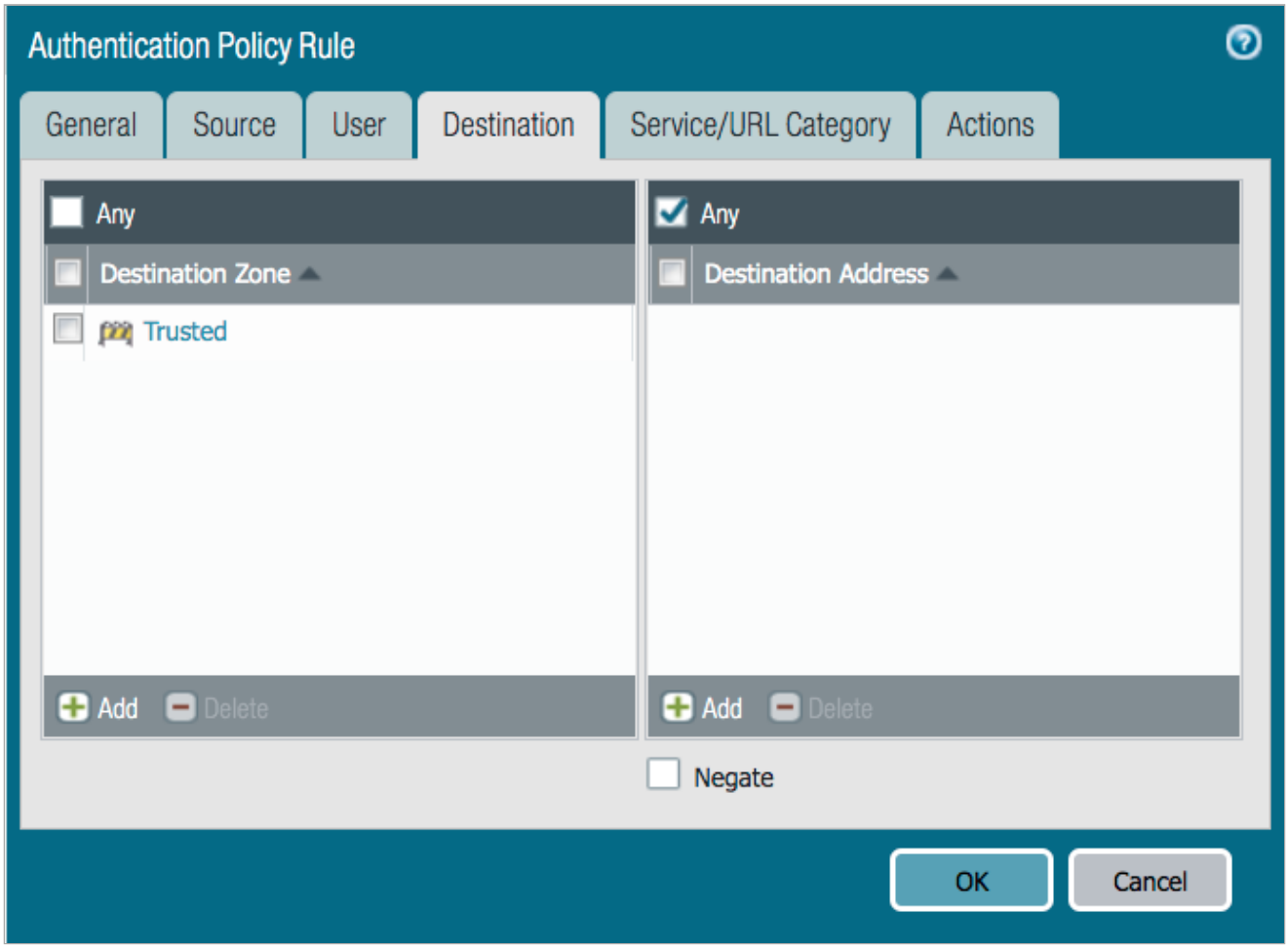


2. On the **General** tab, enter a name for the rule in the **Name** field.

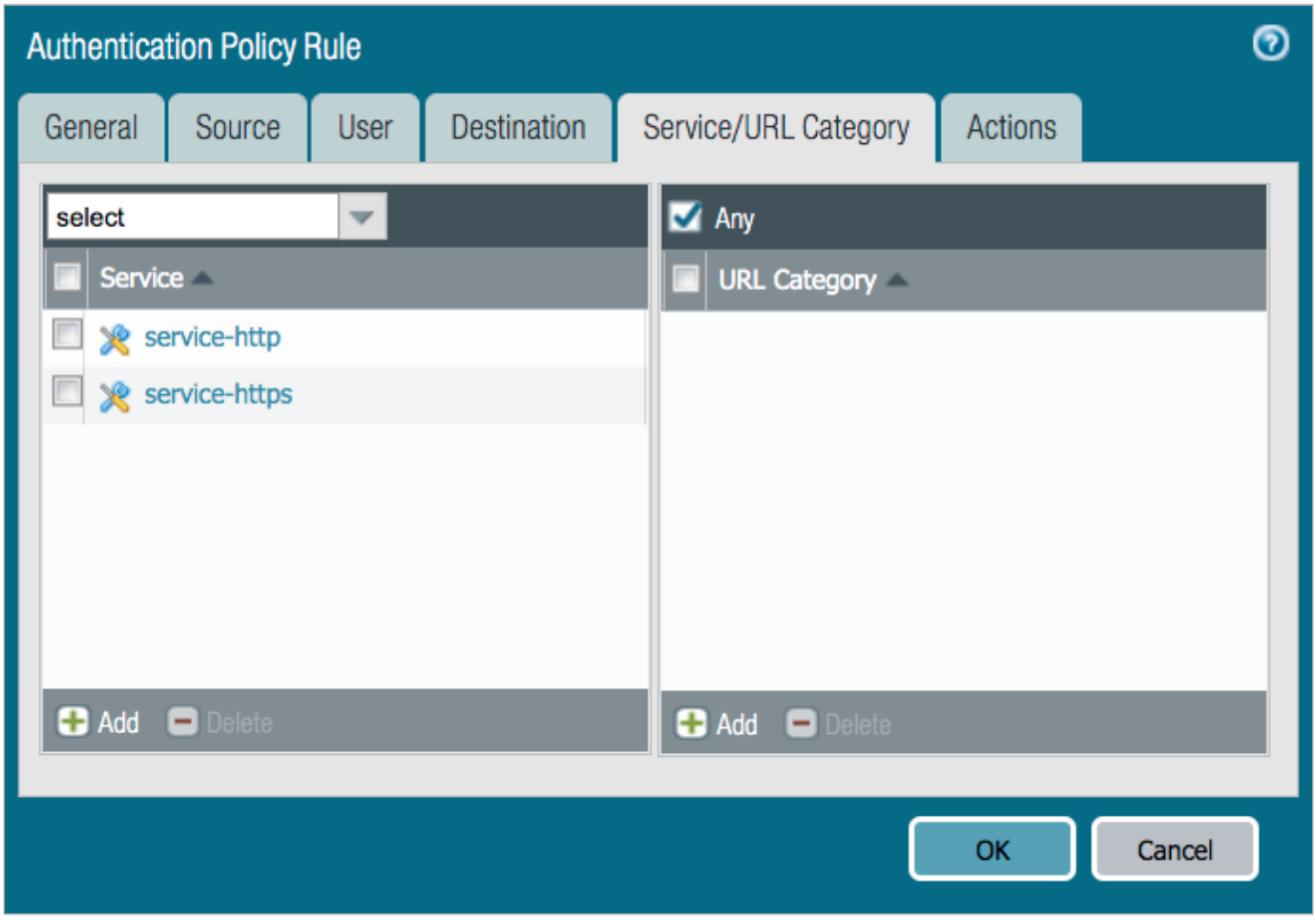
3. On the **Source** tab, from the **Source Zone** list, select an option.



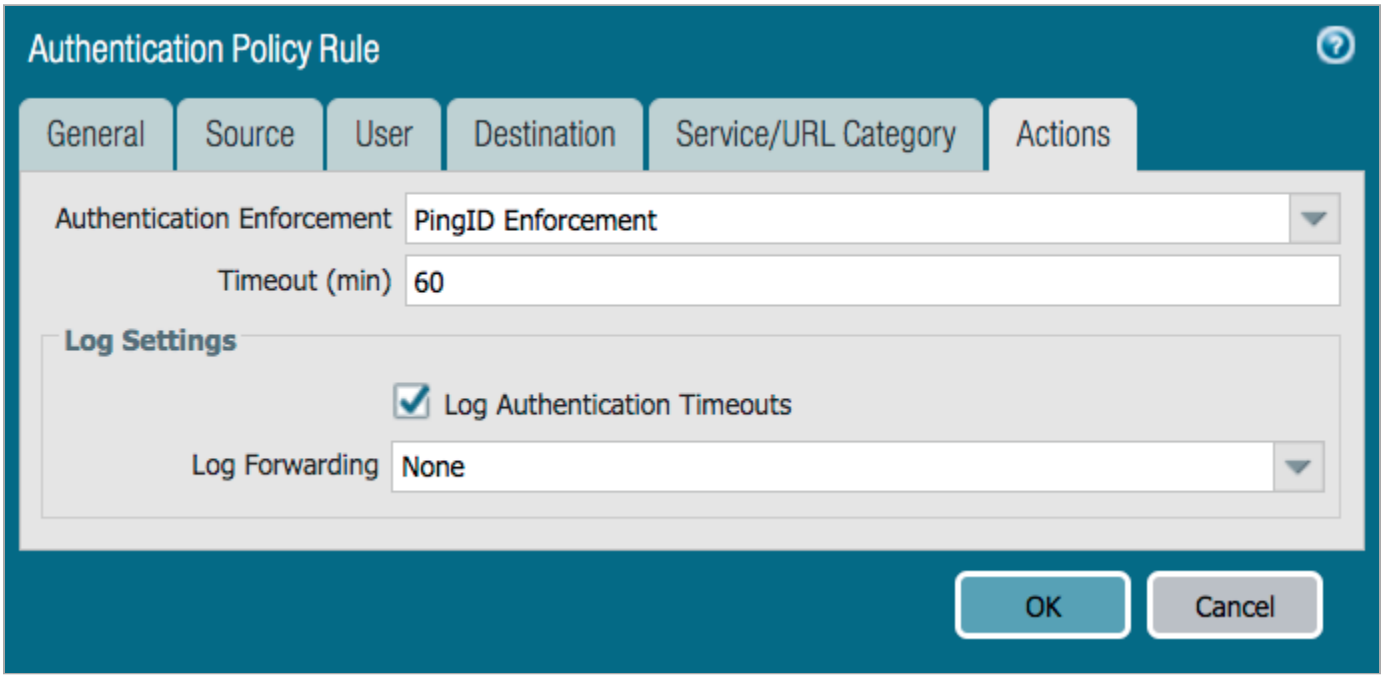
4. On the **Destination** tab, from the **Destination Zone** list, select an option.



5. On the **Service** tab, select the services or URL categories to protect.



6. On the **Actions** tab, from the **Authentication Enforcement** list, select the authentication enforcement that you created in the previous section. Click **OK**.



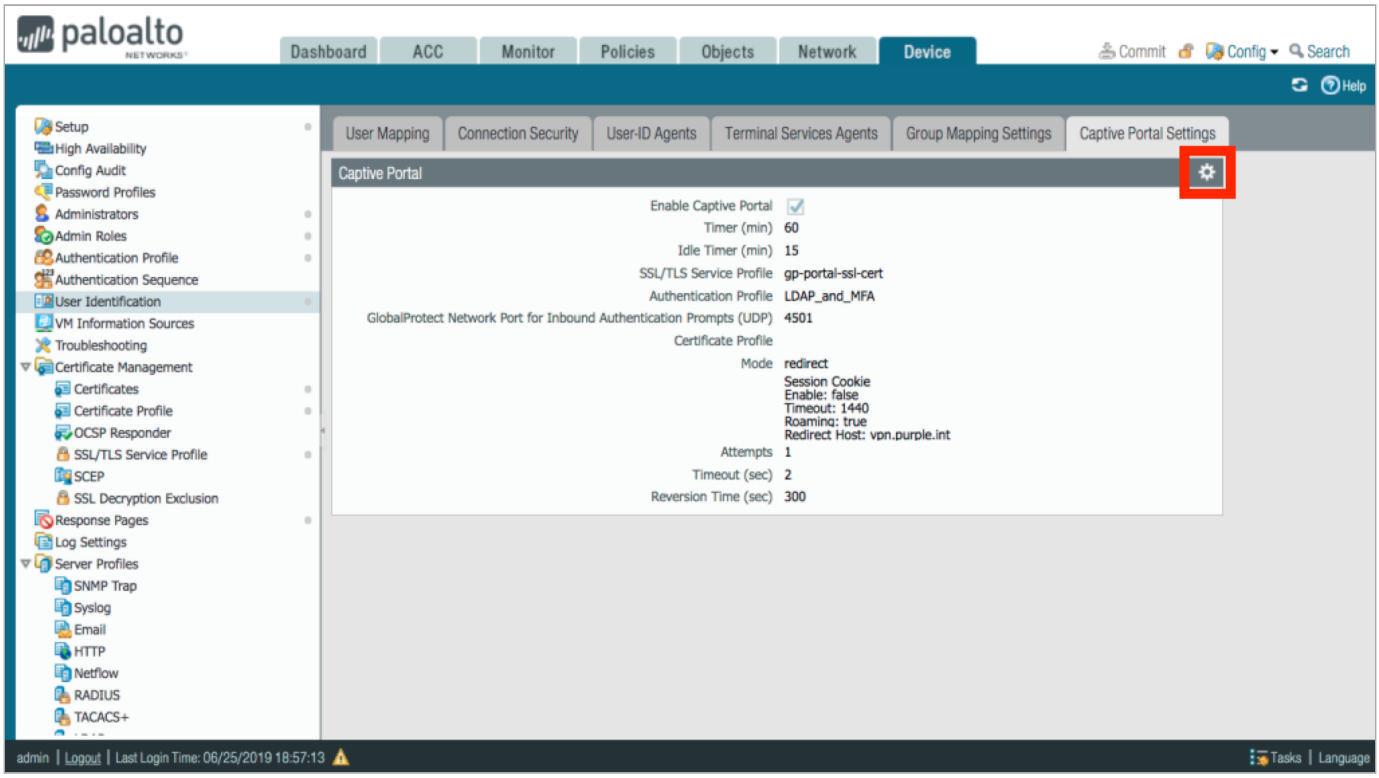
Next steps

For further information, see Authentication Policies.

Enabling the authentication portal

Steps

1. In the Palo Alto NGFW admin portal, go to **Device → User Identification → Captive Portal Settings**.
2. On the **Capture Portal Settings** tab, click the **Gear** icon.



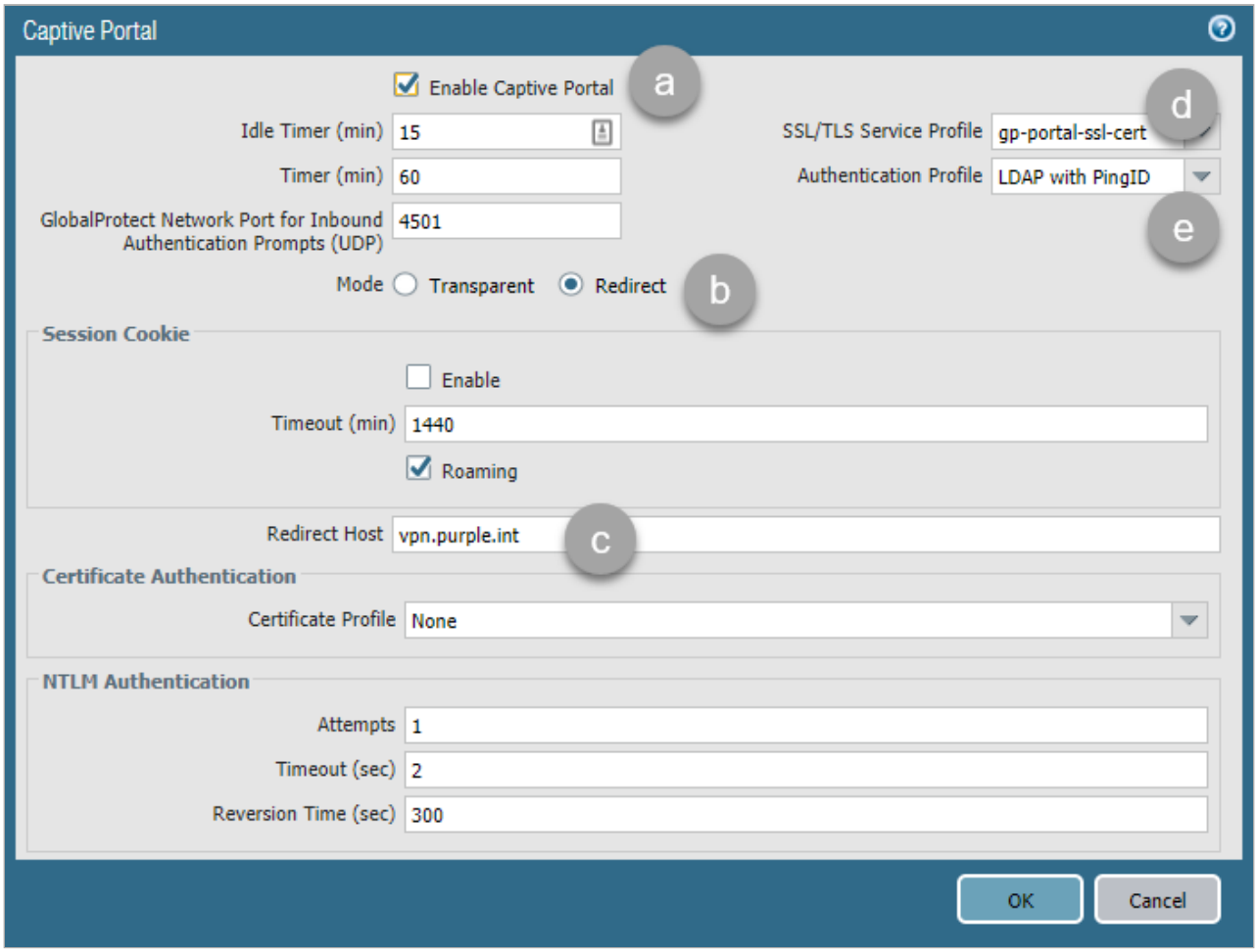
Result:

The **Captive Portal** window is displayed.

3. In the **Captive Portal** window, complete the following fields, and then click **OK**.
    1. Select the **Enable Captive Portal** check box.
    2. In the **Mode** section, click **Redirect**.
    3. In the **Redirect Host** field, enter the redirect host name.

> **Note**
>
> The redirect host name can be a URL or interface IP address on your firewall.

    4. From the **SSL/TLS Service Profile** list, select your SSL certificate.
    5. From the **Authentication Profile** list, select your authentication profile.



Checking that response pages are enabled

Before you begin

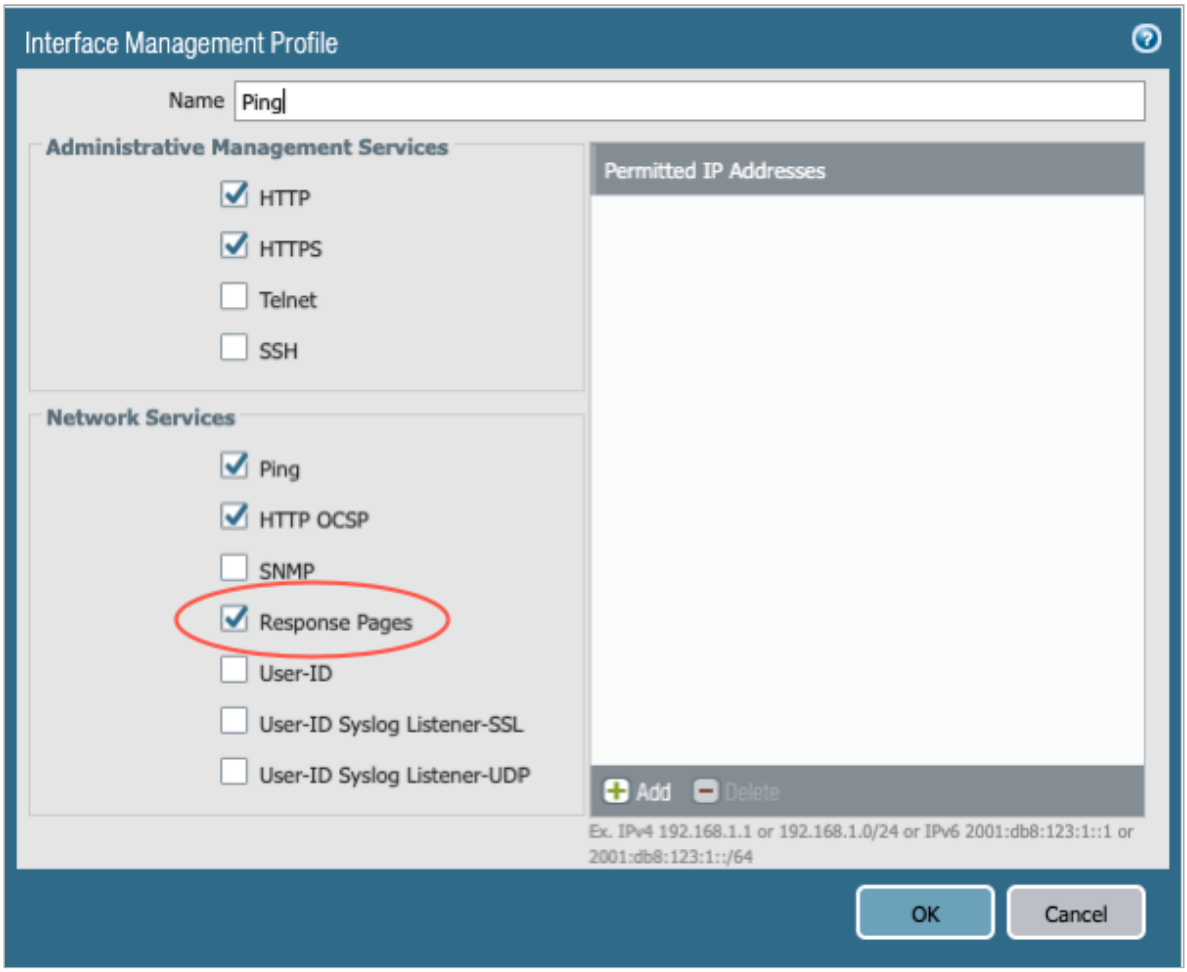
In the Palo Alto NGFW admin portal, go to **Network → Interfaces** and check that the interface you used for the Redirect Host has a management profile.

Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Tag	VLAN / Virtual-Wire	Security Zone	Features
ethernet1/1	Layer3			Dynamic-DHCP Client	main	Untagged	none	Trusted	
ethernet1/2	Layer3	Ping		Dynamic-DHCP Client	main	Untagged	none	Untrusted	
ethernet1/3				none	none	Untagged	none	none	

If no management profile exists, you must add a management profile for the interface. The following steps show how to edit an existing profile.

Steps

1. In the Palo Alto NGFW admin portal, go to **Network → Network Profiles → Interface Mgmt**.
2. Click the **Interface Management Profile** for the required interface.
3. Ensure that the **Response Pages** check box is selected, and then click **OK**.



4. Commit all changes.

Next steps: Creating security policy

To test the authentication portal, set up a security policy. For more information, see Building Blocks in a Security Policy Rule.

Integrate PingID with SSH

PingID provides SSH authentication services to protect local and remote sign on to Linux and Unix systems, including configuration options for Pluggable Authentication Module (PAM) and ForceCommand.

> **Note**
>
> For more information about required web access, see PingID required domains, URLs, and ports.

Important

Before attempting to configure this integration, ensure that you have sufficient expertise in your Linux distro and experience troubleshooting PAM and ForceCommand configurations.
The PingID module simply does MFA when told by the ForceCommand or PAM configuration. If PingID is not being invoked as expected, you most likely have a misconfiguration in your Linux configuration files. Ping Identity Support's ability to assist with questions related to Linux configuration is limited, and you should be prepared to consult Linux forums or other Linux experts for assistance.

Secure Shell (SSH)

SSH is an encrypted network protocol, which provides a remote or local secure channel over an unsecured network in a client-server architecture, connecting an SSH client application with an SSH server.

Pluggable authentication module (PAM)

PAM is a mechanism to integrate low-level authentication schemes into a high-level API. Applications that rely on authentication can be developed independently of the underlying authentication scheme.

ForceCommand

ForceCommand safely executes remote commands through SSH. ForceCommand can be associated with the SSH configuration of authorized keys.

Note

Limitation of ForceCommand

When PingID MFA is configured through ForceCommand, SSH commands that do not support interactive sessions, such as `scp` and `sftp`, do not allow authentication with a one-time Passcode (OTP).

This limitation does not apply when:

- Authenticating using a mobile device (push).
- PingID MFA is configured though the PAM module.

Caution

Adding multi-factor authentication (MFA) to a Unix or Linux system might result in locking you out of the system. To minimize this risk, back up your system before beginning an installation, and during an installation, keep a separate open session with root permissions.

Obtaining the PingID properties file for SSH

A PingID properties file is required during the installation of the PingID SSH agent.

Properties files may have full or restricted permissions. Full permissions should be used with care: They enable on-the-fly enrollment, device management and authentication which may not be desirable. For information on downloading the PingID properties file, see Managing the PingID properties file.

PingID SSH support information

The following tables list the operating systems on which the PingID integration with SSH is supported, and the authentication methods that are supported when using this integration.

Supported operating systems

Operating System	Supported Versions
Ubuntu	14.x to 22.x
Red Hat Enterprise Linux/CentOS	7.x and later. See Integration with RHEL-based distributions incorporating extended SELinux restrictions.
Debian	9.x to 12.x
SUSE Linux Enterprise Server	11.0 to 15.x
openSUSE	42.3, 15.x
Amazon Linux	Latest
Free BSD	9.x to 14.x
NetBSD	5.0 to 9.x
Solaris	10.0 to 11.x
AIX	7.x
HP-UX	11i v3 (B.11.31)
Fedora	19.0 to 39.x

PingID SSH has been tested on the following operating systems.

Tested operating systems

Operating System	Tested Versions
Ubuntu	14.04, 16.04, 18.04, 20.04, 22.04
Red Hat Enterprise Linux	7.0, 8.0, 9.0
CentOS	7.0, 8.0, CentOS Stream 8, CentOS Stream 9
Debian	9.0, 10.0, 11.0, 12.0
openSUSE	15.4, tumbleweed

The following authentication methods can be used when using the integration with SSH.

Supported authentication methods

Authentication method	Supported (yes/no)
PingID Mobile App	Yes
FIDO2 biometrics	No
Security key	No
Desktop soft token	Yes
Authentication app	Yes
OATH token	Yes
YubiKey - Yubico OTP	Yes
Email OTP	Yes
SMS and voice	Yes

Integration with RHEL-based distributions incorporating extended SELinux restrictions

To integrate PingID with Linux distributions that use SELinux restrictions, you must update SELinux policy.

Overview

SELinux is an extended permissions system that is present in most of the Linux distributions.

On CentOS and RHEL 7, SELinux is set to enforcing mode. It is configured to prevent sshd service and local login processes from making outbound HTTPS connections and creating or updating files in the file system. However, these operations are necessary for `pam_pingid` module to connect to PingID servers and to perform logging according to `pingid.conf` settings.

In other words, default SELinux settings and policies of CentOS 7 and RHEL 7 prevent the PAM module of PingID SSH from functioning properly when it is used with the sshd service or a local login process.

With PingID SSH agent 4.0.13, the user can easily update SELinux policy to allow the PAM module to work on CentOS and RHEL 7. When building PingID SSH from source code, the user can pass the `--enable-selinux` flag to the configure command.

```
./configure --with-pam --enable-selinux
```

This causes processes with `sshd_t` and `local_login_t` SELinux context types, or simply sshd and login processes, to be able to:

- Establish TCP connections to the set of ports that SELinux associates with HTTP/HTTPS protocols. The default ports are: 888, 80, 81, 443, 488, 8008, 8009, 8443, and 9000.

- Create a file, open a file, write to a file opened with the `O_APPEND` flag for files with `var_log_t` SELinux context type. Files inside the `/var/log` directory by default have `var_log_t` SELinux context type.

  If you need to write PingID log files into a directory, such as `/tmp/pingid.log`, then such an operation is still blocked by SELinux. To enable writing to this file, create the file manually and change its SELinux context type to `var_log_t:`.

  ```
  touch /tmp/pingid.log
  semanage fcontext -a -t var_log_t /tmp/pingid.log
  restorecon -v /tmp/pingid.log
  ```

Prerequisites

To enable the configure command to update the SELinux policy, the following packages must be installed on the OS:

- `policycoreutils`
- `selinux-policy-devel`

Disable PingID policies

To disable the SELinux policies added by PingID agent installation, run the following commands as root.

```
# disable local login policy
setsebool -P allow_pam_pingid_local_login=off

# disable sshd policy
setsebool -P allow_pam_pingid_sshd=off

# disable both policies
setsebool -P allow_pam_pingid_local_login=off allow_pam_pingid_sshd=off
```

Remove PingID policies

To remove all PingID SELinux policies, run the following command as root.

```
# remove all pingid policies
semodule -r pingid
```

PingID SSH installation and configuration

You can install PingID SSH from the source package or, on some distributions, from binaries.

Installing PingID SSH

Binary installation is supported for Ubuntu, Debian, CentOS, RHEL and SUSE. For details, see Installing PingID SSH binary package.

Source package installation is both OS and individual-system dependent. Use the following installation examples as **guidelines**:

- To install from Red Hat sources, see Installation example for Red Hat.

- To install from Ubuntu/Debian (64 bit) sources, see Installation example for Ubuntu/Debian (64 bit).
- To install from Solaris sources, see Installation example for Solaris.
- To install from AIX sources, see Installation example for AIX.
- To install from HP-UX sources, see Installation example for HP-UX.

Configuring PingID SSH

Installing from the PingID SSH source package produces a generic configuration. Update these configuration settings to implement specific options and requirements, such as PAM or ForceCommand. IMPORTANT: Use either PAM or ForceCommand. Do not implement both.

- For more information about configuring for PAM, see Configuring PAM.
- For more information about configuring for ForceCommand, see Configuring ForceCommand.

Installing PingID SSH binary package

Binary packages for PingID for Secure Shell (SSH) are available for the following Linux distributions: Ubuntu, Debian, CentOS, RHEL, and SUSE.

About this task

The binary packages for PingID for SSH are supported on the following Linux versions:

- Ubuntu 14.x to 22.x
- Debian 9.x to 12.x
- CentOS 7.x and later
- Red Hat Enterprise Linux (RHEL) 7.x and later
- OpenSUSE Leap 42.3, 15.x, and SUSE Linux Enterprise (SLES) 11.0 to 15.x

> **Caution**
>
> Adding multi-factor authentication (MFA) to a Unix or Linux system might result in locking you out of the system. To minimize this risk, back up your system before beginning an installation, and during an installation, keep a separate open session with root permissions.

Steps

1. Get the public key used to sign the package.

   Choose from:

   - On Ubuntu 22.x and Debian 12.x:

     ```
     curl -s https://packages.pingidentity.com/pub-key.gpg | sudo gpg --dearmor -o /etc/apt/trusted.gpg.d/
     pingid.gpg
     ```

- On earlier versions of Ubuntu and Debian:

```
curl -s https://packages.pingidentity.com/pub-key.gpg | sudo apt-key add -
```

- On CentOS, RHEL, and SUSE:

```
sudo rpm --import https://packages.pingidentity.com/pub-key.gpg
```

2. Update the repository information.

Choose from:

- On Ubuntu:

1. Add the PingID repository to the list of sources:

```
echo "deb https://packages.pingidentity.com/repo <release code name> <release code
name>" | sudo tee /etc/apt/sources.list.d/pingid.list
```

For example, on Ubuntu 20.04:

```
echo "deb https://packages.pingidentity.com/repo focal focal" | sudo tee /etc/apt/
sources.list.d/pingid.list
```

2. Update the package information from the list of sources:

```
sudo apt update
```

- On Debian:

1. Add the PingID repository to the list of sources:

```
echo "deb http://packages.pingidentity.com/repo <release code name> <release code
name>" | sudo tee /etc/apt/sources.list.d/pingid.list
```

For example, on Debian 10.x (Buster):

```
echo "deb http://packages.pingidentity.com/repo buster buster" | sudo tee /etc/apt/
sources.list.d/pingid.list
```

2. Update the package information from the list of sources:

```
sudo apt update
```

> **Note**
>
> If you are not sure what Debian release you have, run the following command to check:
>
> ```
> grep PRETTY_NAME /etc/os-release
> ```

- On CentOS:

  Copy file https://packages.pingidentity.com/repo/CentOS/pingidentity.repo to `/etc/yum.repos.d/pingidentity.repo` using the following command:

  ```
  sudo curl -o /etc/yum.repos.d/pingidentity.repo https://packages.pingidentity.com/repo/CentOS/pingidentity.repo
  ```

- On RHEL:

  Copy file https://packages.pingidentity.com/repo/RHEL/pingidentity.repo to `/etc/yum.repos.d/pingidentity.repo` using the following command:

  ```
  sudo curl -o /etc/yum.repos.d/pingidentity.repo https://packages.pingidentity.com/repo/RHEL/pingidentity.repo
  ```

- On SUSE:

  1. Add the PingID repository using the following command:

     ```
     sudo zypper ar https://packages.pingidentity.com/repo/SUSE/pingidentity.repo
     ```

  2. Refresh the repository:

     ```
     sudo zypper ref pingidentity
     ```

3. Install the PingID package.

   Choose from:

   - On Ubuntu and Debian:

     ```
     sudo apt install pingid
     ```

   - On CentOS and RHEL:

     ```
     sudo yum install pingid
     ```

   - On SUSE:

```
sudo zypper in pingid
```

4. Download the properties file. See Integrate PingID with SSH.
5. Copy the properties file to `/etc/pingid/pingid.properties`.
6. Test the installation:

```
pingid_fc -v
```

Result:

You should see a message similar to the following:

```
PingID API version 4.0 (Package version 4.0.12)
                                                Configuration file: /etc/pingid/pingid.conf
```

Upgrading to latest version of SSH integration

If you installed the PingID integration with SSH from the binary package, you can upgrade to the latest version of the integration by using the standard package manager commands for your distribution.

For RedHat, CentOS, SUSE, and SLES, the binary package provided does not depend on the specific release of the distribution that you are using, so there is no need to change the PingID entry in your repository sources. Just use the standard upgrade commands.

- On RedHat and CentOS:

```
sudo yum update pingid
```

- On SUSE and SLES:

```
sudo zypper ref pingidentity
sudo zypper install pingid
```

For Debian and Ubuntu, however, different packages are provided for the different supported releases of the distributions. So before running the commands for upgrading, check that your list of sources includes the correct PingID entry for the release you are using.

Version of Debian/Ubuntu	PingID PingIDentry to use
Ubuntu 14.04	deb https://packages.pingidentity.com/repo trusty trusty
Ubuntu 16.04	deb https://packages.pingidentity.com/repo xenial xenial

Version of Debian/Ubuntu	PingID PingIDentry to use
Ubuntu 18.04	deb https://packages.pingidentity.com/repo bionic bionic
Ubuntu 20.04	deb https://packages.pingidentity.com/repo focal focal
Debian 8	deb http://packages.pingidentity.com/repo jessie jessie
Debian 9	deb http://packages.pingidentity.com/repo stretch stretch
Debian 10	deb http://packages.pingidentity.com/repo buster buster

Once you've verified that you have the correct entry in your list of sources, you can run the standard upgrade commands:

```
sudo apt-get update
sudo apt-get install pingid
```

Install PingID SSH from source package

Installing PingID SSH using source files

Install PingID Secure Shell (SSH) using source files.

Before you begin

Verify that you have already installed the following prerequisite software packages:

- make
- c compiler
- autoconf
- automake
- libtool
- OpenSSL development version
- libCURL development version (Use version 7.2.1.3+ for PingID SSH 4.0.16+)
- libPAM development version. This is an optional dependency.

> **Note**
>
> Installation from operating system-specific source packages is covered here:
>
> - Red Hat: Installation example for Red Hat
> - Ubuntu/Debian: Installation example for Ubuntu/Debian (64 bit)
> - Solaris: Installation example for Solaris
>
> Follow the steps shown below for other Unix/Linux flavors.

About this task

To install PingID SSH from the source package:

Steps

1. Get the latest version of the package from https://www.pingidentity.com/en/resources/downloads/pingid.html
2. Extract the package.
3. Go to the directory of the extracted PingID package:

```
cd pingid-<version>
```

4. Run the configuration utility:

```
./configure --with-pam --prefix=/usr
```

In CentOS 7 & RHEL 7, when SELinux is installed, you might need to add this parameter to the `configure` command: `--enable-selinux`. See SELinux section in PingID SSH support information.

> **Note**
>
> When running the `./configure` command, there is an option to specify that the `use_base64_key` field in the PingID properties file should be obfuscated. To use this option, include the `--with-obfuscation` switch.
> If you have `openssl` and `base64` installed, the key required for obfuscation will be generated automatically so you can just use the following syntax:
>
> ```
> ./configure --with-obfuscation
> ```
>
> If you don't have `openssl` and `base64` installed, this command results in an error message. In this case, you can generate the key manually and then use `--with-obfuscation` as follows:
>
> ```
> ./configure --with-obfuscation=<keyToUse>
> ```

5. Build and install PingID SSH:

```
make
```

```
sudo make install
```

The following files will be installed, assuming the **`configure`** command was executed with the `--prefix=/usr` parameter:

- `/usr/sbin/pingid_fc`
- `/usr/etc/pingid/pingid.conf`

  (`/etc/pingid/pingid.conf` on FHS-compliant systems)
- If PAM was enabled, depending on the platform architecture:
  - `/lib64/security/pam_pingid.so` or
  - `/lib/security/pam_pingid.so`

For more about installation directories, see autoconf installation directories.

6. Test the installation:

```
pingid_fc -v
```

Result:

You should see output similar to the following:

```
PingID API version 4.0 (Package version 4.0.7)
Configuration file: /usr/etc/pingid/pingid.conf
```

7. Download the relevant PingID properties file (see Integrate PingID with SSH).
8. Copy the properties file to `/usr/etc/pingid/pingid.properties`.

Example:

```
sudo cp pingid.properties /usr/etc/pingid/pingid.properties
```

> **Important**
>
> Do not make any changes to the contents of the file.

Installation and configuration from sources: examples

The following procedures are examples of the installation and configuration of PingID SSH for selected operating systems. They should be treated as guidelines.

- Red Hat: Installation example for Red Hat
- Ubuntu/Debian (64bit): Installation example for Ubuntu/Debian (64 bit)
- Solaris: Installation example for Solaris

- AIX: Installation example for AIX
- HP-UX: Installation example for HP-UX

Install and configure Red Hat

Installation example for Red Hat

This is an example installation of PingID SSH for Red Hat. Your installation might vary depending on your particular configuration.

About this task

> **Note**
>
> PAM with SSHD is not supported on Red Hat Enterprise Linux prior to version 7.6.

Steps

1. Install the C compiler:

```
sudo yum install gcc
```

2. Install OpenSSL (development version):

```
sudo yum install openssl-devel
```

3. Install libCURL (development version):

```
sudo yum install curl-devel
```

4. Install libPAM (development version):

```
sudo yum install pam-devel
```

5. Download and extract the PingID package.
6. Go to the PingID installation directory:

```
cd pingid-<version>
```

7. Activate the configuration utility to enable PAM, and set the `/usr` prefix to install below the `/usr` directory:

```
./configure --with-pam --prefix=/usr
```

8. Build and install PingID SSH:

```
make
```

```
sudo make install
```

9. Download the properties file. See Integrate PingID with SSH.
10. Copy the properties file to `/etc/pingid/pingid.properties`.

Example:

```
sudo cp pingid.properties /etc/pingid/pingid.properties
```

> **Important**
>
> Do not make any changes to the contents of the file.

Next steps

In the event of problems, see Troubleshooting the PingID SSH installation.

Configuration example of PAM for Red Hat

This procedure is an example configuration of PingID SSH for PAM on Red Hat.

About this task

> **Note**
>
> This assumes that you specified `--prefix=/usr` in the configure command.

Steps

1. Edit the relevant PAM `conf` file. `sudo vi /etc/pam.d/system-auth`
2. Replace this line:

```
auth      sufficient  pam_unix.so nullok try_first_pass
```

   with these lines:

```
auth      requisite   pam_unix.so nullok try_first_pass
auth      sufficient  pam_pingid.so
```

3. Apply PingID to SSH by editing the `sshd_config` file:
    1. Run

```
sudo vi /etc/ssh/sshd_config
```

2. Set the following parameters:
   - `usePAM` to `yes`
   - `ChallengeResponseAuthentication` to `yes`
   - `PasswordAuthentication` to `no`

4. Configure PAM for public key authentication by adding the following line to the SSHD configuration file, `sshd_config`.

```
AuthenticationMethods publickey,keyboard-interactive
```

Remove `pam_unix.so` from the PAM configuration for SSHD, to prevent display of a password prompt for the keyboard-interactive authentication method.

> **Note**
>
> PAM authentication is supported for SSHD with public key authentication, only when using OpenSSH 6.2 and later.
> To check the OpenSSH version, run **`ssh -V`**.

5. Restart the sshd service.

`sudo service sshd restart`

Configuration example of ForceCommand for Red Hat

This is an example configuration of PingID SSH for ForceCommand on Red Hat.

About this task

> **Note**
>
> This process assumes that you specified `--prefix=/usr` in the configure command.

Steps

1. Edit the `sshd_config` file.

```
sudo vi /etc/ssh/sshd_config
```

   1. Add `pingid_fc` with its full path.

```
Match User joe
ForceCommand /usr/sbin/pingid_fc
```

> **Note**
>
> Disable `PermitTunnel` and `AllowTcpForwarding` in the `sshd_config` file because tunneling and port forwarding are performed before PingID authentication is triggered.

2. To apply the changes and activate PingID MFA integration with SSH, restart the sshd service.

```
sudo service sshd restart
```

Install and configure Ubuntu/Debian (64bit)

Installation example for Ubuntu/Debian (64 bit)

This is an example installation of PingID SSH for 64-bit Ubuntu or Debian distributions. Your installation might vary depending on your particular configuration.

Steps

1. Retrieve the latest versions of packages and their dependencies:

```
sudo apt-get update
```

2. Install the following packages:
    1. Compilers and utilities
    2. OpenSSL development version
    3. libCURL development version
    4. libPAM development version

```
sudo apt-get install build-essential libssl-dev libcurl4-openssl-dev libpam-dev
```

3. Download and extract the PingID package.
4. Go to the PingID installation directory:

```
cd pingid-<version>
```

5. Execute the following command, where `--prefix` points to the base folder into which you wish to install:

```
./configure --with-pam --prefix=/usr
```

6. Build and install PingID SSH:

```
make
```

```
sudo make install
```

7. Download the properties file. See Integrate PingID with SSH.
8. Copy the properties file to `/usr/etc/pingid/pingid.properties`.

   Example:

   ```
   sudo cp pingid.properties /usr/etc/pingid/pingid.properties
   ```

   > **Important**
   >
   > Do not make any changes to the contents of the file.

Next steps

In the event of problems, see Troubleshooting the PingID SSH installation.

Configuration example of PAM for Ubuntu/Debian

This is an example configuration of PingID SSH for PAM on Ubuntu and Debian distributions.

About this task

> **Note**
>
> This process assumes that you specified `--prefix=/usr` in the configure command or installed from the binary package.

Steps

1. Edit the relevant PAM `conf` file.

   ```
   sudo vim /etc/pam.d/common-auth
   ```

2. Replace the line:

   ```
   auth  [success=1 default=ignore]  pam_unix.so nullok_secure
   ```

   with these lines:

   ```
   auth requisite pam_unix.so nullok_secure
   auth  [success=1 default=ignore]  /lib/security/pam_pingid.so
   ```

3. Apply PingID to SSH by editing the `sshd_config` file:

   1. Run

```
sudo vi /etc/ssh/sshd_config
```

2. Set the following parameters:
   - `UsePAM` to `yes`
   - `KbdInteractiveAuthentication` to `yes`
   - `PasswordAuthentication` to `no`

4. Optionally, configure PAM for public key authentication by adding the following line to the SSHD configuration file, `sshd_config`.

```
AuthenticationMethods publickey,keyboard-interactive
```

Remove `pam_unix.so` from the PAM configuration for SSHD, to prevent display of a password prompt for the keyboard-interactive authentication method.

> **Note**
>
> To check the OpenSSH version, run **`ssh -V`**.

5. Restart the sshd service.

`sudo service sshd restart`

Next steps

Pair the end user device.

Configuration example of ForceCommand for Ubuntu/Debian

This is an example configuration of PingID SSH for ForceCommand on Ubuntu and Debian distributions.

About this task

> **Note**
>
> This process assumes that you specified `--prefix=/usr` in the configure command or installed from the binary package.

Steps

1. Edit the sshd_config file.

```
sudo vi /etc/ssh/sshd_config
```

   1. Add the following lines to the end of the file.

```
#enable pingid for all users
ForceCommand /usr/sbin/pingid_fc
```

> **Note**
>
> Disable `PermitTunnel` and `AllowTcpForwarding` in the `sshd_config` file because tunneling and port forwarding are performed before PingID authentication is triggered.

2. To apply the changes and activate PingID MFA integration with SSH, restart the sshd service.

```
sudo service sshd restart
```

Install and configure Solaris

Installation example for Solaris

This is an example installation of PingID Secure Shell (SSH) for Solaris. Your installation might vary depending on your particular configuration.

Steps

1. Download the prerequisite packages, as listed in Installing PingID SSH using source files.
2. Download and extract the PingID package.
3. Go to the PingID installation directory.

```
cd pingid-<version>
```

4. Set the environment variables in preparation for the build process.
    1. For build tools such as AR and MAKE:

```
export PATH=$PATH:/usr/ccs/bin:/usr/sfw/bin
```

    2. For the PingID build:

```
env CFLAGS=-I/usr/local/include LDFLAGS=-L/usr/local/lib ./configure --with-pam --prefix=/usr
```

5. Build and install PingID.

```
make
sudo make install
```

6. Download the properties file. See Integrate PingID with SSH.
7. Copy the properties file to `/usr/etc/pingid/pingid.properties`.

   Example:

   ```
   sudo cp pingid.properties /usr/etc/pingid/pingid.properties
   ```

   > **Important**
   >
   > Do not make any changes to the contents of the file.

Next steps

In the event of problems, see Troubleshooting the PingID SSH installation.

Configuration example of PAM for Solaris

This is an example configuration of PingID SSH for PAM on Solaris.

About this task

> **Note**
>
> This assumes that you specified `--prefix=/usr` in the configure command.

Steps

1. Edit the `pam.conf` file.

   ```
   sudo vi /etc/pam.conf
   ```

2. Replace these lines:

   ```
   #
   # Default definitions for Authentication management
   # Used when service name is not explicitly mentioned for authentication
   #
   other   auth requisite          pam_authtok_get.so.1
   other   auth required           pam_dhkeys.so.1
   other   auth required           pam_unix_cred.so.1
   other   auth required           pam_unix_auth.so.1
   ```

   with these lines:

```
#
# Default definitions for Authentication management
# Used when service name is not explicitly mentioned for authentication
#
other   auth requisite          pam_authtok_get.so.1
other   auth required           pam_dhkeys.so.1
other   auth required           pam_unix_cred.so.1
other   auth requisite          pam_unix_auth.so.1
other   auth required           pam_pingid.so
```

3. If you want to apply PingID on SSH, edit the `sshd_config` file.

```
sudo vi /etc/ssh/sshd_config
```

    1. Set the following configurations:
        - `PAMAuthenticationViaKBDInt` to `yes`
        - `ChallengeResponseAuthentication` to `yes`
        - `PasswordAuthentication` to `no`

4. Configure PAM for public key authentication by adding the following line to the SSHD configuration file, `sshd_config`.

```
                AuthenticationMethods publickey,keyboard-interactive
```

5. Remove `pam_unix.so` from the PAM configuration for SSHD to prevent PingID from displaying a password prompt for the keyboard-interactive authentication method.

> **Note**
>
> To check the OpenSSH version, run:
>
> ```
> ssh -V
> ```

6. To apply the changes and activate PingID multi-factor authentication (MFA) integration with SSH, restart the sshd service.

```
sudo service sshd restart
```

Configuration example of ForceCommand for Solaris

This is an example configuration of PingID SSH for ForceCommand on Solaris.

About this task

> **Note**
>
> This process assumes that you specified `--prefix=/usr` in the configure command.

Steps

1. Edit the `sshd_config` file.

```
sudo vi /etc/ssh/sshd_config
```

    1. Add `pingid_fc` with its full path.

```
# enable pingid for all users
ForceCommand /usr/sbin/pingid_fc
```

> **Note**
>
> Disable `PermitTunnel` and `AllowTcpForwarding` in the `sshd_config` file because tunneling and port forwarding are performed before PingID authentication is triggered.

2. To apply the changes and activate PingID MFA integration with SSH, restart the sshd service.

```
sudo service sshd restart
```

Install and configure AIX

Installation example for AIX

This is an example installation of PingID SSH for AIX. Your installation might vary depending on your particular configuration.

Steps

1. Download **`yum.sh`** from: https://public.dhe.ibm.com/aix/freeSoftware/aixtoolbox/ezinstall/ppc/yum.sh.

   If you experience difficulty downloading **`yum.sh`** directly to the server, first download it to the local machine, and then copy it to the server using **`scp`**.

2. From a terminal session, execute the following commands as root:

```
source yum.sh
yum update
yum install unzip automake libtool gcc curl-devel
```

3. Download and extract the PingID package.

4. Go to the PingID installation directory: `cd pingid-<version>`

5. Set the environment variables in preparation for the build process:

```
export M4=/opt/freeware/bin/m4
env LIBTOOLIZE=glibtoolize
```

6. From the terminal session, execute the following commands:

```
autoreconf --install jansson/jansson-2.13.1
autoreconf --install libjwt/libjwt-1.12.0
autoreconf --install
 ./configure --with-pam --prefix=/usr
 make
 make install #as root
```

7. Download the properties file. See Integrate PingID with SSH.
8. Copy the properties file to `/usr/etc/pingid/pingid.properties`.

   Example:

```
sudo cp pingid.properties /usr/etc/pingid/pingid.properties
```

> **Important**
>
> Do not make any changes to the contents of the file.

Next steps

In the event of problems, see Troubleshooting the PingID SSH installation.

Configuration example of PAM for AIX

This is an example configuration of PingID SSH for PAM on AIX.

About this task

> **Note**
>
> This assumes that you specified `--prefix=/usr` in the configure command.

Steps

1. Edit the `/etc/security/login.cfg` file and change this line near the bottom of the file.

   From:

```
auth_type = STD_AUTH
```

   To:

```
auth_type = PAM_AUTH
```

2. Edit the `/etc/pam.conf` file as follows:

   Choose from:

   - **To add MFA to SSH:**Change the lines starting with **`sshd`**:

     From:

     ```
     sshd auth required pam_aix
     ```

     To:

     ```
     sshd auth requisite pam_aix
     sshd auth required /usr/lib/security/pam_pingid.so
     ```

   - **To add MFA to SU:** Change the lines starting with **`su`**:

     From:

     ```
     su auth sufficient pam_allowroot
     su auth required pam_aix
     ```

     To:

     ```
     su auth sufficient pam_allowroot
     su auth requisite pam_aix
     su auth required /usr/lib/security/pam_pingid.so
     ```

Configuration example of ForceCommand for AIX

This is an example configuration of PingID SSH for ForceCommand on AIX.

About this task

> **Note**
>
> This assumes that you specified `--prefix=/usr` in the configure command, or installed from the binary package.

Steps

1. Edit the sshd_config file:

   `sudo vi /etc/ssh/sshd_config`

2. Add these lines to the end of the file:

   ```
   #enable pingid for all users
   ForceCommand /usr/sbin/pingid_fc
   ```

> **Note**
>
> Disable `PermitTunnel` and `AllowTcpForwarding` in the `sshd_config` file because tunneling and port forwarding are performed before PingID authentication is triggered.

3. Restart the sshd service:

```
sudo service sshd restart
```

Install and configure HP-UX

Installation example for HP-UX

This is an example installation of PingID Secure Shell (SSH) for HP-UX. Your installation might vary depending on your particular configuration.

About this task

The bundled C compiler on HP-UX is intended for building a kernel and is not much use for anything else. We need the HP-UX C/C++ Development Environment that includes the latest C compiler or gcc compiler. (This procedure was tested with gcc-4.2.3 32-bit Itanium 2, now deprecated.)

Steps

1. Download **`depothelper`** and **`gcc`** to local machine from ftp://hpux.connect.org.uk/hpux/Sysadmin/depothelper-2.20/depothelper-2.20-ia64_64-11.31.depot.gz and ftp://hpux.connect.org.uk/hpux/Gnu/gcc-4.2.3/gcc-4.2.3-ia64_32-11.31.depot.gz.
2. Copy **`depothelper`** and **`gcc`** to the hpux server:

```
scp -P <port> depothelper-2.20-ia64_64-11.31.depot.gz user@server.com:/tmp
scp -P <port> gcc-4.2.3-ia64_32-11.31.depot.gz user@server.com:/tmp
```

3. As root, unzip and install **`depothelper`** and **`gcc`**:

```
/usr/contrib/bin/gunzip /tmp/depothelper-2.20-ia64_64-11.31.depot.gz
/usr/contrib/bin/gunzip /tmp/gcc-4.2.3-ia64_32-11.31.depot.gz
```

   and then run:

```
/usr/sbin/swinstall -s /tmp/depothelper-2.20-ia64_64-11.31.depot
/usr/sbin/swinstall -s /tmp/gcc-4.2.3-ia64_32-11.31.depot.gz
```

4. As root, install curl:

```
/usr/local/bin/depothelper curl
```

5. Create simlinks (as root only for gcc-4.2.3 32-bit):

```
mkdir /usr/local/lib/hpux32
sudo ln -s /opt/gtk2.6/lib/libintl.so /usr/local/lib/hpux32/libintl.so
sudo ln -s /opt/gtk2.6/lib/libiconv.so /usr/local/lib/hpux32/libiconv.so
```

6. Copy the pingid tarball from the local machine to the server and unpack it:

```
scp -P <port> pingid-4.0.16.tar.gz user@server.com:/home/user
cd /home/user
/usr/contrib/bin/gunzip pingid-4.0.16.tar.gz
tar xvf pingid-4.0.16.tar
```

7. Set up the environment and build the 64 bit version:

   For gcc-4.2.3 32-bit only:

```
export CC="/usr/local/bin/gcc -mlp64"
```

   For all:

```
cd ~/pingid-4.0.16
aclocal
autoreconf -i
./configure --with-pam
make
sudo make install
```

8. Download the properties file. See Integrate PingID with SSH.

9. Copy your `pingid.properties` file to server:

```
scp -P  <port>  pingid.properties user@server.com:/home/user
sudo cp pingid.properties /usr/local/etc/pingid/
```

> **Important**
>
> Do not make any changes to the contents of the file.

10. If you do not have a collection of trusted root certification authorities on the server, you can download `cacert.pem` from https://curl.haxx.se/ca/cacert.pem to `/usr/local/etc/pingid/` using the command:

```
sudo curl https://curl.haxx.se/ca/cacert.pem -o /usr/local/etc/pingid/cacert.pem
```

Next steps

In the event of problems, see Troubleshooting the PingID SSH installation.

Configuration example of PAM for HP-UX

This is an example configuration of PingID SSH for PAM on HP-UX.

About this task

> **Note**
>
> This assumes that you specified `--prefix=/usr/local` in the configure command.

Steps

1. Create a backup of the common PAM configuration file, `/etc/pam.conf`.
2. Edit the `/etc/pam.conf` file as follows:

   Choose from:

   - **To add MFA to SSH:** Change the lines starting with `sshd`:

     From:

     ```
     sshd auth required libpam_hpsec.so.1
     sshd auth required libpam_unix.so.1
     ```

     To:

     ```
     sshd auth required libpam_hpsec.so.1
     sshd auth required /usr/lib/security/pam_pingid.so
     ```

     1. Apply PingID to SSH by editing the sshd_config file:

        ```
        sudo vi /opt/ssh/etc/sshd_config
        ```

     2. Set `UsePAM` to 'yes', `ChallengeResponseAuthentication` to 'yes' and `PasswordAuthentication` to 'no'.
     3. Configure PAM for public key authentication by adding the following line to the SSHD configuration file, `sshd_config`:

        ```
        AuthenticationMethods publickey,keyboard-interactive
        ```

        > **Note**
        >
        > To check the OpenSSH version, run
        >
        > ```
        > ssh -V
        > ```

4. Restart the sshd service:

```
sudo /sbin/init.d/secsh stop
sudo /sbin/init.d/secsh start
```

- **To add MFA to SU:** Change the lines starting with `su`:

  From:

```
su auth required libpam_hpsec.so.1 bypass_setaud
su auth required libpam_unix.so.1
```

  To:

```
su auth required libpam_hpsec.so.1 bypass_setaud
su auth requisite libpam_unix.so.1
su auth required /usr/lib/security/pam_pingid.so
```

Configuration example of ForceCommand for HP-UX

This is an example configuration of PingID SSH for ForceCommand on HP-UX.

About this task

> **Note**
>
> This assumes that you specified `--prefix=/usr/local` in the configure command.

Steps

1. Edit the sshd_config file:

```
sudo vi /opt/ssh/etc/sshd_config
```

2. Add these lines to the end of the file:

```
#enable pingid for all users
ForceCommand /usr/local/sbin/pingid_fc
```

> **Note**
>
> Disable `PermitTunnel` and `AllowTcpForwarding` in the `sshd_config` file because tunneling and port forwarding are performed before PingID authentication is triggered.

3. Restart the sshd service:

```
sudo /sbin/init.d/secsh stop
sudo /sbin/init.d/secsh start
```

Configuring PAM

Configure the PingID SSH installation to enable it to work with PAM.

About this task

There are two main steps you must carry out to configure PAM for PingID:

- Edit the SSH configuration file `sshd_config` to set it up to use PAM.
- Edit the PAM configuration file to instruct PAM to use the PingID PAM module.

Caution

Do not enable PAM for SSHD while ForceCommand is being used. This will confuse the SSHD service and may cause authentication issues in SSHD-based utilities (for example, ssh, scp, or sftp).

Important

While changing SSHD or PAM configurations, keep an open session with root permissions. This will allow you to reverse any changes without being locked out of the server.

Steps

1. Open the SSHD configuration file `/etc/ssh/sshd_config` in a text editor (requires superuser permissions).
2. Locate the `AuthenticationMethods` line in the file. Add `keyboard-interactive` as a method (if it is not already there), as this is required by PingID. This should be in addition to any other methods you have there. For example, if you use key-based authentication for standard SSH authentication, the `AuthenticationMethods` line should look like this: `AuthenticationMethods publickey,keyboard-interactive`
3. Since each authentication method listed must also be enabled explicitly, make sure that the `sshd_config` file also contains the line `KbdInteractiveAuthentication yes`.
4. Set the following parameters in the `sshd_config` file:
    1. `UsePAM yes`
    2. `ChallengeResponseAuthentication yes`
    3. `PasswordAuthentication no`
5. Open the PAM configuration file in a text editor (requires superuser permissions). This should be the PAM configuration file for the service that you want to protect with PingID. If you are protecting the ssh service, on most Linux installations the relevant configuration file is `/etc/pam.d/sshd`.

> **Note**
>
> Your `/etc/pam.d` directory may contain specific configuration files that are included in the configuration file for ssh, for example, `system-auth`, `common-auth` and `password-auth`. If you include the PingID PAM module in a top-level configuration file, it will affect all the services that are referenced in that configuration file.

6. Since the PingID module is added to serve as a second authentication factor, the configuration changes described in this step can differ slightly, depending on the first authentication factor used.

   Choose from:

   - If the first authentication step consists of username/password:
   - Add `pam_pingid.so` after `pam_unix.so` in the configuration file.
   - Set the control options for `pam_pingid.so` to be the same as those currently set for `pam_unix.so`.
   - Change the control option for `pam_unix.so` to `requisite`, which means that the step must be successful for authentication to continue.
   - If the first authentication step is key-based authentication:
   - Add `pam_pingid.so` after `pam_unix.so` in the configuration file (if `pam_unix.so` appears there).
   - Set the control options for `pam_pingid.so` to be the same as those currently set for `pam_unix.so`.
   - Remove `pam_unix.so` from the file to prevent the username/password dialog from being displayed.

7. Restart the sshd service: `sudo service sshd restart`

Configuring ForceCommand

Configure the PingID SSH installation to enable it to work with ForceCommand.

About this task

> **Important**
>
> While changing SSHD or PAM configurations, keep an open session with root permissions. This will allow you to reverse any changes without being locked out of the server.

> **Note**
>
> **Limitation of ForceCommand:**
> When PingID MFA is configured via ForceCommand, SSH commands that don't support interactive sessions (for example, scp and sftp) do not allow authentication with a One Time Passcode (OTP).
> The above limitation does not apply when authenticating using a mobile device (push).

This procedure assumes that PingID was installed with `--prefix=/usr`:

Steps

1. Add the following lines at the end of the SSH configuration file (for example, `/etc/ssh/sshd_config`).

Option	Description

Enable single user	`# enable pingid for testuser`
	`Match User testuser`
	`ForceCommand /usr/sbin/pingid_fc`

Disable single user	`# disable pingid for testuser`
	`Match User !testuser`
	`ForceCommand /usr/sbin/pingid_fc`

Enable group	`# enable pingid for all users in testgroup`
	`Match Group testgroup`
	`ForceCommand /usr/sbin/pingid_fc`

Disable group	`# disable pingid for all users in testgroup`
	`Match User * Group !testgroup`
	`ForceCommand /usr/sbin/pingid_fc`

Enable all users	`# enable pingid for all users` `ForceCommand /usr/sbin/pingid_fc`

> **Note**
>
> Disable `PermitTunnel` and `AllowTcpForwarding` in the `sshd_config` file because tunneling and port forwarding are performed before PingID authentication is triggered.

2. Restart the sshd service:

`sudo service sshd restart`

Mapping usernames with ForceCommand

Mapping usernames enables PingID SSH for users with specific public keys.

Steps

- Use the command option in the `~/.ssh/authorized_keys` file.

Example:

```
command="/usr/sbin/pingid_fc -u john" ssh-rsa AAA..../KO== john@luni.com
command="/usr/sbin/pingid_fc -u david" ssh-rsa BAB...JIL== david@luni.com
```

> **Note**
>
> This procedure assumes that PingID was installed with `--prefix=/usr`.

PingID SSH configuration file parameters

You can configure the behavior of the PingID SSH agent by modifying the configuration file.

The PingID SSH configuration file, `pingid.conf`, is usually located under `/usr/etc/pingid`.

The following table describes the configuration parameters and their valid and default values.

PingID SSH Configuration File Parameters

Parameter	Description	Valid Values	Default Values
`verbose`	Toggle extended logging.	`true`, `false`	`false`
`log_file`	Define a file name and path for the pingid log file.	Full path of the log file.	None. Messages are written to the system log.
`policy_user_not_registered`	Set the policy for users that are not registered.	• `register`: Start the registration (onboarding) process for the user. • `allow`: Allow access without registration. • `fail`: Deny access. • `grace_fail`: Allow access as long as the organization grace period has not passed. After that, deny access.	`register`
`domain_postfix`	The suffix to be appended to the user in cases where it should be registered with the full domain name.	The domain suffix. For example, `@example.com`.	None
`max_prompts`	The maximum number of prompts the user can receive during the initial registration process.	Any integer from 1 - 10.	`8`

Parameter	Description	Valid Values	Default Values
`fail_mode`	How to behave if the connection to the PingID service cannot be established.	• `restrictive`: only online authentication is permitted. If the PingID server cannot be reached, authentication cannot be carried out. • `passive_offline_authentication`: offline authentication is permitted as a backup method if communication cannot be established with the PingID server • `enforce_offline_authentication`: only offline authentication is used • `permissive`: If the PingID server cannot be reached, bypass authentication.	`restrictive`
`proxy`	The URL of the `http_proxy` or the `https_proxy`.		None
`proxy_verify_cert`	• If set to `true`, the SSH agent uses the default value for `curl` option: `CURLOPT_SSL_VERIFYPEER` • If set to `false`, SSH agent uses 0 value for `curl` option: `CURLOPT_SSL_VERIFYPEER` Relevant only when the `proxy` option is set.	`true`, `false`	`false`
`proxy_ca_file`	Path to CA file Relevant only when the `proxy` option is set.	Path to CA file	Empty

Parameter	Description	Valid Values	Default Values
`proxy_user_pwd`	If your proxy server requires you to provide a username and password for authentication, use `proxy_user_pwd` to specify that information. Relevant only when the `proxy` option is set.	Provide the username and pasword with a colon in between, for example, `proxy_user_pwd=myUserName:myPassword`. If the username or password include a colon, replace the colon in the username/password with `%3A`	If you specified a value for `proxy` but do not provide a value for `proxy_user_pwd`, it is assumed the proxy server does not require a username and password.

Enabling offline MFA in SSH integration

You can modify the settings in the configuration file to enable offline MFA for situations where the PingID MFA service is unavailable. There is also an option to always use offline MFA even when there are no issues that prevent online MFA.

Use the *fail_mode* setting in the configuration file to enable offline MFA. This setting can take the following values:

- *restrictive* - only online authentication is permitted. If the PingID server cannot be reached, authentication cannot be carried out.
- *passive_offline_authentication* - offline authentication is permitted as a backup method if communication cannot be established with the PingID server
- *enforce_offline_authentication* - only offline authentication is used
- *permissive* - if the PingID server cannot be reached, bypass authentication.

When offline authentication is used, PingID uses information from an encrypted file called `.localFallbackDevices` in order to generate the twelve-digit number that is shown to the user. The location of this per-user file on the server is specified by the *offline_devices_path* setting in the configuration file, for example:

```
offline_devices_path=/home/${username}/.localFallbackDevices
```

> **Note**
>
> The `.localFallbackDevices` file is created upon the first successful online authentication with a mobile device. This means that a user can authenticate offline only if they have carried out online authentication at least once.

Troubleshooting the PingID SSH installation

This section can help you diagnose and resolve issues with your PingID SSH installation.

Verifying PingID installation

Verifying your PingID installation

Before performing the post-installation steps, verify the successful installation of PingID.

Steps

1. Run the binary

```
pingid_fc
```

2. Confirm that you get the pairing instructions.

   If there are any problems with the installation, check the log files to identify the problem.

   > **Note**
   >
   > The location of the log file is defined in the configuration file. For more information, see PingID SSH configuration file parameters.

3. Verify connectivity to the PingID server.

   Choose from:

   - For US accounts:

     ```
     curl -I https://idpxnyl3m.pingidentity.com/pingid/heartbeat
     ```

   - For EU accounts:

     ```
     curl -I https://idpxnyl3m.pingidentity.eu/pingid/heartbeat
     ```

   - For Australian accounts:

     ```
     curl -I https://idpxnyl3m.pingidentity.com.au/pingid/heartbeat
     ```

     The actual host name can be found in the `pingid.properties` file.

4. Confirm that you get a 200 response.

5. If the connection fails, make sure that the outbound connection to host and port `443` are open on your system's firewall.

General troubleshooting

Troubleshooting SSH issues

Most SSH issues can be resolved by rerunning the installation package or reverting to a previous system state.

Steps

1. If you installed from the binary package, and got the following error response, `The method driver /usr/lib/apt/methods/https could not be found from apt-get - install apt-transport-https`, then rerun using the following command: `sudo apt-get install apt-transport-https`
2. If you installed and integrated PingID with SSH, but users are unable to authenticate successfully, revert to the system state prior to the PingID SSH installation.

   Choose from:

   - If your installation is on a physical machine:
   - If you have kept an open session with root permissions, use that session.
   - If you do not have an open session, you must access the machine to open a local root console session.
   - If your installation is a virtual machine (VM), you should open a root console session in the VM control console.

     1. Restore the changed `sshd_config` and `authorized_keys` files, (for PAM, also the `system-auth`, `common-auth` or `pam.conf` files) to their state before the PingID installation, or reverse the entries in the configuration files according to the changes that you applied, depending on your operating system and the PAM or ForceCommand options.
     2. Restart the sshd service:

        For all systems except Solaris, `service sshd restart`

        For Solaris systems: `svcadm restart ssh`

Troubleshooting on Solaris 10

Troubleshooting the PingID SSH installation on Solaris 10

Dealing with problems with Solaris 10.

If you are experiencing problems with Solaris 10, checking the following items may assist.

- Run the **`pkginfo`** command. The output might be helpful to find missing packages and for general investigation of Solaris hosts
- Check the console output and contents of `config.log` file produced during execution of the **`./configure`** script. It plays vital role in investigation of compilation/installation issues
- If you use `opencsw` repository to satisfy requirements of **PingID SSH**, then the **libcurl4**, **libcurl_dev**,**libssl1_0_0**,**libssl_dev**,**libcares_dev**,**librtmp_dev**,**libssh2_dev**,**libkrb5_dev**,**libbrotli_dev** and **openldap_dev** packages are mandatory (this list is far longer than the official requirements due to a bug in curl-config from `opencsw` repository). These libraries can be installed with the command:

  ```
  /opt/csw/bin/pkgutil -y -i libcurl4 libcurl_dev libssl1_0_0 libssl_dev libcares_dev librtmp_dev libssh2_dev libkrb5_dev libbrotli_dev openldap_dev
  ```

- **`curl-config`** allows the **`./configure`** script to locate **libcurl** dependencies and their location, so it is preferable to have the containing directory of **`curl-config`** in the **PATH** (for example, `/opt/csw/bin`). Solaris 11 hosts usually do not require any additional changes in this regard.
- If you use the `opencsw` repository it is preferable to install and use a more modern compiler, than default **GCC** which comes with the operating system. One such compiler can be installed with the **`/opt/csw/bin/pkgutil -y -i gcc5core`** command. Preference to the latter **GCC** over the original one is achieved by setting `/opt/csw/bin` ahead of `/usr/sfw/bin` in the command below:

  ```
  export PATH=/usr/sbin:/usr/bin:/opt/csw/bin:/usr/ccs/bin:/usr/sfw/bin
  ```

- If the **cURL** and **OpenSSL** libraries are installed outside of the default-search-path-for-libraries-during-linking (which are usually `/lib` and `/usr/lib`), then it is preferable to add this path via the LDFLAGS variable when calling the **`./configure`** script. For example, if these libraries are installed into `/opt/csw/lib`, the **`./configure`** command becomes:

  ```
  LDFLAGS="-L/opt/csw/lib"
  ./configure --with-pam --prefix=/usr
  ```

Troubleshooting on HP-UX

Troubleshooting integration with SSH on HP-UX

If you are having trouble with the PingID integration with SSH when using it with PAM, it may be due to the X/Open Networking Interfaces of the version of *libcurl* that is installed. The version of *libcurl* may have been built without the additional flag for X/Open Sockets functionality. (For more information, see the xopen_networking man page.)

To resolve this issue:

1. Remove the version of `libcurl` that was installed with depothelper.
2. Build `libcurl` from the source files:
    1. Install the required libraries:

        ```
        depothelper openldap-2.4.45
        depothelper libssh2
        ```

    2. Download `https://curl.se/download/curl-7.54.1.tar.gz` and copy it to the server.
    3. Unzip the downloaded tarball:

        ```
        /usr/contrib/bin/gunzip curl-7.54.1.tar.gz
        tar xvf curl-7.54.1.tar
        ```

    4. Build `libcurl` and install it to `/usr/local/lib/hpux64`:

        ```
        cd curl-curl-7.54.1
        ./configure CC="cc" CFLAGS="-O -AC99 +DD64" CPPFLAGS="-I/usr/local/include -
        D_XOPEN_SOURCE=600 -D_HPUX_ALT_XOPEN_SOCKET_API" LDFLAGS="+DD64 -Wl,+b -Wl,/usr/local/
        lib/hpux64 -L/usr/local/lib/hpux64" --libdir=/usr/local/lib/hpux64 --disable-dict --
        disable-file --disable-ftp --disable-gopher --disable-imap --disable-manual --disable-
        ntlm-wb --disable-pop3 --disable-rtsp --disable-smb --disable-smtp --disable-sspi --
        disable-telnet --disable-tftp --disable-unix-sockets --without-brotli --without-libidn2
        --without-librtmp
        make
        make install
        ```

3. Build the PingID SSH agent, as described in Installation example for HP-UX.

Integrating PingID with Windows login

PingID integrates with local Windows login and Remote Desktop Protocol (RDP) to provide access permissions only to authorized users and to allow organizations to better secure their Windows server environments and end user Windows machine secured login.

PingID adds policy-based multi-factor authentication (MFA) to the Windows default username and password first factor login flow. Users can carry out MFA on any of the authentication devices paired with their account.

PingID integration for Windows login installs a credential provider on each of the protected Windows machines. The credential provider opens a mini web browser that enables the PingID out-of-the-box authentication flow on the user's local or remote Windows machine. Configure authentication through the PingID credential provider either directly with the PingID service in the cloud or though the PingFederate authentication authority to provide cross-organization authentication policy alignment. PingID integration for Windows login is defined in PingID as a service in the same way that SSH and VPN are considered a service.

Windows platforms and supported versions

PingID integrates with the following Windows platforms, 64-bit versions:

- Microsoft Windows 10 and 11
- Microsoft Windows Server 2016, 2019, and 2022 (desktop)

These platforms are supported with the following architectures:

- RDP:
  - With RDP Network Level Authentication (NLA) configuration or without it
  - RDP architectures, including Web proxy

    > **Note**
    >
    > Per Microsoft design, use of MFA is not permitted in Restricted Admin mode.

  - Use of security keys with RDP are only supported on Windows Server 2022

FIDO2 security keys

Windows login supports FIDO2 security keys with the following limitations: * For registration flows, Windows login doesn't support FIDO2 security keys with enterprise attestation. * PingID for Windows login 2.7 and later doesn't support using FIDO U2F security keys for offline authentication.

Windows Hello

Microsoft does not currently support the addition of second factor authentication when using the Windows Hello biometric login flow.

For PingID for Windows login 2.2 integration and later, if Windows Hello biometric authentication is enabled, users can either:

- Sign on using Windows Hello biometric authentication only.
- Authenticate with their user name and password. When authenticating with user name and password, PingID can be used for second-factor authentication.

Web access information: Domains, URLs, and ports

For details about Windows login web access requirements, see PingID required domains, URLs, and ports.

PingID policy for Windows login flow

Windows login might be subject to PingID policy settings under web authentication policy. For more information, see Enabling a Windows login and RDP authentication policy.

PingID offline MFA

PingID integration for Windows login supports PingID Offline MFA. Offline MFA enables users to sign on to their Windows machine, even if it is offline, such as when on an airplane without Wi-Fi or network connectivity. The following authentication methods are supported:

- PingID mobile app, using a one-time passcode
- FIDO2 security key

> **Note**
>
> Offline MFA is called manual authentication in the PingID End User Guide.

Prerequisites for offline MFA:

- To enable offline authentication with the PingID mobile app, the PingID mobile app must be paired to the user's account, and the user must have signed on to their account in online mode at least once.
- FIDO2 security key is supported by PingID integration for Windows login 2.3 or later on a protected Windows machine.

> **Important**
>
> Repudiation of a user for a login: During offline logins, there are no server side logs, neither for successful nor for unsuccessful authentications. Administrators should make sure to export these logs from the local machine event viewer. For details about the default or customizable log path, see Installing the PingID integration for Windows login using CLI.

Integrating directly with PingID

Integrate PingID with Windows login directly, machine to cloud, in a simple deployment architecture.

Use this option if PingID policy provides sufficient options for your organization's authentication experience and security policies and if your organization does not require advanced cross-organization authentication policies.

The following diagram illustrates the authentication flow when integrating PingID with Windows login directly.

To integrate PingID with Windows login directly, you need a PingID account. Download and install PingID Integration for Windows login on each machine that you want to provide the benefits of multi-factor authentication (MFA) with PingID. See Installing the PingID integration for Windows login.

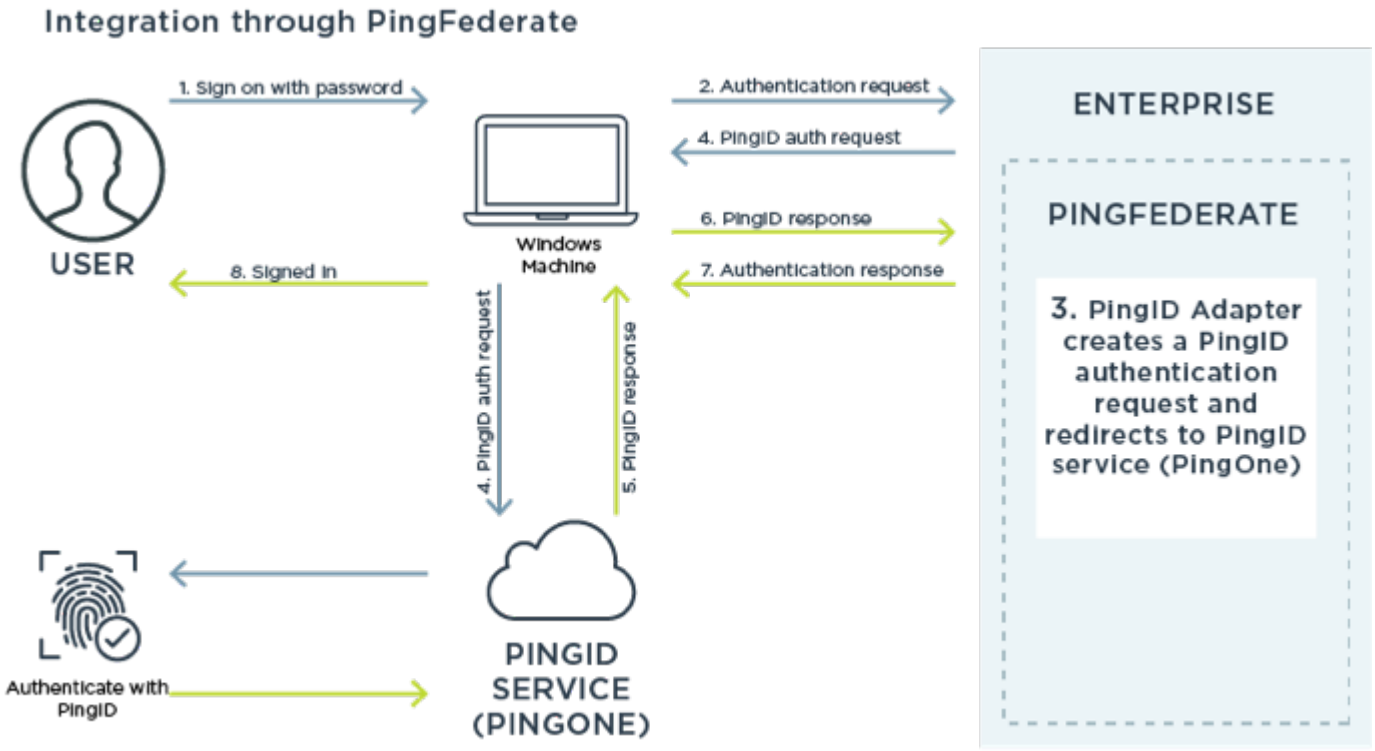
Integrating through PingFederate

Integrate PingID with Windows login through PingFederate authentication authority to streamline your user's authentication experience by leveraging PingFederate's cross-organization authentication policies.

Possible use cases include:

- User name mapping from Windows login. For example, map the sAMAccountName to the User Principal Name (UPN) in your LDAP directory to align the user to a single PingID user identity.
- Creating group-based policies in either PingFederate or PingID.
- Integrating PingFederate orchestrated on-premise or third-party authentication methods into the authentication flow.

The following diagram illustrates the authentication flow when integrating PingID with Windows login through PingFederate.



This section describes how to integrate Windows login with PingID through PingFederate using PingFederate authentication policy. The process includes:

1. Installing the PingID Integration Kit for PingFederate.
2. Configuring a PingID Adapter instance (Windows login).
3. Configuring an authentication policy.

4. Configuring policy contract grant mapping.
5. Configuring access token management.
6. Configuring an OpenID Connect policy (Windows login).
7. Configuring an OpenID Connect client.
8. Installing the PingID integration for Windows login on all relevant Windows machines.

> **Note**
>
> It is also possible to integrate using IdP Adapter mapping. For more information, contact your support representative.

Installing PingID Integration Kit for PingFederate (Windows login)

If your organization wants to integrate PingID for Windows login through PingFederate, you must install the PingID Integration Kit.

Before you begin

Before installing the PingID integration kit for PingFederate:

- Make sure you have an active PingID account.
- Download the PingID properties file (see Managing the PingID properties file).
- Make sure you have installed PingFederate 9.3 or later, with PingID Integration Kit 2.10 or later.
- Make sure you have network access to your PingFederate installation through a secure HTTPS connection.
- Make sure you have administrator permissions in PingFederate.
- Make sure you have a valid TLS certification path for PingFederate.
- Open port 443 from PingFederate to PingOne cloud services. For more information, see PingID required domains, URLs, and ports.
- Offline MFA should not be configured when integrating PingID for Windows login, because offline authentication is managed by Windows.

> **Note**
>
> For general instructions for installing the PingID Integration Kit, see Installing the PingID Integration Kit for PingFederate.

About this task

If you are using PingFederate 9.3 or later, the PingID Integration Kit is bundled as part of PingFederate installation. If you are updating your current version of PingID Integration Kit to a newer version, you must install the integration kit manually, as described in the steps below.

Steps

1. Download and extract the PingID Integration Kit package from the **INTEGRATIONS** section of the PingID download page: https://www.pingidentity.com/en/resources/downloads/pingid.html.

2. Copy the following files from the new `pf-pingid-integration-kit-<version>/pf-pingid-idp-adapter-<version>/dist` directory to the `<pingfederate-installation>/server/default/deploy` directory:
    - `pf-pingid-idp-adapter-<version>.jar`
    - `pingid-web.war`
3. Restart the PingFederate server.
4. If PingFederate is deployed on clustered servers, repeat these steps for all PingFederate nodes.

Configuring a PingID Adapter instance (Windows login)

Configure a PingID Adapter instance when integrating PingID with Windows login through PingFederate.

About this task

- PingID Adapter attributes that are used for offline authentication are not relevant when configuring a PingID Adapter instance for integration with Windows login because the Windows machine determines how to handle authentication requests when the user is offline.
- (Optional) If you want to override the default application name or application icon that the user sees in the PingID mobile app when authenticating, do so in PingFederate. See Identify the target application.

Steps

1. In the PingFederate administrative console:

    Choose from:

    - PingFederate 10.1 and later: Click **Authentication**, and select **IdP Adapters**.
    - PingFederate 10 and earlier: From **Identity Provider** in the **INTEGRATION** section, click **Adapters**.
2. On the **IdP Adapter Instances** window, click **Create New Instance**.
3. On the **Type** tab, enter the following information, and then click **Next**:
    - **Instance Name**: The Adapter name used to identify an adapter instance specific to Windows login (for example, `PingID Adapter for Windows Login Integration`).
    - **Instance ID:** The adapter ID. This ID is for internal use and cannot contain spaces or non-alphanumeric characters.
    - **Type**: From the **Type** list, select the relevant PingID Adapter.
4. Download the Window and Mac login properties file.
5. On the **IdP Adapter** tab, in the PingID `Properties` field, click [.uicontrol] **Choose File** and go to the Windows and Mac login properties file that you downloaded.
6. If you're using LDAP to retrieve user information, click **Show Advanced Fields**, enter the information for the relevant fields, and then click **Save**.

> **Note**
>
> - These attributes are used for a variety of purposes, including pre-populating user details in the registration and backup authentication flows, policy groups, and user name mapping.
> - LDAP attribute fields are case sensitive.

- **LDAP Data Source** (Optional): Select a configured LDAP data store.
- **Query Directory** (Optional): The LDAP query for user information is done for every request. If this option isn't enabled, the query is only made when a PingID user cookie is not found.

  > **Note**
  >
  > If this flag is not enabled, features that rely on LDAP information might not work correctly.

- **Base Domain**: The location that is used to search for the user, including subgroups. This attribute is equivalent to the `Search Base` attribute in Active Directory, such as `Base Domain: CN=Users,DC=domainname,DC=global`.

  > **Note**
  >
  > The `Base Domain` path must include at least one group, as well as the DC.

- **Filter**: LDAP attribute used to find the LDAP entry for a specific user entity. If the **PingID User Attribute** is not defined, the attribute is also used to represent the username in PingID, such as `userPrincipalName=${username}`.
- **LDAP Search Scope**:
  - **OBJECT_SCOPE**: Limits the search to the base object.
  - **ONELEVEL_SCOPE**: Searches the immediate children of a base object, but excludes the base object itself.
  - **SUBTREE_SCOPE** (Default): Searches all child objects as well as the base object.
- **Fname Attribute**: The attribute containing the user first name, such as `givenName`.
- **Lname Attribute**: The attribute containing the user last name, such as `sn`.
- **PingID User Attribute**: The LDAP attribute used to represent the username in PingID, such as `User Principal Name (UPN)`, `sAMAccountName` or `objectGUID`. The value is taken from the user entity identified by the **Filter** attribute. If this field is blank, the **Filter** attribute is used.

  > **Note**
  >
  > This attribute is available in PingID Adapter 2.8 and later.

- **Email Attribute**: The attribute containing the user email address. For example, `mail`. This email address is used during registration if users need to receive a link on their mobile device to download the PingID application.
- **Group Attribute**: The LDAP attribute for group membership.

  > **Note**
  >
  > If you do not provide information for the Group attribute, you will not be able to implement group-based authentication policies for Windows login.

- **Phone Attribute**: The LDAP attribute of the phone number used for SMS messages as well as voice calls if **Voice Number** attribute is left empty.

> **Note**
>
> This attribute must use the Google Library format, which dictates that all phone numbers must include '+', as well as the international country code.

- **Yubikey Attribute**: The LDAP attribute for YubiKey (for future use).
- **Secondary Email Attribute**: A second email address that can be used to verify a user if they don't have a device paired with PingID.
- **Voice Number Attribute**: The LDAP attribute of the phone number used for voice calls. If left empty, the **Phone Attribute** is used for voice calls.

> **Note**
>
> This attribute must use the Google Library format, which dictates that all phone numbers must include '+', as well as the international country code.

- **State Attribute**: This field is not applicable to Windows login and should be left blank.
- **PingID Heartbeat Timeout**: (Optional) Specify how many seconds to wait for a response when verifying the PingID and PingOne services. If not specified, the default is 30 seconds. If set to 0, the system default is used.
- **Authentication During Errors**: For integration with Windows login, therefore, select **Bypass User**, to accept the user's first factor authentication, and allow Windows to manage offline authentication when the PingID multi-factor authentication (MFA) service is unavailable.
- **Users without a paired device**: For integration with Windows login, select **Bypass**: When PingID services are unavailable, bypass the PingID MFA flow, and allow Windows to manage offline authentication when the PingID MFA service is unavailable, and the user does not have a paired device.
- **LDAP Data Source for Devices**: This field is not applicable to Windows login and should be left blank.
- **Encryption Key for Devices**: This field is not applicable to Windows login and should be left blank.
- **Distinguished Name Pattern**: This field is not applicable to Windows login and should be left blank.
- **HTML Template**: This field is not applicable to Windows login and should be left blank.
- **Cookie Duration**: The duration of the cookie (in days) before it expires. The default value is 1 day.
- **PingID Properties File Name**: Ensure the PingID Properties file is unique.

> **Note**
>
> - The PingID properties file name must be unique for each adapter instance. This value is automatically assigned during the adapter configuration process, but when you create a hierarchical adapter configuration it doesn't reset automatically to a unique value.
> - Downloading the PingID for PingFederate properties file provides full permission to perform enrollment, device management, and authentication actions and should only be used with the necessary caution and the guidance of an administrator.

- **Keep cookies at sign-off**: This field is not applicable to Windows login and should be left blank.

  > **Warning**
  >
  > This option prevents a full clean up of the user trace on the machine after single logout (SLO) and might expose your user accounts to additional security risks. This option should only be used with full understanding of the security implications.

- **Refresh UserId Cookie**: Refresh UserId cookie after a successful authentication. By default this option is unchecked.

- **Require PingID Registration**: (Relevant only when using Integrate PingID withPingFederate properties file) If the checkbox is selected, users that do not have at least one device paired with their account are blocked until they successfully pair a device with their account.

  > **Note**
  >
  > Use of the PingID withPingFederate properties file is not recommended. However if you choose to use it, this option is required to maintain optimum security levels. For a more comprehensive list of properties files available see Managing the PingID properties file.

7. **Optional:** On the **Extended Contract** tab, to add attributes to the contract, for each attribute you want to add, in the**Extend the Contract** area, type the name of the attribute and click **Add**, and when finished, click **Next**.

   > **Note**
   >
   > For more information on using the **Extended Contract** tab, see Extend an IdP Adapter Contract.

8. On the**Adapter Attributes** tab in the **Pseudonym** column, select the checkbox for the subject attribute to be used as the expected identifier, then click **Next**.

   > **Note**
   >
   > On the**Adapter Attributes** tab you also have the option to mask attribute values in PingFederate log files. For more information, see Attribute masking.

9. On the **Adapter Contract Mapping** tab, click **Configure Adapter Contract** and then in the **Adapter Contract Mapping** window:

   1. Click **Next**, and then in the **Adapter Contract Fulfillment** tab, for each contract attribute, select the relevant **Source** value with which to fulfill your adapter contract.

10. Click **Next**, and then in the **Issuance Criteria** tab, click **Next**.

11. In the **Summary** tab, verify the information is correct and then click **Done**.

12. In the **Create Adapter Instance** window, click **Next**, and then click **Done**

13. Click **Save**.

    Result:

    The new adapter instance is saved.

Configuring an authentication policy

To use PingID as an authentication solution for Windows login with PingFederate, create an authentication policy contract and an authentication policy in PingFederate.

About this task
Steps

1. In PingFederate, create an authentication policy contract:.

   For more information, see Policy Contracts.

   1. Go to Policy Contracts:
      - PingFederate 10.1 or later: Go to **Authentication → Policies → Policy Contracts**.
      - PingFederate 10 or earlier: On the **Identity Provider** tab, in the **Authentication Policies** section, click **Policy Contracts**.
   2. Click **Create New Contract**.
   3. In the**Contract Name** field, enter a meaningful name for the Windows login policy contract, and click **Next**.
   4. In the **Contract Attributes** tab, for each attribute you want to add, in the**Extend the Contract** area, type the name of the attribute and then click **Add**. The **subject**, and **winlogin.auth.response**, attributes must be included.
   5. Click **Next**, and then click **Save**.

2. Create a PingFederate authentication policy for Windows login authentication:

   For more information, see Policies.

   1. Go to Authentication Policies:
      - PingFederate 10.1 or later: Go to **Authentication → Policies**.
      - PingFederate 10 or earlier: On the **Identity Provider** tab, in the **Authentication Policies** section, click **Policies**.
   2. In the **Policies** tab:
   3. ensure the**IdP Authentication Policies** check box is selected, and then click **Add Policy**.
   4. In the **Name** field, enter a meaningful name for the Windows login authentication policy.
   5. From the **Policy** list, select **IdP Adapters** and then select the PingID Adapter instance for Windows that you created earlier. A branch is added to the PingFederate policy tree, and **Fail** and **Success** fields are added.
   6. In the **FAIL** field, click **Done**.
   7. In the **Success** field, select **Policy Contract** and then select the policy contract you created earlier.
   8. Under the PingID Adapter **Success** field, click **Contract Mapping**, and then click **Next**.

9. In the **Contract Fulfillment** tab:
    1. In the Adapter Contract **subject** row, in the **Source** field, select the PingID Adapter you created for Windows login, and in the **Value** field, select **subject**.
    2. In the **winlogin.auth.response** row, in the **Source** field select the PingID Adapter you created for Windows login, and in the **Value** field, select **winlogin.auth.response**.
    3. Click **Next**, and in the **Issuance Criteria** tab, click **Next**.
    4. In the **Summary** tab, click **Done**.
10. In the **Policy** window, click **Done**.

    Result:

    The PingFederate authentication policy is saved.

Configuring policy contract grant mapping

Configure policy contract grant mapping for the PingFederate integration.

About this task

Manage the mappings from the authentication policy contract you created into the persistent grant contract.

Steps

1. In PingFederate, configure policy contract grant mapping.

   For more information, see Grant mapping.

   Choose from:

   - PingFederate 10.1 or later: Click **Authentication → OAuth**
   - PingFederate 10 or earlier: In the **OAuth Server** tab, **Grant Mapping** area, click **Authentication Policy Contract Mappings**.

2. In the **Policy Contract Mapping** window:
    1. In the **Policy Contract** field, select the authentication policy contract you created earlier and then click **Add Mapping**.
    2. On the **Attribute Sources & User Lookup** tab, click **Next**.
    3. On the **Contract Fulfillment** tab, enter the following and then click **Next**:
        - From the **USER_KEY** source list, select **Authentication Policy Contract**, and in the **Value** field, select **subject**.
        - From the **USER_NAME** source list, select **Authentication Policy Contract**, and in the **Value** field, select **subject**.
    4. On the **Issuance Criteria** tab, click **Next**, and then on the **Summary** tab, click **Save**.

       Result:

The new policy grant mapping is shown in the **Mappings** list.

Configuring access token management

The OpenID Connect (OIDC) response needs to include an access token.

About this task

To create an access token:

- Configure an access token management instance.
- Create the relevant access token mappings.

Steps

1. In PingFederate, create an Access Token Management Instance:

   Choose from:

   - PingFederate 10.1 or later: Go to **Applications → OAuth** and then click **Access Token Management**
   - PingFederate 10 or earlier: On the **OAuth Server** tab, in the **Token Mapping** section, click **Access Token Management**

2. Click **Create New Instance** and then on the **Type** tab, enter the following information, and then click **Next**:
   - **Instance Name**: The name you want to use to identify the Access Token Management instance.
   - **Instance ID:** The Access Token Management ID. This ID is for internal use and cannot contain spaces or non-alphanumeric characters.
   - **Type**: From the **Type** list, select **JSON Web Tokens**.
3. On the **Instance Configuration**tab, do the following:
   1. Click **Add a new row to 'Symmetric Keys'** and in the new row enter the following information and then click **Update**
      - **Key ID**: Enter a unique identifier for the key.
      - **Key**: Enter the encoded symmetrical key. You can find this in the `use_base64_key` attribute in the PingID Properties file that you used to create the PingID Adapter instance earlier.
      - **Encoding**: From the **Encoding** list, select **Base64[url]**.
   2. In the**JWS Algorithm** field, select **HMAC using SHA-256** as the signing algorithm you want to use to protect the integrity of the token.
   3. In the **Active Symmetric Key ID** field, select the new symmetric key that you created, and then click **Next**.
4. On the **Session Validation** tab, click **Next**

5. On the **Access Token Attribute Contract** tab:
    1. In the **Extend the Contract** field, add the following attributes and then click **Add**:
        - **subject**
        - **winlogin.auth.response**
    2. From the **Subject Attribute Name** list, select **subject**, and then click **Next**.
6. On the **Resource URIs** tab, click **Next**.
7. On the**Access Control** tab, click **Next**.
8. On the **Summary** tab, click **Save**.
9. Go to the **Access Token Mappings** window:
    1. Do the following:
        - PingFederate 10.1 or later: Go to **Applications → OAuth** and then click **Access Token Mappings**.
        - PingFederate 10 or earlier: On the **OAuth Server** tab, in the **Token Mapping** section, click **Access Token Mappings**.
    2. From the **Context** list, select the Windows login authentication policy contract that you created earlier.
    3. From the **Access Token Manager** list, select the access token manager instance that you created earlier, and click **Add Mapping**.
    4. On the **Attribute Sources & User Lookup** tab, click **Next**.
    5. On the **Contract Fulfillment** tab, do the following and then click **Next**:
        - In the **subject** row: In the **Source** field, select **Authentication Policy Contract**, and in the **Value** field, select **subject**.
        - In the **winlogin.auth.response** row: In the **Source** field, select **Authentication Policy Contract**, and in the **Value** field, select **winlogin.auth.response**.
    6. On the **Issuance Criteria** tab, click **Next**.
    7. On the **Summary** tab, click **Save**.

       Result:

       The Access Token Mappings are saved

Configuring an OpenID Connect policy (Windows login)

Create an OpenID Connect policy, and then map the policy to the specific OAuth client.

About this task

Steps

1. In PingFederate, before creating a policy, make sure an Open ID Connect (OIDC) scope is defined:
    1. In PingFederate, go to Scope Management:
        - PingFederate 10.1 or later: Go to **System → OAuth Settings** and then click **Scope Management**.
        - PingFederate 10 or earlier: On the **OAuth Server** tab, in the **Authorization Server** section, click **Scope Management**.
    2. Create an OpenID Connect scope:
        1. In the **Scope Value** field, type `openid`.
        2. In the **Scope Description** field, type `OpenID Connect login`.
        3. Click **Add**, and then click **Save**.

            Result:

            The new scope is added to the Common Scopes list, and the entry is saved.
2. In PingFederate, create an OpenID connect policy:
    1. Go to OpenID Connect Policy Management:
        - PingFederate 10.1 or later: Go to **Applications → OAuth** and then click **OpenID Connect Policy Management**.
        - PingFederate 10 or earlier: On the **OAuth Server** tab, in the **Token Mapping** section, click **OpenID Connect Policy Management**.
    2. Click **Add Policy**.
    3. In the **Manage Policy** tab, enter the following:
        - **Policy ID**: Enter a unique ID for the policy.
        - **Name**: Enter a name for the policy.
        - **Access Token Manager**: Select the access token manager that you created earlier from the drop-down list.
        - Select the **Include User Info in ID Token** check box.
    4. Click **Next**.
    5. On the **Attribute Contract**tab, in the **Extend the Contract** section, for each attribute listed, click **Delete** in the relevant row, until all attributes are deleted.
    6. In a new row, enter `winlogin.auth.response`, and click **Add**.

        Result:

        The new attribute is added to the **Extend the Contract**list.
    7. Click **Next**.

8. In the **Attribute Scopes** tab, make an association between the OpenID scope, and the `winlogin.auth.response` attribute:
    - In the **Scope** column, select **Open ID** from the drop-down list.
    - In the **Attributes** column, select the `winlogin.auth.response` check box and then click **Add**.
9. Click **Next**, and then on the **Attribute Sources & User Lookup** tab, click **Next**.
10. In the **Contract Fulfillment** tab:
    - `sub` attribute: From the **Source** list, select **Access Token**. From the **Value** list, select **subject**.
    - `winlogin.auth.response` attribute: From the **Source** list select **Access Token**. From the **Value** list, select `winlogin.auth.response`.
11. Click **Next**, and on the**Issuance Criteria** tab, click **Next**.
12. On the **Summary** tab click **Save**.

    Result:

    The new OpenID Connect policy is listed in the**OpenID Connect Policy Management**window.

3. If more than one policy exists, click **Default** to make this policy your default policy.

Configuring an OpenID Connect client

Define an OpenID Connect (OIDC) client for the Windows login integration.

About this task
Steps

1. In PingFederate, create a new OpenID Connect client:

   Choose from:

   - PingFederate 10.1 or later: Go to **Applications → OAuth → Clients**, and then click **Add Client**.
   - PingFederate 10 or earlier: On the**OAuth Server** tab, in the **Clients** section, click**Create New**.
2. In the **Client** window, fill in the following fields:
    1. **Client ID** (required): Enter the Windows login OIDC client ID `winlogin_oidc_client`.
    2. **Name**: Enter a unique name for the Windows login OIDC client.
    3. **Redirect URIs** (required): Enter the following URL, and then click **Add**.

       ```
       winlogin.pingone.com://callbackauth
       ```

    4. In the **Bypass Authorization Approval** field, select the **Bypass** check box.
    5. In the **Allow Grant Types** area, select the **Authorization Code** check box.

6. (Required) In the**Open ID Connect** section, from the **Policy** list, select the OpenID Connect policy that you created earlier.

3. Click **Save**.

   Result:

   The new client appears in the **Clients** list, and enabled by default.

Installing the PingID integration for Windows login

Install PingID integration for Windows login using the UI wizard or using the command-line interface (CLI).

For large scale deployments of PingID Integration for Windows login, use a deployment management platform for automatic distribution and update, such as Microsoft System Center Configuration Manager (SCCM).

> **Note**
>
> There are a number of references to the PingID properties file (`pingid.properties`) in the installation instructions below. Keep in mind that this refers to the more limited properties file that is generated with the button in the **Integrate with Windows login** section.
> Do not use the properties file that is generated with the button in the **Integrate with PingFederate and other clients** section.

For a list of prerequisites before installing PingID integration for Windows login, see Prerequisites for installing PingID integration for Windows login.

If you are installing PingID integration for Windows login through PingFederate, make sure you have completed all steps in Integrating through PingFederate.

You can install the PingID integration for Windows login in two ways:

- Installing the PingID integration for Windows login using UI wizard
- Installing the PingID integration for Windows login using CLI

Prerequisites for installing PingID integration for Windows login

The PingID integration for Windows login should be installed individually on each Windows machine requiring the PingID authentication service.

If you are installing PingID integration for Windows login through PingFederate, make sure you have completed all steps in Integrating through PingFederate before installing PingID integration for Windows login on the Windows machine.

Adding any multi-factor authentication (MFA) is a procedure that carries the risk of being locked out of the machine. Before proceeding with the installation, consider the following:

- If third party Credential Providers are in use on the target machine or server, you should remove them manually before installing the PingID integration for Windows login. You should also only test compatibility between various Credential Providers on lab machines that do not hold important information.
- Several verifications are done on the parameters supplied for the installation, to minimize any locking. The PingID integration for Windows login permits recovery from a lockout scenario, by restarting the machine in safe mode.

- To avoid restarting the machine due to lockout, keep an open session with admin permissions.
- Restart the machine on successful completion of the installation process.
  - For the UI wizard: The UI installation wizard prompts the installer to restart (default). Admins can select the option to defer the restart.
  - For the CLI: By default, on completion of a successful installation through the CLI, the machine automatically restarts. Admins can add the command line option `/NORESTART` to prevent the automatic restart.

The installation of PingID requires the following prerequisites:

- Administrator privileges on the target Windows machine.
- An active internet connection on the target Windows machine.
- A copy of the organization's `pingid.properties` file (generated with the button in the **Integrate with Windows login** section). For more information on the properties file, see Managing the PingID properties file.

Installing the PingID integration for Windows login using UI wizard

Before you begin

> **Important**
>
> Adding multi-factor authentication (MFA) is a procedure that carries the risk of being locked out of the machine. See Prerequisites for installing PingID integration for Windows login before proceeding.

About this task

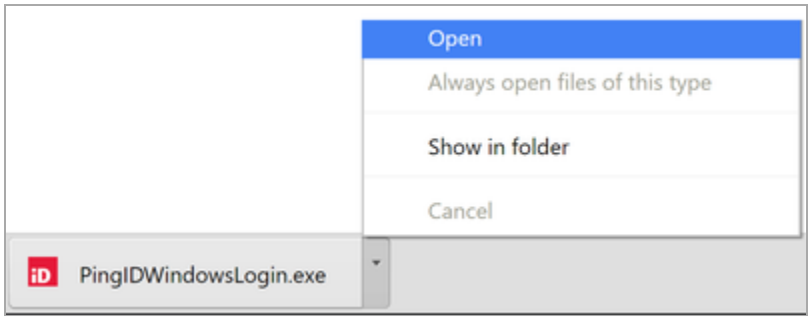
To install the PingID integration for Windows login using the UI wizard:

Steps

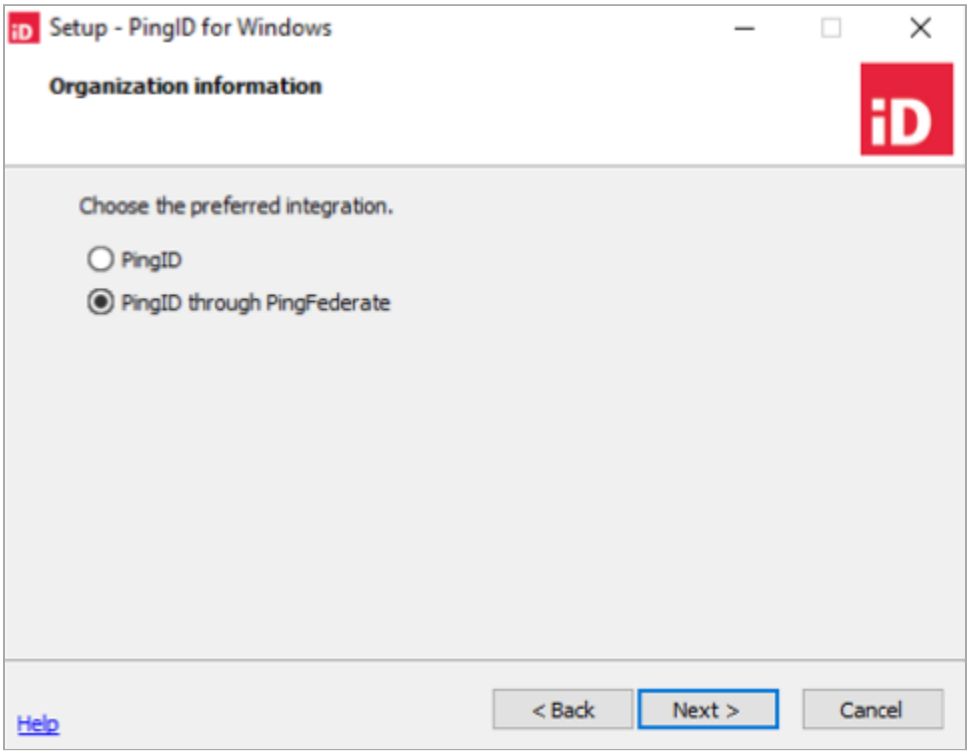
1. On the PingID Downloads page, go to **Integrations**, and download and extract PingID for Windows login.

   > **Note**
   >
   > If your version of Windows login is more than two versions behind the current version listed on the downloads page, you must uninstall your current version of PingID for Windows login before you install the new version.

2. Double-click the `PingIDWindowsLogin<version>.exe` file to launch the setup wizard, and then click **Next**.



3. Review the Software License Agreement, click **I accept the agreement**, and then click **Next**.



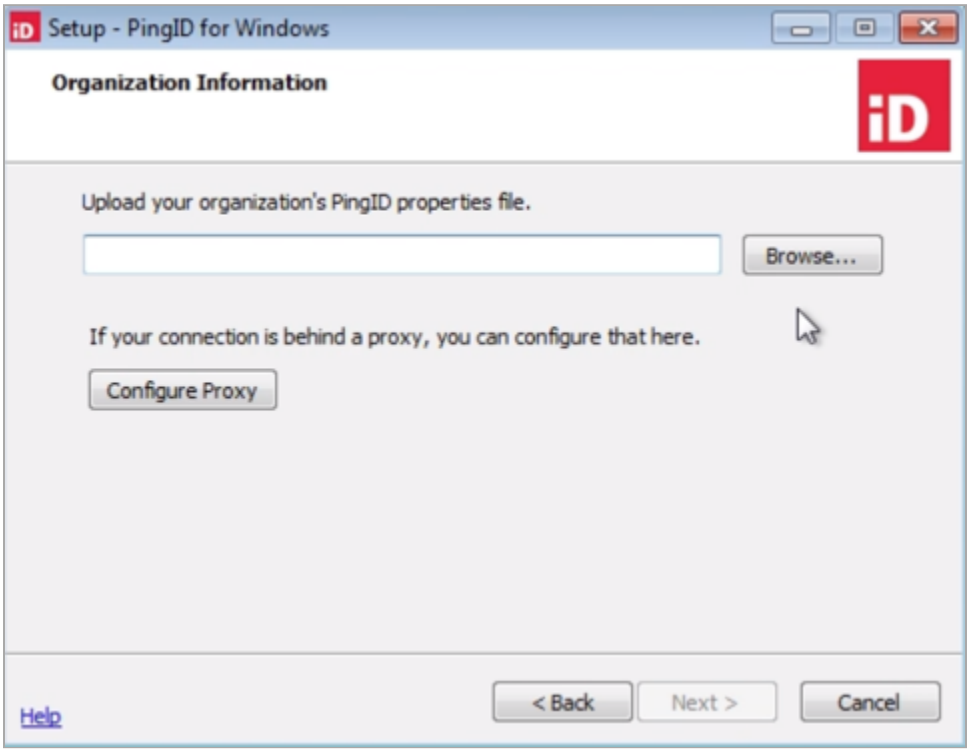
4. In the **Organization Information** window, select either:

   Choose from:

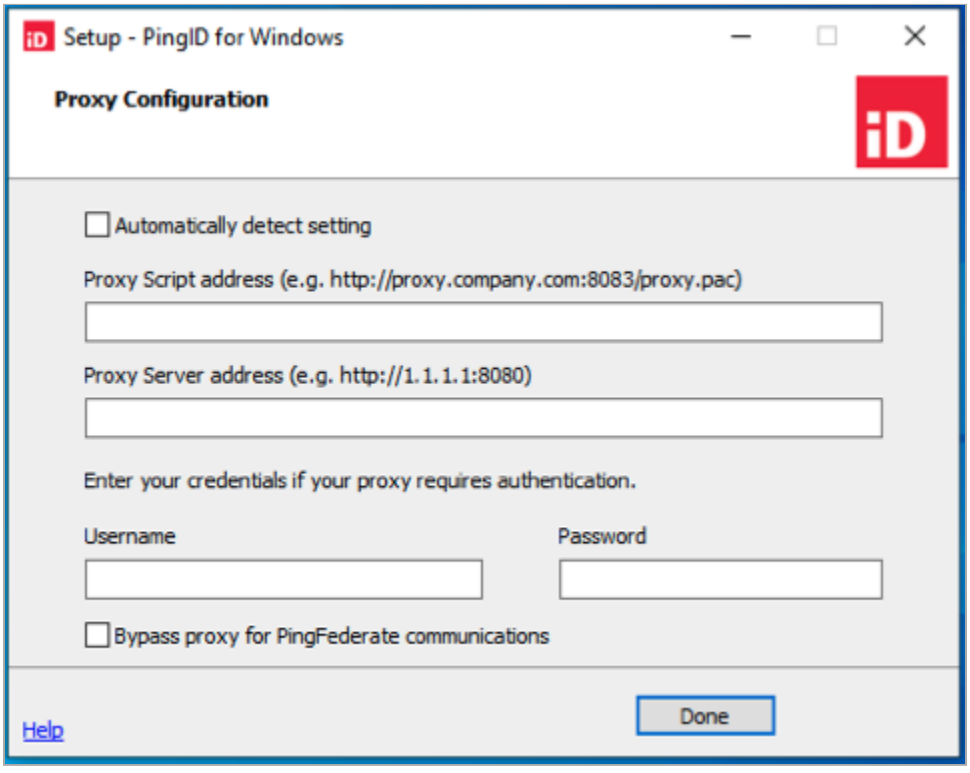
   - **PingID**: Integrate PingID directly with Windows login.
   - **PingID through PingFederate**: Integrate PingID with Windows login through PingFederate.

5. In the **Organization Information** window, click **Browse**, and then select the `pingid.properties` file that you want to use.

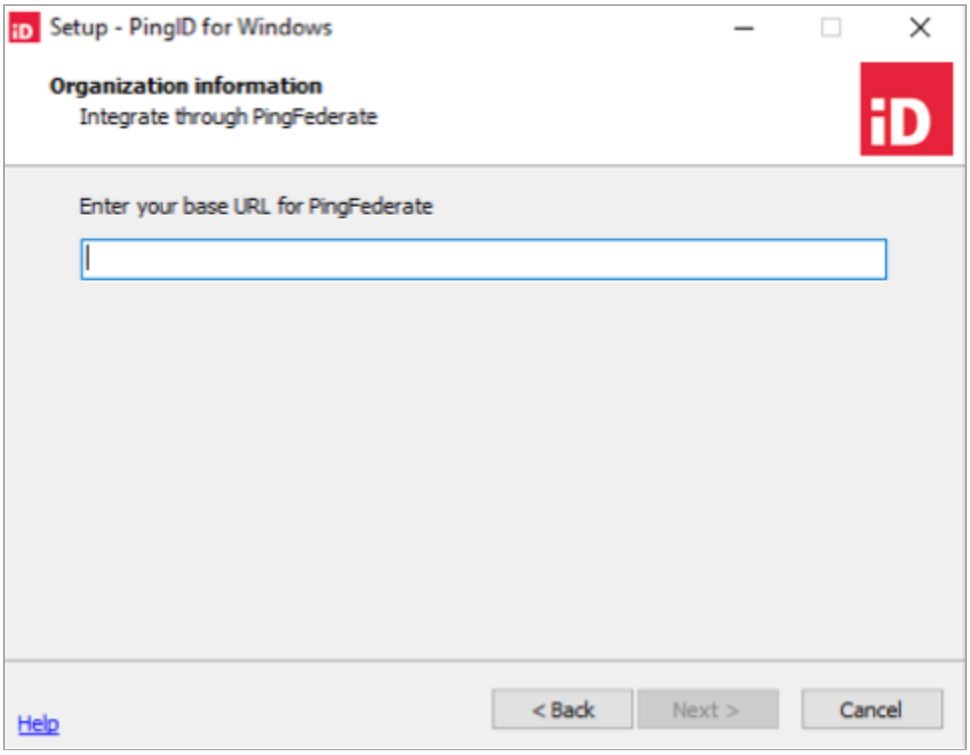
> **Note**
>
> When integrating with PingFederate, for security reasons it is recommended that you use the `Windows and Mac login PingID properties file` in both the PingID Adapter, and in the Windows Login installation.



6. If your connection is behind a proxy: click **Configure Proxy** and then configure the options relevant for your proxy. If you prefer to have the communication with PingFederate not go through the proxy, click the **Bypass proxy for PingFederate communications** check box.



7. For PingID through PingFederate integration only: In the **base URL** field, enter the PingFederate base URL, and then click **Next**.



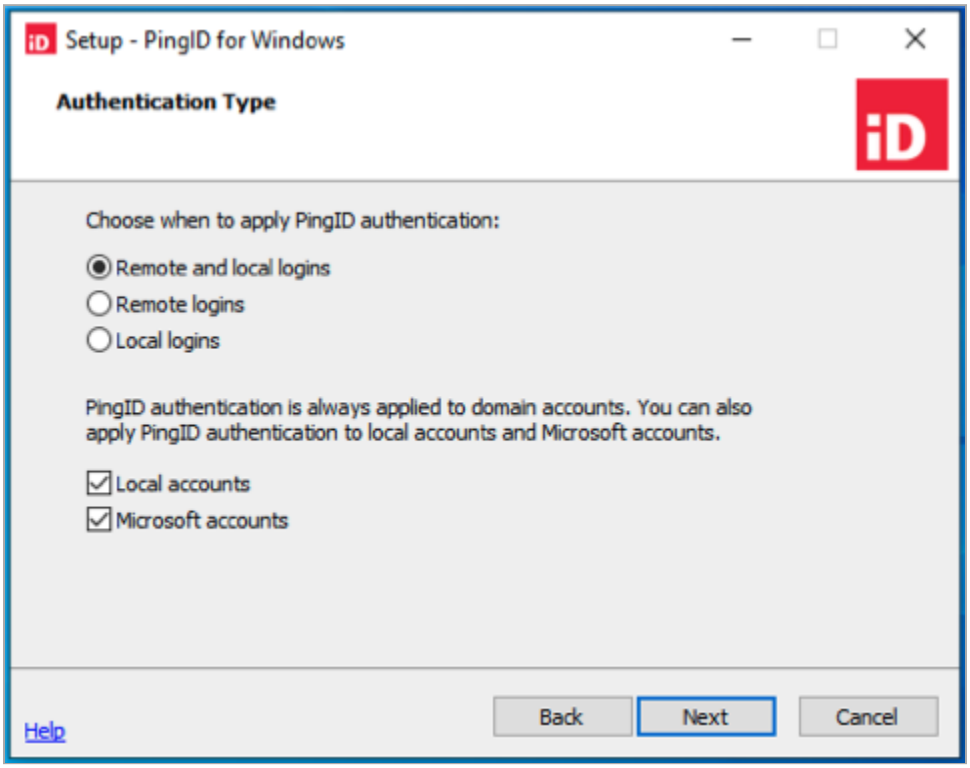
8. In the **Authentication Type** window:

    1. Select when you want to apply PingID authentication. Choose from:

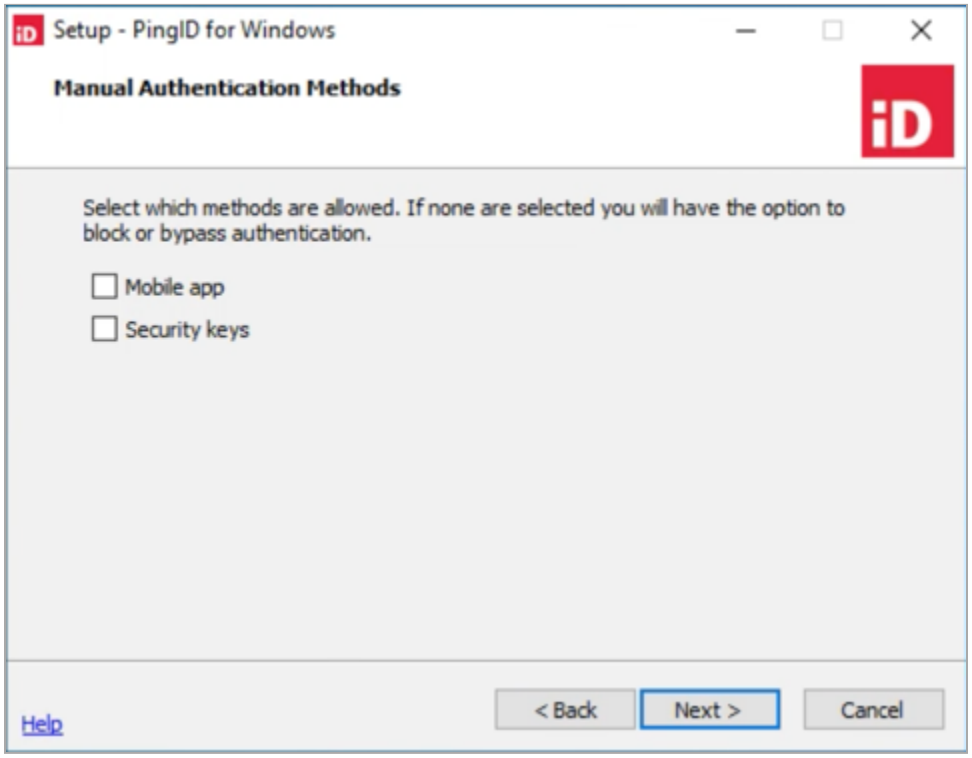
        - **Remote and local login**: Users are required to authenticate with PingID when connecting to Windows login locally or remotely.
        - **Remote logins**: Users connecting to the Windows login machine remotely are required to authenticate with PingID. Users bypass PingID authentication when logging in locally.
        - **Local logins**: Users connecting to the Windows login machine locally are required to authenticate with PingID. Users bypass PingID authentication when signing on remotely.

    2. (Optional) Select the relevant check box to apply PingID to **Local accounts**, **Microsoft accounts**, or both.

        - **Local accounts**: User accounts that are stored on the local machine.
        - **Microsoft accounts**: Microsoft account used to access Microsoft devices and services associated with a specific user. For example, `johndoe@outlook.com`. The PingID integration for Windows recognizes all types of Microsoft accounts.



3. Click **Next**. The **Manual Authentication Methods** window is displayed.



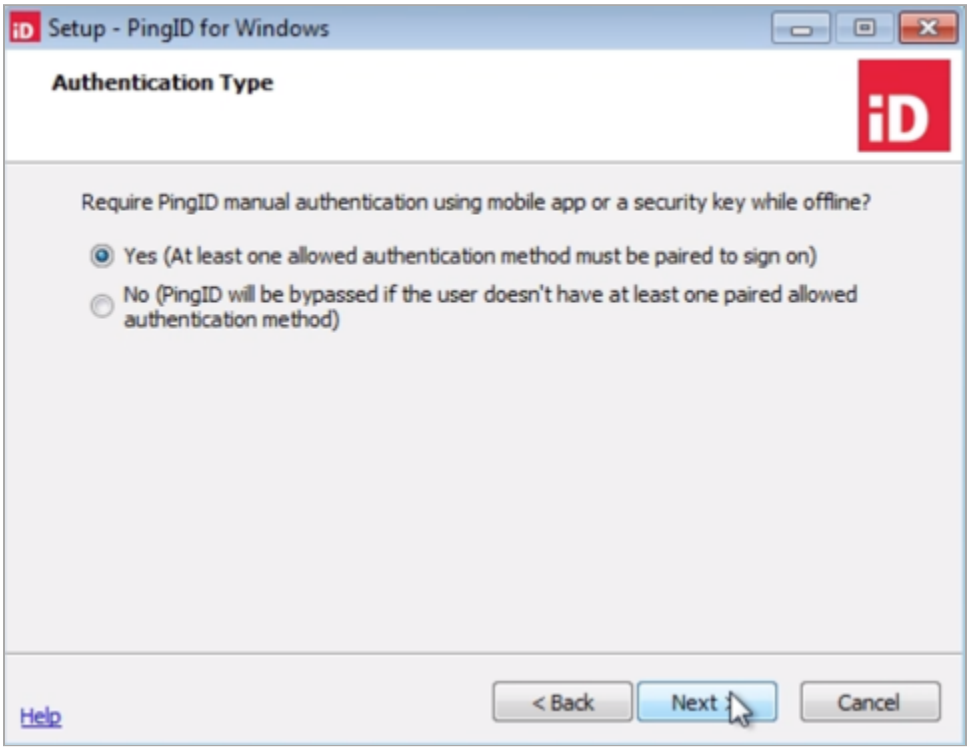
9. If PingID server is unavailable or the user is offline, for example, the connection with the PingID server can't be verified at the time of sign on, either enable or disable manual authentication:

Choose from:

- Enable manual authentication:

    1. In the **Manual Authentication Methods** window, select at least one manual authentication method and then click **Next**. The **Authentication Type** window displays offline authentication options.
    2. In the **Authentication Type** window, select whether to use PingID offline MFA or allow the user to bypass PingID MFA if the user is offline, such as no internet connection. Select one of the following and then click **Next**:

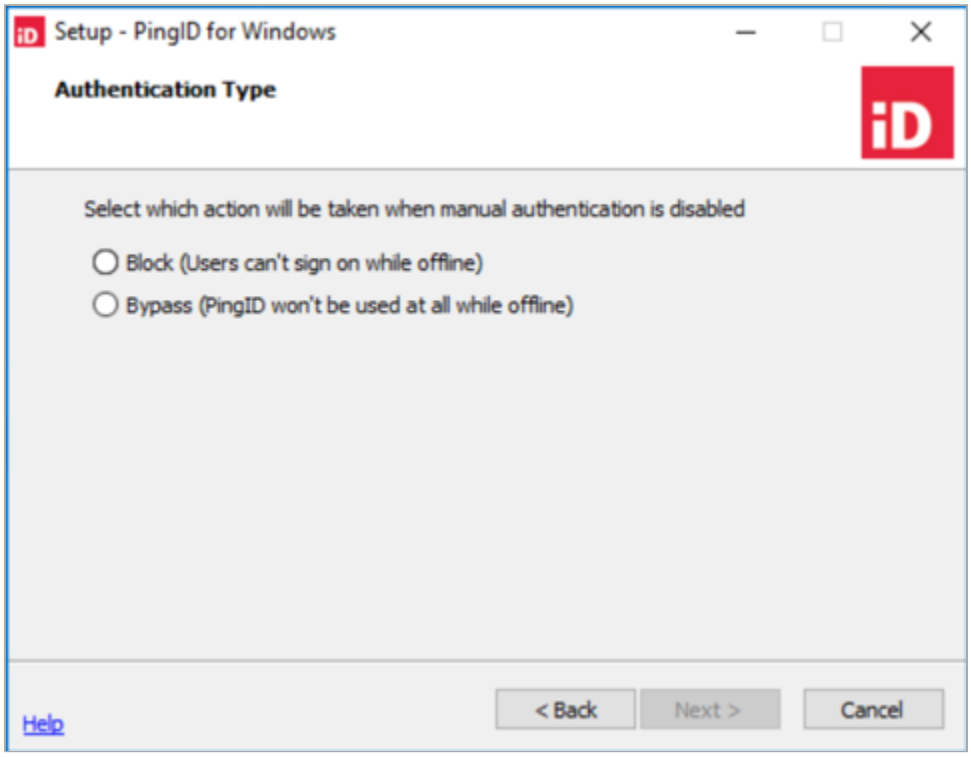
        - **Yes**: The user is prompted to authenticate through the manual (offline) authentication flow. At least one offline authentication method must be paired for the user to authenticate, otherwise the user is blocked.
        - **No**: If the user does not have at least one offline authentication method paired with their account, PingID bypasses MFA during sign on.



- Disable manual authentication and define behavior when the PingID server is offline:

    1. In the **Manual Authentication Methods** window, leave all check boxes cleared and click **Next**. The **Offline Authentication** page displays a list of options when the user is offline.
    2. In the **Authentication Type** window, select one of the following, and then click **Next**:

        - **Block**: The user cannot sign on while offline.
        - **Bypass**: Bypass MFA with PingID, allowing user to complete sign on.



> **Note**
>
> - The PingID offline MFA feature is available from PingID integration for Windows login 2.0 or later, with a paired mobile device using PingID mobile app 1.8+.
> - Pairing and use of a security key for offline authentication requires PingID integration for Windows login 2.3 or later. If using PingID integration for Windows login 2.2 or earlier, security key for offline authentication is not permitted, and the flow is different.

10. In the **PingID Username Mapping** window:
    1. In the **Legacy username parsing convention** field:
       - Specify your organization's default domain. Domain format should be:
         - `@domainname`, such as `@somewhere.com`.
         - Maximum of 50 characters.
         - The string entered in this field is appended to the username during sign on.

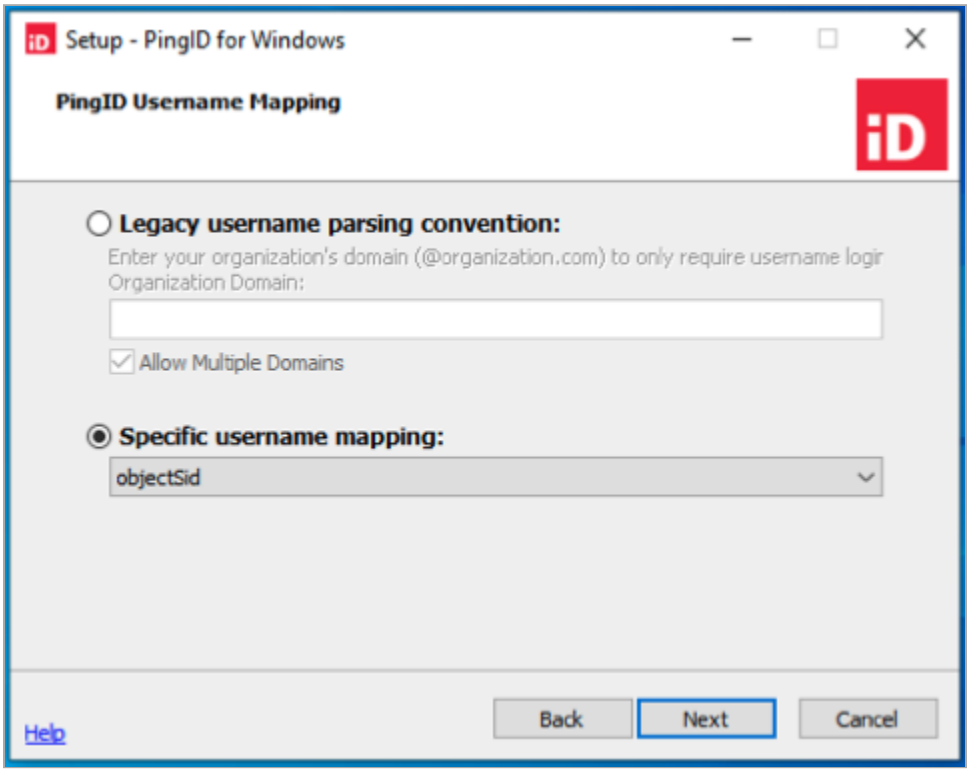
           If specified, users can enter their username, such as `jsmith`, rather than entering full user and domain name, as in `jsmith@pingidentity.com`.

> **Note**
>
> - If you select this option without providing a default domain, the SAMAccountName is used.
> - This option is not recommended in environments with multiple domains, or environments where PingID is also used to sign on locally.

- (Optional) Select **Allow Multiple Domains** to allow the user to sign on from any domain in addition to the default domain. If the user specifies a domain, that domain is used, otherwise the default domain is used. This option is available with PingID for Windows login 2.2 and higher.

> **Note**
>
> - Do not use this option if you did not specify a default domain in the **Legacy username parsing convention** field.
> - If you selected **Allow Multiple Domains**, users should use only the UserPrincipalName format (and not the samAccountName).
> - If you applied PingID authentication to local or Microsoft accounts, the recommended username mapping is objectSID.

2. In the **Specific username mapping** field, select the attribute that you want to use to verify the user account.



Examples showing how the username is mapped in PingID:

- **objectSid**: Use the object SID.

```
S-1-5-21-668608636-2615149724-2645577550-1111
```

- **userPrincipalName**: Use the userPrincipalName.

```
jsmith@domain.com
```

- **sAMAccountName (DOMAIN\UserName)**: Use the Domain Name as prefix, or the computer name when logged in locally, and then the SAM Account Name.

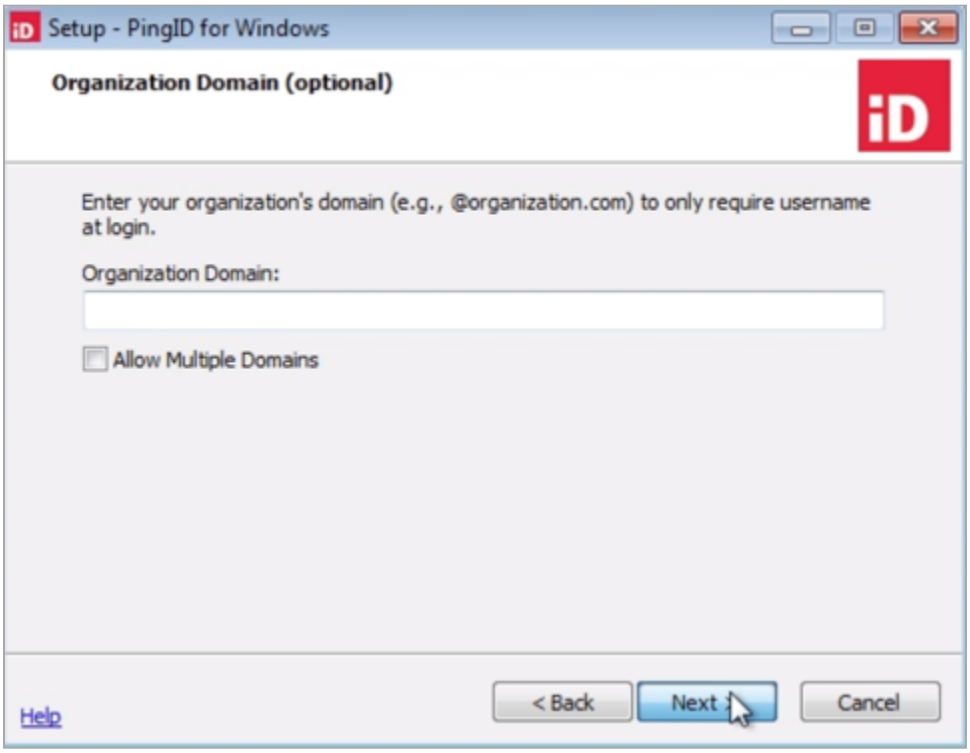
```
DOMAIN\jsmith
```

- **sAMAccountName (UserName only)**: Use only the SAM Account Name.

```
jsmith
```

> **Note**
>
> For security reasons, when using Windows login in a multiple domain environment, it is recommended that you use specific username mapping rather than the legacy username parsing convention.

3. Click **Next**.



11. In version 2.8 of the Windows login integration, an improved implementation was introduced for the use of security keys while offline. If the installation program detects security keys that were paired prior to this change, you are presented with the following options:
    - Allow: Allow users to continue using these keys (this option is not recommended)
    - Inform: Allow users to continue using these keys, but inform them that these keys should be manually deleted

- Delete: Automatically delete the keys that were paired before the change was introduced

12. To select the folder in which to install PingID, click **Browse**, select the destination folder or accept the default, and click **Next**.
13. Click **Install**.
14. When the installation is complete, click **Yes** to restart the computer and apply the changes.

The next time the user signs on to the Windows machine, they will need to authenticate with PingID.

15. Delete the downloaded `pingid.properties` file after the installation has completed.

> **Note**
>
> The `OrgData1`, `OrgData2`, ... fields in the `HKEY_LOCAL_MACHINE\SOFTWARE\Ping Identity\PingId\PingIdCredProv` registry are encrypted and should not be edited.

16. To verify the installation was successful, test that the user can sign on to the Windows machine using their password and PingID MFA.

Installing the PingID integration for Windows login using CLI

Install PingID integration for Windows login through the command-line interface (CLI).

Before you begin

> **Important**
>
> Adding any multi-factor authentication (MFA) method is a procedure that carries the risk of being locked out of the machine. See Prerequisites for installing PingID integration for Windows login before proceeding.

About this task

Running the installer program for PingID integration for Windows login from the command line is useful for deploying to multiple machines in batch mode.

Steps

1. On the PingID Downloads page, go to **Integrations**, and download and extract PingID for Windows login.
2. Using the parameters table below, from the **Command Prompt**, create a `.bat` or `.cmd` file containing the command for the PingID integration for Windows with the parameters you require. Alternatively, run the installer directly from the command prompt for a list of parameters.

   > **Note**
   >
   > To integrate PingID integration for Windows login through PingFederate, you must include the `/PingFedAddress=` <*baseurl*> parameter.

   Choose from:

   - Install using the `pingid.properties` file to supply parameter values.

     ```
     <Full filepath of the installer for PingID integration for Windows>\PingIDWindowsLogin_<ver>.exe
     /SILENT /VERYSILENT /SUPPRESSMSGBOXES /SP- /LOG=<Full output log filepath>  /
     orgSettingsFilePath= <Full pingid.properties filepath> /OfflineAuthType /OfflinePolicy  <[Optional
     parameters]>
     ```

   - Install without using the `pingid.properties` file and supply the `/orgAlias`, `/orgKey`, `/authenticatorAddress`, `/idpUrl`, and `/token` parameter values on the command line.

     ```
     <Full filepath of the installer for PingID integration for Windows>\PingIDWindowsLogin_<ver>.exe
     /VERYSILENT /SUPPRESSMSGBOXES /SP- /LOG=<Full output log filepath>  /orgAlias=<organization's
     alias string>
     /orgKey=<organization's key string>  /authenticatorAddress=<URL of PingID data center>  /
     idpUrl=<URL of server used for PingID API requests>  /token=<API key identifier>  /
     OfflineAuthType /OfflinePolicy  <[Optional parameters]>
     ```

     Example:

     ```
     C:\Users\Admin\Downloads\PingIDWindowsLogin_28.exe  /VERYSILENT /SUPPRESSMSGBOXES
     /SP- /LOG=C:\Users\Admin\Temp\Logs\PingIDWindowsLogin.log  /orgSettingsFilePath=C:
     \Users\Admin\Downloads\pingid.properties
     /OfflineAuthType=3 /OfflinePolicy=0 /NORESTART
     ```

     This example instructs the installer to configure the PingID integration for Windows login, with the following settings:

   - Run the installer executable, located in the `Downloads` folder.
   - Do not display the background window and installation progress window (`/VERYSILENT` parameter).
   - Do not display message boxes and prompts (`/SUPPRESSMSGBOXES` and `/SP-` parameters).

- Retrieve settings from the organization's `pingid.properties` file, located in the `Downloads` folder (`/orgSettingsFilePath` parameter).
- Send the log output to a customized destination (`/LOG` parameter).
- Allow PingID Mobile App and FIDO2 security key for offline (manual) authentication `(/OfflineAuthType` parameter). At least one manual authentication type must be paired for the user to authenticate (`/OfflinePolicy` parameter).
- Do not automatically restart the machine at the end of the installation process (`/NORESTART` parameter).

The command-line parameters are described in the following table.

Parameter	Description
`/SILENT`	If a restart is necessary and the `/NORESTART` command isn't used, it prompts with a `Reboot now?` message box. When using this parameter, the installation progress window is displayed.
`/VERYSILENT`	If a restart is necessary and the `/NORESTART` command isn't used (see below), it reboots without asking. When using this parameter, the installation progress window is not displayed.
`/SP-`	Disables the `This will install… Do you wish to continue?` prompt at the beginning of the installation.
`/SUPPRESSMSGBOXES`	Instructs the installer to suppress message boxes. It only has an effect when combined with `/SILENT` or `/VERYSILENT`. The default response in situations where there's a choice is: ■ `Yes` in `Keep newer file?` situations. ■ `No` in `File exists, confirm overwrite` situations. ■ `Abort` in `Abort/Retry` situations. ■ `Cancel` in `Retry/Cancel` situations. ■ `Yes` (continue) in `DiskSpaceWarning, DirExists, DirDoesntExist, NoUninstallWarning, ExitSetupMessage,` and `ConfirmUninstall` situations. ■ `Yes` (restart) in `FinishedRestartMessage` and `UninstalledAndNeedsRestart` situations.
`/LOG` = `<Full output log filepath>`	■ `/LOG` without an assigned value causes the installer to create a log file in the user's `TEMP` directory, detailing file installation and actions taken during the installation process. ■ `/LOG` = `<Full output log filepath>` allows you to specify a fixed path or filename to use for the log file. If a file with the specified name already exists, it is overwritten. If the file cannot be created, the installer aborts with an error message.

Parameter	Description
`/orgSettingsFilePath=<Full pingid.properties filepath>`	The full filepath of the PingID `properties file`. For example, `C:\Users\admin\Downloads\pingid.properties`. The PingID `properties file` is referenced from this location during the installation process. It is mandatory to specify either: ■ `/orgSettingsFilePath` Or all of the following parameters: ■ `/orgAlias` ■ `/orgKey` ■ `/authenticatorAddress` ■ `/idpUrl` ■ `/token` **Note** If any of the above parameters are specified, and `/orgSettingsFilePath` is also specified on the command line, then the values are retrieved from the `pingid.properties` file only, and the values of these other parameters specified on the command line are ignored.
`/orgAlias=`*<organization's alias string>*	The organization's alias. This value is an entry in the PingID `properties file`. If the `/orgSettingsFilePath` parameter is not specified, it is mandatory to provide the `/orgAlias` parameter. If both the `/orgSettingsFilePath` and `/orgAlias` are specified, the value is retrieved from the `pingid.properties` file, and the value of the `/orgAlias` parameter is ignored.
`/orgKey=`*<organization's key string>*	The organization's base64 key. This value is an entry in the PingID `properties file`. If the `/orgSettingsFilePath` parameter is not specified, it is mandatory to provide the `/orgKey` parameter. If both the `/orgSettingsFilePath` and `/orgKey` are specified, the value is retrieved from the `pingid.properties` file, and the value of the `/orgKey` parameter is ignored.
`/authenticatorAddress=`*<URL of PingID data center>*	The URL of the PingID data center to which the organization is associated. It is the URL that is listed on the line in the `pingid.properties` file that begins with `authenticator_url=`. If the `/orgSettingsFilePath` parameter is not specified, it is mandatory to provide the `/authenticatorAddress` parameter. It is ignored if `/orgSettingsFilePath` is also specified. **Important** When the `/orgSettingsFilePath=<Full pingid.properties filepath>` parameter is not supplied, the /authenticatorAddress value defaults to the North America data center. Administrators of organizations using the Europe or Australia and New Zealand data centers should ensure that they provide the relevant `/authenticatorAddress` value on configuration.

Parameter	Description
`/idpUrl` =*<URL of server used for PingID API requests>*	URL of the server used for PingID API requests. Take this value from the *idp_url* entry in the PingID `properties file`. If the `/orgSettingsFilePath` parameter is not specified, it is mandatory to provide the `/idpUrl` parameter. It is ignored if `/orgSettingsFilePath` is also specified.
`/token` =*<API key identifier>*	The identifier of the API key. This value is an entry in the PingID `properties file`. If the `/orgSettingsFilePath` parameter is not specified, it is mandatory to provide the `/token` parameter. It is ignored if `/orgSettingsFilePath` is also specified.
`/proxyAutoDetect` =*<0 or 1>*	Automatically detect the proxy settings. Possible values: ■ `0` = Disabled ■ `1` = Enable automatic detection of proxy settings
`/scriptProxyAddress` =*<URL>*	When the organization uses a PAC script for automatic proxy configuration, the `/scriptProxyAddres`s parameter should be specified using the http:// or https:// convention. `/scriptProxyAddress` is the proxy script URL, for example, `http://proxy.company.com:8083//proxy.pac`.
`/proxyAddress` =*<proxy's URL>*	When the connection is behind a proxy, the `/proxyAddress` parameter must be specified using the `http://` or `https://` convention. `/proxyAddress` is the URL address of the proxy, for example, `http://1.1.1.1:8080`. **Note** If the proxy requires credentials for authentication, the `/proxyUserName` and `/proxyPassword` parameters must be specified.
`/proxyUserName` =*<proxy's username>*	When the connection is behind a proxy, and the proxy requires credentials for authentication, the `/proxyUserName` and `/proxyPassword` parameters must be specified. The proxy's username must be supplied as the value of the `/proxyUserName` parameter.
`/proxyPassword` =*<proxy's password>*	When the connection is behind a proxy, and the proxy requires credentials for authentication, the `/proxyUserName` and `/proxyPassword` parameters must be specified. The proxy's password must be supplied as the value of the `/proxyPassword` parameter.
`/proxyBypassList` =*<comma-separated list of IP addresses or DNS names>*	The `/proxyBypassList` option can be used to specify that the communication with PingFederate should not go through the proxy that you configured. The value should be a list of one or more computers, separated with commas. The format can be domain name or IP address. For example, `/proxyBypassList="pingfed.example.com"` or `/proxyBypassList="pingfed.example.com,250.15.147.17"`.

Parameter	Description
`/ignoreConnectionErrors`	The installer attempts to address the PingID authenticator heartbeat as an initial part of the installation flow, to confirm connectivity. When there is no response, the installer ends the flow with an error status, before installing any of the elements. The `/ignoreConnectionErrors` parameter may be used to bypass this status, and to continue the installation, even without connectivity.
`/authenticationType` *=<0, 1 or 2>*	`/authenticationType` configures the installation for when to apply PingID authentication on logins via the PingID integration for Windows. Possible values: ■ `0` : Both RDP and local logins (default, when not specified). ■ `1` : Only RDP logins. ■ `2` : Only local logins. **Caution** Any other value causes the installation to abort.
`/excludeLocalUsers` *=<0 or 1>*	`/excludeLocalUsers` configures whether to apply PingID authentication to local user logins. Possible values: ■ `0` : Local users must authenticate with PingID. ■ `1` : Disable PingID authentication for local users. **Note** ■ This parameter is now replaced by `/excludeLocalAccounts` and `/excludeMicrosoftAccounts` . ■ If `1` , `/excludeLocalUsers` is set to `1` , `/excludeLocalAccounts` and `/excludeMicrosoftAccounts` are automatically set to `1` . ■ Domain users are always required to authenticate using PingID.
`/excludeLocalAccounts` *=<0 or 1>*	`/excludeLocalAccounts` defines whether to apply PingID authentication to local user logins: ■ `0` : Use PingID authentication for local user logins as well ■ `1` : Do not use PingID authentication for local user logins
`/excludeMicrosoftAccounts` *=<0 or 1>*	`/excludeMicrosoftAccounts` enables you to include or exclude Microsoft accounts used to access the Microsoft devices and services associated with a specific user. ■ `0` :Apply PingID authentication to Microsoft accounts. ■ `1` : Do not apply PingID authentication to Microsoft accounts.

Parameter	Description
`/offlineAuthType` =*<0, 1, 2 or 3>*	The `/offlineAuthType` specifies whether to allow PingID offline (manual) MFA, and defines the manual authentication methods that can be used. Possible values: ■ `0` : Do not allow MFA for offline authentication. ■ `1` : Allow offline MFA using PingID mobile app only. ■ `2` : Allow offline MFA using a FIDO2 security key only. ■ `3` : Allow offline MFA using either PingID mobile app or a FIDO2 security key. **Note** This parameter is only available when installing PingID integration for Windows login v2.3 or later.
`/RSA_PADDING` =*<oaep or none>*	■ Use `oaep` to specify that OAEP padding should be used in the encryption for offline authentication (default). ■ If you do not want to use OAEP padding for offline authentication, use none.
`/offlinePolicy` =*<0, 1>*	`/offlinePolicy` configuration defines whether it is possible to bypass MFA if the user is offline. Options available for this parameter depend on the values selected in the `/offlineAuthType` parameter as follows: ■ If `/offlineAuthType` = `0` : offline (manual) authentication is not allowed and the `/offlinePolicy` options are: ■ `0` : The user is blocked. ■ `1` : PingID bypasses MFA during sign on. ■ If `/offlineAuthType` = `1, 2, or 3` : offline (manual) authentication is allowed and `/offlinePolicy` options are: ■ `0` : At least one allowed authentication method must be paired for the user to authenticate with offline MFA, otherwise the user is blocked. ■ `1` : If the user does not have at least one allowed authentication method for offline authentication paired with their account, PingID bypasses MFA during login. **Note** This parameter is only available when installing PingID integration for Windows login 2.3 or later.
`/domainPostfix` =*<@organization's domain name>*	`/domainPostfix` configures the installation to append the value supplied in this parameter, to the username at login time. A suffix, such as `@domain.com` , can be defined, however, a prefix, such as `domain\` , cannot be defined. **Note** Enter the leading "@" before the domain name, for example `[.parmname]` / domainPostfix `=@somewhere.com` . This parameter has a maximum length of 50 characters, including the leading "@".

Parameter	Description
`/MultipleDomain` *=<0 or 1>*	`/MultipleDomain` allows the user to log in from multiple domains. This option is available with PingID for Windows login 2.2 and later. Options include: ■ `0` : Use of multiple domains is not permitted. (default) ■ `1` : Multiple domains are permitted. This option should not be used when `/usernameMapping` is set to `None` and a `/domainPostfix` is not specified.
`/usernameMapping` = `=UPN/SAM/SID/UserName/None`	Select the attribute that you want to use to identify the user. The examples show how the username is mapped in PingID ■ `None` (default): Use the legacy username parsing convention. This can be either with or without `/domainPostfix` . Example: ■ `/domainPostfix` set to @domain.com: `jsmith@domain.com` ■ `/domainPostfix` not specified: `jsmith` **Note** ■ If you don't specify `/domainPostfix` , do not set the `/MultipleDomains` parameter to `1` . ■ This option isn't recommended in environments with multiple domains or environments where PingID is also used to sign on locally. ■ `SID` : Use the objectSID. For example, `S-1-5-21-668608636-2615149724-2645577550-1112` ■ `UPN` : Use the userPrincipalName. For example, `jsmith@domain.com` ■ `SAM` : Use the Domain Name as prefix, or the computer name when logged in locally, and then the SAM Account Name. For example, `DOMAIN\jsmith` ■ `UserName` : Use the SAM Account Name only. For example, `jsmith`
`/DIR` *=<installation destination folder's full filepath>*	The default installation location for the PingID integration for Windows login is `C:\Program Files\Ping Identity\PingID\WindowsLogin` . If you want the installation in a different folder, specify the `/DIR` parameter with the destination value.
`/PingFedAddress=` *<baseurl>*	The PingFederate Base URL used to integrate PingID for Windows login through PingFederate. This field must be included when integrating through PingFederate, as in the following example. + `/PingFedAddress=https://10.132.102.92:9031`
`/CPWhiteList ={CP_GUID1};{CP_GUID2}`	Enables you to exclude one or more credential providers that are not PingID credential provider (CP) from being filtered out by PingID integration with Windows login. Enter the credential provider GUID for each credential provider that you want to exclude, separated by a semicolon. PingID MFA does not work with any credential provider that is on the CP allow list.

Parameter	Description
`/thirdPartyCredentials=<0 or 1>`	Enables integration with a third party credential provider, such as McAfee Drive Encryption credential provider. Options include: ■ `0`: Do not integrate (default). ■ `1`: Integrate with McAfee Drive Encryption credential provider.
`/HttpRequestTimeout`=<timeinms>	Defines the HTTP request timeout value. Possible values between 1000-30000 ms. **Note** The value configured for HTTP Timeout does not influence the timeout for embedded browser requests.
`/NORESTART`	Prevents the installer from restarting the system following a successful installation. **Note** The `/NORESTART` parameter is not an override. In some cases, the operating system (OS) will still require a restart to proceed with installation because of events like the OS installing a newer version of software, such as Visual C++ Runtime. If a restart is required, the installation logs will display the following: `The computer needs to be restarted before the setup can continue. Please restart the computer and run the PingID setup again.` + **Important** The `/NORESTART` parameter allows the user to continue working without restarting their machine. Windows login client is not fully installed until the machine is restarted. To prevent issues when the user locks their machine (prompting Windows login client to start functioning), is recommended that the user restart their machine as soon as possible after the installation. If the `/NORESTART` parameter is omitted, a successful installation automatically triggers a machine restart.
`/DeprecatedSecurityKeys=<Allow, Inform, or Delete>`	In version 2.8 of the Windows login integration, an improved implementation was introduced for the use of security keys while offline. The `/DeprecatedSecurityKeys` parameter allows you to specify how PingID should relate to the security keys paired previously: ■ Allow: Allow users to continue using these keys (this option isn't recommended) ■ Inform: Allow users to continue using these keys, but inform them that these keys should be manually deleted ■ Delete: Automatically delete the keys that were paired before the change was introduced If the `/DeprecatedSecurityKeys` parameter is omitted, the default behavior is *Inform*.

Parameter	Description
`/AllowFullPermissionsPropertiesFile`	If you include the `/AllowFullPermissionsPropertiesFile` option during installation, PingID will allow you to use the full-permissions properties file (rather than the restricted-permissions properties file intended for use with Windows login). However, it is strongly recommended that you refrain from doing so. Using the full-permissions properties file with Windows login is a security risk (for details, see CVE-2022-23717).
`/SkipMFAGracePeriod`	Include `/SkipMFAGracePeriod` if you want to define a period following authentication during which the user isn't asked to authenticate again if they lock their computer. The maximum period is 15 minutes. The period is defined in seconds so the range of values you can use is 1-900. **Caution** Use this option with caution because it leaves the computer with a lower level of protection for the defined period.

Result:

The next time the user signs on to the Windows machine, they must authenticate with PingID.

3. **Optional:** The downloaded `pingid.properties` file can be deleted once the installation has completed.

> **Note**
>
> The `OrgData1`, `OrgData2`, … fields in the `HKEY_LOCAL_MACHINE\SOFTWARE\Ping Identity\PingId\PingIdCredProv` registry are encrypted and should not be edited.

4. To verify the installation was successful, test that the user can sign on to the Windows machine using their password and PingID MFA.

Uninstalling the PingID integration for Windows login

Uninstall the PingID integration for Windows login on your machine.

Before you begin

Before uninstalling PingID from your Windows machine, you should unpair the device. See Managing your devices in the PingID User Guide.

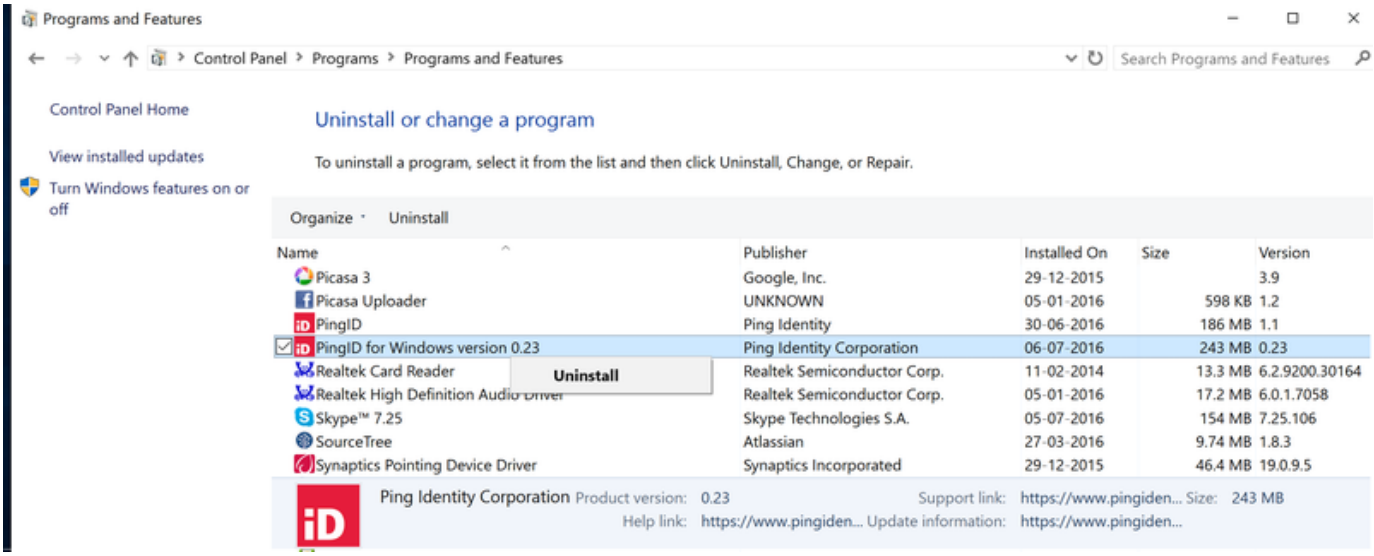
Note

If you want to run the uninstallation program from the command line, you can run `unins000.exe`, located in the top-level of the installation directory. When uninstalling from the command line, you can use the following options:

- `/SILENT` - Don't display the background window, but show the installation progress window. If a restart is necessary, the user is prompted with a **Reboot now?** message box.
- `/VERYSILENT` - Don't display the background window or the installation progress window. If a restart is necessary, the reboot is performed without asking the user.

Steps

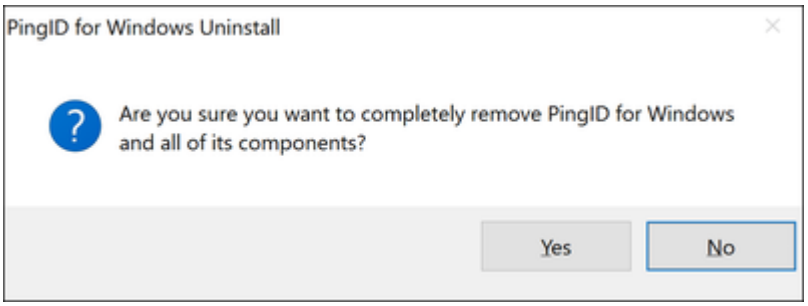
1. In Windows, go to **Control Panel → Programs → Programs and Features**, right click the listing of **PingID for Windows**, and select **Uninstall**.



Caution

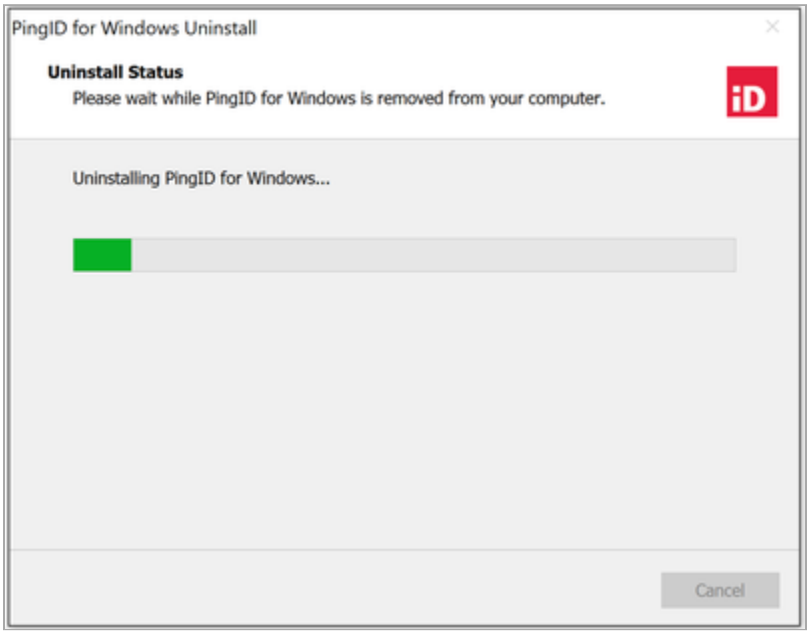
If you also have an installation of the PingID desktop app on the same machine, make sure that you select the correct entry (**PingID for Windows**) to uninstall.

2. Confirm the removal.



Result:

You see a status window.



After the program is uninstalled, you see a confirmation message showing that the application was successfully uninstalled.

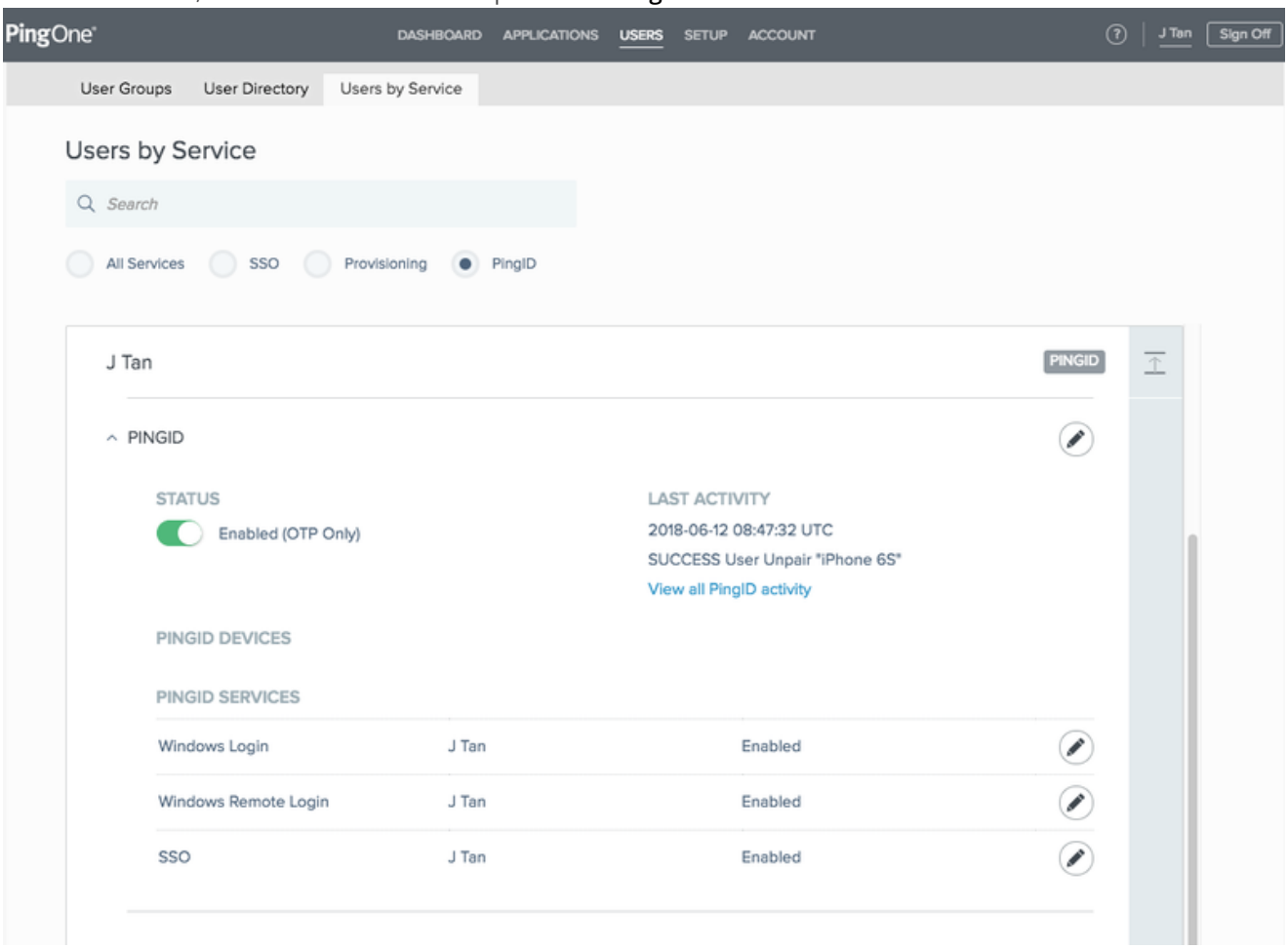
Managing PingID integration for Windows login users

Manage users of the PingID integration for Windows login service from the admin portal.

About this task
Steps

1. Go to **Users → Users by Service**.
2. Click **PingID**.

3. To select the user, click on their name and expand their **PingID** section.



Depending on the configuration of PingID integration for Windows for remote and local login authentications, the following new entries might appear in the user's **PingID Services** list:

- **Windows Remote Login**: The PingID service for signing on to a remote server.
- **Windows Login**: The PingID service for signing on to a local machine.

All other user management and reporting functions are identical to those of other services.

Troubleshoot the PingID integration for Windows login

The following sections describe common issues that administrators or end users might encounter and their solutions.

Installation completed successfully, but users are unable to access the Windows machine using PingID MFA

> **Important**
>
> An open admin session is required to investigate or recover from this scenario.

If an admin session is open

- Analyze the registry values in `HKEY_LOCAL_MACHINE\SOFTWARE\Ping Identity\PingId\PingIdCredProv` to verify that the correct settings have been defined. For more information, see the parameter table in the topic Installing the PingID integration for Windows login using CLI.

> **Note**
>
> The three OrgData fields are encrypted and should not be edited.

If your organization uses PingID's Europe or Australia & New Zealand data centers verify that the correct URL entry is listed for their data center's authenticator address.

- Analyze the installation log file and confirm that the parameter values entered are correct. If necessary, forward the log file to PingID support.

> **Note**
>
> The installation log file is located in the admin installation user's `TEMP` directory, unless the CLI option /LOG was used to create it in a different location.

- Optionally, change registry settings temporarily to suspend PingID MFA for local or remote users.
- Optionally, uninstall PingID from the machine and attempt the installation again. Then, check the results.

If there are no open admin sessions, check if one of the following options can be used to open an admin session and then continue with the previous steps ("If an admin session is open").

- If the installation was configured for PingID authentication for remote logins only, then sign on locally as administrator to bypass PingID authentication.
- If the installation was configured for PingID authentication for local logins only, then sign on remotely as administrator to bypass PingID authentication.
- If the installation was configured to bypass PingID authentication when there is no Internet connection available at the time of sign on, then disconnect the machine from the network to permit signing on.
- If none of the above scenarios permit you to open an admin session, restart the machine in Windows Safe Mode and sign on as an administrator.

If the installation was completed but the machine was not restarted yet, a restart might be required.

Admin console: Users by Service has duplicate entries for the same user

Go to **Users → Users by Service**. In the **Users by Service** section, there appear to be duplicate rows for some users.

This is the result of different values for the username of the PingID account compared with the username value in the Windows Security Account Manager (SAM). For example, an existing user of other PingID services, `johndoe`, starts to use PingID integration for Windows login to access a Windows server, where his username is `johndoe@somewhere.com`. Although this is the same user, PingID regards him as two different users, resulting in two entries in the **Users by Service** table.

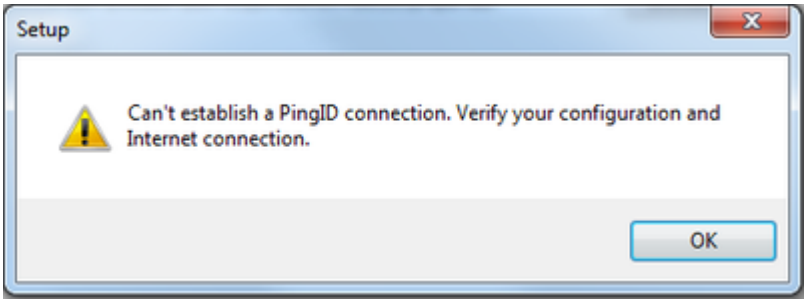
Files not removed when installation was canceled

There can be scenarios where files were not removed after the installation has been canceled. These situations depend on the state of progress the installation reached at the time that it was canceled, and they are more prevalent when the CLI is used and interrupted in the middle of the installation.

To remove the files, you should first attempt to uninstall the PingID integration for Windows login according to the uninstall instructions page. For more information, see Uninstall the PingID integration for Windows login.

If the uninstall procedure does not succeed, go to the installation directory, default `C:\Program Files\Ping Identity\PingID\WindowsLogin`, or other destination if the default was changed during installation, and manually remove the files.

Installation fails on message "Can't establish a PingID connection. Verify your configuration and Internet connection."



This error message indicates that the Windows machine being configured for PingID integration with Windows login is unable to connect to the PingID server. Check the following when troubleshooting:

- The Windows machine must have a working Internet connection.
- Verify that the authenticator URL matches the entry in your organization's `pingid.properties` file.
- If a proxy address and credentials are required, verify the values entered.

For further details, see Installing the PingID integration for Windows login.

Integrating PingID with Windows login (passwordless)

Windows Login - Passwordless makes it possible for users to log-in to their Windows computer without a password, using just the PingID mobile app (version 1.15 or higher) or a FIDO2 security key.

A number of points to take into account before setting up Windows Login - Passwordless:

- For users to use the passwordless login, they must already have a device that has been paired for PingID.
- Windows Login - Passwordless includes support for *Run as Admin*.
- Windows Login - Passwordless includes support for remote desktop (RDP). If you plan on using RDP, you must install Windows Login - Passwordless on both the accessing client and the remote computer.

Basic steps for setting up Windows Login - Passwordless

These are the main steps the administrator must carry out to set up the PingID integration with passwordless Windows login:

1. Create a new environment in PingOne and connect it to your existing PingID account.
2. Configure identity store provisioners.
3. Create an "issuance" certificate in PingOne.
4. Create an authentication policy in PingOne.
5. Create and configure a passwordless Windows login application in PingOne.
6. Generate a KDC certificate (if necessary).
7. Install the Windows Login - Passwordless integration software on the individual Windows client computers.

System requirements and prerequisites

To set up and use the PingID integration for passwordless Windows login, the following requirements must be met:

System requirements

- Microsoft Active Directory running on Windows Server 2016 or higher
- Users' computers must be running Windows 10 (64-bit) or Windows 11, and must support TPM 2.0.

> **Note**
>
> If you have set the **Resident Key** option to Required for FIDO2 security keys, users do not require TPM on their computer in order to use the passwordless login, provided that they paired their keys after the setting was changed to Required. For more information on the **Resident Key** option, see (Legacy) Configuring the FIDO2 security key for PingID. Since TPM 2.0 provides a higher degree of security, the passwordless login for Windows will always use TPM for storage if the relevant computer has the necessary support.

Prerequisites

- Admin rights for the Domain Controller
- A PingOne account
- A PingID account
- Users must have the PingID mobile app installed on their devices or a security key that can be used for authentication, and must have paired their device already.

Create PingOne environment and connect it to a PingID account

Carry out these steps to create a new environment in PingOne and connect it to an existing PingID account (to allow syncing of the PingID data) or to a newly-created PingID account. You must create a new PingOne environment even if you have an existing environment because you cannot connect a PingID account to an existing PingOne environment.

1. In the PingOne console, click **Add Environment**.
2. Select **Build your own solution**.
3. Hover over the **PingOne SSO** element and click **Select**.
4. Hover over the **PingID** element and click **Select**.
5. Click **Next**.
6. When you are presented with the two options for PingID, select either the option of connecting to an existing PingID account or the option of creating a new PingID account.
7. If you selected the option of connecting to an existing PingID account, provide the credentials you use for the PingID account.
8. Click **Next**.
9. Provide a name for the new environment.
10. Select the relevant license.
11. Click **Finish**.

Configuring identity store provisioners

To use passwordless Windows login, user attributes must be mapped to attributes in PingOne.

If you have been using PingFederate with the PingID connector for user provisioning, you will have to make the transition to using PingFederate with the PingOne Provisioning connector for user provisioning. You can find information on using this integration in Provisioning connector.

> **Note**
>
> When mapping attributes, keep in mind that the *ObjectSID* attribute must be mapped to a unique attribute in PingOne. You can find information on passing binary attributes in Passing binary attributes to PingOne.

Creating an issuance certificate in PingOne

The PingID Windows Login - Passwordless solution uses Certificate-Based Authentication (CBA), and therefore a certificate is required for each user that will be logging in. This requires that you create an "issuance" certificate in PingOne, and then publish the certificate..

Steps

1. Create an issuance certificate in PingOne, following the instructions in Adding a certificate and key pair in the PingOne documentation. When creating the certificate, set the **Usage Type** to Issuance and for the **Signature Algorithm** select SHA256withRSA.
2. Publish the issuance (CA) certificate to Active Directory: `certutil -dspublish -f` <CA certificate filename> `NTAuthCA`
3. To verify that the certificate was published, run the following command and make sure that you see the CA certificate in the list: `certutil -viewstore "ldap:///CN=NTAuthCertificates,CN=Public Key Services,CN=Services,CN=Configuration,DC=`<domain name>`"`
4. Import the CA certificate in the Group Policy Management Console (GPMC) in order to publish the CA certificate to end users' computers:
    1. Open the Group Policy Management Console (GPMC).
    2. Locate the relevant domain.
    3. Locate the group policy you will be using.
    4. Under **Computer Configuration\Windows Settings\Security Settings\Public Key Policies**, select **Trusted Root Certification Authorities** and import the CA certificate.

Creating an authentication policy (Windows passwordless)

Steps

1. Go to the PingOne console and open the environment you are using for Windows Login - Passwordless.
2. In the icon menu, click the **Identities** icon.
3. In the menu, click **Attributes**.
4. In the list of attributes, locate the PingOne attribute that you mapped to *ObjectSID*.
5. Click the Pencil icon to edit the attribute properties.
6. Select the **Enforce Unique Values** check box, and confirm the choice if prompted to do so.
7. Click **Save**.
8. In the icon menu, click the **Experiences** icon.
9. In the menu, click **Authentication Policies**.
10. Click **Add Policy**.

    Result:

    The policy definition screen is displayed.
11. Give the policy a name.
12. For **Step Type**, select *Windows Login Passwordless*.

13. Under **Match Attributes**, select the attribute that you mapped to *ObjectSID*.

> **Note**
>
> This drop-down list includes any attributes that you have specified as unique by selecting the **Enforce Unique Values** option.

14. Select the **Offline Mode** option if you want to allow users to log in when PingOne or PingID are not available.
15. Click **Save** to save the policy.

Creating and configuring a passwordless Windows login application in PingOne

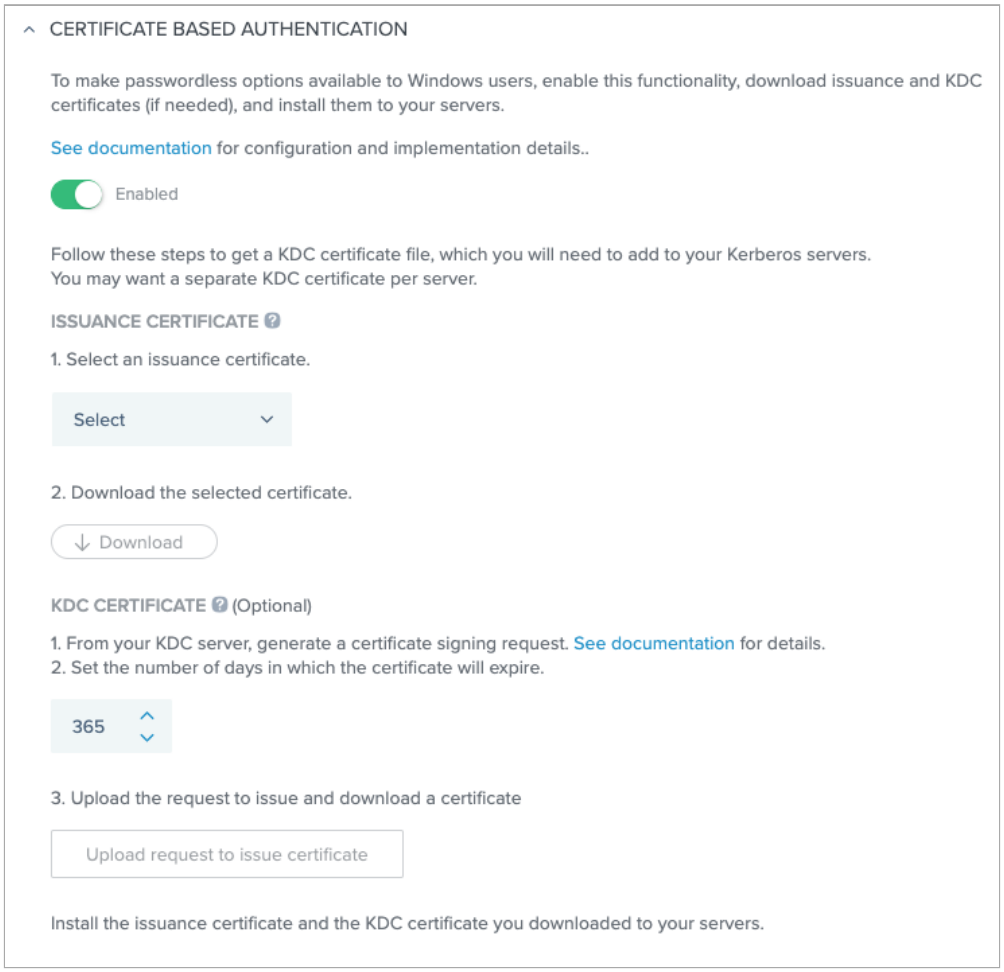
After creating the authentication policy, you can now create the application for passwordless Windows login.

Steps

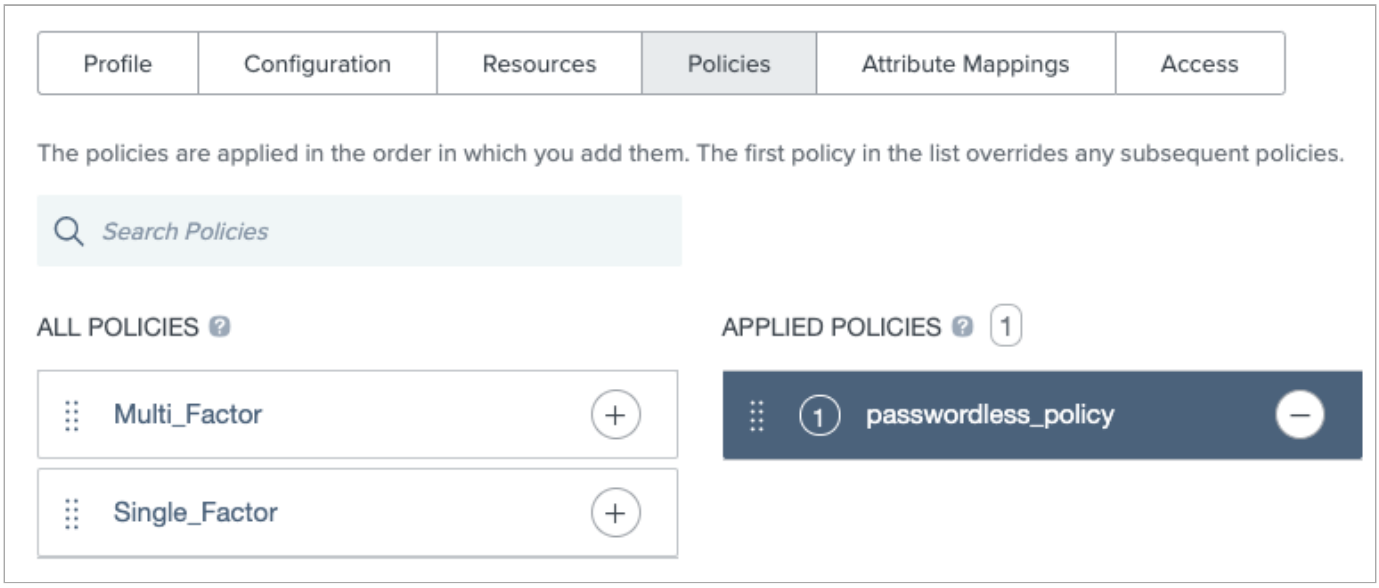
1. Go to the PingOne console and open the environment you are using for Windows Login - Passwordless.
2. In the icon menu, click the **Connections** icon.
3. Click **Applications**.
4. Click the plus sign to add a new application.
5. For the application type, select **Native App**.
6. Click the **Configure** button to continue with the creation of the application.
7. Provide a name and description for the application, and click **Next**.
8. Add the redirect URL `winlogin.pingone.com://callbackauth`, and then click **Save and Continue**.

You can skip the steps **Grant Resource Access** and **Attribute Mapping**.

1. Scroll down to the **Certificate-based authentication** section.



2. Set the slider to **Enabled**.
3. Select an existing issuance certificate.
4. Go to the application's **Policies** tab.
5. Drag the passwordless policy that you created from the **All Policies** list to the **Applied Policies** list.



Generating a KDC certificate

If there is not yet a certificate for the KDC server that you will be using, you will need to generate such a certificate.

About this task

The KDC certificate is used as part of the Kerberos PKINIT mutual authentication mechanism. If you already have a KDC certificate installed on your Active Directory Domain Controllers, there is no need to carry out the steps listed here.

Steps

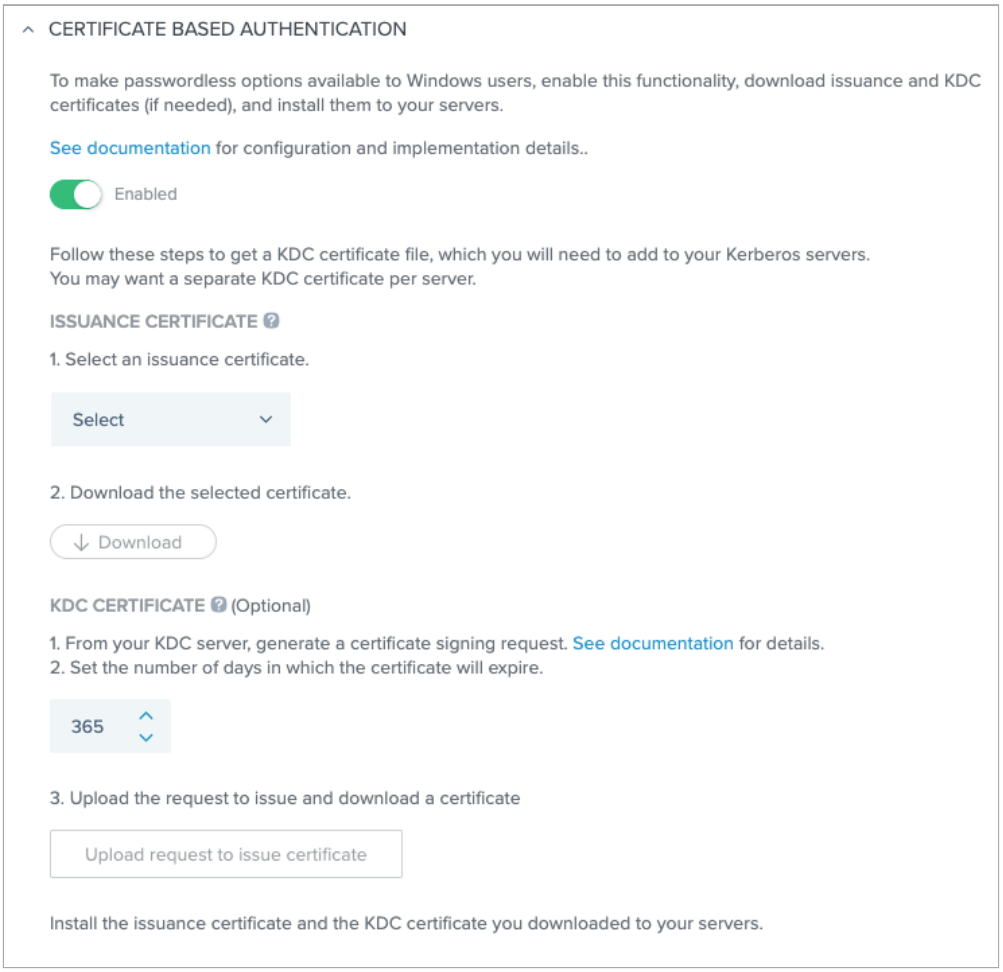
1. Create an .inf file containing the following information:

```
[newrequest]
        subject = "CN=<hostname>"
        KeyLength = 2048
        MachineKeySet = TRUE
        Exportable = FALSE
        RequestType = PKCS10
        SuppressDefaults = TRUE
        [Extensions]
        ;Note 2.5.29.17 is the OID for a SAN extension.
        2.5.29.17 = "{text}"
        _continue_ = "dns=<DNS hostname>"
```

> **Note**
>
> In the example above, *<hostname>* and *<DNS hostname>* should be replaced with the FQDN of the domain controller server, for example, servername.example.com. For more information on the contents of `.inf` files for the `certreq` command, see the certreq documentation.

2. Generate a certificate signing request from your KDC server by running the command: `certreq -new ``<path to the .inf file>[.codeph]`` 'kdc.req'`

3. Go to the PingOne console, and open the application that you created for passwordless Windows login.
4. Click the **Configuration** tab of the application.
5. Scroll down to the **Certificate-based authentication** section.



6. For the KDC certificate signing request that you created earlier with the `certreq` command:
    1. Set the number of days until the certificate should expire.
    2. Click the **Upload request and Issue Certificate** button to have the certificate issued.

> **Note**
>
> The KDC certificate does not necessarily have to be signed by the issuance certificate that you created with PingOne. Any valid certification path will work.

7. Install the KDC certificate on your server: `certreq -accept -machine -f` <KDC certificate filename>

> **Note**
>
> You must install the KDC certificate on each Active Directory Domain Controller that will be used to authenticate users with Windows Login - Passwordless.

Installing passwordless Windows Login integration on client computers

You can install the integration for passwordless Windows login on your users' computers with the command-line interface that is provided or with the UI-based installation.

Requirements

- To use the passwordless Windows login feature, users' computers must be running Windows 10 (64-bit) or Windows 11, and must support TPM 2.0.

  > **Note**
  >
  > If you have set the **Resident Key** option to Required for FIDO2 security keys, users do not require TPM on their computer in order to use the passwordless login, provided that they paired their keys after the setting was changed to Required. For more information on the **Resident Key** option, see (Legacy) Configuring the FIDO2 security key for PingID. Since TPM 2.0 provides a higher degree of security, the passwordless login for Windows will always use TPM for storage if the relevant computer has the necessary support.

- The first time that a user carries out passwordless Windows login, they need to be online and connected to the organizational network because certificate enrollment requires a connection to Active Directory. Afterwards, there is no need for a connection to the network, and authentication can be carried out online or offline (for as long as the certificate is valid).

UI-based installation

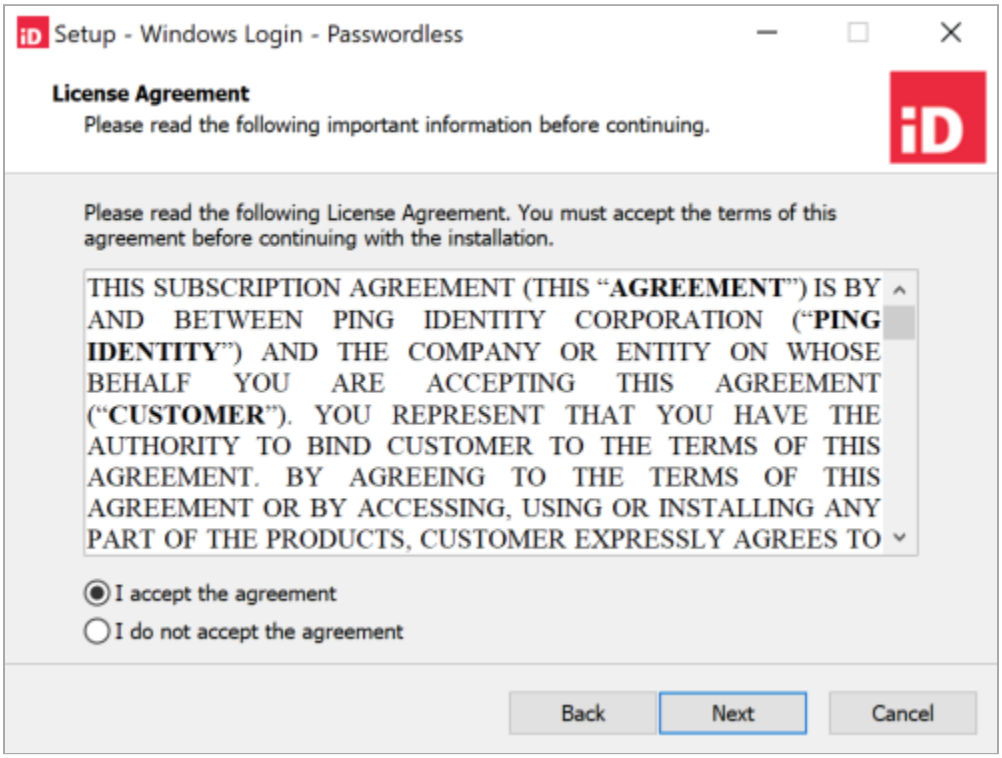
Installing passwordless Windows Login integration on client computers (UI)

You can install the integration for passwordless Windows Login on your users' computers with the UI-based installation described in this topic.

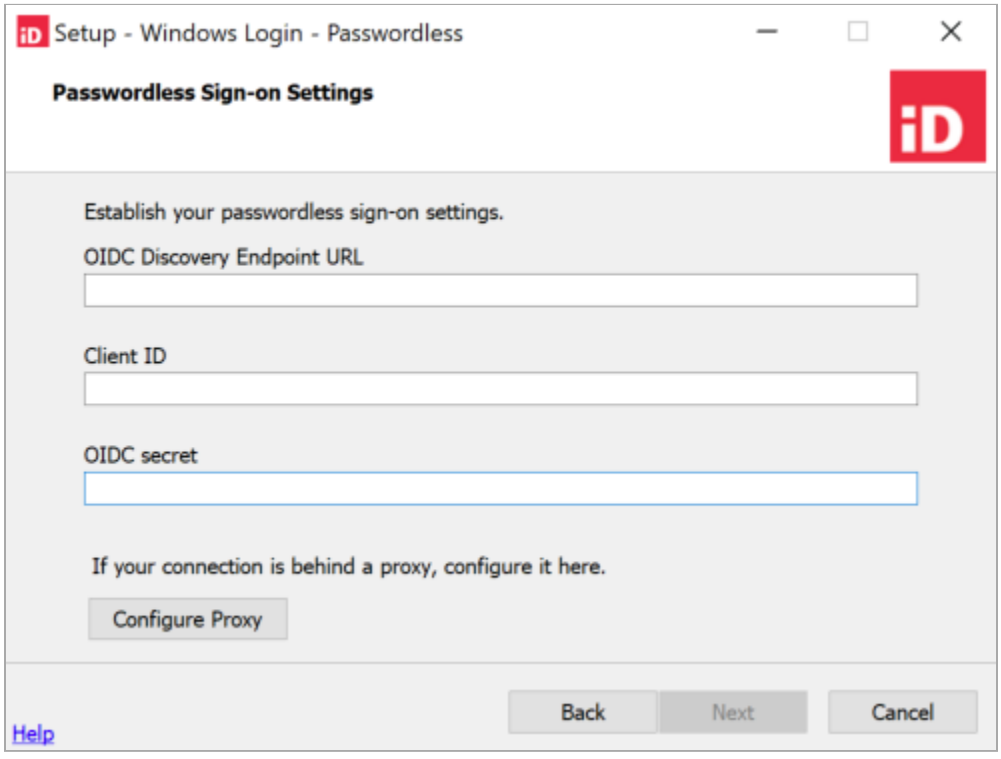
Steps

1. Run the provided executable, and when the welcome screen is displayed, click **Next**.

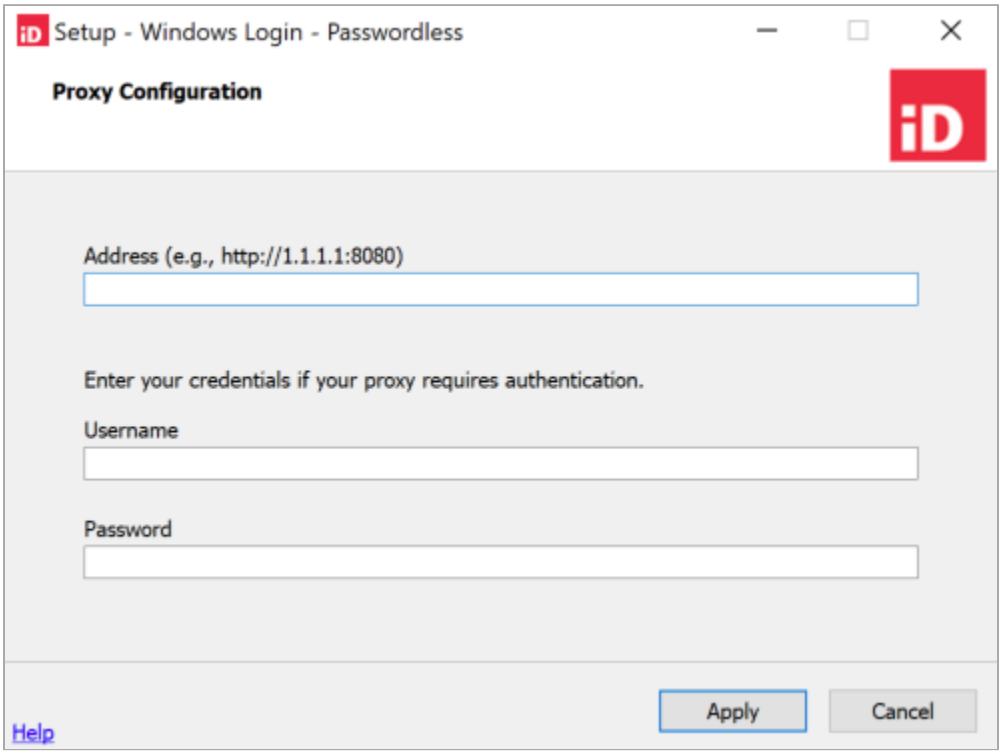
2. Accept the license agreement and click **Next**.



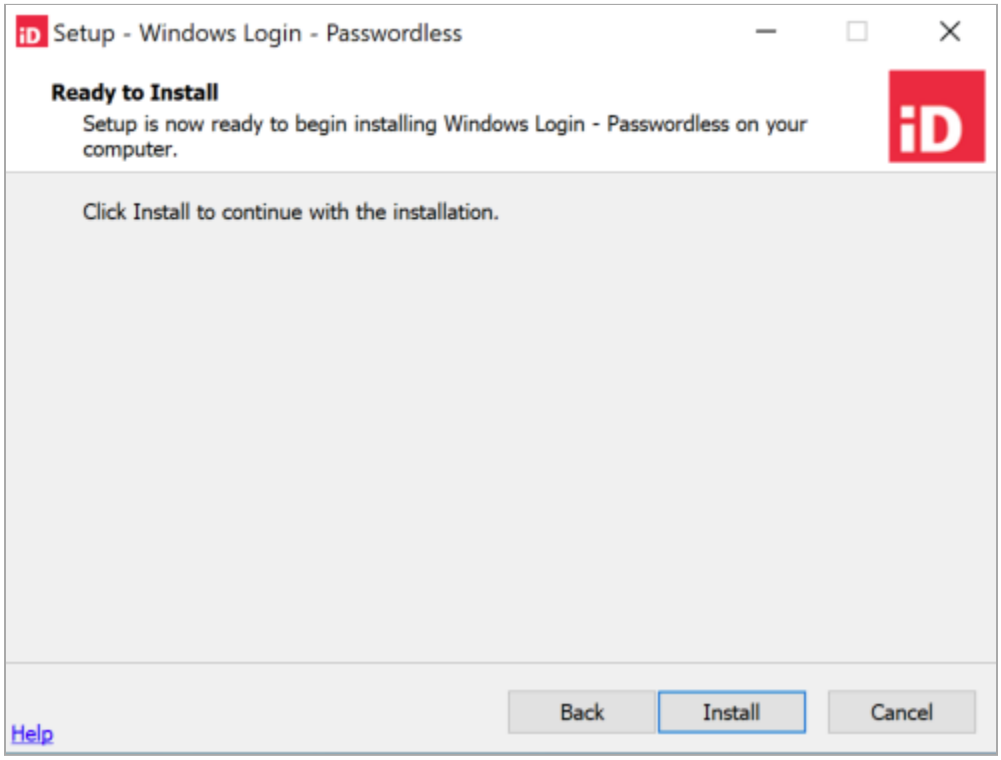
3. The settings that must be entered on the **Passwordless Sign-on Settings** screen should be copied from the **Configuration** tab of the application you created for Windows Login - Passwordless in PingOne. If your organization uses a proxy, click **Configure Proxy**. Otherwise, click **Next**.



4. If you clicked **Configure Proxy** in the previous step, enter the proxy information, click **Apply**, and when you are returned to the **Passwordless Sign-on Settings** screen, click **Next**.



5. When the **Ready to Install** screen is displayed, click **Install** to start the installation.



Command-line installation

Installing passwordless Windows Login integration on client computers (CLI)

While you can install the integration for passwordless Windows Login on your users' computers with the UI wizard that is provided, you can also use the CLI-based installation that is described in this topic.

== Mandatory parameters

The following parameters are mandatory and should be copied from the **Configuration** tab of the application you created for Windows Login - Passwordless, in PingOne.

- `/OIDCDiscoveryEndpoint` - the OIDC discovery endpoint, from the **URL** section of the Configuration tab
- `/OIDCClientID` - the client ID, from the **General** section of the Configuration tab
- `/OIDCSecre` t - the client secret, from the **General** section of the Configuration tab. Click the Show Secret icon, and then copy the text displayed.

== Optional Parameters

- `/DIR` - the path where the software should be installed. If this parameter is not specified, it will be installed to `C:\Program Files\Ping Identity\PingID\Windows Passwordless`
- `/LOG` - specify a path if you want a log file to be created for the installation
- `/VERYSILENT` - neither the background window nor the installation progress window are displayed
- `/SILENT` - the background window is not displayed, but the installation progress window is displayed
- `/ProxyAddress` - proxy URI, if you are using a proxy
- `/ProxyUserName` - user name if you are using a proxy
- `/ProxyPassword` - password if you are using a proxy
- `/HttpRequestTimeout` - timeout to use for HTTP requests, in milliseconds - can be between 1000 and 30000, default is 10000 milliseconds
- `/NORESTART` - prevents installer from restarting the system following a successful installation. Note that Windows Login - Passwordless will not work until after the computer is rebooted.
- `/RSA_PADDING -` use the value `oaep` to specify that OAEP padding should be used in the encryption for offline authentication (default). If you do not want to use OAEP padding for offline authentication, use the value `none`.
- `/ALG_KEY_TYPE` - set the registry key algorithm type. Possible values:
  - 0 = RSA
  - 1= ECC
- `/AllowInsecureDiscouragedUV` - Skip user verification for Windows login passwordless users when using any FIDO device. Possible values:
  - 0 = Disabled
  - 1 = Enabled

> **Caution**
>
> Use this option with caution, as it relies solely on the FIDO device to authenticate, and does not distinguish between different users.

- `/SUPPORT_CAMERA_LAUNCHER` : When enabled, the user can scan the manual authentication QR code from their device camera. When the user scans the manual authentication QR code with their device camera, PingID mobile app opens automatically, displaying the manual authentication key. This option requires PingID mobile app 2.3 or later. Possible values:
  - 0 = Disabled
  - 1 = Enabled

== Sample installation command

`"PingIDWindowsLogin - Passwordless_1.0.0.0.exe" /LOG=C:\Users\user\Desktop\log.txt /VERYSILENT /ProxyAddress=http://1.1.1.1:8080/ /ProxyUserName=` <username> `/ProxyPassword=` <password> `/HttpRequestTimeout=5000 /OIDCDiscoveryEndpoint=https://auth-test.pingone.com/71ab9623-dd25-4eaf-8a72-597ee70532b1/as/.well-known/openid-configuration /OIDCClientID=17fbc3dc-aa45-6854-9a82-761d906cbcff /OIDCSecret=` <secret>

Configuration for use with RDP

You can also use Windows Login - Passwordless when authenticating to access a remote computer via RDP. To use the integration with RDP, there are a number of configuration steps you must carry out.

The first section in this topic describes the steps you must carry out both for authentication via the PingID mobile app and authentication via a security key.

The second section describes additional steps you may have to carry out if your users will be authenticating with a security key.

Configuration steps for using Windows Login - Passwordless for RDP authentication

The use of Windows Login - Passwordless to access a remote computer via RDP is based on use of the certificate and private key from the client computer.

This approach uses named pipes as a transport layer between the two computers. To allow the necessary messages to be sent over this transport layer, you must ensure that two-way TCP traffic is allowed between the host and the client computers on port 445.

Additional configuration steps for using security key authentication for RDP

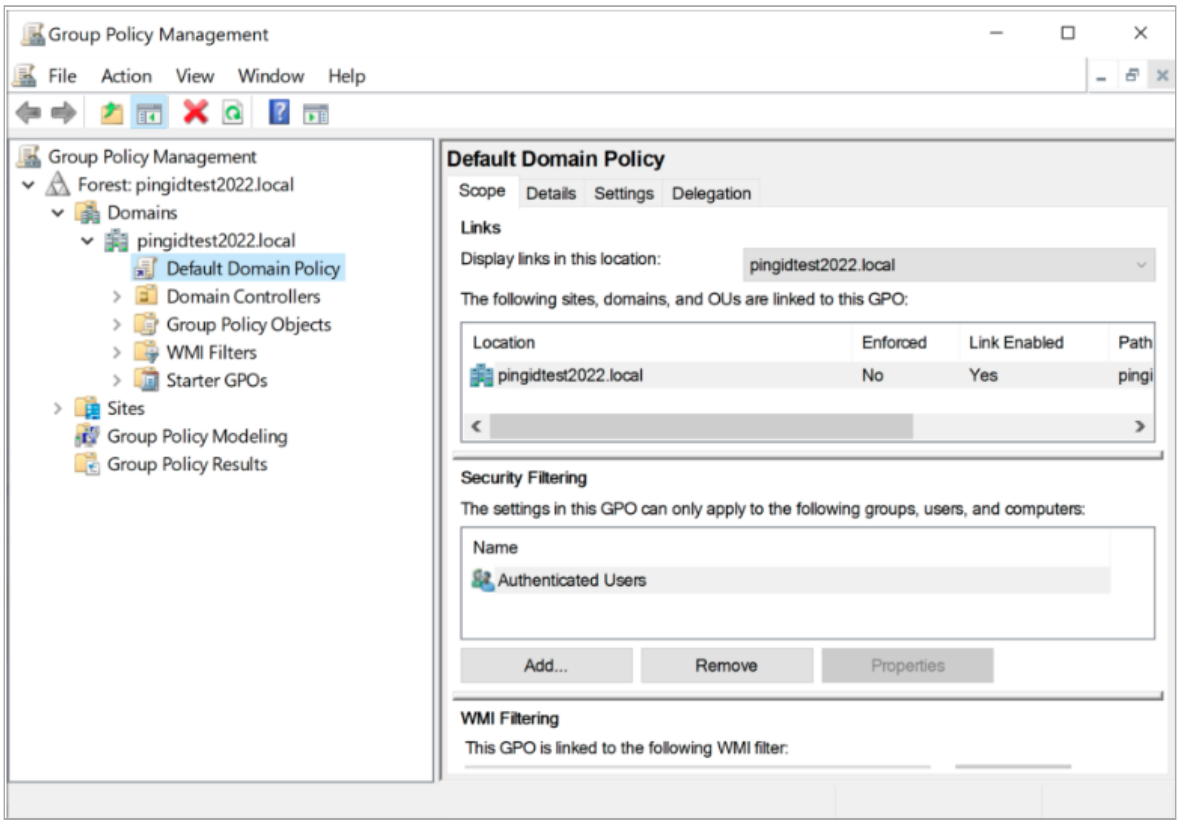
The step described in the previous section allows you to carry out basic authentication for RDP with a security key. However, because security keys are not visible to remote computers by default when accessing the computers via RDP, there are additional steps that you must carry out if you need to allow any of the following on the remote computer:

- Locking/unlocking of the remote computer
- User Access Control (UAC)

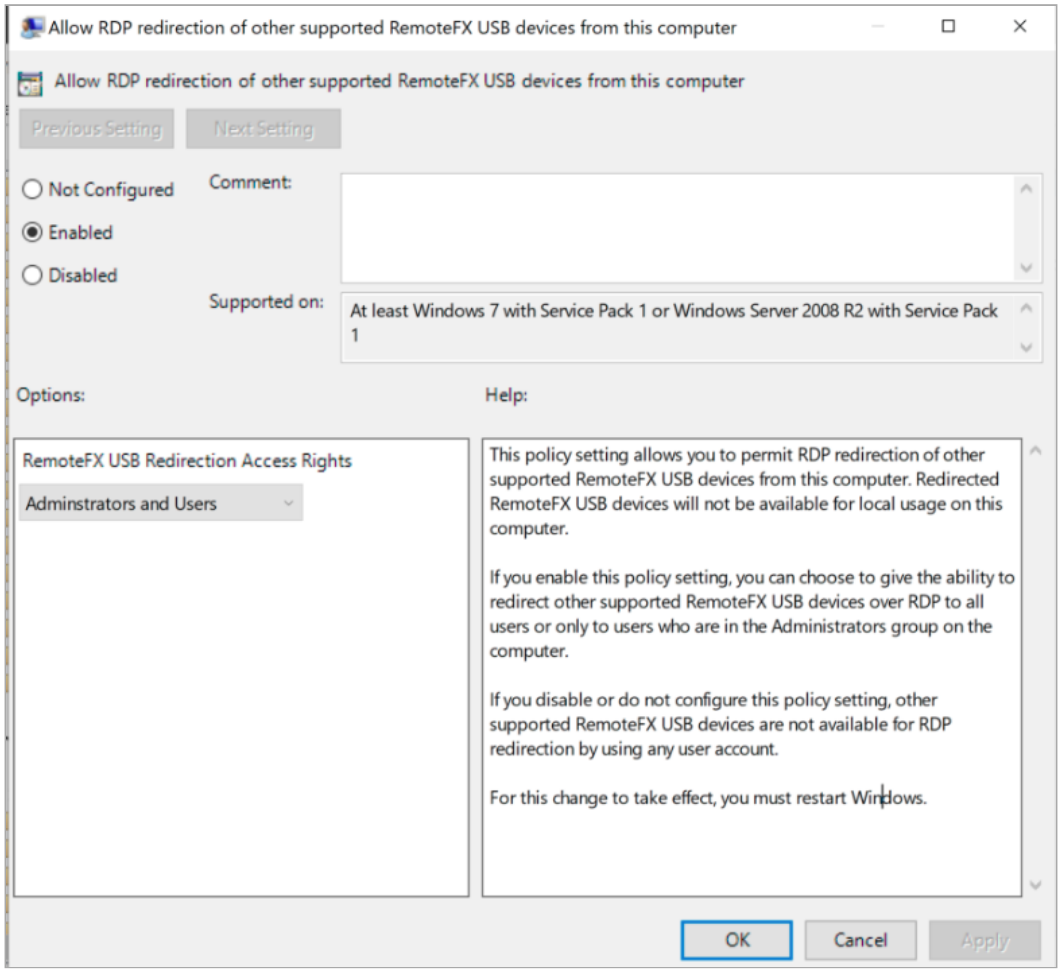
- RDP to a second remote computer

Changes that must be made to group policy

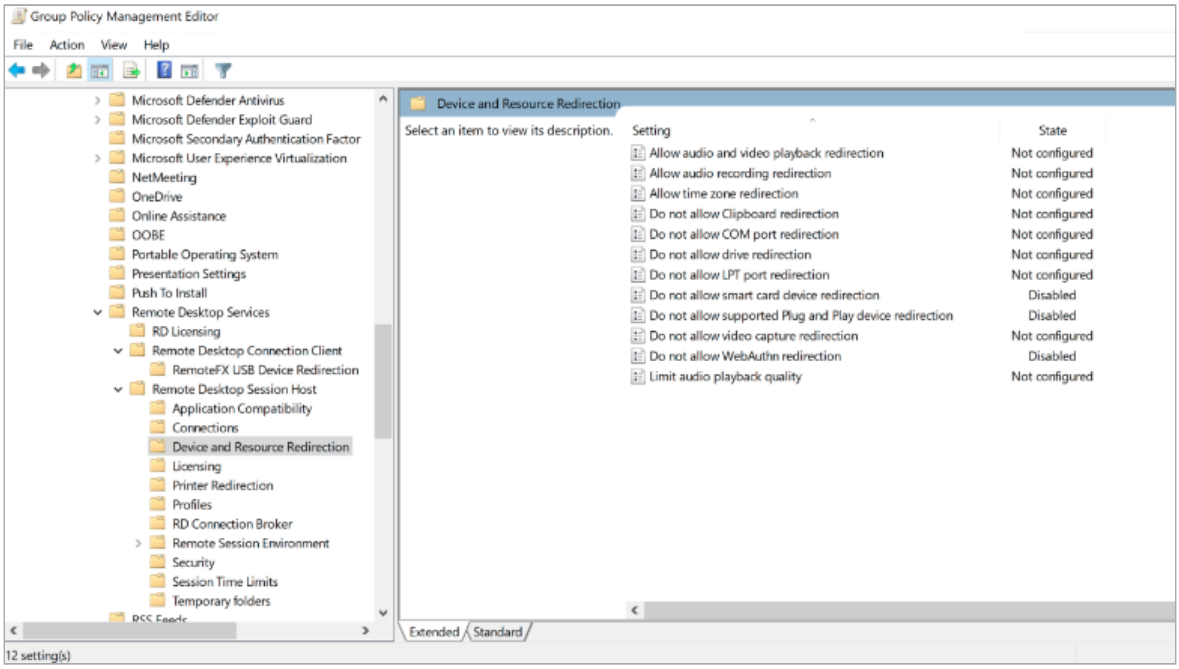
1. Run `gpmc.msc` to open the **Group Policy Management** application.
2. Navigate to the relevant domain policy, and select **Edit** from the context menu.



3. Go to **Computer Configuration → Policies → Administrative Templates → Windows Components → Remote Desktop Services → Remote Desktop Connection Client → RemoteFX USB Device Redirection**.
4. Edit **Allow RDP Redirection of other supported RemoteFX USB devices from this computer**.



5. Set **Allow RDP Redirection of other supported RemoteFX USB devices from this computer** to **Enabled**.
6. Set **RemoteFX USB Redirection Access Rights** to **Administrators and Users**.
7. Go to **Computer Configuration → Policies → Administrative Templates → Windows Components → Remote Desktop Services → Remote Desktop Session Host → Device and Resource Redirection**



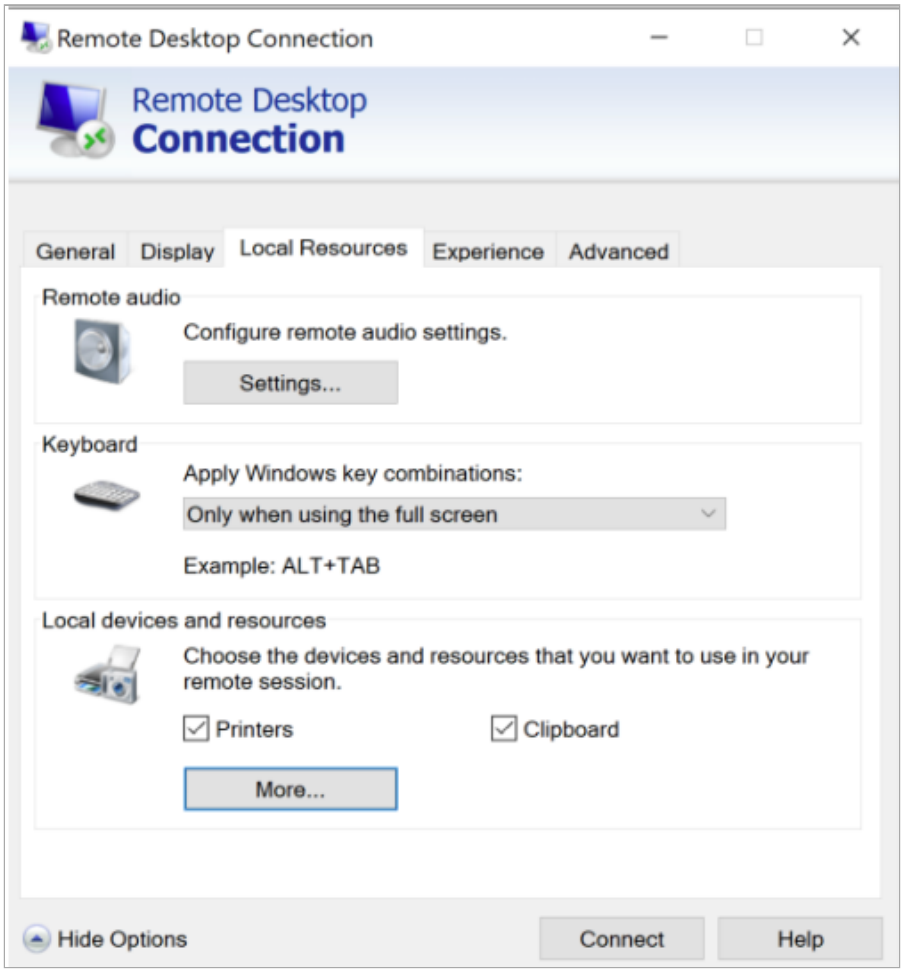
8. Edit **Device and Resource Redirection**.
9. Under **Device and Resource Redirection**:
    - Set **Do not allow smart card device redirection** to **Disabled**.
    - Set **Do not allow supported Plug and Play device redirection** to **Disabled**.
    - Set **Do not allow WebAuthn redirection** to **Disabled**.

    After making the changes to the group policy, propagate the changes to the computers in the domain.

Remote Desktop Connection settings

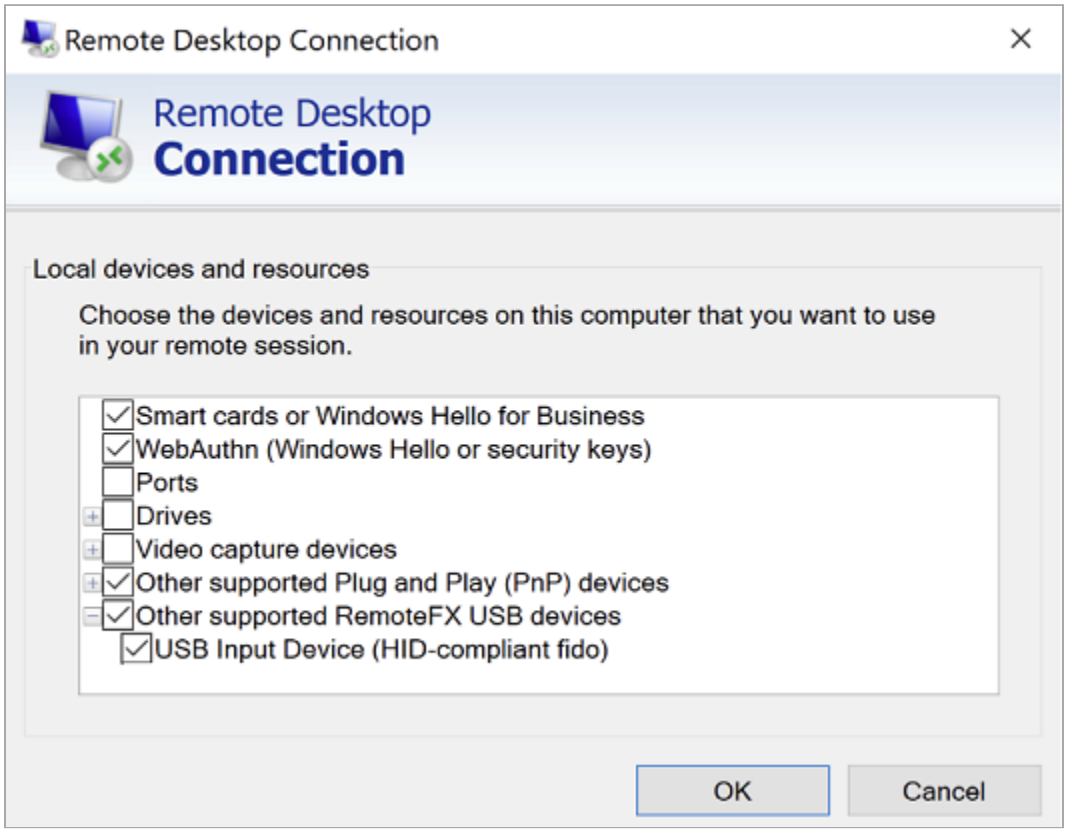
Verify that Remote Desktop resource redirection is configured properly:

1. Click the **More...** button on the **Local Resources** tab of the Remote Desktop Connection UI.



2. Select the security key listed under **Other supported RemoteFX USB devices**.

3. If you will be authenticating with an NFC-based security key, verify that **Smart cards or Windows Hello for Business** is selected.



Powershell script for setting up Windows Login - Passwordless

The script `Configure-Passwordless.ps1` can be used to quickly carry out the steps required to set up Windows Login - Passwordless. This can be useful for purposes such as informal testing or demos.

The script carries out the following steps:

- Creates and installs the CA certificate, also to the group policy
- Sets `externalId` to be a unique attribute
- Creates the authentication policy
- Creates and configures the passwordless Windows login application
- Creates a KDC certificate: request creation, issuing of certificate from request, installation of certificate

You can download the script here.

Troubleshooting passwordless Windows login

Try these troubleshooting steps if you encounter any issues with passwordless Windows login.

Check the log files

You can review the information that is recorded in the log files and the event information that is displayed in the Audit window in PingOne.

- You can find detailed activity information regarding Windows Login - Passwordless in the log files that are located in the `/logs` folder below the folder that you specified during installation (default location is `C:\Program Files\Ping Identity\PingID\Windows Passwordless\logs`).
- To include a greater level of detail in the log files, carry out the following steps to set the logging level to DEBUG:

    1. Open the Registry Editor.
    2. Under HKEY_LOCAL_MACHINE\SOFTWARE\Ping Identity\PingId\WindowsPasswordless, add a new key of type *Dword32* called *LogLevel*.
    3. Set the value of the new key to 1.
    4. After making the change to the registry, restart the PingIDESVC service or restart the computer.

       To restore the logging level to INFO, change the value of the key to 0 and restart the PingIDESVC service or the computer.

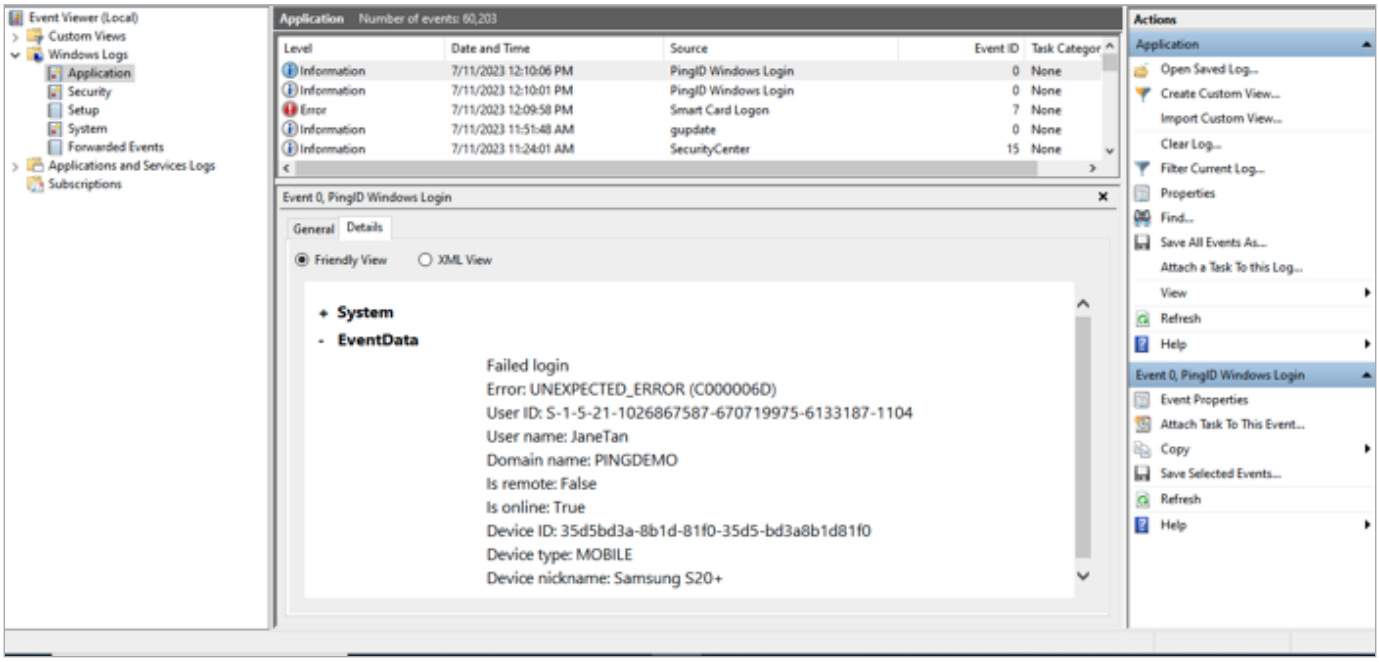
       > **Note**
       >
       > For some of the log files, there is no mechanism to limit the file size. So it's best not to leave the logging at DEBUG level for an extended period of time.

- The **Audit** window in PingOne includes information on events such as certificate creation and user authentication (Learn more in the PingOne help Audit section).

Check Windows Event Viewer

View user information related to Windows login passwordless events, including online and offline authentication, failed login attempts, and RDP authentication attempts in Windows Event Viewer.

1. Open Windows Event Viewer.
2. Go to **Windows Logs → Application**.



Windows login passwordless events are listed in the **Source** column as `PingID Windows login`.

Check for certificate configuration errors

If you encounter errors related to certificate configuration, carry out the following steps to try to identify the problem:

> **Note**
>
> In the steps below, it is assumed that the installation folder used for the PingID integration is `C:\Program Files\Ping Identity\PingID\Windows Passwordless`. If your installation folder is different, update the paths accordingly.

1. Open the `.cer` file to check whether the certificate is valid:
    1. Look in the folder `C:\Program Files\Ping Identity\PingID\Windows Passwordless\Certificates` and find the subfolder that is composed of letters and numbers, such as 19-92-6E-C6-01-A1-40-0E-63-B7-A1-BB-C3-E0-D1-75-85-00-49-4B-53-A2-E7-9F-15-E0-75-AD-20-0C-B4-F0.
    2. In the subfolder, you'll see a file called `Certificate.cer`.
    3. Double-click the `.cer` file and go to the **Certification Path** tab. You can see the Certificate Status there.
2. Assuming the certificate is valid, open a command prompt and navigate to the folder containing the `.cer` file. Run the command:

    ```
    certutil.exe -verify -urlfetch Certificate.cer
    ```

    If the certificate is OK, the command should exit with the message:

    ```
    CertUtil: -verify command completed successfully
    ```

3. If the `certutil` command ran successfully, enable EventViewer logging for Security-Kerberos and the CAPI2:
    1. Run Event Viewer.
    2. In Event Viewer, select **Applications and Services Logs → Microsoft → Windows**.
    3. Below **Windows**, find **Security-Kerberos**, right-click it, and enable logging.
    4. Below **Windows**, find **CAPI2**, right-click it, and enable logging.
4. Try the passwordless log-in again, and then check for errors in Event Viewer. See if there are any Security-Kerberos errors (under **Applications and Services Logs → Microsoft → Windows → Security-Kerberos → Operational**) or CAPI2 errors (under **Applications and Services Logs → Microsoft → Windows → CAPI2 → Operational**).

PingID integration for Mac login

PingID integrates with Mac local login to allow organizations to better secure their server environments and end user Mac login, providing access only to authorized users. Authentication is possible using PingID's wide variety of authentication methods.

Requirements

Web access

For details about required web access, see PingID required domains, URLs, and ports.

Policy settings

Mac login might be subject to policy settings.

Mac operating system

PingID integrates with Mac OS versions 10.15 (Catalina), 11 (Big Sur), and 12.4 or higher (Monterey).

Processor architecture

The PingID integration with Mac login can be used with both Intel and Apple silicon.

> **Note**
>
> You should install the PingID integration for Mac login individually on each Mac machine requiring the PingID authentication service. After it has been installed on a Mac, all users of the machine must authenticate with PingID.

Support for PingID offline MFA

PingID integration for Mac login supports PingID offline multi-factor authentication (MFA).

> **Note**
>
> The PingID User Guide refers to offline MFA as manual authentication.

To use PingID offline MFA, you must have:

- PingID integration for Mac login on the protected Mac machine
- A paired mobile device with PingID mobile app 1.8+ installed on it

Important

- The PingID offline MFA solution for Mac login is based on the assumption that an employee won't have administrative permissions to the machine. Otherwise, the administrative permissions could be used to remove and bypass PingID.
- Users must go through online authentication the first time after installation and only then will they be able to perform offline authentication.
- To guarantee online authentication, the machine must have a network connection prior to completion of the login process.
- Repudiation of a user for a login: During offline logins, there are no server side logs for successful or unsuccessful authentications. Admins should export these logs from the local console app or from the log path, `/Library/Logs/PingIdentity`.

Installing the PingID integration for Mac login

You can install the PingID integration for Mac login with the UI wizard or with the command-line installation.

Note

If for some reason you decide to downgrade to an earlier version of the PingID integration with Mac login, you must completely remove the installed version and only then install the earlier version.

UI

Installing PingID integration for Mac login using UI wizard

Install PingID integration for Mac login through the user interface (UI).

Before you begin

> **Important**
>
> Adding any multi-factor authentication (MFA) is a procedure that carries the risk of being locked out of the machine.
>
> - Several verifications are done on the parameters supplied for the installation to minimize any locking. The PingID integration for Mac login permits recovery from a lockout scenario by restarting the machine in **Single User Mode**.
> - Ensure that the **remote login** option is enabled on the Mac to allow connection to the machine by Secure Shell (SSH).

To install the PingID integration, you must have:

- Administrator privileges on the target Mac machine.
- A copy of the organization's `pingid.properties` file. For instructions on how to download the relevant PingID properties file (with full or restricted permissions), see Managing the PingID properties file using SSH.

About this task

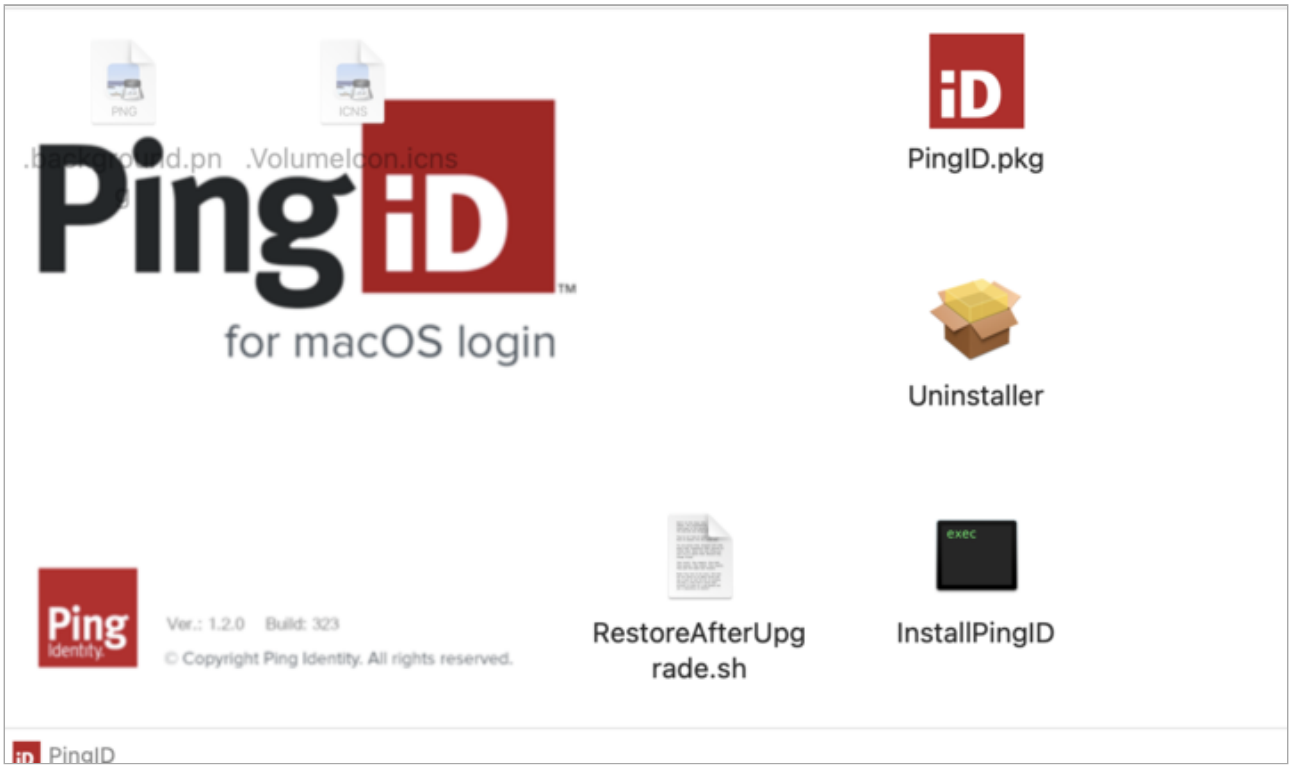
To install the PingID integration for Mac login using the UI wizard:

Steps

1. On the PingID Downloads page, go to **Integrations** and download the PingID package `.pkg` file for Mac login.
2. Double-click the `PingID-MacOS-Login<version>.dmg` file to launch the setup wizard.

   Result:

   The installer opens.



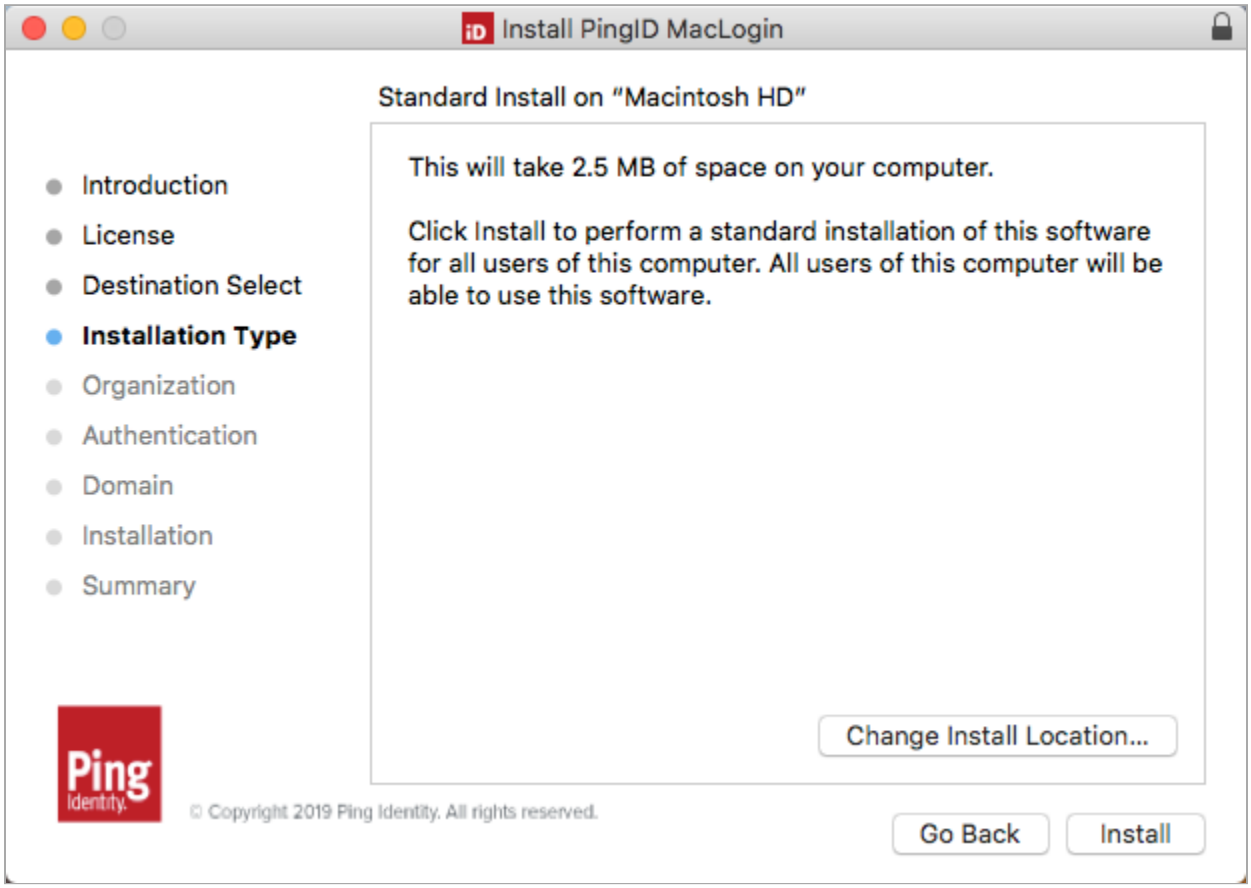
3. Double-click the **PingID.pkg** icon.
4. At the security check window, click **Continue**.
5. At the installer commencement window, click **Continue**.

   Result:

   The Software License Agreement window is displayed.
6. Review the Software License Agreement, click **Continue**, and when prompted, click **Agree**.

   Result:

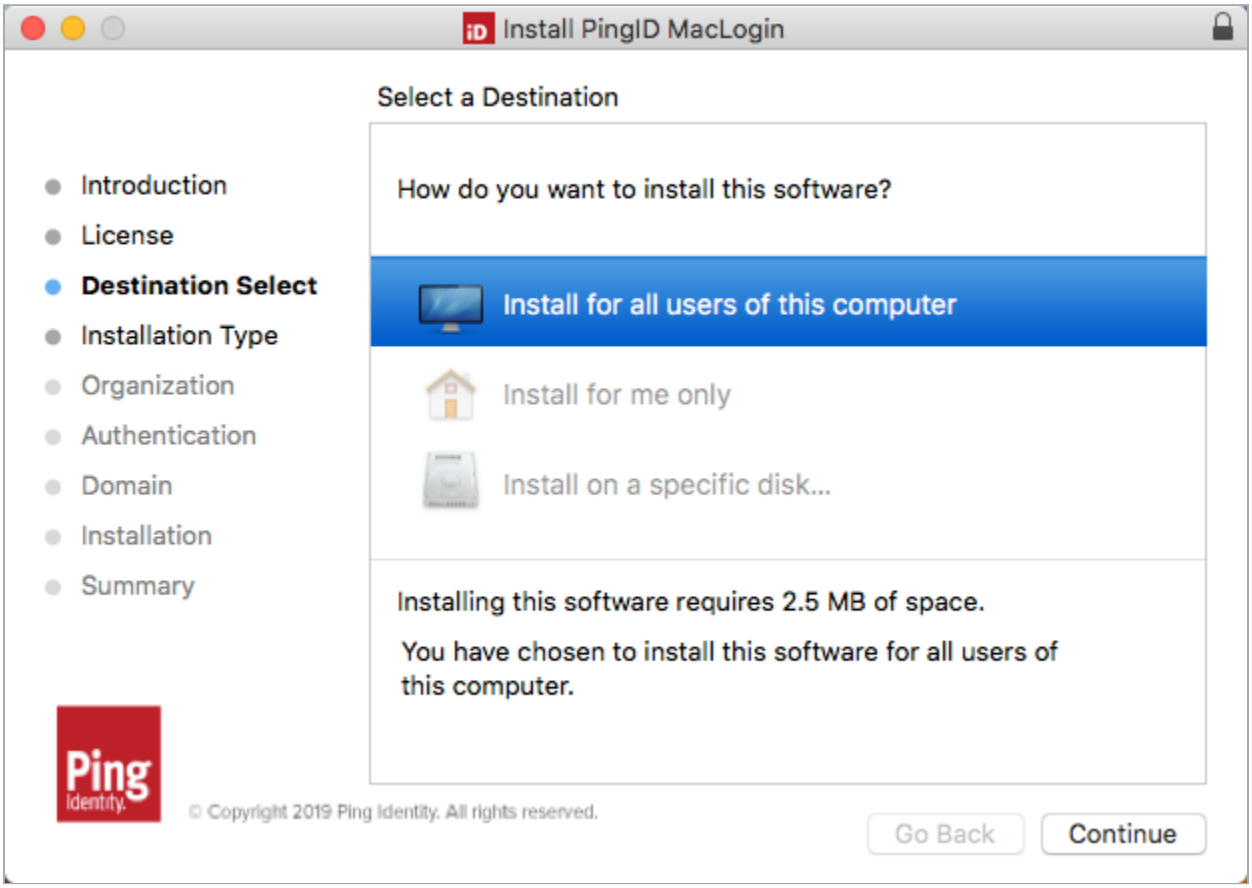
   The installation proper starts with the **Installation Type** window.



7. **Optional:** Click **Change Install Location**.

   Result:

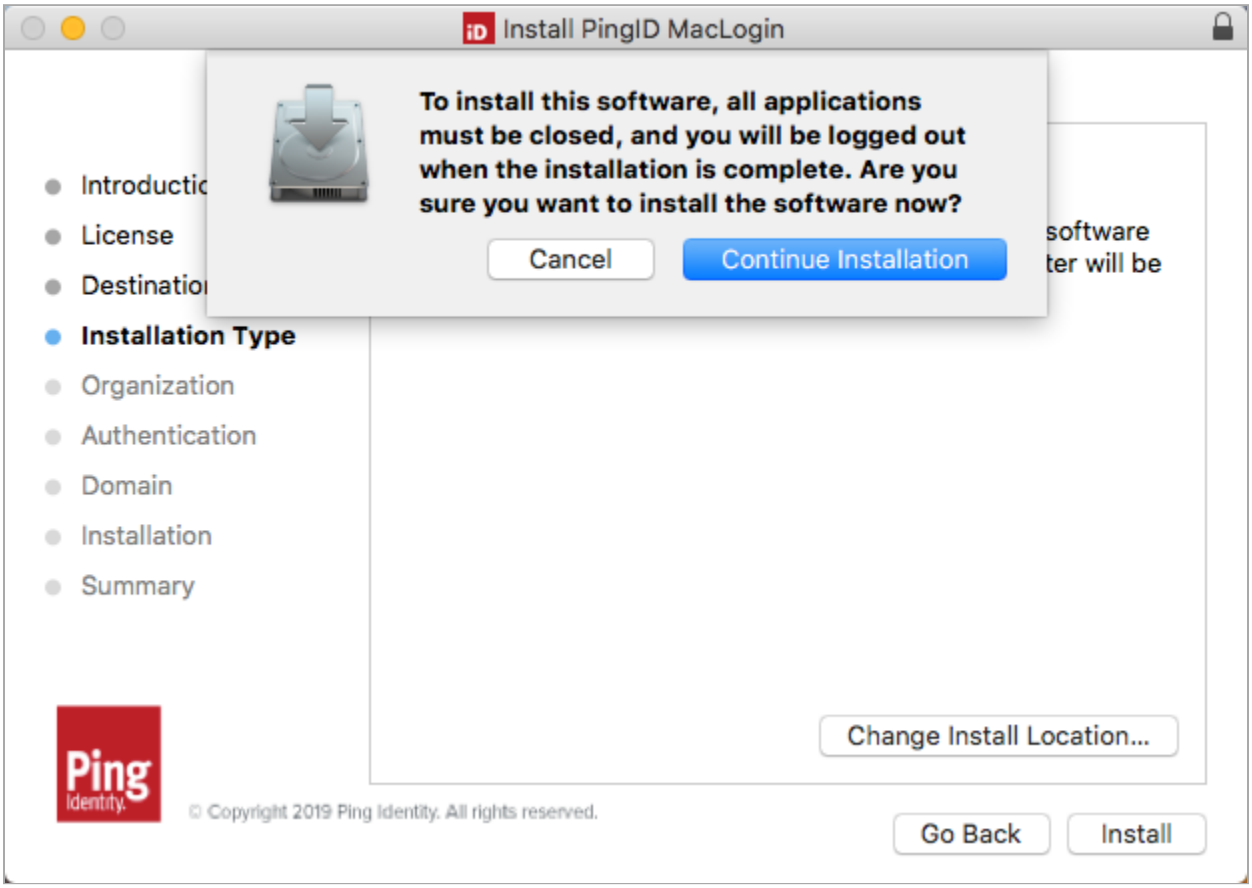
   The **Destination Select** window opens.



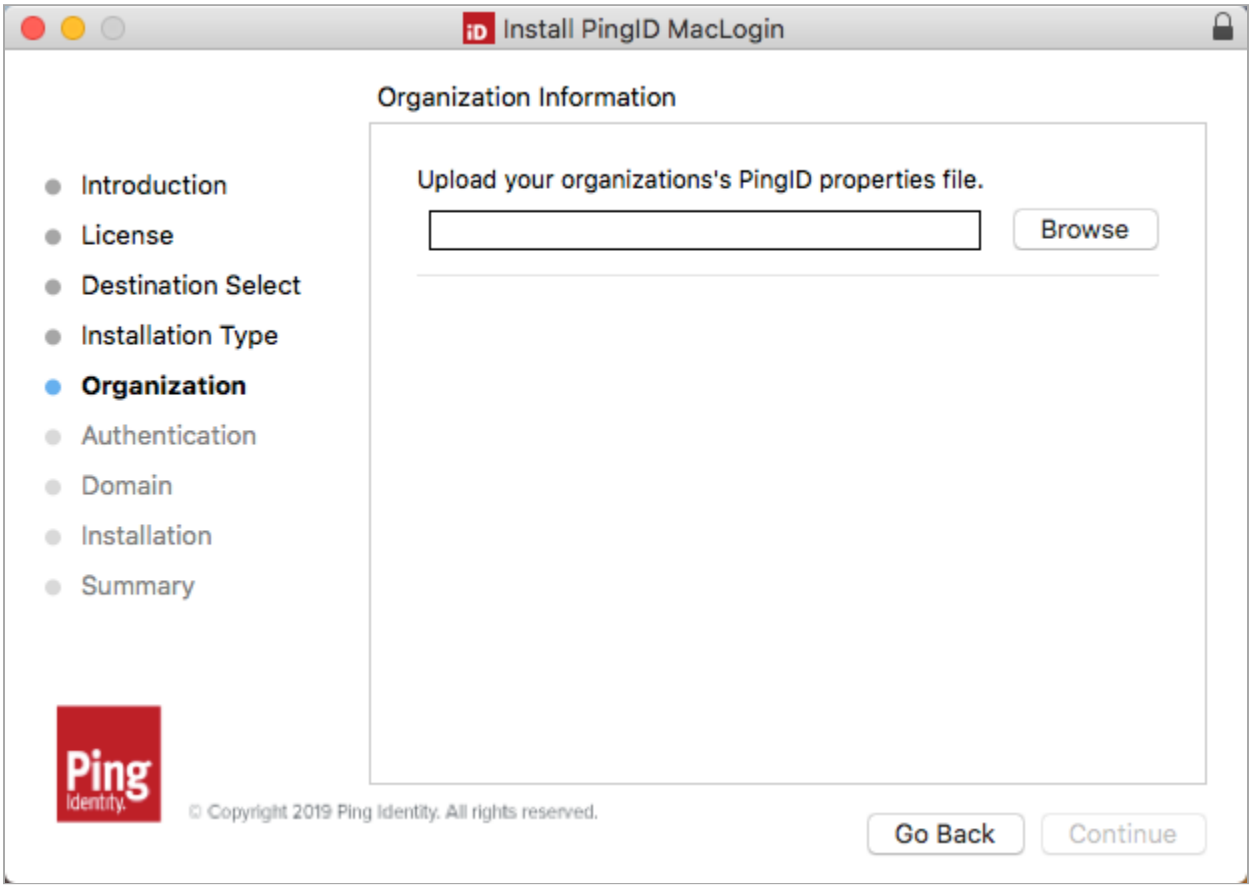
8. Keep the highlighted option unless there are compelling reasons for a different choice. Click **Continue** and then click **Install**.
9. If required, enter your machine user name and password.

   Result:

   You see the following caution message.



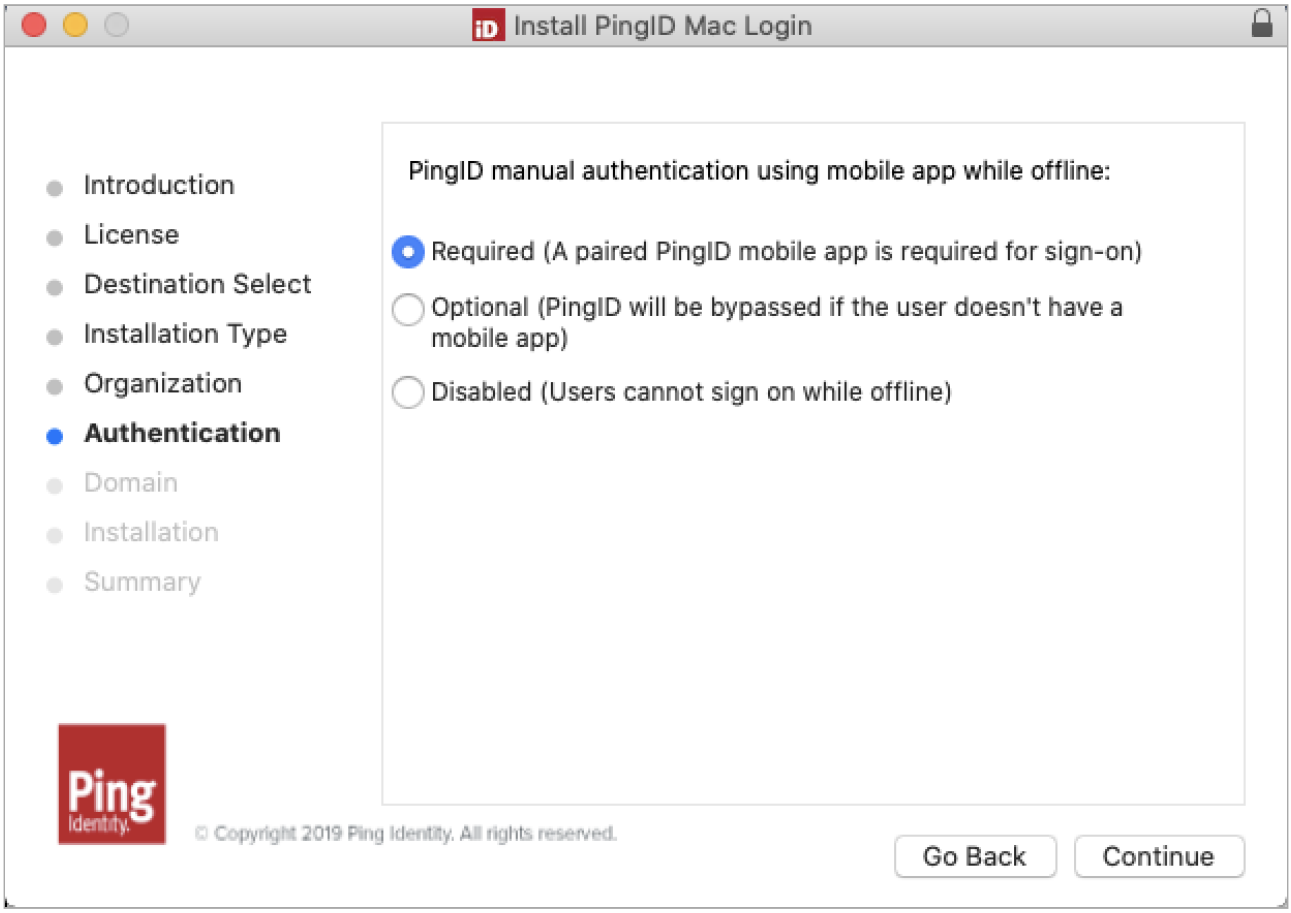
10. Click **Continue Installation**.
11. In the **Organization Information** pane, click **Browse**, and then select the `pingid.properties` file that you downloaded from the Admin portal. For more information, see Managing the PingID properties file for Windows and Mac login.



12. Click **Continue**.

    Result:

    The **Manual Authentication** window opens.



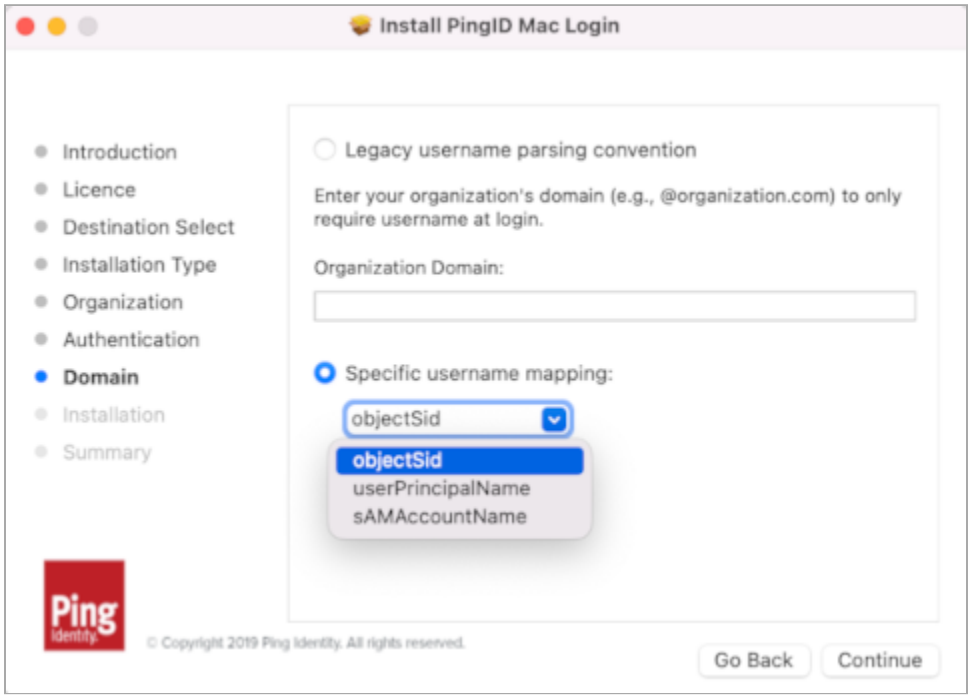
Choose the option to use for situations where the user cannot communicate with the PingID server:

- Required: User can use the PingID mobile app for offline access. If they do not have a paired mobile device, their access is blocked.
- Optional: User must use the PingID mobile app for offline access, but if they don't have a paired mobile device, MFA is bypassed.
- Disabled: Offline access is not permitted.

13. Click **Continue**.

    Result:

    The **The Domain / Username Mapping** window is displayed.



14. In the **Domain / Username Mapping** window, select **Specific username mapping** and choose one of the available Active Directory attributes to use for identifying users, or select the **Legacy username parsing convention** option.

    If you select **Legacy username parsing convention**, you can optionally provide the organization domain so that users can provide just their user name when logging in, for example, `john.smith`, rather than entering user name plus domain name, such as `john.smith@somewhere.com`.

    The domain format should be:

    - `@domainname`, such as `@somewhere.com`
    - Maximum of 50 characters
    - The string entered in this field is appended to the username during sign on

    By default, domain validation is carried out for the domain that you specify in the **Organization Domain** field. You can use the **Skip domain validation** option to specify that PingID should skip domain validation.

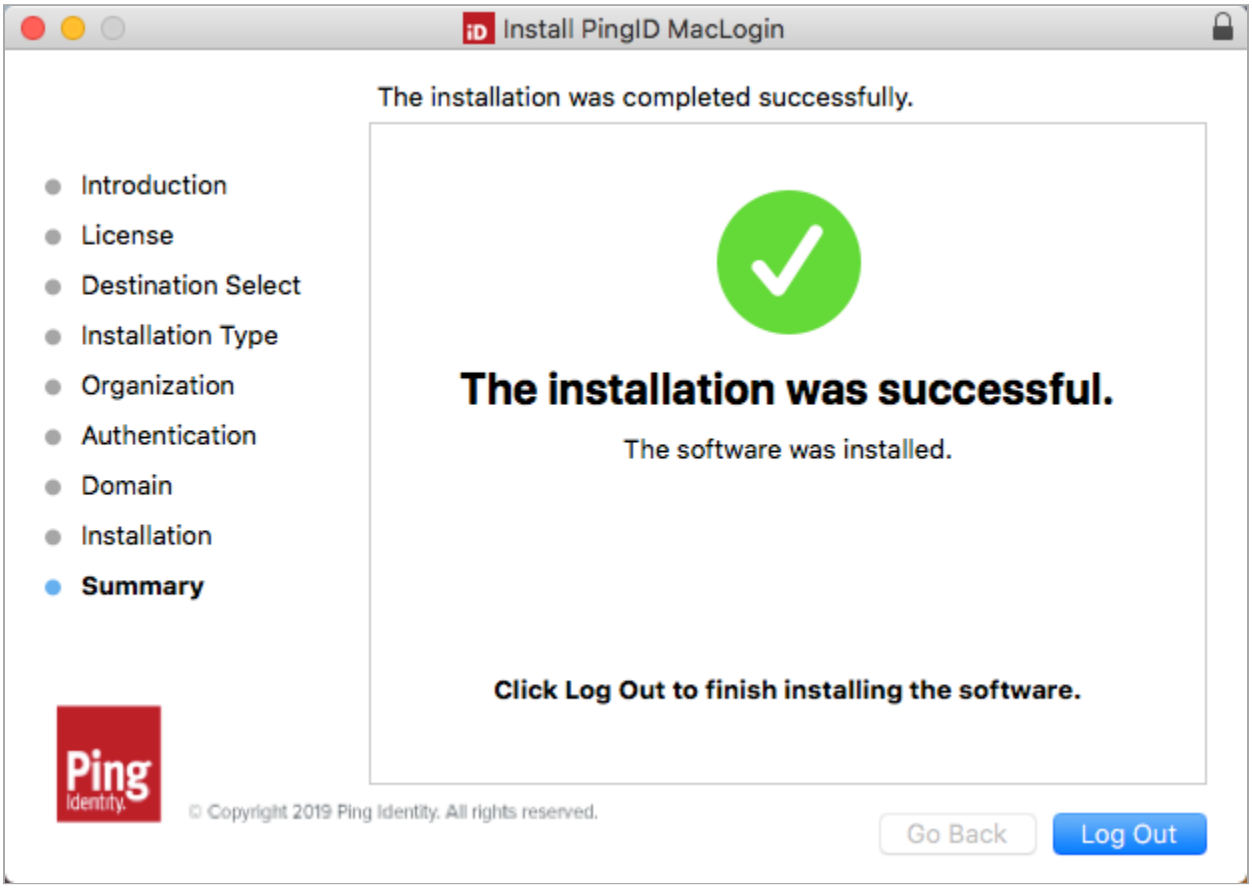
    > **Note**
    >
    > Because the username (plus domain name if set here) is sent to PingID for second factor authentication, it must precisely match a username entered through the admin portal. For PingID, user `john.smith` is not the same as `johm.smith@somewhere.com` even if the domain is correct.

15. Click **Continue**.

    If you changed anything in the previous step, you might be asked to enter your machine username and password.

    Result:

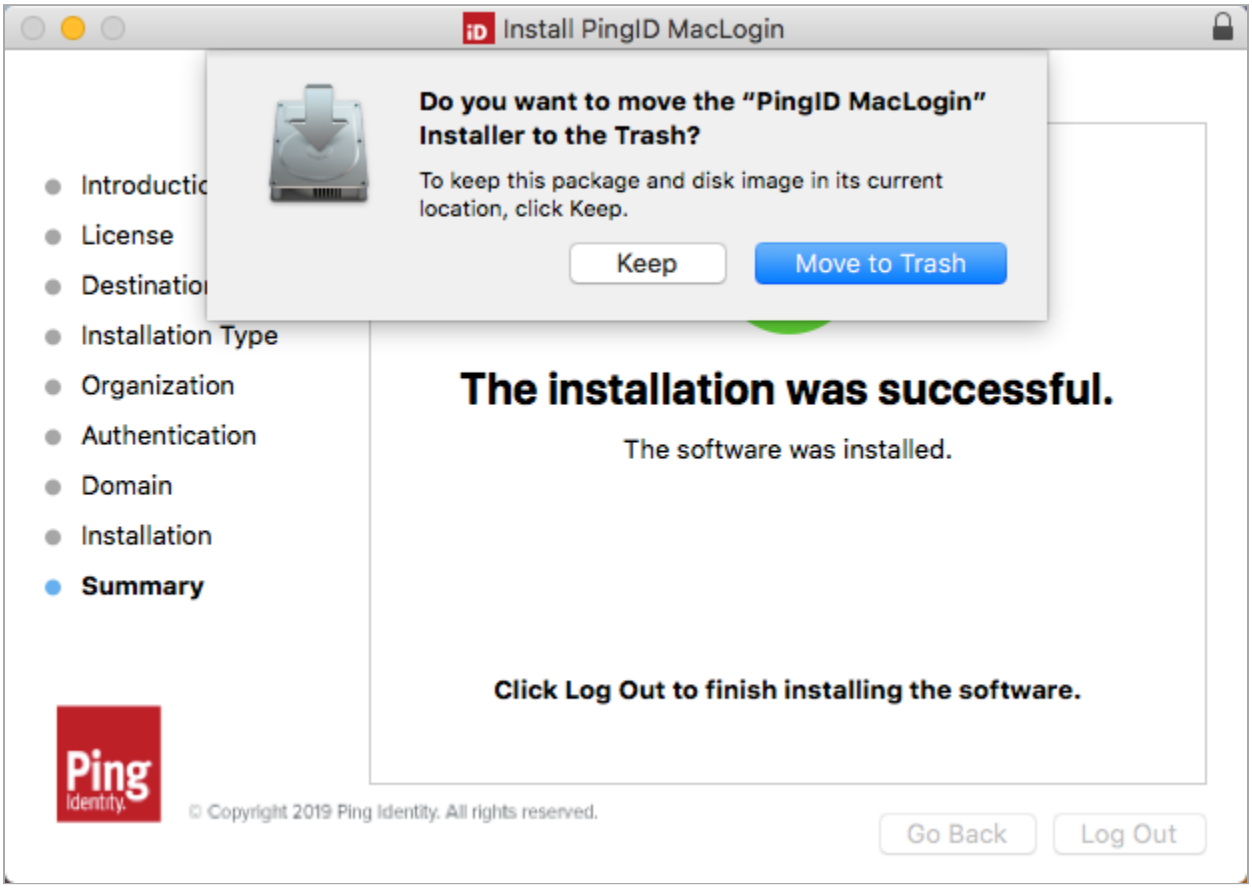
    When the installation is complete, you see the following window.



16. Click **Log Out**.

    Result:

    You are asked what to do with the installer package.



17. Decide whether to keep the installer package.

    The installer exits and the machine is logged out to apply the changes.

18. **Optional:** After successful installation, the downloaded `pingid.properties` file may be deleted from the Mac.

19. To verify the installation, test that a user can sign on to the Mac machine using the PingID integration for Mac login.

CLI

Installing PingID integration for Mac login using CLI

Install the PingID integration for Mac login using the command-line interface (CLI).

Before you begin

> **Important**
>
> Adding any multi-factor authentication (MFA) is a procedure that carries the risk of being locked out of the machine.
>
> - Several verifications are done on the parameters supplied for the installation to minimize any locking. The PingID integration for Mac login permits recovery from a lockout scenario by restarting the machine in **Single User Mode**.
> - Ensure that the **remote login** option is enabled on the Mac to allow connection to the machine by SSH.

To install the PingID integration, you must have:

- Administrator privileges on the target Mac machine.
- A copy of the organization's `pingid.properties` file. For instructions on how to download the relevant PingID properties file (with full or restricted permissions), see Managing the PingID properties file.

About this task

Installing the PingID integration from the command line is useful for deploying to multiple machines in batch mode.

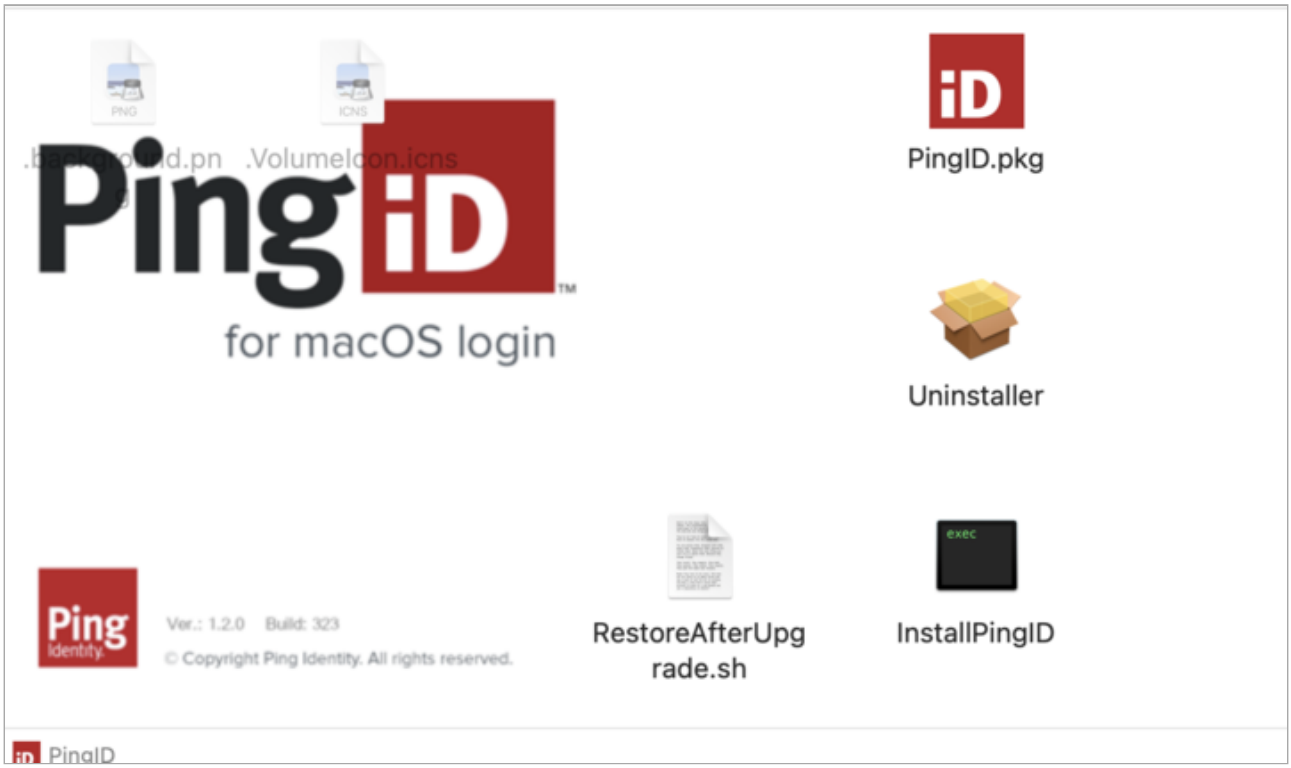
To install the PingID Integration for Mac login using the CLI:

Steps

1. On the PingID Downloads page, go to **Integrations**, and download the PingID package `.pkg` file for Mac login.
2. Double-click the **PingID-MacOS-Login<version>.dmg** file to launch the setup wizard.

   Result:

   The installer opens.



3. Copy and paste the `PingID.pkg` and `InstallPingID` files to a convenient location.
4. Download the PingID properties file to the location in step 3.
5. Open a terminal session and change directory to where you copied the file in step 3.
6. **Optional:** To see the available CLI help, run the `./InstallPingID --help` command.
7. Run the installation from a command prompt or create a script containing the required install command.

   Choose from:

   - Install using the `pingid.propertie`s file to supply parameter values.

     ```
     ./InstallPingID --orgSettingsFilePath /Users/admin/Downloads/pingid.properties [optional parameters]
     ```

   - Install without using the `pingid.properties` file. Supply the `--orgAlias`, `--orgKey`, `--authenticatorAddress`, `--idpUrl`, and `--token parameter` values on the command line.

     ```
     ./InstallPingID --orgAlias <organization alias string> --orgKey <organization key string> --authenticatorAddress <URL of PingID data center> --idpUrl <URL of the server used for PingID API requests> --token <API key identifier> [optional parameters]
     ```

CLI reference

Mac login command line reference

The following tables provide an overview of the command line commands you can use for the PingID integration for Mac login

== Running the installer from the CLI

The general command line is `./InstallPingID [options] [filepath_opt]`

Where:

`[filepath_opt]` takes the form `-p <PingID.pkg file path>` or `--package <PingID.pkg file path>`.

PingID properties

Parameter<Argument>	Description
`-f, --orgSettingsFilePath <Full pingid.properties filepath>`	The full file path of the PingID properties file. For example, `/Users/admin/Downloads/pingid.properties`. The PingID properties file is referenced from this location during the installation process. You must specify either: • `-f, --orgSettingsFilePath` OR all of the following parameters: • `-a, --orgAlias` • `-k, --orgKey` • `-u, --authenticatorAddress` • `--idpUrl` • `-t, --token` **Note** If any of the above parameters are specified, and `/orgSettingsFilePath` is also specified on the command line, then the values are retrieved from the `pingid.properties` file only, and the values of these other parameters specified on the command line are ignored.
`-a, --orgAlias <organization's alias string>`	The organization's alias. This value is an entry in the PingID properties file. If the `--orgSettingsFilePath` parameter is not specified, it is mandatory to provide the `--orgAlias` parameter. If both the `--orgSettingsFilePath` and `--orgAlias` are specified, the value is retrieved from the `pingid.properties` file, and the value of the `--orgAlias` parameter is ignored.

Parameter<Argument>	Description
`-k, --orgKey <organization key string>`	The organization's base64 key. This value is an entry in the PingID properties file. If the `--orgSettingsFilePath` parameter is not specified, it is mandatory to provide the `--orgKey` parameter. If both the `--orgSettingsFilePath` and `--orgKey` are specified, the value is retrieved from the `pingid.properties` file, and the value of the `--orgKey` parameter is ignored.
`-u, --authenticatorAddress <URL of PingID data center>`	The URL of the PingID data center to which the organization is associated. It is the URL that is listed on the line in the `pingid.properties` file that begins with `authenticator_url=`. If the `--orgSettingsFilePath` parameter is not specified, it is mandatory to provide the `--authenticatorAddress` parameter. If both the `--orgSettingsFilePath` and `--authenticatorAddress` are specified, the value is retrieved from the `pingid.properties` file, and the value of the `--authenticatorAddress` parameter is ignored.
`--idpUrl <URL of the server used for PingID API requests>`	The URL of the server used for PingID API requests. Take this value from the `idp_url` entry in the `pingid.properties` file. If the `--orgSettingsFilePath` parameter is not specified, you must provide the `--idpUrl` parameter. If both the `--orgSettingsFilePath` and `--idpUrl` parameters are specified, the value is retrieved from the `pingid.properties` file, and the value of the `--idpUrl` parameter is ignored.
`-t, --token <API key identifier>`	The identifier of the API key. This value is an entry in the PingID properties file. If the `--authenticatorAddress` parameter is not specified, it is mandatory to provide the `--token` parameter. If both the `--orgSettingsFilePath` and `--token` are specified, the value is retrieved from the `pingid.properties` file, and the value of the `--token` parameter is ignored.
`--usernameMapping <type>`	Use the `usernameMapping` parameter if you want to use an Active Directory attribute to identify users. Use one of the following values: • `UPN` - use the *userPrincipalName* attribute • `SAM` - use the *SamAccountName* attribute • `SID` - use the *objectSid* attribute • `None` - use the legacy username parsing convention `None` is the default value, so if you do not include the `usernameMapping` parameter, the legacy username parsing convention will be used.

Parameter<Argument>	Description
`--excludeLocalAccounts <value>`	Use the `excludeLocalAccounts` parameter to control whether PingID authentication should be applied to local user logins. • 0 - Use PingID authentication for local user logins as well • 1 - Do not use PingID authentication for local user logins
`-i, --ignoreConnectionErrors`	The installer attempts to address the PingID authenticator heartbeat to confirm connectivity. If there is no response before installing any of the elements, continue the installation.
`-s, --silent`	The installer will prompt with a **Log out now?** message box.
`-m, --very-silent`	The installer will sign out without asking.

Domain

Parameter<Argument>	Description
`-d, --domainPostfix <@organization domain name>`	Configures the installation to append the value supplied in this parameter to the username at sign-on time. **Note** You can define a suffix, such as @domain.com, but not a prefix, such as domain/. **Important** Enter the leading "@" before the domain name, for example `--domainPostfix @somewhere.com`. This parameter has a maximum length of 50 characters, including the leading "@".
`--skipDomainValidation`	By default, domain validation is carried out for the domain that you specify with the `--domainPostfix` option. You can use the `--skipDomainValidation` option to specify that PingID should skip domain validation.

Offline Authentication

Parameter<Argument>	Description
`-o, --offlineAuthType <type>`	The `--offlineAuthType` parameter specifies whether to allow PingID offline (manual) MFA. Possible values for *<type>* are: • 0: Allow offline MFA with the PingID mobile app. • 1: If the user does not have a paired PingID mobile app with their account, bypass MFA during login. • 2: Do not allow offline MFA.
`-r, --rsa_padding <none>`	By default, OAEP padding is used in the encryption for offline authentication. Use `--rsa_padding none` if you do not want to use OAEP padding for offline authentication.

HTTP Request Timeout

Parameter<Argument>	Description
`--timeout <ms>`	Defines HTTP request timeout value. Possible values are between 1000-30000 ms.

Common

Parameter<Argument>	Description
`-h, --help`	Show a user guide.
`-v, --version`	Show the Installer version.
`--allowFullPermissionsPropertiesFile`	If you include the `--allowFullPermissionsPropertiesFile` option during installation, PingID will allow you to use the full-permissions properties file (rather than the restricted-permissions properties file intended for use with Mac login). However, it is strongly recommended that you refrain from doing so. Using the full-permissions properties file with Mac login is a security risk (for details, see CVE-2022-23717).

Uninstalling the PingID integration for Mac login

You can uninstall the PingID integration for Mac login with the UI wizard or with the command-line installation.

UI

Uninstalling the PingID integration for Mac login using UI wizard

Uninstall the PingID integration for Mac login using the User Interface (UI) wizard.

Steps

1. Ensure that you have available the same `PingID-MacOS-Login<version>.dmg` file that you used to install PingID integration.

   For more information, see Installing PingID integration for Mac login using UI wizard, step 2.

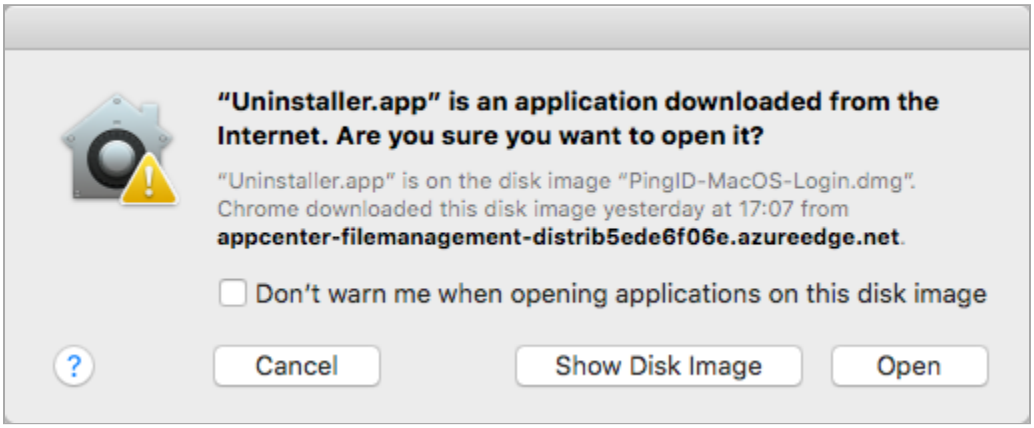
2. Double-click the `PingID-MacOS-Login<version>.dmg` file to launch the setup wizard.

   The installer opens.

3. Double-click the **Uninstaller.app** icon.

   Result:

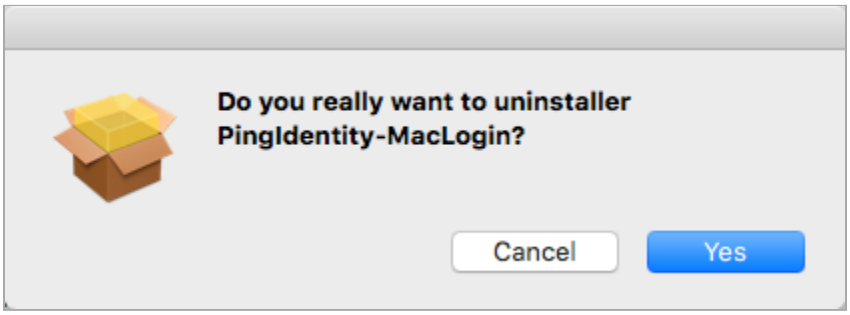
   You see a downloaded app warning.



4. Click **Open**.

   Result:

   You are asked to confirm the uninstall.



5. Click **Yes**.
6. If required, enter your machine user name and password.

   Result:

   As soon as you authenticate, the uninstall completes without further interaction.

CLI

Uninstalling the PingID integration for Mac login using the CLI

Uninstall PingID integration for Mac login using the command-line interface (CLI).

About this task

To uninstall the PingID integration, you must have administrator privileges on the relevant Mac machine.

Steps

1. Open a terminal window and type `cd /Library/Application\ Support/PingIdentity`
2. Enter the following command:

   ```
   sudo sh ./perform_uninstall.sh
   ```

3. Enter your admin user name and password.

   Result:

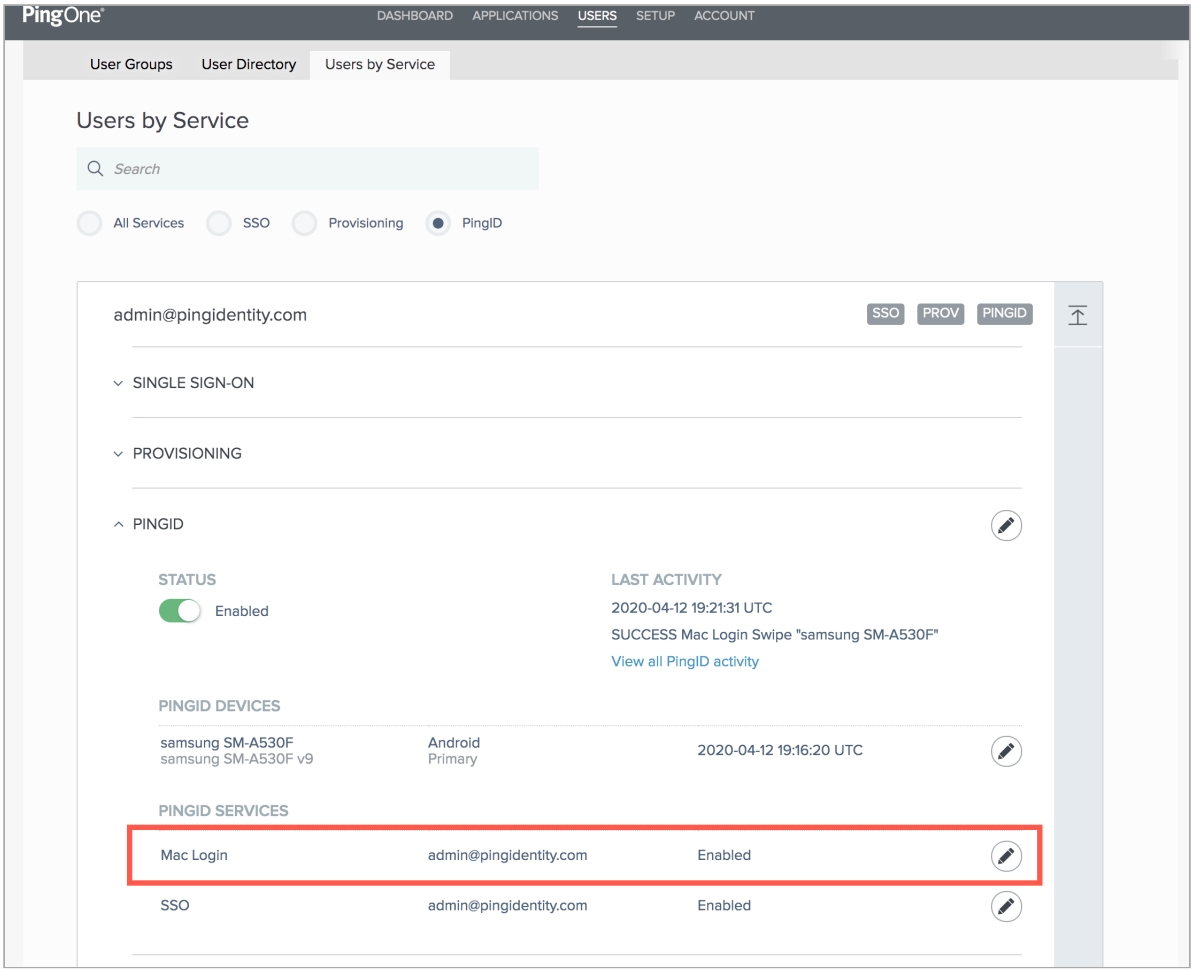
   The uninstall completes.

Managing users of PingID integration for Mac login

You can use the Users by Service page in the admin portal to manage the list of users of the PingID integration for Mac login.

Steps

1. In the admin portal, go to **Users → Users by Service**.
2. Select the user that you want to view.
3. Select the **PingID** tab.



Depending on the configuration of PingID integration for Mac Login authentications, the new entry in the red rectangle might appear in the user's **PingID Services** list. It indicates the PingID service for signing on to a local Mac machine.

All other user management and reporting functions are identical to those of other services.

Troubleshooting PingID integration for Mac login

The following describes possible issues with the PingID integration for Mac login and how to resolve them.

Lockout

If you are locked out of the Mac following the installation and you have a remote SSH connection or you have set the option to use Single User mode, you can run an uninstall script, `/Library/Application Support/PingIdentity/uninstall.sh`.

Mac user cannot complete second factor authentication

Ensure that the user's login name has been registered to PingID in the Admin portal identically to the Mac admin user name.

Mac user is blocked after installation

Online Authentication is required after installation. If the machine cannot reach the PingID service due to lack of an internet connection, ensure the machine can connect to the internet before the sign-on process is completed.

> **Note**
>
> Users must go through online authentication the first time after installation and only then can perform offline authentication.

Integrate PingID with AD FS

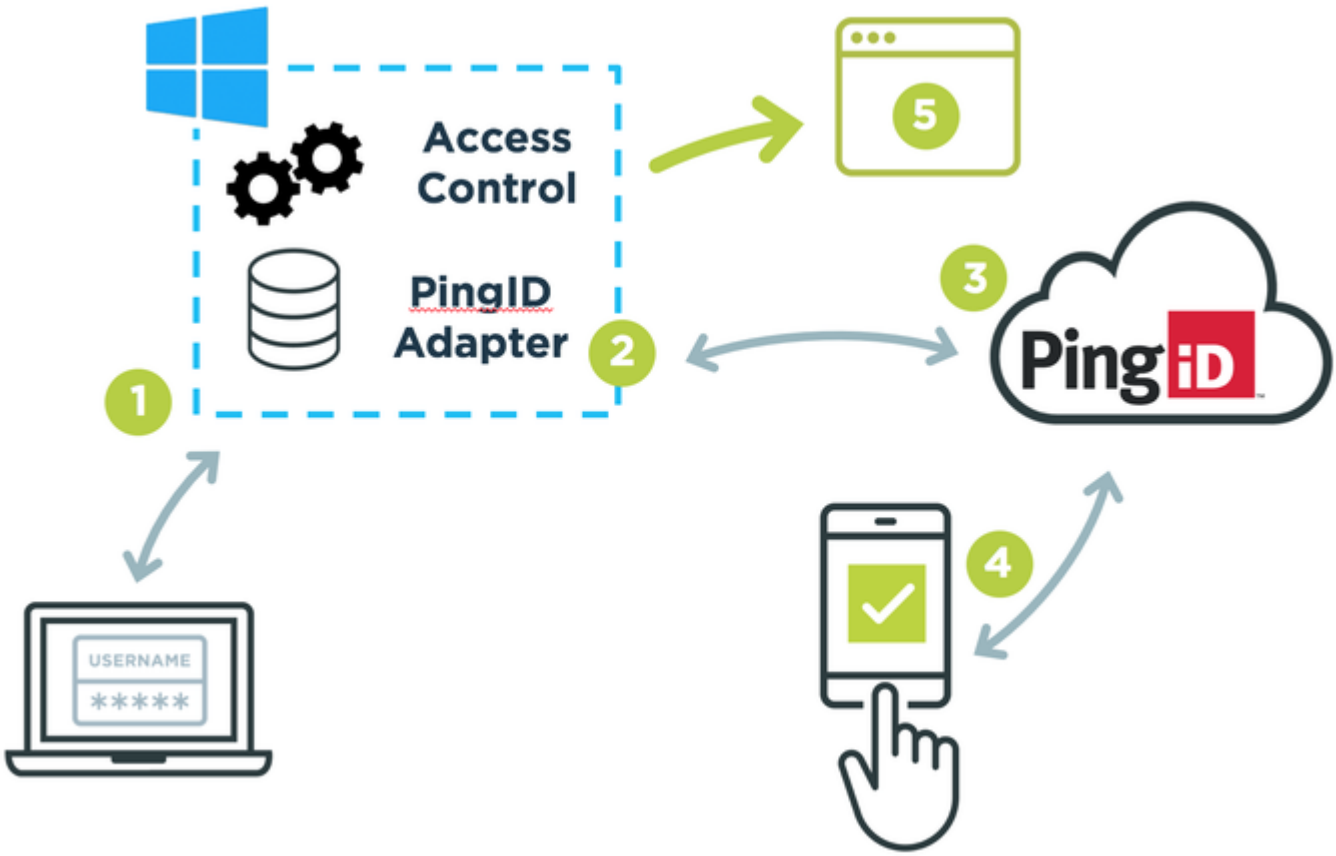
PingID MFA Adapter for AD FS enables multi-factor authentication (MFA) capabilities for users that are signing on using Microsoft Active Directory Federation Services (AD FS).

You can install the PingID MFA Adapter on a single AD FS instance. If you have an AD FS farm deployment, you must install PingID MFA Adapter on each AD FS instance in the farm to enable MFA.

PingID MFA Adapter for AD FS can query user data originating from multiple Active Directory domains, based on the user claim presented during authentication.

An AD FS app is available in the **Policy Apps** list. Use it to apply PingID authentication policies specific to AD FS MFA. For more information, see Configuring an app or group-specific authentication policy

The following figure demonstrates a typical user flow.



Processing steps

1. The user attempts to login to an application using their credentials. AD FS validates the user credentials against Active Directory.
2. The PingID adapter for AD FS initiates an MFA request to the PingID service in the cloud.
3. The PingID cloud service sends an MFA request to the user, as configured by their PingID policy.
4. The user authenticates using the configured authentication method, such as Swipe, Mobile App Biometrics, or YubiKey. The PingID cloud service redirects the user back to AD FS.
5. Using the SAML or OpenID Connect (OIDC) protocol, AD FS authorizes the Service Provider to grant access to the user.

For more information on getting started with PingID for AD FS, see Installing PingID MFA Adapter for AD FS and Enabling PingID as an MFA provider in AD FS.

Installing PingID MFA Adapter for AD FS

The PingID multi-factor authentication (MFA) Adapter for Microsoft Active Directory Federation Services (AD FS) is required to enable PingID for AD FS.

Before you begin

Make sure:

- You have installed AD FS 4.0 on Windows Server 2016 or AS FS 3.0 on Windows Server 2012 R2.
- You have installed .NET 4.6 or later.
- Port 443 is open to allow outbound communication with the PingID service. For further details about required URLs, see PingID required domains, URLs, and ports.
- PingID integration for AD FS employs redirects and cross-site requests. Changes to cookie behavior implemented by browsers, such as Google Chrome v80, can cause disruptions to authentication flows. To ensure changes to cookie behavior do not cause disruptions to your authentication flows, make sure your AD FS servers have the latest SameSite cookie support updates from Microsoft. For information about the SameSite cookie changes introduced in Chrome v80, and details on how to upgrade your server, see this Microsoft support article.

About this task

Important

This operation involves restarting the AD FS service. After the installation is complete, you must select the PingID MFA Adapter as an MFA method in AD FS.

Note

If you have another MFA provider installed on your AD FS instance, but it is not configured correctly, you might not be able to install PingID MFA Adapter for AD FS and might receive an error when running the PingID MFA installer. We recommend that you disable any existing MFA authentication methods that you are not using before you install the PingID Adapter for AD FS.

Steps

1. In the PingOne admin portal, go to **Setup → PingID → Client Integration**.
2. In the **Integrate with PingFederate and Other Clients** section, click **Download** to download the `pingid.properties` file.
3. On the PingID Downloads page, go to **Integrations**, and download and extract the **PingID MFA Adapter for AD FS** file.
4. To launch the setup wizard, run `PingIdAdfsAdapter<version>.exe`.
5. When the wizard launches, click **Next**.
6. Review the Software License Agreement, click **I accept the agreement**, and then click **Next**.
7. Click **Browse**, and then navigate to the `pingid.properties` file that you downloaded from the admin portal.
8. Select the claim type that should be passed to the MFA adapter, and then click **Next**.

   PingID MFA adapter for AD FS supports the following claim types.

Claim Type	Description	URI
UPN	The user principal name (UPN) of the user, in the format `user@domain.com`	`http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn`
Windows account name	The Windows Account Name of the user in the in the format `DOMAIN\USER`	`http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname`

> **Note**
>
> After the installation is complete, the claim type cannot be modified. For more information about claim types, see Microsoft's documentation on The role of claims.

> **Note**
>
> Assess your environment and decide which claim type fits your specific environment. You must consider the effect the claim type will have on your environment setup.
> For example, if you have a split DNS implementation, where the UPN carries the external domain name, and the `WindowsAccountName` carries the internal domain name, you must use the `WindowsAccountName` claim type for the MFA Adapter. If you use the UPN claim type instead, the MFA Adapter attempts to locate the external domain name as an AD domain that does not exist and fails to retrieve the user from the AD.

9. If you want to change the destination folder, click **Browse** and navigate to the relevant location, otherwise click **Next**.
10. Click **Install**.

    Result:

    After the installation finishes, the path to the installation log is displayed. The installation log provides additional information about the installation.

11. Click **Next**, and then click **Finish**.

Next steps

After the adapter is installed, enable PingID as an MFA provider. For more information, see Enabling PingID as an MFA provider in AD FS.

Installing PingID MFA Adapter for AD FS using the CLI

Use the command-line interface (CLI) to install and register the PingID multi-factor authentication (MFA) Adapter for Microsoft Active Directory Federation Services (AD FS).

Before you begin

Make sure:

- You have installed AD FS 4.0 on Windows Server 2016 or AS FS 3.0 on Windows Server 2012 R2.
- You have installed .NET 4.6 or later.
- Port 443 is open to allow outbound communication with the PingID service. For further details about required web access, see PingID required domains, URLs, and ports.
- PingID integration for AD FS employs redirects and cross-site requests. Changes to cookie behavior implemented by browsers, such as Google Chrome 80, can cause disruptions to authentication flows. To ensure changes to cookie behavior do not cause disruptions to your authentication flows, make sure your AD FS servers have the latest SameSite cookie support updates from Microsoft. For information about the SameSite cookie changes introduced in Chrome 80 and details on how to upgrade your server, see this Microsoft support article.

Important

This operation involves restarting the AD FS service. After the installation is complete, you will need to select the PingID MFA Adapter as an MFA method in AD FS.

Note

If you have another MFA provider installed on your AD FS instance, but it is not configured correctly, you may not be able to install PingID MFA Adapter for AD FS and may receive an error when running the PingID MFA installer. To avoid potential software conflicts, we recommend that you disable any unused MFA authentication methods before you install PingID Adapter for AD FS.

Steps

1. In the PingOne admin portal, go to **Setup → PingID → Client Integration**.
2. To download the `pingid.properties` file, in the **Integrate with PingFederate and Other Clients** section, click **Download**.
3. On the PingID Downloads page, go to **Integrations**, and download and extract the file for **AD FS**.
4. Open a command prompt and run the following:

```
PingIdAdfsAdapter<version>.exe /p=[full-path-to-properties-file]
/ct=[claim-type-uri] [/SILENT | VERYSILENT] [/SUPPRESSMSGBOXES] [/AcceptTerms]
```

Where:

Switch	Description
`/p=[full-path-to-properties-file]`	The path to the pingid.properties file that you downloaded from the admin portal.
`/ct=[claim-type-uri]`	The claim type URI. For more information, see the following Claim Type table.
`/SILENT`	Hide the install wizard window and show the installation progress window.
`/VERYSILENT`	Hide the install wizard window and the installation progress window.
`/SUPPRESSMSGBOXES`	Suppress message boxes during installation. This switch only has an effect when combined with `/SILENT` or `/VERYSILENT`.
`/AcceptTerms`	Suppress message boxes and silently accept the terms of PingID installation.

PingID MFA Adapter for AD FS supports the following claim types.

Claim Type	Description	URI
UPN	The user principal name (UPN) of the user, in the format `user@domain.com`	`http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn`
Windows account name	The Windows Account Name of the user in the in the format `DOMAIN\USER`	`http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname`

Note

After the installation is complete, the claim type cannot be modified.
Assess your environment and decide which claim type fits your specific environment. You must consider the effect the claim type will have on your environment setup.
For example, if you have a split DNS implementation, where the UPN carries the external domain name, and the `WindowsAccountName` carries the internal domain name, you must use the `WindowsAccountName` claim type for the MFA Adapter. If you use the UPN claim type instead, the MFA Adapter attempts to locate the external domain name as an AD domain that does not exist, and fails to retrieve the user from the AD.
For more information about claim types, see Microsoft's documentation on The role of claims.

Upgrading PingID MFA adapter for AD FS

Upgrade the PingID multi-factor authentication (MFA) Adapter for Microsoft Active Directory Federation Services (AD FS).

About this task

To upgrade PingID MFA Adapter, you must already have a working version of PingID MFA Adapter for AD FS installed on your machine. For more information, see Installing PingID MFA Adapter for AD FS.

> **Important**
>
> This operation involves restarting the AD FS service. Once the upgrade is complete, select the PingID MFA Adapter as an MFA method in AD FS.

> **Note**
>
> If you have another MFA provider installed on your AD FS instance, but it is not configured correctly, you may not be able to upgrade PingID MFA Adapter for AD FS and may receive an error when running the PingID MFA installer. To avoid potential software conflicts that could prevent proper installation, we recommend that you disable any existing MFA authentication methods that are not used before you install PingID Adapter for AD FS.

Steps

1. On the PingID Downloads page, go to **Integrations**, and download and extract the file for **AD FS**.
2. To launch the setup wizard, run `PingIdAdfsAdapter<version>.exe`.
3. When the wizard launches, click **Next**.
4. Review the Software License Agreement, click **I accept the agreement**, and then click **Next**.
5. Click **Install**.

   Result:

   After the installation finishes, the path to the installation log is displayed. The installation log provides additional information about the installation.
6. Click **Next**, and then click **Finish**.

Next steps

After the adapter is upgraded, enable PingID as an MFA provider. For more information, see Enabling PingID as an MFA provider in AD FS.

Upgrading PingID MFA Adapter for AD FS using the CLI

Use the command-line interface (CLI) to upgrade the PingID multi-factor authentication (MFA) Adapter for Microsoft Active Directory Federation Services (AD FS)

About this task

To upgrade PingID MFA Adapter, you must already have a working version of PingID MFA Adapter for AD FS installed on your machine. For more information about installing PingID MFA Adapter, see Installing PingID MFA Adapter for AD FS using the CLI.

Important

This operation involves restarting the AD FS service. Once the installation is complete, you will need to select the PingID MFA Adapter as an MFA method in AD FS.

Note

If you have another MFA provider installed on your AD FS instance, but it is not configured correctly, you may not be able to upgrade PingID MFA Adapter for AD FS and may receive an error when running the PingID MFA installer. . To avoid potential software conflicts that could prevent proper installation, we recommend that you disable any existing MFA Authentication methods that are not used before you install PingID Adapter for AD FS.

Steps

1. Go to the PingID Downloads page, and from the **Integrations** section, download the **PingID MFA adapter for AD FS**.
2. Open a command prompt and run the following.

```
PingIdAdfsAdapter<version>.exe [/SILENT | VERYSILENT] [/SUPPRESSMSGBOXES] [/AcceptTerms]
```

Where:

Switch	Description
/SILENT	Hide the install wizard window and show the installation progress window.
/VERYSILENT	Hide the install wizard window and the installation progress window.
/SUPPRESSMSGBOXES	Suppress message boxes during installation. This switch only has an effect when combined with /SILENT or /VERYSILENT.
[/AcceptTerms]	Suppress message box and silently accept terms of the PingID installation.

Enabling PingID as an MFA provider in AD FS

The process of enabling PingID as a multi-factor authentication (MFA) provider in Microsoft Active Directory Federation Services (AD FS) varies slightly between AD FS 4.0 and 3.0. The process for each is described in the following sections.

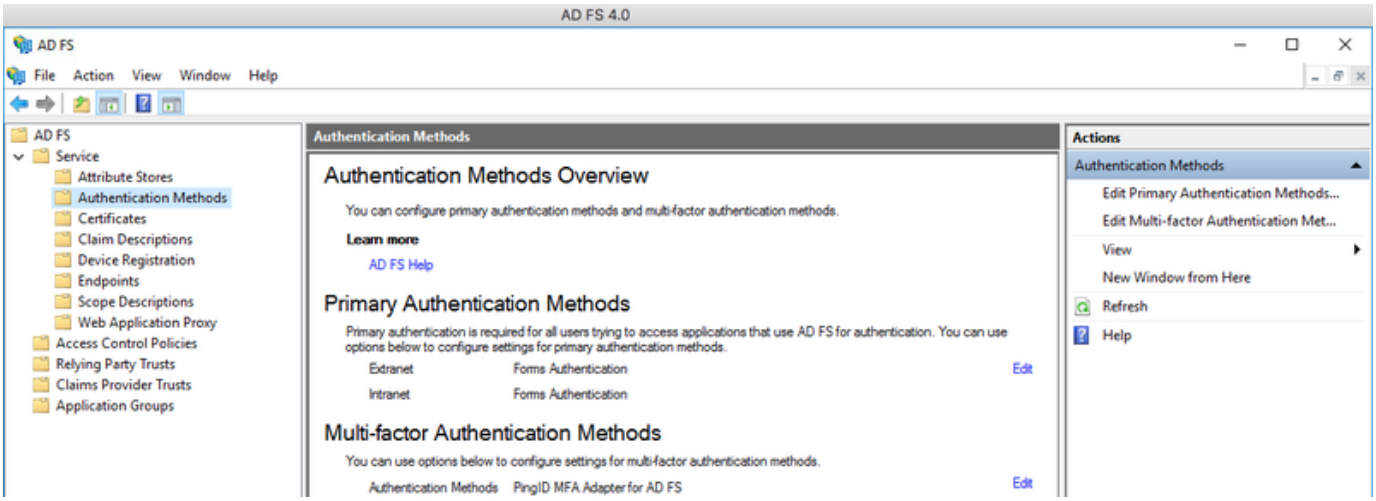
Enabling PingID as an MFA provider in AD FS 4.0

After installing the PingID MFA Adapter, enable it as the MFA provider for AD FS 4.0.

Steps

1. In Windows, open **Server Manager** and go to **Tools → AD FS Management → AD FS → Service → Authentication Methods**.

2. From the **Actions** menu, select **Authentication Methods**, and then click **Edit Multi-factor Authentication Methods**.



Result:

The **Edit Authentication Policy** window opens.

3. In the **Multi-factor**tab, select **PingID MFA Adapter for AD FS**, then click **OK**.

Result

PingID MFA is applied to the AD FS login process, according to the policy and general configurations of AD FS.

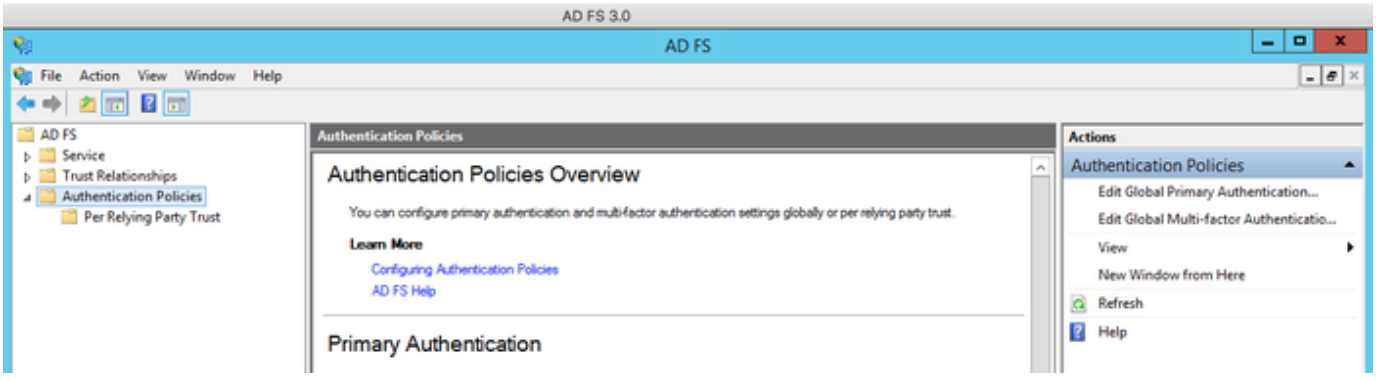
Enabling PingID as an MFA provider in AD FS 3.0

After installing the PingID MFA Adapter, enable it as the MFA provider for AD FS 3.0.

About this task
Steps

1. In Windows, open **Server Manager** and go to **Tools → AD FS Management → AD FS → Authentication Policies**.

2. From the **Actions** menu, select **Authentication Policies**, and then click **Edit Global Multi-factor Authentication Methods**.



3. On the **Multi-factor** tab, select **PingID MFA Adapter for AD FS**, and then click **Apply**.

Result

PingID MFA is applied to the AD FS login process, according to the policy and general configurations of AD FS.

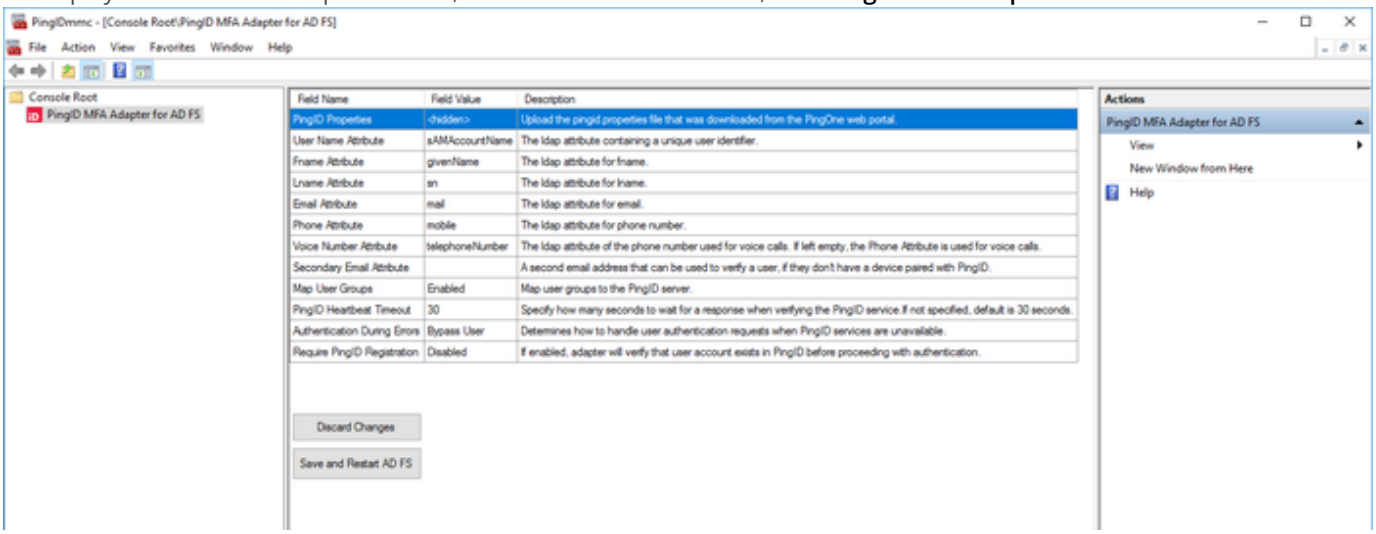
Configuring advanced settings

Configure optional advanced settings for PingID MFA Adapter for AD FS.

About this task

Steps

1. In the Microsoft Management Console, go to **File → Add/Remove Snap-in**.
2. If the PingID MFA Adapter for AD FS folder is not shown under the **Console Root** folder, in the **Available snap-ins** section, select **PingID MFA Adapter for AD FS** and click **Add** and then click **OK**.
3. To display a list of advanced parameters, in the **Console Root** folder, click **PingID MFA Adapter for AD FS**.



4. Double-click the attributes you want to change and enter the relevant value.

Attribute	Description
`PingID Properties`	Go to the `pingid.properties` file, and click **Open**. If you have not yet configured the PingID service, see Configure the PingID service for instructions.
`User Name Attribute`	The name of the user name attribute that will be mapped to the PingID user name value , such as `sAMAccountName` . The value of this attribute must be unique for each user identity.
`Fname Attribute`	The LDAP attribute containing the user first name.
`Lname Attribute`	The LDAP attribute containing the user last name.
`Email Attribute`	The LDAP attribute containing the user email address. This email address is used during registration if users need to receive a link on their mobile device to download the PingID application.

Attribute	Description
`Phone Attribute`	The LDAP attribute of the phone number used for SMS messages, as well as voice calls if the **Voice Number attribute** is left empty. **Note** This attribute must use the Google Library format, which dictates that all phone numbers must include '+', as well as the international country code.
`Voice Number Attribute`	The LDAP attribute of the phone number used for voice calls. If left empty, the Phone Attribute is used for voice calls. **Note** This attribute must use the Google Library format, which dictates that all phone numbers must include '+', as well as the international country code.
`Secondary Email Attribute`	A second email address that can be used to verify a user if they don't have a device paired with PingID.
`Map User Groups Attribute`	Determine whether to map user groups to enable the PingID server to evaluate group-based policy during authentication. Select either: ◦ **Enable**: User group information is sent to the PingID server. PingID group-based polices are evaluated during authentication. ◦ **Disable**: User group information is not to the PingID server. PingID group-based polices are not evaluated during authentication. **Note** For information on configuring a group-based policy, see PingID policy settings. The LDAP attribute for group membership (e.g. `memberOf`).
`PingID Heartbeat Timeout`	Time to wait for a response when verifying the PingID and PingOne services. If a value is not specified, the default is 30 seconds.

Attribute	Description
`Authentication During Errors`	Determines how to handle user authentication requests when PingID services are unavailable. Allowed values are: ◦ **Bypass User**: Accept the user's first factor authentication, and bypass the PingID MFA flow when the PingID MFA service is unavailable. ◦ **Block User**: Reject and block the user's login attempt when the PingID MFA service is unavailable.
`Require PingID Registration`	If enabled, requires that users are registered with PingID and verify their registration prior to authentication.
`Proxy URL`	If you want PingID to use a specific proxy, provide the URL here. The proxy URL format must be `http://`<server name or IP>:<port>. Https is not supported.
`Alternate Domain`	If the users belong to a domain that is not reflected in the login information provided, you can use this field to specify the relevant domain.

5. After you have configured all relevant attributes, click **Save and Restart AD FS**.

> **Caution**
>
> Modifying advanced settings requires you to restart the AD FS service. This might affect users that are using this instance of AD FS.

Result

Windows applies the configuration changes after restarting the AD FS service.

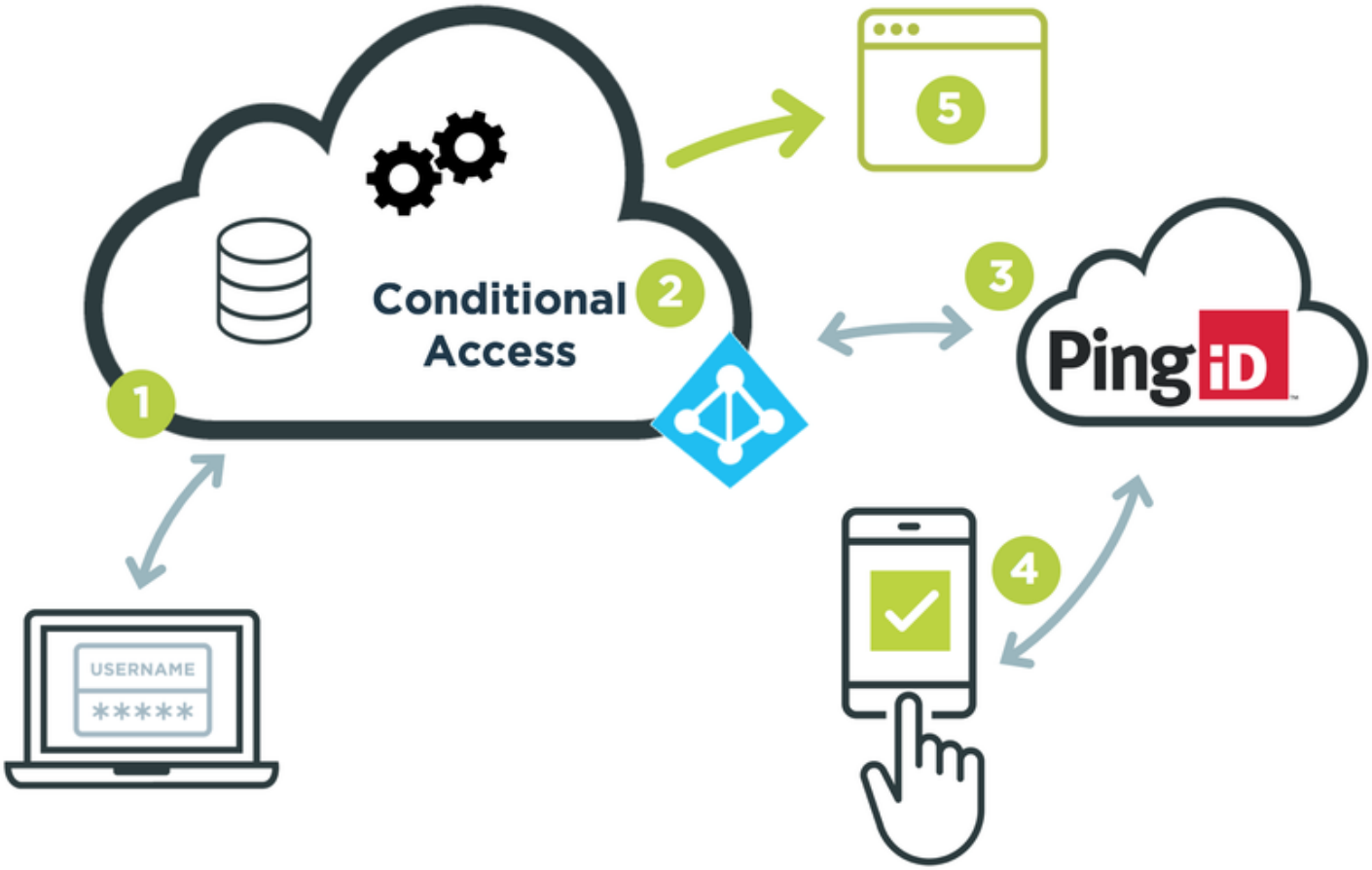
Next steps

To apply a PingID authentication policy to your AD FS integration, see Configuring an app or group-specific authentication policy). The AD FS app should appear in the PingID Policy app list.

Integrate PingID with Azure AD

PingID for Azure AD enables multi-factor enrollment and authentication capabilities for users who are authenticating using Azure Active Directory. PingID's detailed and flexible access policies also allow for the extension of the conditional access policies defined in Azure AD.

The following figure demonstrates a typical user flow.



1. The user attempts to login to an application using their credentials. Their credentials are validated against Azure Active Directory.
2. Azure evaluates the Conditional Access Policy, which indicates that a PingID custom control is protecting the application.
3. Azure redirects the user to the PingID service to perform multi-factor authentication.
4. PingID performs multi-factor authentication using the configured authentication method (e.g., Swipe, Mobile App Biometrics, YubiKey, etc.). Once the user has successfully authenticated, PingID returns a response to Azure indicating a successful completion of multi-factor authentication for that user.
5. Once all the Conditional Access Policy conditions are evaluated and complete, Azure authorizes the user's access to the target application.

Prerequisites and requirements

Confirm you have all prerequisites and requirements before configuring PingID integration for Azure AD.

To configure PingID integration for Azure AD, you will need:

- An Azure AD Premium P1 subscription with administrator rights
- A PingOne for Enterprise account with administrator rights

  For more information, see Registering a PingOne for Enterprise account.

If you have users who registered with PingID prior to setting up PingID integration for Azure AD, make sure you map the username to the same attribute that your PingID users were registered with, such as the `sAMAccountName` or `userPrincipalName` attribute (see also Configuring PingID MFA for Microsoft Azure AD Conditional Access). If you need additional attributes to carry over from Azure AD, do not register users through the Conditional Access flow. Instead, make sure users are created with the required attributes in PingOne before going through the Conditional Access flow, such as through SSO or provisioning.

Authorization requests sent from Azure AD to PingID use the Azure AD `userPrincipalName` attribute to identify the PingID user. Other attributes cannot be configured to identify the user in PingID.

Configuring PingID MFA for Microsoft Azure AD Conditional Access

Integrating PingID multi-factor authentication (MFA) requires setting up the configuration in the admin portal and in Azure AD.

About this task

Setting up PingID MFA for Microsoft Azure AD Conditional Access involves the following steps:

- In the admin portal, set up the integration, including attribute mapping.
- In Azure AD:
  - Create a PingID MFA custom control.
  - Create a PingID MFA conditional access policy.
- Optionally apply a PingID MFA policy to the Azure AD integration.

Default attribute mapping is based on the attributes that Azure sends to PingOne during the authorization request to trigger PingID MFA and includes the following attributes.

PingID PingIDattribute	Azure AD attribute
`username`	`upn`
`fname`	`given_name`
`lname`	`family_name`

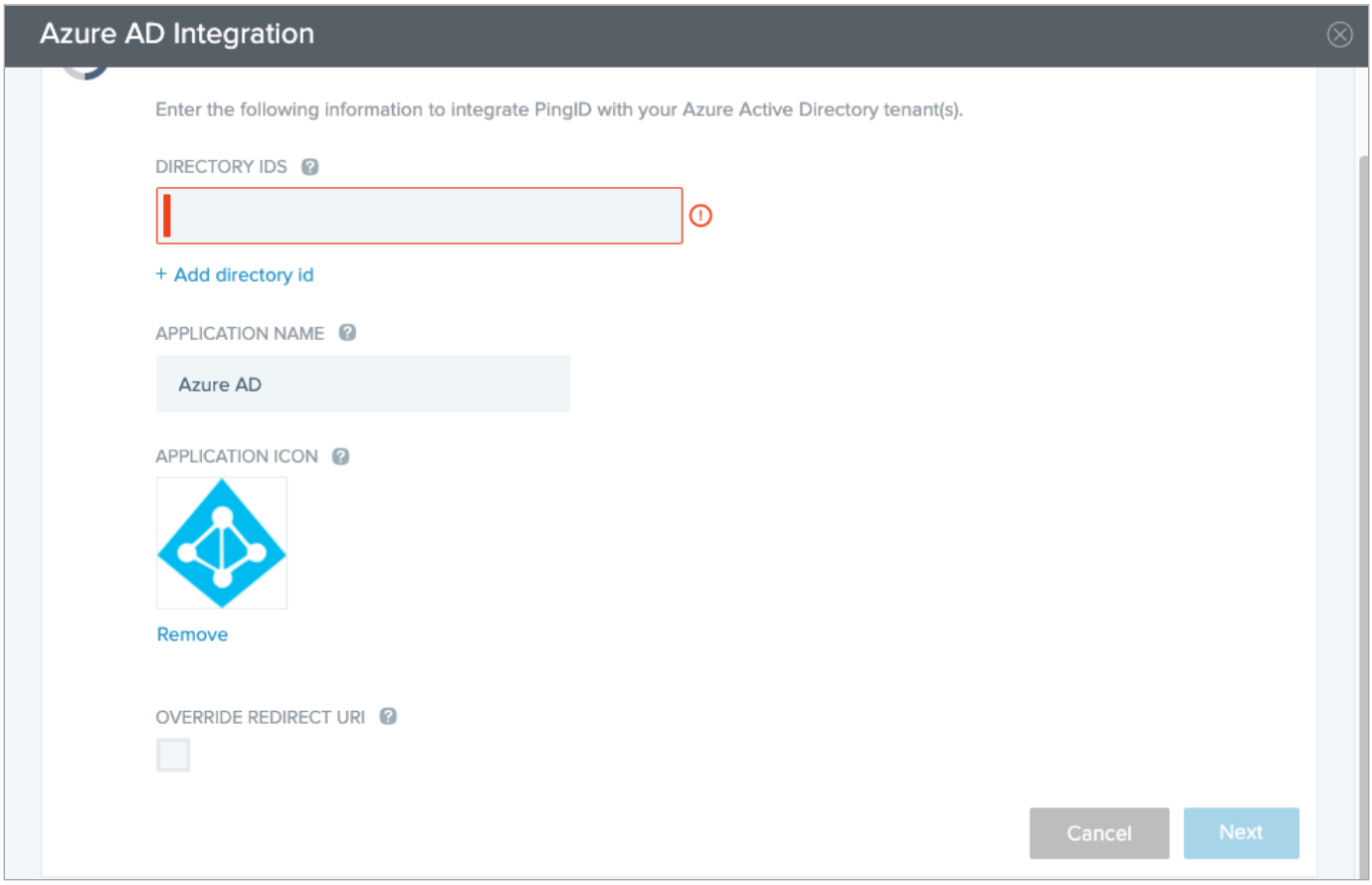
{{{ Video removed }}}

Steps

1. In the Admin portal, go to **Setup → PingID → Client Integration**.
2. In the **Integrate with Microsoft Azure AD** section, click **Setup Integration**.

   Result:

   The **Azure AD Integration** window opens.



3. To find the relevant Directory ID, in the Azure portal:
    1. In the **FAVORITES** menu in the left side bar, go to **Azure Active Directory**.
    2. In the **Manage** section, click **Properties**.
    3. Copy the value from the **Directory ID** field.
4. In the Admin portal:
    1. Paste the directory ID value into the **Directory IDS** field.
    2. **Optional:** To add additional directory IDs, click **Add directory ID** and paste the relevant Directory ID, as it appears in the relevant Azure AD account.

        > **Note**
        >
        > The directory ID must be a valid UUID string.

    3. In the **Application Name** field, enter the name you want to use to represent authorization requests from Azure AD.

        This is the name that users will see displayed if using the PingID mobile app during authorization. This name is also used to identify the Azure AD application in the PingID policy applications list.

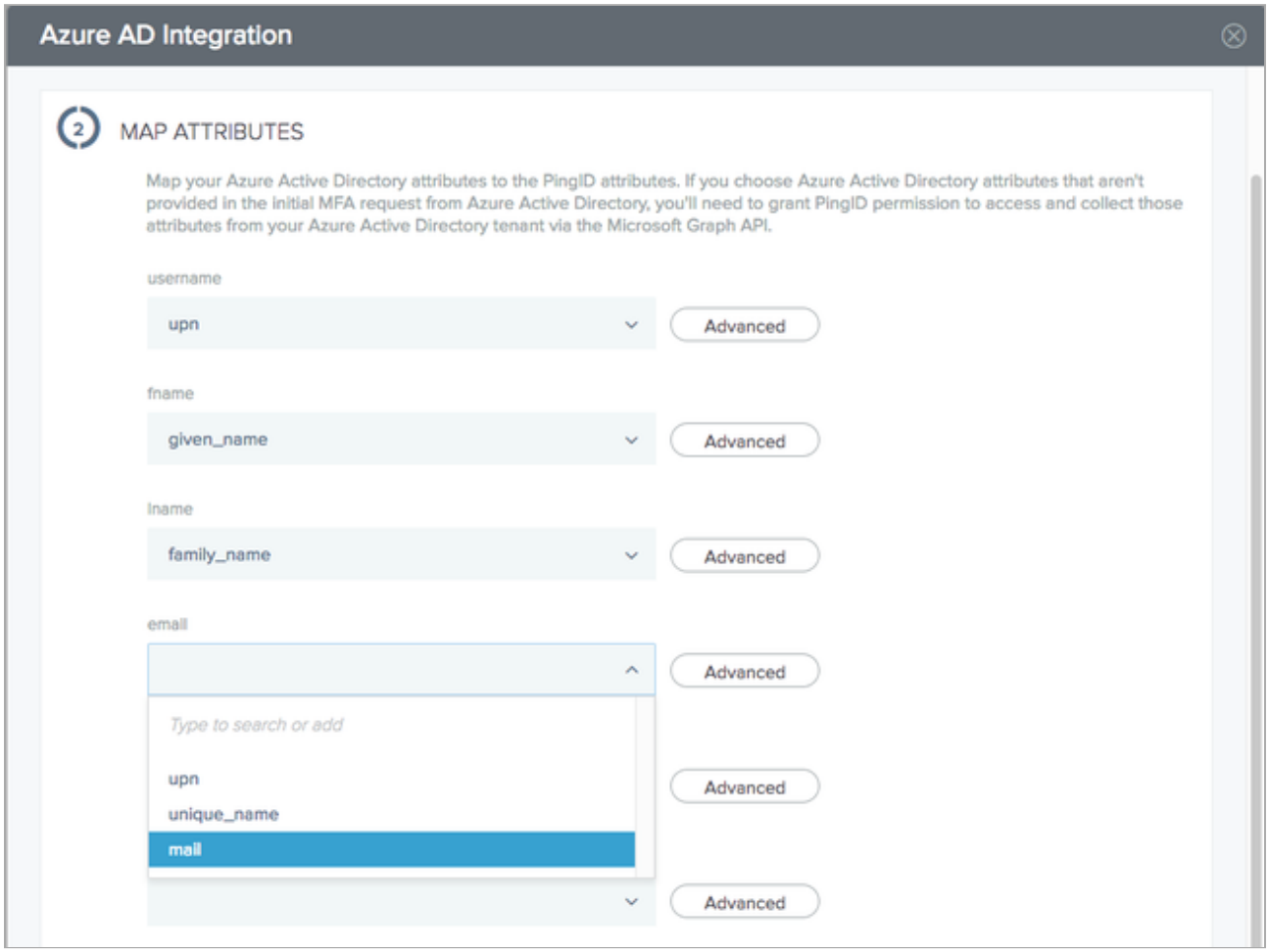
    4. To change the application icon, choose one of the following:
        - Select a new icon: Click the application icon and go to the icon you want to use.

- Use the default icon: Click **Remove**.

> **Note**
>
> The PingID mobile app displays the selected icon during authorization.

5. If your environment uses a redirect URI that is different than the default Azure AD redirect URI, use the **Override Redirect URI** field to specify the correct URI.
6. Click **Next**.

The **Map Attributes** tab opens, displaying the default attribute mapping.



5. **Optional:** To map Azure AD attributes that are not provided in the initial MFA request to the relevant PingID attributes:
   1. In the relevant attribute field, select the Azure AD attribute from the drop-down list, or type the attribute into the field.

> **Note**
>
> By default, the username for PingID is taken from the *upn* attribute in Azure. However, if you are also using Azure as the identity provider (IdP) for PingOne for Enterprise, make sure that you select from the list the attribute that you mapped to *MFA_SUBJECT*. Otherwise, you may end up with a situation where a single user is listed as two different users: one whose username comes from the *upn* attribute and one whose username comes from the attribute mapped to *MFA_SUBJECT*.

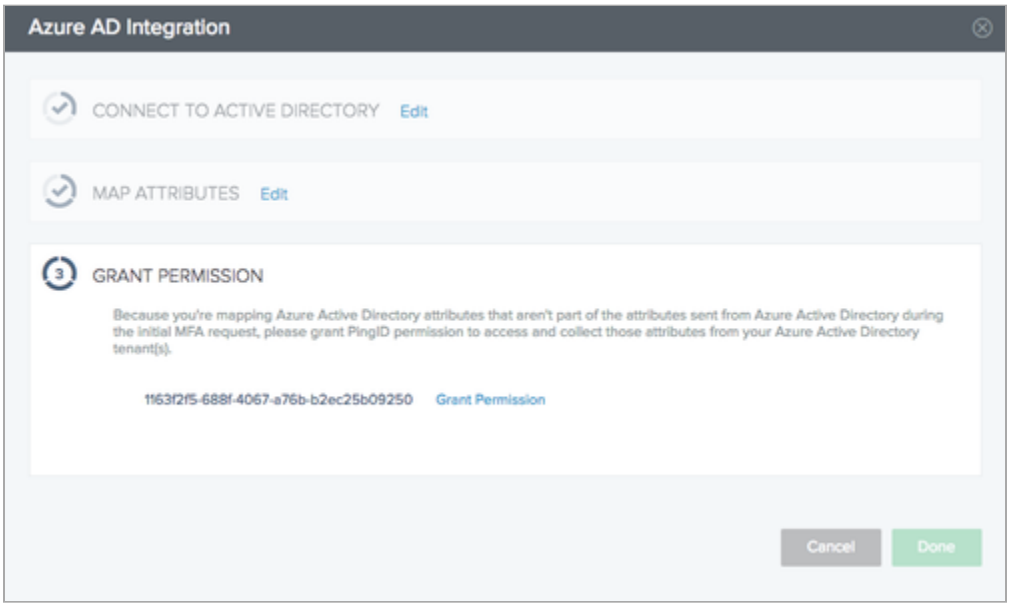
2. To perform attribute transformations on a specific attribute, in the relevant row, click **Advanced** and configure the fields as required.

   For more information, see Creating advanced attribute mappings.

3. Click **Next**.

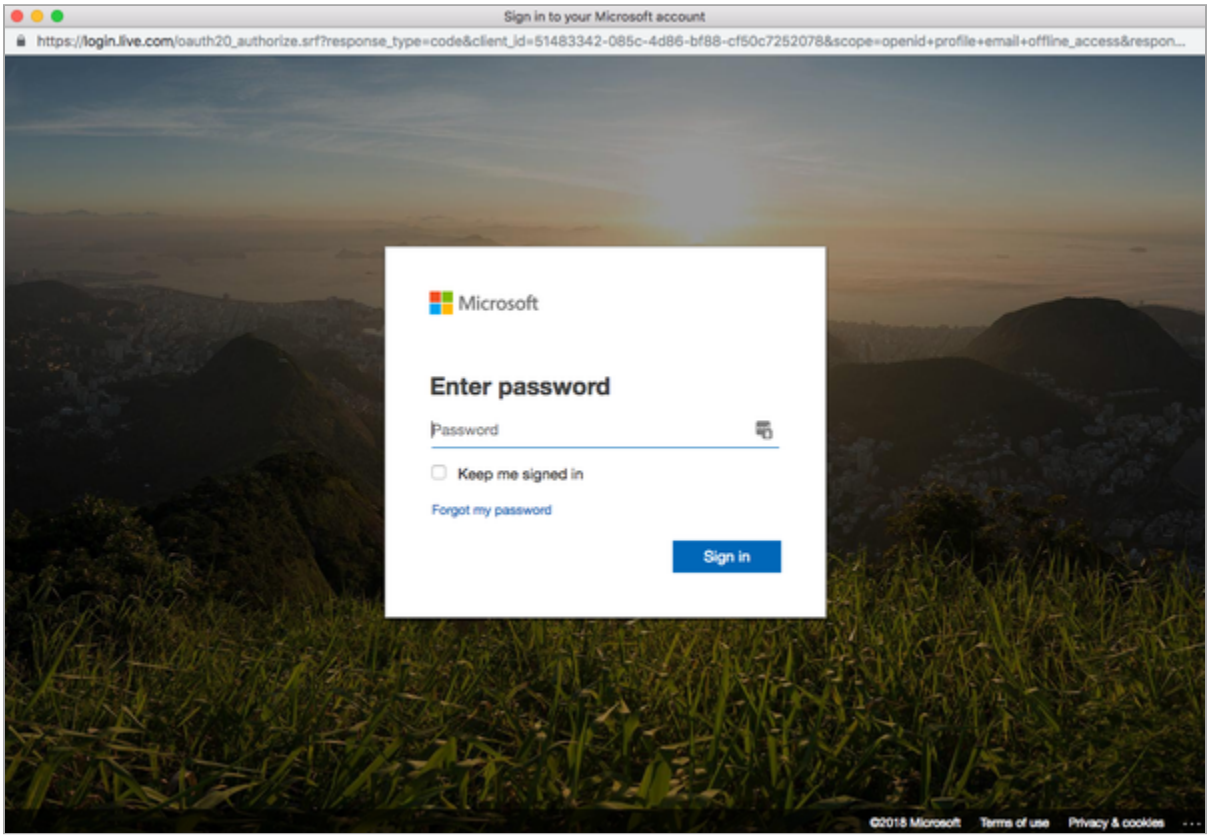
4. If you included Azure AD attributes that are not provided in the initial MFA request from Azure AD, you'll receive a prompt requesting that you grant PingID permission to access and collect those attributes from your Azure AD tenant.

   > **Note**
   >
   > If you are not prompted to grant permissions, skip this step.

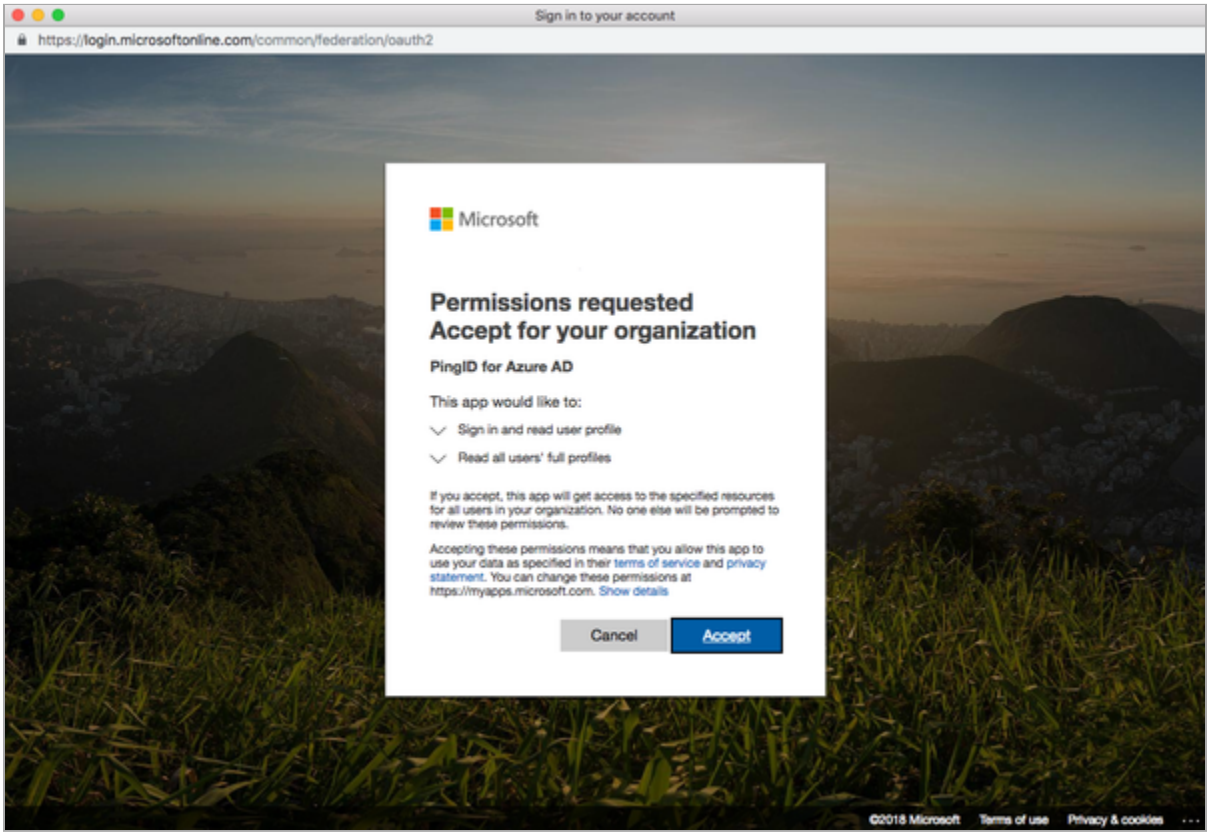


   In the **Grant Permission** window, for each Azure AD tenant:

   1. To open the Azure login window, in the **Grant Permission** section, click **Grant Permission**.

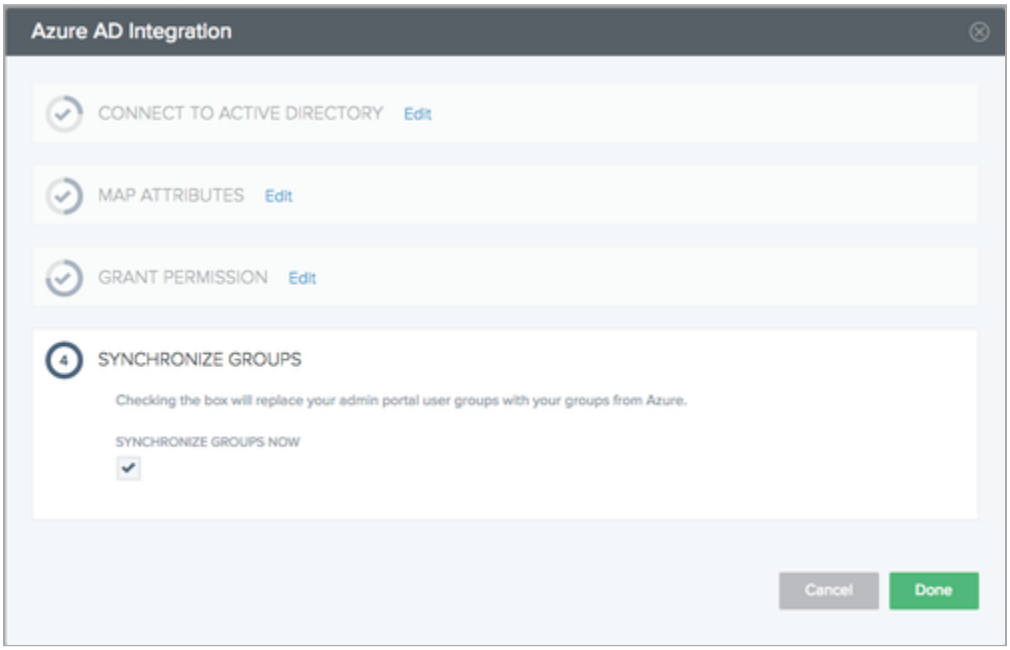


2. To grant the relevant access to PingID, sign on to your Azure AD Tenant and click **Accept**.



You are redirected back to the Azure AD Integration window.

5. If you selected an attribute mapping for the `memberOf` group attribute in the Admin portal, when prompted to synchronize groups, select the **Synchronize Groups** box to copy your Azure AD group names into PingID and click **Next**.



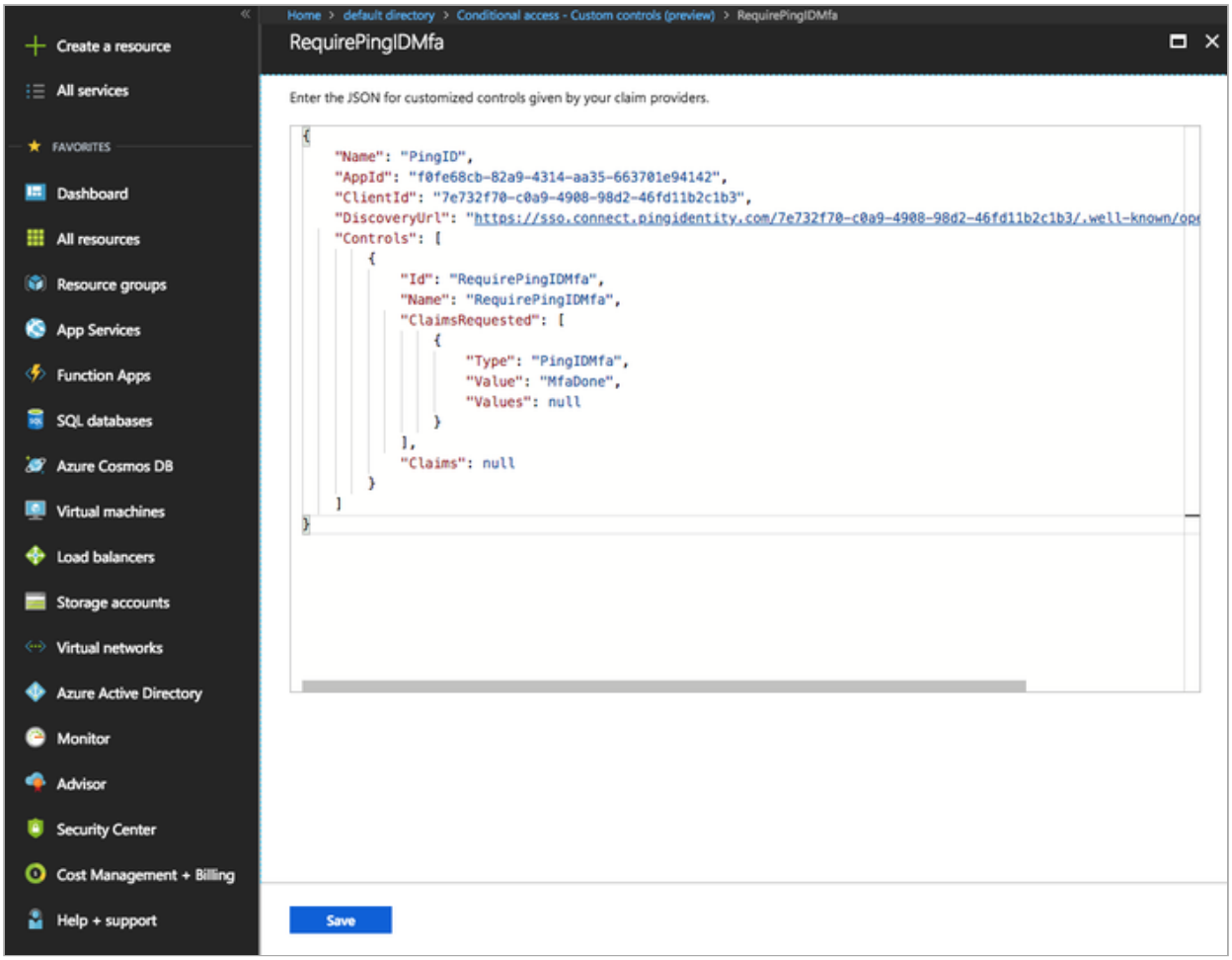
Result:

After groups are synchronized and the integration is complete, Azure groups appear in the PingID policy groups list, and the **User Groups** list at **Users → User Groups**, enabling you to apply the PingID policy to your Azure groups.

6. To save the integration, click **Done**.

The custom control JSON object that is generated includes a summary of the attribute mapping. This custom control JSON must be provided to your Azure AD account.

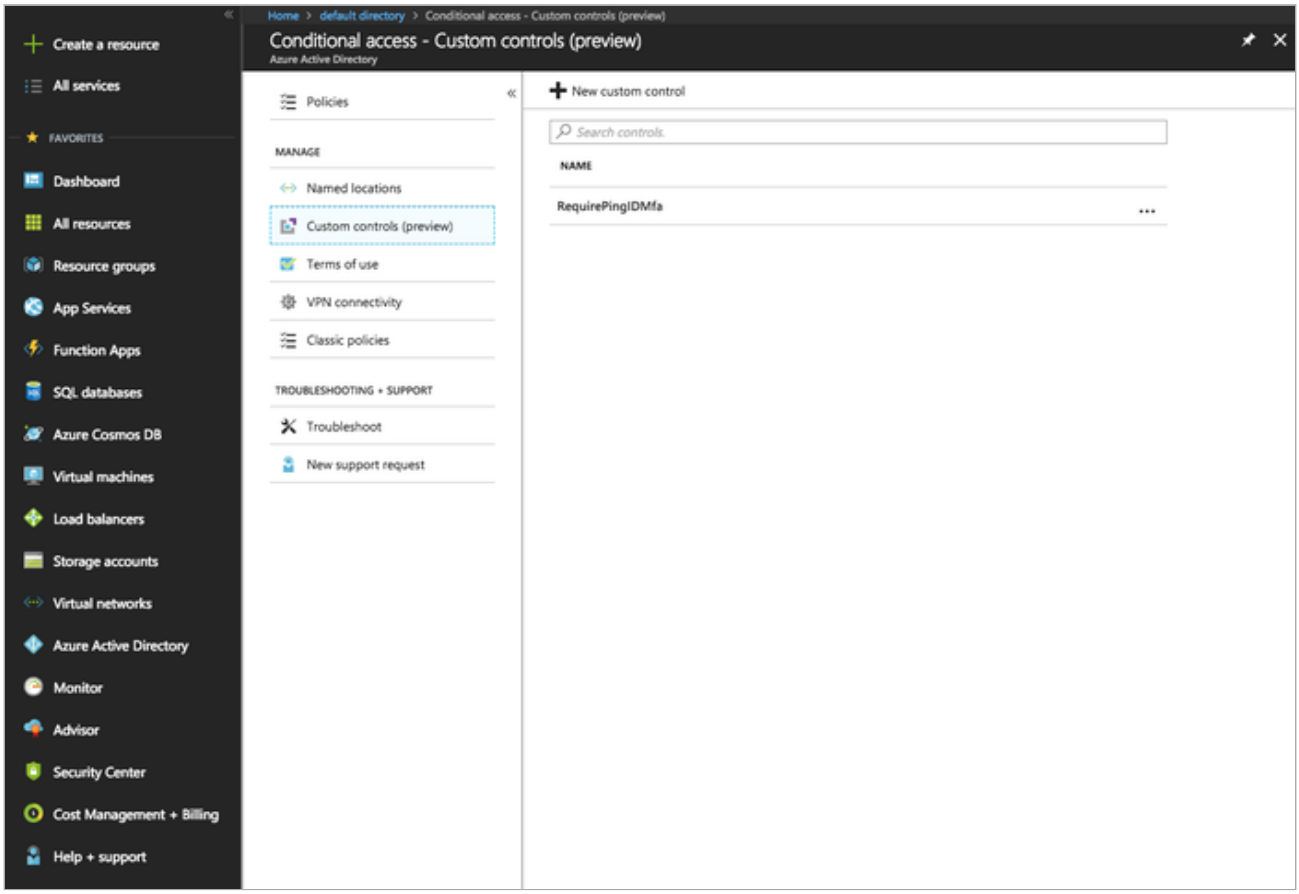
7. In the Azure AD portal, create a new PingID MFA custom control:
    1. On the left side bar, click Azure Active Directory.
    2. In the **Security** section, go to **Conditional access → Custom controls**.
    3. Click **New custom control**.



4. Delete the default JSON text, and then paste the custom control JSON that you copied from the PingOne admin portal into the Azure AD custom control field.
5. Click **Create**.

   Result:

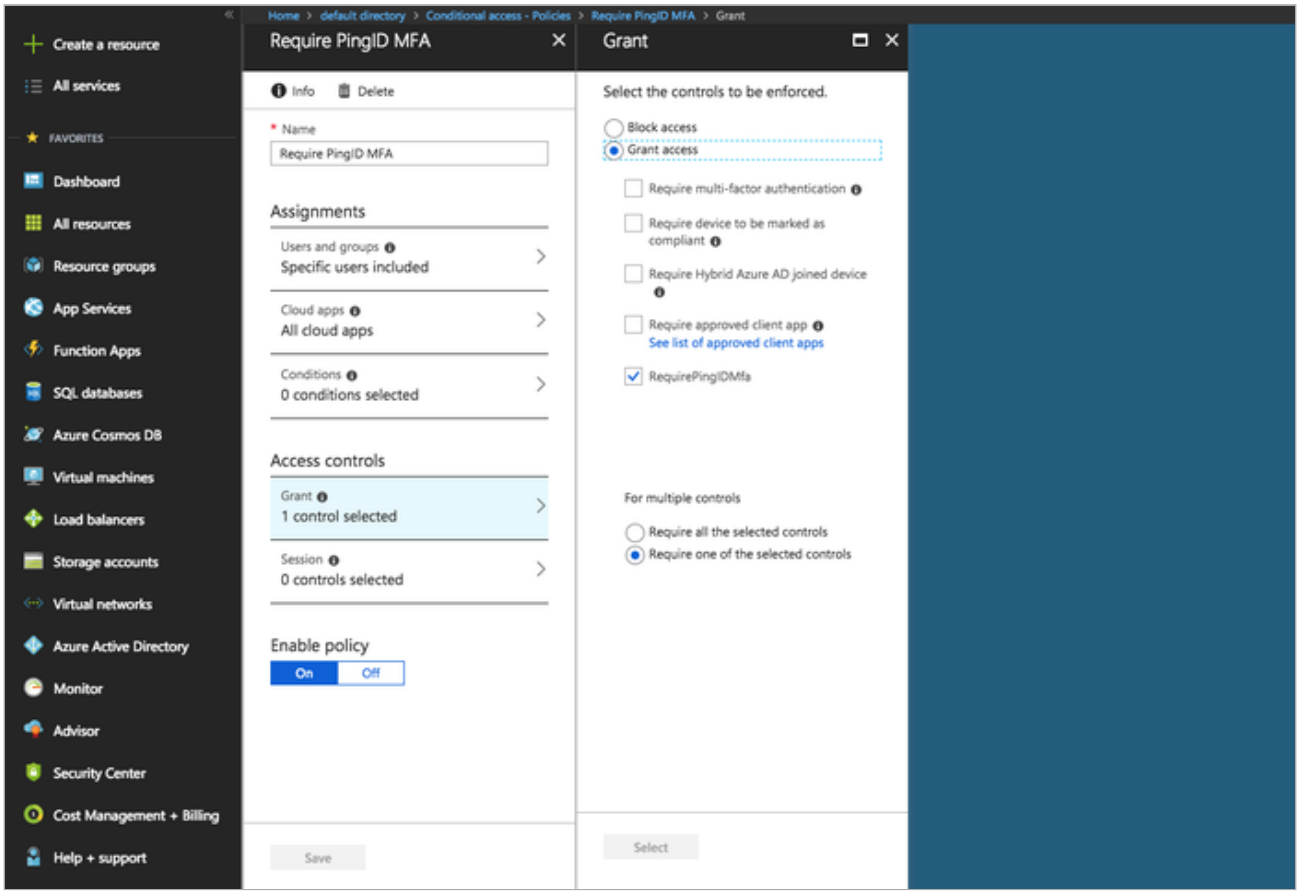
   The new custom control appears in the custom controls list.



8. In the Azure AD portal, create a new PingID MFA conditional access policy.

> **Note**
>
> To avoid blocking administrator access to the Azure AD portal, do not apply the PingID policy to all users and applications until you have successfully tested the integration between Azure AD and PingID.

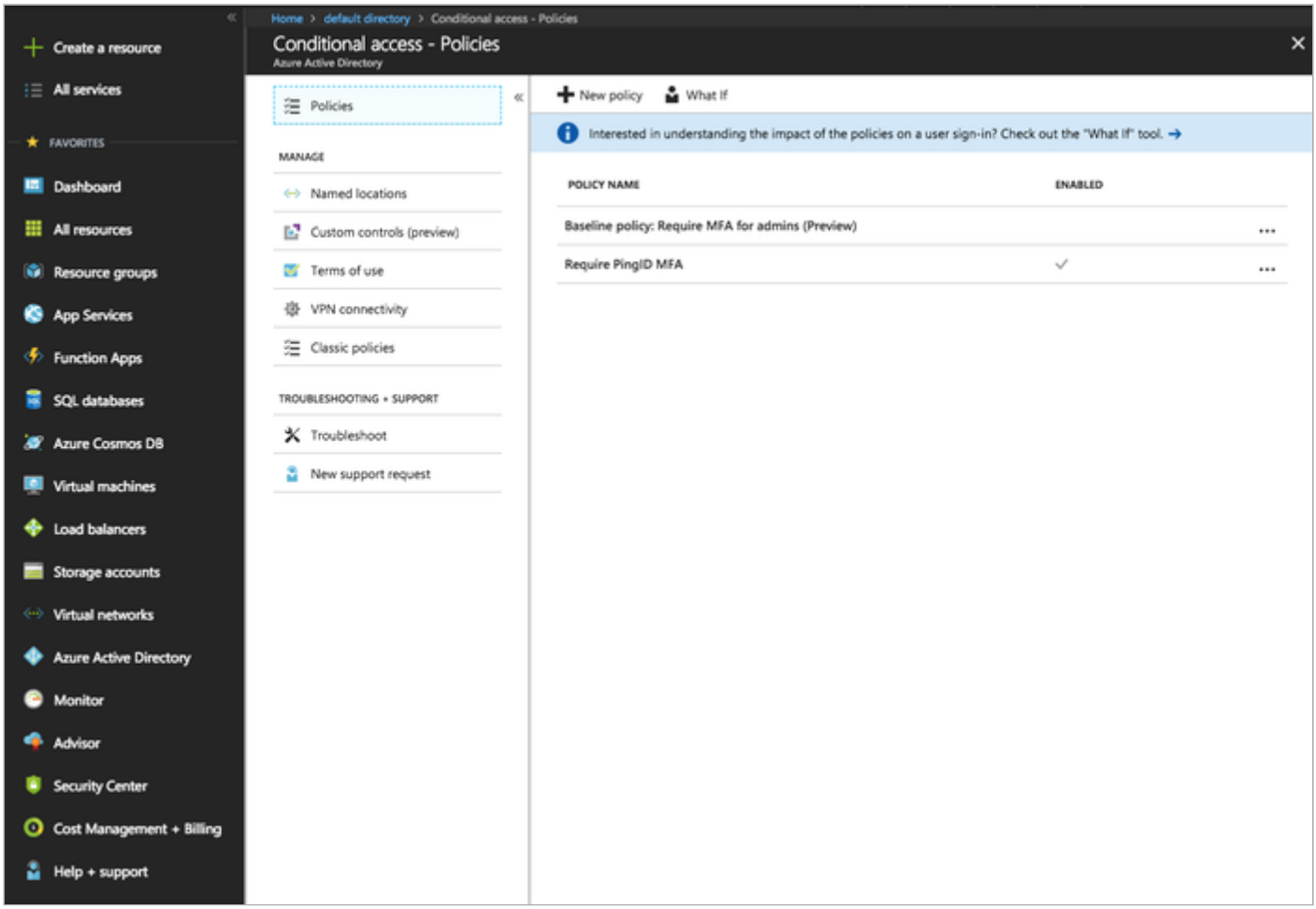
1. Go to **Azure Active Directory → Conditional access**.
2. Click **New policy**.
3. Enter a meaningful name for the policy (for example, Require PingID MFA).
4. To specify which users and groups the policy applies to, in the **Assignments** section, click **Users and groups**. On the **Include** tab, select the users and groups that you want to include in the policy. Click **Select**.
5. To specify which cloud apps you want the policy to apply to, in the **Assignments** section, click **Cloud apps**. On the **Include** tab, click **Select apps**, and select the relevant apps. Click **Select**.
6. Go to **Access controls → Grant**, click **Grant access**, and select the check box next to the custom control that you created earlier. Click **Select**.



7. Click **Create**.

Result

The conditional access policy is created and is shown in the Azure **Policies** list.



Next steps

For information about applying a PingID MFA policy to your Azure AD integration, see Configuring an app or group-specific authentication policy. The Azure AD app will appear in the PingID policy app list.

Disabling the PingID integration for Azure AD

Temporarily disable the PingID integration for Azure AD in the PingOne admin portal.

About this task

Disabling the PingID integration for Azure AD configuration blocks all MFA requests from Azure AD to PingID. When the integration is disabled, users are denied access to applications requiring PingID MFA as part of the Azure evaluated conditional access policy.

Steps

1. In the Admin portal, go to **Setup → PingID → Client Integration**.
2. Under the **Integrate with Microsoft Azure AD** heading, click the **Status** toggle.

   Result:

   The toggle turns gray to indicate that the Azure integration is disabled.

Deleting the PingID integration for Azure AD

Deleting the PingID integration for Azure AD configuration blocks all MFA requests from Azure AD to PingID.

About this task

When the integration is deleted, users are denied access to applications requiring PingID MFA as part of the Azure evaluated conditional access policy.

If you want to permanently delete the PingID integration for Azure AD for one or more directory ID, do so from the PingOne admin portal.

Steps

1. In the PingOne admin portal, go to **Setup → PingID → Client Integration**.
2. In the **Integrate with Microsoft Azure AD** section:

   Choose from:

   - To remove a specific directory ID, click **Edit**, and next to the relevant directory ID, click **Delete**, and then click **Save**.
   - To remove the PingID integration for Azure AD: click **Delete**.

     Result:

     The PingID integration for Azure AD is deleted for all Azure AD tenants.
3. in the Azure AD portal, under the left side bar, click Azure Active Directory.
4. In the left side bar, under Manage, click **Conditional Access**.

   Result:

   The policy list shows all conditional access policies.
5. Open the PingID MFA conditional access policy.
6. Click the **Enable policy** toggle to **Off**.
7. Click **Save**.

Managing the PingID properties file

The various integrations with PingID require information that is stored in the PingID properties file, which can be downloaded from the admin console.

Download the PingID properties file relevant for your platform:

PingFederate

PingFederate

You can download the PingID for PingFederate properties file for use when integrating PingID with PingFederate.

About this task

The Integrate with PingFederate Bridge properties file provides full permission to perform enrollment, device management, and authentication actions. You can rotate or revoke generated properties files with minimal downtime.

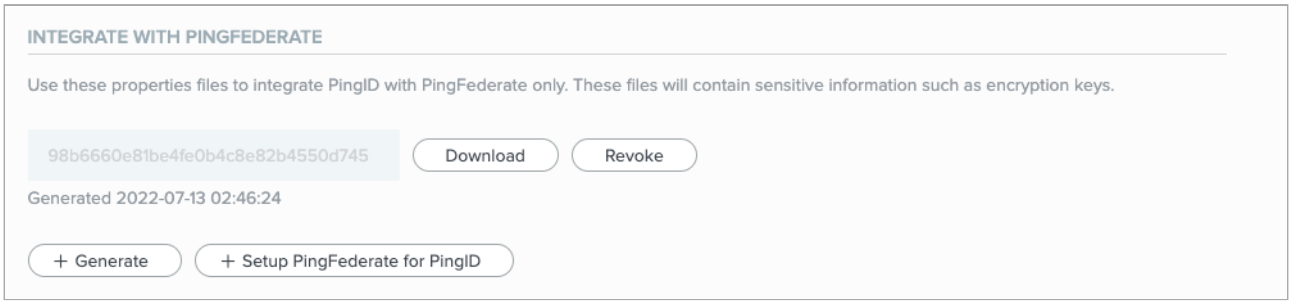
> **Note**
>
> For Window login, Mac login, and SSH integrations, you should download the version of the properties file that restricts user permissions to authentication only. For more information, see the relevant tabs on this page.

The PingID properties file contains sensitive information including the secret encryption key. It should only be handled by administrators and should not be distributed more than is necessary.

> **Warning**
>
> To ensure minimal downtime when rotating a PingID properties file (key rotation), first generate the PingID properties file and link it to the relevant client, and then revoke the old properties file.

Steps

1. In the PingOne admin portal, go to **Setup → PingID → Client Integration**.



Result:

The **Integrate with PingFederate and Other Clients** section is displayed, listing any PingID properties files that are already defined.

2. To generate a new PingID properties file, click **+ Generate**, and then click **Save**.

> **Note**
>
> You can have a maximum of five active PingID properties files. If you have five active files and want to generate a new one, you must first revoke one of your existing files.

Result:

A new entry is added to the properties file list, showing the new PingID properties file.

3. In the relevant row, click **Download**, and then save the file to the desired location with a meaningful name.

4. To revoke an old PingID properties file:

    1. Download and open the PingID properties file you want to revoke, and ensure the token matches the token listed in the web portal.
    2. In the relevant row of the properties file list, click **Revoke**, and then click **Save**.

        Result:

        The selected file is removed from the PingID server and can no longer be used for authentication.

Windows and Mac login

Windows and Mac login

The Windows and Mac login PingID properties file provides a limited subset of permissions that enable users to perform Windows or Mac login authentication while preventing them from performing management actions, such as enrollment and device management.

About this task

The PingID Windows and Mac login properties file contains sensitive information, including the secret encryption key. It should only be handled by administrators and should not be distributed more than is necessary.

> **Note**
>
> The outcome of a login attempt by this user can differ if Windows or Mac login was installed with full permissions as opposed to restricted permissions.
> Under full permissions, if valid user `john.smith` creates a new user, `joe.blogs`, on his Mac and then uses it to login, he is offered a QR code or one-time passcode (OTP) on his registered second factor device and PingID will create a new user named `joe.blogs`. The full permissions case both registers and provides access to logins. In the restricted permissions case, attempting to log-in as `joe.blogs` fails with an error message. The restricted permissions case provides access only.
> To avoid ad hoc registrations, the admin should always install the login using the restricted permissions properties file.

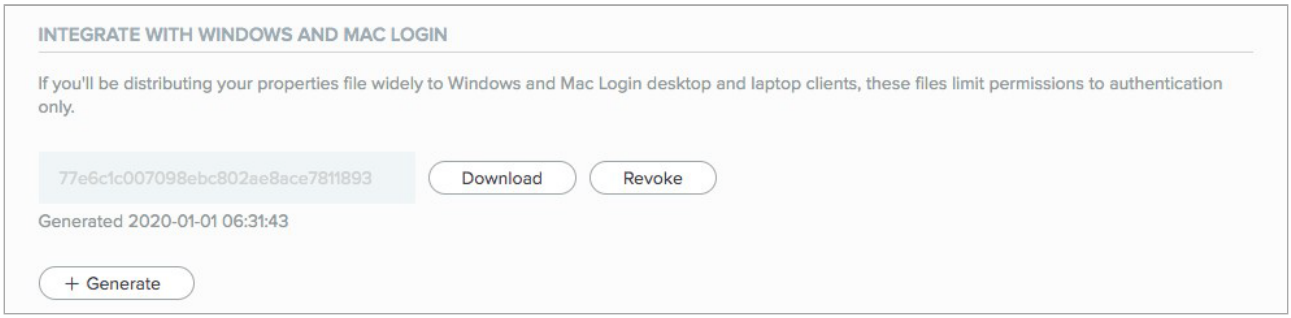
To download the PingID properties file to integrate with Windows login or Mac login:

Steps

1. In the PingOne admin portal, go to **Setup → PingID → Client Integration**.

   Result:

   The **Integrate With Windows and Mac Login** section is displayed.

2. To generate a new Windows or Mac login PingID properties file, click **+ Generate**, and then click **Save**.

   > **Note**
   >
   > You can have a maximum of five active PingID properties files. If you have five active files and want to generate a new one, you must first revoke one of your existing files.

   Result:

   A new entry is added to the Properties file list showing the new PingID properties file.

3. Select the **Enable Device Management** option if you want to allow users to manage their devices from their **Devices** page and allow users to register their device the first time they try to access a resource that requires authentication ("on-the-fly registration"). When this option is selected, these features will be available to any user that uses that copy of the PingID properties file when installing the integration with Windows login.

   > **Note**
   >
   > To carry out on-the-fly registration of FIDO2 security keys, users must have installed version 2.11 or higher of the integration with Windows login.

4. In the relevant row, click **Download**, and then save the file to the desired location using a meaningful name.

SSH

SSH

About this task

The SSH Properties file provides a limited subset of permissions that enable users to perform authentication while preventing them from performing management actions (such as enrollment and device management).

The PingID SSH Properties file contains sensitive information including the secret encryption key. It should only be handled by administrators, and should not be distributed more than is necessary.

> **Note**
>
> The outcome of a login attempt by this user can differ if SSH was installed with full permissions as against restricted permissions.
> Under full permissions, if valid user `john.smith` creates a new user, `joe.blogs`, on his Mac and then uses it to login, he will be offered a QR code or OTP on his registered second factor device and PingID will create a new user named `joe.blogs`. The full permissions case both **registers** and provides access to logins. In the restricted permissions case, attempting to login as `joe.blogs` will fail with an error message. The restricted permissions case provides access only.
> To avoid ad hoc enrollments, the admin should always install SSH using the restricted permissions properties file.

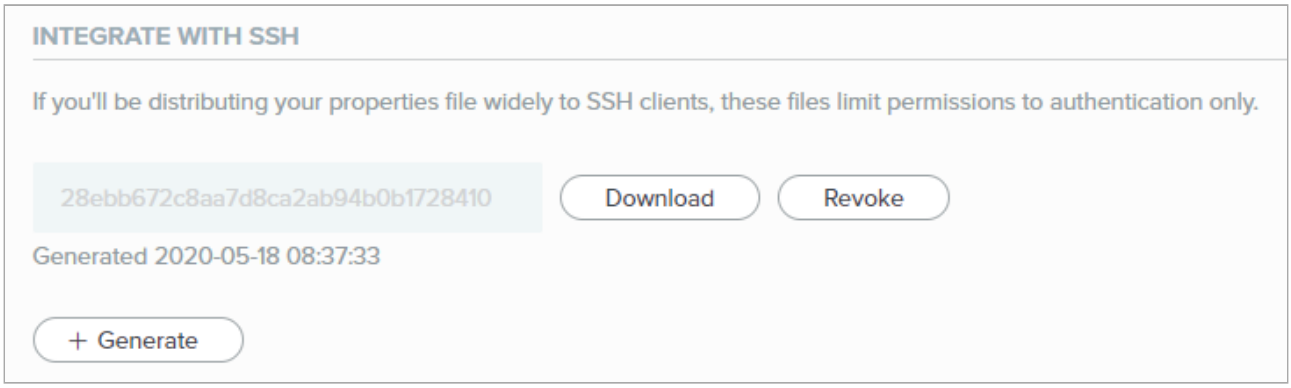
To download the PingID properties file to integrate with SSH:

Steps

1. In the PingOne admin portal, select **Setup → PingID → CLIENT INTEGRATION**.

   Result:

   The **INTEGRATE WITH SSH** area is displayed.

2. To generate a new SSH PingID properties file, click **+ Generate** and then click **Save**.

   > **Note**
   >
   > You can have a maximum of five active PingID properties files. If you have five active files and want to generate a new one, you must first revoke one of your existing files.

   Result:

   A new entry is added to the Properties file list showing the new PingID Properties file.

3. In the relevant row, click **Download**, and then save the file to the desired location using a meaningful name.

Revoking or rotating property files

Rotating and revoking a PingID properties file

You can rotate or revoke a PingID properties file.

About this task

Revoking a properties file removes it from PingID, invalidating any devices that used it.

> **Caution**
>
> Revoking a properties file should be done with extreme caution. Users signed on to machines with authentication based on a revoked properties file can continue to work normally. However, at their next sign on, they won't be able to authenticate and will be locked out of their machines.

Rotating a properties file involves replacing a properties file with a new one. To minimize downtime to users:

Steps

1. In the PingOne admin portal, go to **Setup → PingID → Client Integration**.

   The **Client Integration** page shows all PingID properties files associated with each type of properties file, such as PingFederate and unrestricted, Windows and Mac login, or SSH login properties files.

2. To ensure minimal downtime when rotating a PingID properties file (key rotation):

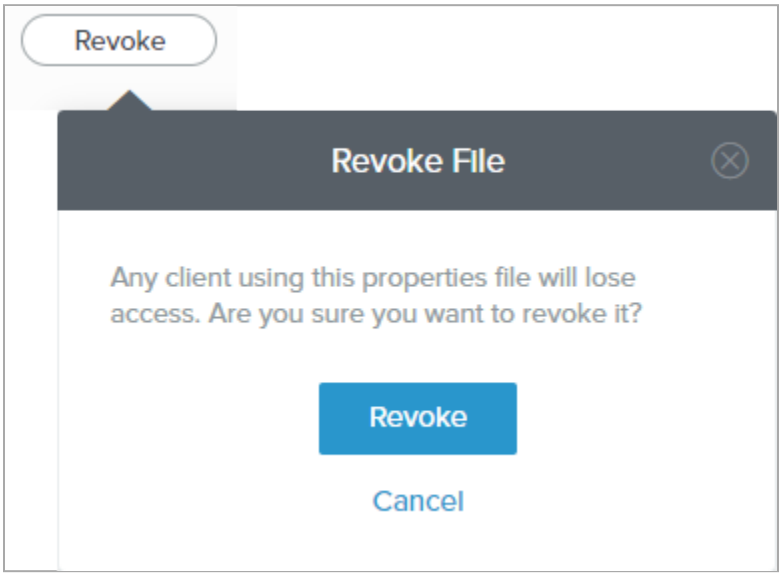
   1. To generate a new PingID properties file, click **+ Generate**.
   2. The **Download** button next to the name of the generated file is displayed as disabled. Click **Save** at the bottom of the page to enable the **Download** button.
   3. Click **Download**.
   4. Link it to the relevant client.

      The documentation for each client explains how it is linked, such as by running the GUI or CLI installer.

3. In the properties file list, select the file to be revoked (the old properties file from step 2, if relevant) and click **Revoke**.

   Result:

   A confirmation window is displayed.



4. Click **Revoke**, and then click **Save**.

   Result:

   The selected file is removed from the PingID server and can no longer be used for authentication.

PingID User Life Cycle Management

Managing the PingID User Life Cycle involves multiple tasks.

The life cycle tasks include:

- Monitoring service activity
- Disabling a user's service
- Bypassing a user's service
- Unpairing a user's device from the PingID service
- Changing a user's primary device
- Removing a PingID user
- Automatically update and remove PingID users
- User management reports

> **Note**
>
> If you have already connected your existing PingID account to PingOne SSO, you must use the PingOne SSO portal to manage users and their devices. For details, see Users.

Monitoring service activity

Several options are available for filtering and monitoring service activity.

About this task

View a list of users by service, filter the list by a specific service, or search for a specific user.

Steps

1. In the PingOne admin portal, go to **Users → Users by Service**.

   Result:

   The **Users by Service** window displays users for all services. By default, each user entry lists all services associated with that user. Hover over a service to view its full name.

2. Choose from the following options to filter the list.

Choice	Description
View users by a specific service	Select the service to filter. A list of all users associated with the selected service is displayed
View the services for a specific user	In the search bar, enter any part of the user name or email address. If you filter the list by a specific service the search returns results only for users of that service.

Choice	Description
View the service details of a specific user	Click the **Expand** icon. If more than one service is shown for the user, you can expand each service to see the last activity details.
View a report showing all user activity for a specific service	Click the relevant link in the user entry, such as **View SSO Activity**.

Disabling a user's service

Disable a user's service if you want to block the user's access to a service for an unspecified length of time, such as due to security issues or user absence.

About this task

You can subsequently re-enable the user's access if you choose.

Steps

1. In the PingOne admin portal, go to **Users → Users by Service**.
2. From the list of services, click the desired service.
3. For the selected user, click the **Expand** icon to expand the user activity panel for the service.
4. Click **Disable** to disable the user's access to the service.

   You can choose to re-enable the user's service access from this panel later.

Bypassing a user's service

Bypass the need for a user to authenticate using their secondary authentication method.

About this task

If a user of the PingID service doesn't have access to the mobile device that is paired with PingID, you can bypass a user's secondary authentication for a selected duration. At the end of a limited duration, secondary authentication for the user resumes automatically.

Steps

1. In the PingOne admin portal, go to **Users → Users by Service**.
2. Click the desired service.

   The list is filtered to display only the selected service users.
3. For a selected user, click the **Expand** icon to expand the user information for the service.
4. Click the **Edit** icon, then click the **Bypass** toggle.

5. From the list, select the duration to bypass the service.

   Only global administrators can select **Unlimited Time** to bypass the service indefinitely. All other administrators that have bypass permissions are restricted to a maximum period of 3 days.

   > **Note**
   >
   > For more information on the types of administrative roles available, see Assign administrative roles in the PingOne for Enterprise help.

6. To enable your bypass setting, click the **Bypass** toggle again.

   When the selected length of time has passed, authentication automatically resumes for the user.

   If you select **Unlimited Time**, the user will never be authenticated using this authentication provider.

   Result:

   The bypass is implemented and effective immediately.

Unpairing a user's device from the PingID service

Unpair a user's device from the PingID service.

About this task

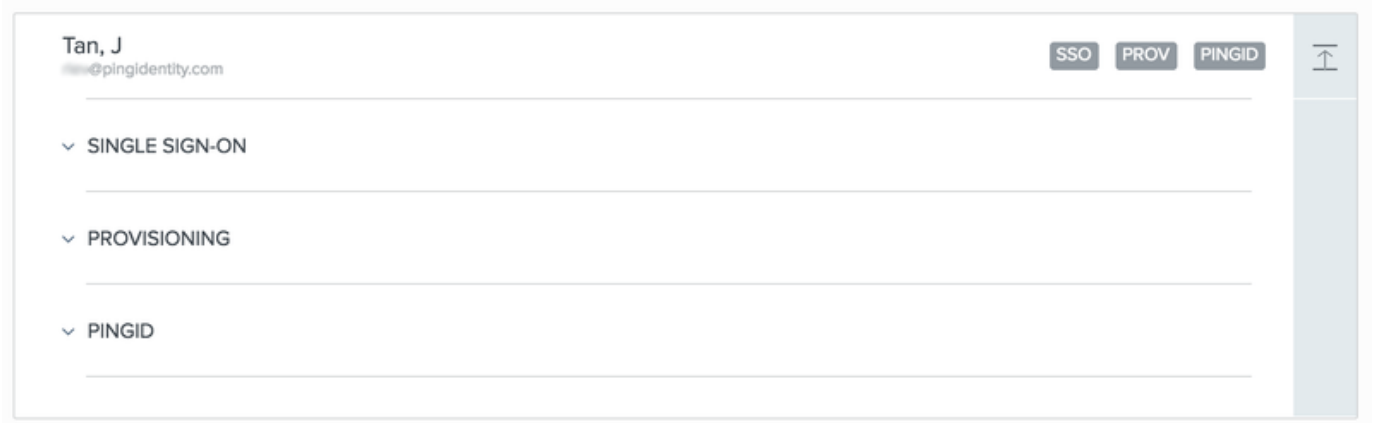
If a user unpairs a device while offline, they can only unpair a device locally, and the PingID service remains paired, blocking the user from pairing that device again until the device is unpaired from the PingID service.

> **Note**
>
> When the user next attempts to single sign on (SSO) to PingOne, they'll be prompted to pair a new device to complete the SSO process. If the new device isn't yet available to the user, you can set the PingID service to bypass PingID authentication for the user for a selected duration. For more information, see Bypassing a user's service.

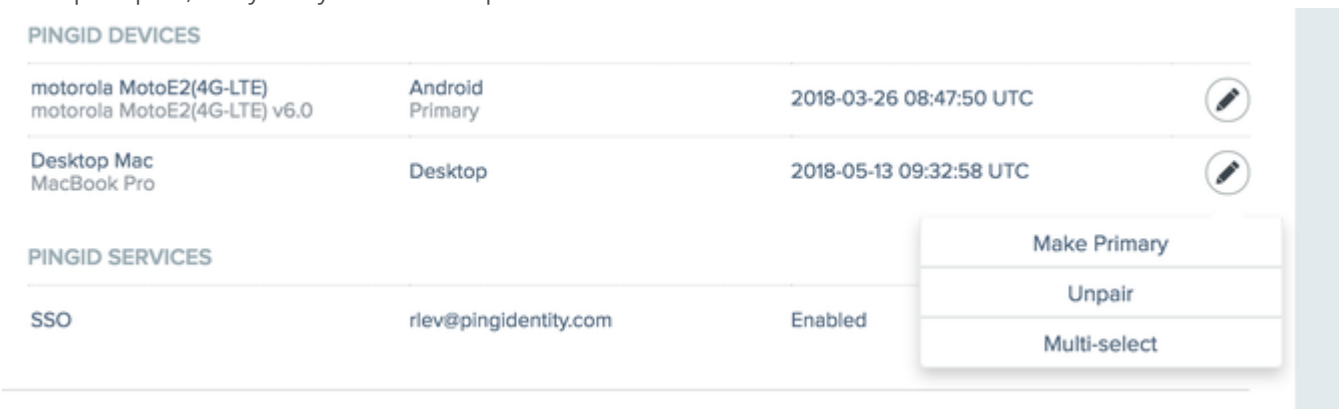
Steps

1. In the PingOne admin portal, go to **Users → Users by Service**.
2. From the services list, click **PingID**.

3. Click the **Expand** icon to expand the user activity panel for the relevant user.



4. Click **PingID** to expand the entry.
5. Click the **Pencil** icon next to the relevant desktop app entry, and then click **Unpair**.
6. When prompted, verify that you want to unpair the device.



Result:

The device is unpaired from the PingID service. The user will be prompted to pair a new device the next time they SSO to PingOne, unless you've set the PingID service bypass option.

> **Note**
>
> It might be necessary for the user to unpair the device locally in order to be able to pair the device again.

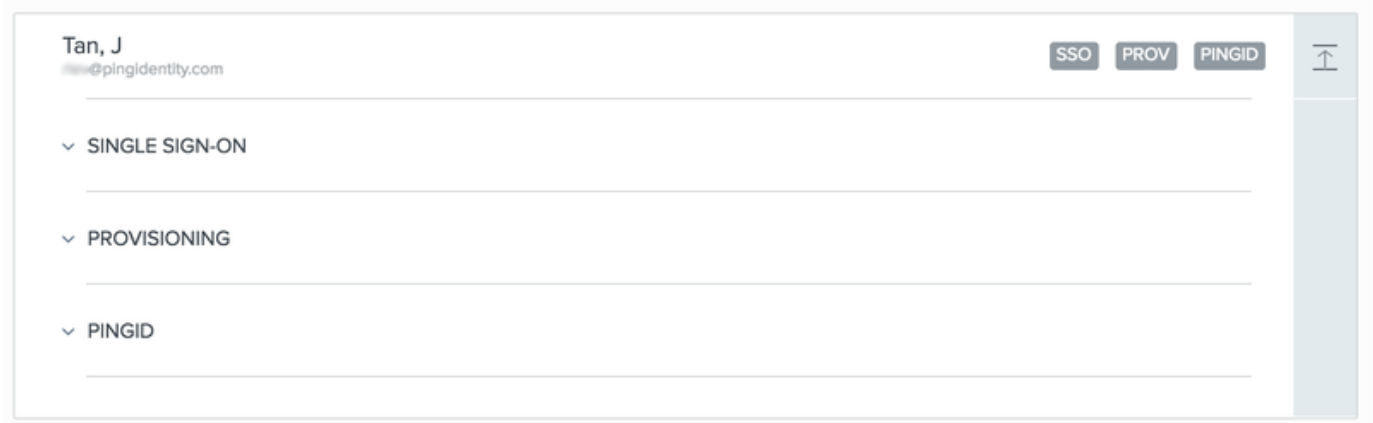
Changing a user's primary device

If you have enabled multiple devices, and a user has more than one device, change the user's primary device from the PingID service.

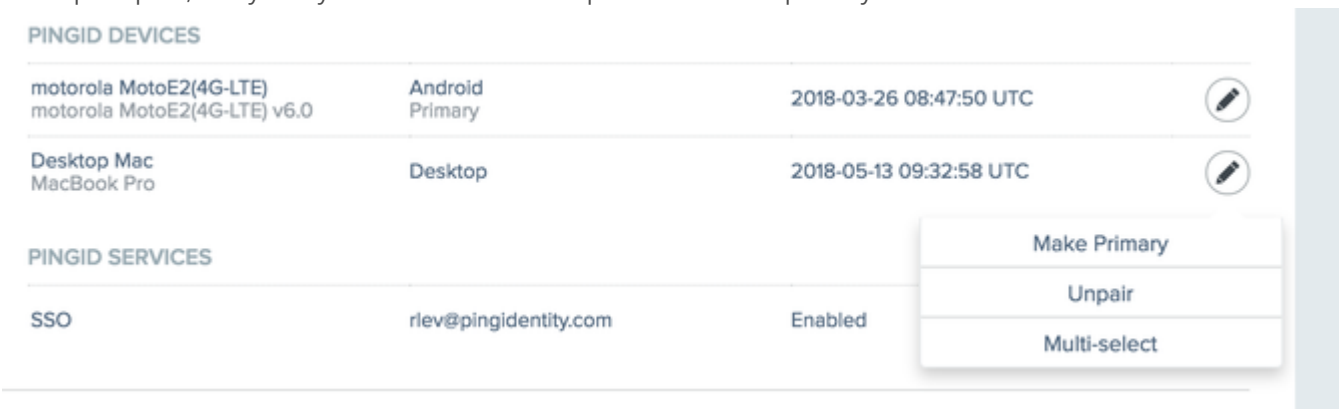
Steps

1. In the PingOne admin portal, go to **Users → Users by Service**.
2. From the list of services, click **PingID**.

3. Click the **Expand** icon to expand the user activity panel for the relevant user.



4. Click **PingID** to expand the entry.
5. Click the **Pencil** icon next to the relevant secondary device, and then click **Make Primary**.
6. When prompted, verify that you want to make that specific device the primary device for that user .



Result:

The device is promoted to Primary. If Default to Primary is configured for your organization, the user is prompted to authenticate using the selected device by default.

> **Note**
>
> The user can still change their device during the authentication process.

Removing a PingID user

Permanently remove a PingID service user.

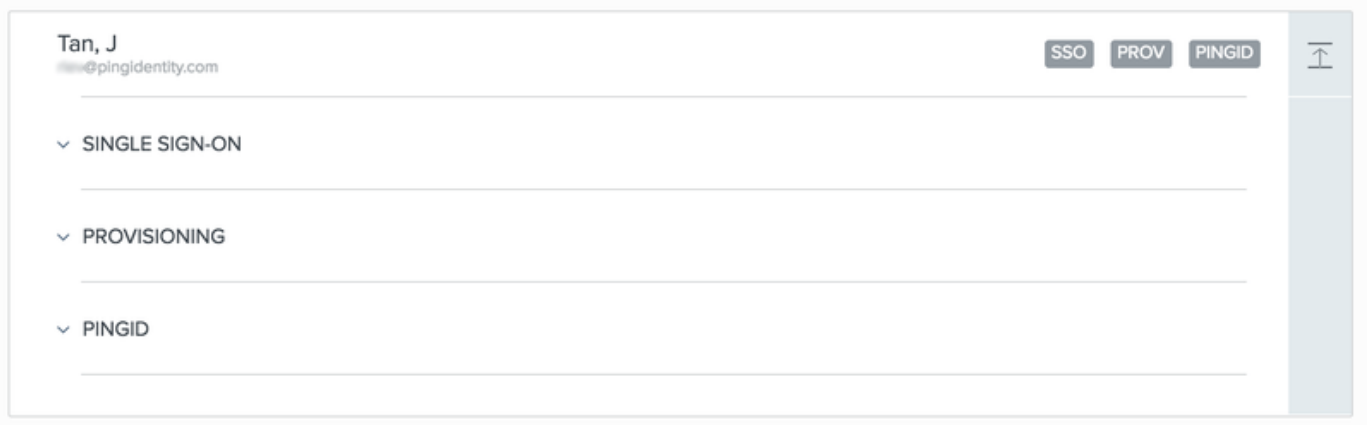
About this task

This might be necessary if a user has left your organization. For more information, see Disabling a user's service.

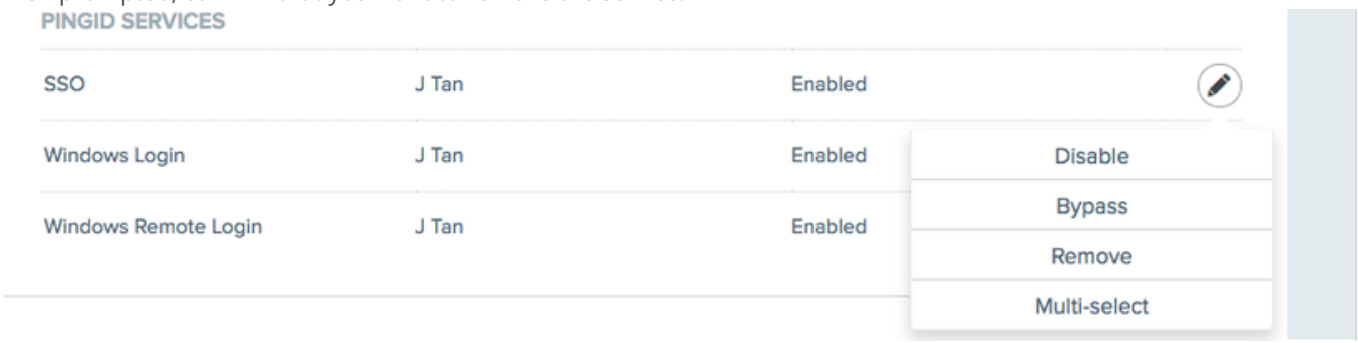
Steps

1. In the PingOne admin portal, go to **Users → Users by Service**.

2. From the list of services, click **PingID**.
3. Click the **Expand** icon, to expand the user activity panel for the relevant user.



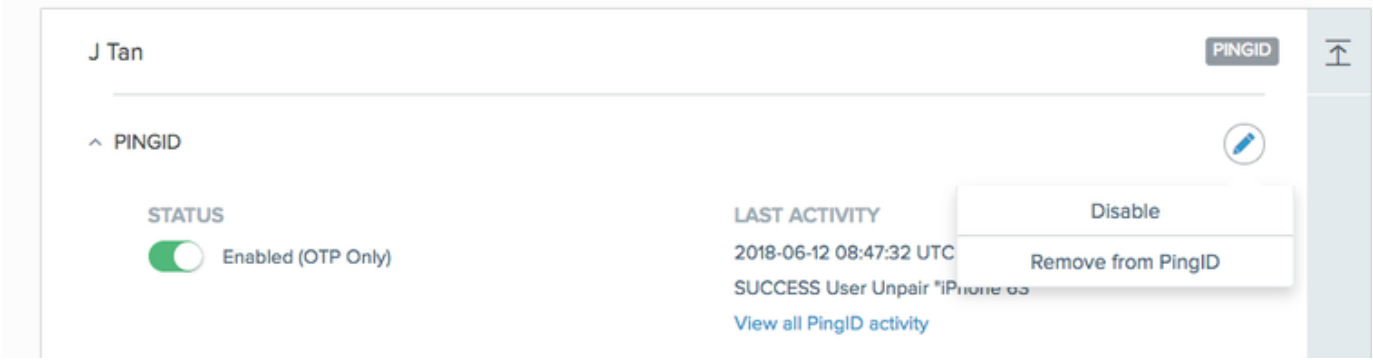
4. Click **PingID** to expand the entry.
5. To remove a user from a specific service, click the **Pencil** icon next to the relevant service, and then click **Remove**.
6. When prompted, confirm that you want to remove the service.



Result:

The user is removed from the selected service.

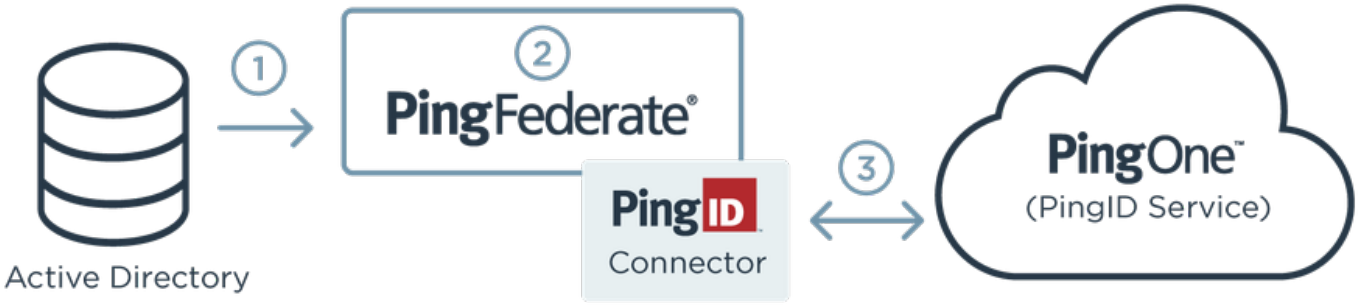
7. To remove the user from all services, click **Remove from PingID**.



Automatically update and remove PingID users

The PingID Connector synchronizes user identities and their profile attributes from a configured datastore within PingFederate to PingID.

Ping Identity offers a catalog of connectors that provide provisioning capabilities to software as a service (SaaS) providers. The connectors act as mediators to handle transactions safely and securely. The PingID Connector offers profile management solutions to multiple directory types, such as LDAP, Active Directory (AD), and PingDirectory.



Processing steps

1. PingFederate polls the user directory for any changes to user records at regular intervals, configurable in PingFederate.
2. Records requiring action found during step 1 are stored within PingFederate's intermediary database and marked as a requiring an update in PingID (PingOne).
3. The connector pulls the marked record from the intermediary database and performs the necessary Read (Get), Update, or Delete operation against the PingID record. These changes are reflected in the PingOne admin portal.

   The PingID Connector:

   - Provides support for PingID API 4.9
   - Includes support for user life cycle management including updates, disabling users, and deleting users
   - Includes configuration options for workflow capabilities, such as the ability to disable updates.

To download the PingID for PingFederate connector, see PingFederate Server SaaS Connectors.

For details on how to configure the PingID for PingFederate connector, see PingFederate PingID Connector Guide.

PingID Offline MFA

PingID runs as a cloud service on the PingOne platform. To allow users to authenticate even if the PingID service is unreachable, PingID includes offline multi-factor authentication (MFA).

Offline MFA must be configured, so make sure to carry out the steps outlined here before you actually encounter such a situation.

You can configure PingID offline MFA for the following use cases:

- Access through PingFederate single sign-on (SSO)
- Access through RADIUS password credential validator (PCV)
- Access through Windows login
- Access through Windows login (passwordless)
- Access through Mac login
- Access through the PingID integration with SSH

Below is an outline of the steps required to configure offline MFA for each of these cases. Links are provided to the detailed information for each case.

Note

- PingID policy rules that have been defined are not enforced when authenticating in offline mode.
- Device requirements are taken into account when authenticating in offline mode.
- Changes to the device list that occur during offline mode are updated in the user directory only when the user next authenticates online.

PingID offline MFA when authenticating through PingFederate single sign-on (SSO)

Offline MFA requires the following:

- A user directory to store user device information from PingID. For more information, see User directory for PingID offline MFA.
- Unlimited Strength Java Cryptography Extension (JCE), which is required for supporting the 256-bit key size for cryptographic algorithms. Without it, the feature will return an exception related to the missing library, and will not function.

When the PingID service is unreachable, after first-factor authentication, the user receives a QR code on an offline authentication screen.

To enable offline authentication, carry out the optional offline MFA step described in Installing the PingID Integration Kit for PingFederate, and configure offline MFA for the PingID Adapter as described in Configuring offline MFA (PingID Adapter).

When configuring the PingID Adapter for offline MFA, the key option to configure is **AUTHENTICATION DURING ERRORS**, which can be set to one of:

- Bypass User

- Block User
- Passive Offline Authentication

> **Note**
>
> In addition to the standard options listed above, if you encounter a situation where PingID is down but the Passive Offline Authentication option is not prompting users to authenticate offline, you can select the **Enforce Offline Authentication** option for a limited time until the issue is resolved. This will force all your users to authenticate offline until you switch back to one of the standard options.

PingID offline MFA when accessing through RADIUS password credential validator (PCV)

When the PingID service is unreachable, after first-factor authentication, the user receives a 12-digit security key in the VPN client.

For detailed instructions on configuring offline MFA with PingID RADIUS PCV, see Configuring offline MFA (RADIUS PCV).

> **Note**
>
> PingID offline MFA does not support RADIUS VPNs with no challenge.

When configuring offline MFA for the PingID RADIUS PCV, the key option to configure is **Authentication During Errors**, which can be set to one of:

- Bypass User
- Block User
- Passive Offline Authentication

> **Note**
>
> In addition to the standard options listed above, if you encounter a situation where PingID is down but the Passive Offline Authentication option is not prompting users to authenticate offline, you can select the **Enforce Offline Authentication** option for a limited time until the issue is resolved. This will force all your users to authenticate offline until you switch back to one of the standard options.

PingID offline MFA when accessing through Windows login

When the PingID service is unreachable, after first-factor authentication, the user is prompted to authenticate using a security key or the PingID mobile app in offline MFA mode (manual authentication).

For detailed information about configuring offline MFA for Windows login, see Installing the PingID integration for Windows login.

The behavior for offline situations is determined by the value provided for the `offlineAuthType` parameter when carrying out command-line installation of the integration with Windows login. You can set `offlineAuthType` to:

- 0 - do not allow MFA for offline authentication
- 1 - allow offline MFA using PingID mobile app only

- 2 - allow offline MFA using a FIDO2 security key only
- 3 - allow offline MFA using either PingID mobile app or a FIDO2 security key

PingID offline MFA when accessing through Windows login (passwordless)

When the PingID service is unreachable, after authentication is initiated, the user is prompted to authenticate using a security key or the PingID mobile app in offline MFA mode (manual authentication).

For details, see the description of the **Offline Mode** option in Creating an authentication policy (Windows passwordless).

PingID offline MFA when accessing through Mac login

When the PingID service is unreachable, after first-factor authentication, the user is prompted to authenticate using a security key or the PingID mobile app in offline MFA mode (manual authentication).

For detailed information about configuring offline MFA for Mac login, see Installing the PingID integration for Mac login.

The behavior for offline situations is determined by the value provided for the `offlineAuthType` parameter when carrying out command-line installation of the integration with Mac login. You can set `offlineAuthType` to:

- 0 - allow offline MFA with the PingID mobile app
- 1 - if the user does not have a paired PingID mobile app with their account, bypass MFA during login
- 2 - do not allow offline MFA

Offline MFA when using the PingID integration with SSH

When the PingID service is unreachable, after first-factor authentication, the user receives a 12-digit security key in the terminal window.

For detailed information, see Enabling offline MFA in SSH integration.

The behavior for offline situations is determined by the value provided for the `fail_mode setting` in the configuration file, which can set to:

- `restrictive`
- `passive_offline_authentication`
- `permissive`

> **Note**
>
> In addition to the standard options listed above, if you encounter a situation where PingID is down but the `passive_offline_authentication` option is not prompting users to authenticate offline, you can select the `enforce_offline_authentication` option for a limited time until the issue is resolved. This will force all your users to authenticate offline until you switch back to one of the standard options.

User directory for PingID offline MFA

PingID offline multi-factor authentication (MFA) supports storage of user authentication device details according to different user directory deployments.

User directory

PingID offline MFA can access device information stored in the directory's user object, or in a directory object separate from the user object, either in the same directory as the user object, or in a different directory.

> **Note**
>
> The PingID offline MFA feature is designed to work with directories from several vendors, including Active Directory, Oracle Directory, and Ping Directory.
> Directory setup scripts are provided for Active Directory as part of the PingID Integration Kit 2.0 and later. You must configure other directories manually.
> For more information on directory configuration, see Installing the PingID Integration Kit for PingFederate.

Scripts provided in the PingID Integration Kit 2.0 or later add the following attributes to the directory:

`pf-pingid-state`

The `pf-pingid-state` attribute holds the authentication state of the user during offline MFA.Administrators can use this attribute to bypass or block individual users.It is an optional attribute. When it is used, it must be coupled with the `user` object class on the main user directory. The optional values, `block` or `bypass`, stored in this attribute are managed by the administrator. For more information, see Configuring offline MFA (PingID Adapter) or Configuring offline MFA (RADIUS PCV).PingFederate only requires read access to the `pf-pingid-state` attribute.The value of the `pf-pingid-state` attribute is always stored in the user's object. You can assign a different name to the attribute using the setup script, within the limits permitted by the user directory.When PingID is offline, the identity provider checks the configuration.

- If the user's `pf-pingid-state` configuration is empty, the authentication flow continues.
- If `pf-pingid-state` is set to `bypass`, the user bypasses MFA.
- If `pf-pingid-state` is set to `block`, the user is blocked from logging in.

`pf-pingid-local-fallback`

The `pf-pingid-local-fallback` attribute holds the user's authentication devices list information.It is a mandatory attribute.The administrator must decide between:

- Adding the attribute to the `user` objectClass on the main user directory.
- Adding the attribute to a separate custom `pf-pingid-device` objectClass.

If you add `pf-pingid-local-fallback` to `pf-pingid-device`, you must decide which directory should hold the `pf-pingid-device` objects. These objects can be stored in the same directory as the users in a different location in the directory tree, or in an entirely separate directory. PingFederate configuration will vary according to the design you choose.

Multiple Adapter/PCV Instances: When running a single PingFederate server with multiple PingID tenants, the `pf-pingid-local-fallback` attribute cannot be linked to the user objectClass. It is mandatory to set up a separate custom `pf-pingid-device` objectClass. The location of the `pf-pingid-device` objects must be different for each Adapter/PCV instance.

If multiple Adapter/PCV instances use the same PingID tenant, there is no restriction on the `pf-pingid-local-fallback` attribute location.

For more information, see Installing the PingID Integration Kit for PingFederate.PingFederate will have read and write access to the `pf-pingid-local-fallback` attribute, because values stored in this attribute are managed by PingFederate.

Priority of parameter settings during the flow of PingID offline MFA

1. If the `Authentication During Errors` parameter is set to `Bypass` or `Block`, the user's `state` attribute is ignored during offline authentication. All users will either bypass PingID offline MFA or be blocked from authenticating, according to the `Authentication During Errors` setting.
2. If the `Authentication During Errors` parameter is set to `Passive` or `Enforce`, PingFederate checks the user's `state` attribute.

The user's `state` *attribute is empty*

If the user has a paired mobile device, the flow proceeds to offline MFA.If the user does not have a paired mobile device, the flow proceeds according to the setting in the `Users Without a Paired Device` parameter.

The user's `state` *attribute is set to* `Bypass`

The user will bypass PingID offline MFA.

The user's `state` *attribute is set to* `Block`

The user is blocked from authenticating.

PingID SDK

PingID SDK enables you to provide your customers with advanced multi-factor authentication (MFA) functionality that balances security and convenience.

> **Note**
>
> Because PingID SDK is no longer actively supported and will be deprecated, you should migrate to PingOne MFA. For more information on migrating to PingOne MFA, contact your Ping account executive or customer success manager.

To send your consumers branded, customizable push notifications, you can embed the PingID mobile SDK into new or existing iOS or Android applications. As an alternative authentication factor, you can also use SMS, voice, and email notifications with customized content and a one-time passcode (OTP). QR code-based authentication is available as a passwordless authentication option. These methods allow your organization to provide MFA without introducing unnecessary friction or forcing your consumers to download a separate MFA application. For more information, see Introduction to PingID SDK.

PingOne hosts the PingID services and provides the web administrative portal for PingID SDK application and user management. Register for a PingOne account at https://admin.pingone.com/web-portal/register.

PingID SDK default settingsPingID SDK has a number of configuration settings, according to the following groups:

*

+ System settings:::

System settings apply system-wide to all tenants and all applications and are not configurable.

+

System parameter	Description	Value (not configurable)	Relevant error or status
`Authentication session lifetime`	The period during which application logic can check the status of an authentication. In cases where users didn't receive a push notification or they use an offline device, they can complete the authentication.	30 minutes	Top level error code: `NOT_FOUND`
`Push notification timeout`	The time a new authentication notification request has to reach a user's mobile device before timeout occurs. There might be a difference between the response of iOS and Android platforms when an app moves the push notification payload to the mobile SDK. The push notification period is included in the `Online session timeout` period. Factors such as specific implementations and platform limitations might also impact the time it takes for an app to move the push notification payload to the mobile SDK.	20 seconds	`status`: `TIMEOUT`

System parameter	Description	Value (not configurable)	Relevant error or status
`Online session timeout`	The total amount of time a new authentication request has before timing out. The difference between the `Push notification timeout` and `Online session timeout` indicates the amount of time the user has to respond upon receiving an authentication request before timeout occurs.	40 seconds	`status` : `TIMEOUT`
`Silent push timeout`	The extension of time for approval of a trusted device when `VERIFY DEVICES USING APPLE/ANDROID PUSH SERVICE` is set to **Enable**.	7 seconds	N/A
`SMS lifetime limit`	The time for the counters of the `DAILY USED SMS LIMIT` and `DAILY UNUSED SMS LIMIT` to accumulate the count of authentication requests per user, per application. The daily counters are reset every night at midnight UTC.	1 calendar day	N/A
`SMS pairing limit`	The maximum number of pairing SMS messages permitted per account.	Full license: unlimited Trial license: 100	Top level error code: `REQUEST_FAILED` Detailed error code: `SMS_QUOTA_EXCEEDED`

*

+ Application settings:::

Application settings are configurable settings per application in the admin portal. For configuration instructions and default settings, see Updating a PingID SDK app's configuration.

+

> **Note**
>
> Some of the application configurations are restricted or not configurable for tenants with trial licenses.

PingID SDK application management

PingIDK SDK administrators can configure, update, enable, disable, and distribute settings for the application.

PingID SDK enables developers of mobile apps on iOS or Android to include advanced multi-factor authentication (MFA) functionality that is on-brand and customizable within their mobile applications. This allows organizations to preserve their brand experience rather than force customers to download a separate MFA application.

As part of the integration of a the PingID SDK component into a customer's mobile application, the PingID SDK account administrator should create an application entry in the PingOne account.

During this process, an application ID will be generated. This application ID is used by the customer server and the customer mobile application for identification of the customer mobile application in PingID SDK.

The administrator's role in a PingID SDK application's lifecycle comprises the following activities:

Configuring a new PingID SDK app

Creation of an entry for a new PingID SDK application in the admin portal with a basic default configuration.

Updating a PingID SDK app's configuration

Configuration of an existing PingID SDK application's settings, applying changes to the default configuration, and other updates to the application's configuration, as might be required during the app's lifecycle.

Enabling or disabling a PingID SDK app

Configuration of a PingID SDK application's enabled or disabled state.

Distributing the PingID SDK settings file and application ID

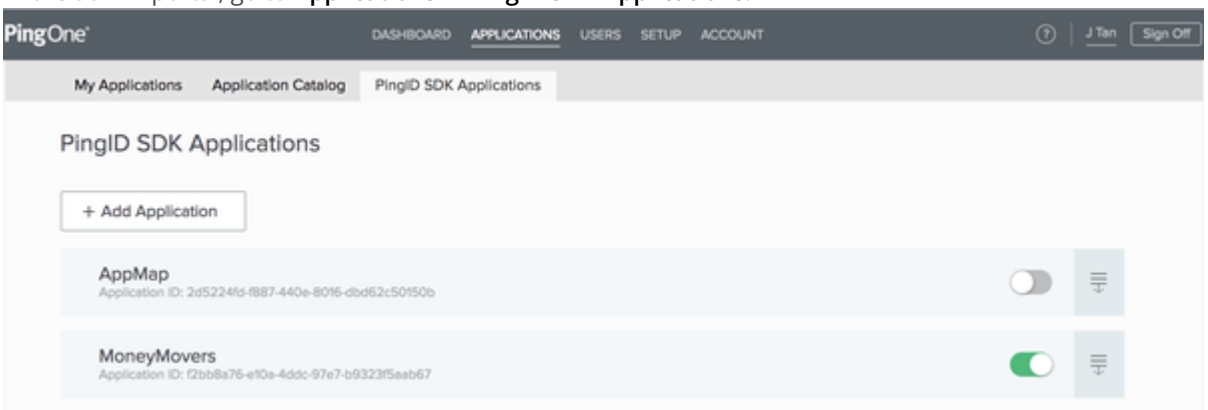
Retrieval of resources required for distribution to developers, in order for them to integrate the PingID SDK component into their mobile application code.

Configuring a new PingID SDK app

Create and configure a new PingID SDK application in the admin web portal.

Steps

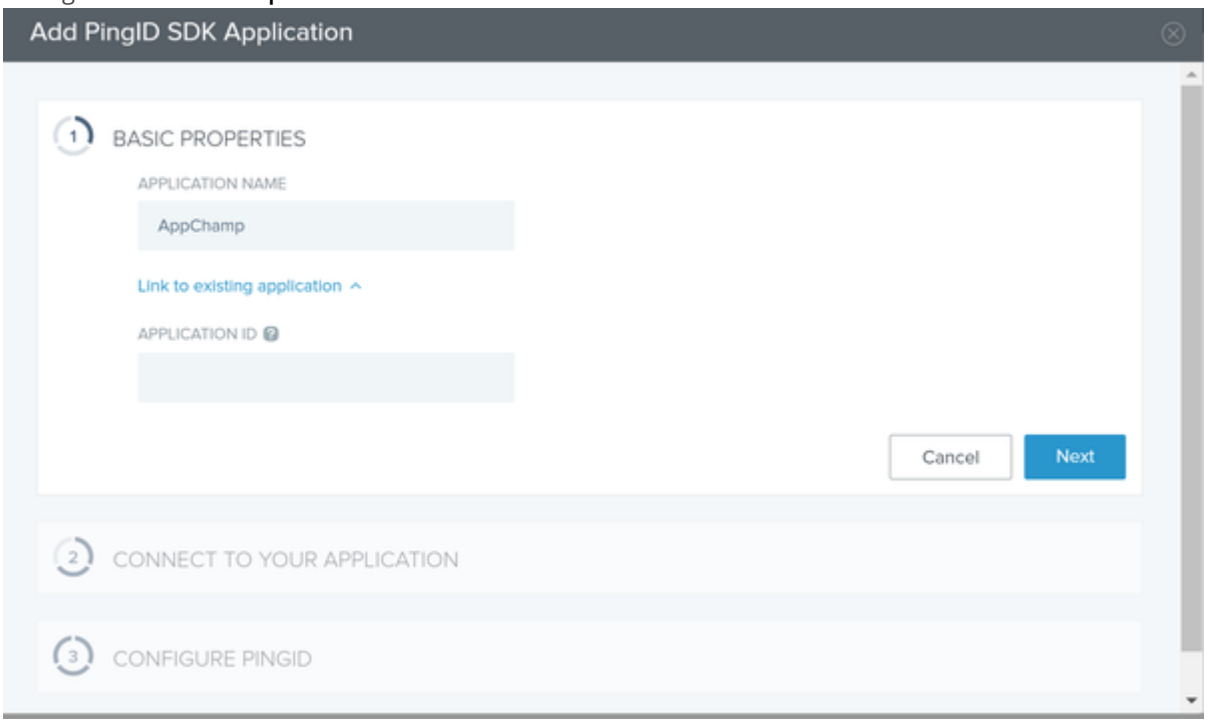
1. In the admin portal, go to **Applications → PingID SDK Applications**.



   If there are applications already defined for your organization, they are listed on this page.

2. To open the **Add PingID SDK Application** wizard, click **+ Add Application**.

3. Configure the **Basic Properties** fields:



   1. In the **Application Name** field, enter the application name.

      > **Note**
      >
      > The **Application Name** field is required, and each name must be unique. If the name is in use, an error message appears and the **Next** button is disabled.
      > Whitespaces are permitted, except for the first and last characters.

   2. To enter the **Application ID** (UUID) of a shared application that is already registered in another PingOne tenant, click **Link to existing application**.

      > **Note**
      >
      > Any **Application ID** can appear only once in an organization's list of registered PingID SDK applications. A link icon appears next to a linked application, both in the original organization and in the organization referencing the **Application ID**.

   3. Click **Next**.

4. Configure the **Connect to your application** fields:

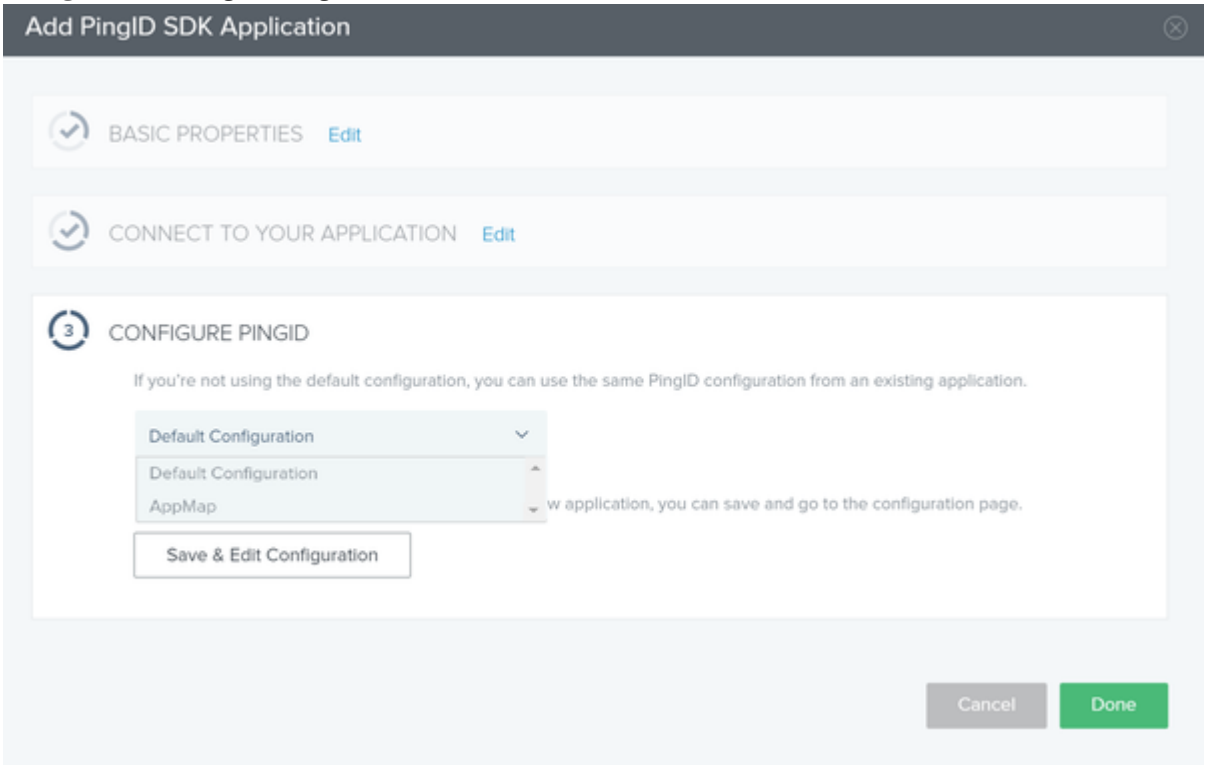
   Choose from:

   - On iOS: You can upload and associate separate certificate files for the Sandbox and for Production.
   - On Android: Both of the connection details fields, **Sender ID** and **Server Key**, can either be left blank or must both be filled.

+ image::div1569483765690.png[alt="Screen capture illustrating the Connect To Your Application section of the Add PingID SDK Application window.",role="border-no-padding"]

1. Click **Next**.

5. Configure the **Configure PingID** fields:



The **Configure PingID** section lets you:

- Access the **Configuration Edit** window directly.
- Simplify the configuration process by allowing you to copy the configurations of an existing application. This feature is only available after at least one application has been configured.

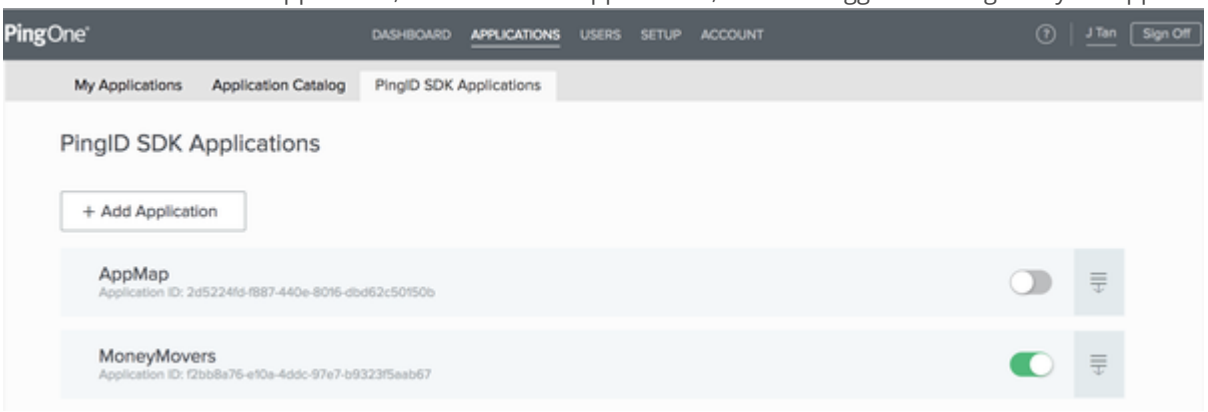
> **Note**
>
> - When there are more than 5 applications, a **Search** field appears. Entering part of an application's name in the **Search** field immediately shortens the returned list of apps to entries that contain the input search string.
> - If you choose an already existing application configuration, all of its configurations automatically apply to the new application.
> - Any of the configuration settings can be changed.
> - Updating a configuration setting in either the original application or the newly created application does not have any impact on the other application's configuration.

1. From the **Configuration** list, select a configuration or predefined application to copy its configuration.
2. To navigate directly to the app's **Integration** and **Configuration** tabs or to view or change the configuration settings, click **Save & Edit Configuration**.

For more information, see Updating a PingID SDK app's configuration.

1. To save the app's integration and configuration settings as defined with the wizard and return to the**PingID SDK Applications** list, click **Done**.

6. Go to **Applications → PingID SDK Applications**.
7. To enable or disable an application, from the list of applications, click the toggle to the right of your application.



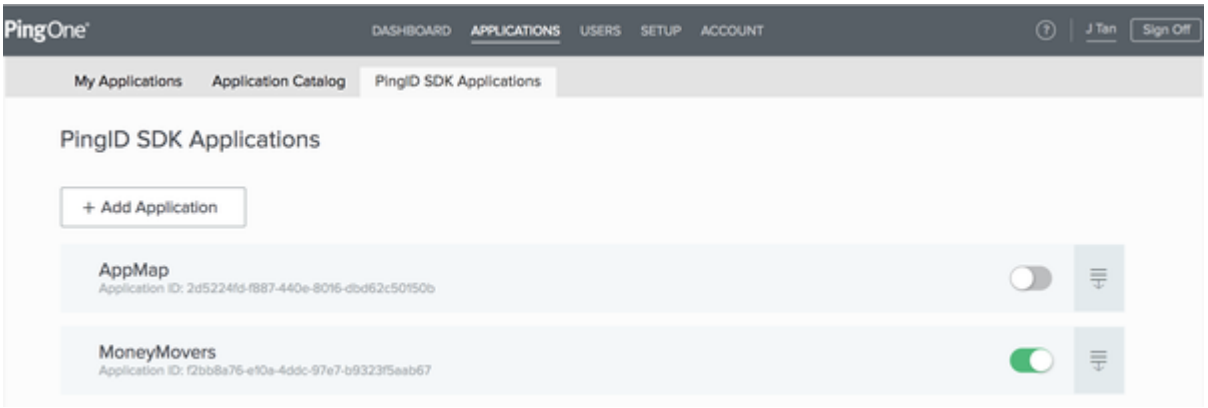
Updating a PingID SDK app's configuration

About this task

The following steps describe all the configurable options available for a PingID SDK app.

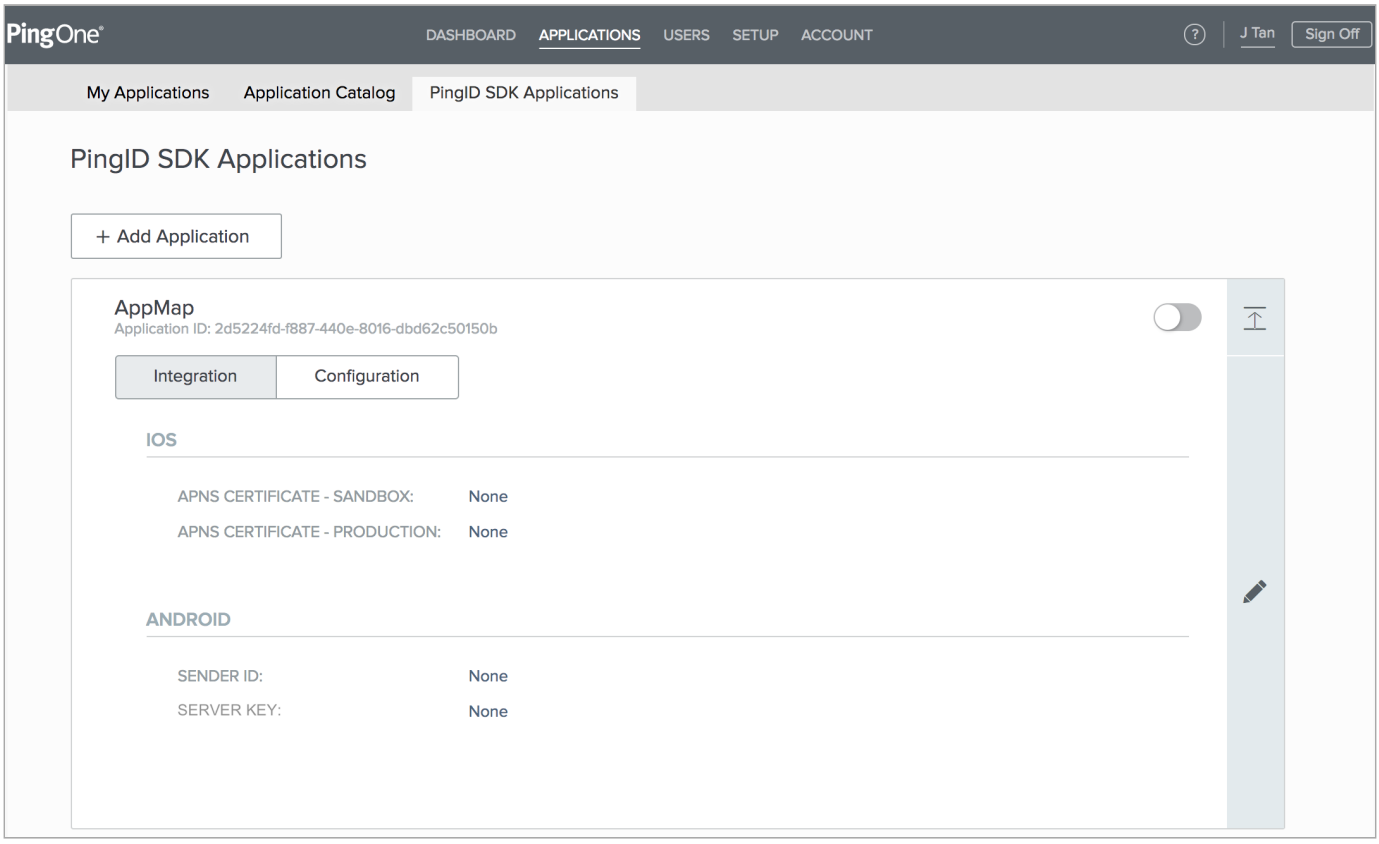
Steps

1. Log in to the admin web portal.
2. Select **Applications → PingID SDK Applications**.



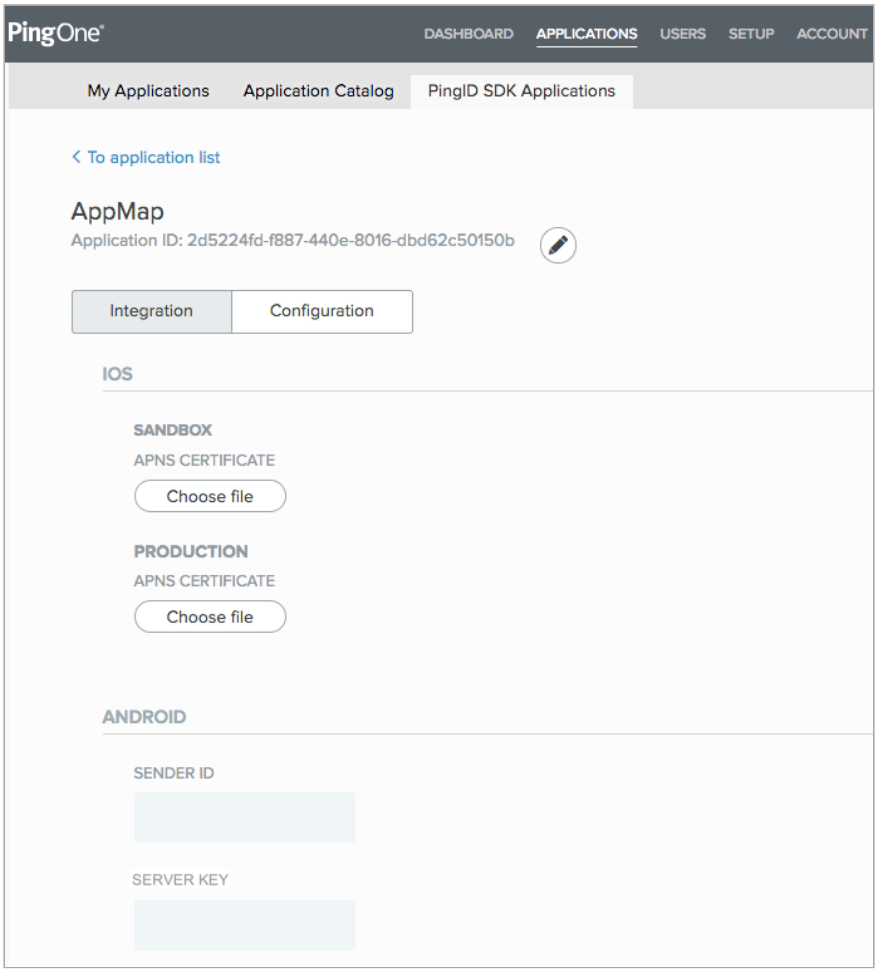
If there are apps already defined for your organization, they will be listed on this page.

3. Select the **Down arrow** icon to the right of the app you want to configure, to expand the view. Click the **Pencil** icon in the right margin to edit the app's settings.



4. Click the **Pencil** icon to the right of the app name, to change the name that appears in the application list.

   The system checks that there are no other apps registered for this organization with the identical name.



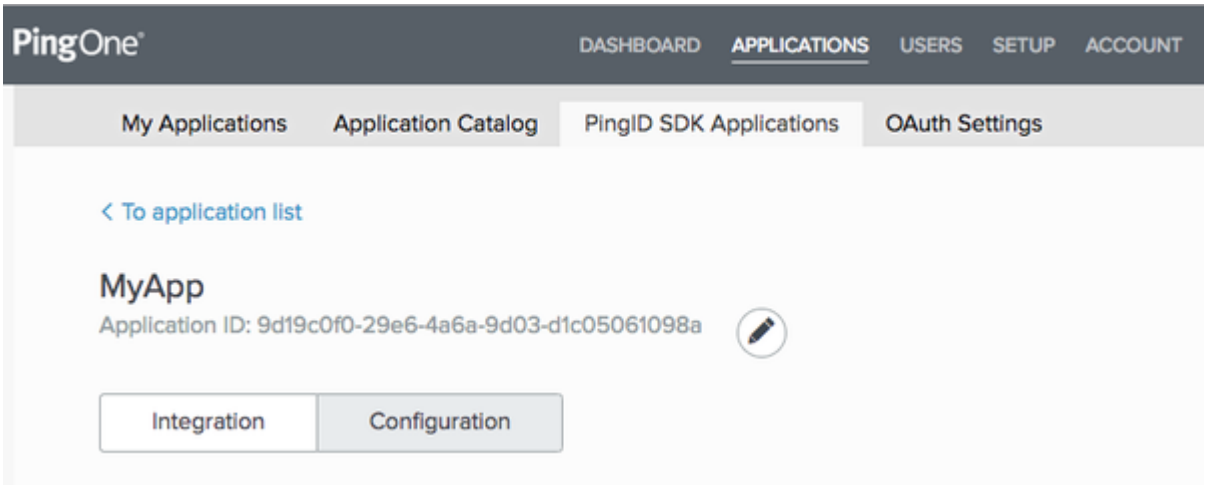
Select **Save** to save your changes.

5. Select the **Integration** tab to view the iOS and Android connection settings for the app. Click the **Pencil** icon in the right margin, to edit the settings.

    - **iOS**: You can upload and associate separate certificate files, for the **SANDBOX** and for **PRODUCTION**. When uploading a certificate file, a prompt appears for the **CERTIFICATE PASSWORD**. By selecting the **Eye** icon toggle, you can choose whether the password will be displayed on the screen, or masked.

    - **Android**: Both of the connection details fields, **SENDER ID** and **SERVER KEY**, may either be left blank, or both must be filled. Select **Save** to save your changes.

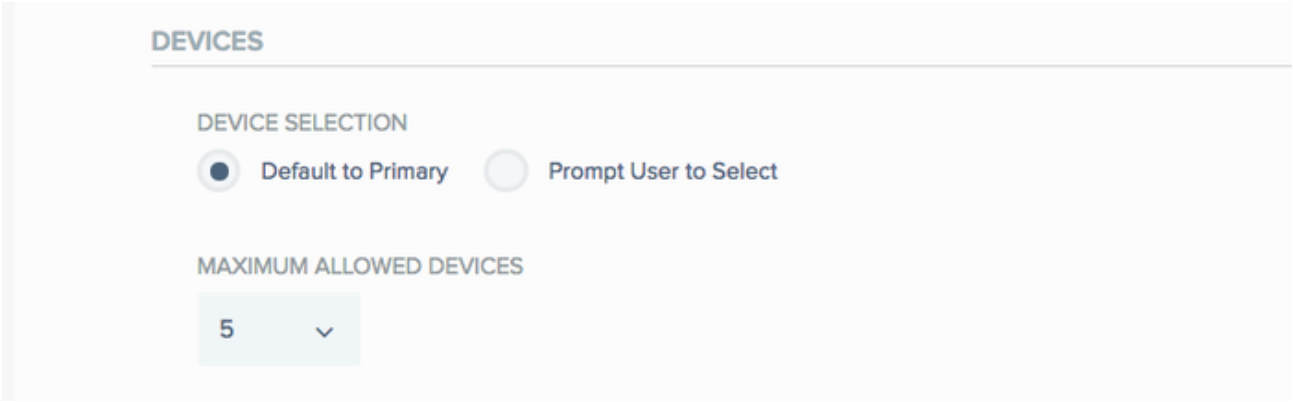
6. Select the **Configuration** tab to view the app's PingID configuration settings. Click the **Pencil** icon to edit the settings.



Important

Changes to the configuration will only take effect for new pairings.

1. **DEVICES**:



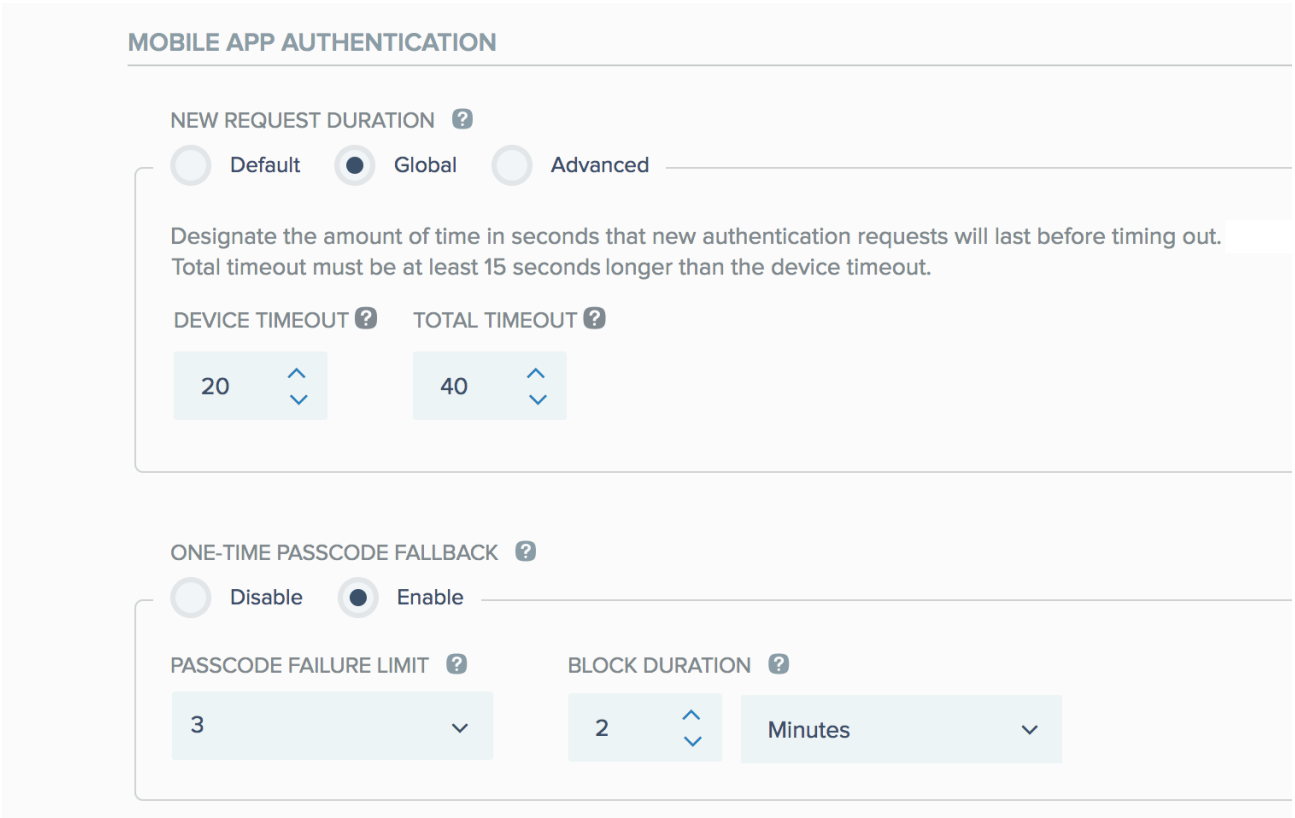
- **DEVICE SELECTION**:
  - **Default to Primary** is the default option for users to be automatically authenticated with their primary device.

    Note

    If the user doesn't have a primary device, they will automatically be prompted with the first best fitting trusted device:
    - If the first device is a mobile phone, it will be regarded as the primary device.
    - If the first paired device is not a mobile phone (for example an iPad), and there is another paired device which is a mobile phone, then the mobile phone will be regarded as the primary device.
  - **Prompt User to Select** for users to receive a prompt on each authentication to choose the device to use.

- **MAXIMUM ALLOWED DEVICES**:
  - You may determine the **MAXIMUM ALLOWED DEVICES** that each user can have. The default value is 5, the minimum is 1, and the maximum value is 15. The user will not be able to add more devices for authentication than the maximum number that was configured. Assuming that **Prompt user to select** was chosen, this is the maximum number of devices the user will see listed, and be able to choose from, for authentication.
  - Possible error codes returned:
    - Top level error code: `REQUEST_FAILED`
    - Detailed error code: `SIZE_LIMIT_EXCEEDED`

2. **MOBILE APP AUTHENTICATION**:



- **NEW REQUEST DURATION**:

  You can configure the amount of time that an authentication request lasts before timing out. Use this feature to customize the authentication experience to your user's needs, and reduce the number of users that experience a push notification timeout on authentication attempts.

  An authentication request's duration is determined by two configurable measurements:

  - **Device Timeout**: The amount of time in seconds that a new authentication request notification must reach a user's mobile device, before timing out.
  - **Total Timeout**: The total amount of time in seconds that a new authentication request will last, before timing out. This includes the time for **Device Timeout**, plus the time that the user has to respond to the authentication request.

- Select **Default** to use the system's default timeout values:
  - Device timeout default: 20 seconds
  - Total timeout default: 40 seconds.
- Select **Global** to apply a custom **Device Timeout** value and a custom **Total Timeout** value globally to all mobile application authentication requests, irrespective of where the request originated.

> **Note**
>
> The value in the **Total Timeout** field must be at least 15 seconds greater than the value in the **Device Timeout** field.

Timeout setting	Device Timeout	Total Timeout
Minimum	15 seconds	40 seconds
Maximum	40 seconds	150 seconds
Default	20 seconds	40 seconds

- Select **Advanced** to apply individual custom **Device Timeout** and **Total Timeout** values to each origin of mobile application authentication requests.

> **Note**
>
> The valid values range appears in parentheses for each origin's timeout. The value in the **Total Timeout** field must be at least 15 seconds greater than the value in its corresponding **Device Timeout** field.

Configure timeout values of mobile application authentication requests according to their origins:

- **API**

  The amount of time in seconds for a new authentication request notification before timing out, for any API request that does not originate from either the CIBA Authenticator (version 1.1.2 and later) or from the PingID SDK Adapter (version 1.8.2 and later).

Timeout setting	Device Timeout	Total Timeout
Minimum	15 seconds	40 seconds
Maximum	40 seconds	150 seconds
Default	20 seconds	40 seconds

- **CIBA**

  The amount of time in seconds for a new authentication request notification before timing out, for any API request that originates from the CIBA Authenticator.

> **Note**
>
> Relevant from CIBA Authenticator 1.1.2.
> If the CIBA Authenticator version is earlier than 1.1.2, the **API** timeout configuration is applied.

Timeout setting	Device Timeout	Total Timeout
Minimum	15 seconds	40 seconds
Maximum	40 seconds	150 seconds
Default	20 seconds	40 seconds

■ **SDK Adapter**

The amount of time in seconds for a new authentication request notification before timing out, for any API request that originates from the PingID SDK Adapter for PingFederate.

> **Note**
>
> Relevant from SDK Adapter 1.8.2.
> If the SDK Adapter version is earlier than 1.8.2, the **API** timeout configuration is applied.

Timeout setting	Device Timeout	Total Timeout
Minimum	15 seconds	40 seconds
Maximum	40 seconds	150 seconds
Default	20 seconds	40 seconds

■ **Extra verification silent push**

If **Verify Devices** is enabled, you can configure the duration of the **Device Timeout** of the additional silent verification notification.

Timeout setting	Device Timeout
Minimum	3 seconds
Maximum	15 seconds
Default	7 seconds

■ **QR code**

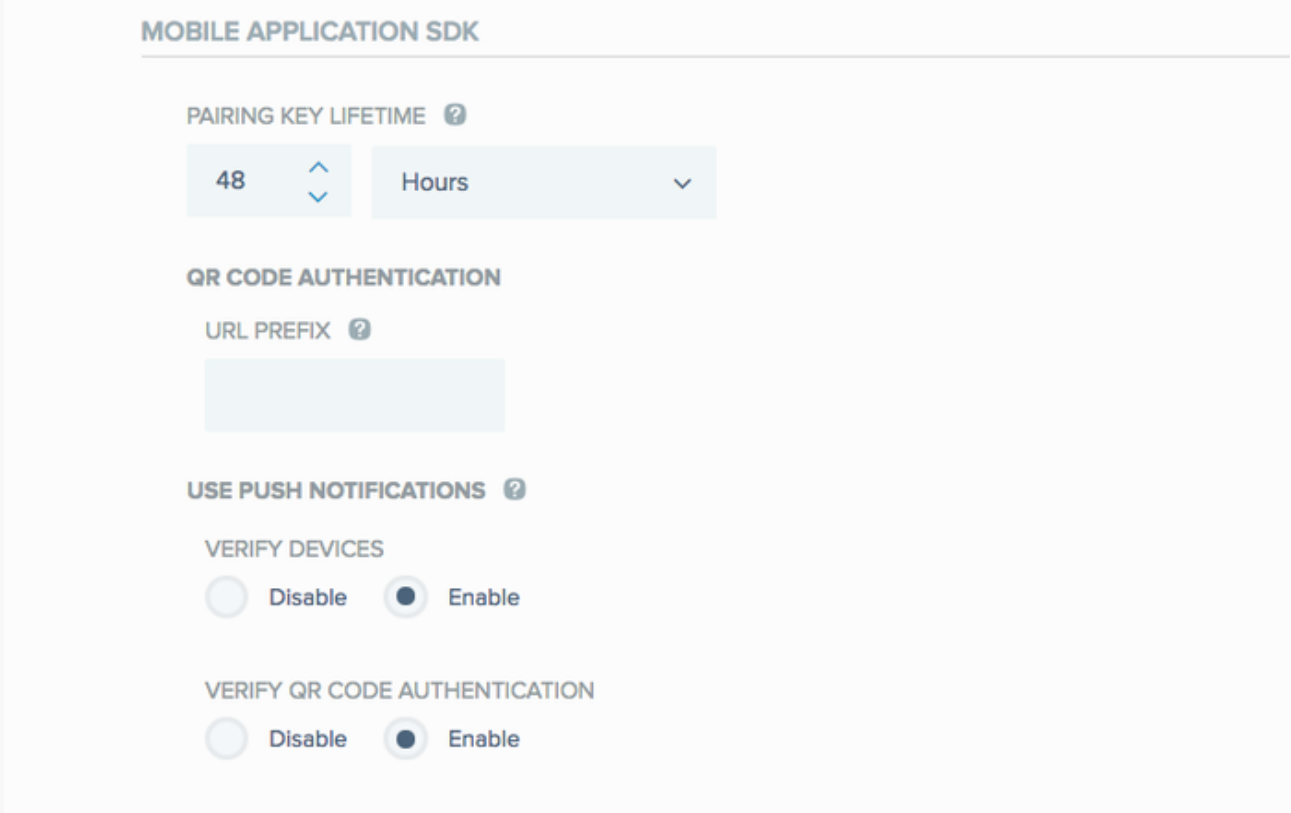
If **Verify QR Code Authentication** is enabled, you can configure the duration of the **Device Timeout** of the QR code's additional silent verification notification.

Timeout setting	Device Timeout
Minimum	1 second
Maximum	15 seconds
Default	7 seconds

- **ONE-TIME PASSCODE FALLBACK**:
  - **Enable** (default): Upon mobile app response timeout, or if the device is pushless, the user will be presented with the OTP input screen, and may use OTP to authenticate.
    - **PASSCODE FAILURE LIMIT**: The maximum number of times that the OTP entry can fail for a user, before they are blocked.
      Default: 3
      Minimum: 1
      Maximum: 7
    - **BLOCK DURATION**:
      The amount of time a user's device will be blocked if they exceed the maximum number of passcode failures. The duration may be set in units of minutes or seconds.
      Default: 2 minutes
      Minimum: 2 minutes
      Maximum: 30 minutes
  - **Disable**:
    Upon mobile app response timeout, the user will not be able to authenticate using OTP as an alternative.

> **Important**
>
> Customized **PASSCODE FAILURE LIMIT** and **BLOCK DURATION** values are not saved when **ONE-TIME PASSCODE FALLBACK** is set to **Disable**. The next time it is enabled, these configurable settings initial values will be reset to the system default.

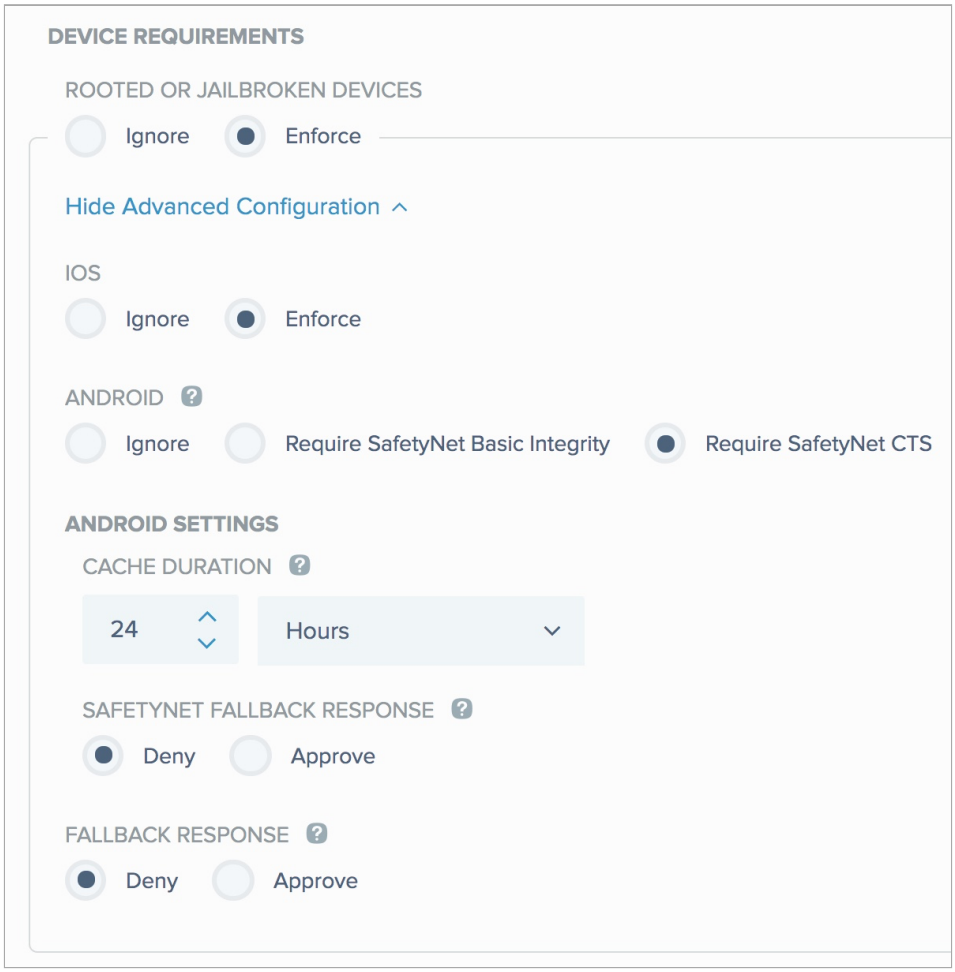
3. **MOBILE APPLICATION SDK**:



- **PAIRING KEY LIFETIME**: Set the duration of validity in minutes, hours or days for a manual pairing key, before it expires. The default is 48 hours, and the maximum is 31 days.
    - Possible status or error returned:
        - Top level error code: `NOT_FOUND`
- **QR CODE AUTHENTICATION**:
    - **URL PREFIX**: Provide the application's URI prefix (URL or URI scheme), to which a user will be directed after successfully scanning the QR code or clicking the deep link.
        - The **URL PREFIX** must conform to the following requirements:
            - A string of up to 30 characters starting with an English character (a-z)
            - Subsequent characters may comprise only English alphanumerics (a-z, 0-9), the plus (+), minus (-) or dot(.) characters.
        - The resulting URL will have the format `[URL PREFIX]://pingidsdk?authentication_token=[generated_token]`. For example, if the Moderno application scheme (**URL PREFIX**) is "moderno", the resulting URL is: `moderno://pingidsdk?authentication_token=[generated_token]`.
        - If the **URL PREFIX** is not specified, the QR code content is only the generated token, and the resulting URL has the format: `pingidsdk?authentication_token=[generated_token]`. In this case, the user must use the camera from within the application.

- When using the mobile browser, it is logical that this scheme should display the resulting URL as a deep link instead of the QR code. In such a case, when the user clicks the link, they will be navigated to the app specified in the application scheme. If the application scheme is not configured, the deep link won't work.

- **USE PUSH NOTIFICATIONS**:
  - **VERIFY DEVICES**: Select **Enable** to use the Apple or Android push server to provide extra verification during device authorization. This is the default setting.
  - **VERIFY QR CODE AUTHENTICATION**: Select **Enable** to use the Apple or Android push server to provide extra verification during QR code based authentication. This is the default setting.
- **DEVICE REQUIREMENTS**:



  - **ROOTED OR JAILBROKEN DEVICES**:

> **Note**
>
> Root and jailbroken devices detection can be invoked for applications built with:
> - PingID Mobile SDK for Android 1.4 and later
> - PingID Mobile SDK for iOS 1.4 and later
>
> **iOS only**: We recommend using PingID Mobile SDK for iOS 1.6.1 or later. When the check for jailbroken devices is activated, applications using PingID Mobile SDK for iOS versions before 1.6.1 for authentication are regarded as missing the required data to determine whether the device is jailbroken. Those requests proceed according to the **FALLBACK RESPONSE** configuration.

The default setting is **Ignore**.
Select **Enforce** to check integrity of devices as part of the MFA flow, and detect rooted or jailbroken devices. Click **Show Advanced Configuration** to configure the following parameters:

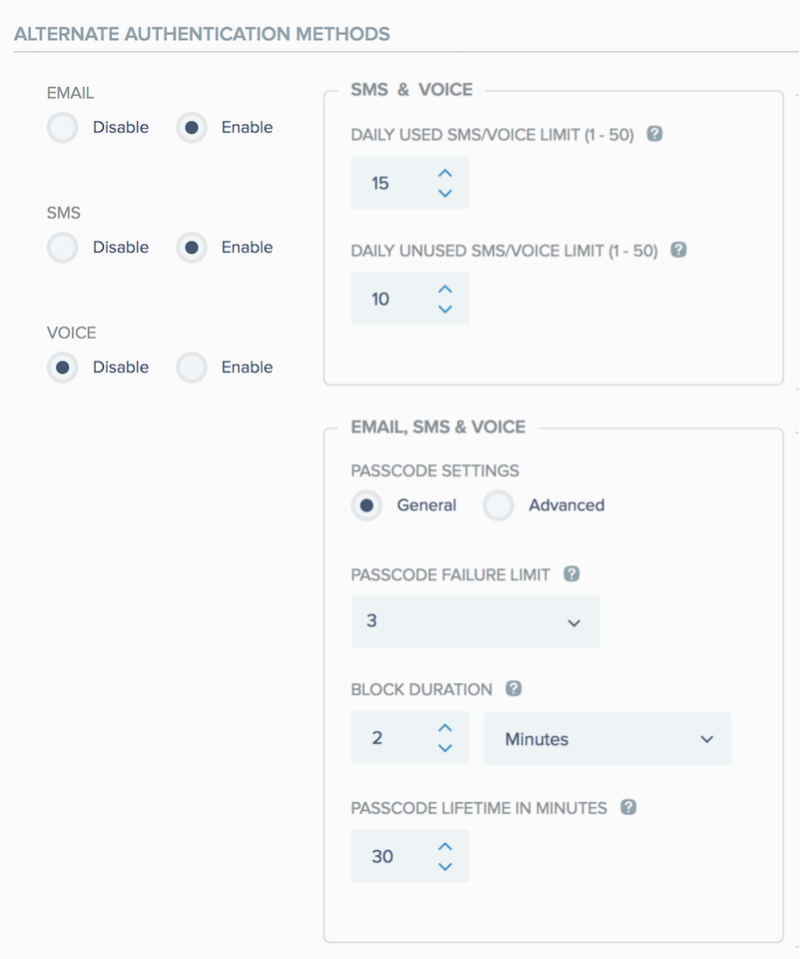
- **IOS**: The PingID SDK integrity check solution uses its proprietary algorithm to determine if an iOS mobile device is jailbroken.
  - **Ignore** jailbreak detection for iOS devices.
  - Select **Enforce** to check the integrity of iOS devices and to detect jailbroken iOS devices (default).
- **Android**: The PingID SDK root detection solution utilizes Google's SafetyNet attestation API to determine the integrity of Android mobile devices.
  See Google's documentation for further information about SafetyNet integrity levels: https://developer.android.com/training/safetynet/attestation.html#potential-integrity-verdicts
  - **Ignore** root detection for Android devices.
  - Select **Require SafetyNet Basic Integrity** for the basic integrity check.
  - Select **Require SafetyNet CTS** to return a verdict for the more stringent Compatibility Test Suite standard (default).
- **ANDROID SETTINGS**: Configurable when **Require SafetyNet Basic Integrity** or **Require SafetyNet CTS** are selected.
  - **CACHE DURATION**: Since SafetyNet is an external service provided by Google, every attestation request entails a certain time tradeoff. You may choose to cache successful SafetyNet calls for a predefined duration, between a minimum of 1 minute and a maximum of 48 hours.

    > **Caution**
    >
    > Reducing this period once it has already been set, may cause users to fail MFA authentications, forcing them to re-authenticate.

- **SAFETYNET FALLBACK RESPONSE** Determine if PingID SDK should consider a failed SafetyNet response as a rooted or non-rooted device. Following an Android device's pairing or authentication request, determine whether the request will be granted, if SafetyNet doesn't respond in time, or if Google Play is not installed on the device:
  - **Deny** the Android device's pairing or authentication request. This is the default setting.
  - **Approve** the Android device's pairing or authentication request.

- **FALLBACK RESPONSE**: Determine PingID SDK's behavior when an authentication or pairing request is missing the required data to determine the requesting device's integrity.
  This could occur in apps using old mobile SDK component versions, or in apps using a new mobile component versions that call the root detection API with a false flag. The **Approve** setting may assist in a gradual rollout of the integrity check to all users.
  Following an Android or iOS device's pairing or authentication request, determine whether the request will be granted, if the rooted or jailbroken status of the device can't be determined:
  - **Deny** the device's pairing or authentication request. This is the default setting.
  - **Approve** the device's pairing or authentication request.

4. **ALTERNATE AUTHENTICATION METHODS**:



- **EMAIL**:
  The default setting is **Disable**.
  Select **Enable** to permit users to authenticate via email. When **EMAIL** is selected, a one time passcode will be sent to the user's email address.

  > **Note**
  >
  > PingID SDK supports use of your organization's own trusted email domains and email addresses, using the PingID SDK APIs. This reinforces trust from the customer and also from the receiving servers. The APIs provide a further option to configure DKIM and SPF verification for outbound emails. In the PingID SDK developer's guide, see:
  >
  > - Trusted email domains
  > - Trusted email addresses
  > - Email templates
  > - Authenticate with email

- **SMS**:
  The default setting is **Disable**.
  Select **Enable** to permit users to authenticate via SMS. The **SMS & VOICE** daily limits configuration options appear.

- **VOICE**:
  The default setting is **Disable**.
  Select **Enable** to permit users to authenticate via VOICE. The **SMS & VOICE** daily limits configuration options appear.

- **SMS and VOICE daily limits**:

  When SMS or VOICE are selected, admins have the option to configure the daily limit for users' SMS and VOICE authentications:

  - **DAILY USED SMS/VOICE LIMIT: 1-50:** (default = 15).

    Configure the maximum combined number of SMS and VOICE authentication requests a user may receive and respond to each day.

    - Possible status or error returned:

      - Top level error code: `INVALID_REQUEST`
      - Detailed error code: `SMS_QUOTA_EXCEEDED`

  - **DAILY UNUSED SMS/VOICE LIMIT: 1-50:** (default = 10).

    Configure the maximum combined number of SMS and VOICE authentication requests a user may receive and not respond to each day.

    - Possible error codes returned:

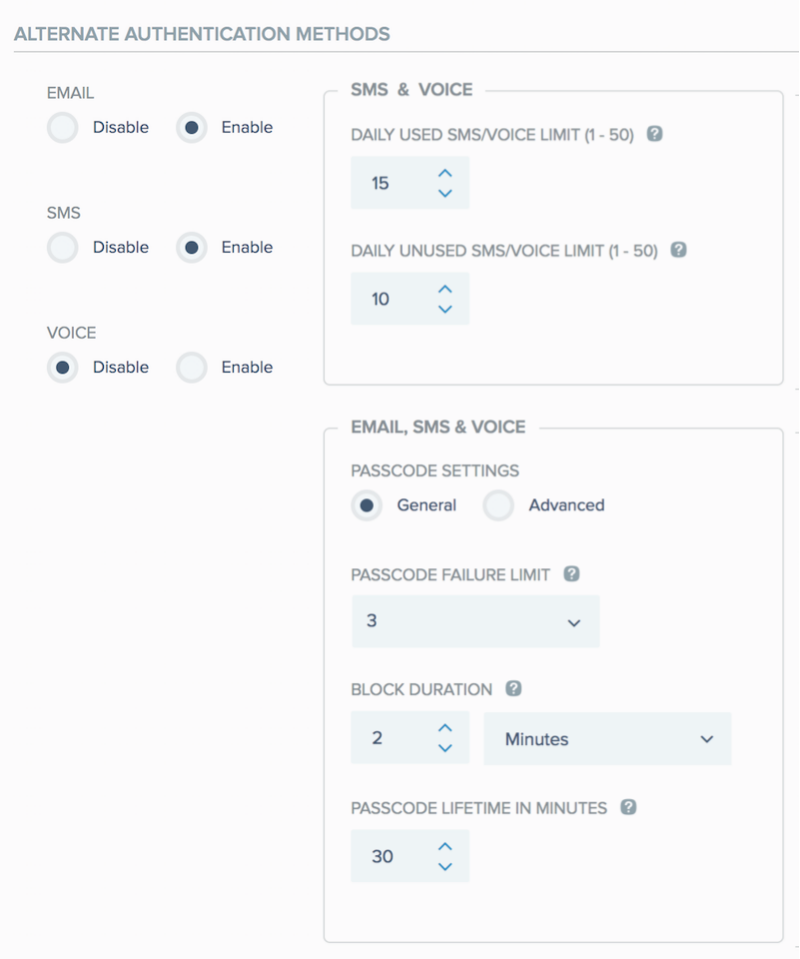
      - Top level error code: `REQUEST_FAILED`
      - Detailed error code: `SMS_QUOTA_EXCEEDED`

- **PASSCODE FAILURE LIMIT**, **BLOCK DURATION** and **PASSCODE LIFETIME IN MINUTES** for EMAIL, SMS and VOICE:

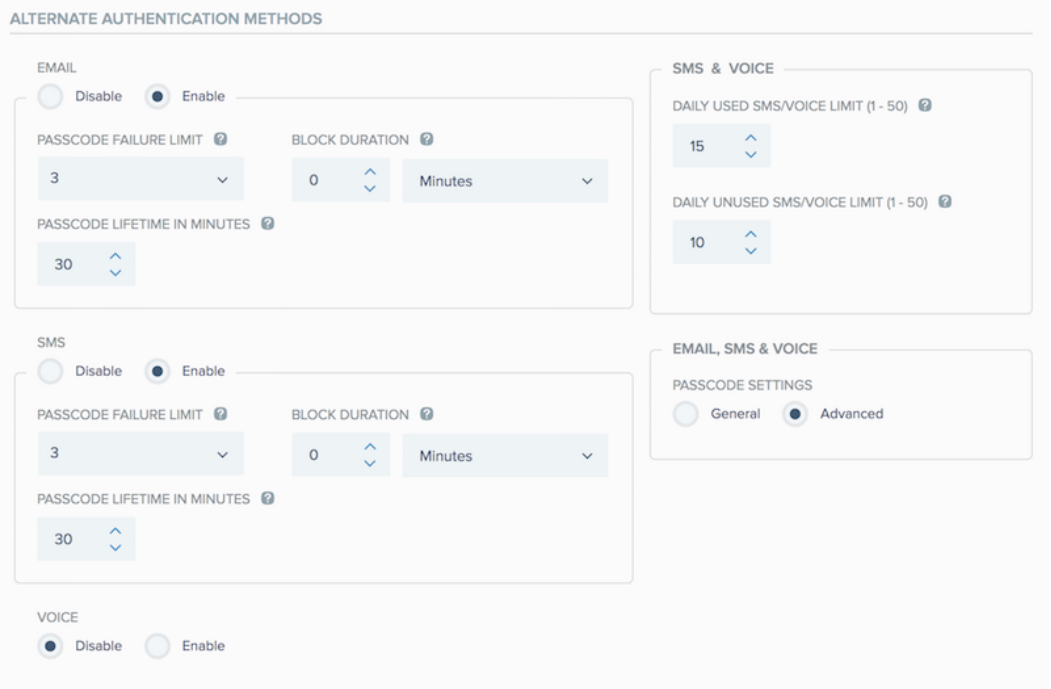
  When at least one of EMAIL, SMS or VOICE is enabled, admins have the option to configure the permitted number of OTP attempt failures before a user is blocked, the duration of the block, or the duration of an OTP.

  - **PASSCODE SETTINGS**:

    - **General**:
      Admins can configure a single **PASSCODE FAILURE LIMIT**, **BLOCK DURATION** and **PASSCODE LIFETIME IN MINUTES**, which will apply equally to all of the enabled EMAIL, SMS and VOICE options.



- **Advanced**:
  Admins can configure a separate individual **PASSCODE FAILURE LIMIT**, **BLOCK DURATION** and **PASSCODE LIFETIME IN MINUTES** for each of the enabled EMAIL, SMS and VOICE options.



- **PASSCODE FAILURE LIMIT**:
  The maximum number of times that the OTP entry can fail for a user, before they are blocked.
  Default: 3
  Minimum: 1
  Maximum: 7
  After reaching the maximum number of failure attempts, the flow ends and the exits the OTP entry screen.

- **BLOCK DURATION**:
  The amount of time a user's device will be blocked if they exceed the maximum number of passcode failures. The duration may be set in units of minutes or seconds.
  Default: 0 minutes (not blocked)
  Minimum: 0 minutes
  Maximum: 30 minutes

- **PASSCODE LIFETIME IN MINUTES**:
  The amount of time an OTP is valid before it expires.
  The duration may be set in units of minutes.
  Default: 30 minutes
  Minimum: 1 minute
  Maximum: 30 minutes

- **Authentication** scenarios:
  All of the **PASSCODE FAILURE LIMIT**, **PASSCODE LIFETIME IN MINUTES** and **BLOCK DURATION** settings apply for authentication attempts.

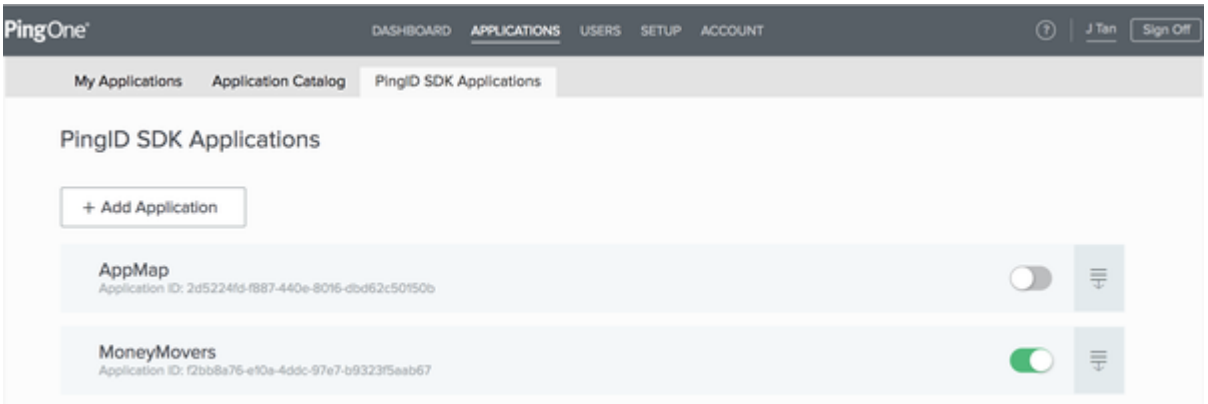
- **Pairing** scenarios:
  Only the **PASSCODE FAILURE LIMIT** and the **PASSCODE LIFETIME IN MINUTES** apply for pairing attempts, whereas **BLOCK DURATION** does not apply.

- When switching configurations between the **General** and **Advanced** modes, only the current mode's **PASSCODE FAILURE LIMIT**, **BLOCK DURATION** and **PASSCODE LIFETIME IN MINUTES** settings are saved. Switching back to the other mode will not reinstate its previously saved configuration, but rather, it will reset back to its default values.

> **Important**
>
> Customized parameter values such as **PASSCODE FAILURE LIMIT**, **BLOCK DURATION** and **PASSCODE LIFETIME IN MINUTES** are not saved for the specific **EMAIL**, **SMS** or **VOICE** feature, if that feature is set to **Disable**. The next time it is enabled, these configurable settings initial values will be reset to the system default.

> **Note**
>
> **Dedicated SMS and VOICE subaccounts**:
> PingID SDK supports a dedicated subaccount for pairing and authentication with SMS and VOICE one time passcodes (OTPs). You can determine the amount of dedicated phone numbers and the country-code from which the SMS and VOICE messages will be sent to the users.
> For further details and to activate subaccounts, contact Ping Support.
>
> - Note that if you wish to delete a subaccount's dedicated number, users associated with the deleted number will receive their OTP messages from one of the PingID primary account's assigned numbers for 2 minutes until completion of the deletion process. Once the deletion process is complete, they will receive their OTP messages from one of the subaccount's remaining numbers.

7. Select **Save** to save your changes.
8. In the **Applications → PingID SDK Applications** list, select the gray/green toggle to the right of your app to **Enable** or **Disable** it.

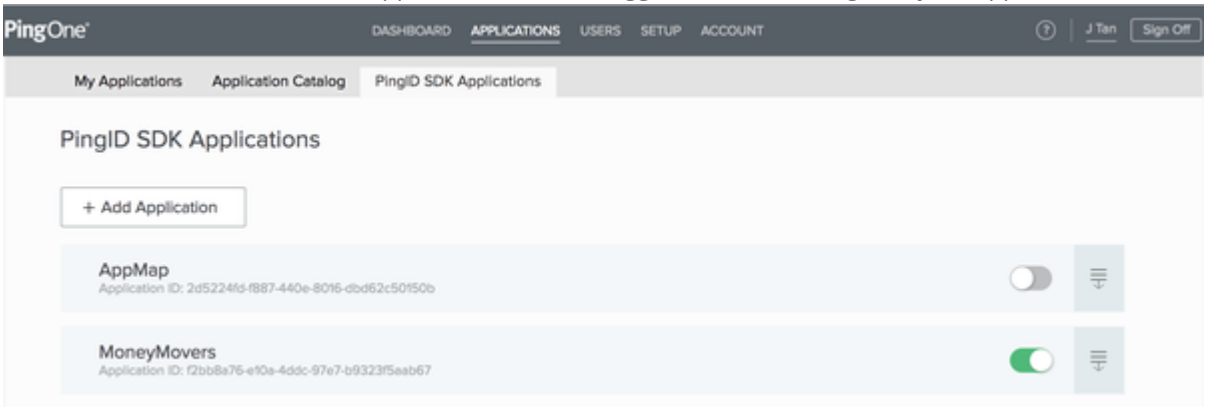


Enabling or disabling a PingID SDK app

Enable or disable a PingID SDK application.

Steps

1. In the admin web portal, go to **Applications → PingID SDK Applications**.
2. To enable or disable the desired application, click the toggle button to the right of your app.



Distributing the PingID SDK settings file and application ID

Distribute the PingID SDK settings file and application ID to integrate the component into the application code.

About this task

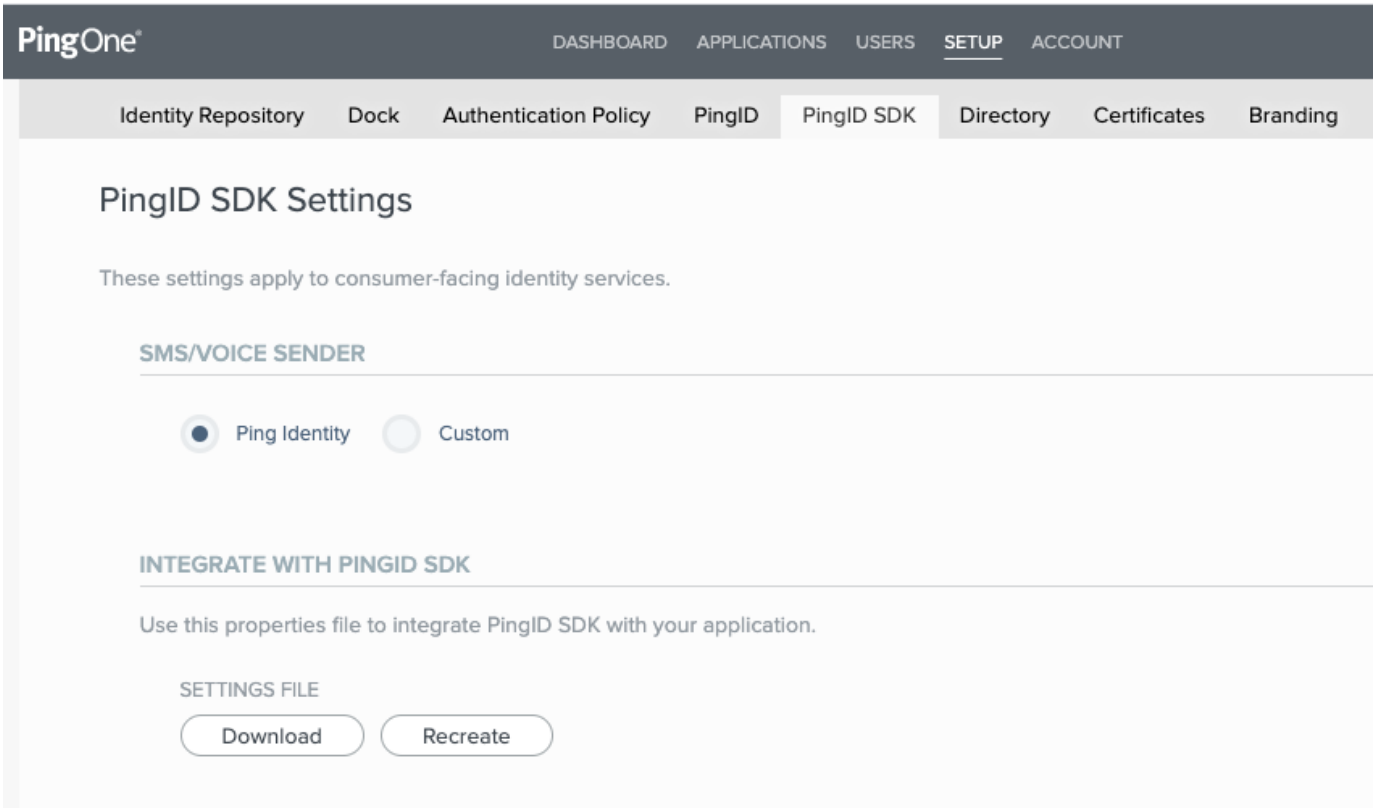
Application developers require the following resources in order to integrate the PingID SDK component into their application code:

- PingID SDK settings file
- Application ID

Administrators download the PingID SDK settings file and access the application ID in the administrative web portal for distribution to the application developers.

Steps

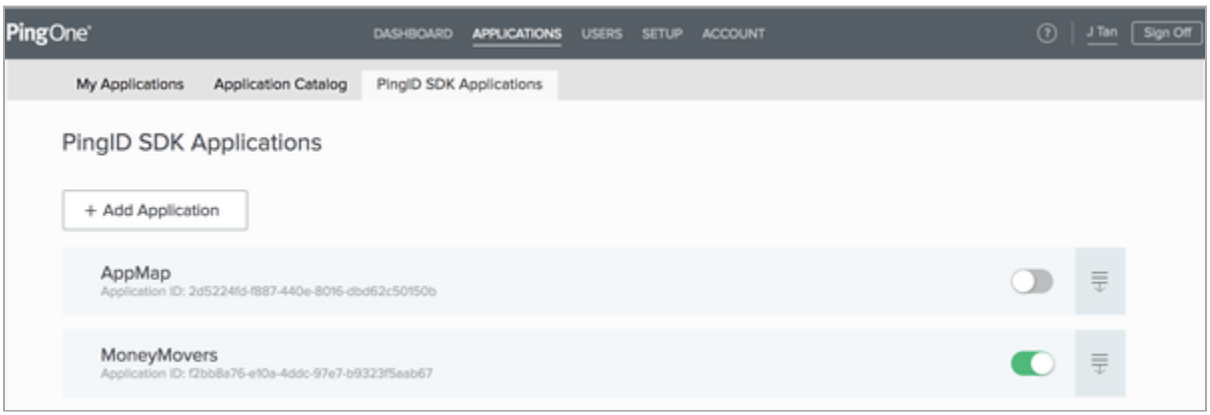
1. In the admin web portal, go to **Setup → PingID SDK → Integrate with PingID SDK → Settings File → Download**.



2. From the PingOne web portal, go to **Applications → PingID SDK Applications**.

   Result:

   The **Application ID** displays below the application's name.



Using a custom Twilio account with PingID SDK

Using a custom Twilio account with PingID SDK

If you have an existing custom Twilio account, you can configure PingID SDK to use it for SMS or voice pairing and authentication.

Keep the following points in mind:

Daily used SMS/voice limits

- PingOne full license accounts - The daily SMS and voice limits are enforced for fully licensed PingOne accounts that use a custom Twilio account.
- PingOne trial accounts - The daily SMS and voice limits are not enforced for PingOne trial accounts that use a custom Twilio account.

Billing

You must set up your Twilio billing arrangements before you can configure PingID SDK to use your Twilio account.

Multiple Twilio accounts

If you have more than one Twilio account, you can only use one of them. If you have Twilio subaccounts, you can use either:

- The main account
- A single subaccount of the main account

> **Note**
>
> Configuring a custom Twilio account overrides a PingID SDK subaccount if a PingID SDK subaccount is configured.

Inactive Twilio accounts

It is the administrator's responsibility to delete a Twilio account configuration in PingID SDK if the account becomes inactive. For more information on deleting a custom Twilio account from PingID SDK, see Managing a Twilio account for PingID SDK.

Configuring a Twilio account for PingID SDK

Configure PingID SDK for a Twilio account.

About this task

> **Note**
>
> PingID SDK uses Twilio for voice and SMS. By enabling your own Twilio account, you are taking responsibility for despatching SMS and voice messages.

Ensure that you have available your Twilio account SID and auth token. You can copy them as required from the Twilio dashboard. You should also have set up one or more origination phone numbers. The following procedure will guide you in configuring PingID SDK to use your Twilio account.

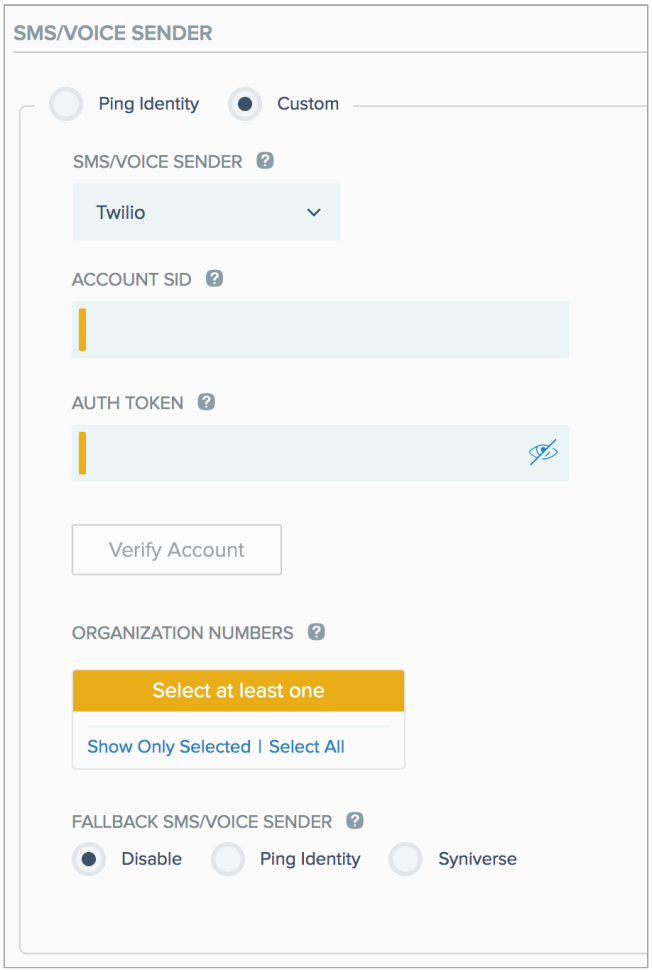
To configure PingID SDK for a Twilio account:

Steps

1. Sign on to the admin console.

2. Go to **Setup → PingID SDK**.
3. Under **SMS/Voice Sender**, choose **Custom**.

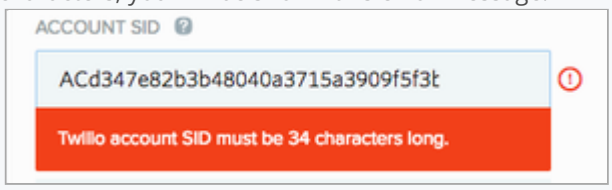
   The custom configuration settings appear.



4. In the **SMS/Voice Sender** dropdown, select **Twilio**.

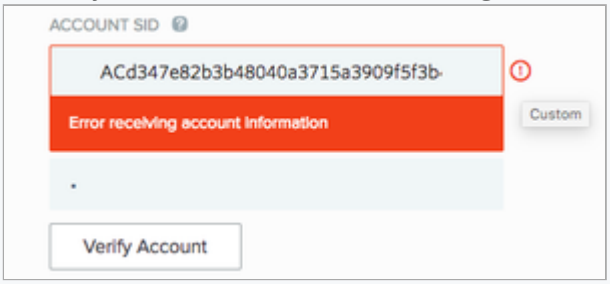
> **Note**
>
> A custom Twilio account applies across all PingID SDK applications of the organization.

5. Copy/paste the Twilio account SID to the indicated field.

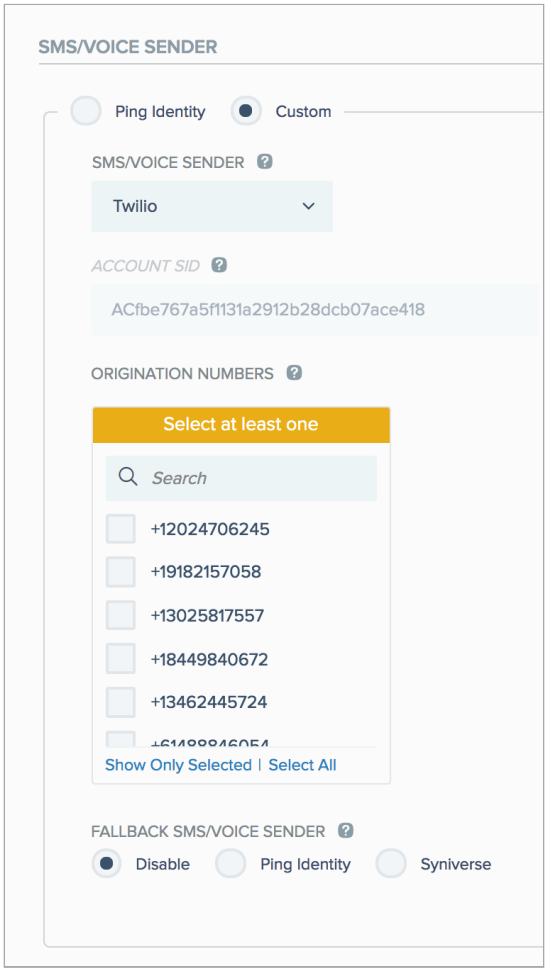
> **Note**
>
> If the SID is shorter than 34 characters, you will be shown this error message:
>
> 
>

6. Copy/paste the Twilio auth token to the indicated field.

7. Click the **Verify Account** button. That validates the account to PingID SDK and populates the **Origination Numbers** list from your Twilio account.

> **Note**
>
> - If the auth token is incorrect, you will be shown this error message:
>
> 
>
>
> - If there are no originating phone numbers in the Twilio account, it will not be validated to PingID SDK.

If the account was successfully verified, the display will change to show a list of originating numbers from Twilio:



8. Select at least one originating telephone number to use.

> **Note**
>
> - Twilio allows you to define phone numbers for use with either voice or SMS or both. PingID SDK uses the same number for both voice and SMS and will so relate to the Twilio defined numbers. Twilio numbers (excluding short codes) that are defined as voice only or SMS only are filtered out from the numbers list to avoid operational errors.
> - Twilio allows the use of sender IDs (in place of telephone numbers) for commercial use or to comply with regulations requiring SMSs to be sent as **transactional** and not **promotional**.
>
> When using the Ping Identity account, all originating numbers are defined as transactional with a sender ID in Twilio. To achieve the same functionality in a custom Twilio account, you must configure it directly in Twilio. **Sender IDs are displayed according to the sender IDs sent in the API requests.** Short codes are supported only for the United States, and only for SMS messages. If only short codes are chosen, but the number is not a United States number:
>
> - If the admin configures **FALLBACK SMS/VOICE SENDER** as **Ping Identity** or **Syniverse**, the selected fallback account's phone numbers are used.
> - If the admin **Disables** the **FALLBACK SMS/VOICE SENDER** option, the SMS will not be sent.

9. Enable **FALLBACK SMS/VOICE SENDER** as **Ping Identity** or **Syniverse** to fall back to one of these alternatives if Twilio becomes unavailable for reasons explained in the following note.

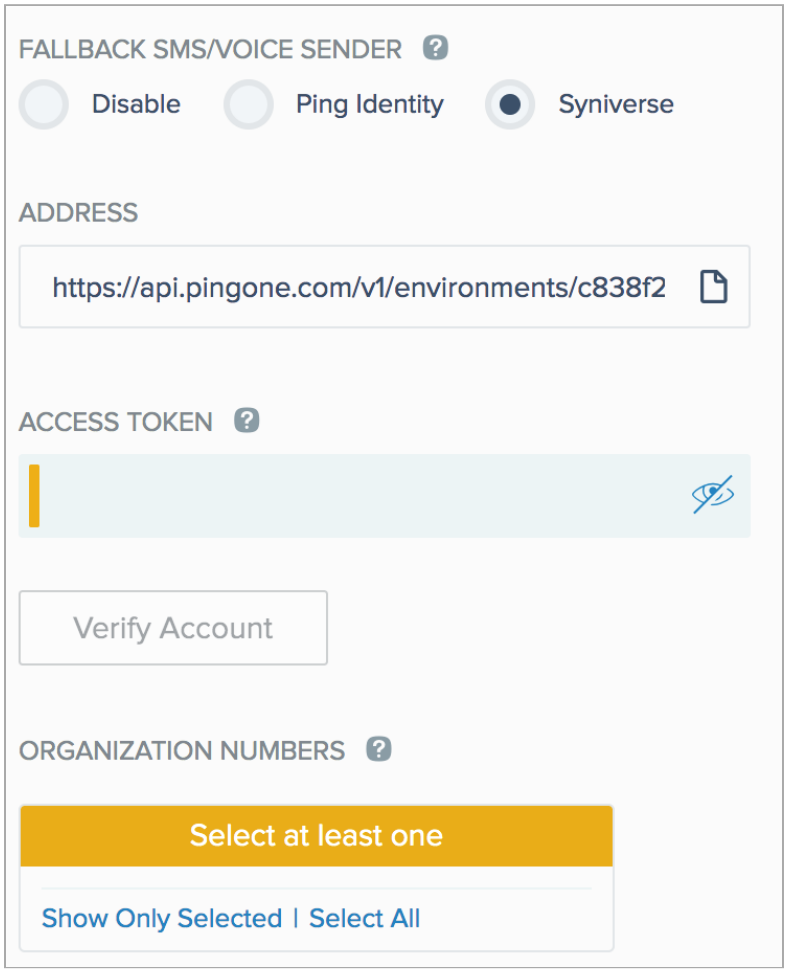
> **Note**
>
> **Under fallback:**
> If PingID SDK receives an error during the message despatch process that the used number is invalid, it will retry using the fallback option.
>
> - If there was no way originating the SMS or voice event with tenant's own account, and admin defined a fallback to Syniverse or Ping Identity's account, the event will be originated from the fallback account.
> - The following errors will cause fallback:
>   - All API errors (but not SMS delivery errors)
>   - No origination number was found on the Twilio account
> - If a transaction was charged to a specific account (Ping or custom), it does not imply that subsequent transactions will be charged to the same account. The account charged for each transaction is determined on an individual basis. Preference is always given to the custom account.
> - If you configured **FALLBACK SMS/VOICE SENDER** as **Ping Identity**, you will be billed at Ping Identity's rates and not at any preferential rates you have directly from Twilio. In addition, Ping Identity originating numbers and setup parameters will be in force.

- **Ping Identity**:

  Use Ping Identity's SMS/voice sender account in cases of fallback.

- **Syniverse**:

  Enter the Syniverse **Access Token** and select at least one **Origination Number**:



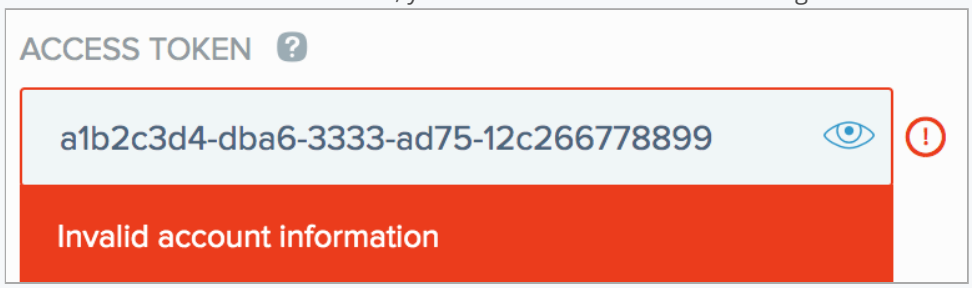
1. Copy/paste your Syniverse **Access Token** to the indicated field.

> **Note**
>
> The system uses your access token to connect to your Syniverse account. Recommended: In your account in the Syniverse portal, define an application that is dedicated to PingID SDK traffic. Use this application for analyzing PingID SDK traffic throughput, and troubleshooting SMS or voice message despatch cases.

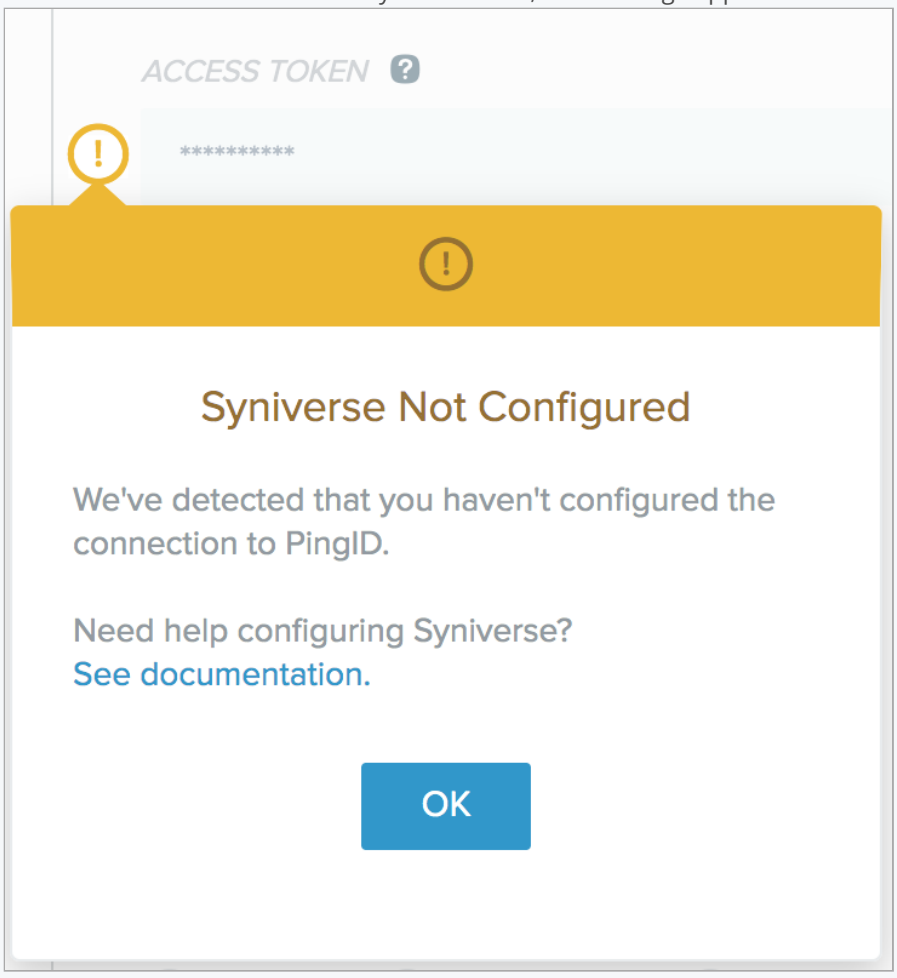
2. Click the **Verify Account** button. That validates the account to PingID SDK and populates the **Origination Numbers** list from your Syniverse account.

Note

- If the **Access Token** is incorrect, you will be shown this error message:



- If your Syniverse account is not fully configured a yellow exclamation mark appears next to the **Access Token** field. If you click on it, this message appears:



- If there are no originating phone numbers in the Syniverse account, it will not be validated to PingID SDK.
- To configure your Syniverse account to work with PingID SDK:
  1. Copy the URL from the **Address** field.
  2. In your Syniverse account:
     - In the **Delivery Configuration**, paste the URL that you copied from the PingID SDK **Address** field.
     - Create two subscriptions: **SCG-Message** and **SCG-Voice-Calls**.

See How to setup a Webhook for Receiving Messages and Notifications in the Syniverse Developer Community for more information.

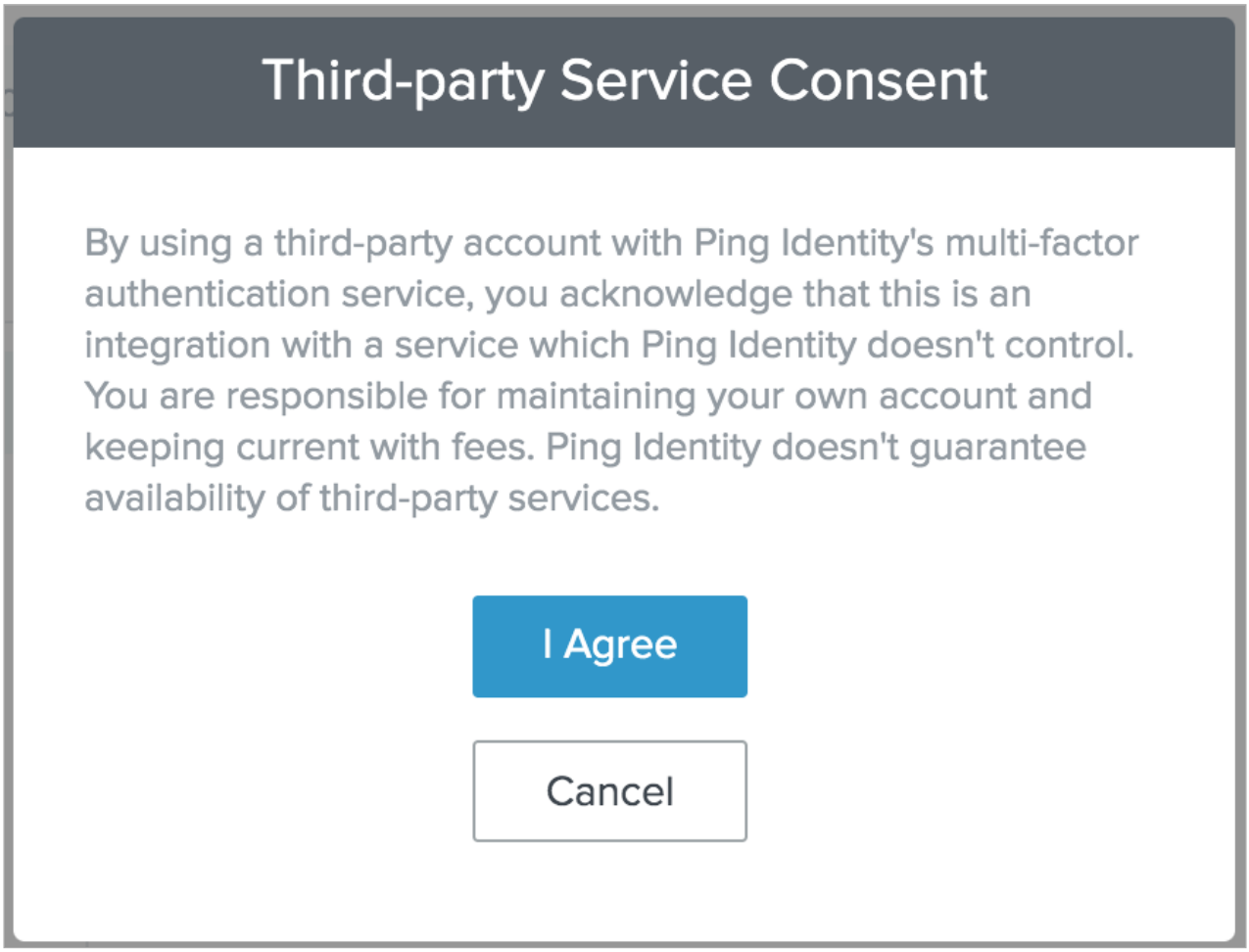
> These Syniverse configurations are required in order that Ping Identity's dashboards and reports will reflect complete and accurate data. Ping Identity will not be able to troubleshoot SMS or voice events related to Syniverse if these configurations are incomplete.

If the account was successfully verified, the display will change to show a list of originating numbers from Syniverse:

+ image::itu1597828167369.png[alt="A screen capture of the list of Organization Numbers.",role="border-no-padding"]

1. Select at least one originating telephone number to use.

10. To save your settings, click **Save** at the bottom of the **Setup** window.
11. To complete the setup process, enter your legal consent:



> **Note**
>
> You will only be asked for legal consent when entering a new SID.

Managing a Twilio account for PingID SDK

Manage a custom Twilio account.

About this task

Managing an account includes:

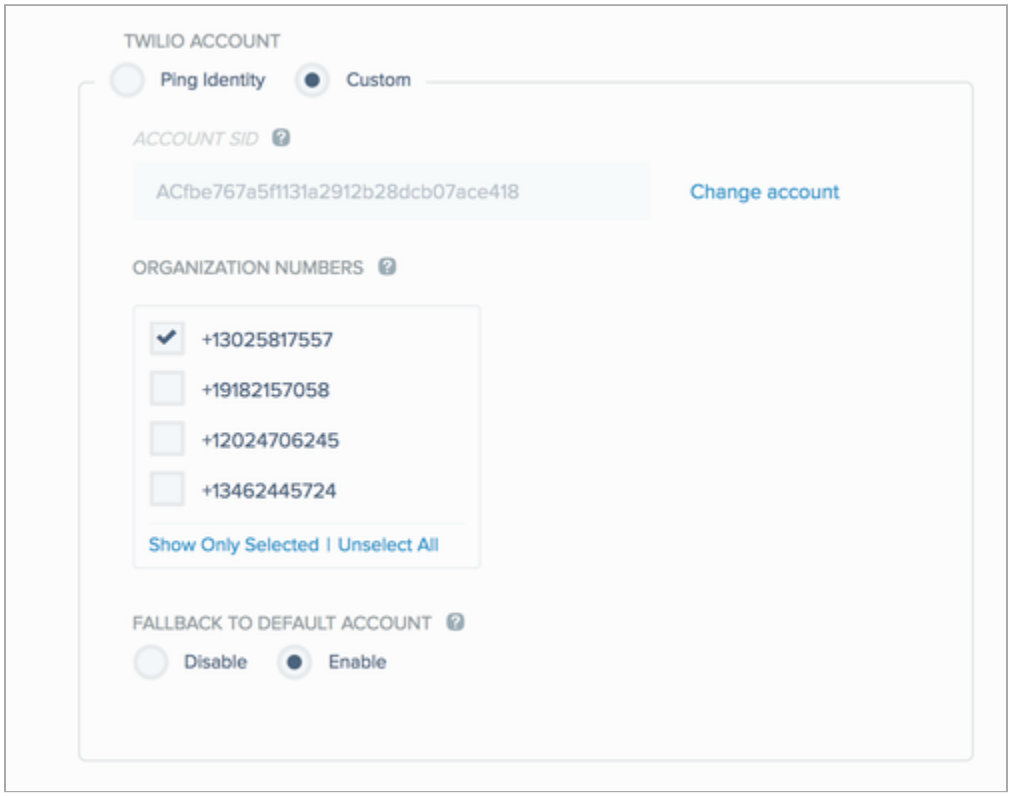
- Changing active originating numbers and fallback setting, as in Configuring a Twilio account for PingID SDK
- Changing to another account
- Deleting the custom account

Steps

1. In the PingID admin portal, go to **Setup → PingID SDK**.

   Result:

   The **Twilio Account** configuration displays.



2. Select at least one originating telephone number to use.
3. To change the fallback settings, in the **Fallback To Default Account** section, click the desired setting.
4. To switch to a different account, click **Change Account**.

   Result:

   The configuration window for a new account appears.

5. To delete the active custom account, click **Ping Identity**.
6. Click **Save**.

Using a custom Syniverse account with PingID SDK

Using a custom Syniverse account with PingID SDK

If you have an existing custom Syniverse account, you can configure PingID SDK to use it for SMS or voice pairing and authentication.

Keep the following points in mind:

- **Daily used SMS/Voice limits:**
  - **PingOne full licence accounts:** The daily SMS and Voice limits are enforced for fully licensed PingOne accounts that use a custom Syniverse account.
  - **PingOne trial accounts:** The daily SMS and Voice limits are not enforced for PingOne trial accounts that use a custom Syniverse account.
- **Billing:** Your Syniverse billing arrangements must be setup before you can configure PingID SDK to use your account.
- **Multiple Syniverse accounts:** If you have more than one Syniverse account, you can only use one of them.
- **Inactive Syniverse accounts:**It is the administrator's responsibility to delete a Syniverse account configuration in PingID SDK, if the account becomes inactive. See Managing a Syniverse account for PingID SDK for deleting a custom Syniverse account from PingID SDK.

To configure a custom Syniverse account go to Configuring a Syniverse account for PingID SDK.

To manage a custom Syniverse account go to Managing a Syniverse account for PingID SDK.

Configuring a Syniverse account for PingID SDK

About this task

> **Note**
>
> By default, PingID SDK uses Twilio for voice and SMS. By enabling your own Syniverse account, you are taking responsibility for despatching SMS and voice messages.

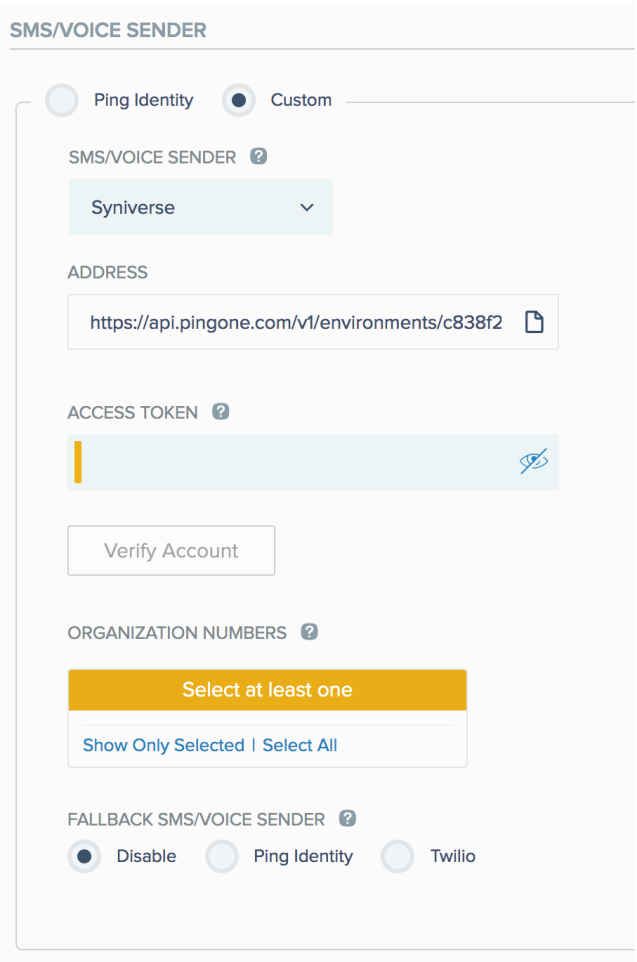
Ensure that you have available your Syniverse account Access Token. You can copy it as required from the Syniverse dashboard. You should also have set up one or more origination phone numbers. The following procedure will guide you in configuring PingID SDK to use your Syniverse account.

To configure PingID SDK for a Syniverse account:

Steps

1. Log in to the admin console.
2. Go to **Setup → PingID SDK**.
3. Under **SMS/Voice Sender**, choose **Custom**.

   The custom configuration settings appear.



4. In the **SMS/Voice Sender** dropdown, select **Syniverse**.

> **Note**
>
> A custom Syniverse account applies across all PingID SDK applications of the organization.

5. To configure your Syniverse account to work with PingID SDK:

    1. Copy the URL from the **Address** field.
    2. In your Syniverse account:
        1. In the **Delivery Configuration**, paste the URL that you copied from the PingID SDK **Address** field.
        2. Create 2 subscriptions: **SCG-Message** and **SCG-Voice-Calls**.

        See the Syniverse article How to setup a Webhook for Receiving Messages and Notifications for more information.

        > **Note**
        >
        > These Syniverse configurations are required in order that Ping Identity's dashboards and reports will reflect complete and accurate data. Ping Identity will not be able to troubleshoot SMS or voice events related to Syniverse if these configurations are incomplete.

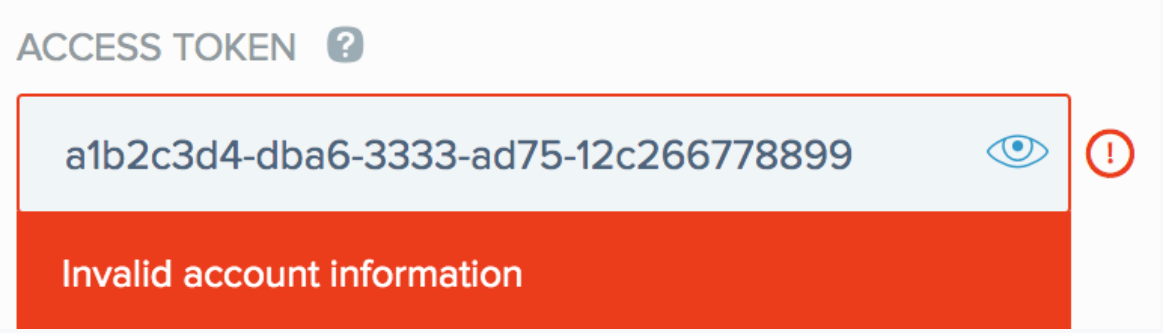
6. Copy/paste your Syniverse Access Token to the indicated field.

> **Note**
>
> The system uses your access token to connect to your Syniverse account.
> Recommended: In your account in the Syniverse portal, define an application that is dedicated to PingID SDK traffic. Use this application for analyzing PingID SDK traffic throughput, and troubleshooting SMS or Voice message despatch cases.

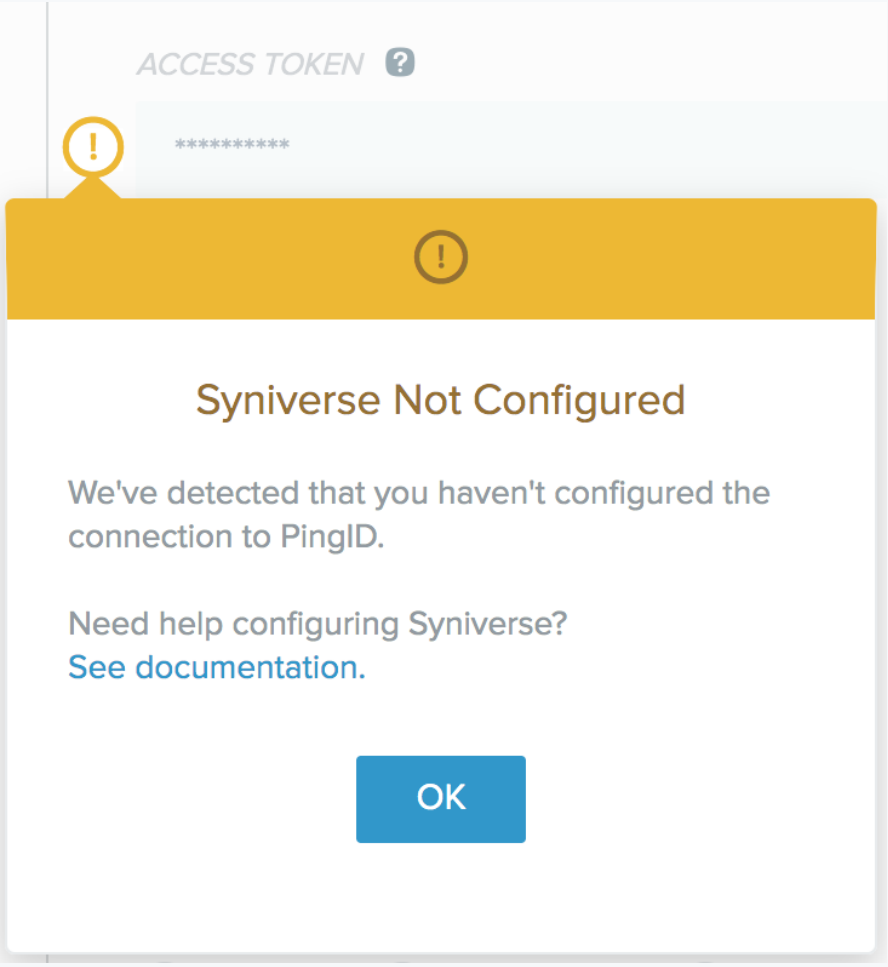
7. Click the **Verify Account** button. That validates the account to PingID SDK and populates the Origination Numbers list from your Syniverse account.

Note

- If the Access Token is incorrect, you will be shown this error message:

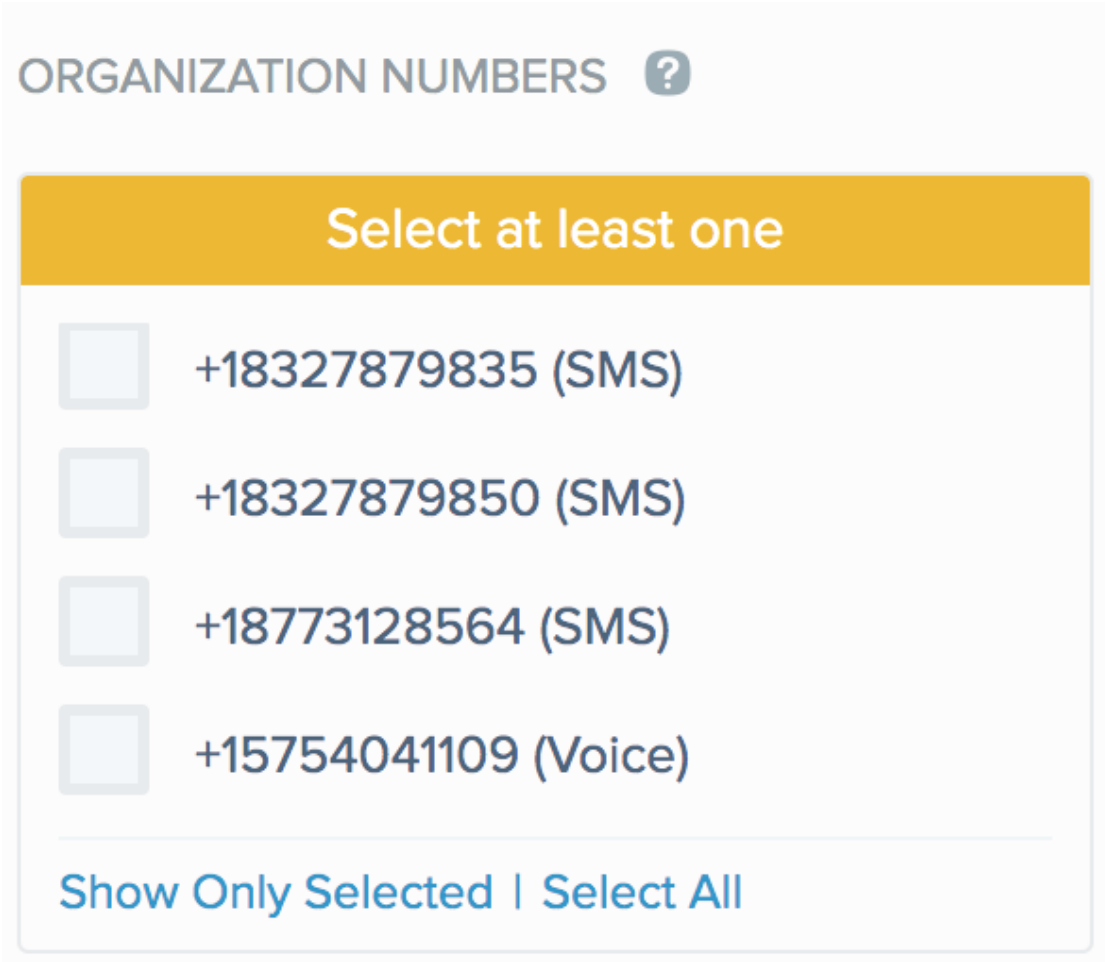


- If your Syniverse account is not fully configured a yellow exclamation mark appears next to the Access Token field. If you click on it, this message appears:



- If there are no originating phone numbers in the Syniverse account, it will not be validated to PingID SDK.

If the account was successfully verified, the display will change to show a list of originating numbers from Syniverse:



8. Select at least one originating telephone number to use.

> **Note**
>
> - Syniverse allows you to define phone numbers for use with either voice or SMS.
> - Syniverse allows the use of sender IDs (in place of telephone numbers) for commercial use or to comply with regulations requiring SMSs to be sent as **transactional** and not **promotional**. When using the Ping Identity account, all originating numbers are defined as transactional with a senderID in Syniverse. To achieve the same functionality in a custom Syniverse account, you must configure it directly in Syniverse.
> - Sender IDs are displayed according to the Sender IDs sent in the API requests.
> - Short codes are supported only for the United States, and only for SMS messages. If only short codes are chosen, but the number is not a US number:
>   - If the admin configures **FALLBACK SMS/VOICE SENDER** as **Ping Identity** or **Twilio**, the selected fallback account's phone numbers are used.
>   - If the admin **Disables** the **FALLBACK SMS/VOICE SENDER** option, the SMS will not be sent.

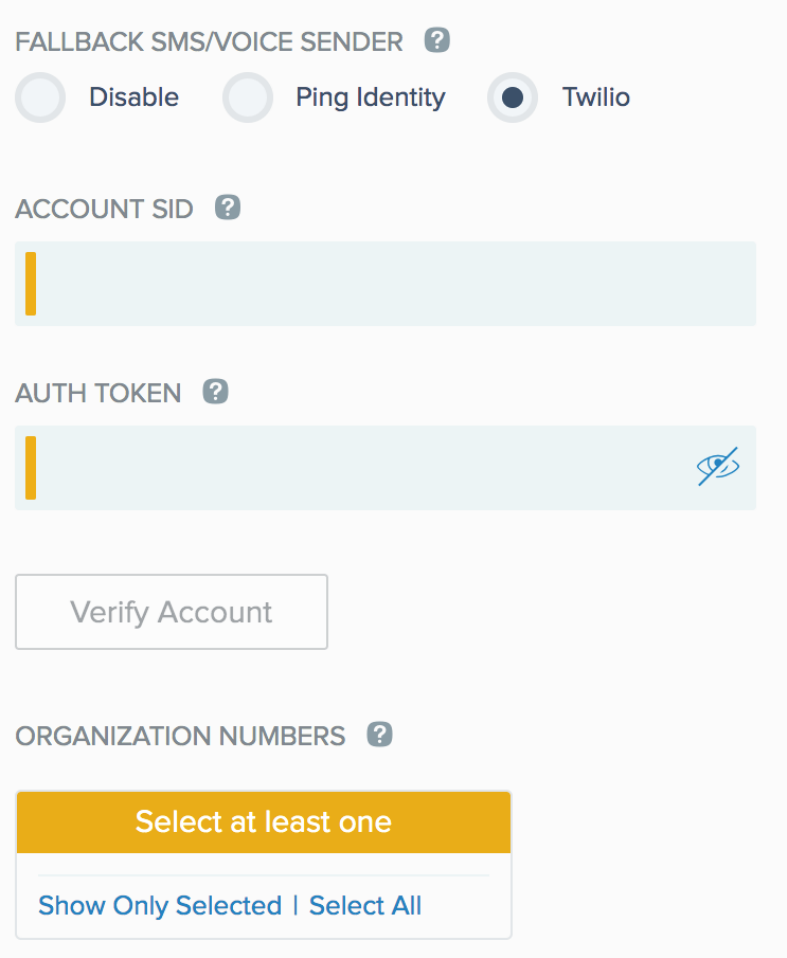
9. Enable **FALLBACK SMS/VOICE SENDER** as **Ping Identity** or **Twilio** to fall back to one of these alternatives if Syniverse becomes unavailable for reasons explained in the following Note.

> **Note**
>
> **Under fallback:**
> If PingID SDK receives an error during the message despatch process that the used number is invalid, it will retry using another configured Syniverse number. After attempting to despatch the message and receiving an error for all configured numbers, the fallback flow is triggered.
>
> - If there was no way originating the SMS or voice event with the tenant's own Syniverse account and admin defined a fallback, the event will be originated from the configured fallback account
> - The following errors will cause fallback:
>   - All API errors (but not SMS delivery errors)
>   - No origination number was found on the Syniverse account
> - If a transaction was charged to a specific account (Ping or custom), it does not imply that subsequent transactions will be charged to the same account. The account charged for each transaction is determined on an individual basis. Preference is always given to the custom account.
> - If you configured **FALLBACK SMS/VOICE SENDER** as **Ping Identity**, you will be billed at Ping Identity's rates and not at any preferential rates you have directly from Syniverse. In addition, Ping Identity originating numbers and setup parameters will be in force.

- **Ping Identity**:

  Use Ping Identity's SMS/Voice sender account in cases of fallback.

- **Twilio**:

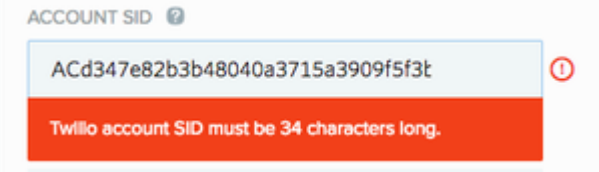


Enter the Twilio Account SID, Auth Token and select at least one Origination Number:

1. Copy/paste the Twilio account SID to the indicated field.

   Note

   If the SID is shorter than 34 characters, you will be shown this error message:

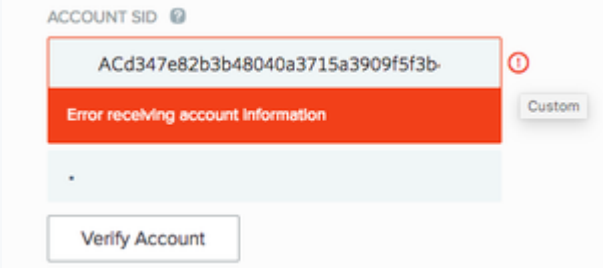
   

2. Copy/paste the Twilio Auth Token to the indicated field.

3. Click the **Verify Account** button. That validates the account to PingID SDK and populates the Origination Numbers list from your Twilio account.

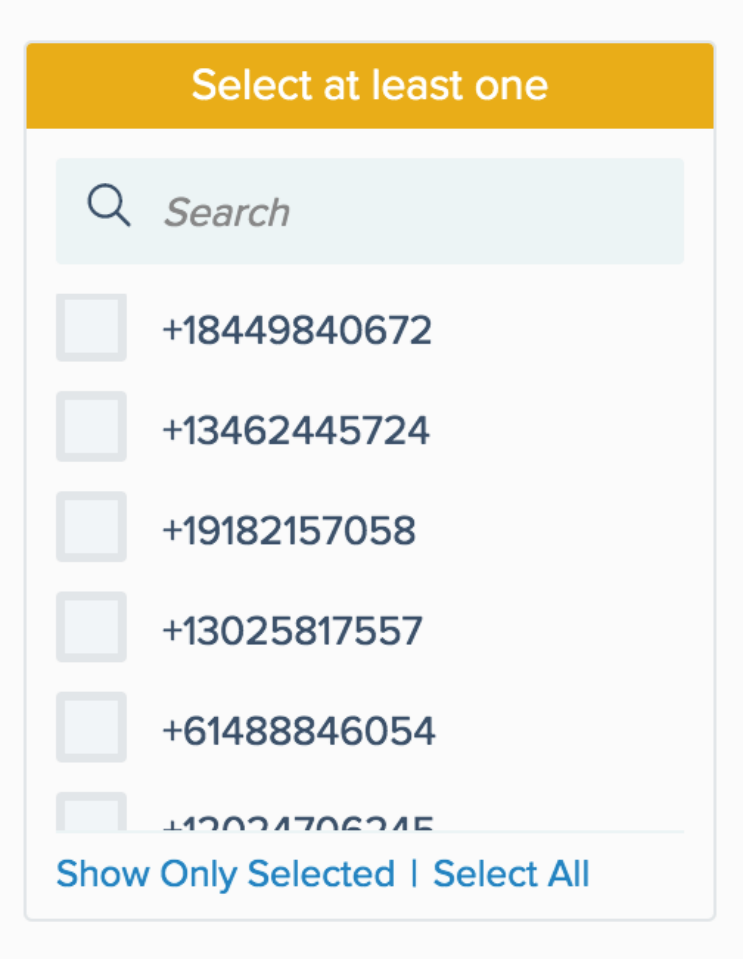
   Note

   - If the AUTH TOKEN is incorrect, you will be shown this error message:

   - If there are no originating phone numbers in the Twilio account, it will not be validated to PingID SDK.

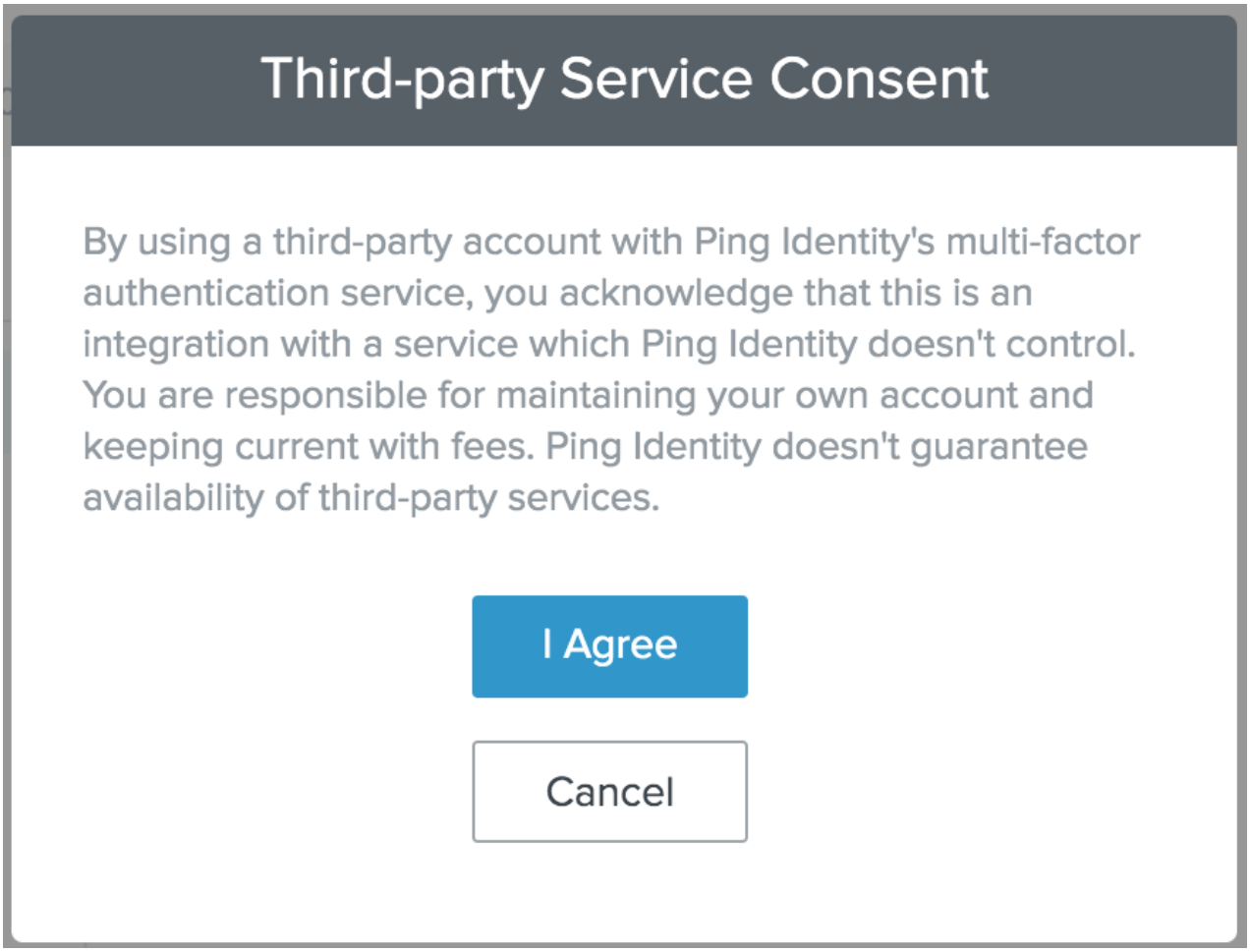
   If the account was successfully verified, the display will change to show a list of originating numbers from Twilio:



4. Select at least one originating telephone number to use.

10. To save your settings, click **Save** at the bottom of the **Setup** window.

11. To complete the setup process, enter your legal consent:



Note

You will only be asked for legal consent when entering a new Access Token.

Managing a Syniverse account for PingID SDK

About this task

Managing an account includes:

- Changing active originating numbers and fallback setting (as in Configuring a Syniverse account for PingID SDK)
- Changing to another account
- Deleting the custom account

To manage a custom Syniverse account:

Steps

1. Log in to the admin console.
2. Go to **Setup → PingID SDK**.

The **SYNIVERSE ACCOUNT** configuration is displayed.

1. Select at least one originating telephone number to use.
2. You may change the Fallback settings.
3. To switch to a different account, click **Change Account**. You will be offered the configuration window for a new account. Proceed as in Configuring a Syniverse account for PingID SDK.
4. To delete the active custom account, click the **Ping Identity** radio button.
5. To save your settings, click **Save** at the bottom of the **Setup** window.

Running the PingID SDK Admin Activity Report

Run the PingID SDK Admin Activity Report from the admin portal.

About this task

The PingID SDK admin activity report outputs detailed information regarding admin-related activity during the past week.

Steps

1. From the admin portal, go to **Dashboard → Reporting → Reports**.

   Result:

   A list of pre-defined reports display.

2. Next to **PingID SDK Admin Activity of the last 7 Days**, click **Run**.

   Result:

   The report output is presented. For a detailed description of the report output fields, see PingID Admin Activity Report fields for PingID SDK.

   > **Note**
   >
   > - You can customize the report output by adding optional field columns, removing default fields, and changing default runtime parameters, according to the steps in the generic PingOne Run a custom report procedure.
   > - You can stream PingID event information to Splunk or other third-party products. You can view and analyze this information when you subscribe to PingID audit events through the PingOne subscription facility. For more information, see Subscriptions in the PingOne Admin Guide.

3. To download the report in `.csv` format, click **Export**.

   Result:

   The report is saved in your browser's default downloads folder. The export process can take several minutes to complete, depending on the size of the report.

PingID Admin Activity Report fields for PingID SDK

The PingID Admin Activity Report produces output with the following default and optional fields.

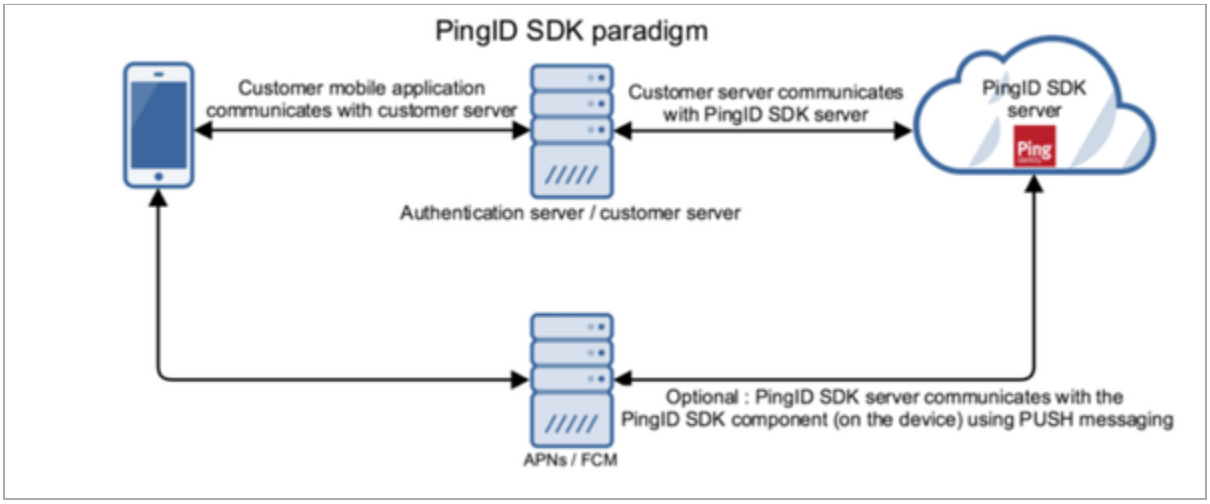
Customize the report output by adding optional field columns, removing default fields, and changing default runtime parameters. For more information, see https://docs.pingidentity.com/access/sources/dita/topic?resourceid=p14e_run_custom_report**Run a custom report**].

Field name	Description	Default/Optional
Timestamp	The date and time when the admin action event occurred, according to the current time zone.	Default
Admin	The email address, username, or LDAP name assigned to the administrator who performed the action.	Default
Admin Type	The type of administrator. This will be "user" unless the action was performed by a Ping Identity employee.	Default
Action	The type of resource and the action of the event. Possible values: • `account updated` • `report updated` • `user updated`	Default
Resource Name	The name of the resource on which the action was performed.	Default
Resource Type	The type of resource on which the action was performed. Possible values: • `account` • `report` • `user`	Default
Message	Detailed information regarding the action event, including the resource type, resource name, and nature of the admin action.	Default
Admin Id	The unique identifier assigned by PingOne to the administrator.	Optional
Browser Agent	The browser name and version used for PingOne SSO.	Optional
IP Address	The IP address of the host used to initiate the event.	Optional
Resource Id	The unique identifier assigned by PingOne to the resource.	Optional
Status	The status of the action. Possible values: • `SUCCESS` • `FAILURE`	Optional

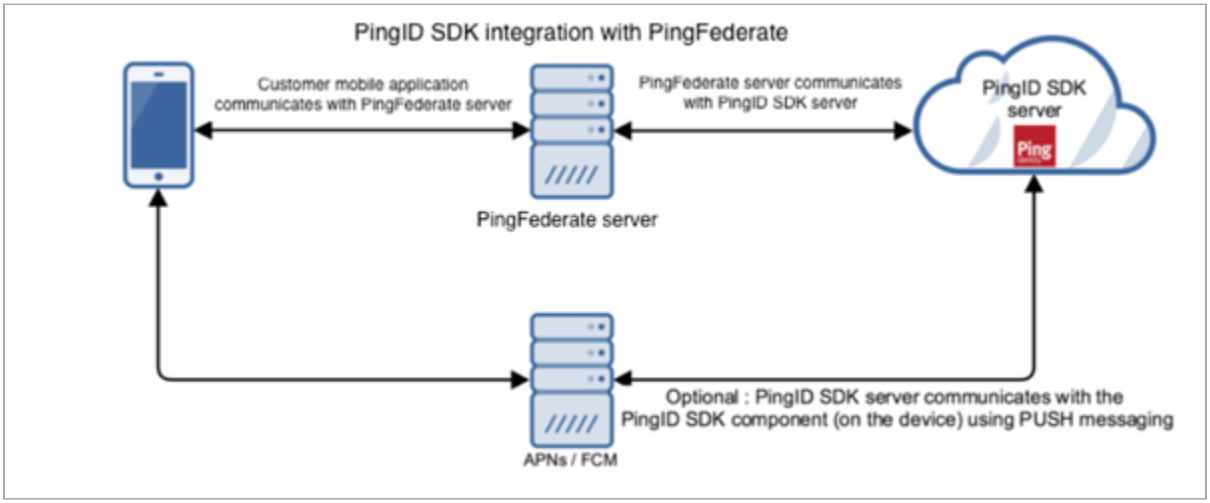
The PingID SDK adapter for PingFederate

The PingID SDK adapter for PingFederate is an out-of-the-box integration between PingID SDK and PingFederate user authentication flow and adapter chain that permits the option to replace the customer server with PingFederate.

PingID SDK is a mobile SDK for support of PingID multi-factor authentication (MFA) for customer use cases on organizations' own mobile applications. The basic implementation of PingID SDK requires the organization to set up a customer server.



The PingID SDK adapter for PingFederate permits the option to replace the customer server with PingFederate in several use cases.



The PingID SDK adapter for PingFederate supports all of the PingID SDK authentication methods, including mobile SDK, SMS, voice, and email.

- PingID SDK adapter for PingFederate contains the `pingid.sdk.status` attribute. When an authentication flow using the PingID SDK adapter for PingFederate is successful, `pingid.sdk.status` provides additional information that can be used for determining user permission levels.
- PingID SDK adapter includes customizable pages that are presented to the user as part of the authentication flow.

Supported flows

There are several use cases in which the PingID SDK adapter for PingFederate can replace a customer server, for the purpose of pairing and authenticating a user.

Automatic device registration (web view)

Automatic mobile device registration when a user initiates a pairing process for a mobile device.

Device authorization (web view)

Seamless user sign-on to an already trusted mobile application which includes PingID mobile SDK

QR code authentication

User scanning a QR code with a trusted mobile device. The major objective of this approach is to permit secure passwordless authentication. The customer server does not need advance knowledge of who the user is (for example, first factor authentication is not required).

Out of band / step up authentication from web

MFA during user sign-on to a web application

Out of band / step up authentication from mobile

MFA during user sign-on to a non trusted mobile device, using the user's primary device for the approval process.

Transaction approval

Elevated security for a high value or high risk resource or service, within the particular context of an application, which requires authentication using a higher assurance credential than previously required for general access of the application.

CIBA authenticator

Out-of-band MFA using a trusted mobile device as a Client-Initiated Backchannel Authentication (CIBA) authenticator.

PingFederate Authentication API

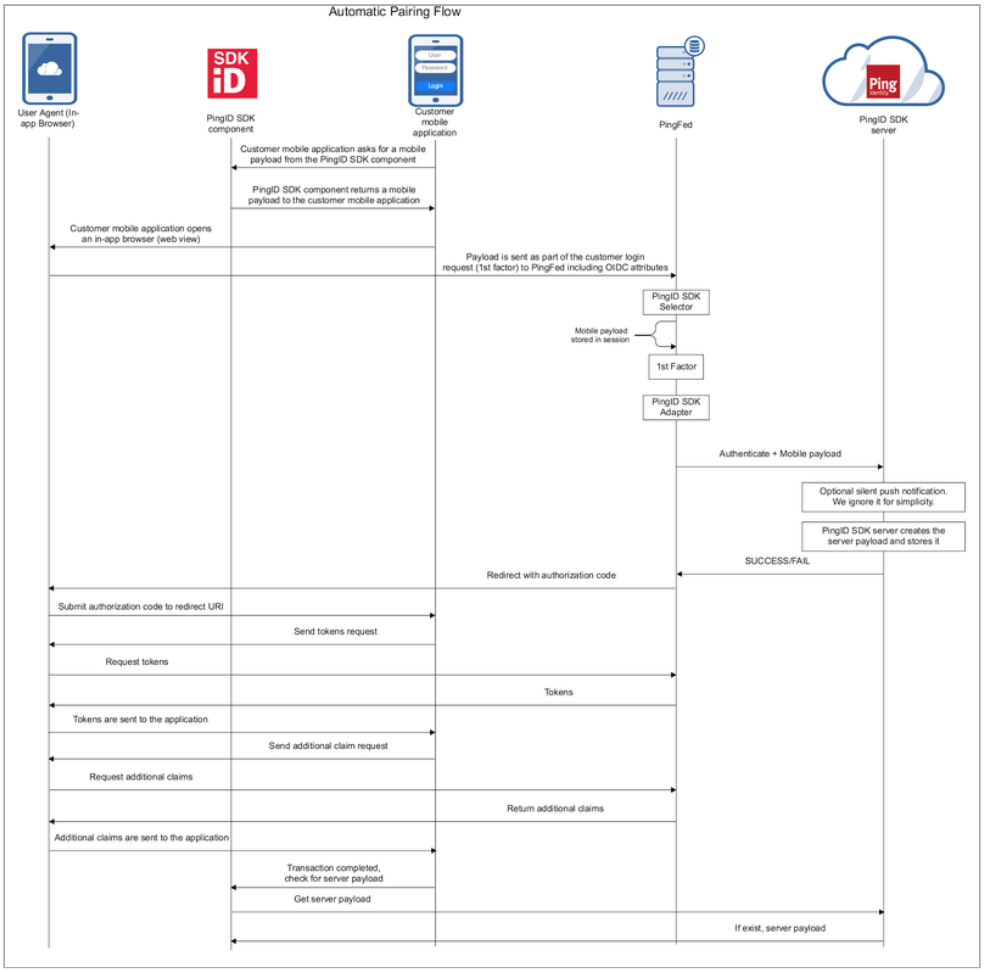
Enables integration with the PingFederate Authentication API for end-user interactions, for step-up authentication and transaction approval. Additionally, it supports mobile device initiated flows such as mobile device registration and seamless device authorization.

For more information, see Supported PingID SDK adapter for PingFederate flows.

Supported PingID SDK adapter for PingFederate flows

The PingID SDK adapter for PingFederate permits the option to replace the customer server with PingFederate for pairing and authenticating a user.

Administrators and developers should consider the supported flows when implementing the PingID SDK adapter for PingFederate.



Supported use cases and flows

The PingID SDK adapter for PingFederate supports the following use cases:

Automatic device registration (web view)

Automatic mobile device registration when a user initiates a pairing process for a mobile device.

- This flow only supports the mobile web view. The user is authenticated as part of the PingFederate authentication flow, and after the user is successfully authenticated, control is returned to the mobile application and trust with the PingID SDK server is initiated. The adapter returns control to the mobile application.
- This flow supports registration of mobile devices.

Device authorization (web view)

A seamless user sign-on to an already trusted mobile application, which includes PingID mobile SDK.

- This flow only supports sign-on to the mobile application using mobile web view and then returns control to the mobile application.
- This flow takes the user through the PingID SDK adapter authentication. On successful seamless device authentication, the user is signed on to the application.

QR code authentication

A user scanning a QR code with a trusted mobile device. The major objective of this approach is to permit secure passwordless authentication. The customer server does not need advance knowledge of who the user is. For example, first-factor authentication is not required.

- The PingFederate PingID SDK adapter displays a QR code image in the web browser.
- The user scans the QR code with their trusted mobile device, and the mobile application passes it back to the PingID SDK server. QR code-based authentication also supports authentication of multiple users who use the same device.
- The PingID SDK server validates the QR code.
- If the QR code is valid, the user is approved and authentication is completed.
- If extra verification is required, a silent push is sent to verify the device. In addition, a user approval message can also be sent to the user for additional user confirmation.

Out-of-band / step up authentication from web

multi-factor authentication (MFA) during user sign-on to a web application.

- Signing on through a web browser initiates PingFederate first-factor authentication. Since it is web based, no payload is sent to the PingID SDK server.
- All of the PingID SDK authentication methods are supported: mobile SDK, SMS, voice, and email.
- After successful first factor authentication, the adapter directs the PingID SDK server to send a push notification, SMS, voice message, or email to the authenticating device.
- An application development design consideration would be to permit SMS, voice, and email device registration although not using PingFederate.

Out-of -and / step up authentication from mobile

MFA during user sign-on to a non-trusted mobile device, using the user's primary device for the approval process.

- This flow supports pairing of new mobile devices only. Mobile, SMS, voice, and email devices can be used for approving the new device pairing.
- The PingID SDK server sends an authentication request to the primary device, either as a push notification for a mobile device or a one-time passcode (OTP) for SMS, voice, or email. The PingID SDK adapter returns a success or failure status.
- This flow is relevant only when **Additional Trusted Devices** is configured to **Verify New Devices with Primary Device**. In cases where **Additional Trusted Devices** is configured to **Pair Each Device Individually**, the **Automatic device registration** flow is performed every time a user tries to pair an additional device.

Transaction approval

Transaction approval, also known as step-up authentication, is elevated security for a high-value or high-risk resource or service, within the particular context of an application. This requires authentication using a higher assurance credential than previously required for general access of the application.

In some applications, do not use the second-factor authentication capabilities during the sign-on process. Instead, activate it during certain user actions, such as a payments or bank transfers. These actions are called transaction approvals because they elevate the user's security context only when required by the business logic.

PingID SDK enables the developer to incorporate transaction approval flows and authentications into native applications quickly and easily. Transaction approvals rely on context-related information as part of the authentication. The context-related information is implemented using the dynamic parameters feature of the PingID SDK adapter for PingFederate. The native application can use it to show the transaction information or to display different behavior during the authentication.

CIBA authenticator

Out-of-band MFA using a trusted mobile device as a client-initiated backchannel authentication (CIBA) authenticator.

The accessing device initiates the authentication request. The authentication request is sent to a trusted mobile device for authentication, without the need for an additional redirect to PingFederate. The request is received by PingID SDK on the mobile device, and PingID SDK returns a success or failure status.

> **Note**
>
> The PingID SDK CIBA authenticator supports mobile devices only.

PingFederate Authentication API

Enables integration with the PingFederate Authentication API for end-user interactions, for step-up authentication and transaction approval. Additionally, it supports mobile device initiated flows such as mobile device registration and seamless device authorization. The PingFederate Authentication API provides access to the current state of the flow as an end user steps through a PingFederate authentication policy.

Installing the PingID SDK Integration Kit for PingFederate

Install the PingID SDK integration kit for single sign-on (SSO) with PingFederate.

Before you begin

Your organization is using PingID SDK as an authentication solution for federated SSO with PingFederate.

PingID SDK integration kit requirements:

- Register for the PingID Enterprise service on PingOne.
- Configure the PingID service and download the PingID SDK properties file. For more information, see Distributing the PingID SDK settings file and application ID.
- PingFederate 8.2 or later.

  > **Note**
  >
  > If your installation should support integration with the PingFederate Authentication API, the following minimum software versions are required:
  >
  > - PingFederate 9.3+
  > - PingID SDK adapter 1.7+ for PingFederate

- Network access to a PingFederate installation.

- Open ports:
  - 443 (in external firewall)
  - 1812 (in internal firewall)
- Administrator permissions on PingFederate.

About this task

The PingID SDK integration kit is part of the PingID SDK package. Download the full PingID SDK package, including the PingID SDK integration kit from https://www.pingidentity.com/en/resources/downloads/pingid.html.

Steps

1. Extract the integration kit package.

   > **Note**
   >
   > The integration kit includes the following directories:
   > - `dist` : The PingID SDK adapter for SSO using PingFederate, the PingID SDK selector, the default HTML sign-on template, and language support.
   > - `legal` : Legal details, attributions, copyrights, patents, and licenses.

2. On the PingFederate host, stop the PingFederate server if it is running.
3. Remove any previous PingID SDK integration kit version files in the `<pingfederate-installation>/server/default/deploy` directory.
4. Copy the following files from the `<PingID SDK Integration Kit>/dist` directory to the `<pingfederate-installation>/server/default/deploy` directory:
   - `pf-pingid-sdk-idp-adapter-<version>.jar`
   - `pf.plugin.pingid-sdk-idp-selector-<version>.jar`
   - `pingid-sdk-web.war`
5. Copy `pingid.sdk.login.template.html` to `<pingfederate-installation>/server/default/conf/template`.
6. Copy `pingid-sdk-messages_en.properties` to `<pingfederate-installation>/server/default/conf/language-packs`.
7. If `<pingfederate-installation>/server/default/lib/pf-authn-api-<version>.jar` is older than the `pf-authn-api-<version>.jar` in the PingID SDK Integration Kit, replace it with the `pf-authn-api-<version>.jar` from the PingID SDK Integration Kit.
8. If you want to use the PingFederate Authentication API, merge the contents of the `authn-api-messages.properties` file from the PingID SDK Integration Kit into the `<pingfederate-installation>/server/default/conf/language-packs/authn-api-messages.properties` file.
9. Restart the PingFederate server.
10. If PingFederate is deployed on clustered servers, repeat these steps for all PingFederate nodes.

Configuring the PingID SDK adapter for PingFederate

About this task

This procedure describes the process of creating and configuring a PingID SDK adapter for the purpose of providing pairing and authentication solutions integrated with PingFederate.

Prerequisites:

- PingFederate 8.2+
- If your installation should support integration with the PingFederate Authentication API, the following minimum software versions are required:
  - PingFederate 9.3+
  - PingFederate PingID SDK IDP Adapter 1.7+

> **Note**
>
> The admin console UI menu labels in this document are those used in PingFederate 9.0. These may differ slightly from earlier versions of PingFederate.

The creation and configuration of an adapter comprises three mandatory steps:

- [createConfigureSelector]
- [createConfigureAdapter]
- [createConfigurePolicy]

The following optional enhancements improve the user authentication experience:

- [optConfigProxy] (requires PingFederate PingID SDK IDP Adapter 1.4+)
- [optHtmlFormQRbutton]
- [optCancelButton]

> **Note**
>
> - QR code based authentication requires PingFederate 9.2+ and PingFederate PingID SDK IDP Adapter 1.2+.
> - QR code based authentication is not supported for the PF Authentication API.

Steps

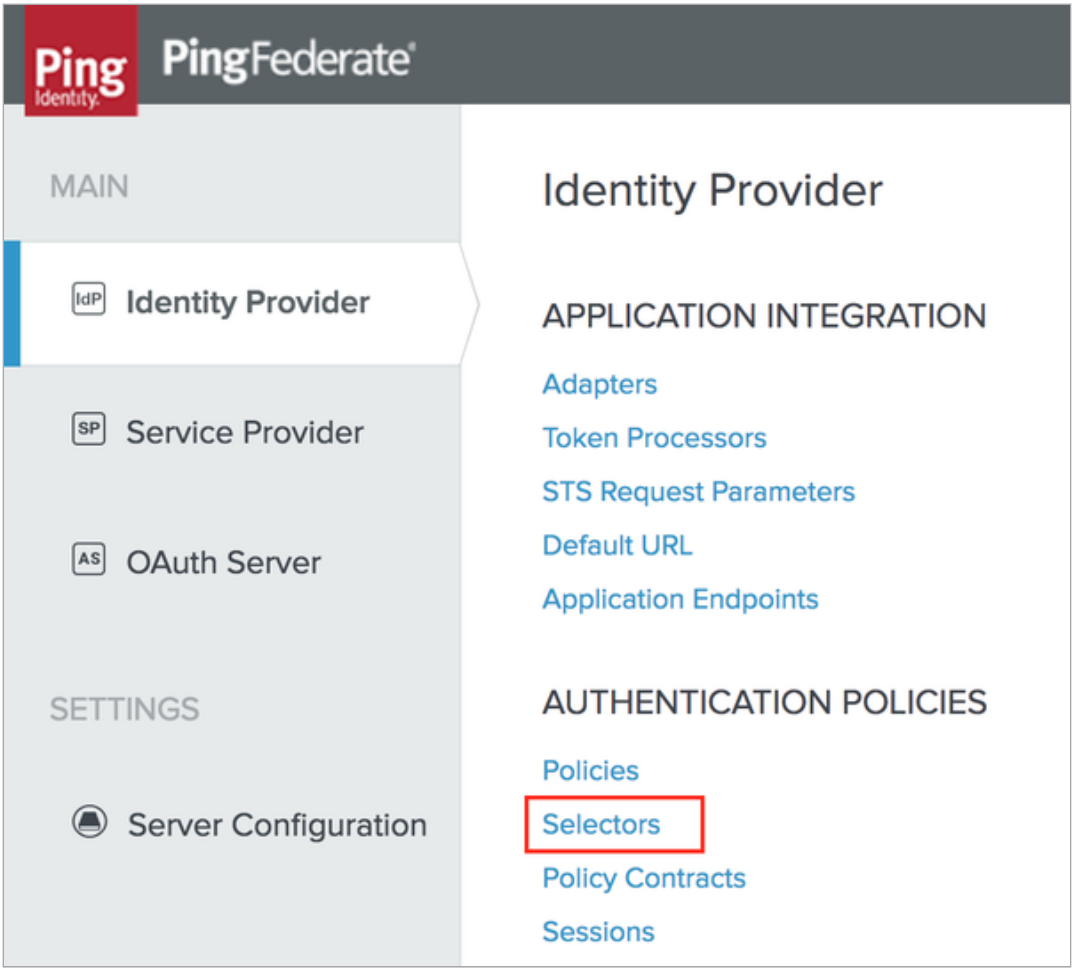
1. Create and configure a selector or tracked HTTP parameter:

   Create an instance of the PingID SDK Payload Handling Selector, which is required as a preprocessor to an authentication policy that uses the PingID SDK adapter.

Important

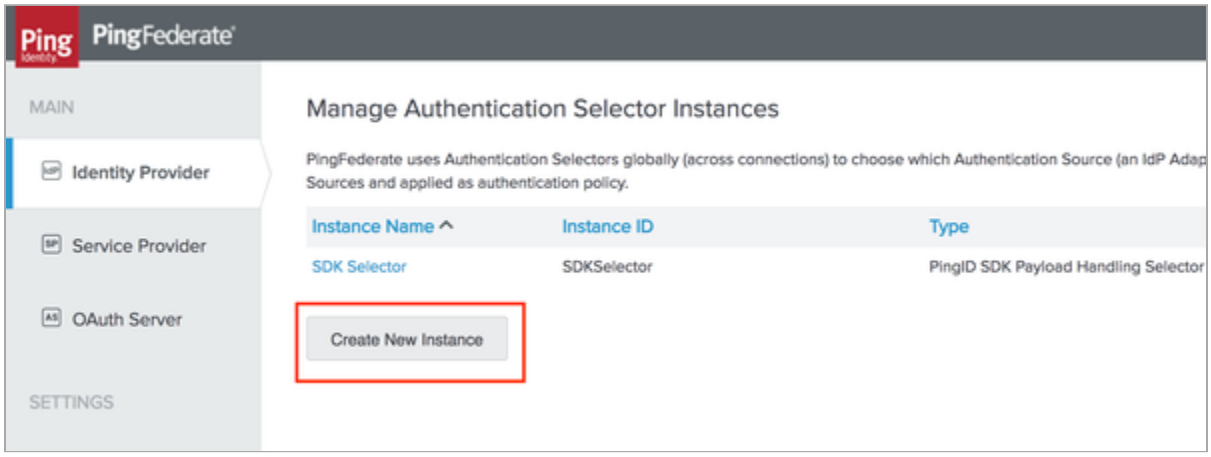
- **PingFederate 9.1.x and below**: Creation of a PingID SDK Payload Handling Selector is mandatory.
- **PingFederate 9.2+**: Creation of a PingID SDK Payload Handling Selector is not required, only if the " `payload` " parameter has been added to PingFederate's Tracked HTTP Parameters (see https://support.pingidentity.com/s/document-item?bundleId=pingfederate-92&topicId=adminGuide%2Fpf_t_defineAuthenticationPolicies.html):
  `*Identity Provider → AUTHENTICATION POLICIES → Policies → Tracked HTTP Parameters → Add*: [.codeph]``payload``

1. In the PingFederate admin console, select: **Identity Provider → AUTHENTICATION POLICIES → Selectors**.



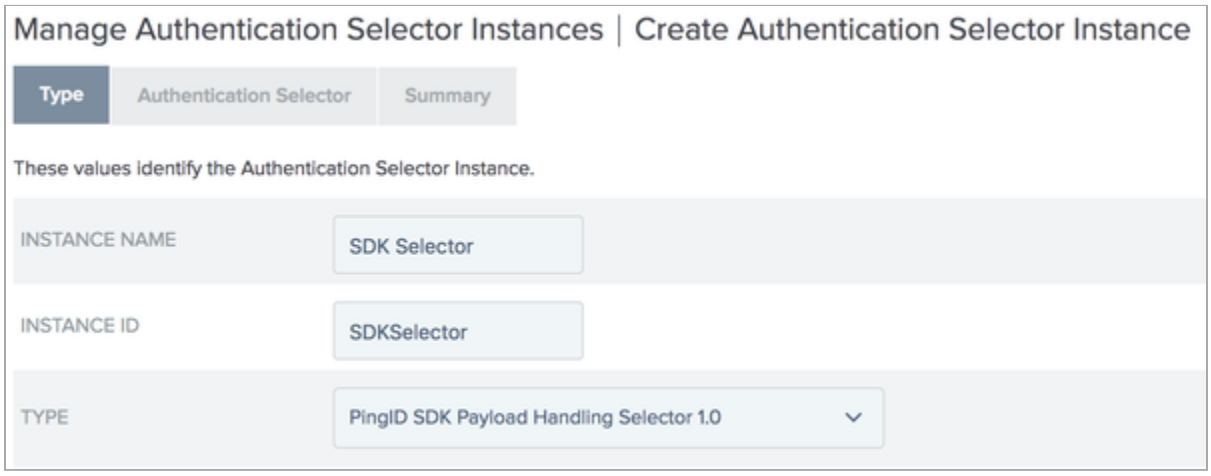
The **Manage Authentication Selector Instances** screen is displayed.

2. Click **Create New Instance** to create a new selector, or click on an existing selector to edit it.



The selector's **Type** step is displayed.

3. All fields in the **Type** step are mandatory:



INSTANCE NAME

Enter a descriptive name for this selector.

INSTANCE ID

Enter a string which will be used as an ID for this selector. Spaces are not allowed.

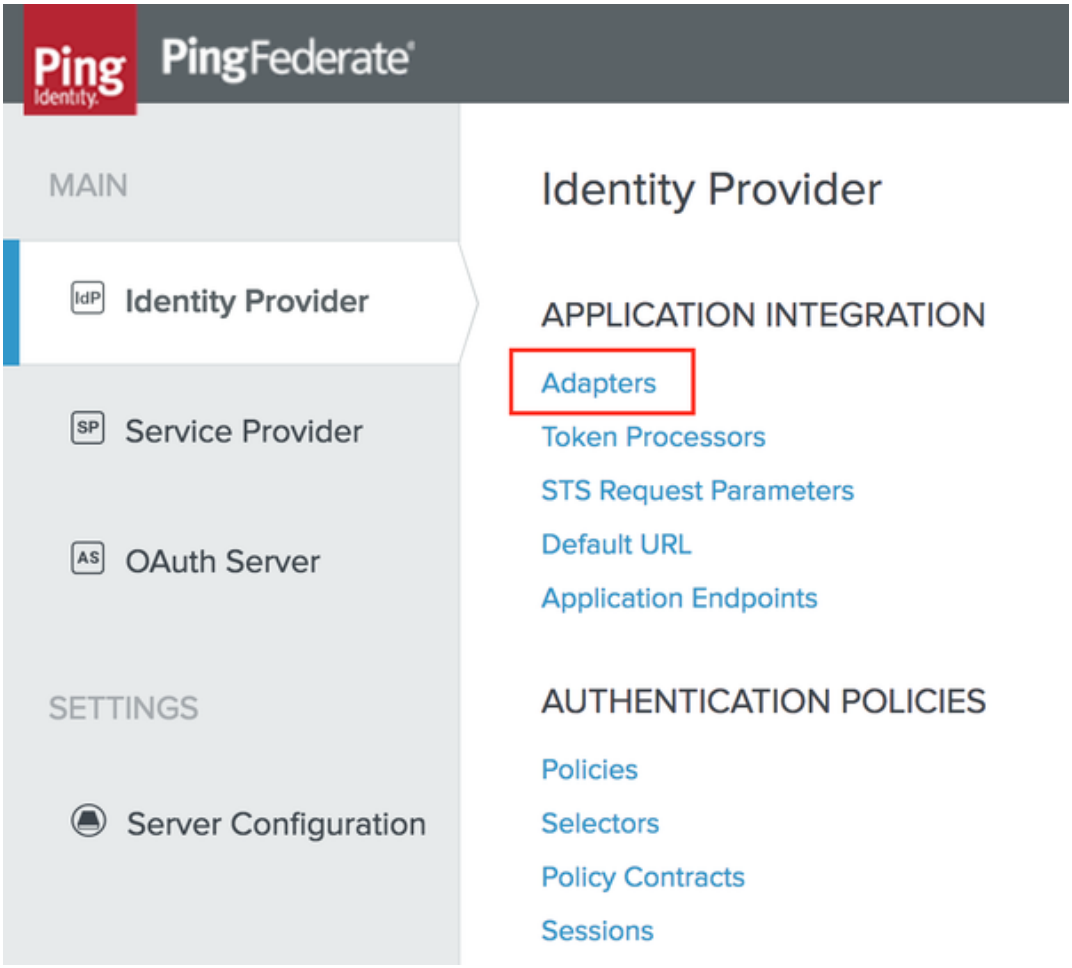
TYPE

Select PingID SDK Payload Handling Selector from the dropdown options.

4. Click **NEXT**.
5. Click **NEXT** in the **Authentication Selector** screen.
6. Click **DONE** in the **Summary** screen, to return to the **Manage Authentication Selector Instances** screen.
7. Click **SAVE** to persist changes.

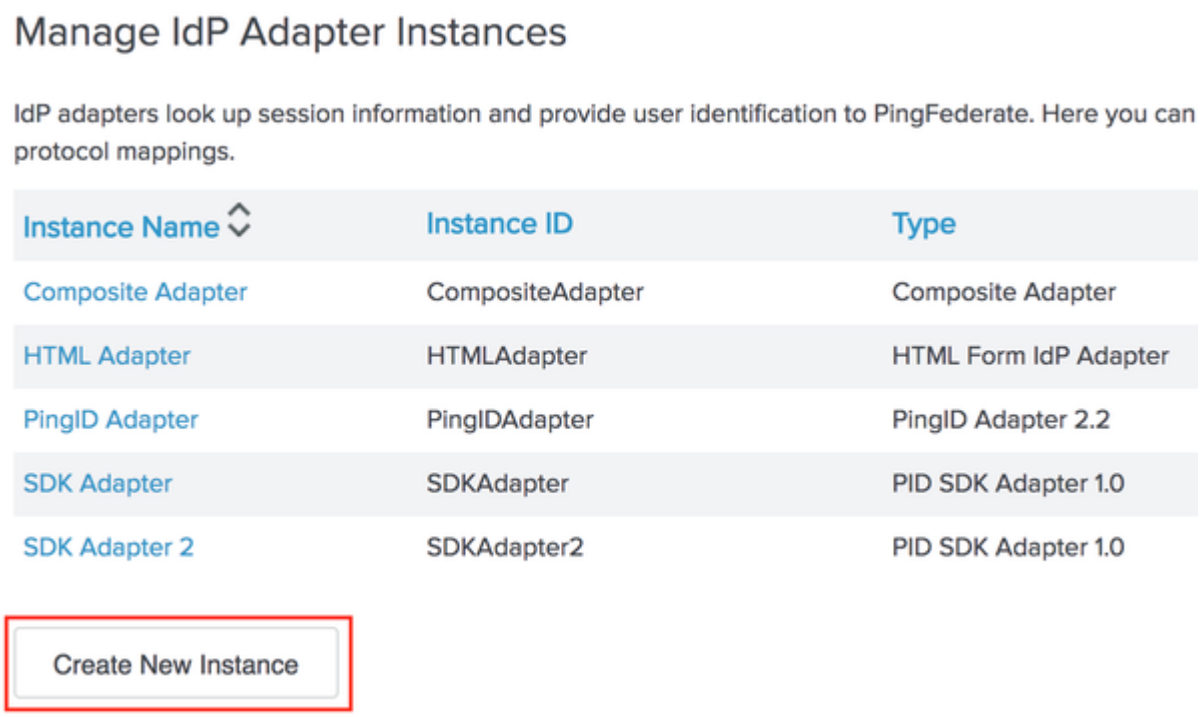
2. Create and configure an adapter:

1. In the PingFederate admin console, select: **Identity Provider → APPLICATION INTEGRATION → Adapters**.



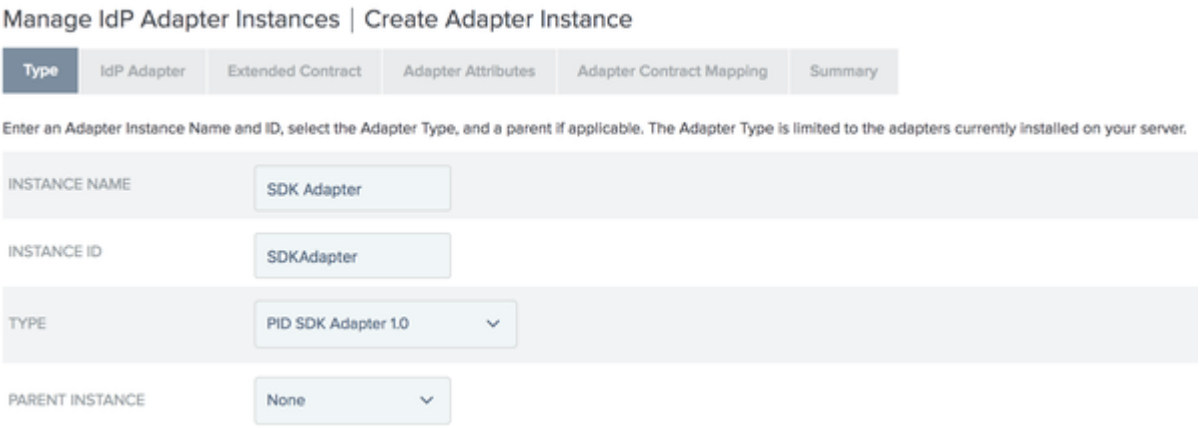
The **Manage IdP Adapter Instances** screen is displayed.

2. Click **Create New Instance** to create a new adapter, or click on an existing adapter to edit it.



The adapter's **Type** step is displayed.

3. Enter the following fields in the **Type** step:



INSTANCE NAME

Enter a descriptive name for this adapter.

INSTANCE ID

Enter a string which will be used as an ID for this adapter. Spaces are not allowed.

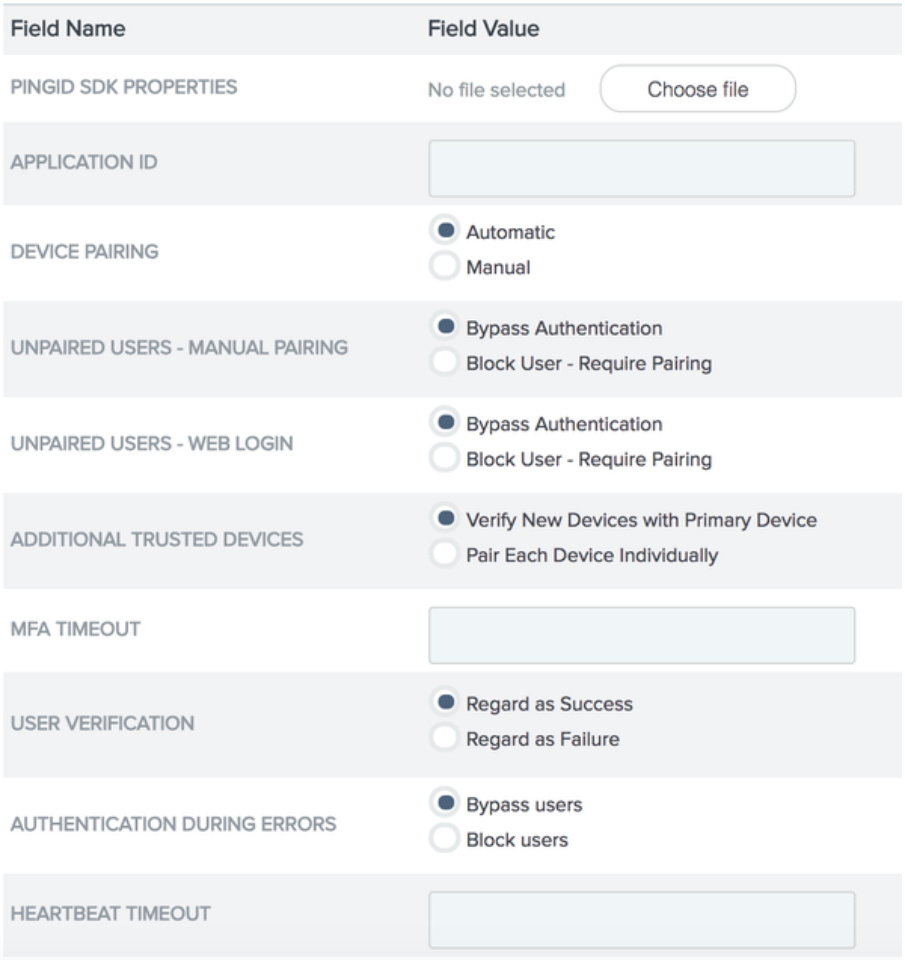
TYPE

Select **PID SDK Adapter**from the dropdown options.

PARENT INSTANCE

Leave this field with the default value: **None**.

4. Click **NEXT** to continue to the **IdP Adapter** step.



5. Configure the following fields:

PINGID SDK PROPERTIES

- Mandatory.
- Upload the PingID SDK properties file from your PingOne admin console:
  - In the PingOne admin console, go to **Setup → PingID → CLIENT INTEGRATION → INTEGRATE WITH PINGID SDK → SETTINGS FILE**.
  - Click **Download**. You may want to provide the file with a more meaningful name.
  - If you use a proxy, note that the deprecated configuration of the `pingidsdk_proxy_url` entry in the PingID SDK properties file is still supported. Configuration of an entry in the PingFederate `run.properties` file (see [optConfigProxy]), is the preferred configuration.

> **Note**
>
> If entries are defined in both the PingFederate `run.properties` and the PingID SDK properties files, the definition in the PingID SDK properties file will take precedence.

> **Important**
>
> The PingID SDK settings file should not be confused with the PingID properties file.

APPLICATION ID

- Mandatory.
- Enter the application ID that was generated by PingID SDK in your application configuration:
  - In the PingOne admin console, go to **Applications → PingID SDK Applications**, and copy the **Application ID**.

> **Note**
>
> - From PingFederate 8.4 and PingFederate PingID SDK IDP Adapter 1.2, multiple applications can be linked to a single PingID SDK adapter for PingFederate. This is achieved with dynamic parameters overriding the value of **Application ID**. Refer to Dynamic parameters support in the PingID SDK developers guide for further details.
> - In earlier versions of PingFederate and the PingID SDK Adapter, each application requires its own separate PingID SDK adapter for PingFederate.

DEVICE PAIRING

- Choose how users will pair their first device when it's a mobile device:
  - **Automatic** (default).

Once authorization of the adapter completes successfully, the automatic pairing process begins.

- **Manual**.

  Once authorization of the adapter completes, the pairing process is not initiated. The pairing process is initiated separately. Depending on the **UNPAIRED USERS - MANUAL PAIRING**Bypass field configuration, the user will be allowed into the application or denied access.

  Refer to User device pairing in the PingID SDK developer's documentation.

UNPAIRED USERS - MANUAL PAIRING

- Relevant only when **Manual** pairing is selected:
- Choose whether to allow users without a paired device to **Bypass Authentication** (default), or **Block User - Require Pairing** a device before continuing.

UNPAIRED USERS - WEB LOGIN

Choose whether to allow users without a paired device to **Bypass Authentication** (default), or **Block User - Require Pairing** a device before continuing, when signing in from a web platform.

ADDITIONAL TRUSTED DEVICES

When a user who already has a paired device, is pairing an additional device, choose whether to allow the user to approve pairing of the new device using a device in their existing trusted devices network and **Verify New Devices with Primary Device** (default), or to **Pair Each Device Individually**, without primary device verification.

MFA TIMEOUT

The duration of the PingID SDK MFA session with the adapter in minutes, before it times out and users need to authenticate again. (Default: 10 minutes, maximum 30 minutes.)

USER VERIFICATION

When the application setting **VERIFY DEVICES USING APPLE/ANDROID PUSH SERVICE** is enabled (in the PingOne admin console: **Applications → PingID SDK Applications → [Application] → Configuration**) and there is no approval for a silent push sent for extra verification, choose whether to **Regard as Success** or **Regard as Failure**.

> **Note**
>
> This configuration is relevant only to logins from mobile devices, and will be applied to pushless device scenarios, and events when the network is not accessible.

AUTHENTICATION DURING ERRORS

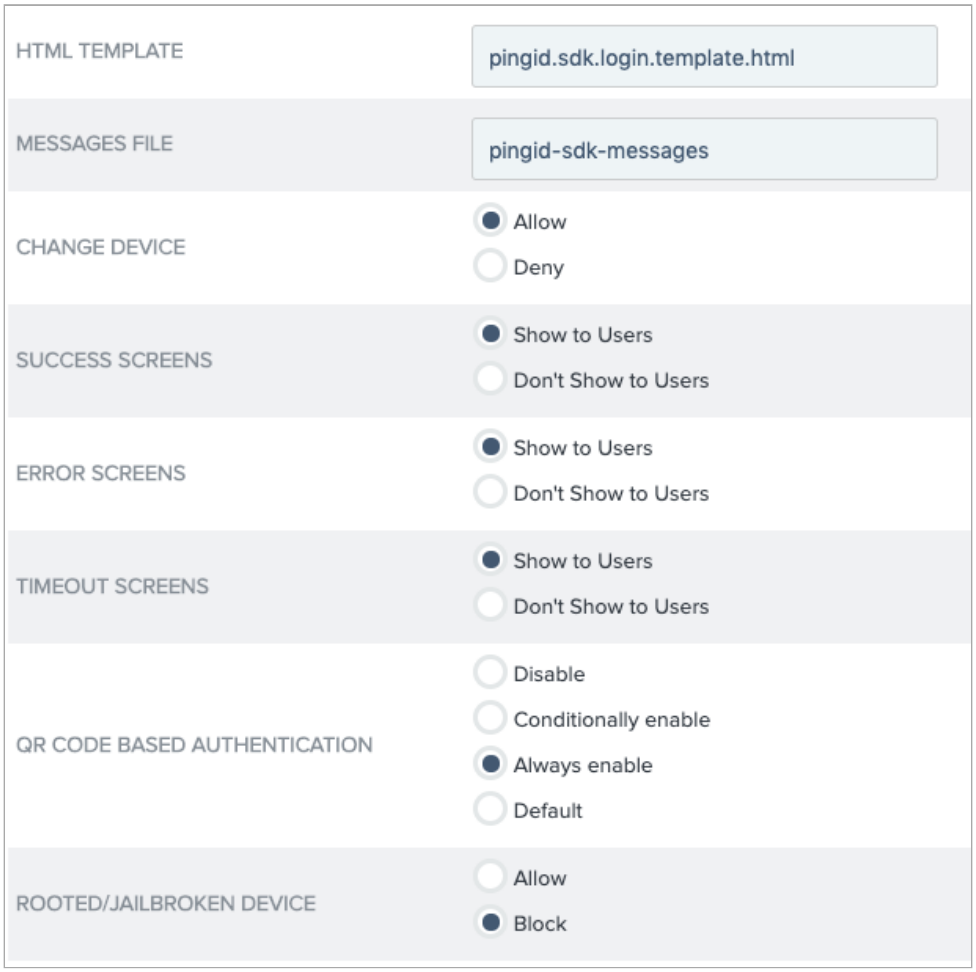
If there are network problems or the PingID SDK service is unreachable, choose whether to **Bypass users** (default) or **Block users** who attempt to authenticate.

HEARTBEAT TIMEOUT

The duration in seconds that the PingID SDK adapter should wait for a heartbeat to verify PingID SDK services, before timing out (default 30 seconds).

6. Click **Advanced fields**.

The advanced fields are displayed.



7. Configure the following fields:

HTML TEMPLATE

> **Note**
>
> This field is relevant only when the PF Authentication API is not used.

- The name of the HTML template file whose screens are displayed to the user during the adapter authorization flow.
- The default is `pingid.sdk.login.template.html`. This default value is applied even if this field is left empty.
- Templates are located at `/server/default/conf/template`.

MESSAGE FILE

- The prefix of the name of the PingID SDK messages file.
- The default is `pingid-sdk-messages`. This default value is applied even if this field is left empty.
- Templates are located at `/server/default/conf/language-packs.`

- The file prefix (for example `pingid-sdk-messages`) may be changed, but the suffix for the locale must be in the format "`_<locale>.properties`", for example: `pingid-sdk-messages_en.properties`.

CHANGE DEVICE

> **Note**
>
> This field is relevant only when the PF Authentication API is not used.

- Choose whether the **CHANGE DEVICE** flow is allowed or denied.
  - **Allow** (default): Users will see the **CHANGE DEVICE** button on all relevant screens.
  - **Deny**: Users will not see the **CHANGE DEVICE** button, and will not have this option as part of their authentication flow.

SUCCESS SCREENS

> **Note**
>
> This field is relevant only when the PF Authentication API is not used.

- Choose whether to present the **SUCCESS SCREENS** as part of the authentication flow.
- Default: **Show to Users**.

ERROR SCREENS

> **Note**
>
> This field is relevant only when the PF Authentication API is not used.

- Choose whether to present the **ERROR** screens as part of the authentication flow.
- Default: **Show to Users**.

TIMEOUT SCREENS

> **Note**
>
> This field is relevant only when the PF Authentication API is not used.

- Choose whether to present the **TIMEOUT** screens as part of the authentication flow.
- Default: **Show to Users**.

QR CODE BASED AUTHENTICATION

> **Note**
>
> QR code based authentication is not supported for the PF Authentication API.

Choose whether to use QR code based authentication, and in which cases:

- **Disable** (default).
- **Conditionally enable**: The QR code is displayed only when the user is unknown.
- **Always enable**: Allows QR code based authentication, whether the user is known or not.
- **Default**: QR code based authentication is the default authentication method, and the QR code is presented by default to the user.

> **Note**
>
> - The **Default** setting overrides the **DEVICES SELECTION** setting in the PingID SDK Applications Configuration in the PingOne admin web portal.
> - QR code based authentication is supported from PingFederate 9.0. Note that PingFederate PingID SDK IDP Adapter 1.2 will work on versions earlier than 9.0 only when **QR CODE BASED AUTHENTICATION** is set to **Disable**. Attempting to save **QR CODE BASED AUTHENTICATION** using a setting other than **Disable** on versions of PingFederate earlier than 9.0 will result in the error message.

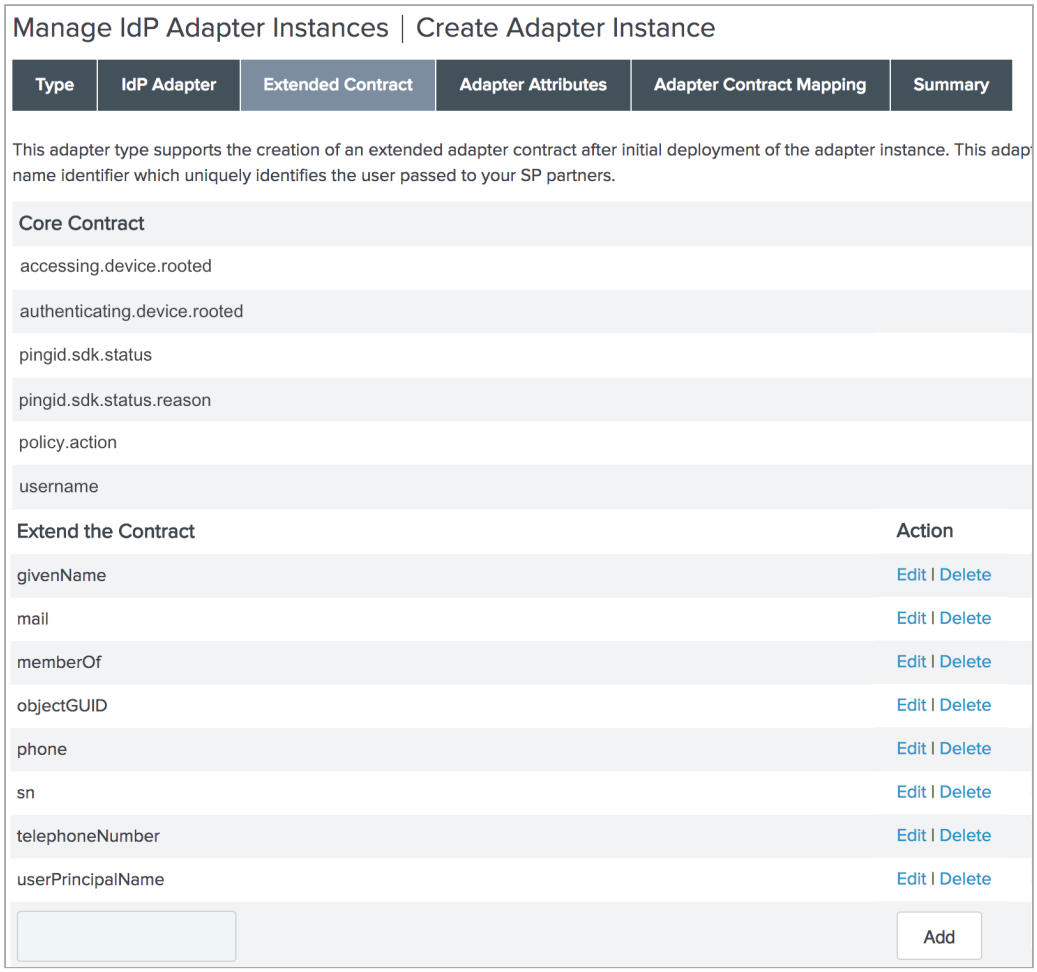
ROOTED/JAILBROKEN DEVICE

- When an authentication device is identified as rooted or jailbroken:
  - **Allow**: Allow the authentication flow to continue.
  - **Block** (default): Deny the authentication request.

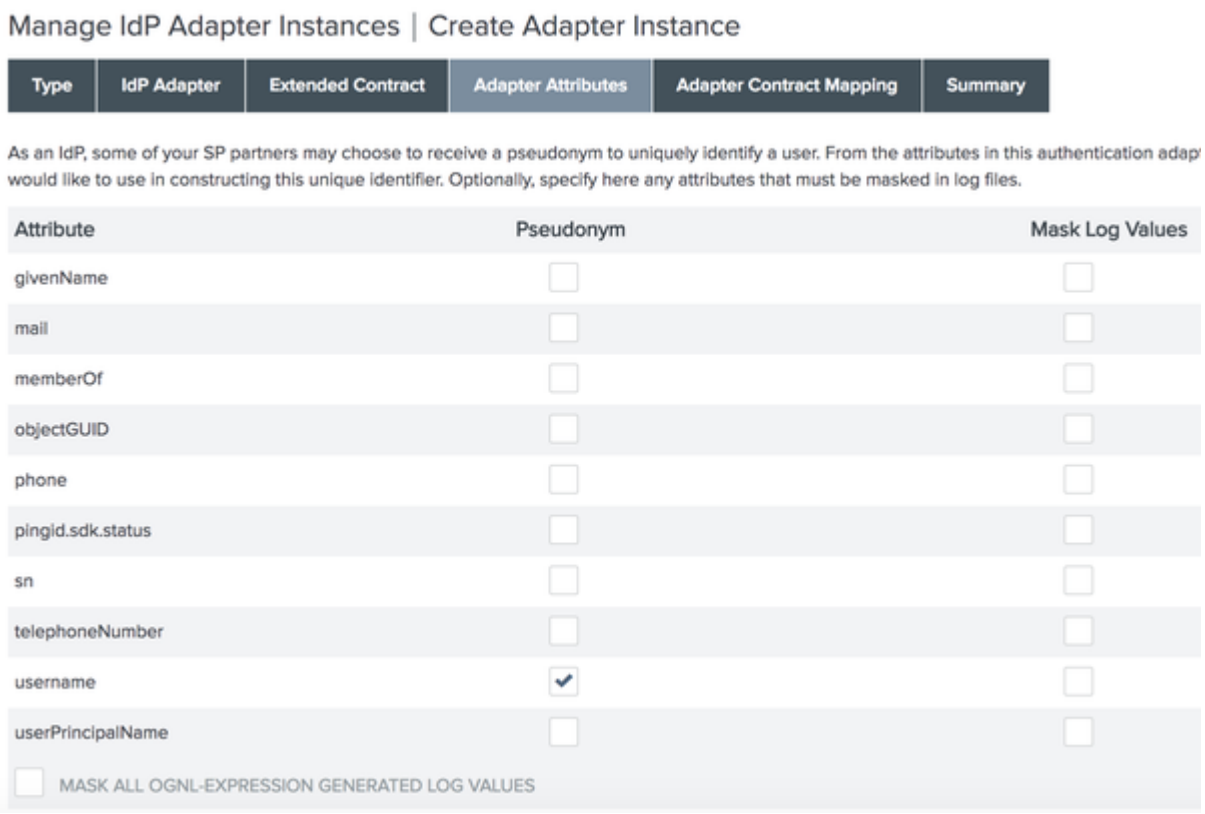
8. Click **NEXT** to continue to the **Extended Contract**step.

The contract fields are displayed. In addition to the `username` attribute, the **Core Contract** also displays the following attributes:

- `pingid.sdk.status` holds information about the level of authentication through which the user was authenticated. For further information about this attribute, refer to PingFederate access token - pingid.sdk.status attribute in the PingID SDK developer guide.From PingFederate PingID SDK IDP Adapter 1.5, the following **Core Contract** attributes provide information about devices that are rooted or jailbroken:
- `pingid.sdk.status.reason` : Possible value is "device_rooted_or_jailbroken", which will appear only when the `pingid.sdk.status` has the value "pairing_error" and the device is rooted.
- `authenticating.device.rooted` : True or false.
- `accessing.device.rooted` : True or false.You can add more attributes to the contract under Extend the Contract, per the example below.



9. Click **NEXT** to continue to the **Adapter Attributes** step.



Check the **Pseudonym** checkbox for the username attribute.

10. Click **NEXT** through each of the subsequent steps.
11. Click **DONE** in the **Summary** step to return to the **Manage IdP Adapter Instances** screen.
12. Click **SAVE** to persist changes.

> **Important**
>
> *Adapter session considerations*
> + It is important to update the `<pf_install>/pingfederate/server/default/conf/size-limits.conf` file to adjust the session configuration to ensure that the PingID SDK adapter functions correctly.
> + Note that the settings in `size-limits.conf` are global, affecting all adapters.

3. **Create and configure a policy**:

   Create a policy in PingFederate, for the purpose of determining the authentication flow.

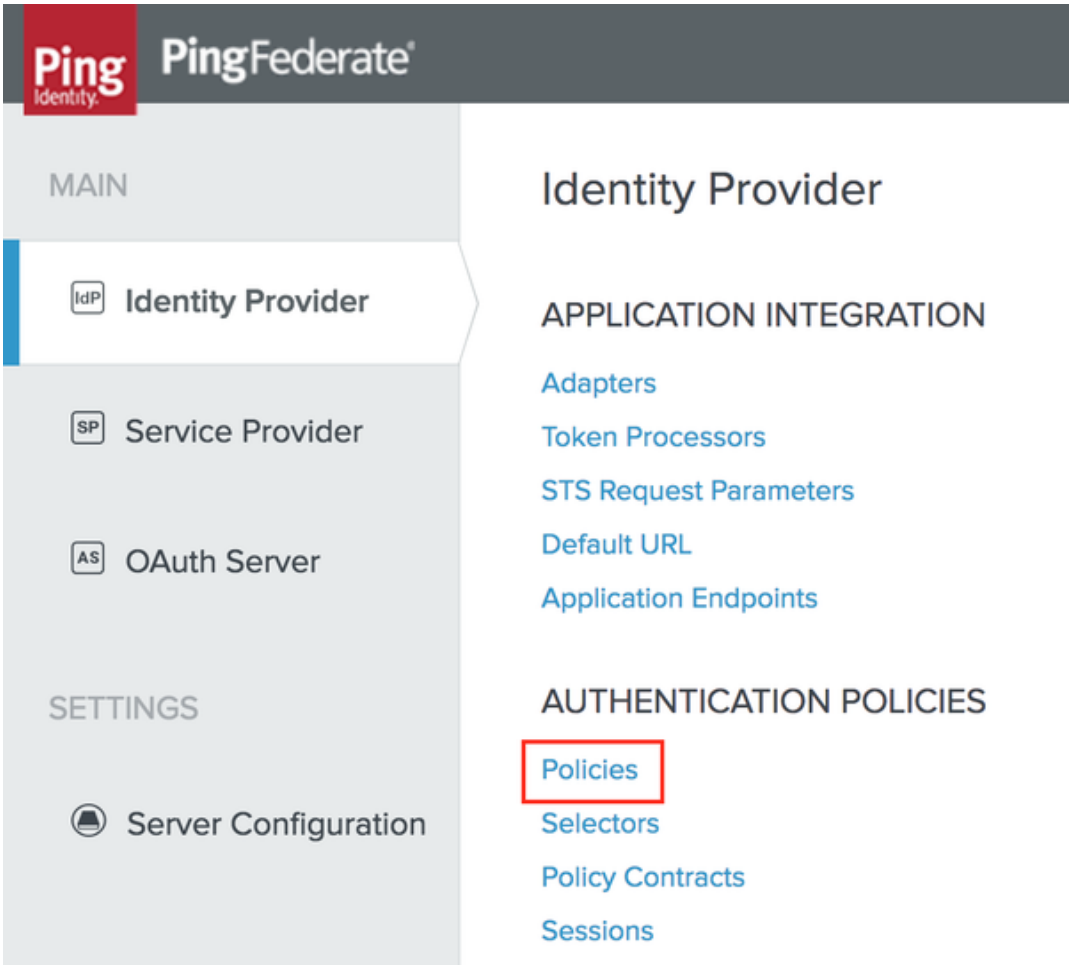
   The flexibility of PingFederate permits implementation of different policy models, and may vary according to organizational or application requirements.

   The following example describes a basic policy configuration for the PingID SDK adapter, highlighting mandatory settings. The example defines a 1st factor authentication method before the SDK adapter, from which the username must then be mapped to the SDK adapter.

Important

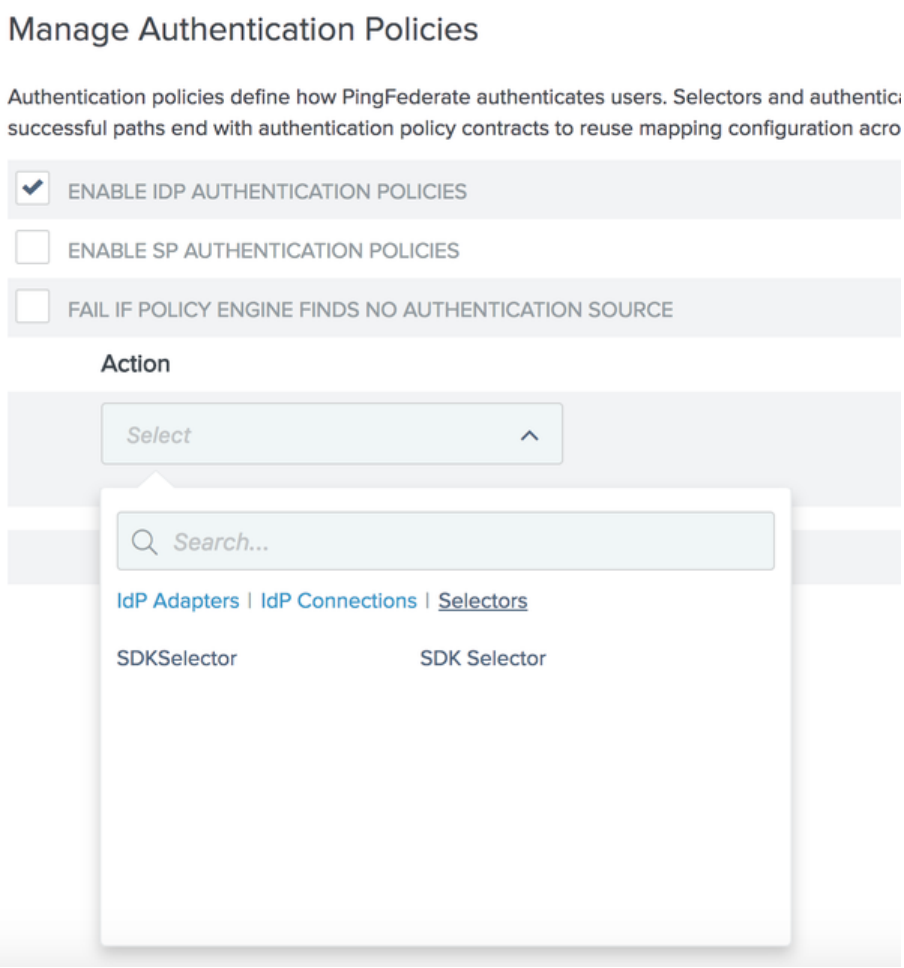
- The SDK selector or Tracked HTTP Parameter:
  - **PingFederate 9.1.x and below**: The PingID SDK Payload Handling Selector that was created earlier must be the first action in a policy actions chain.
  - **PingFederate 9.2+**: The PingID SDK Payload Handling Selector is not required, only if the " `payload` " parameter has been added to PingFederate's Tracked HTTP Parameters (see https://support.pingidentity.com/s/document-item?bundleId=pingfederate-92&topicId=adminGuide/pf_t_defineAuthenticationPolicies.html).
- The SDK adapter created earlier must participate in the policy flow.

1. In the PingFederate administrative console, select: **Identity Provider → AUTHENTICATION POLICIES → Policies**.



The **Manage Authentication Policies** screen is displayed.

1. Enter the following fields:



1. Check the **ENABLE IDP AUTHENTICATION POLICIES** checkbox.
2. The SDK selector or Tracked HTTP Parameter:
    - **PingFederate 9.1.x and below**: The first **ACTION** in the policy chain **must** be mapped to the SDK selector created earlier:
        - Open the **ACTION** dropdown.
        - Click **IdP Adapters**.
        - Select the **SDK selector**.
        - The SDK selector has only one return status: **Success**.

          For the policy's following action, select **HTML Adapter** (or any other 1st factor adapter) from the **ACTION** dropdown.
    - **PingFederate 9.2+**: If the "`payload`" parameter has been added to PingFederate's Tracked HTTP Parameters (see https://support.pingidentity.com/s/document-item?bundleId=pingfederate-92&topicId=adminGuide/pf_t_defineAuthenticationPolicies.html):
        - Open the **ACTION** dropdown.
        - Click **HTML Adapter** (or any other 1st factor adapter).

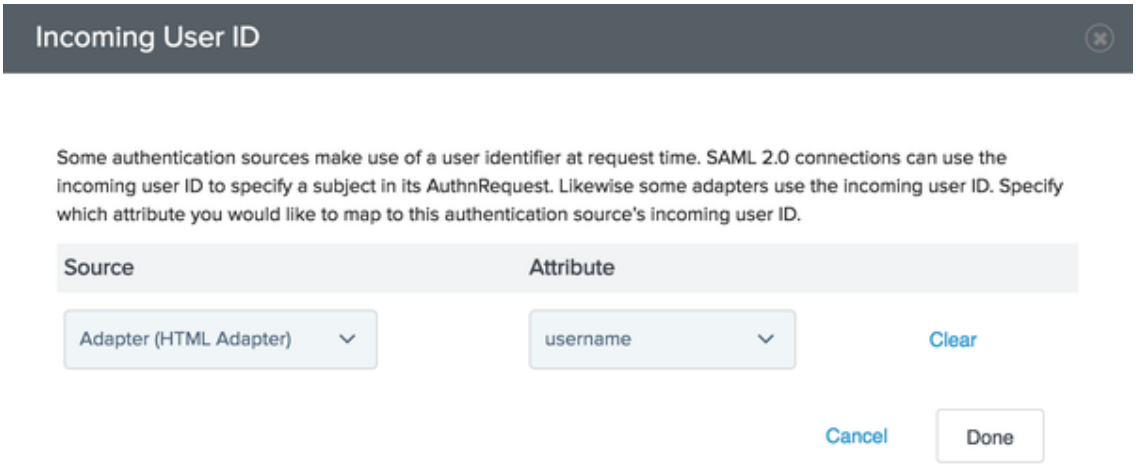
- Select the **HTML Adapter**.

3. The **HTML Adapter** has two resulting states:
   - **Fail**:

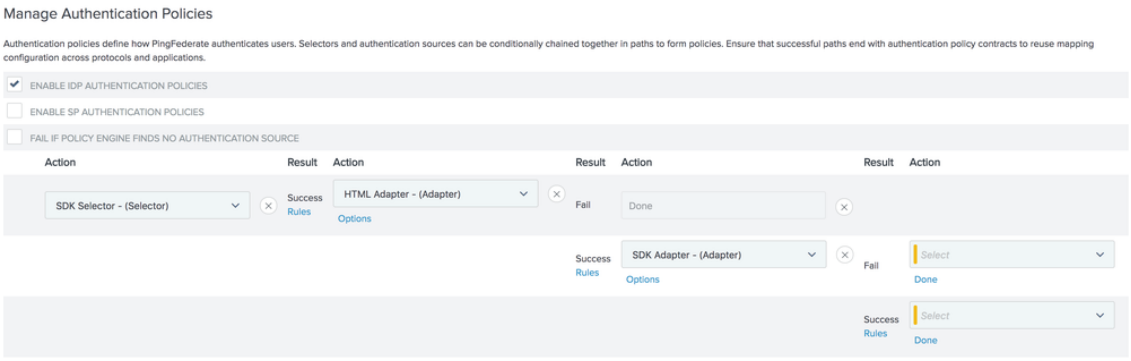
     The action following **Fail** will be **Done**, meaning the policy flow ends at this point.
   - **Success**:

     Select the **SDK Adapter** for the action following **Success**.
4. Map the username from the **HTML Adapter** (or any other 1st factor adapter) step in the policy flow to the **SDK Adapter**:
   - Click on **Options** below the SDK Adapter.

     The **Incoming User ID** screen opens.

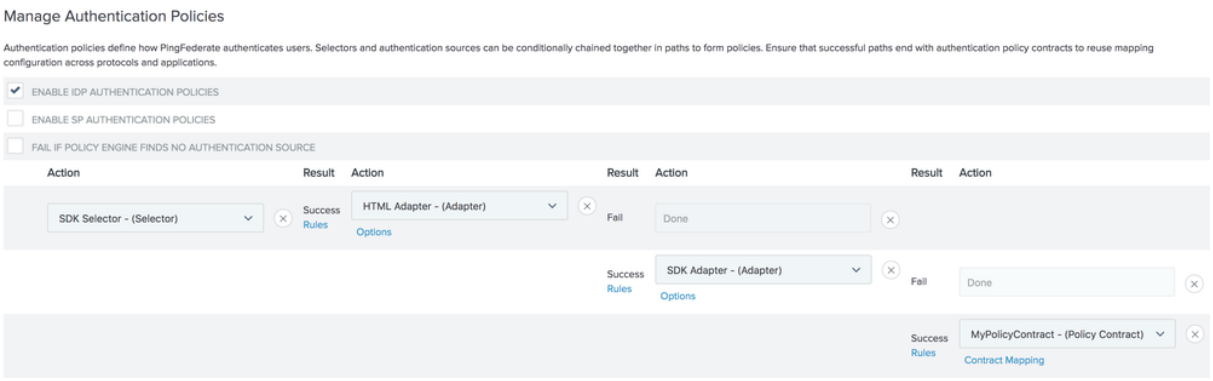


     - **Source**: Select **HTML Adapter**.
     - **Attribute**: Select **username**.
   - Click **Done** to return to the **Manage Authentication Policies** screen.



5. An Authentication Policy Contract should then be mapped into the target application (SP Connection, OAuth Grant Mapping, etc.) for which you want to provide SSO services.

   For example:



6. Click **Save**.

4. (Optional) **Configure proxy settings**:

   Define an entry in the PingFederate `run.properties` file, as described in the PingFederate admin guide (see https://documentation.pingidentity.com/pingfederate/pf/index.shtml#adminGuide/pf_t_configureForwardProxyServerSettings.html).

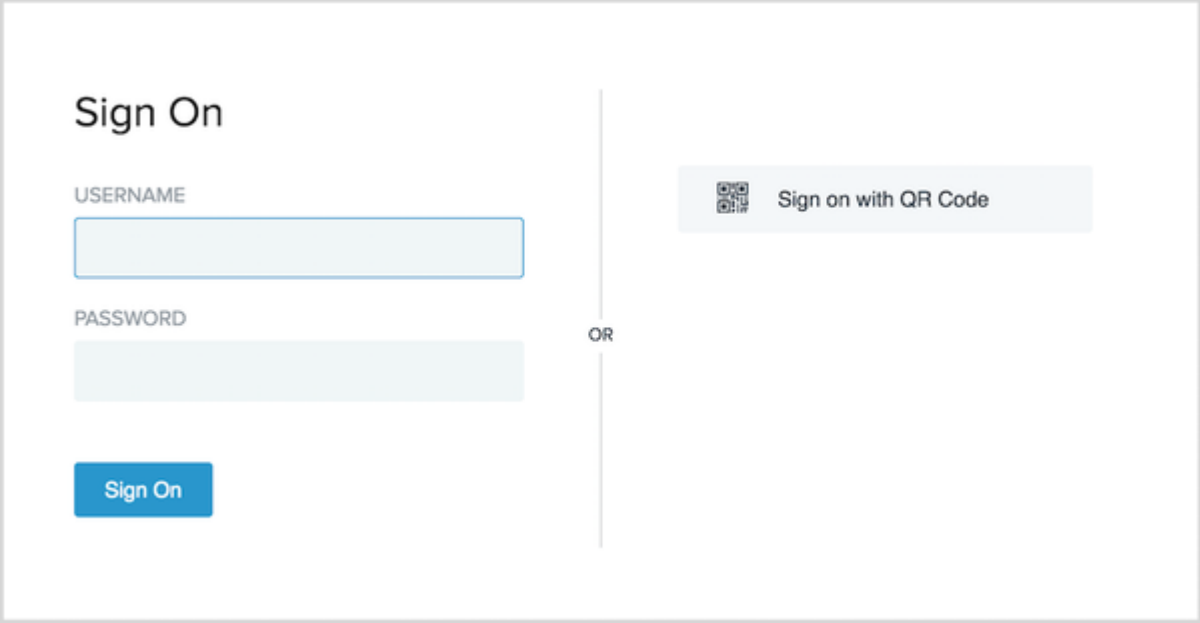
   > **Note**
   >
   > The native PingFederate method for defining a proxy is the preferred option. The following deprecated method is still supported:
   >
   > 1. Manually add a `pingidsdk_proxy_url` entry to your PingID SDK properties file:
   >
   >    ```
   >    pingidsdk_proxy_url=<your proxy address>
   >    ```
   >
   > 2. Do not change the `pingidsdk_url` entry.
   >
   > If entries are defined in both the PingFederate `run.properties` and the PingID SDK properties files, the definition in the PingID SDK properties file will take precedence.

5. (Optional) **HTML Form Adapter QR code button - passwordless login**:

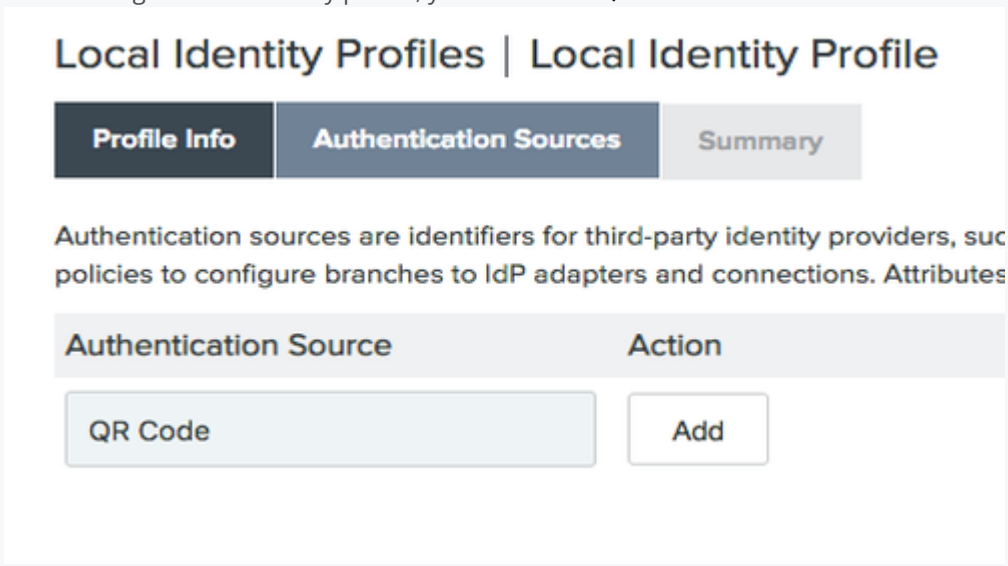
   > **Note**
   >
   > - QR code based authentication requires PingFederate 9.2+ and PingFederate PingID SDK IDP Adapter 1.2+.
   > - QR code based authentication is not supported for the PF Authentication API.

   QR code based authentication is an alternative method, which offers secure, passwordless authentication. QR code based authentication can effectively eliminate the need for first factor authentication. This method combines the strength of a strong secure authentication measure, with a streamlined user experience.

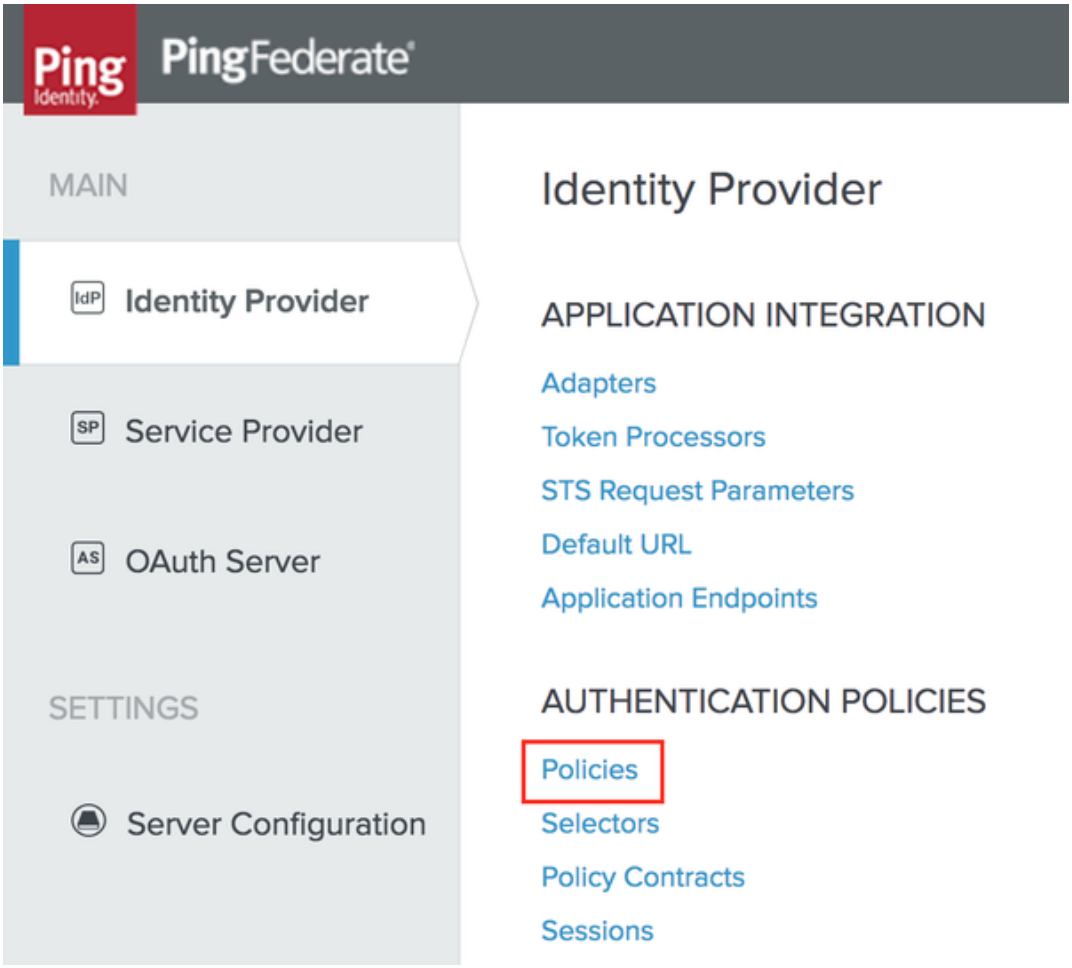
   The following image presents the user HTML Form Adapter access screen. Once configured, the user can either use the traditional username and password sign on at the left, or select the **Sign on with QR code** button on the right. **Sign on with QR code** generates a QR code image which the user can scan with a trusted mobile device, thus achieving rapid secure passwordless authentication.



1. Refer to the Enable third-party identity providers without registration topic in the PingFederate documentation, specifically the following steps:
    1. Make a note of which authentication policy contract is currently being used in your policy.
    2. Create a local identity profile.

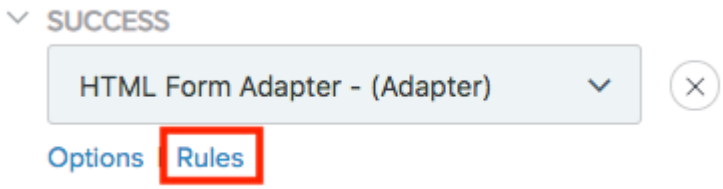
    > **Note**
    >
    > When creating the local identity profile, you must add " `QR Code` " as an **Authentication Source**.
    >
    > 
    >

    3. Configure the HTML Form Adapter instance for customer identities.
2. Navigate to **Identity Provider → Authentication Policies → Policies**.



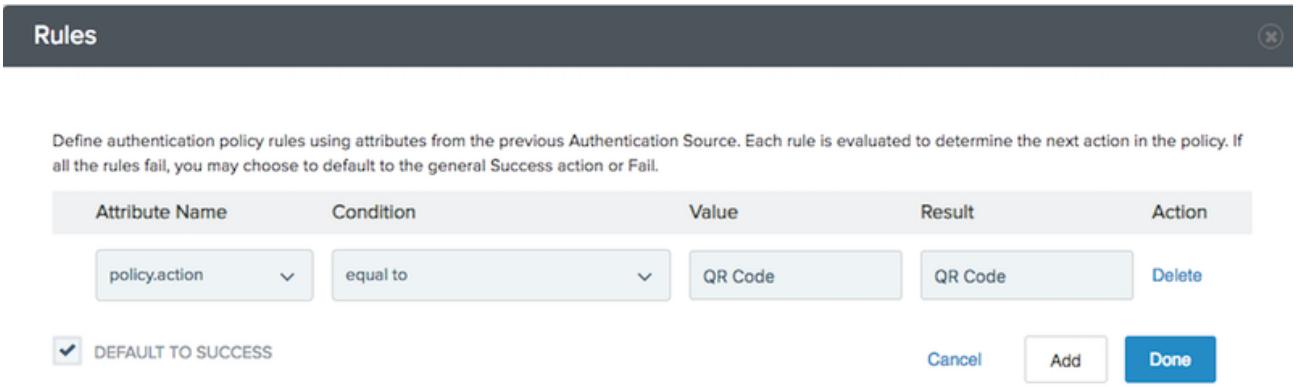
3. In the **Authentication Policies** page, edit your PingID SDK authentication policy.

4. Below the HTML Form Adapter, expand the policy tree and select **Rules**.

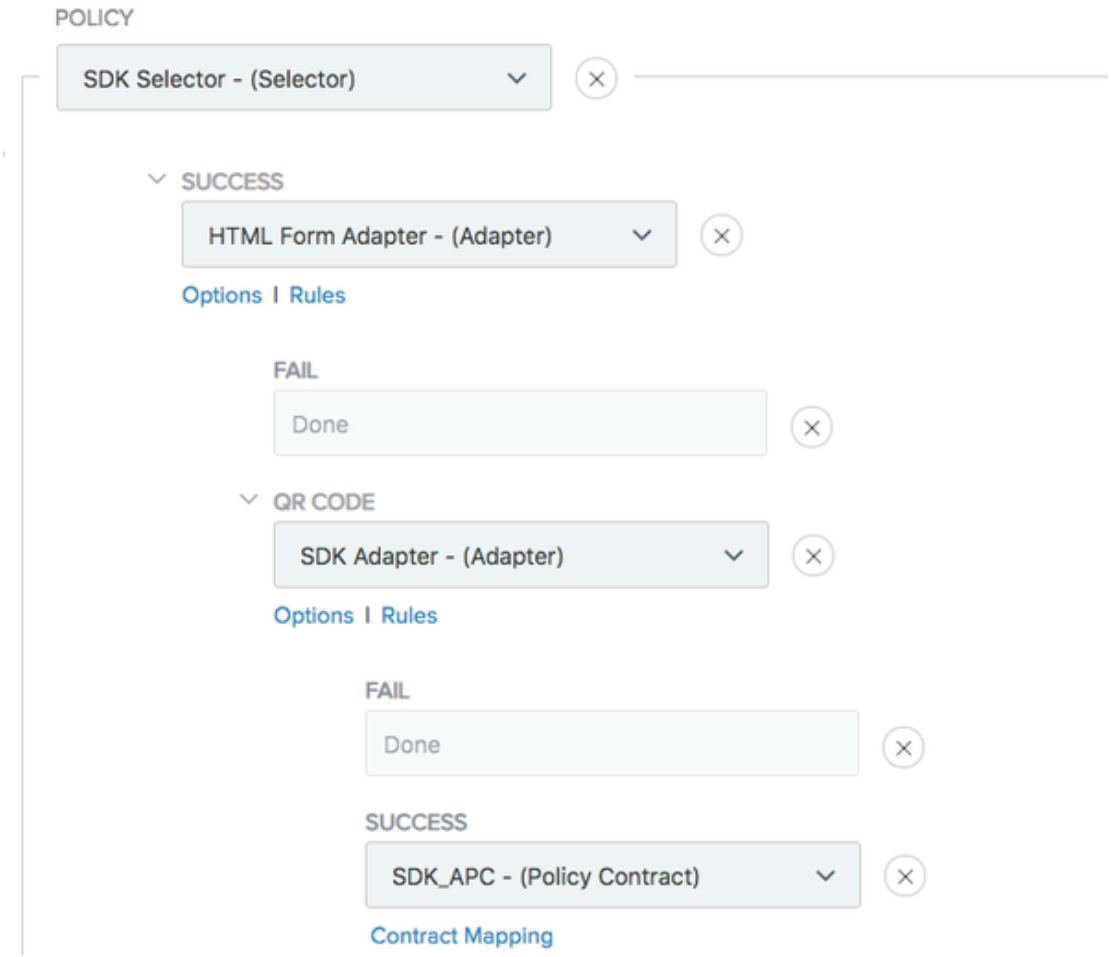


5. In the **Rules** popup, fill in the following values:

Field	Value
`Attribute Name`	`policy.action`
`Condition`	`equal to`
`Value`	`QR Code`
`Result`	`QR Code`

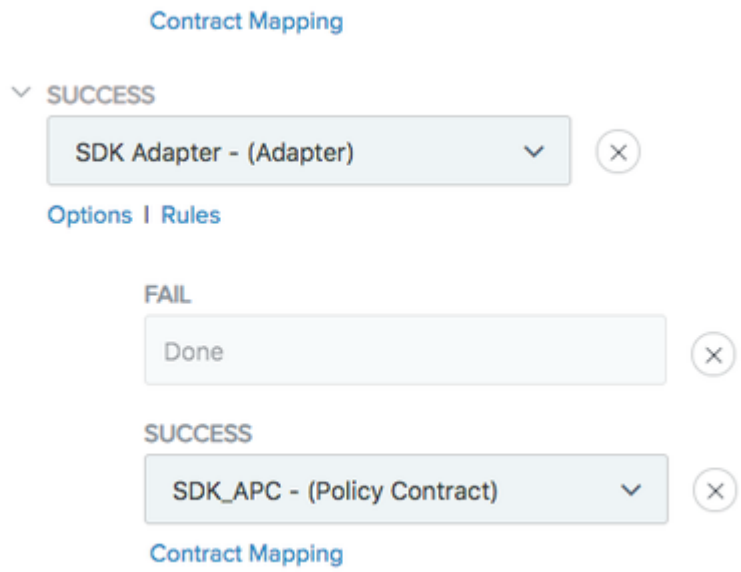


6. Click **Done**.
7. Below the **HTML Form Adapter** branch, the **QR CODE** policy result is displayed, in addition to the FAIL and SUCCESS branches.



8. In the **QR Code** result, select the **SDK Adapter**, and finish building the flow according to the steps in the [createConfigurePolicy] section.

   The final result should appear similar to the following image:



6. (Optional) **Add a CANCEL button to the QR code based authentication flows**:

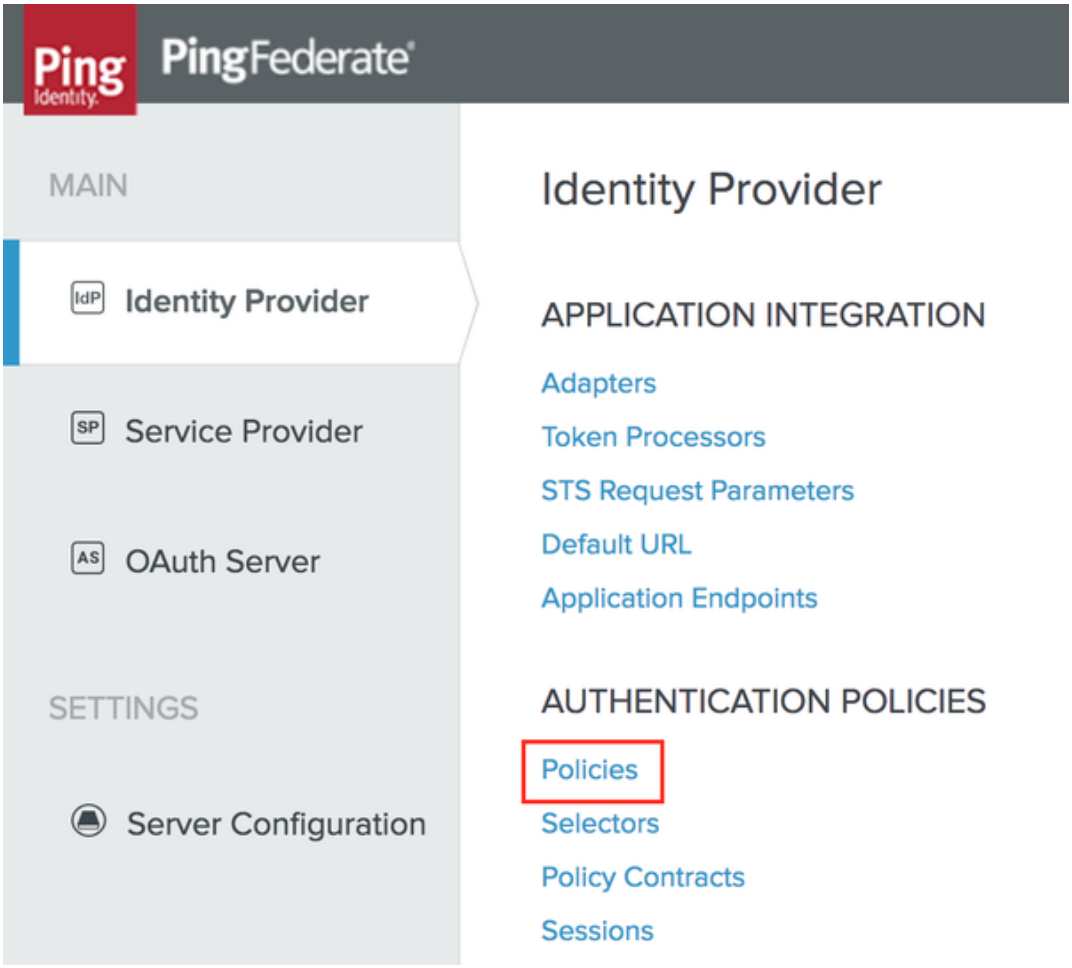
> **Note**
>
> - QR code based authentication requires PingFederate 9.2+ and PingFederate PingID SDK IDP Adapter 1.2+.
> - QR code based authentication is not supported for the PF Authentication API.

There may be scenarios where an organization wants to allow users of QR code based authentication to cancel an authentication request. This can be achieved by configuring a CANCEL button in the QR based authentication flow, and defining its functionality in the authentication policy. By default, the CANCEL button is not enabled.

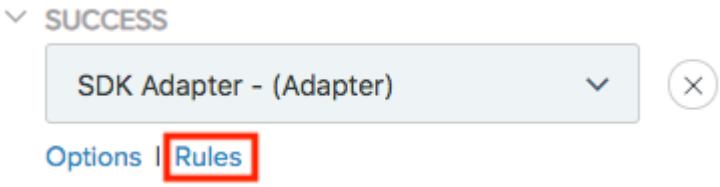
1. **Configure a CANCEL Button in the HTML template**:
    1. Open the HTML template file `<PingFederate installation folder>/pingfederate-<version>/pingfederate/server/default/conf/template/pingid.sdk.login.template.html` in a text editor.
    2. Scroll down to the **QR Code section**. You'll see the following commented out lines, where you can add a CANCEL button in the QR image page, deep link page and loading page:

```
<!-- uncomment the following line if you "cancel" is supported -->
<!-- <a class="button"
onclick="cancelQRCode(this)"href="javascript:void(0);">$messages.getMessage("pingid.sdk.authentica
a>-->
```

    3. To add a CANCEL button to the page, uncomment the second line (containing the <a> tags).
2. **Add a CANCEL function in the authentication policy**:
    1. In the PingFederate admin console, navigate to **Identity Provider → Authentication Policies → Policies**.

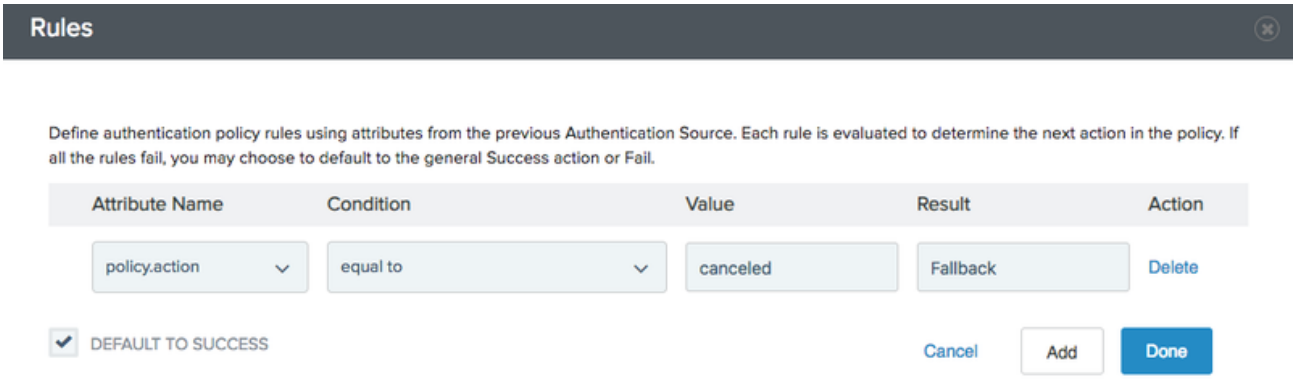


1. In the **Authentication Policies** page, edit your PingID SDK authentication policy.
2. Below the SDK Adapter, expand the policy tree and select **Rules**.



3. In the **Rules** popup, fill in the following values:

Field	Value
`Attribute Name`	`policy.action`
`Condition`	`equal to`
`Value`	`canceled`
`Result`	`Fallback` (You may choose a different name.)



4. Click **Done**.
5. Below the **SDK Adapter** branch, the **FALLBACK** policy result is displayed, in addition to the FAIL and SUCCESS branches.

6. To configure it as a restart flow action, select **Restart**.

> **Note**
>
> You can also choose different actions. For example, redirect the user to a different adapter.

7. Click **Done**.
8. Click **Save**.
9. (Optional): If you want to change the action's default value ("canceled") to a different value:
   - Go to the following line in the HTML template:

```
<form id="cancelQRCodeForm" name="cancelQRCodeForm"
          action="$resumePath?cancel=1&action=canceled" method="post">
          <input type="hidden" name="csrfToken" id="csrfToken" value="$csrfToken"
          encode="false"/>
</form>
```

   - Change `&action=canceled` to `&action=<your value>`. Make sure that this new value is identical to the "`Value`" field in the **Authentication Policies → Rules** popup.
   - Click **Done**.
   - Click **Save**.

Configuring the CIBA Authenticator for PingID SDK

Create and configure a Client-Initiated Backchannel Authentication (CIBA) Authenticator for PingID SDK.

About this task

This procedure describes the process of creating and configuring a Client Initiated Backchannel Authentication (CIBA) Authenticator for the purpose of authenticating users via an out-of-band authentication method.

Prerequisites:

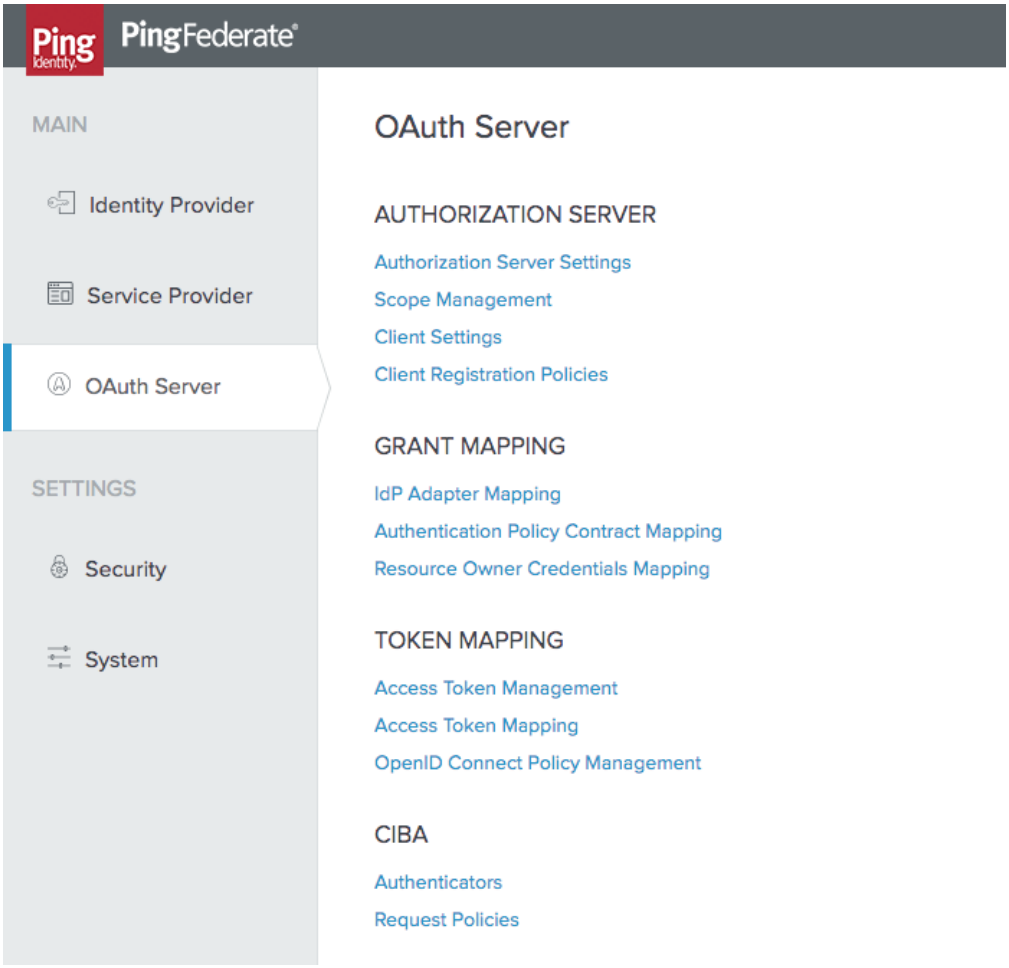
- PingFederate 9.3+
- PingID SDK Package v1.10+ (comprising PingID SDK Integration Kit v1.7+ and PingID SDK Adapter for PingFederate v1.6+)

Note

- The PingID SDK CIBA Authenticator supports mobile devices only.
- The PingID SDK CIBA Authenticator is part of the PingID SDK integration with PingFederate, but is not part of the PingID SDK Adapter for PingFederate.
- The CIBA configuration for PingID SDK assumes that a user has at least one mobile device.
- A push notification is sent to the user's primary device. If the user's primary device is not a mobile, the push notification is sent to their first enabled mobile device.
- If an authenticating device is bypassed or pushless, that device is ignored.
- The admin console UI menu labels presented in this topic are those used in PingFederate 9.3. These may differ slightly from other versions of PingFederate.

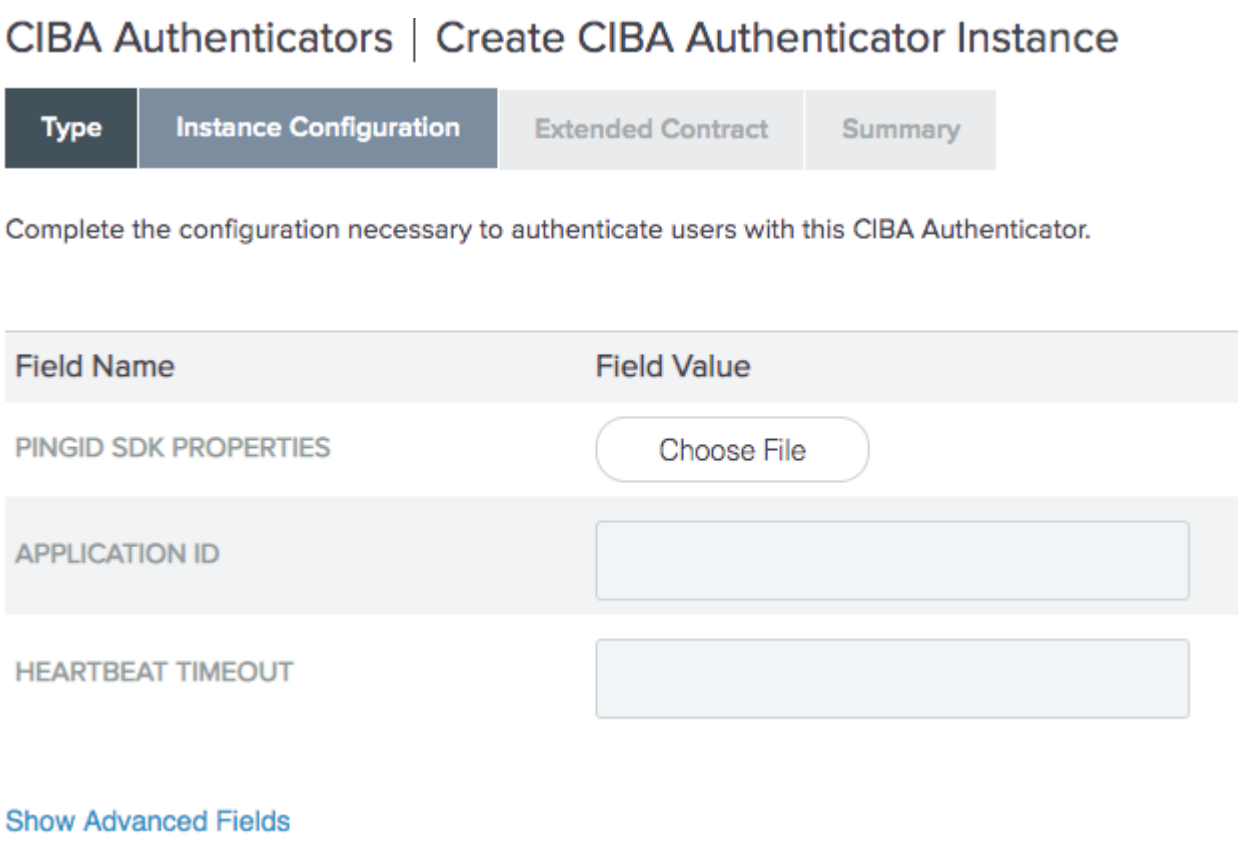
Steps

1. In the PingFederate admin console, select: **OAuth Server → CIBA → Authenticators**.



2. Click **Create New Instance** to create a new authenticator, or click on an existing authenticator to edit it.
3. Enter the CIBA authenticator's initial instance definitions:
    1. **INSTANCE NAME**: Enter a descriptive name for this authenticator.
    2. **INSTANCE ID**: Enter a string which will be used as an ID for this authenticator. Spaces are not allowed.
    3. **TYPE**: Select **PingID SDK CIBA Authenticator** from the dropdown options.
4. Click **NEXT**.

    The CIBA authenticator's **Type** step is displayed.



5. Enter the fields in the authenticator's **Type** step:

    1. **PINGID SDK PROPERTIES**: Upload the PingID SDK properties file from your PingOne admin console:

        - In the PingOne admin console, go to **Setup → PingID → CLIENT INTEGRATION → INTEGRATE WITH PINGID SDK → SETTINGS FILE**.
        - Click **Download**. You may want to provide the file with a more meaningful name.

    > **Important**
    >
    > The PingID SDK settings file should not be confused with the PingID properties file.

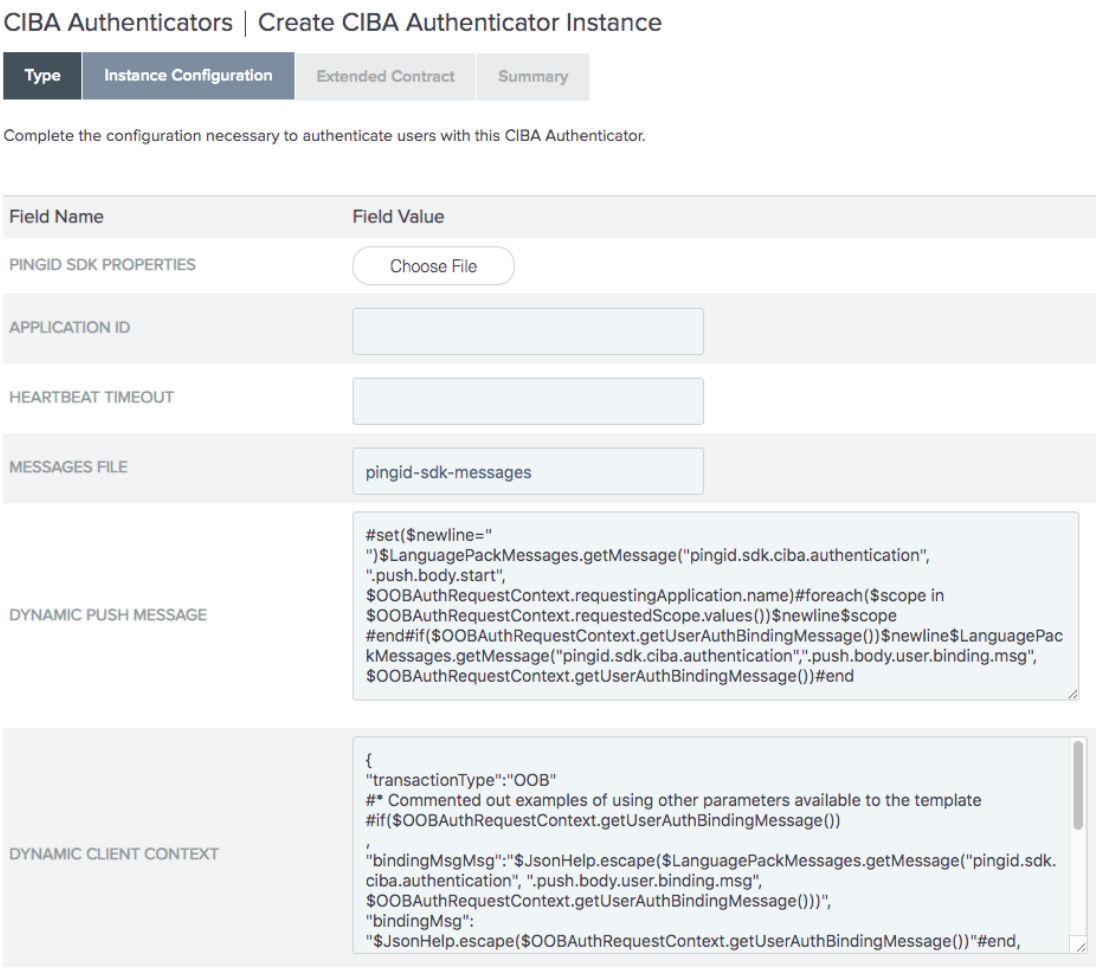
    1. **APPLICATION ID**: Enter the application ID that was generated by PingID SDK in your application configuration:

        - In the PingOne admin console, go to **Applications → PingID SDK Applications**, and copy the **Application ID**.

    2. **HEARTBEAT TIMEOUT**: The duration in seconds that thePingID SDK CIBA Authenticator should wait for a heartbeat to verify PingID SDK services, before timing out (default 30 seconds).

6. Click **Show Advanced Fields**.

    The **Type** step's advanced fields are displayed.



7. Enter the following advanced fields:

    1. **MESSAGES FILE**: The prefix of the name of the PingID SDK messages file.

        - The default is `pingid-sdk-messages`. This default value is applied even if this field is left empty.
        - Templates are located at `/server/default/conf/language-packs.`
        - The file prefix (for example `pingid-sdk-messages`) may be changed, but the suffix for the locale must be in the format "`_<locale>.properties`", for example: `pingid-sdk-messages_en.properties`.
        - The following parameters are required for the default values of the push message's title and body texts in the **DYNAMIC PUSH MESSAGE** and **DYNAMIC CLIENT CONTEXT** fields:
            - `pingid.sdk.ciba.authentication.push.title`: populates the `pushMessageTitle` parameter.
            - `pingid.sdk.ciba.authentication.push.body.start`: The default **DYNAMIC PUSH MESSAGE** template uses this key.
            - `pingid.sdk.ciba.authentication.push.body.user.binding.msg`: The default **DYNAMIC CLIENT CONTEXT** template uses this key.

            These parameters may be replaced, or removed.

2. **DYNAMIC PUSH MESSAGE**: A velocity language template that PingID SDK uses to pass push authentication messages to the device. The template is used to populate the `pushMessageBody` parameter, using the following variables:

    - `OOBAuthRequestContext` : Refer to the PingFederate developer documentation https://www.pingidentity.com/content/dam/developer/documentation/pingfederate/server-sdk/9.3/index.html?com/pingidentity/sdk/oobauth/class-use/OOBAuthRequestContext.html.
    - `LanguagePackMessages` : Refer to the PingFederate developer documentation https://www.pingidentity.com/content/dam/developer/documentation/pingfederate/server-sdk/9.3/index.html?com/pingidentity/sdk/locale/LanguagePackMessages.html.

3. **DYNAMIC CLIENT CONTEXT**: A velocity language template that PingID SDK uses to pass push authentication messages to the device. The template is used to populate the `clientContext` parameter, using the following variables:

    - `OOBAuthRequestContext` : Refer to the PingFederate developer documentation https://www.pingidentity.com/content/dam/developer/documentation/pingfederate/server-sdk/9.3/index.html?com/pingidentity/sdk/oobauth/class-use/OOBAuthRequestContext.html.
    - `LanguagePackMessages` : Refer to the PingFederate developer documentation https://www.pingidentity.com/content/dam/developer/documentation/pingfederate/server-sdk/9.3/index.html?com/pingidentity/sdk/locale/LanguagePackMessages.html.
    - `SimpleTitle` : String. The push message's title.
    - `SimpleBody` : String. The push message's body text.
    - `JsonHelp` : Jose4j JSONValue class. Refer to https://javadoc.io/doc/org.bitbucket.b_c/jose4j/0.4.1/org/jose4j/json/internal/json_simple/JSONValue.html.

8. Save the configuration.
9. **Optional:** Configure a dynamic notification push category or dynamic application ID.

    CIBA authenticators support dynamic notification push categories and dynamic application IDs, and their configurations are similar.

Dynamic notification push categories

A CIBA authenticator can receive a notification push category as a dynamic attribute. This enables a single CIBA authenticator to work with multiple categories, and submit push notifications according to categories.

> **Note**
>
> **Dynamic notification push category** configuration requires the following software versions:
> - PingFederate 9.3+
> - PingID SDK Package v1.13+ comprising:
>   - PingID SDK Integration Kit v1.9+
>   - PingID SDK Adapter for PingFederate v1.8+
>   - PingID SDK CIBA Authenticator 1.1+

Dynamic application IDs

A CIBA authenticator can receive an application ID as a dynamic attribute. This enables a single CIBA authenticator to work with multiple applications. The dynamic application ID overwrites the default application ID value (see APPLICATION ID configuration above). If the CIBA authenticator receives an invalid or non-existent application ID, an error is generated.

> **Note**
>
> **Dynamic application ID** configuration requires the following software versions:
> - PingFederate 9.3+
> - PingID SDK Package v1.14.4+ comprising:
>   - PingID SDK Integration Kit v1.11+
>   - PingID SDK Adapter for PingFederate v1.8.1+
>   - PingID SDK CIBA Authenticator 1.1.1+

10. In the PingFederate admin console, select: **OAuth Server → CIBA → Authenticators**.
11. In the authenticator's **Extended Contract** step, under **Extend the Contract**:

    Choose from:

    - To configure a dynamic notification push category, enter `pingIdSdkPushCategory`
    - To configure a dynamic application ID, enter `pingIdSdkApplicationId`

    Click **ADD**.
12. Click **SAVE**.
13. In the PingFederate admin console, select: **OAuth Server → CIBA Request Policies**.
14. Click **Add Policy**.

    For more information, see Managing CIBA request policies and Defining issuance criteria for identity hint contract in the PingFederate Administration Guide.
15. In the **Identity Hint Contract** step, under **Extend the Contract**:

    Choose from:

    - To configure a dynamic notification push category, enter `request.pingIdSdkPushCategory`
    - To configure a dynamic application ID, enter `request.pingIdSdkApplicationId`

    Click **ADD**.
16. Click **NEXT**.

    The CIBA policy's **Identity Hint Mapping** step is displayed.
17. Click **Manage Fulfillment**.
18. In the **Identity Hint Mapping** step:

Choose from:

- To configure a dynamic notification push category, select `Request` in the **Source** column of the `request.pingIdSdkPushCategory` contract.
- To configure a dynamic application ID, select `Request` in the **Source** column of the `request.pingIdSdkApplicationId` contract.

Click **ADD**.

19. Save the configuration.

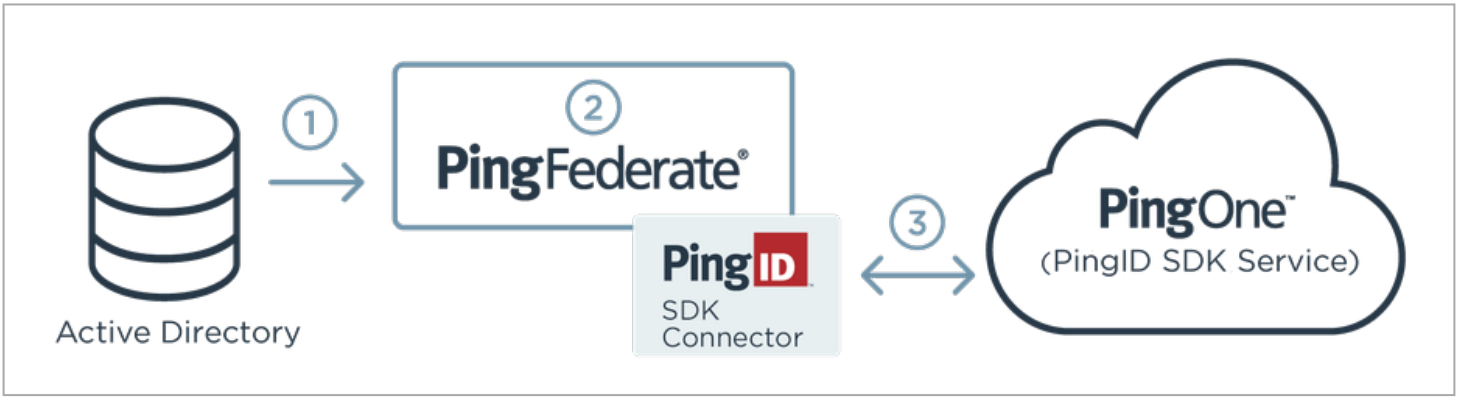
Automatic synchronization of PingID SDK with a PingFederate user directory

The PingID SDK Connector synchronizes user identities and their profile attributes from a configured datastore within PingFederate to PingID SDK.

Ping Identity offers a catalog of connectors that provide provisioning capabilities to SaaS providers. The connectors act as a mediator to handle transactions safely and securely. The PingID SDK Connector offers profile management solutions to multiple directory types, such as LDAP, Active Directory (AD), and PingDirectory.

The PingID SDK Connector:

- Includes support for user life cycle management that lets you create, update, disable, and delete users
- Includes configuration options for workflow capabilities, such as the ability to disable updates



The PingID SDK Connector flow:

1. PingFederate polls the user directory for any changes to user records at regular intervals, configurable in PingFederate.
2. Returned records are stored within PingFederate's intermediary database and marked as requiring an update in PingID SDK (PingOne).
3. The connector pulls the marked record from the intermediary database and performs the necessary operation (Create, Get, Update, Delete) against the PingID SDK record. These changes are reflected in the PingOne admin portal.

To download the PingID SDK for PingFederate connector, go to PingID Server SaaS Connectors.

For more information on configuring the PingID SDK for PingFederate connector, see PingFederate PingID SDK Connector Guide.

Accessing the PingID End User Guide

The PingID End User guide describes the user experience, and includes all the information a user needs to know to pair, and authenticate with PingID. It also details how to pair more than one device, how to manage devices, and some basic troubleshooting information.

To view the PingID End User Guide, see PingID End User Guide.