Enterprise Connect

July 4, 2025

ENTERPRISE CONNECT

Version: Latest

Copyright

All product technical documentation is
Ping Identity Corporation
1001 17th Street, Suite 100
Denver, CO 80202
U.S.A.

Refer to https://docs.pingidentity.com for the most current product documentation.

Trademark

Ping Identity, the Ping Identity logo, PingAccess, PingFederate, PingID, PingDirectory, PingDataGovernance, PingIntelligence, and PingOne are registered trademarks of Ping Identity Corporation ("Ping Identity"). All other trademarks or registered trademarks are the property of their respective owners.

Disclaimer

The information provided in Ping Identity product documentation is provided "as is" without warranty of any kind. Ping Identity disclaims all warranties, either express or implied, including the warranties of merchantability and fitness for a particular purpose. In no event shall Ping Identity or its suppliers be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages, even if Ping Identity or its suppliers have been advised of the possibility of such damages. Some states do not allow the exclusion or limitation of liability for consequential or incidental damages so the foregoing limitation may not apply.

Table of Contents

Understand passwordless

Add-on

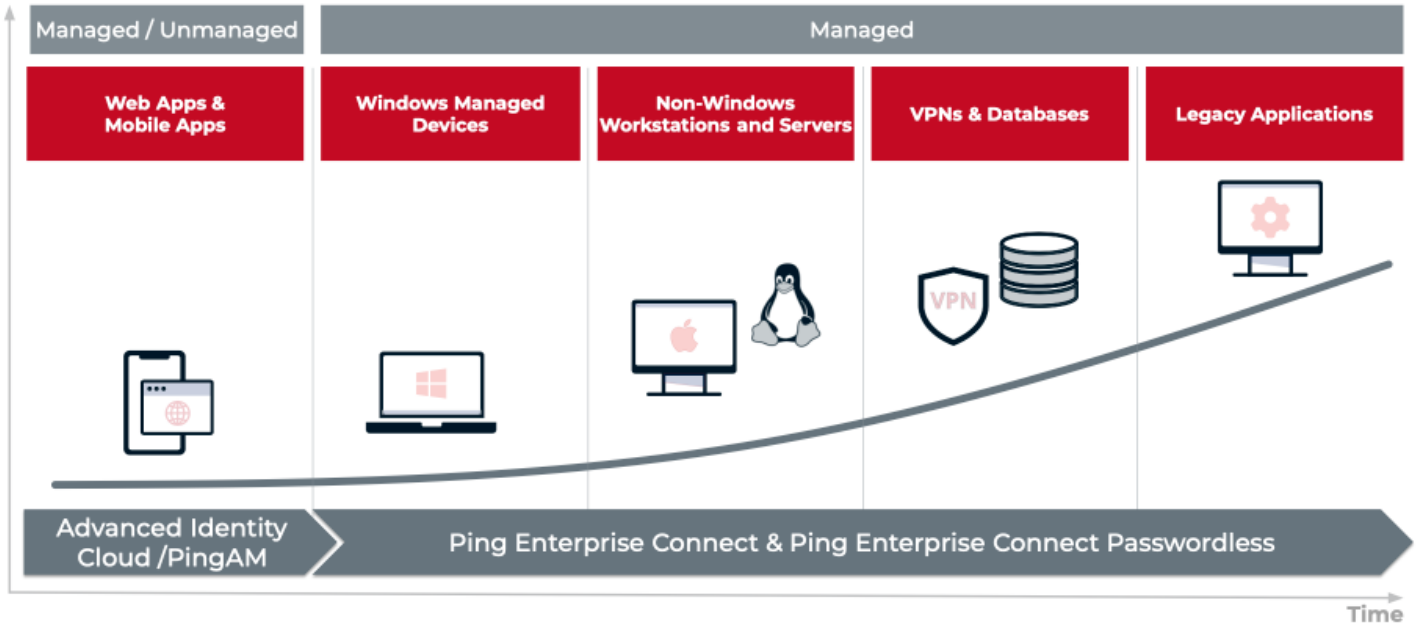
Ping Enterprise Connect and Ping Enterprise Connect Passwordless are add-on capabilities available for purchase for PingOne Advanced Identity Cloud and self-managed versions of PingAM. Contact your Ping representative for more details on how these capabilities can enhance your organization's security posture.

Note

Ping Enterprise Connect documentation only supports English at this time.

The term passwordless often has multiple meanings in today's technological landscape. While complete passwordless is the final stage of a passwordless journey, not all organizations can move directly to this end-state and not all applications/systems can be in this state.

Where you are on your journey to passwordless will differ depending on time and if the workstations, servers, applications, and systems can adopt passwordless technologies.



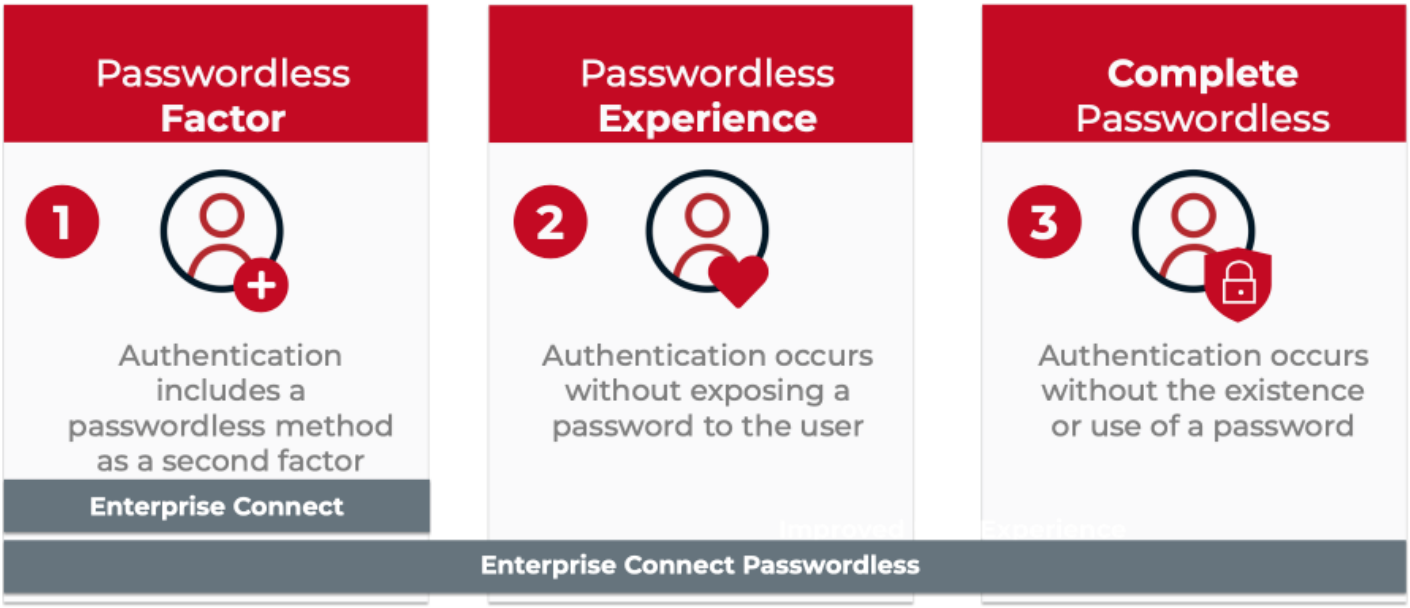
While PingOne Advanced Identity Cloud and PingAM provide the capability to use multi-factor authentication (MFA) or complete passwordless for web and mobile apps for authentication, managed devices are often left unaddressed.

Devices such as:

- Windows workstations
- Non-Windows workstations and servers, such as Macs and Linux
- VPNs and databases
- Legacy systems

This is where Enterprise Connect and Enterprise Connect Passwordless come into play.

Copyright © 2025 Ping Identity Corporation



- 1 Passwordless Factor - Use a passwordless method, such as a push notification or a one-time passcode (OTP), as an additional authentication factor beyond a password. This is also referred to as a second-factor or multi-factor authentication.
- 2 Passwordless Experience - Remove the password from the user experience and perform any password-based authentication securely in the background.
- 3 Complete Passwordless - Eliminate the need for passwords completely by authenticating users using passwordless factors or private-key cryptography.

Organizations desire to be in a complete passwordless state, however, in some cases this is not feasible or may require a phased-approach.

For organizations that want to implement a complete passwordless state, this may not be possible or may require a phased approach. For example, you may need to provide a second factor of authentication for users when they log in to their workstation to increase your security posture. This allows you to start the journey to passwordless using Enterprise Connect.

Another example could be that your legacy systems require passwords for authentication, or they cannot accommodate the new technologies/protocols a complete passwordless state needs. In this scenario, opting for the passwordless experience is what you need. This rotates passwords securely in the background, without the user needing to know their password. Implementing this option improves the user experience while also increasing the overall security of your organization. This allows you to continue on the journey of passwordless using Enterprise Connect Passwordless.

Should you use Enterprise Connect or Enterprise Connect Passwordless?

Enterprise Connect and Enterprise Connect Passwordless both offer solutions to move towards passwordless. Which solution you choose will depend on the needs and state of your organization.

Refer to the following table to assist you with your decision.

Copyright © 2025 Ping Identity Corporation

Product	Passwordless Factor	Passwordless Experience	Complete Passwordless	Description
Enterprise Connect	✓ Yes	✕ No	✕ No	Enterprise Connect improves security and provides: • A passwordless factor for: ◦ Windows ◦ Mac ◦ Linux workstations ◦ Servers • A Windows RADIUS proxy to use with RADIUS clients, such as Linux, VPNs, or databases • Faster deployment cycle than Enterprise Connect Passwordless • Less infrastructure than Enterprise Connect Passwordless • Desktop single-sign on (SSO) to Ping portal upon success authentication
Enterprise Connect Passwordless	✓ Yes	✓ Yes	✓ Yes	Enterprise Connect Passwordless improves user experience, security and: • Brings together Ping's web-based capabilities by leveraging its infrastructure • Uses servers to remove passwords from the user experience, securely managing passwords for the users in the background. This delivers a true passwordless experience to your users. • Helps achieve passwordless for managed devices in your organization including: ◦ LDAP ◦ Windows ◦ Mac ◦ Linux ◦ Servers ◦ VPNs and databases ◦ Legacy applications • Provides a built-in RADIUS server • More robust than Enterprise Connect • Desktop SSO to Ping portal upon successful authentication • Additional authentication factors such as FIDO2 and certificate-based authentication

Copyright © 2025 Ping Identity Corporation

Enterprise Connect

Enterprise Connect

Windows Workstation Authentication

What's new

3.7.2.7293

New features

- OATH Multi-language support: Adds support for setting alternate text for the default message in the `OathTokenVerifierNode.properties` file for Self Managed deployments of PingAM 7.3 software or later.

  Refer to line 42 below:

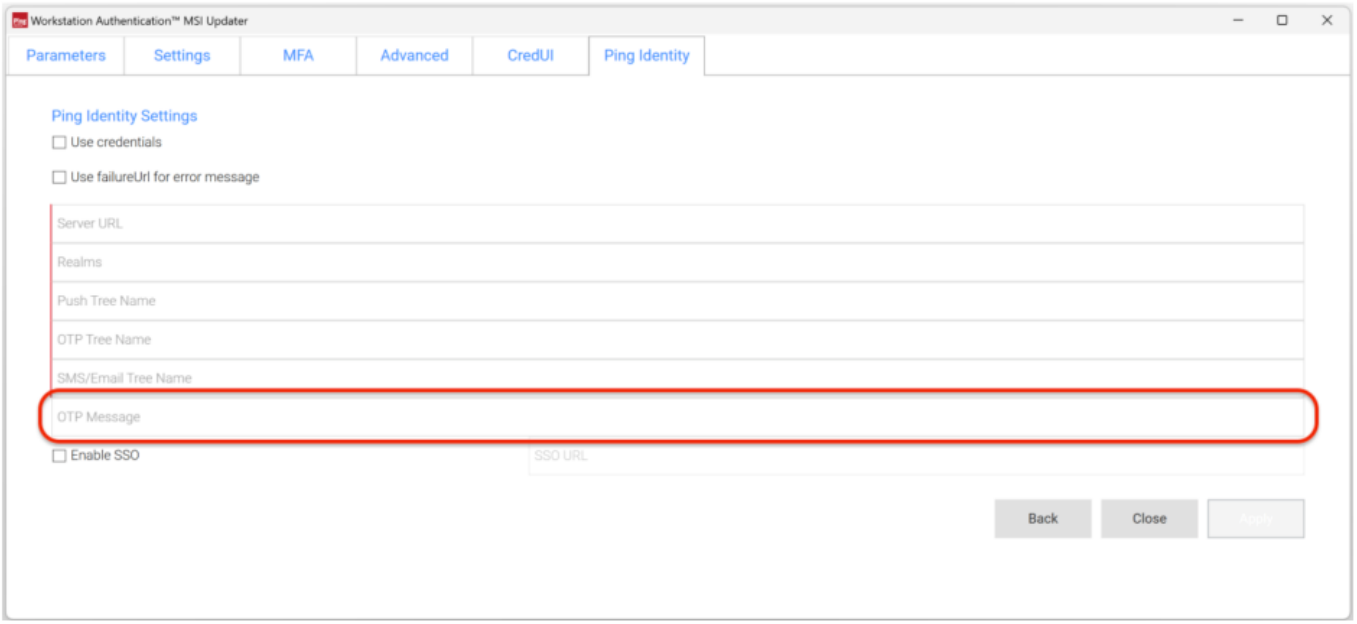
```
 9 nodeDescription=OATH Token Verifier
10 nodeHelp=Collects and verify the One-Time Password code provided by the user.
11
12 successOutcome=Success
13 failureOutcome=Failure
14 notRegisteredOutcome=Not registered
15 recoveryCodeOutcome=Recovery Code
16
17 algorithm=OATH Algorithm
18 algorithm.hep=Choose the algorithm your device uses to generate the OTP. HOTP uses a counter value that is incremented
   \
19   every time a new OTP is generated. TOTP generates a new OTP every few seconds as specified by the time step interval.
20 totpTimeInterval=TOTP Time Step Interval
21 totpTimeInterval.help=This is the time interval that one OTP is valid for. For example, if the time step \
22   is 30 seconds, then a new OTP will be generated every 30 seconds. This makes a single OTP valid for only 30 seconds.
23 maximumAllowedClockDrift=TOTP Maximum Allowed Clock Drift
24 maximumAllowedClockDrift.help=Number of time steps a client is allowed to get out of sync with the server before manual
    \
25   resynchronization is required. For example, with 3 allowed drifts and a time step interval of 30 seconds the server \
26   will allow codes from up to 90 seconds from the current time to be treated as the current time step. The drift for \
27   a user's device is calculated each time they enter a new code. If the drift exceeds this value, the user's \
28   authentication code will be rejected.
29 totpTimeSteps=TOTP Time Steps
30 totpTimeSteps.help=This is the number of time step intervals to check the received OTP against both forward in time \
31   and back in time. For example, with 1 time step and a time step interval of 30 seconds the server will allow a code \
32   between the previous code, the current code and the next code.
33 totpHashAlgorithm=TOTP Hash Algorithm
34 totpHashAlgorithm.help=The Hmac hash algorithm to be used on generating the OTP codes.
35 hotpWindowSize=HOTP Window Size
36 hotpWindowSize.help=This sets the window that the OTP device and the server counter can be out of sync. For example, \
37   if the window size is 100 and the servers last successful login was at counter value 2, then the server will accept \
38   a OTP from the OTP device that is from device counter 3 to 102.
39 isRecoveryCodeAllowed=Allow recovery codes
40 isRecoveryCodeAllowed.help=Allow users to use one of the recovery codes to proceed with the login.
41
42 default.message=Verifizierungscode eingeben
43 default.submit=Absenden
44 default.recoveryCodes=Benutze Wiederherstellungscodes
45
46 passwordLength.SIX_DIGITS=6
47 passwordLength.EIGHT_DIGITS=8
48
49 totpHashAlgorithm.HMAC_SHA1=HMAC-SHA1
50 totpHashAlgorithm.HMAC_SHA256=HMAC-SHA256
51 totpHashAlgorithm.HMAC_SHA512=HMAC-SHA512
```

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> Modifying the `OathTokenVerifierNode.properties` file as-is is beyond the scope of this document. Follow the steps below to change the `default.message` field.

Steps

1. Follow the steps in Windows client installation with MSI Updater to configure the MSI Updater.
2. On the Workstation Authentication MSI Updater, click the Ping Identity tab. Add the non-default value set for `default.message` in the `OathTokenVerifierNode.properties` file and change it to the `OTP Message` field. Click the **Apply** button when done.



> **Note**
>
> Modifying the `` `OathTokenVerifierNode.properties `` file as-is is beyond the scope of this document.

3. If users are enrolled in the Enterprise Connect Offline OTP, upgrade the existing Enterprise Connect client installation. Follow the steps in Perform MSI upgrade.

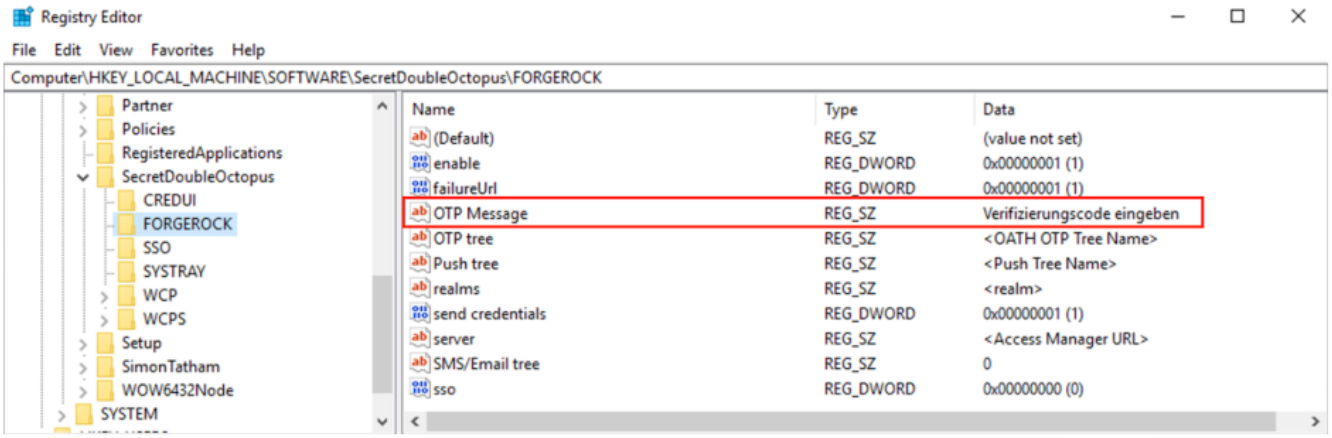
> **Note**
>
> If your deployment is not using Enterprise Connect Offline OTP, you can uninstall the current Enterprise Connect client and install the MSI you created in the previous step.

4. Validate the installation of the new Enterprise Connect client with the non-default OTP Message validate using the following registry key:

   HKEY_LOCAL_MACHINE\SOFTWARE\SecretDoubleOctopus\Ping Identity

Copyright © 2025 Ping Identity Corporation

5. Validate that the `OTP Message = <custom default message>`:



6. Validate that users with an enrolled Authenticator App OATH OTP can authenticate to the workstations with the new Enterprise Connect client deployment.

3.7.2.7291

- Initial release of Mac Workstation Authentication, which provides protection for your Windows endpoints by requiring multi-factor authentication on login.

Fixes

3.7.2.7293

There are no fixes because this is this release of Windows Workstation Authentication.

3.7.2.7291

There are no fixes because this is the initial release of Windows Workstation Authentication.

Doc updates

In addition to the changes described elsewhere in these notes, the published documentation for this version includes the following important changes.

Date	Description
January 2025	Updated Windows Workstation Authentication 3.7.2.7293 with Ping Identity branding.
September 2022	• Updated the Windows Workstation Authentication version 3.7.2 to 3.7.2.7291 with Ping Identity. • Initial release of Windows Workstation Authentication 3.7.2.

Copyright © 2025 Ping Identity Corporation

Windows RADIUS proxy

What's new

3.0.2

Initial release of Windows RADIUS proxy, which brings the capability for a remote authentication dial-up service (RADIUS) proxy to be installed on a Windows machine via the RADIUS protocol. Updated branding and screenshots.

Learn more in Windows RADIUS proxy.

2.7.1

Initial release of Windows RADIUS proxy, which brings the capability for a remote authentication dial-up service (RADIUS) proxy to be installed on a Windows machine via the RADIUS protocol.

Fixes

3.0.2

There are no fixes because this is the initial release of Windows RADIUS proxy.

2.7.1

There are no fixes because this is the initial release of Windows RADIUS proxy.

Doc updates

In addition to the changes described elsewhere in these notes, the published documentation for this version includes the following important changes.

Date	Description
January 2025	Release of Windows RADIUS proxy 3.0.2
September 2022	Release of Windows RADIUS proxy 2.7.1.

Mac Workstation Authentication

Copyright © 2025 Ping Identity Corporation

What's new

3.0.3

Initial release of Mac Workstation Authentication which provides protection for your Mac endpoints by requiring MFA on login. Updated branding and screenshots.

Learn more in Mac Workstation Authentication.

2.7.2

> **Note**
>
> Version 3.7.2 was an incorrect version number. The actual version was 2.7.2.

Initial release of Mac Workstation Authentication 2.7.2 which provides protection for your Mac endpoints by requiring MFA on login. Updated branding and screenshots.

Fixes

3.0.3

There are no fixes because this is the initial release of Mac Workstation Authentication.

Doc updates

In addition to the changes described elsewhere in these notes, the published documentation for this version includes the following important changes.

Date	Description
January 2025	Release of Mac Workstation Authentication 3.0.3
April 2023	Release of Mac Workstation Authentication 2.7.2.

Copyright © 2025 Ping Identity Corporation

Enterprise Connect Passwordless

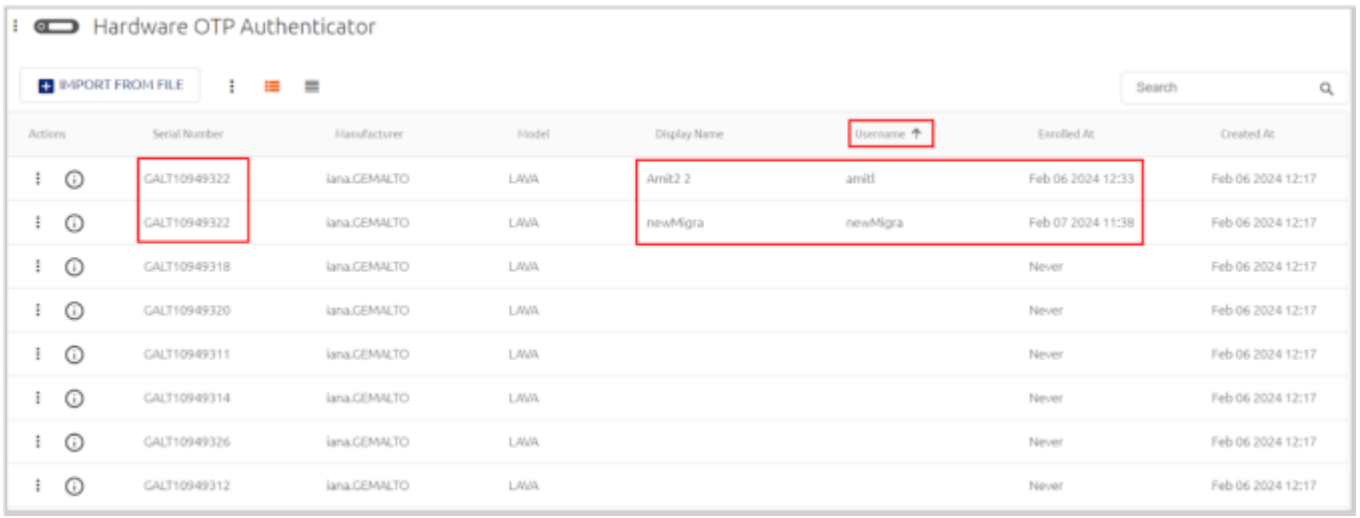
Servers

What's new

5.8.2

> **Important**
>
> Enterprise Connect Passwordless 5.8.2 introduces multiple features that further enhance security while maintaining a seamless user experience. As some of these features require the latest Agent versions, we strongly recommend to use the following:
>
> - Enterprise Connect Passwordless Windows Agent 3.9.3
> - Enterprise Connect Passwordless Mac Agent 2.7.1
> - Latest version of the Authenticator mobile app

- **Hardware OTP token bulk operations [SSA-13659]**: Administrative operations (e.g., deleting tokens) can now be performed on multiple tokens simultaneously. Selection options include several tokens on a page of the Hardware OTP Authenticator list, all tokens on a page, or all tokens on the list.
- **Multiple users per HW token [SSA-13889]**: To accommodate users who have more than one AD account, Enterprise Connect Passwordless Server now supports enrollment of multiple users with a single hardware OTP token.



- **HW OTP support for RADIUS login [SSA-13930]**: Hardware OTP tokens can now be used as a means of authentication to RADIUS services.

Copyright © 2025 Ping Identity Corporation

- **Nginx server security enhancements [SSA-13235] [SSA-12938]**: Enterprise Connect Passwordless Server version 5.8.2 supports use of optional enhanced security settings for the Nginx server. After installing the server, you can enforce these settings by simply uncommenting the relevant lines in the following files:
    - /etc/nginx/conf.d/sdomon.conf
    - /etc/nginx/conf.d/sdomcbe.conf

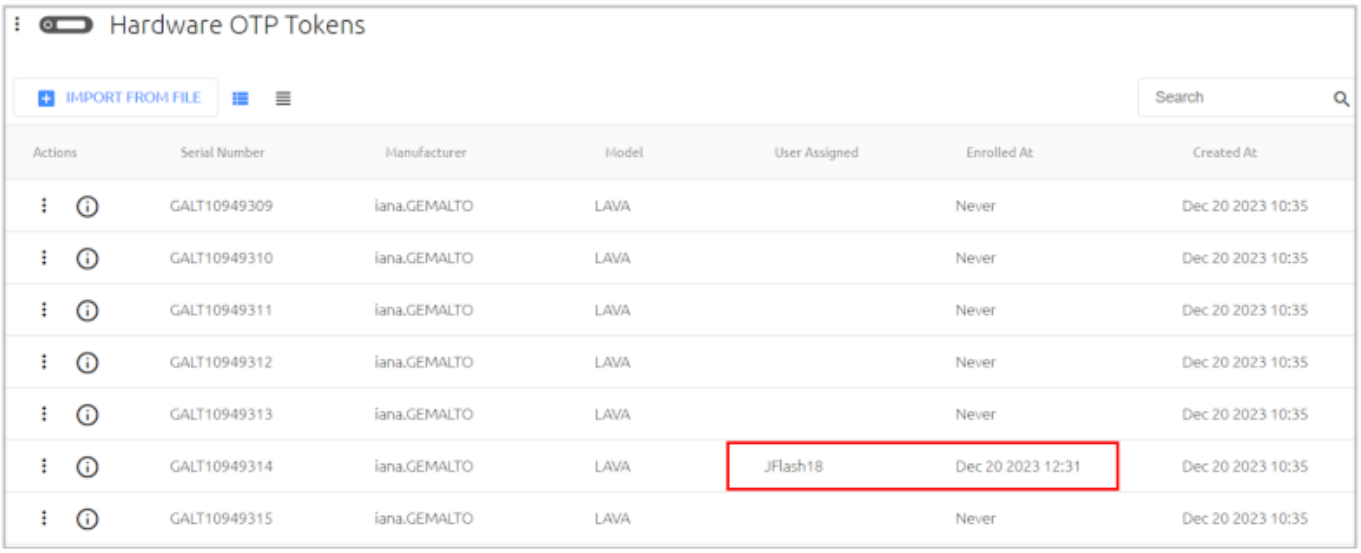
    To enable stronger cipher suites, uncomment this line:

    ```
    # ssl_ciphers "ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-CHACHA20-
    POLY1305:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA
    -AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384";
    ```

- **Shared user accounts** [SSA-12370]: Designated users can now log into a generic account on a shared workstation using their personal credentials and devices. This feature facilitates smooth login while enhancing authentication security for specific groups of personnel (such as IT, DevOps, manufacturing floor workers, etc.) who use shared workstations.

  New checkboxes in the Settings tab of the MSIUpdater client allow the admin to enable support of shared accounts and control whether the Windows Login screen will allow switching between shared account login and standard account login. Shared account support also requires some configuration in the Enterprise Connect Passwordless Server. For more information, please refer to the ECP Windows Agent.

- **Hardware OTP token support** [SSA-13179]: Enterprise Connect Passwordless Server now supports use of HW OTP tokens for login to Windows and the User Portal, in online and/or offline mode. New functionality in the Management Console enables the system admin to easily import lists of supported tokens, and users then enroll using their unique device.



  Like other authenticators, support of HW OTP token authentication is specified in the settings of integrated directories. For more information, please refer to the Enterprise Connect Passwordless Server Guide.

- **Strong authentication per service** [SSA-13514]: Global settings for Adaptive Authentication (which requires an extra layer of security for initial logins from unrecognized devices) can now be overridden for specific services in the new Devices tab of the service settings. Adaptive Authentication can be enabled / disable for a service, or individual settings within the mechanism (such as length of verification code) can be changed as required.

Copyright © 2025 Ping Identity Corporation

- **Legacy mode support per ADPA service** [SSA-12880]: The global setting for Legacy Workstation Agent support (enabled or disabled) can now be overridden for individual Active Directory Authentication services. Legacy workstations are those running versions below Windows Agent 3.3 and Mac Agent 2.3.0.
- **List paging and scrolling enhancements** [SSA-13230]: New paging and navigation features in many menus of the Enterprise Connect Passwordless Server Console enable the admin to choose the number of items displayed on a page (10, 20, 50 or 100) and to immediately navigate to any page of the list by selecting the relevant page. Note: These features are not yet implemented for the Manage Users menu.

- **Enhanced Database Server support** [SSA-13232]: Enterprise Connect Passwordless Server version 5.8 supports PostgreSQL 15.
- **Option for controlling upgrade of external components** [SSA-13714]: The Enterprise Connect Passwordless Server installation file now supports an optional parameter to prevent upgrade of various external components during the installation process, including the Nginx web server, the Redis server and the Node.js runtime environment.

  To implement the parameter:

  1. Add the -s switch followed by the relevant comma-separated keywords: `nginx`, `redis`, `node`.
  2. Make sure to use the following required syntax:
     - -s must be preceded by a double dash
     - There must be no spaces in the comma-separated list

     For example:

     ```
     ./octopus-el7-5.8-b0062.run – -s nginx,node
     ```

- **Option for disabling auto-search** [SSA-13405]: To reduce load on the database, a new parameter in the `production.json` file can now be set to disable autocomplete when searching for users in the Enterprise Connect Passwordless Server Console.

  To implement this option:

  1. Change the value of the autoSearchEnabled parameter from `true` to `false`:

     ```
     "autoSearchEnabled": false
     ```

  2. Then, restart the service.

In addition, the following additional security-related headers are provided:

- **Content Security Policy**: Helps protect your site from XSS attacks by whitelisting sources of approved content.
- **Referrer Policy**: Allows your site to control how much information the browser sends to destination servers with navigations away from a document.

Copyright © 2025 Ping Identity Corporation

- **Permissions Policy**: Allows your site to control which features and APIs can be used in the browser.

To use these headers, uncomment the following lines:

```
# add_header Content-Security-Policy "default-src 'self'; script-src 'self'
'unsafe-inline'; style-src 'self' 'unsafe-inline'; img-src 'self' data:";
# add_header Referrer-Policy 'origin';
# add_header Permissions-Policy
geolocation=(),midi=(),microphone=(),camera=(),magnetometer=(),gyroscope=(),
fullscreen=(self),payment=()";
```

- **Alternative ACS URL parameter**: A new custom parameter for generic SAML services, `altAcsUrl`, enables you to route SAML requests originating from a mobile device to a dedicated ACS URL. When the parameter is set, the user-agent header of the request is checked. If a mobile user-agent is detected, the `altAcsUrl` value is used instead of the ACS URL defined in the service settings.

5.4.8

> **Important**
>
> Enterprise Connect Passwordless 5.4.8 provides features that enhance security and we recommended that you install the latest following agents versions for compatibility:
>
> - Enterprise Connect Passwordless Windows Agent 3.8.4
> - Enterprise Connect Passwordless Mac Agent 2.6.7

Workstation limit per user

You can now define a limit on the number of workstations an end user can authenticate from. Once the end user reaches the limit, authentication to other workstations fails. To accommodate users who need access to many workstations, the **Override Workstation Limit** setting in a user's details (Security tab) enables you to specify a limit for each user.

DMZ delegation support

You can now Enable Authentication Servers in the DMZ to communicate directly with a server within the network.

Reporting authenticator plugin

You can enable a third-party authenticator to be the designated reporting authenticator. The third-party authenticator receives workstation authentication event logs so you can view the log reports in a third-party platform.

To enable third-party event reporting, you must specify the reporting authenticator in the **Authentication** tab of the directory settings.

Management Console minimum password length support

For on-prem deployments, you can now define the minimum number of characters required for local user passwords to access the management console. You specify the value in a new parameter in the configuration file.

Copyright © 2025 Ping Identity Corporation

Automatic password sync

A new setting enables users to authenticate using the mobile app even when the AD password has changed. When the agent detects a mismatch, the Octopus Authentication Server sends a password reset request, and the user must approve the authentication request to log in successfully. Enable this setting in the Management Console under corporate directory settings.

5.4.4

Initial release of Enterprise Connect Passwordless Servers that provides instructions on how to install the Authentication and Management Console servers and configure the Management Console.

For more information, refer to Install Enterprise Connect Passwordless Servers and Configure the management console.

Requirements

The Enterprise Connect Passwordless Servers software is available at https://backstage.forgerock.com.

5.8.2

Operating systems

The following operating systems support Enterprise Connect Passwordless Servers:

Operating system	Version
Red Hat Enterprise Linux (RHEL)	8.2 - 8.8
Oracle Linux	8.3 - 8.7
Rocky Linux	8.4 - 8.8

5.4.8

Operating systems

The following operating systems support Enterprise Connect Passwordless Servers:

Operating system	Version
Red Hat Enterprise Linux (RHEL)	8.2 - 8.8
Oracle Linux	8.3 - 8.7
Rocky Linux	8.4 - 8.8

Copyright © 2025 Ping Identity Corporation

Supported PingAM versions

While PingOne Advanced Identity Cloud supports Enterprise Connect Passwordless, only specific versions of the self-managed PingAM are compatible.

PingAM	7.x.x

Compatible versions

The following agent versions are compatible with the Enterprise Connect Passwordless Servers:

Product	Versions
Enterprise Connect Passwordless Windows Agent	3.8.2, 3.8.4
Enterprise Connect Passwordless Mac Agent	2.6.7

Fixes

5.8.2

There are no fixes because this is the initial release of Ping Enterprise Connect Passwordless.

5.4.8

- SSA-11986: Login failures when working with many machine types, such as Windows and Macs
- SSA-11972: Nginx pool size and database connection issues
- SSA-11537: Ping journey session not captured during authentication flow

5.4.4

There are no fixes because this is the initial release of Ping Enterprise Connect Passwordless.

Doc updates

In addition to the changes described in these notes, the published documentation for this version includes the following important changes.

Date	Description
April 2024	Release of Enterprise Connect Passwordless Servers 5.8.2.
September 2023	Release of Enterprise Connect Passwordless Servers 5.4.8.

Copyright © 2025 Ping Identity Corporation

Date	Description
May 2023	Release of Enterprise Connect Passwordless Servers 5.4.4.

Windows agent

What's new

3.9.3

> **Important**
>
> - Enterprise Connect Passwordless Windows Agent version 3.9.3 is intended for use with **Enterprise Connect Passwordless Server version 5.8.2 (and higher)** only.
> - Enterprise Connect Passwordless Windows Agent version 3.9.3 does not support Windows 7 or Windows 8.1 (32/64 bit).

New features in 3.9.3

Enterprise Connect Passwordless Windows Agent version 3.9.3 introduces the following features:

- [SSA-12370] **Shared user accounts** – Designated users can now log into a generic account on a shared workstation using their personal credentials and devices. This feature facilitates smooth login while enhancing authentication security for specific groups of personnel (such as IT, DevOps, manufacturing floor workers, etc.) who use shared workstations.

  New checkboxes in the **Settings** tab of the MSIUpdater client allow the admin to enable support of shared accounts and control whether the Windows Login screen will allow switching between shared account login and standard account login. Shared account support also requires some configuration in the Enterprise Connect Passwordless Server. For more information, please refer to the Enterprise Connect Passwordless Windows Agent Installation Guide.

- [SSA-12771] **Retrieval of temporary login token with certificate** – A new systray setting enables users to retrieve the temporary token required for RADIUS login after performing authentication using a smart card signed by the organization's root CA. The token expires after 60 seconds.

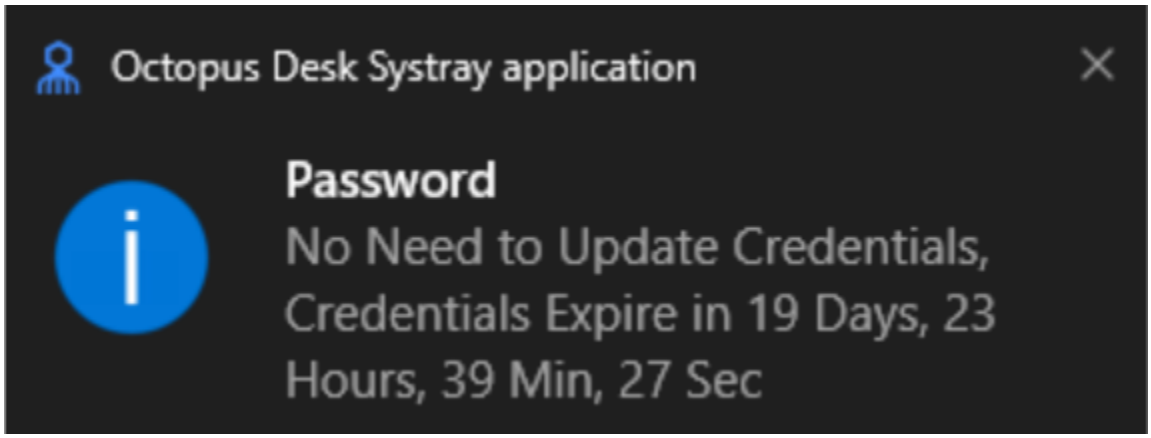
- **[SSA-13141] Dynamic web proxy support** – Enterprise Connect Passwordless Windows Agent now supports both static and dynamic web proxy. Proxy type is determined according to the syntax of the Proxy EndPoint URL in the MSIUpdater. For more information, please refer to the Enterprise Connect Passwordless Windows Agent Installation Guide.

- **[SSA-13819] Credentials retrieval with HW OTP tokens** – A new systray option allows users to view and copy the AD password after performing authentication using a hardware OTP token. To enable this option, the OTP authenticator in the Parameters tab of the MSIUpdater must be selected.

  > **Important**
  >
  > This feature is supported for Enterprise Connect Passwordless Server **version 5.8.2 (and higher)** only.

Copyright © 2025 Ping Identity Corporation

- **Hardware OTP offline authentication** – Enterprise Connect Passwordless Windows Agent now supports hardware OTP tokens as a means of authentication for offline login. To enable this feature, Offline OTP with PIN protection needs to be configured in the Enterprise Connect Passwordless Server, and the Windows workstations must have TPM support.
- **[SSA-13855] Credentials retrieval with HW OTP tokens** – A new systray option allows users to view and copy the AD password after performing authentication using a hardware OTP token. To enable this option, the OTP authenticator in the Parameters tab of the MSIUpdater must be selected.
- **[SSA-13927] Enhanced credential status data** – The Check Credential Status systray option now provides detailed password expiration information.

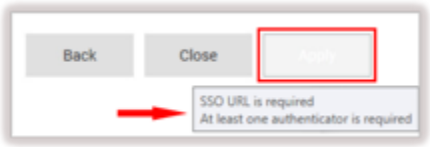


3.8.4

> **Important**
>
> Enterprise Connect Passwordless Windows Agent 3.8.4 is only compatible with Enterprise Connect Passwordless Server 5.4.8 or above.
> Using older versions of Enterprise Connect Passwordless Server is not recommended and requires the selection of the **Legacy Server Support** checkbox in the MSIUpdater client.

Missing mandatory parameters list

If one or more mandatory settings are missing from the MSIUpdater client, a list of the missing settings now displays in a tooltip when hovering over the disabled **Apply** button.



User defined log file location

A new setting in the MSIUpdater client enables changing the default location of the log files to a user specified directory.

Hide BLE authentication option

When Octopus BLE is selected as an authenticator in the MSIUpdater client, you can now choose to show or hide this authentication mechanism in the Windows credential provider's login method selection list.

Copyright © 2025 Ping Identity Corporation

3.8.2

Initial release of Enterprise Connect Passwordless Windows Agent that provides instructions on how to install and deploy the Enterprise Connect Passwordless Windows Agent (ECP Windows Agent).

For more information, refer to the ECP Windows Agent 3.8.2 guide.

Fixes

3.9.3

- SSA-12158: In certain circumstances, the SSO portal launches in a browser with maximum user privileges
- SSA-12709: When performing RDP authentication, Network Login Type is logged as Interactive Login Type
- SSA-12400: Smart card authentication failure following an offline reboot
- SSA-13408: Incorrect text for shared account login on first interaction
- SSA-13446: Authentication failures related to FIDO PIN length
- SSA-13948: Systray app not executed automatically following MSI installation

3.8.4

- SSA-11445: When you enable **Enforce Adaptive Authentication**, offline login with BLE succeeds only after two online logins

3.8.2

There are no fixes as this is the initial release of Enterprise Connect Passwordless Windows Agent.

Doc updates

In addition to the changes described in these notes, the published documentation for this version includes the following important changes.

Date	Description
April 2024	Release of Enterprise Connect Passwordless Windows Agent 3.9.3.
September 2023	Release of Enterprise Connect Passwordless Windows Agent 3.8.4.
May 2023	Release of Enterprise Connect Passwordless Windows Agent 3.8.2.

Mac agent

Copyright © 2025 Ping Identity Corporation

What's new

2.7.1

> **Important**
>
> - Enterprise Connect Passwordless Mac Agent version 2.7.1 is intended for use with Enterprise Connect Passwordless Server version 5.6 (and higher) only. Working with older versions of the Enterprise Connect Passwordless Server is unadvised.
> - When upgrading from previous versions, make sure you log out of the user account when the installation finishes. You may then immediately log back in using your preferred authentication method.

2.6.7

> **Important**
>
> Enterprise Connect Passwordless Mac Agent 2.6.7 is only compatible with Enterprise Connect Passwordless Server 5.4.8 or above.

Authentication widget support

The authentication widget now supports shutdown and logoff password prompts when another user is logged in.

Enhanced uninstallation process

To remove the Mac agent from their machine when uninstalling,, users are now prompted to perform FileVault teardown.

Fixes

2.7.1

- SSA-13862: FIDO authentication setup fails when users are enabled with FIDO as the first and only authenticator

2.6.7

- SSA-11701: Agent conflict with CyberArk EPM Agent
- SSA-12259: FileVault set up fails for a second user on the same machine
- SSA-11915: FileVault password operation fails in rare instances

Copyright © 2025 Ping Identity Corporation

Known issues

Enterprise Connect Passwordless Mac Agent version 2.7.1 contains the following known issues, which will be fixed in coming versions:

- **Refresh User Profile doesn't work for Local users**: This option, in the Security tab of the user details in the Management Console, doesn't work properly on the Mac. Clicking Refresh User Profile deletes the password history and the correct local password won't be successfully retrieved to the Mac. Mac users are advised not to use this option.
- **Jamf policy issues**: In some cases when Jamf is installed on the Mac, Enterprise Connect Passwordless Mac Agent is unable to sync the password. Users might need to disable Jamf password policies in order to resolve this issue.
- **sudo for Bypass users**: A password is currently required for users in Bypass mode to run sudo.
- **Password sync failure related to multiple user accounts**: Passwords do not automatically update when there is switching between accounts. Users need to lock and unlock the machine to initiate the password sync.
- **Misleading Kerberos error message**: When Kerberos does not connect to the server because of login failure, the message displayed to users mistakenly states that the Kerberos ticket is expired.
- **Automatic password sync**: The automatic password sync feature works only on the latest MacOS (Sonoma). Users of previous MacOS versions will receive the sync password popup screen.
- **Password Free Experience**: If authentication is rejected by the Server when enabling Enterprise Connect Passwordless, users receive confirmation that the process has succeeded, although they will be unable to login.

Operating system support

Enterprise Connect Passwordless Mac Agent version 2.7.1 supports the following operating systems:

- macOS Sonoma
- macOS Monterey
- macOS Ventura

Doc updates

In addition to the changes described in these notes, the published documentation for this version includes the following important changes.

Date	Description
April 2024	Release of Enterprise Connect Passwordless Mac Agent 2.7.1.
September 2023	Release of Enterprise Connect Passwordless Mac Agent 2.6.7.

Copyright © 2025 Ping Identity Corporation

Getting support

Ping provides support services, professional services, training through Ping University, and partner services to assist you in setting up and maintaining your deployments. You can find a general overview of these services in Ping website.

Ping has staff members around the globe who support our international customers and partners. For details on Ping's support offering, including support plans and service level agreements (SLAs), visit Ping support.

Ping publishes comprehensive documentation online:

- The Ping Knowledge Base offers a large and increasing number of up-to-date, practical articles that help you deploy and manage Ping software.

  While many articles are visible to community members, Ping customers have access to much more, including advanced information for customers using Ping software in a mission-critical capacity.

- Ping product documentation, such as this document, aims to be technically accurate and complete with respect to the software documented. It's visible to everyone and covers all product features and examples of how to use them.

Copyright © 2025 Ping Identity Corporation

Enterprise Connect overview

Add-on

Ping Enterprise Connect is an add-on capability available for purchase for PingOne Advanced Identity Cloud and self-managed versions of PingAM. Contact your Ping representative for more details on how this capability can enhance your organization's security posture.

Note

You can find more information about concepts and high-level information in passwordless overview.

Enterprise Connect provides a rich multi-factor authentication (MFA) to modern enterprises via:

- **Windows Workstation MFA**: Protects your endpoints by enforcing MFA on Windows workstations.
- **Windows Remote desktop MFA**: Protects your virtual Windows machines through MFA.
- **Windows Desktop SSO**: Allows end users to be signed in to the Ping environment automatically after logging into Windows.
- **Windows RADIUS proxy MFA**: Protects your organization's tools, such as your organization's VPN, via the Windows RADIUS proxy.
- **Mac Workstation MFA**: Protects your endpoints by enforcing MFA on Mac workstations.

Deploy the installation files relevant to the feature that is desired along with connecting into PingOne Advanced Identity Cloud or PingAM to access these capabilities.

Windows Workstation Authentication

Configure MFA for Windows workstations via an MSI package and configured journeys.

Windows RADIUS proxy

Configure the Windows RADIUS proxy for rich MFA via an installation and configured journeys.

Copyright © 2025 Ping Identity Corporation

Mac Workstation Authentication

Configure MFA for Mac workstations.

Supported PingAM versions

While Enterprise Connect is fully supported in PingOne Advanced Identity Cloud, only specific versions of the self-managed PingAM are compatible.

Table 1: PingAM supported versions

PingAM	7.x.x

Copyright © 2025 Ping Identity Corporation

Windows Workstation Authentication

Windows Workstation Authentication provides your organization with the capability to secure Windows workstations or servers with rich multi-factor authentication (MFA) either via SMS/email/voice call or push/one-time passcode (OTP) notifications through the ForgeRock Authenticator application.

Benefits of Windows Workstation Authentication:

- Provides the fastest and safest way to close the desktop security gap. The first desktop MFA solution to integrate fully with the Ping directory and ForgeRock Authenticator application.
- Offers unprecedented endpoint security using the familiar Ping Authenticator. The solution offers end users the best MFA experience while relieving IT teams from the expensive and cumbersome deployment of OTP tokens and security keys to protect workstations.
- A plug-and-play solution that is easy to install on employee endpoints. No dedicated server is required, enabling fast deployment for the entire workforce. Your organization can now dramatically boost their domain security, improve user experience, and take the first step toward becoming fully passwordless in the future.

> **Note**
>
> To support MFA (push or OATH OTP) in Windows Workstation Authentication, end users must download the ForgeRock Authenticator application to their smartphone via the Apple store or Google Play store.

Windows Workstation Authentication installation/configuration checklist

Download and install the binaries from Backstage (you must be logged in). This includes the base MSI file as well as the MSI Updater client.

- ☐ Pre-configure the relevant journey(s).
- ☐ Install the MSI Updater client on an administrative Windows machine.
- ☐ Configure the MSI Updater client specific to your organization's needs.
- ☐ (Optional) Consider additional configurations.
- ☐ Deploy the generated MSI file through your desired mechanism.
- ☐ Verify and test your deployment.

Prerequisites

Before beginning installation, verify that:

- Workstations support **TPM version 2.0**.
- You decide if the Windows workstation will be domain-joined or standalone. Windows Workstation Authentication supports both.

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> Ensure all usernames (profiles/accounts) match from *Windows (or the authoritative source)* > *Ping* and vice versa. Set up a connector from Ping to the datastore (for example, AD) and sync the data.
> Credentials entered are always verified against the local Windows machine (or AD if configured). You can configure the credentials (via the **Use credentials** setting) to be validated against Ping as well.

- End users install the ForgeRock Authenticator application.
- Establish connectivity between the Ping environment and the end user's Windows workstations.

> **Note**
>
> Communication with the Ping environment is crucial for Windows Workstation Authentication to function properly. Adjust your network settings appropriately.

- Pre-configure journeys and services, as described in Create authentication journey(s).
  - End users must pre-register in the appropriate journey, if the push MFA method is an option the organization desires.

    > **Important**
    >
    > It is crucial for users to pre-register for push notifications, otherwise, this authentication method will not work on Windows login.

  - For HOTP journeys using out-of-band (OOB) channels, such as SMS, email, or voice call, the user profile in Ping **must** have their phone number and email populated accordingly.

Supported environments

Windows Workstation Authentication can only be installed on the following operating systems:

- Windows 10
- Windows 11
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

> **Important**
>
> Windows 8.1 and Windows Server 2012 are not supported.

Create authentication journey(s)

To enable workstation authentication integration, you need to create relevant journeys to support the MFA authentication method(s) you want. These journeys allow workstation authentication to work directly with the Ping environment.

Copyright © 2025 Ping Identity Corporation

Since Enterprise Connect integrates with PingOne Advanced Identity Cloud or self-managed PingAM, the examples that follow depict the various UI changes between the two.

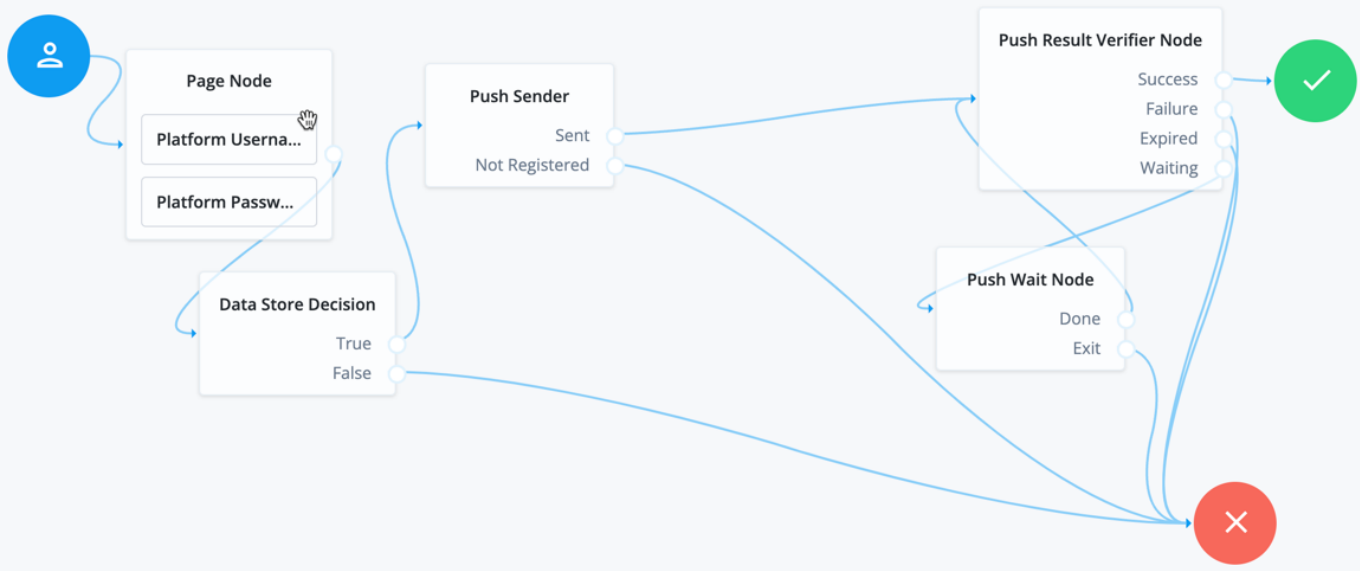
Important

Do not deviate from the following journeys when you configure Enterprise Connect or use the journeys you create for any other purpose (including repurposing the journeys). You must strictly follow the placement of the nodes to ensure the product works correctly.
Failure to do so or the addition of other nodes could result in unexpected behavior.

Example of push journey

The push journeys for Enterprise Connect allow users to approve a push notification from the ForgeRock Authenticator application. End users must download the ForgeRock Authenticator application and pre-register (from another journey you define) to be able to use the push journeys.

PingOne Advanced Identity Cloud



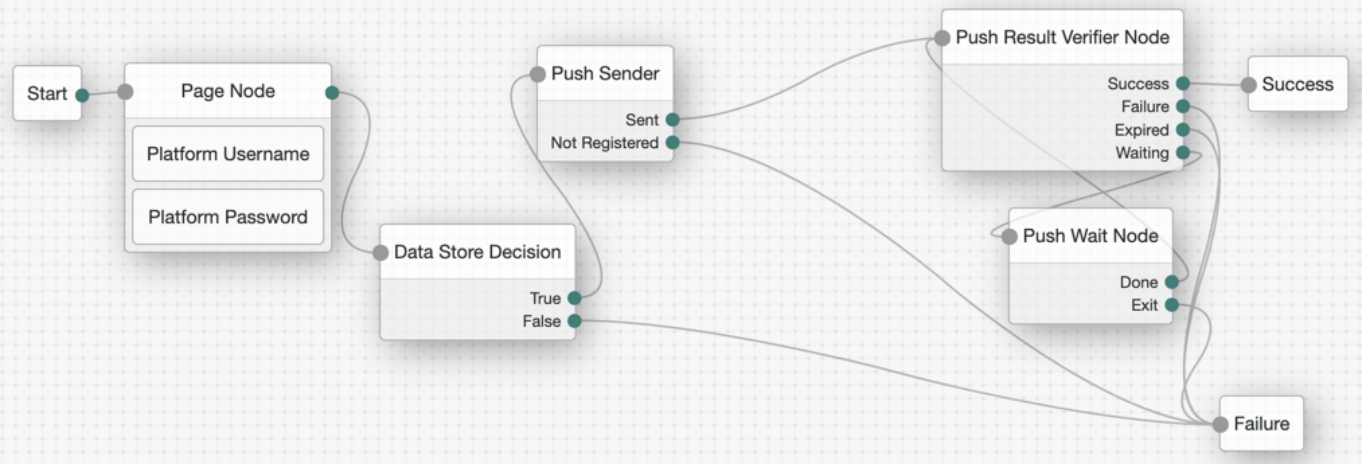
If you configure **Use credentials** in the MSI Updater client, then you must include the *Platform Password* and *Data Store Decision* nodes. Otherwise, you must omit these nodes in your journey configuration.

Note

When configuring the push journey in PingOne Advanced Identity Cloud, you must enable services in the AM admin UI (native console). For more information, refer to Create a push authentication journey.

Copyright © 2025 Ping Identity Corporation

PingAM



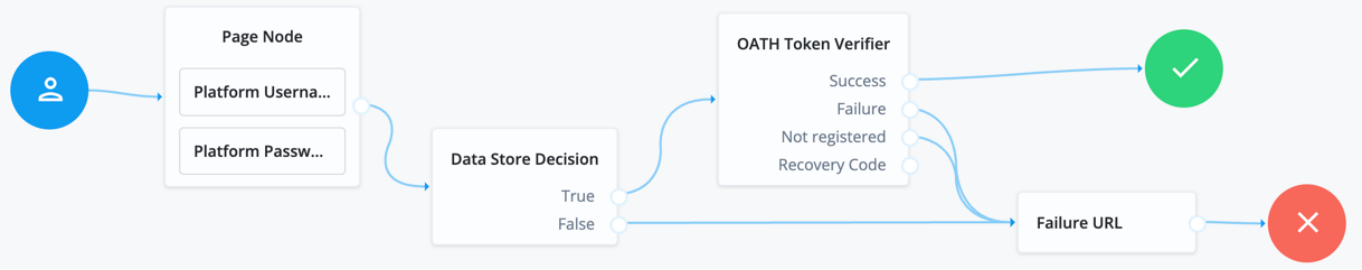
If you configure **Use credentials** in the MSI Updater client, then you must include the *Platform Password* and *Data Store Decision* nodes. Otherwise, you must omit these nodes in your journey configuration.

> **Note**
>
> When configuring the push journey in PingAM, you must enable services in the AM admin UI (self managed). For more information, refer to Create a push authentication journey.

Example of OTP from authenticator app journey

The following journeys show the OTP that is presented from the ForgeRock Authenticator application. End users must download the ForgeRock Authenticator application and pre-register (from another journey you define) to be able to use the OTP journeys.

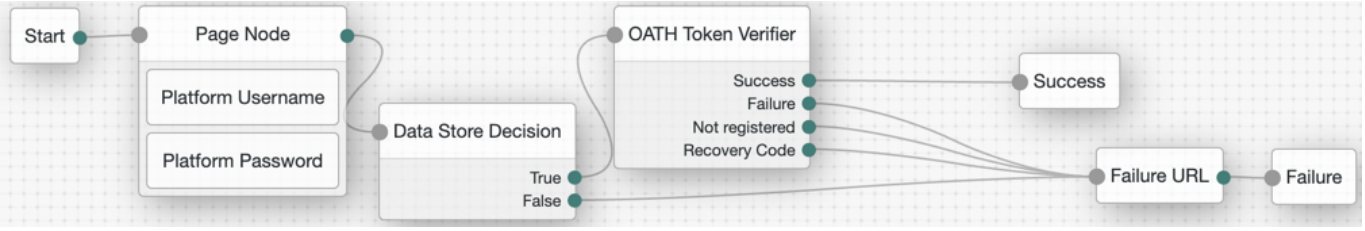
PingOne Advanced Identity Cloud



If you configure **Use credentials** in the MSI Updater client, then you must include the *Platform Password* and *Data Store Decision* nodes. Otherwise, you must omit these nodes in your journey configuration.

Copyright © 2025 Ping Identity Corporation

PingAM

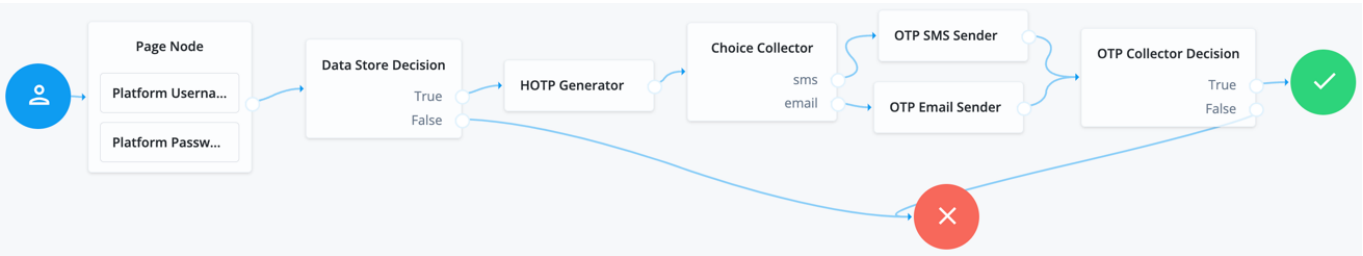


If you configure **Use credentials** in the MSI Updater client, then you must include the *Platform Password* and *Data Store Decision* nodes. Otherwise, you must omit these nodes in your journey configuration.

Example of OTP SMS/email/voice call journey

The following journeys show the OATH OTP (HOTP) that can be presented to an end user via SMS/email/voice. Ensure end users have the appropriate data in their user profile to facilitate the MFA method(s) you allow an end user to select.

PingOne Advanced Identity Cloud



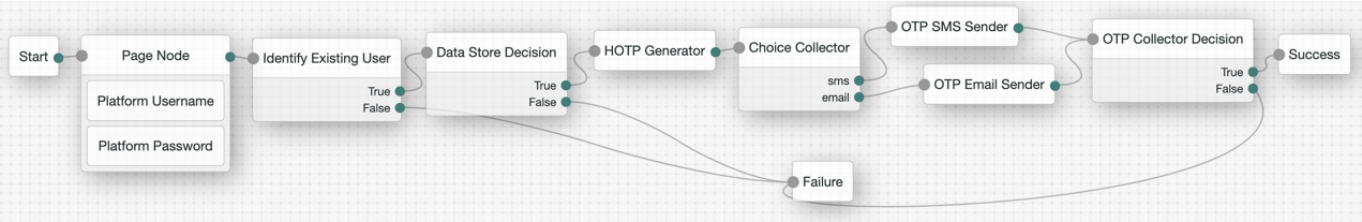
If you configure **Use credentials** in the MSI Updater client, then you must include the *Platform Password* and *Data Store Decision* nodes. Otherwise, you must omit these nodes in your journey configuration.

> **Important**
>
> In the **Choice Collector** node, the options correlate to the following MFA methods within Windows Workstation Authentication:
>
> 1. SMS
> 2. Email
> 3. Voice
>
> Therefore, ensure SMS is the first choice in the node, followed by email. If voice call is a method you configure, it must be the third option.
> Do not deviate from this order.

If you choose to use the *voice* option, you could use the Twilio nodes (you must have a valid subscription with Twilio).

Copyright © 2025 Ping Identity Corporation

PingAM



If you configure **Use credentials** in the MSI Updater client, then you must include the *Platform Password* and *Data Store Decision* nodes. Otherwise, you must omit these nodes in your journey configuration.

> **Important**
>
> In the **Choice Collector** node, the options correlate to the following MFA methods within Windows Workstation Authentication:
>
> 1. SMS
> 2. Email
> 3. Voice
>
> Therefore, ensure SMS is the first choice in the node, followed by email. If voice call is a method you configure, it must be the third option.
> Do not deviate from this order.

If you choose to use the *voice* option, you could use the Twilio nodes (you must have a valid subscription with Twilio).

Example of SSO journey

The following journeys depict the flow that Enterprise Connect uses after a user authenticates to their workstation. The end user Ping environment opens in a default browser.

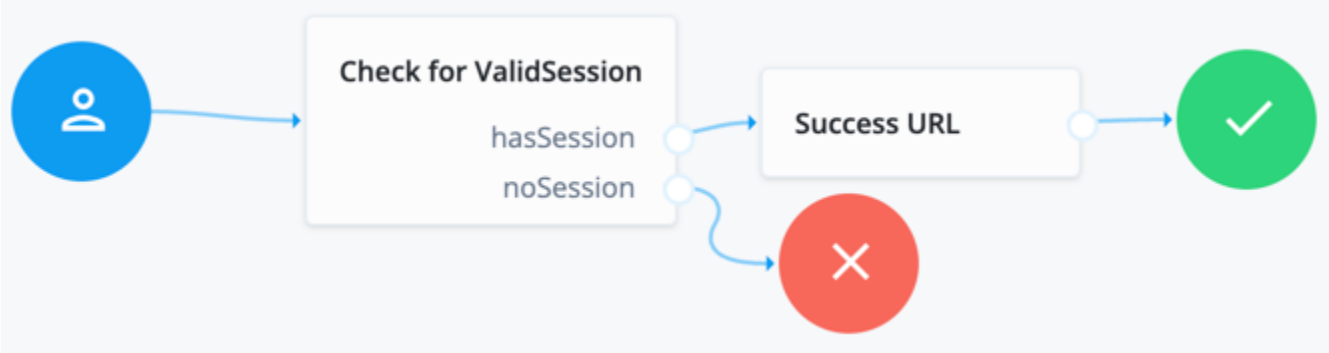
If you configure the Enable SSO setting in the MSI Updater client, then this journey applies to you. In this setting, you must supply the journey URL.

An example SSO URL to enter in this field is `https://<tenant-env-fqdn>/am/XUI/?realm=alpha&authIndexType=service&authIndexValue=sso-journey&ForceAuth=true`.

> **Important**
>
> The `authIndexValue` references the journey to use for SSO. Ensure to add `ForceAuth=true` to the end of your SSO URL.

Copyright © 2025 Ping Identity Corporation

PingOne Advanced Identity Cloud



The **Check for ValidSession** node (shown in the image above) is the **Scripted Decision** node. In this example, it references a simple authentication JavaScript script:

```
if (typeof existingSession !== 'undefined')
{
  outcome = "hasSession";
}
else
{
  outcome = "noSession";
}
```

PingAM

The **Check for ValidSession** node (shown in the image above) is the **Scripted Decision** node. In this example, it references a simple authentication JavaScript script:

```
if (typeof existingSession !== 'undefined')
{
  outcome = "hasSession";
}
else
{
  outcome = "noSession";
}
```

Copyright © 2025 Ping Identity Corporation

Windows Workstation Authentication installation/configuration checklist

Download and install the binaries from Backstage (you must be logged in). This includes the base MSI file as well as the MSI Updater client.

Pre-configure the relevant journey(s).

- ☐ Install the MSI Updater client on an administrative Windows machine.
- ☐ Configure the MSI Updater client specific to your organization's needs.
- ☐ (Optional) Consider additional configurations.
- ☐ Deploy the generated MSI file through your desired mechanism.
- ☐ Verify and test your deployment.

Windows client installation with MSI Updater

To add MFA functionality to Windows Workstation Authentication, complete the following steps:

1. Install the MSI Updater client for workstation authentication from Backstage.

> **Note**
>
> A Backstage account is required to log in and download the file.

2. Configure the MSI Updater client to produce a deployment specific MSI file.
3. Deploy the specific outputted MSI file to workstations/servers.

Install the MSI Updater client for workstation authentication

The MSI Updater client provides a tool for a basic MSI with specific customizable parameters to support different use cases. This enables MSI silent installation to Windows clients.

The output of the MSI Updater client is an MSI package, which is to be installed on workstations. A base MSI file is referenced by the MSI Updater client to output the **customized MSI package** for your organization.

Before beginning, verify that you meet all prerequisites.

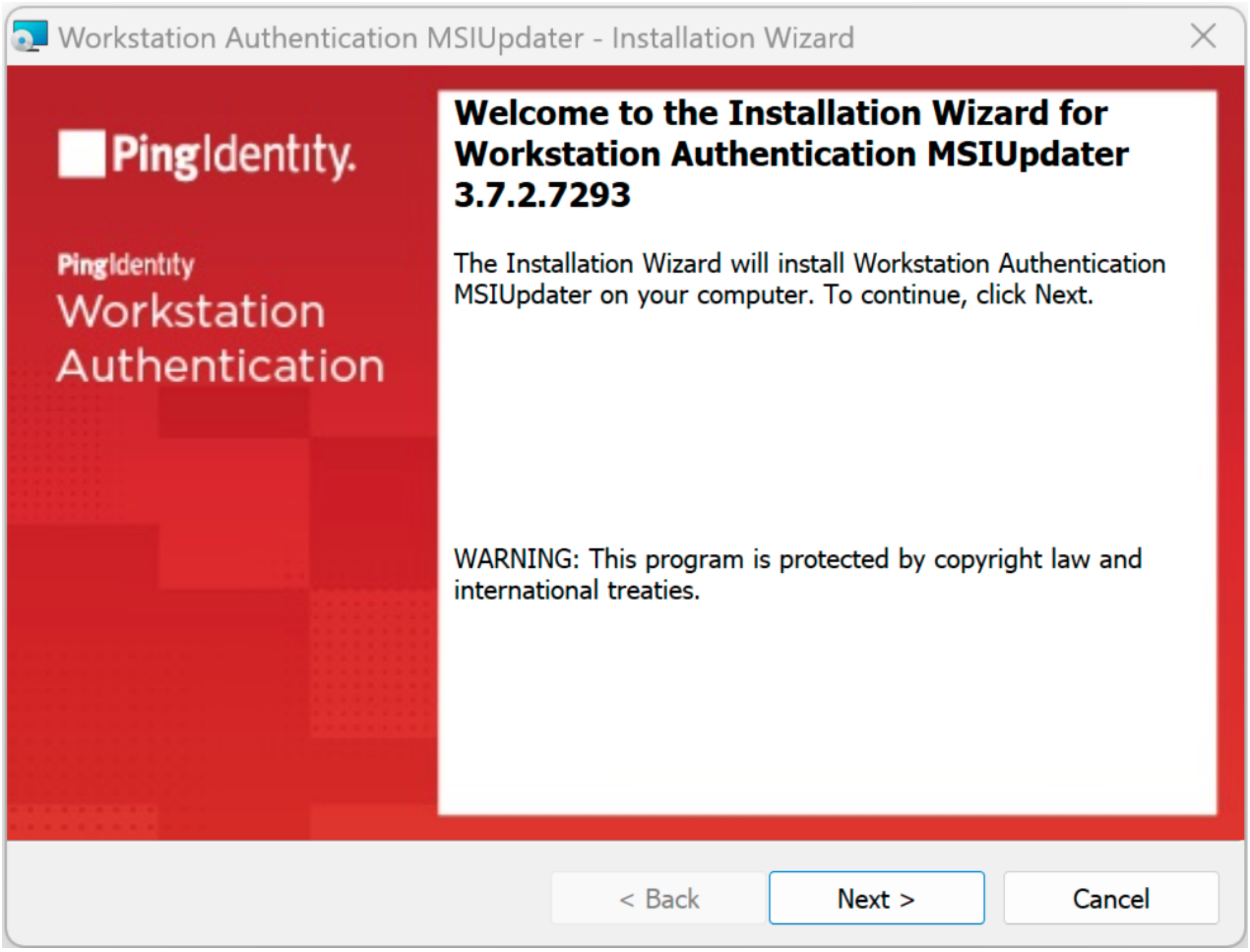
Install the MSI Updater client:

1. Download the MSI Updater client and base MSI file binaries from Backstage.

> **Note**
>
> You must have a Backstage account and be logged in to view the download.

2. Run Workstation Authentication MSI Updater - *version*.exe as an administrator.
3. On the **Welcome** page, click **Next**.

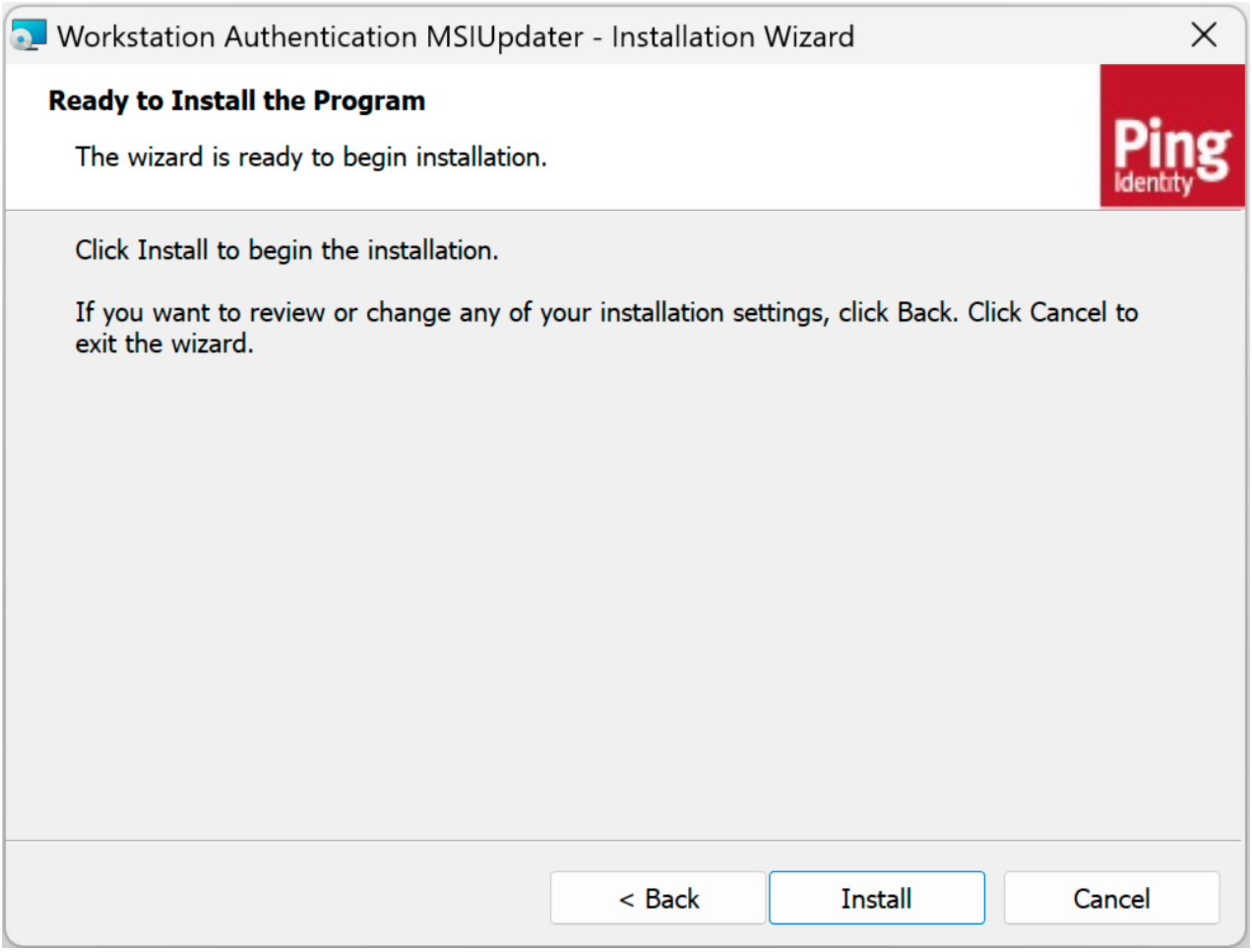
Copyright © 2025 Ping Identity Corporation



1. On the page that opens, accept the license agreement, and then click **Next**.

2. To start installation, click **Install**.

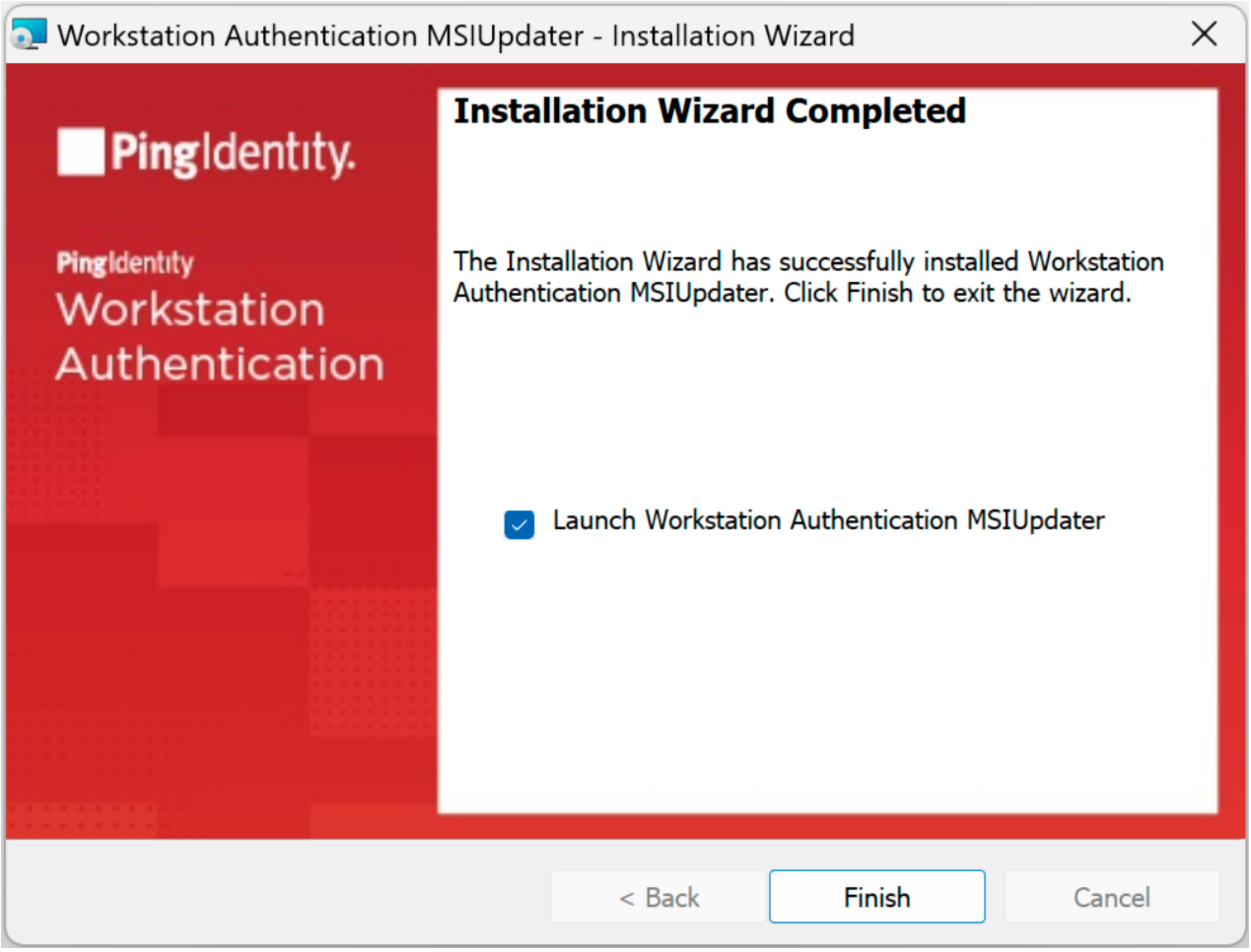
Copyright © 2025 Ping Identity Corporation



The window displays a progress message during the installation process. After completion, a confirmation message displays.

1. To exit the wizard, click **Finish**. If you would like for the MSI Updater client to *auto-launch* tick the **Launch Workstation Authenticator MSI Updater** box.

Copyright © 2025 Ping Identity Corporation



When installation is complete, the next step is to configure the MSI Updater client.

Windows Workstation Authentication installation/configuration checklist

Download and install the binaries from Backstage (you must be logged in). This includes the base MSI file as well as the MSI Updater client.

Pre-configure the relevant journey(s).

Install the MSI Updater client on an administrative Windows machine.

- ☐ Configure the MSI Updater client specific to your organization's needs.
- ☐ (Optional) Consider additional configurations.
- ☐ Deploy the generated MSI file through your desired mechanism.
- ☐ Verify and test your deployment.

Configure the MSI Updater client

The MSI Updater client can launch automatically (if the option is selected at the last installation screen) after you exit the installer and updates the Windows Workstation Authentication MSI with relevant Ping environment details. You can then configure various settings related to authentication and the Windows login experience.

Copyright © 2025 Ping Identity Corporation

Before you begin working with the MSI Updater, verify the following information is available:

- **Server URL:** Environment URL for the Ping environment.
- **Realm:** The realm in Ping that corresponds to where the journeys reside.
- **Push journey name:** Name of the journey for push notifications. For more information on the journey, refer to Example of push journey.
- **OTP journey Name:** Name of the journey for TOTPs (OATH). For more information on the journey, refer to Example of OTP journey.
- **SMS/email/voice journey name:** Name of the journey for SMS/email/voice. For more information on the journey, refer to Example of SMS/email journey.
- **SSO URL (optional):** Ping SSO URL. If enabled and supplied, on successful login to the Windows machine, the default browser opens a logged-in session into the specified Ping environment.
    - With this URL, an additional journey can be referenced. For example, to check for an existing session. For more information, refer to Example of SSO journey.

MSI Updater client tab overview

Tab name	Description
Parameters	Select the base MSI file to update, as well as which MFA methods to allow on Windows login.
Settings	Configure various settings, such as caching the last used username to pre-populate on next login or enabling trace logs by default.
MFA	Enable MFA settings, such as allowing a Windows group to bypass MFA login or enabling Offline OTP (TOTP/OATH).
Advanced	Change the UI text of the MFA method(s) that users select on Windows login.
CredUI	Select scenarios in which you can bypass MFA on Windows login.
Ping	Ping specific settings, such as the Ping URL or the names of the journeys that correspond to each MFA method.

To begin the configurations, launch the MSI Updater client as an **administrator**.

To configure the MSI Updater client:

In the **Parameters** tab, configure the relevant settings:

1. With the MSI Updater client launched, at the top of the **Parameters** tab, click **Browse** and upload the workstation authentication MSI file to be updated. This is the base MSI file that came with the downloads.
2. If preferred, enter an uninstall password in the **Uninstall** field.

Copyright © 2025 Ping Identity Corporation

> **Note**
> Entering an uninstall password ensures end users cannot uninstall the MSI package without the administrator password.

3. Select one or more of the following authentication options:

Authenticator	Description
Ping Push	Select this checkbox to enable login to Windows using Ping's push notification authentication. This is used in conjunction with the ForgeRock Authenticator application.
OTP	Select this checkbox to enable authentication with TOTP (OATH). This corresponds to the journey used for TOTP (OATH). This is also referred to as Offline OTP. This is used in conjunction with the ForgeRock Authenticator application.
SMS	Select this checkbox to enable authentication with OTP via SMS. This corresponds to the journey used for OTP over SMS.
Email	Select this checkbox to enable authentication with OTP via email. This corresponds to the journey used for OTP via email.
Voice Call	Select this checkbox to enable a two-factor authentication voice call. This corresponds to the journey used for OTP via a voice call.

> **Note**
> SMS, email, and voice call all utilize the same journey configuration.

4. Click **Next** to open the **Settings** tab.

1. In the **Settings** tab, configure the relevant settings:

> **Note**
> The MSI Updater version appears at the top of the tab.

Setting	Description
Show Default Credential Providers	Determines whether Windows default credential providers (Windows and Active Directory) are displayed when logging into Windows. ⚠ **Warning** Select this option for testing or debugging. **Do not** use this in production (the MSI deployed on your end user's workstation).
Use Last Username	When selected, the username of the user who logged in most recently is saved and automatically presented for the next login.

Copyright © 2025 Ping Identity Corporation

Setting	Description
TPM Support	If TPM 2.0 is enabled, selecting this option allows TPM to store the private key for BLE password encryption.
Local User Support	When selected, workstation authentication for Windows will be enabled for local users and will verify that the local user matches with the corresponding user in Ping. **Note** This setting is relevant for non-domain users only.
POC Mode	When selected, workstation authentication for Windows will not check the certificate with the server. This setting is used mainly for POC.
Azure AD Joined Machine	Select this checkbox when the workstations are configured to connect with the Azure AD domain. When the setting is selected, users will be prompted to log in with UPN and not their username.
Enable Trace	Select this checkbox to enable the logs by default immediately after installation. For more information on Windows Workstation Authentication logging, refer to Log files with Windows Workstation Authentication.

1. Click **Next**.

1. In the **MFA** tab, configure the relevant settings:

Setting	Description
MFA Change Password Support	When selected, users are able to change the password on the Windows workstation without the Workstation Authentication credential provider (CP) intercepting the process. When the checkbox is cleared, the workstation authentication CP controls the password change process.
Bypass Local User Login	When selected, administrators with a local user account can bypass workstation authentication and log in with their username and password.
Use Offline OTP	When selected, users are able to log into Windows using a one time password that is stored locally. When Offline OTP is activated, a list of OTPs is securely stored on the Windows workstation to allow users to authenticate to the workstation when not connected to the network. The OTPs are timed-based and use the standard TOTP mechanism. For more information, refer to Offline OTP enrollment.
Force Offline OTP After Installation	When selected, users are unable to perform offline authentication until they complete at least one online login successfully.

Copyright © 2025 Ping Identity Corporation

Setting	Description
Bypass MFA on Unlock when Connected to AD	When selected, users connected to the organization network who have already authenticated with MFA are not required to authenticate with 2nd factor again when unlocking the workstation. This will work as long as you are inside the network (no time limit). **Important** When selecting this option, verify that the **Bypass MFA Groups** checkbox is **NOT** selected.
Force Lock After Offline OTP	When selected, workstations that were unlocked using an Offline OTP and then connected back to the organization network (online) are automatically locked, and the user is asked to authenticate. This setting prevents users from using weak authentication to log into the organization network (online).
Bypass MFA from NLA Login	When selected, users who are members of the Bypass MFA Group will not require MFA authentication when using a Network Level Authentication (NLA) login.
Bypass MFA Groups	When selected, you can specify ONE group in the AD that will not require MFA authentication. Enter *<Domain>\>Group Name>* in the field to the right. **Important** When selecting this option, verify that the **Bypass MFA on Unlock when Connected to AD** checkbox is **NOT** selected.
Offline OTP Buffer Period	If **Use Offline OTP** is selected, enter the maximum period of time (in days) that users will be able to continue authenticating offline without performing an online login. Once expired, users will be forced to authenticate online before being able to use the **Offline OTP** option again.

1. Click **Next**.

1. In the **Advanced** tab, configure the relevant settings:

Setting	Description
Change OTP Name	Allows you to change the default name of the TOTP (OATH or Offline OTP) displayed in the Windows credential provider's login authentication method selection list. After selecting the checkbox, enter the desired name in the field (for example, *ForgeRock OTP*). This setting is available only when the **OTP** checkbox in the **Parameters** tab is selected.
Change Ping Push Name	Allows you to change the default name of the authenticator displayed in the Windows credential provider's login authentication method selection list. After selecting the checkbox, enter the desired name in the field. This setting is available only when the **Ping Push** checkbox in the **Parameters** tab is selected.

Copyright © 2025 Ping Identity Corporation

Setting	Description
Change SMS Name	Allows you to change the default name of the SMS option displayed in the Windows credential provider's login authentication method selection list. After selecting the checkbox, enter the desired name in the field.
Change Email Name	Allows you to change the default name of the Email option displayed in the Windows credential provider's login authentication method selection list. After selecting the checkbox, enter the desired name in the field.
Change Voice Call Name	Allows you to change the default name of the Voice Call option displayed in the Windows credential provider's login authentication method selection list. After selecting the checkbox, enter the desired name in the field.
Enable CP Bypass List	Allows you to specify credential providers (in addition to Ping) that will be available for Windows login. After selecting the checkbox, paste the registry key(s) representing the relevant credential provider(s) in the field to the right. The specified providers will be displayed as login options on the Windows Login screen.

1. If desired, customize the Windows login experience by replacing the default organization logo with your own image.

> **Important**
>
> The images must be 448x448 in 24-bit BMP (bitmap image file) format. For Windows Servers, the images must be 448x448 in 16-bit BMP format.

2. Click **Next**.

1. In the **CredUI** tab, select the scenarios in which an additional MFA credential, for example, push or OTP, will **not** be required. When a Bypass is selected, the default Windows login screen is presented and end users authenticate by entering their username and password.

   Selecting **Bypass All** activates MFA bypass for all the scenarios listed below in the tab.

2. Click **Next**.

1. In the **Ping** tab, configure the relevant settings:

Setting	Description
Use credentials	When selected, user credentials are sent to Ping for validation. You must configure the journey to support the validation of the user credentials.
Use failureUrl for error message	When selected, error descriptions are displayed on the Windows Login screen (in the event of error/authentication failure). This means that your journey, in the event of a failure, must reference the Failure URL node.
Server URL	Enter the URL of your Ping authentication server. For example, `https://<tenant-env-fqdn>/openam`. Ensure to include the path to AM in the URL.

Copyright © 2025 Ping Identity Corporation

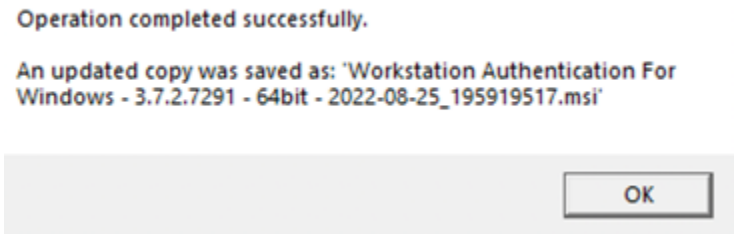
Setting	Description
Realms	Enter the name of the Ping realm to authenticate to. For example, `alpha`. **Note** There is no leading `/` when defining the realm for Windows Workstation Authentication.
Push Tree Name	Enter the name of the push journey. For example, `windows-push`.
OTP Tree Name	Enter the name of the OTP journey. For example, `windows-otp`.
SMS/Email Tree Name	Enter the name of the SMS/email/voice call journey. For example, `windows-sms-email-voice`.
Enable SSO	When selected, the SSO Portal opens automatically upon successful login to Windows. This will open, in the default browser on the Windows machine, a logged in instance to the specified Ping environment. Enter the **SSO URL** in the field to the right. If this box is selected, the URL box becomes available for editing. This is also known as a transfer of trust. An example SSO URL to enter in this box is `https://<tenant-env-fqdn>/am/XUI/?realm=alpha&authIndexType=service&authIndexValue=sso-journey&ForceAuth=true`. **Important** The `authIndexValue` references the journey to use for SSO. Ensure to add `ForceAuth=true` to the end of your SSO URL.

Note

For examples of the pre-configured journeys to have in your environment, refer to Create authentication journey(s).

1. At the bottom of the **Ping** tab, click **Apply**.

   A confirmation screen will appear.



A new modified MSI file is created in the same location as the original MSI file. The name of the new file will include Workstation Authentication for Windows 64-bit and the timestamp of file creation.

Copyright © 2025 Ping Identity Corporation

> **Caution**
>
> The base (original) MSI file will not be updated and can be reused. **Do not use** the base MSI file for deployment. Use the deployment specific MSI file generated as the output of the MSI Updater configurations.

Windows Workstation Authentication installation/configuration checklist

Download and install the binaries from Backstage (you must be logged in). This includes the base MSI file as well as the MSI Updater client.

Pre-configure the relevant journey(s).

Install the MSI Updater client on an administrative Windows machine.

Configure the MSI Updater client specific to your organization's needs.

- ☐ (Optional) Consider additional configurations.
- ☐ Deploy the generated MSI file through your desired mechanism.
- ☐ Verify and test your deployment.

MSI deployment of Windows Workstation Authentication

Once the MSI package is generated post the MSI Updater client, it is ready to be deployed to your end user's workstations.

The three options for deployment are:

1. Through a silent installation. This installation type should be used for **organizational** and other **large-scale deployments**.
2. Through the Installation Wizard.
3. Through your preferred distribution tool.

> **Note**
>
> The MSI package to be used is generated from the MSI Updater client, as described in Configure the MSI Updater client. The following sections will reference a `WorkstationAuthentication.msi` file. Substitute those references with your outputted file.

Perform silent installation

Silent installation allows administrators to manually install workstation authentication or push the installation to all client workstations from a central tool silently without disturbing the end user's workstation.

This is the **preferred** method for organizational and other large-scale deployments.

Before performing installation with software distribution tools, make sure the Visual C++ 2017 (or later) Redistributable (x64)/(x86) - 14.30.30704.0 is installed. If this package is not installed, the installation will abort and an error message will be displayed.

> **Note**
>
> Administrator permissions are required to run the workstation authentication for Windows MSI.

Copyright © 2025 Ping Identity Corporation

To perform silent installation:

1. **Open the command prompt as an administrator**, and run `workstation authentication.msi`.
2. Run `Workstation Authentication.msi`:

```
C:\>msiexec -i Workstation Authentication – xx_xxx_xx.msi /qn
```

3. If you want the workstation authentication credential provider to be disabled on some workstations after installation (allowing for gradual deployment), refer to Enable/disable the workstation authentication CP post-installation.

Perform deployment using the Installation Wizard

This method deploys the MSI package using the workstation authentication installation wizard. All required components (including the Visual C++ Redistributable) are automatically installed as part of the deployment.

> **Note**
>
> This deployment option must be run directly from the end user's workstation.

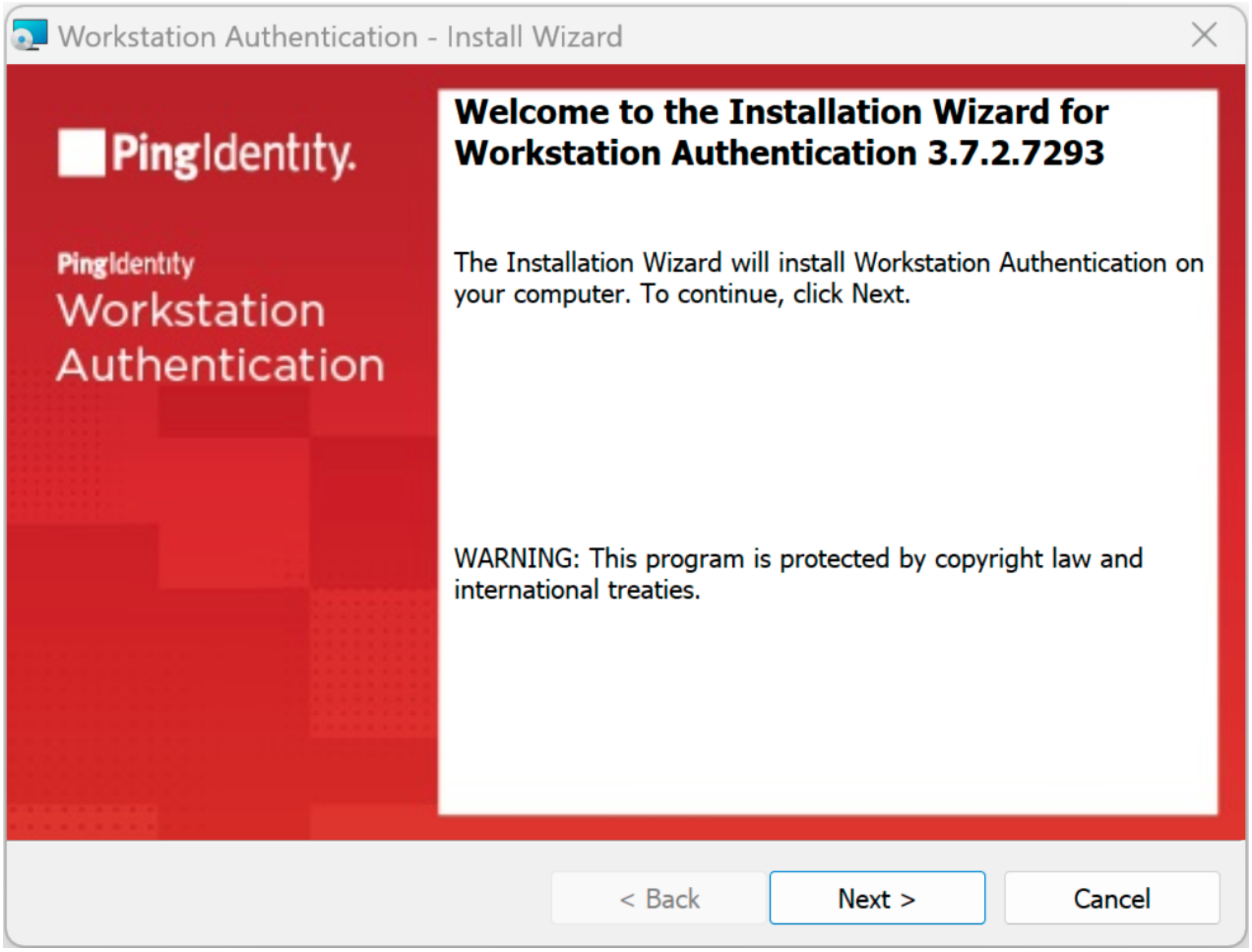
To deploy workstation authentication using the installation wizard:

1. To launch the wizard, run the updated workstation authentication MSI file. This is the outputted file from the MSI Updater client, as described in configuring-windows-msiupdater.adoc#configure_the_msiupdater_client.

   > **Note**
   >
   > A warning screen from *Windows Defender* can pop up stating "*Windows Protected your PC*". Click **More Info** > **Run anyway** to continue to run the MSI file.

2. On the Welcome page, click **Next**.

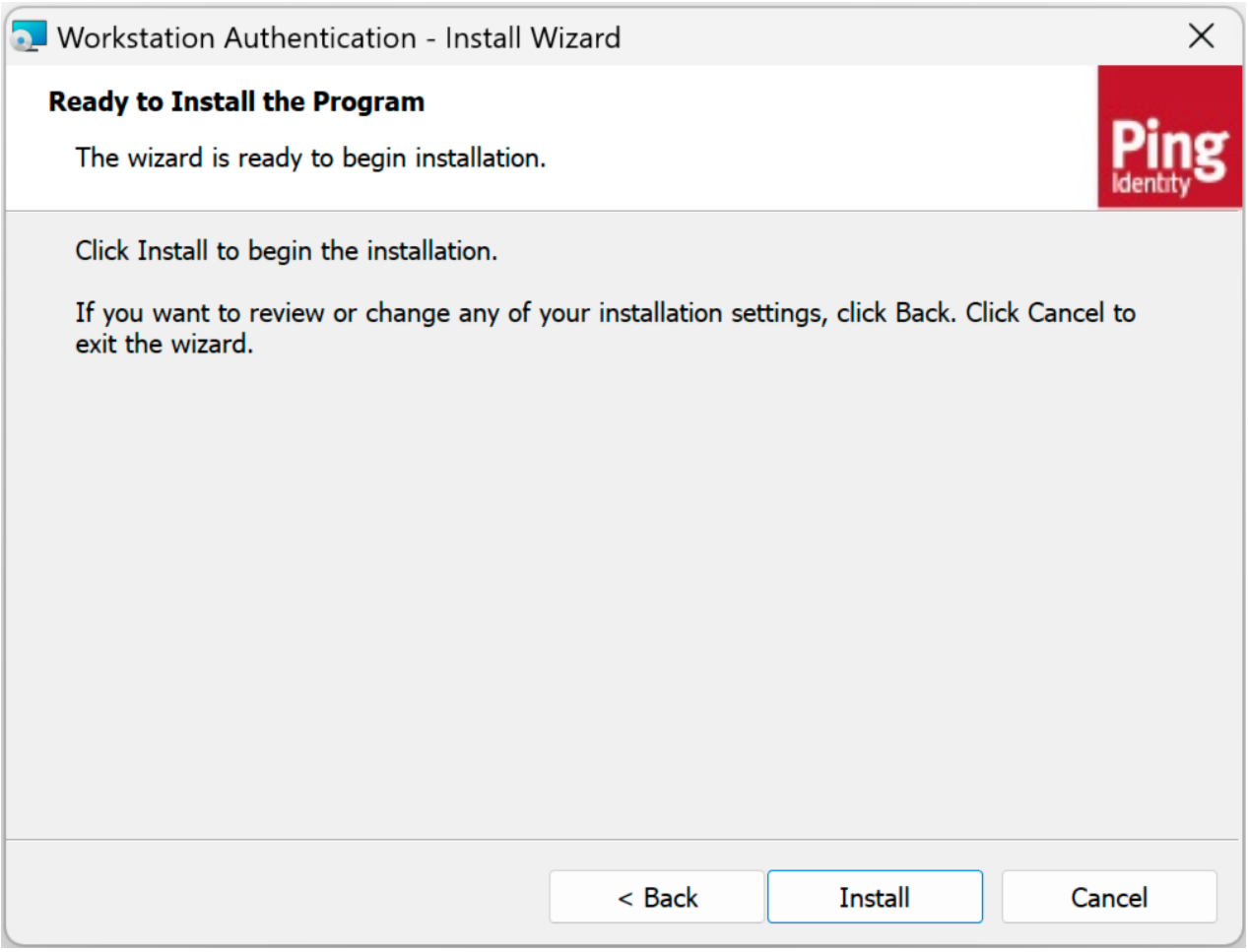
Copyright © 2025 Ping Identity Corporation



3. On the page that opens, accept the license agreement, and then click **Next**.

4. To begin the installation, click **Install**.

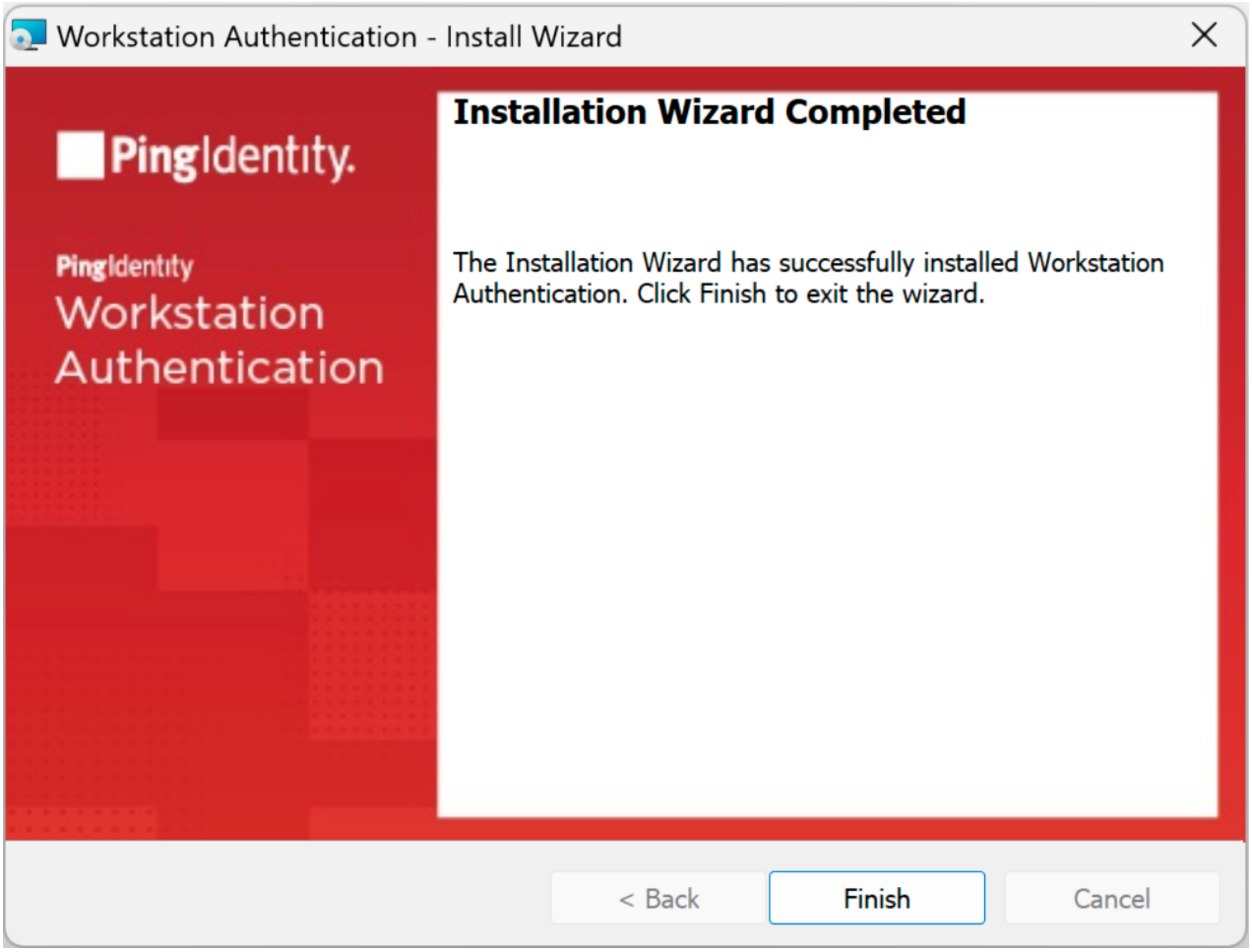
Copyright © 2025 Ping Identity Corporation



A status bar is displayed during the installation process.

5. To exit the wizard, click **Finish**.

Copyright © 2025 Ping Identity Corporation



Perform installation through distribution tools

Follow the steps below to push the installation through your endpoint management or software distribution tool.

> **Note**
>
> Administrator permissions are required to run the workstation authentication for Windows MSI.

To push installation through distribution tools:

1. Open and run your distribution software.
2. Install Visual C++ 2017 (or later) Redistributable (x64)/(x86) - 14.30.30704.0.
3. **Open the command prompt as Admin**, and run `Workstation Authentication.msi`:

```
C:\> Workstation Authentication – xx_xxx_xx.msi /qn
```

> **Note**
>
> Substitute the file name with your outputted, deployment specific, MSI file.

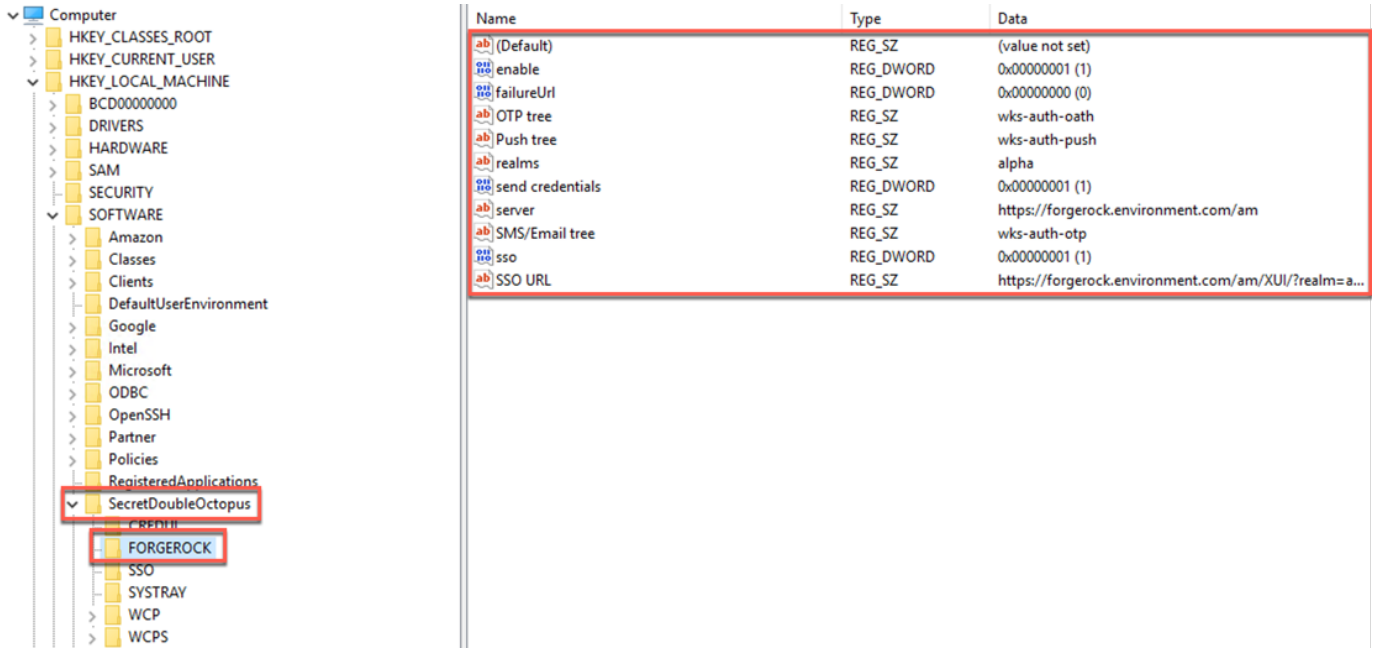
Copyright © 2025 Ping Identity Corporation

Windows Registry Keys post-deployment

Upon deployment of your specific MSI file, registry keys are created/updated on the target Windows machine. To reference the specific registry keys pertaining to Windows Workstation Authentication:

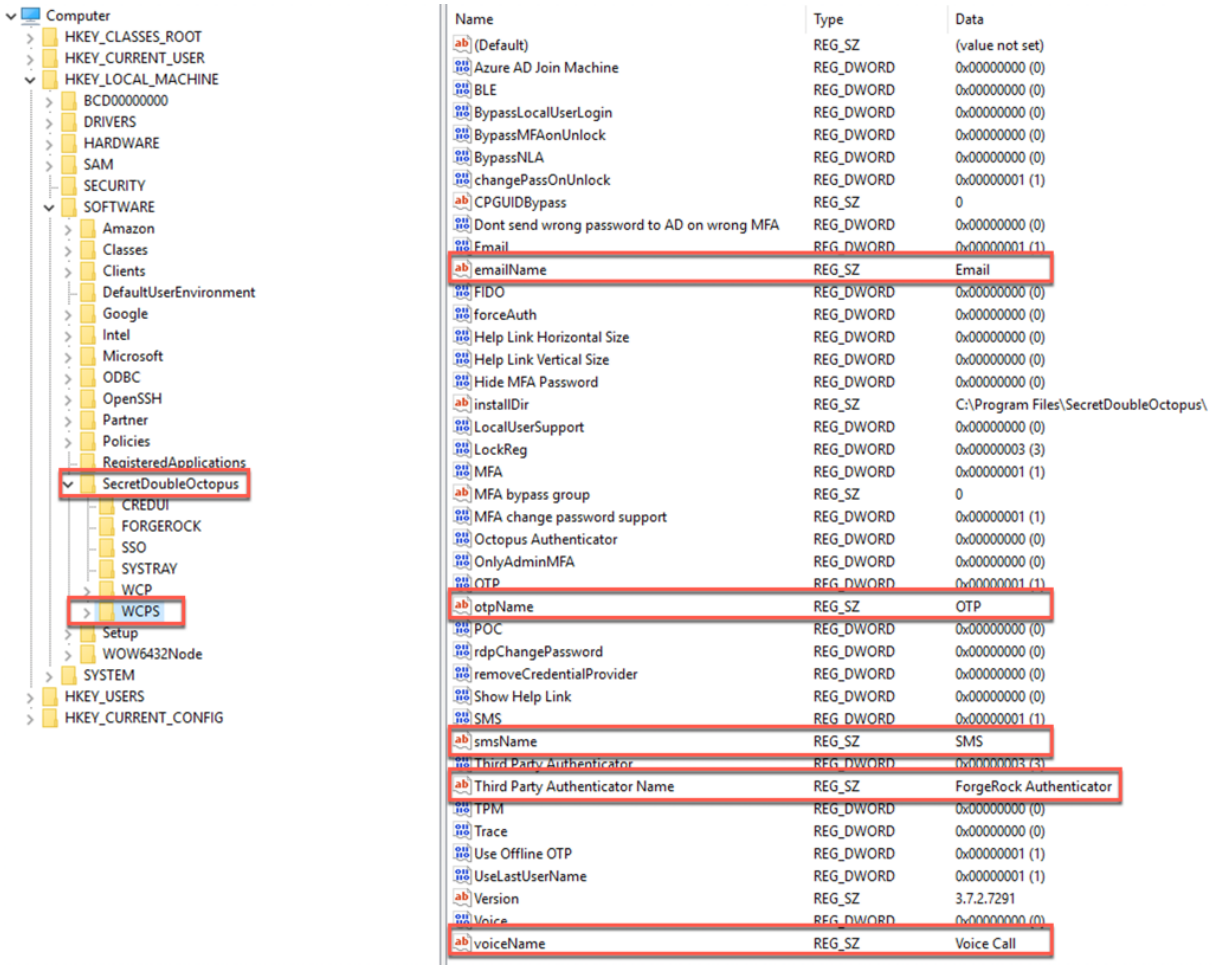
1. Open *Registry Editor* as an administrator.
2. Navigate to Enterprise Connect specific registry keys by going to **HKEY_LOCAL_MACHINE > SOFTWARE > SecretDoubleOctopus**.
3. From here, select the various tabs to see the specific values of the Registry Keys. You will notice values that you configured during the Configure the MSI Updater client process.

   During the MSI Updater client configurations, on the Ping tab, the corresponding registry key and values (under the **Ping** directory) are shown below:



   During the MSI Updater client configurations, on the advanced tab. The corresponding registry key and values (under the **WCPS** directory) are shown below:

Copyright © 2025 Ping Identity Corporation



> **Caution**
>
> Changing the registry key values must only take place if required (for example, resetting the Offline OTP process). Otherwise, all configurations should come through configuring the MSI Updater client for consistent values on all Windows workstations.

Windows Workstation Authentication installation/configuration checklist

Download and install the binaries from Backstage (you must be logged in). This includes the base MSI file as well as the MSI Updater client.

Pre-configure the relevant journey(s).

Install the MSI Updater client on an administrative Windows machine.

Configure the MSI Updater client specific to your organization's needs.

(Optional) Consider additional configurations.

Deploy the generated MSI file through your desired mechanism.

☐ Verify and test your deployment.

Copyright © 2025 Ping Identity Corporation

Verify functionality

Following installation, configuration, and deployment (on a test machine first), it is recommended to test the functionality of workstation authentication to verify that the Windows login process proceeds as expected.

Before beginning the verification process, make sure that the following prerequisites are met:

- You can access the local machine with administrative permissions.
- Users whose authentication will be tested are enrolled, enabled and allowed to log into the local machine.
- Users to be tested have a smartphone with the ForgeRock Authenticator application installed.
- User to be tested has been successfully enrolled to the relevant journey(s), such as push, TOTP (OATH or Offline OTP), or SMS/email/voice call, as defined as a prerequisite and in MSI Updater client configurations.
- The Ping Server URL (as defined in the MSI Updater client configurations) can be accessed from the test machine.

Test Windows login:

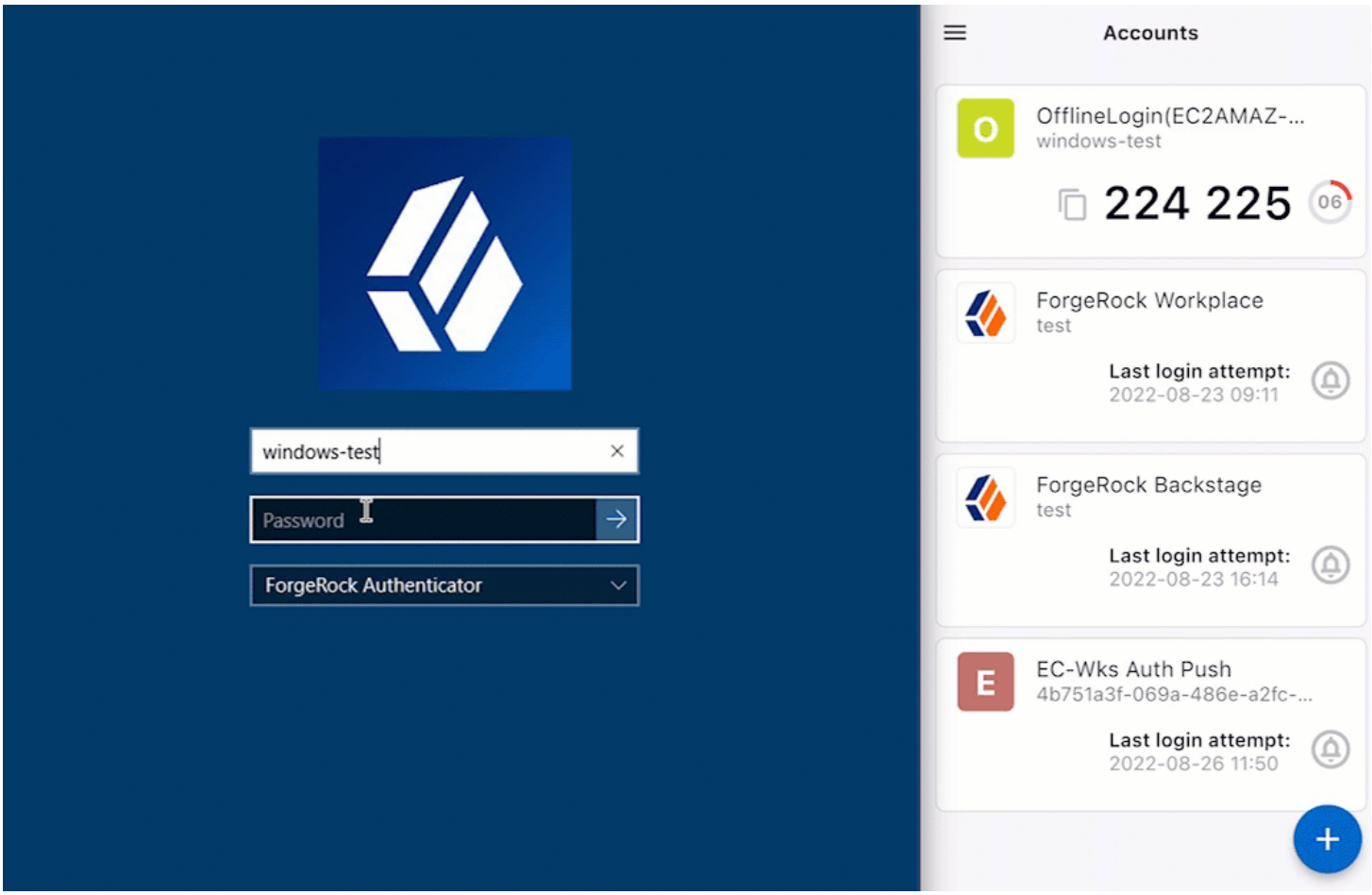


Figure 1. Example of a push login on Windows

1. Access the Windows Login screen and select the authentication option.
2. Enter the appropriate username and password.

Copyright © 2025 Ping Identity Corporation

3. Select the relevant MFA method (Push, OTP or SMS).

   Then, provide the required MFA factor and verify successful login.

> **Note**
>
> If **Use Offline OTP** was enabled during the MSI Updater client configuration, then post the first login (either using push, OTP email, or OTP SMS), an additional screen will appear to scan a QR code for an offline account to be created.
>
> 
>
>
> Once scanned and the account is created in the ForgeRock Authenticator application, the end user must input the **6-digit code** (as shown in the image above) and click **Verify Code**. For more information, refer to Offline OTP enrollment.

4. Repeat steps 1-3 for each available MFA method assigned to the current user.

Windows Workstation Authentication installation/configuration checklist

Download and install the binaries from Backstage (you must be logged in). This includes the base MSI file as well as the MSI Updater client.

Pre-configure the relevant journey(s).

Install the MSI Updater client on an administrative Windows machine.

Configure the MSI Updater client specific to your organization's needs.

Copyright © 2025 Ping Identity Corporation

(Optional) Consider additional configurations.

Deploy the generated MSI file through your desired mechanism.

Verify and test your deployment.

You have completed the checklist. Congratulations!

Offline OTP enrollment

The **Offline OTP** (TOTP/OATH) option enables users to authenticate to Windows when they are not connected to a network.

> **Note**
>
> **Use Offline OTP** must be enabled during the MSI Updater client configuration; otherwise, the end user will not be able to enroll in **Offline OTP**.

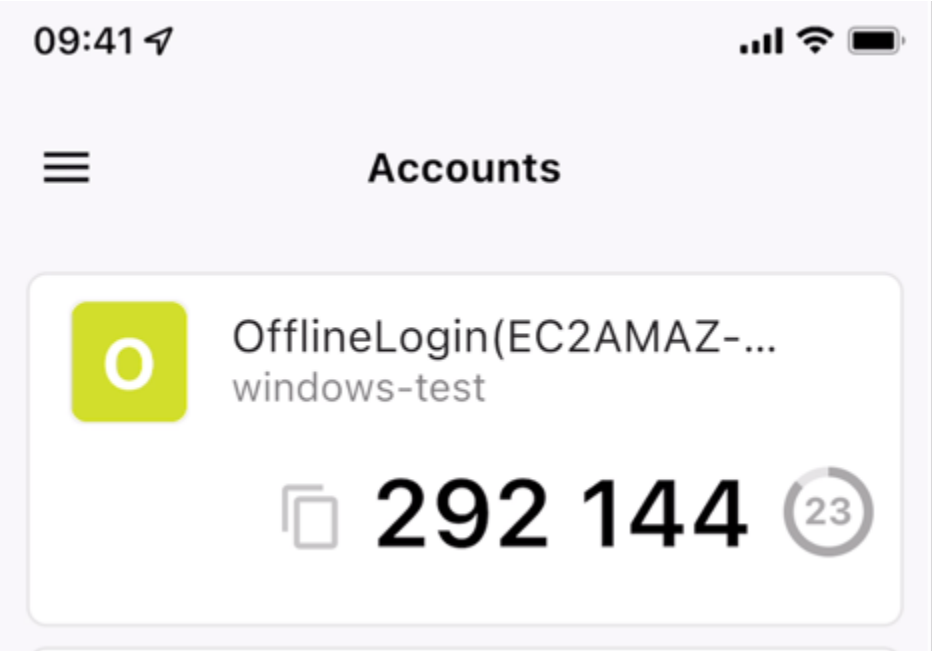
User to enable **Offline OTP**

1. The invitation QR code is initiated and presented to the end user after the first successful login (either push, SMS, or email).

> **Note**
>
> The screens presented correspond to the OTP journey, as described in Example OTP journey and configured in MSI Updater Ping tab.

2. Using the ForgeRock Authenticator application, scan the invitation QR code.

> **Note**
>
> When the end user scans the QR code, an offline account is created in the ForgeRock Authenticator application.



3. Tap the *offline account* to view the six-digit code.

4. Enter the code in the field below the QR code and click **Verify Code**.

> **Note**
>
> Offline mode will be enabled following the next online login. To verify that the system is ready and offline mode is enabled, it is recommended to sign out and login again.

Reset Offline OTP process

In the event that an end user loses their phone or needs to have their Offline OTP reset, as an administrator, follow the below steps:

1. Go to the appropriate directory of registry keys as described in Windows Workstation Authentication registry keys.

2. Select the **WCP** directory.

3. On this page, there are two registry keys with the names prefixed with the user's username:

    1. `username:lastOnlineLogin`

Copyright © 2025 Ping Identity Corporation

2. `usernameOTPS`

> **Note**
>
> There can be multiple sets of these keys if there are multiple users on the same workstation, and they have enrolled in Offline OTP.

4. Delete these two keys.
5. If the end user has the previous OTP profile on their ForgeRock Authenticator application, they must delete the profile.
6. Upon the next successful initial login to their Windows machine, the end user will be re-prompted to enroll in the Offline OTP process, as described in Offline OTP enrollment.

Additional reference

The subsequent sections explore additional uses of the Windows Workstation Authentication.

Windows Workstation Authentication installation/configuration checklist

Download and install the binaries from Backstage (you must be logged in). This includes the base MSI file as well as the MSI Updater client.

Pre-configure the relevant journey(s).

Install the MSI Updater client on an administrative Windows machine.

Configure the MSI Updater client specific to your organization's needs.

(Optional) Consider additional configurations.

☐ Deploy the generated MSI file through your desired mechanism.

☐ Verify and test your deployment.

Perform MSI upgrade

When substantial changes need to be made to the deployed MSI file, you need to "upgrade" the MSI.

An upgrade is also applicable if there is a newer version of the MSI Updater.

Upgrade MSI

1. Create your new deployment specific MSI file.
2. Rename the outputted deployment specific MSI file to the original deployment specific file you first deployed on the Windows machine(s).

Copyright © 2025 Ping Identity Corporation

> **Important**
>
> To perform an MSI upgrade successfully, the MSI file must have the same filename as the one used for the **original** installation. The MSI updater creates an MSI file with the update date in the filename. **This file needs to be renamed** to match the name of the original installation file (the outputted deployment specific MSI file from the MSI Updater configurations).
> If you try to upgrade using an MSI file that is named differently from the original installation file, the following error message will appear:
> `Error 1316: The specified account already exists`
> This message is a notification that you are trying to install an MSI file with a different name from the one that is already installed.

> **Tip**
>
> If you are not sure of the name of the original installation file, follow these steps:
> 1. Navigate to `C:\Windows\Installer`.
> 2. Open the following file:
>   `SourceHash{F04AB2CC-5585-4069-9B95-AABB3CD21DF0}`
> 3. Search for the name of the file that was used for installation. You will find it at the end of the SourceHash file.

3. To upgrade an MSI, run the following command:

```
C:\> msiexec /I "workstation authentication.msi" REINSTALL=ALL
REINSTALLMODE=vomus IS_MINOR_UPGRADE=1 /norestart /qn
```

> **Note**
>
> The `workstation authentication.msi` is to be replaced with your changed or upgraded filename.

For more information and a list of additional optional installation parameters, refer to Microsoft's documentation.

Log files with Windows Workstation Authentication

By default, log files are disabled, but if you need to troubleshoot, logging can be enabled.

Enable and view logging

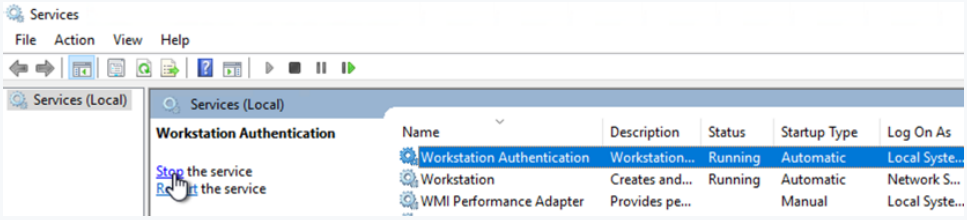
1. Open *Regsitry Editor* as an administrator.
2. Navigate to Enterprise Connect specific registry keys by going to **HKEY_LOCAL_MACHINE > SOFTWARE > SecretDoubleOctopus**.
3. Click on the **WCPS** tab.
4. To turn logging on, change the value of the **Trace** key to `4`.
5. To turn logging off, change the value of the **Trace** key to `0`.
6. Once enabled, logging will begin.

Copyright © 2025 Ping Identity Corporation

7. Log files are stored in `C:\Windows\Temp` and consist of:

> **Note**
>
> The log files start with `sdo` , followed by a function, date, and a serial number. For example, `sdorest06.09.2022190447.txt` .

1. `sdocred` : Records front-end UI activities.
2. `sdoguard` : Records *Workstation authentication* service activities.
3. `sdorest` : Records REST API activities

> **Important**
>
> To access the log files, you must first temporarily **stop** the **Workstation Authentication** service running on the Windows machine. The services holds a lock on the log files and must be suspended for you to view them.
>
> 
>

8. When you have finished troubleshooting, change the **Trace** key back to `0` and start the **Workstation Authentication** service back up.

Remote Desktop Windows Login

To enable MFA for a remote desktop login (RDP), the following additional configurations are required.

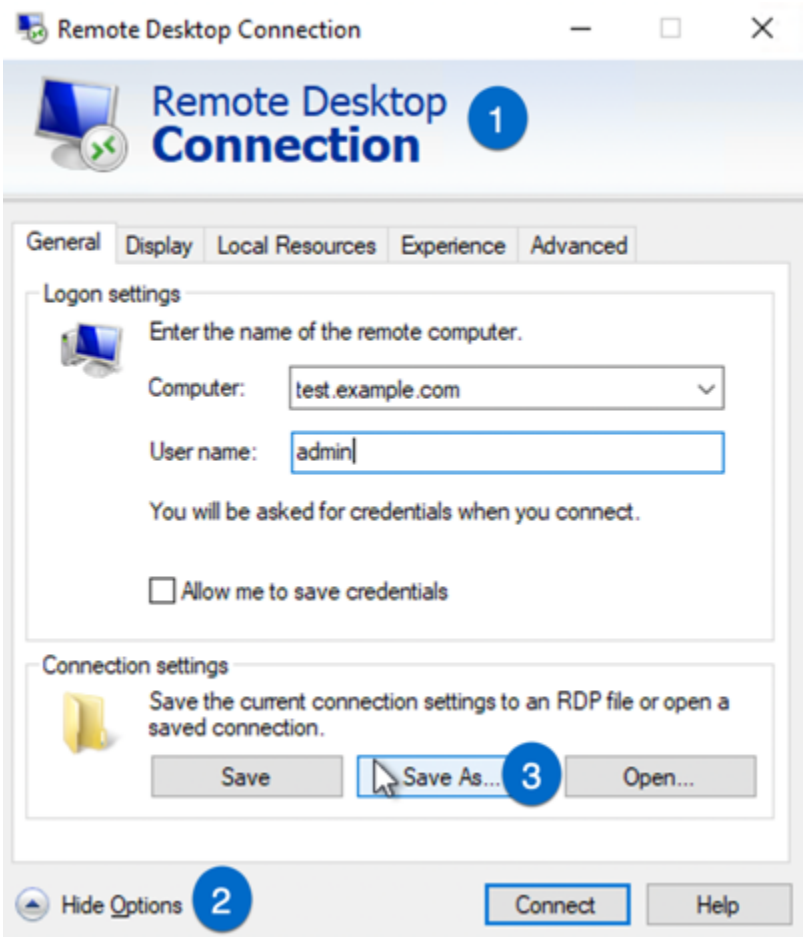
Editing the remote desktop script

Edits are required to the RDP script.

Edit RDP script

1. Launch a Remote Desktop Connection.
2. Select the remote computer and click **Show Options**.
3. Under **Connection Settings**, click **Save As** and save the RDP script.

Copyright © 2025 Ping Identity Corporation



4. Add the following line to the end of the script:

```
enablecredsspsupport:i:0
```

> **Tip**
>
> To open the RDP file in a text editor, you must first open the text editor and then open up the RDP file from there. If you select the RDP file directly in Windows, it will attempt to run the RDP application.

5. Save the script.

Configuring Windows system properties

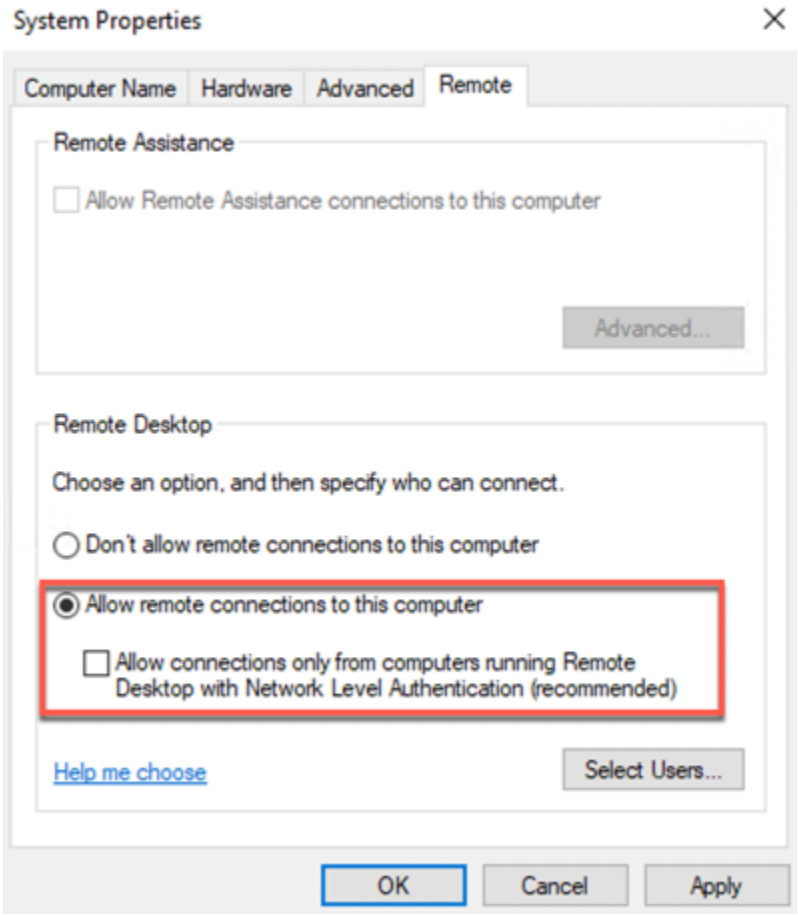
System protection settings need to be in place for the remote desktop.

Configure system protection settings

1. Log into the relevant remote desktop Windows machine.
2. Go to **Control Panel > System and Security > System**.
3. Click **Remote settings**.

Copyright © 2025 Ping Identity Corporation

4. Under **Remote Desktop**:
    - Select the **Allow remote connections to this computer** radio button.
    - Verify that the Allow connections only from computers running Remote Desktop with Network Level Authentication checkbox is **NOT** selected.
5. Click **Apply**.



> **Note**
>
> Administrative privileges are required to perform this action.

Enable/disable the workstation authentication CP post-installation

Windows Workstation Authentication supports the ability to control availability of the workstation authentication credential provider (CP) on target workstations after installation.

Considerations for enabling or disabling the workstation authentication CP:

- This feature allows for bulk installation, followed by gradual deployment on group or user workstations.
- Workstations on which the workstation authentication CP is manually disabled post-installation will not support workstation authentication as a means of logging into Windows.

Copyright © 2025 Ping Identity Corporation

- The installation of workstation authentication is transparent to users, who will not see the Workstation CP on the login screen and will continue to login as they did prior to installation.
- If it is **crucial** for your organization to be able to control the workstation authentication CP, it needs to be enabled.
- To enable or disable the workstation authentication CP post-installation, the *Windows registry* must be updated.

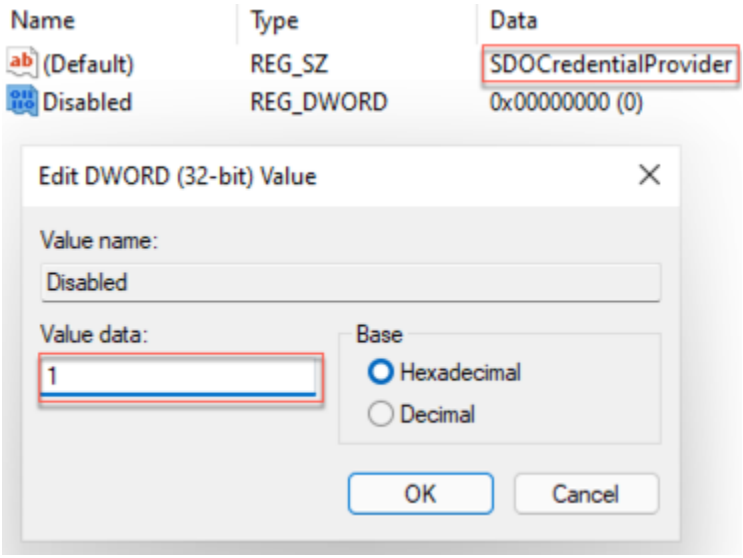
> **Note**
>
> Administrative privileges might be required.

To disable the workstation authentication CP post-installation:

1. Open **Registry Editor** application and navigate to `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers{a95d85be-778f-4ed1-9ded-9f62ecc8a744}`.

   > **Note**
   >
   > The hexadecimal GUID `{a95d85be-778f-4ed1-9ded-9f62ecc8a744}` is subject to change and *could* be different in your environment.

2. Change the `REG_DWORD` data value to `1`.



3. Click **OK**.

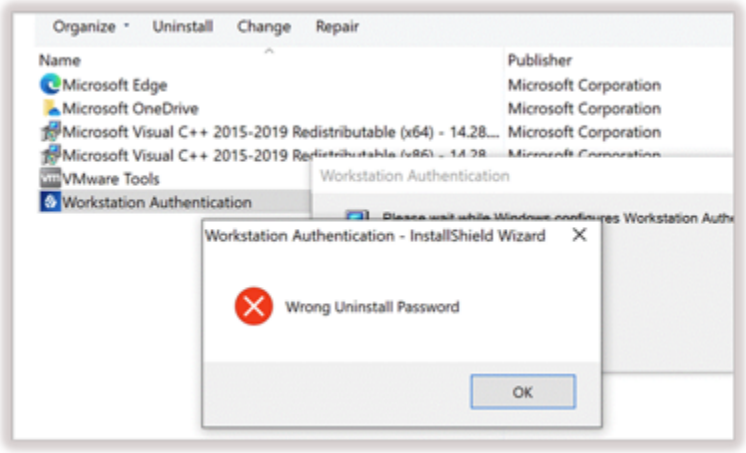
   > **Note**
   >
   > To enable workstation authentication CP, change the value to `0`.

Copyright © 2025 Ping Identity Corporation

Uninstall Windows Workstation Authentication

To uninstall Windows Workstation Authentication, keep the following in mind:

- If the **Uninstall** field of the **Parameters** tab was filled out during the configuration of the MSI Updater client, then the MSI is protected with an administrator password. If this is the case, then **Admin permissions** are required to uninstall. For more information regarding this configuration, refer to Configure the MSI Updater client.
- Uninstalling Windows Workstation Authentication can be done from the **command line only**. Uninstalling the application from the *System Settings* can result in an error, as shown below.



To uninstall workstation authentication, open the command prompt as an **Admin** and run:

```
C:\> msiexec /x \ {F04AB2CC-5585-4069-9B95-AABB3CD21DF0}
PASSWORD=”AdminPassword!!”
```

Tip

Replace *"AdminPassword!!"* with the password used during the MSI Updater client configuration.

Copyright © 2025 Ping Identity Corporation

Windows RADIUS proxy

Enterprise Connect brings the capability for a remote authentication dial-up service (RADIUS) proxy to be installed on a Windows machine via the RADIUS protocol.

The RADIUS proxy changes the local RADIUS call to a secured REST API call, allowing local RADIUS clients to connect to Ping for authentication. In turn, the capability to use MFA is provided, allowing tools, such as a virtual private network (VPN), to be enhanced.

Install Windows RADIUS proxy

Install and configure the Windows RADIUS proxy on a Windows machine(s).

Configure Linux SSH to use Windows RADIUS proxy for MFA

Post installation of the Windows RADIUS proxy on a Windows machine(s), explore the use case of setting up MFA on SSH login with Linux machines.

The Ping integration supports the following authentication methods via **PAP** (password authentication protocol):

- Push notifications (this is the preferred and **recommended** method) via the ForgeRock Authenticator application.
- Time-based one-time passcodes (TOTP/OATH) via the ForgeRock Authenticator application.
- Simple username and password credentials.

The subsections serve as the basis for installing the RADIUS proxy on a Windows machine.

Prerequisites

Before beginning the installation you must:

- Have administrative privileges on the target Windows machine.
- Obtain the Windows Workstation Authentication installation file from Backstage.

> **Note**
>
> You must have a Backstage account and be logged in to view the download.

- Create a service account user for the Windows RADIUS proxy to run as. The minimum account privileges this user needs are:
  - Enable *Log on as a service*. For more information, refer to Microsoft's documentation.

Copyright © 2025 Ping Identity Corporation

- Write permission to C:\windows\system32 to have access to create the `logs` folder.
- Write permission to C:\Windows\System32\logs folder.

- Pre-configure journeys and services, as described in Create authentication journey(s).
- Ensure all usernames (profiles/accounts) match from *Windows (or the authoritative source)* > *Ping* and vice versa.
  - Set up a connector from Ping to the datastore (for example, AD) and sync the data.
- For push and OTP (TOTP/OATH) authenticator methods, users pre-register in the appropriate journeys.

> **Important**
>
> It is crucial for users to pre-register; otherwise, these MFA methods will not work through the RADIUS proxy.

> **Note**
>
> Your RADIUS client **must** support the exchange of the TOTPs from **Ping journey > RADIUS proxy > RADIUS client** and conversely to work. This includes handling *challenge-response* flows. If your client cannot handle the calls, use the **push** method instead.

- Users install the ForgeRock Authenticator application to their smartphone via the Apple store or Google Play store.
- For high availability/disaster recovery, it is recommended to deploy the necessary amount of Windows Workstation Authentication behind load balancers. Additionally, only **one instance per machine is allowed**.

Supported environments

Windows Workstation Authentication can only be installed on the following operating systems:

- Windows 10
- Windows 11
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

> **Important**
>
> Windows 8.1 and Windows Server 2012 are not supported.

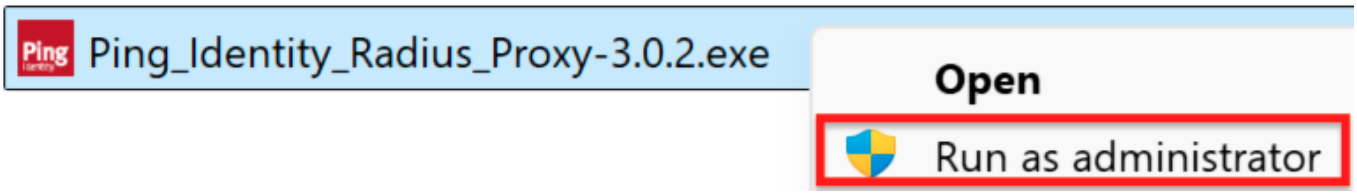
Install Windows RADIUS proxy

Installing the RADIUS proxy is an intuitive process that utilizes an Installation Wizard to assist you. You must complete the prerequisites before following the below steps.

Install the Ping RADIUS proxy on Windows

1. Right-click on the `Ping Radius Agent.exe` file and select **Run as administrator**.

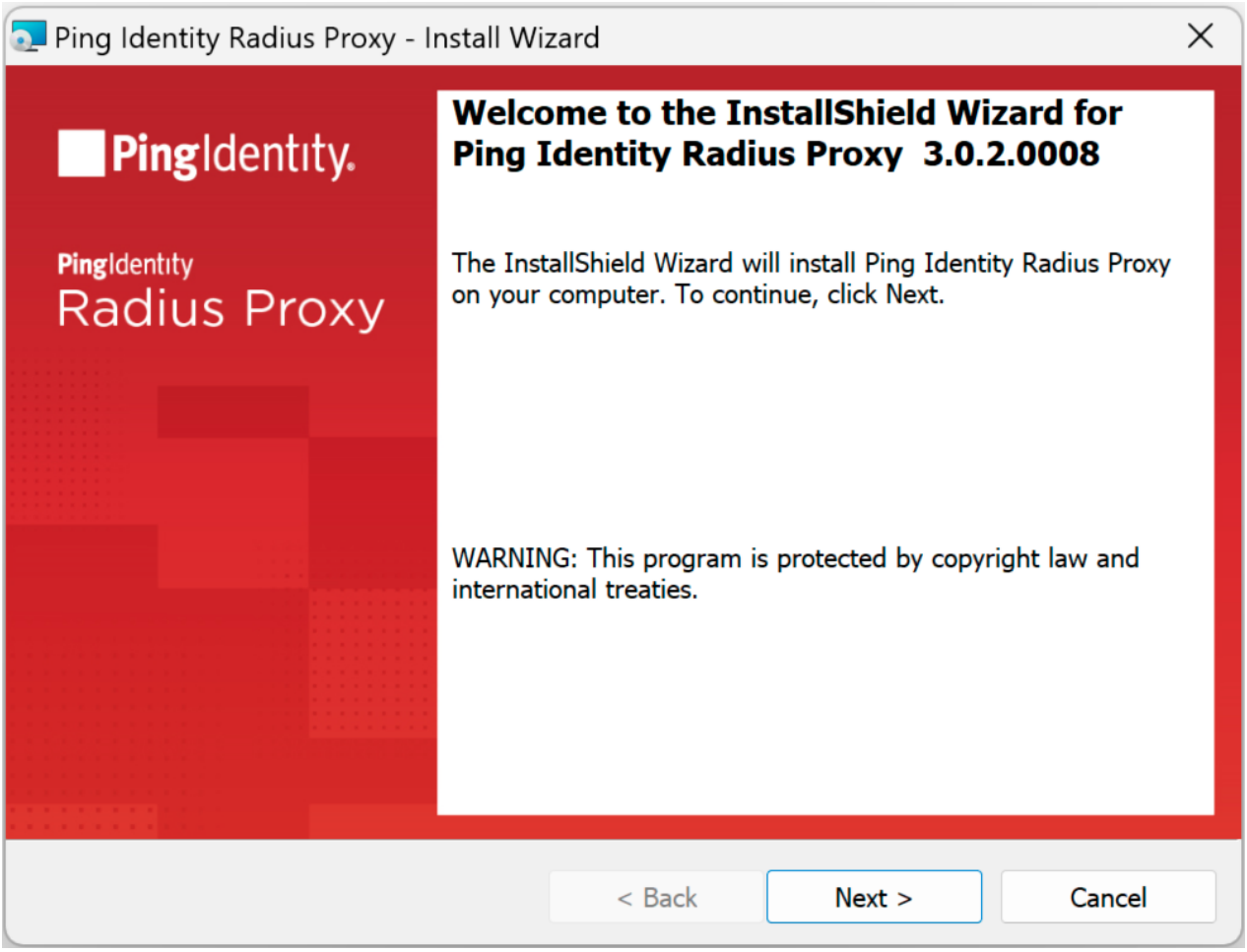
Copyright © 2025 Ping Identity Corporation



The installation wizard opens.

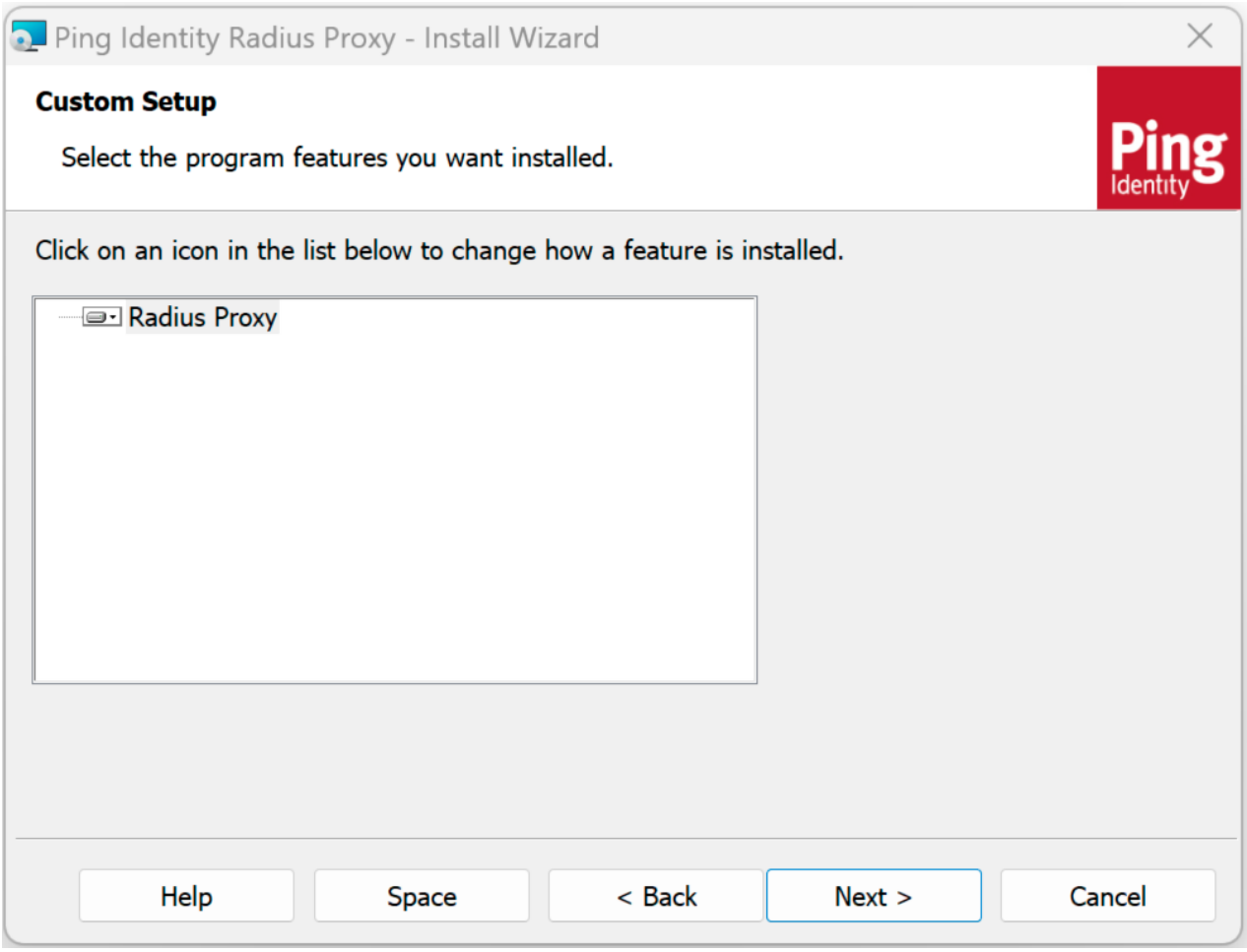
> **Note**
>
> The file name of the RADIUS proxy is subject to change from the download. If you do not run the executable as an administrator, the installation will fail.

2. On the Welcome screen, click **Next**.



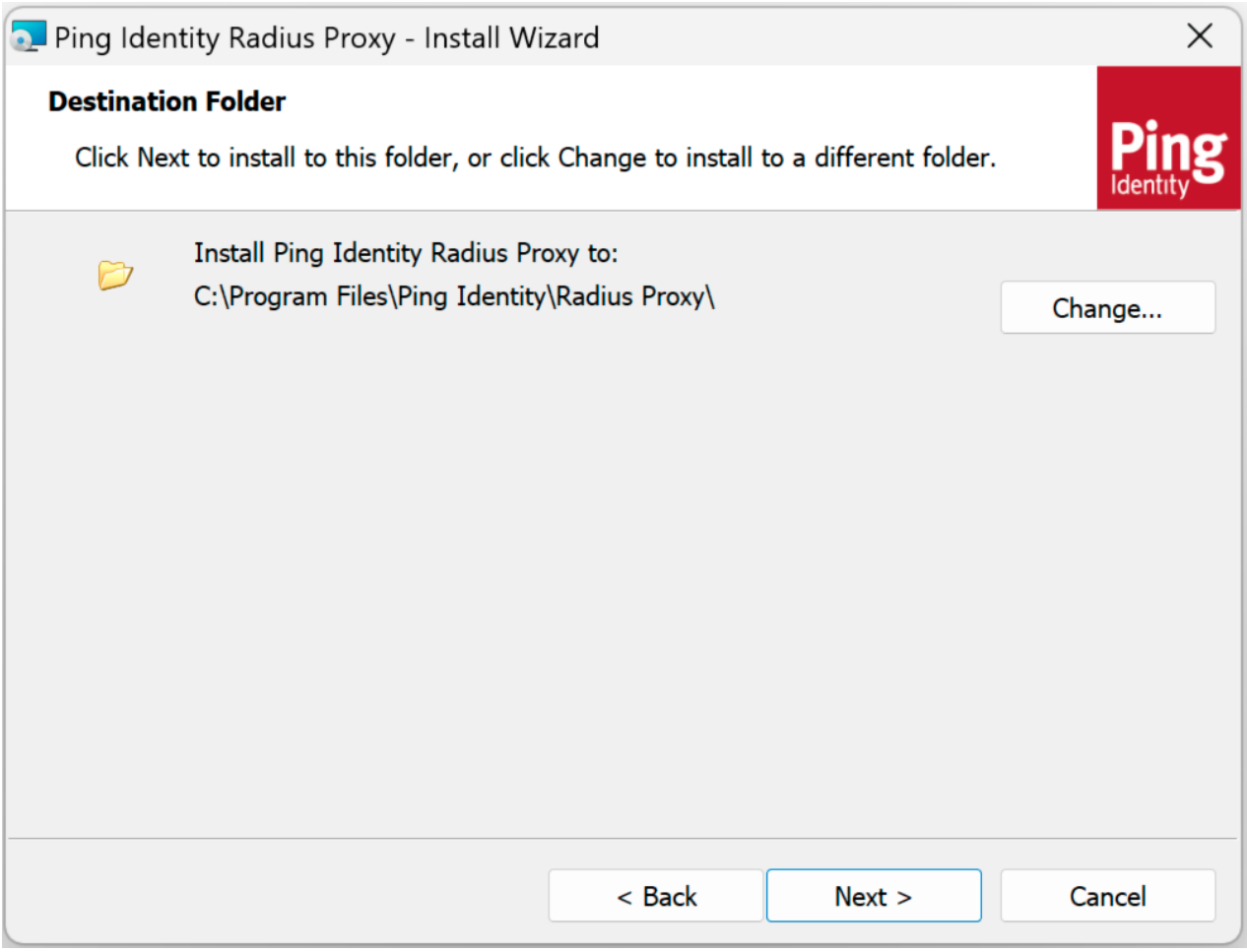
3. On the **Custom Setup** screen, click **Next**.

Copyright © 2025 Ping Identity Corporation



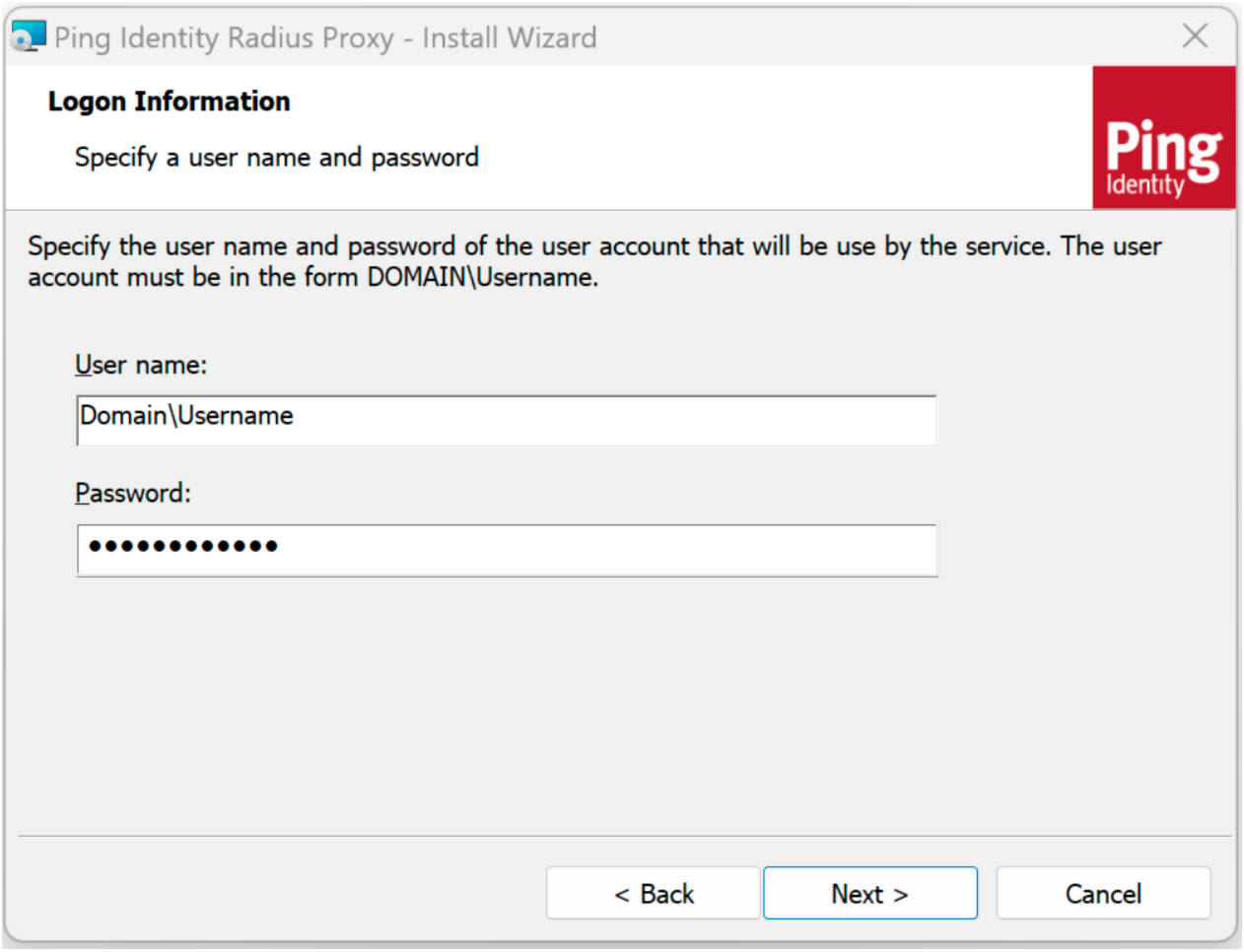
4. On the **Destination Folder** screen, click **Next**.

Copyright © 2025 Ping Identity Corporation



5. On the **Logon Information** screen, enter the service account user credentials for the service account using the Ping RADIUS service. Make sure the syntax for the username is *Domain\Username*. For more information on the privileges required for this account, refer to prerequisites.

Copyright © 2025 Ping Identity Corporation



> **Note**
>
> If the machine is not a part of a domain, then the domain for the service account user is the machine name.

6. On the **Agent Parameters** page, configure the required settings:
   - Enter the relevant **URL**. For example, `https://<tenant-env-fqdn>/openam`.
   - Enter the relevant **Realm**. For example, `/alpha`.
   - Enter the **Journey** field for the selected authentication method:
     - **Push** (for example, `push-radius`)

       For an example of a push journey (used with the ForgeRock Authenticator application), refer to Example of a push journey.
     - **TOTP** (for example, `otp-radius`)

       For an example of a TOTP/OATH journey (used with the ForgeRock Authenticator application), refer to Example of a TOTP/OATH journey.

Copyright © 2025 Ping Identity Corporation

> **Note**
>
> Your RADIUS client **must** be able to support the exchange of the TOTPs from **Ping journey > RADIUS proxy > RADIUS client** and conversely for the TOTP (OATH) method to work.

- **Simple** (for example, `simple-radius`)

Figure 1. Simple authentication journey in PingOne Advanced Identity Cloud

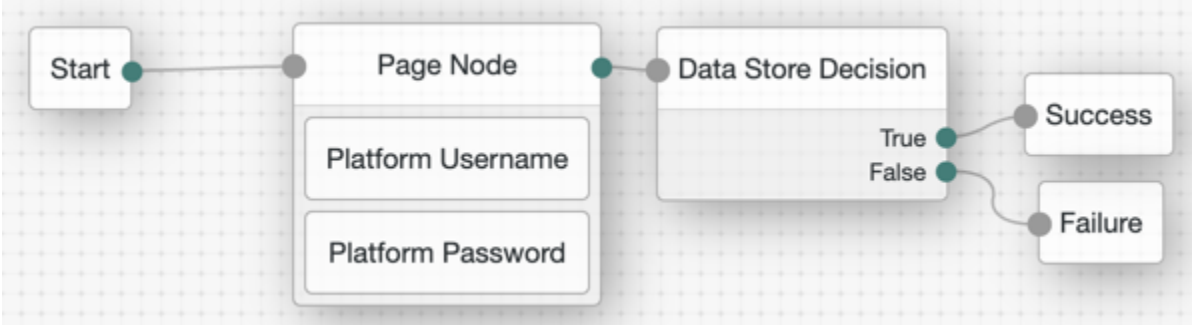
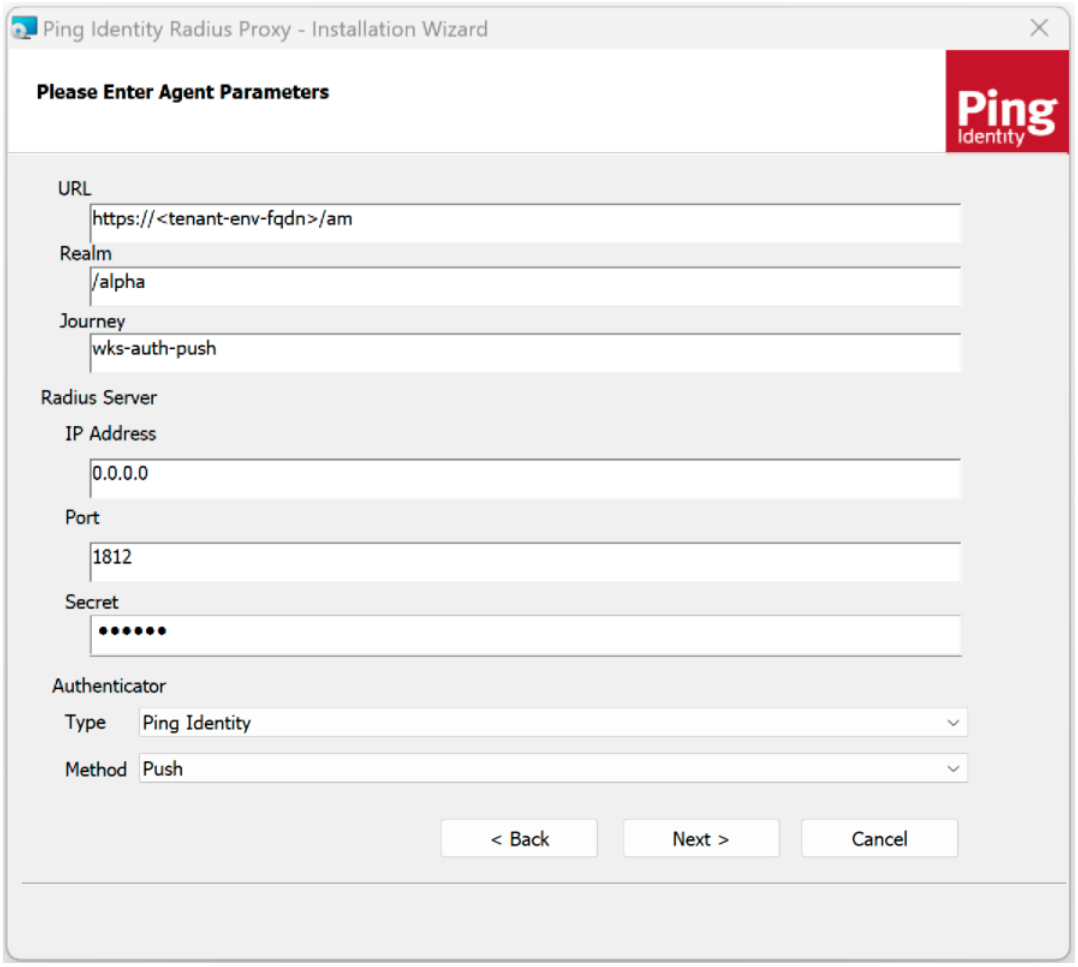


Figure 2. Simple authentication journey in PingAM

> **Note**
>
> You can only configure one journey and one authenticator method. The journey entered will correspond to the authenticator method selected in subsequent steps.

Copyright © 2025 Ping Identity Corporation



1. Review the default values in the **Radius Server** section of the **Agent Parameters** screen, and if necessary, change them.
    1. **IP Address**: Enter the IP address of the interface the RADIUS Proxy communicates on. If the default value (127.0.0.1) is used, RADIUS Proxy only communicates with traffic from the local machine.

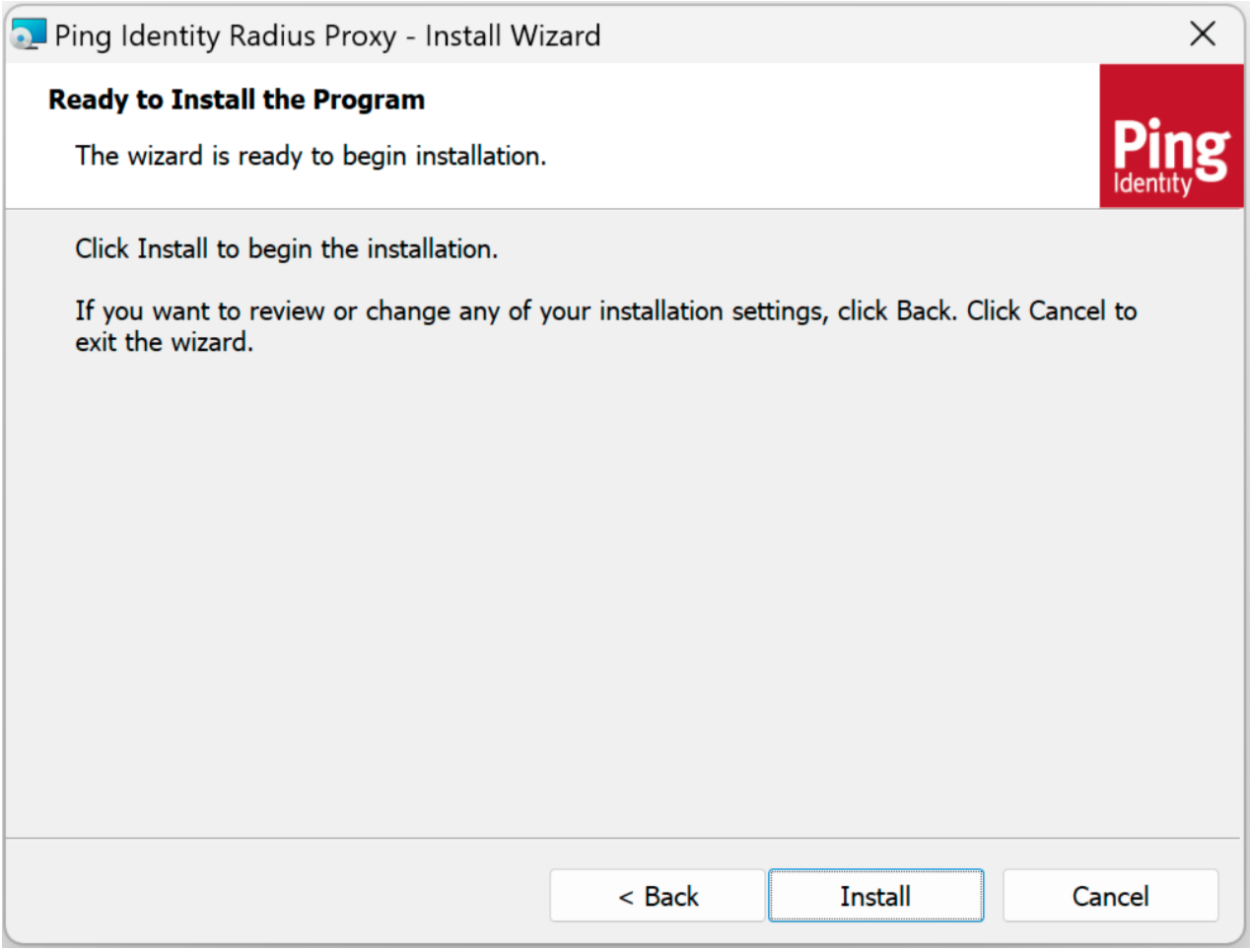
        > **Important**
        >
        > Change the IP Address to `0.0.0.0` to allow the Windows RADIUS proxy to listen on all interfaces.

    2. The default **Port** is `1812` (via UDP). Change if necessary.
    3. Input a value into the **Secret** field that is strong and complex. Take note of the secret, as it might be needed when configuring your RADIUS client to the RADIUS proxy. The **Secret** value appears to be pre-populated, but it is not.

        > **Note**
        >
        > Ensure that the RADIUS client you are configuring with the Windows RADIUS proxy allows the characters in the **Secret** field. For instance, some RADIUS clients can not process special characters.

2. Review the settings in the **Authenticator** section of the **Agent Parameters** screen and verify they match the authenticator type and method you configured. If necessary, you can correct the **Authenticator** configuration by selecting the correct settings from the drop-down lists.
3. To begin the installation, click **Install**.

Copyright © 2025 Ping Identity Corporation



A status bar is displayed during the installation process.

4. To exit the installation wizard, click **Finish**.

Once you have completed the installation of the RADIUS proxy, proceed to the post-installation steps.

Post-installation steps

Following installation, it is recommended to perform the following checks to verify that your environment has been **set up as expected**.

Check Windows Services

Make sure that the *Ping Identity Radius Proxy* service is installed and running via *Windows Services*:

1. Press **Windows + R** on your keyboard.
2. Type services.msc.
3. Hit **Enter** to open the service.
4. Search for the service under the name column. The service name is *Ping Identity Radius Proxy*.

Copyright © 2025 Ping Identity Corporation

Verify installation of folders and files

Verify that all the folders and files are installed under C:\Program Files{ping_name_full}\Radius Agent.

> **Note**
>
> The configuration settings are stored in `appSettings.Production.json`. If you modify the configuration settings directly from this file, you must restart the RADIUS service (via Windows Services). The service name is `Ping Identity Radius Proxy`.

Verify functionality with RADIUS client

Once the Windows RADIUS proxy has been configured and installed on a Windows machine, it is important to test the setup.

Before beginning the verification process, make sure the following prerequisites are met:

- The Windows RADIUS proxy is installed.
- On a separate Windows machine, a test RADIUS client is installed. For example, NTRadPing.
  - Ensure the appropriate network connectivity is allowed between the two Windows machines. The default port is `1812` unless changed in the installation of the Windows RADIUS proxy.
- Have a test account with a username and password.

Validate service is listening

To validate the service is listening, use a tool such as `netstat` on the Windows machine running the Windows RADIUS proxy:

```
netstat -ano | find "1812"
```

Test with RADIUS client

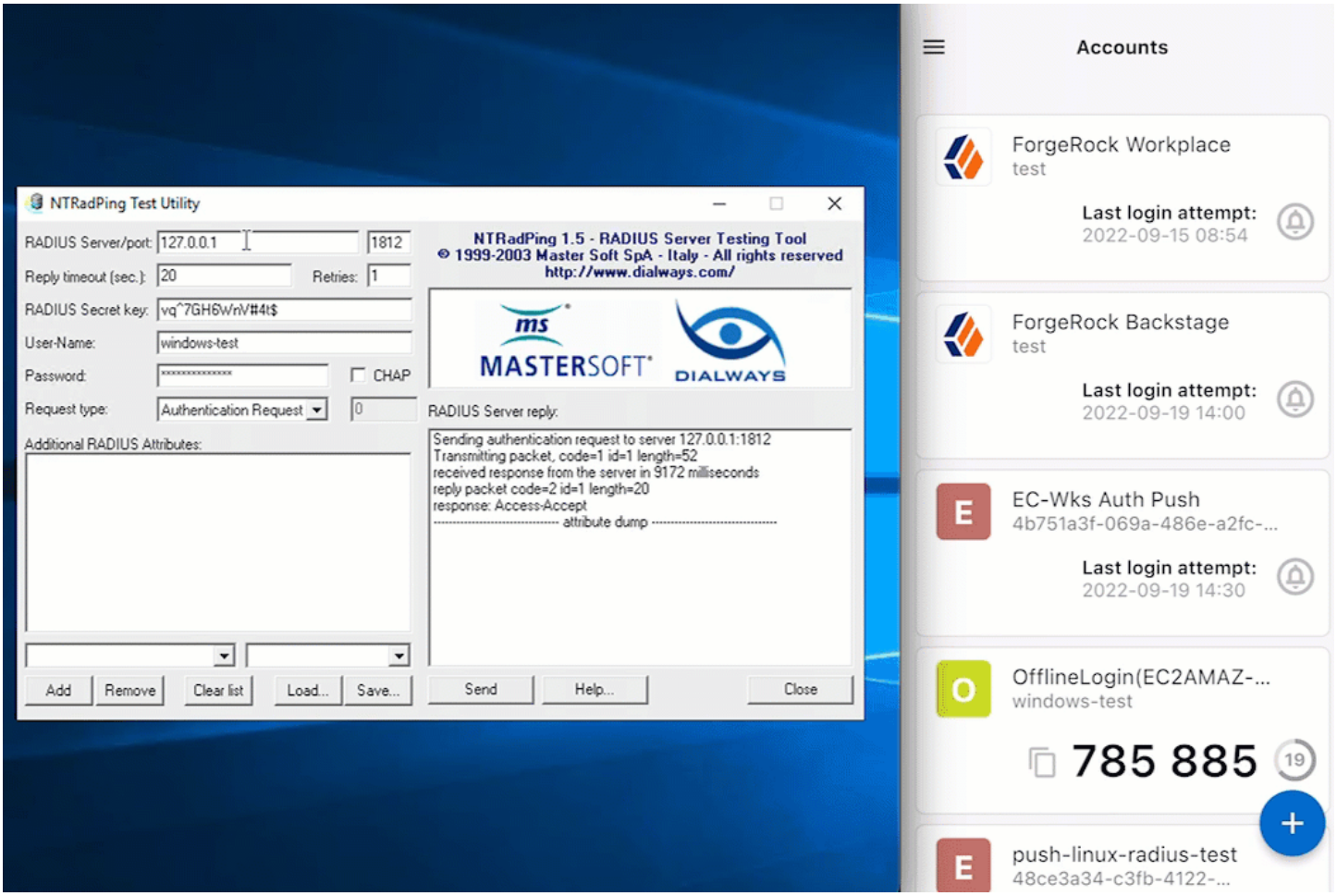
To test with the RADIUS client, you must have the following information from the Windows RADIUS proxy installation:

- Windows RADIUS proxy server and port.
- RADIUS **Secret**.
- Test account with username and password to use with the RADIUS client. Ensure the user account exists in the Ping environment.

For this example, NTRadPing is used as a test RADIUS client; however, any other RADIUS client will work.

Test Windows RADIUS proxy with RADIUS client

Copyright © 2025 Ping Identity Corporation



1. Open desired RADIUS client, in this case, NTRadPing.
2. Enter the Windows RADIUS proxy specific items. This includes the server, port, secret, and username and password for the test account.
3. Click **Send** to initiate communication from the RADIUS client to the Windows RADIUS proxy.
4. If the MFA method push was selected, for example, approve the login attempt from the ForgeRock Authenticator application.

> **Note**
>
> For push, users must pre-register as described in Prerequisites and Create push journey.

5. Await a response from the Windows RADIUS proxy (server) that states `Access-Accept`.

Change Windows RADIUS proxy secret

Due to security reasons or change management, it can become necessary to change the secret you configured for the Windows RADIUS proxy (during the time of installation).

The installation path includes an executable to assist with the updating of the secret:

1. Via *Command Prompt*, go to C:\Program Files{ping_name_full}\Radius Agent on your Windows machine.

Copyright © 2025 Ping Identity Corporation

2. Run the ConfigTool.exe file with the appropriate parameters:

   ```
   ConfigTool.exe set-secret --secret enterNewSecretHere
   ```

3. A message such as `` `appsettings.Production.json` Updated Successfully! `` should appear.

4. The Windows RADIUS proxy secret has now been updated.

   > **Tip**
   >
   > Ensure you update the new Ping Identity RADIUS proxy secret on dependent applications using the service.

   The new secret will be used after the restart of the Windows service `Ping Identity Radius Proxy`.

Additional reference

The subsequent sections explore additional features of Windows RADIUS proxy:

- Configure Linux SSH to use Windows RADIUS proxy for MFA
- Uninstall Windows RADIUS proxy
- Log files with Windows RADIUS proxy

Configure Linux SSH to use Windows RADIUS proxy for MFA

With the Windows RADIUS proxy installed and configured on a Windows machine, you are ready to add MFA to an SSH login on Linux.

This use case is explored in this section.

> **Note**
>
> The subsequent sections and examples utilize the Red Hat Enterprise Linux (RHEL) distribution. The commands can vary slightly. For example, RHEL uses `yum` to install packages while the Debian Linux distribution uses `apt`.
> The following subsections assume you are logged into the Linux terminal as the **root** user or equivalent.

Prerequisites

Before setting up the SSH login on a Linux machine to use MFA via the Windows RADIUS proxy, you must:

- Install the Windows RADIUS proxy.
- Validate and test the Windows RADIUS proxy.
- Establish network connectivity between the Linux machine(s) and the Windows machine(s).
- Confirm all usernames (profiles/accounts) match from the *Linux machine(s)> ForgeRock* and vice versa.
  - Set up a connector from Ping to the datastore and sync the data.
  - The Ping journey validates the credentials when you configure MFA on an SSH login for Linux.

Copyright © 2025 Ping Identity Corporation

- Confirm users pre-register in the appropriate journey if required. For example, for the push MFA method, users download the ForgeRock Authenticator application. For more information, refer to Windows RADIUS proxy prerequisites.

> **Important**
>
> Ensure you properly patch, lock down, and harden the Linux machine(s) you expose to the Windows RADIUS proxy.

Install required packages

Packages are required to install relevant RADIUS configurations.

1. Install the EPEL release by running the following command:

```
sudo yum install epel-release
```

2. Install the PAM RADIUS client by running the following command:

```
sudo yum install pam_radius.x86_64
```

3. Using an RPM command, verify that the installations were successful.

> **Note**
>
> If any of the install commands return as not found by the package manager, locate the appropriate package name via an internet search as these are subject to change slightly depending on your Linux distribution.

Configure PAM RADIUS

After you install the required packages (which installs the PAM RADIUS), you must configure the PAM RADIUS module.

1. Edit the `/etc/pam_radius.conf` file (using vim or an equivalent text editor).
2. In the file, remove all entries below the `127.0.0.1` entry, under the table `# server[:port] shared_secret timeout (s)`.
3. Add an entry using the syntax `<WindowsRADIUSProxyIPAddress>:<portOfProxy> <Windows RADIUS Secret> <timeoutInSeconds>`.

```
# server[:port] shared_secret   timeout (s)     source_ip       vrf
127.0.0.1       secret          3
{insertIP}:1812 {insertSecret} 60
```

Figure 1. Linux PAM RADIUS configuration

Configure SSH Daemon

After the PAM RADIUS configurations are complete, the `sshd` configuration must be updated to utilize the RADIUS settings on SSH login.

1. Edit the `/etc/pam.d/sshd` file (using vim or an equivalent text editor).
2. Add the following line to the top of the file:

Copyright © 2025 Ping Identity Corporation

```
auth required /usr/lib64/security/pam_radius_auth.so
```

This line instructs Linux that for authentication, use the PAM RADIUS configurations. It requires the authentication service to enforce users to log in via the Windows RADIUS proxy. For more information on this, refer to RHEL's documentation.

3. Save changes and exit the file.
4. Restart the `sshd` service:

```
sudo systemctl restart sshd.service
```

> **Caution**
>
> Verify these changes with a test user and machine before applying them to your environments. Ensure the selected MFA method (defined in Install Windows RADIUS proxy) works with the test user.
> Failure to confirm this successfully may result in users being locked out of the Linux machine(s).

Verify and test functionality

With the Windows RADIUS proxy installed and tested, the required packages installed on the Linux machine(s), and relevant configuration changes to PAM RADIUS and the SSH Daemon, you are ready to verify and test SSH login with a user.

> **Important**
>
> Ensure the user you test in your Linux environment matches what is in your Ping environment.

Add a Linux user

To add a user on a Linux machine:

1. Create the user:

   `adduser <username>`

2. Modify the password of the newly created user:

   `passwd <username>`

   You will be prompted to enter and re-enter the password of the user.

   > **Note**
   >
   > Create the user in your Ping environment with the same username and password for testing. In a production scenario, syncing should be set up.

Copyright © 2025 Ping Identity Corporation

Perform SSH login

After you create a test user in the Linux environment with an equivalent account in the Ping environment, you are ready to perform an SSH login test. The below steps assume the push MFA method was configured in the Windows RADIUS proxy setup.

1. Initiate an SSH connection to the target Linux machine.
2. Enter the username and password as prompted. A push notification should appear on your phone.
3. Tap **Approve** on the ForgeRock Authenticator application.
4. Verify that you have successfully logged into the Linux terminal with a valid session.

Uninstall Windows RADIUS proxy

The RADIUS proxy can be uninstalled at any time via the **Control Panel** of your Windows machine.

Uninstall the Windows RADIUS proxy

1. Press **Windows + R** on your keyboard.
2. Type `control panel`.
3. Hit **Enter** to open the control panel.
4. Navigate to **Programs > Programs and Features**.
5. Select **Ping Identity Radius Proxy**.
6. Click **Uninstall**.

Log files with Windows RADIUS proxy

With the Windows RADIUS proxy set up and configured, logs are generated automatically. They can be found under `C:\Windows\System32\logs`. The file format is `radius_log-service-date`. For example, `radius_log-20220830.log`.

> **Note**
>
> If you don't see the log files, ensure the service account for Windows RADIUS proxy has sufficient privileges to write to `C:\Windows\System32\logs`.
> If the service doesn't have the privileges, update the user's privileges or change the login user for the Ping Identity Radius Proxy service to a user with sufficient privileges, then restart the service.

Copyright © 2025 Ping Identity Corporation

Mac Workstation Authentication

Mac Workstation Authentication provides your organization with the capability to secure Mac workstations or servers with rich multi-factor authentication (MFA) using:

- Push notifications through the ForgeRock Authenticator application.
- OATH one-time passcodes (HOTP or TOTP) through the ForgeRock Authenticator application.

Benefits of Mac Workstation Authentication:

- Provides the fastest and safest way to close the desktop security gap. The first desktop MFA solution to integrate fully with the Ping directory and ForgeRock Authenticator application.
- Offers unprecedented endpoint security using the familiar ForgeRock Authenticator application. The solution offers end users the best MFA experience while relieving IT teams from the expensive and cumbersome deployment of OTP tokens and security keys to protect workstations.
- A plug-and-play solution that is easy to install on employee endpoints. No dedicated server is required, enabling fast deployment for the entire workforce. Your organization can now dramatically boost their domain security, improve user experience, and take the first step toward becoming fully passwordless in the future.

Mac Workstation Authentication installation/configuration checklist

Download and install the binaries from Backstage (you must be logged in).

- ☐ Install the Mac client on end users machines.
- ☐ (Optional). Onboard and enable local users on their Mac machine.
- ☐ (Optional). Enable Offline OTP to allow users to login to their Mac when not connected to the internet.
- ☐ Verify and test with a test user.

Prerequisites

Before beginning installation, verify that:

- You decide if the Macs will be domain-joined or standalone. Mac Workstation Authentication supports both.
- You establish connectivity between the Ping environment and the end user's Mac workstations.

> **Note**
>
> Communication with the Ping environment is crucial for Mac Workstation Authentication to function properly. Adjust your network settings appropriately.

- To support the MFA methods in Mac Workstation Authentication, end users must download the ForgeRock Authenticator application to their smartphone via the Apple store or Google Play store.
- For push or OATH TOTP MFA methods to work, you must pre-configure the journey.
  - End users must also be pre-registered in the respective journey.
  - For an example of a push journey, refer to Example of a push journey.

Copyright © 2025 Ping Identity Corporation

    - For an example of an OATH OTP journey, refer to Example of OATH OTP journey.

- You have administrative permissions in the Ping environment.
- Download and install the binaries from Backstage (you must be logged in).
- The Mac configuration XML file is ready to be deployed.

Supported environments

Mac Workstation Authentication can only be installed on the following operating systems:

- macOS Sonoma
- macOS Ventura
- macOS Monterey

> **Note**
>
> Mac Workstation Authentication supports both Intel x86-64 and Mac M1/M2/M3 architecture.

Install Mac Workstation Authentication

There are three steps to install the Mac Workstation Authentication:

1. Prepare for installation
2. Install the Mac Workstation Authentication
3. Onboard local users

Prepare for installation

To install the Mac Workstation Authentication, there are two files provided in the download that are required:

- `WorkstationAuthenticationForMac.pkg` : The Mac installer file.
- `WorkstationAuthenticationForMac.xml` : The configuration file for the installation.

> **Note**
>
> For successful installation, you must store these files in the same folder and have the same name (with the file type differing).

In Mac Workstation Authentication there are two options for MFA:

- Push notifications using the ForgeRock Authenticator application.
- An OATH OTP provided by the ForgeRock Authenticator application.

You can only configure one of the MFA methods to use with Mac Workstation Authentication.

Copyright © 2025 Ping Identity Corporation

Configure the XML file

Before you can install Mac Workstation Authentication, you must configure the XML file. The XML file includes details about your Ping environment.

To configure the XML file:

1. Open `WorkstationAuthenticationForMac.xml`.
2. At a **minimum**, fill out the required fields `server`, `realm`, and `tree`.
3. Save the file.

Parameters in the XML file

Parameter	Description
`server`	Required. Enter the URL of your Ping authentication server. For example, `https://test.forgerock.com/am`. You must include the path to AM in the URL.
`realm`	Required. Enter the name of the Ping realm to authenticate to. For example, `alpha`. **Note** There is no leading `/` when defining the realm for Mac Workstation Authentication.
`tree`	Required. The preconfigured journey to use for Mac Workstation Authentication For example, `mac-otp`. For examples on the journeys, refer to create push or journey or create an OTP journey.
`otpdigits`	Optional. This field is relevant only when you want your users to use the OTP MFA method. **Important** If you enter anything in this field, then the OTP method will be configured for your users. Leaving this blank assumes the MFA push notification method is used. This is the number of digits in the OTP verification code. A value is required to successfully use the OTP journey. You must configure the appropriate journey to use this method. Ensure that the number you put here matches the number you configure in the **One Time Password Length** field of the **OATH Registration** node. You use this node when your end users preregister. For more information, refer to Prerequisites.

Copyright © 2025 Ping Identity Corporation

Parameter	Description
`credentials`	Optional. Determines whether user credentials are sent to Ping. You must configure the journey to support the validation of the user credentials. To enable sending credentials, the value should be `true`. To disable the sending of credentials, set the value to `false`.
`ssourl`	Optional. The URL of the journey that checks for a session and redirects the user, after successfully logging in to their Mac, to an end user portal. By default, this parameter is empty and no browser opens after login. For example, the URL to the journey could be `https://test.forgerock.com/enduser/am/XUI/?realm=alpha&authIndexType=service&authIndexValue=wks-sso&ForceAuth=true`. The **Success URL** node in that journey could be `https://test.forgerock.com/enduser/?realm=alpha#/dashboard`. For an example of this journey, refer to the SSO journey.
`ssobrowser`	Optional. Determines the browser that opens when the `ssourl` parameter is defined. Select one of the following values: • `system`: Uses the default browser configured on the machine. • `firefox` • `safari` • `chrome`

Note

Configure the `ssourl` and `ssobrowser` parameters if you want an SSO portal to automatically open on the end users machine upon login.

An example of the XML file completed is:

Copyright © 2025 Ping Identity Corporation

```
<?xml version="1.0" encoding="UTF-8"?>
<octopus>

    <!-- ********************************************************************************** -->
    <!-- ***  REQUIRED                                                                  *** -->
    <!-- ********************************************************************************** -->

    <server>https://test.forgerock.com/am</server>
    <realm>alpha</realm>
    <tree>wks-push</tree>
    <otpdigits></otpdigits>
    <credentials>true</credentials>


    <!-- ********************************************************************************** -->
    <!-- ***  OTHERS                                                                    *** -->
    <!-- ********************************************************************************** -->
    <!--
        Logging (default: 'info')

        Controls the number and verbosity of logging messages written by Octopus for Mac.

        The valid values for this setting are (in order of increasing verbosity):
            * none
            * error
            * info
            * debug

        Note that no passwords, encryption keys or any other secrets are ever written in
        any of the above logging levels.
    -->
    <logging>info</logging>


    <!-- ********************************************************************************** -->
    <!-- ***  SINGLE SIGN ON                                                            *** -->
    <!-- ********************************************************************************** -->

    <ssourl>https://test.forgerock.com/am/XUI/?realm=alpha&amp;authIndexType=service&amp;authIndexValue=wks-
sso&amp;ForceAuth=true</ssourl>
    <ssobrowser>safari</ssobrowser>

</octopus>
```

Install Mac Workstation Authentication

Once you configure the XML file, the Mac Workstation Authentication is ready for installation.

To install the client on your user's workstation, utilize the following options:

- As an administrator, manually install the client on the machine.
- Utilize a deployment tool for Macs, such as Jamf. This method is recommended for large deployments.

The steps that follow explore the manual configuration of Mac Workstation Authentication on a machine. When using a deployment tool, adjust the steps and settings accordingly.

Copyright © 2025 Ping Identity Corporation

To install Mac Workstation Authentication:

1. As an Administrator, run the `WorkstationAuthenticationForMac.pkg` file to open the installer.
2. On the **Introduction** page, click **Continue**.
3. On the **Installation Type** page, click **Install**.

   You might be prompted to enter credentials.
4. Click **Ok** to allow the software to access the required locations. You are prompted to do this twice.
5. A pop-up screen to enable Mac Workstation Authentication for the logged-in user appears. To configure this now, click **Enable Workstation Authentication**. For more information, refer to Onboard local users.

   To set up later for yourself (or another user), click **Not Now**.
6. Click **Close** to exit the installation setup.
7. Verify the installation by locating the Ping icon in the top right of the menu bar. This shows that the Mac Workstation Authentication is running in the background.

   To access Mac Workstation Authentication settings at any time, click the logo and click **Open Workstation Authentication Preferences...**.

> **Note**
>
> After you enable Mac Workstation Authentication, the end user is prompted to set up Mac Workstation Authentication when logging into their machine.

Mac Workstation Authentication installation/configuration checklist

- Download and install the binaries from Backstage (you must be logged in).
- Install the Mac client on end users machines.
- ☐ (Optional). Onboard and enable local users on their Mac machine.
- ☐ (Optional). Enable Offline OTP to allow users to login to their Mac when not connected to the internet.
- ☐ Verify and test with a test user.

Onboard local users

If there are local (non-domain) users, for example, users not in AD, then those users must be manually enabled before they can log into their workstation using Mac Workstation Authentication.

To onboard a local user:

1. Log into the Mac as a local user.

Copyright © 2025 Ping Identity Corporation

2. Click the Ping icon in the top right of the menu bar.
3. Click **Enable For This User...**.
4. Enter the user's username in the **Account** field and click **Next**.
5. Enter the user's Mac credentials.
    1. If you are using the push MFA method, after you validate the Mac credentials, a notification is sent to the ForgeRock Authenticator application to approve.
    2. If you are using the OATH OTP MFA method, **put the OTP code** from the ForgeRock Authenticator application right after the password in this step.

       Failure to do this will result in the end user not being registered.

Mac Workstation Authentication installation/configuration checklist

Download and install the binaries from Backstage (you must be logged in).

Install the Mac client on end users machines.

(Optional). Onboard and enable local users on their Mac machine.

☐ (Optional). Enable Offline OTP to allow users to login to their Mac when not connected to the internet.

☐ Verify and test with a test user.

Enable Offline OTP

Offline OTP is performed by the user.

After a user is configured to use Mac Workstation Authentication, the user can enable **Offline OTP**.

This option provides the ability to for users to authenticate to their Mac when they are not connected to a network or their machine cannot access the Ping environment.

> **Note**
>
> Users must download the ForgeRock Authenticator application to their smartphone via the Apple store or Google Play store to set up Offline OTP.

To enable **Offline OTP**:

1. Click the Ping icon in the top right of the menu bar and click **Open Workstation Authentication Preferences...**.

   > **Note**
   >
   > You can also access the **Workstation Authentication** application by opening it in **Finder**.

2. From the Mac Workstation Authentication application screen, click **Manage** to launch the offline login wizard.
3. After the wizard opens, click **Setup**.

Copyright © 2025 Ping Identity Corporation

4. When prompted, enter your password in the dialog.
    1. If the push notification MFA method has been set up, approve the push notification on your phone.
    2. If the OATH OTP MFA method was set up, append the OTP to the end of your password with no spaces in between.
5. Scan the QR code that is presented on the screen with you ForgeRock Authenticator application.
6. Enter the OTP from the newly created profile in your ForgeRock Authenticator application to the screen titled **Verify Your Code**. Note the name of the profile in the application for later reference.
7. To exit the wizard, click **Done**.

Login with Offline OTP

After you enable and configure **Offline OTP**, you are ready to log in using this method.

To login using the **Offline OTP** MFA method:

1. Enter your password to your Mac.
2. In the password box (right after you enter the password with no space in between the password and OTP) enter the OTP from the ForgeRock Authenticator application.
3. Press **Enter**.

Mac Workstation Authentication installation/configuration checklist

Download and install the binaries from Backstage (you must be logged in).

Install the Mac client on end users machines.

(Optional). Onboard and enable local users on their Mac machine.

(Optional). Enable Offline OTP to allow users to login to their Mac when not connected to the internet.

☐ Verify and test with a test user.

Verify functionality

Following installation, configuration, and deployment (on a test machine first), it is recommended to test the functionality of workstation authentication to verify that the Mac login process proceeds as expected.

Before beginning the verification process, make sure that the following prerequisites are met:

- User to be tested has a smartphone with the ForgeRock Authenticator application installed.
- User to be tested has been successfully enrolled to the relevant journey depending on the method chosen (push notification or OATH OTP) as described in Install Mac Workstation Authentication.
- The **Ping Server URL**, as defined in the xml file, is accessible from the test machine.
- Mac Workstation Authentication has been enabled for the account on the Mac machine.

There are two MFA methods an administrator can enable for Mac Workstation Authentication. Only one can be selected.

Copyright © 2025 Ping Identity Corporation

The methods are:

- Push notification using the ForgeRock Authenticator application
- OATH OTP using the ForgeRock Authenticator application

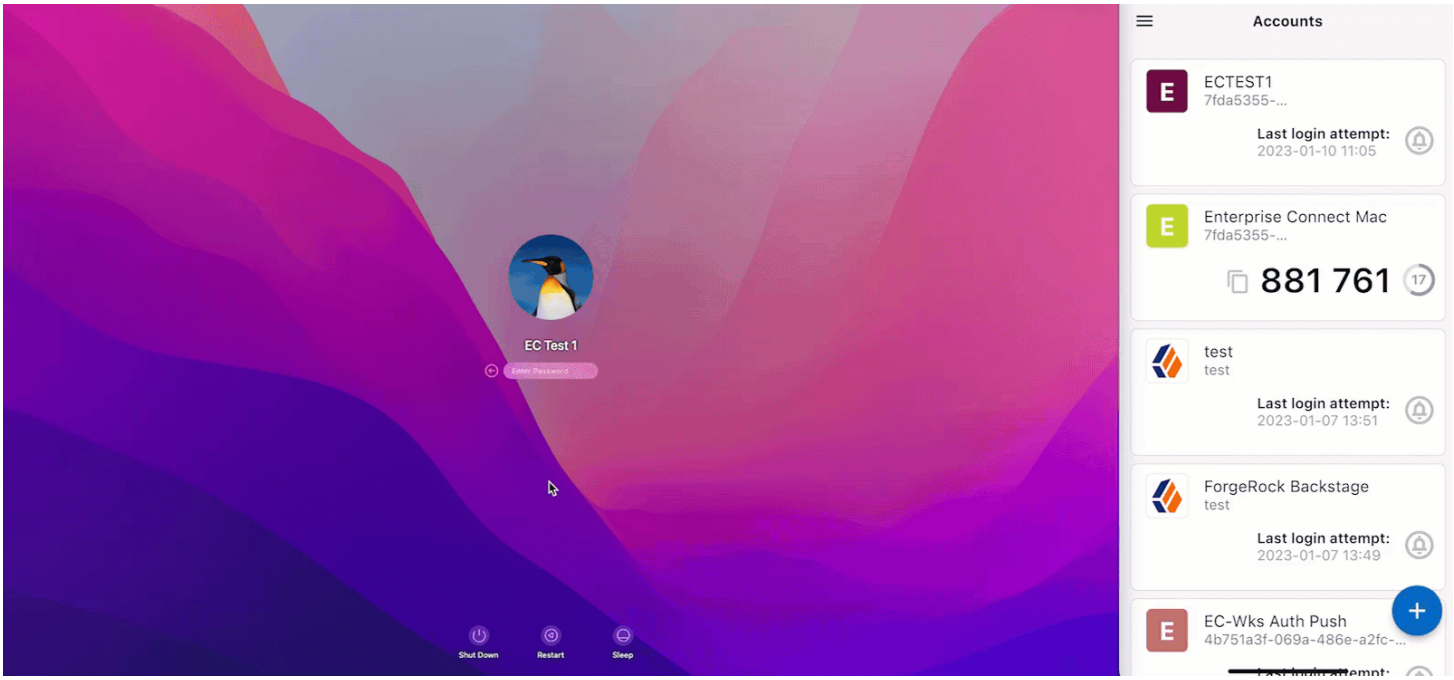
Offline OTP can also be enabled for either of these methods. For more information on this, refer to Enable Offline OTP.

The following sections show how to test these methods.

Validate push notification MFA method

You configure the push notification MFA method when you Install Mac Workstation Authentication.

To log in to your Mac with this method:



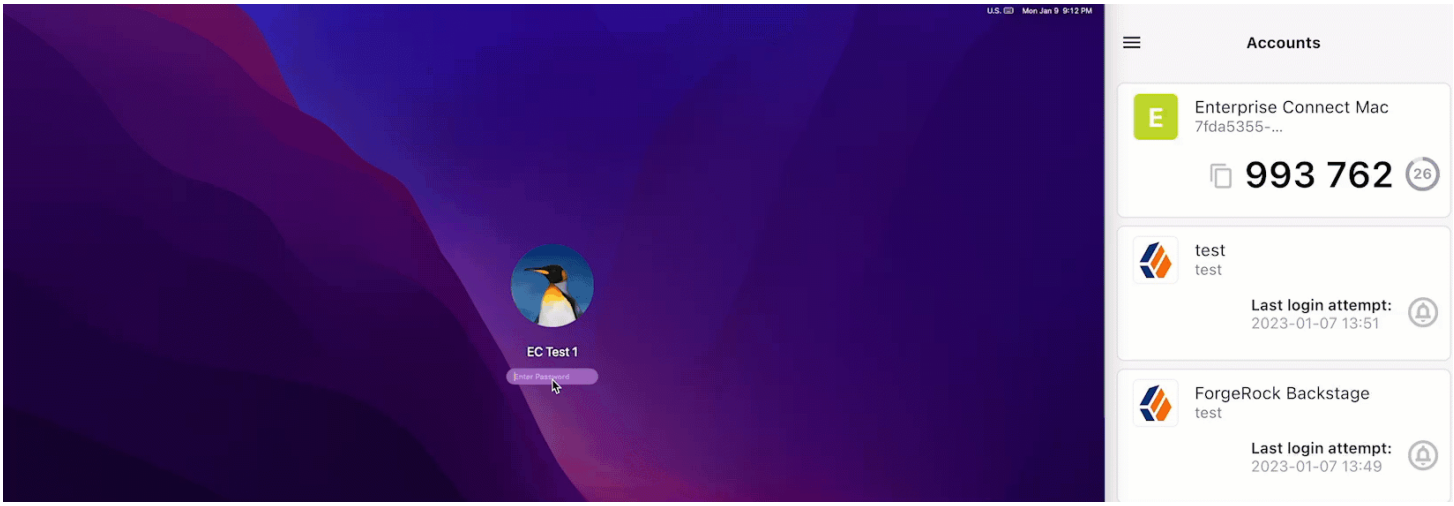
1. Access the Mac login screen.
2. Enter the username and password for the user.
3. Approve the push notification sent to the ForgeRock Authenticator application.
4. You are successfully logged in.

Validate OATH OTP MFA method

You configure the OATH OTP MFA method when you Install Mac Workstation Authentication.

To log in to your Mac with this method:

Copyright © 2025 Ping Identity Corporation



1. Access the Mac login screen.
2. Enter the username and password for the user.
3. Right after you enter the password, input the OTP from the application immediately (with no spaces in between).
4. You are successfully logged in.

Mac Workstation Authentication installation/configuration checklist

Download and install the binaries from Backstage (you must be logged in).

Install the Mac client on end users machines.

(Optional). Onboard and enable local users on their Mac machine.

(Optional). Enable Offline OTP to allow users to login to their Mac when not connected to the internet.

Verify and test with a test user.

Additional reference

The subsequent sections explore additional features of Mac Workstation Authentication:

- Perform Mac Workstation Authentication upgrade
- Log files
- Modify Mac Workstation Authentication

Perform Mac Workstation Authentication upgrade

When substantial updates are released in a newer version of Mac Workstation Authentication, you need to upgrade.

Copyright © 2025 Ping Identity Corporation

Upgrade Mac Workstation Authentication

> **Caution**
>
> When you upgrade Mac Workstation Authentication, run the `.pkg` file over the existing installation. Do not uninstall the older version as this would require end users to re-enable Mac Workstation Authentication.

1. Download the binary from Backstage to the machine(s) that require an upgrade.
2. Configure the XML file for the new version as described in configure the `XML` file.
3. Install the new version as described in install Mac Workstation Authentication.

> **Note**
>
> For larger deployments, utilize a deployment tool, such as Jamf to upgrade.

Log files

Mac Workstation Authentication logs various items, such as installation activities and authentication events.

To access the log file:

1. Click the Ping icon in the top right of the menu bar and click **Open Workstation Authentication Preferences...**.

   > **Note**
   >
   > You can also access the **Workstation Authentication** application by opening it in **Finder**.

2. Click **Help**.
3. In the **Troubleshooting** section, click **View logs**.

   > **Tip**
   >
   > You can also access the log file directly via the terminal at `/var/log/octopus.log`.

Modify Mac Workstation Authentication

After you install and configure Mac Workstation Authentication, there are many cases in which you will need to modify the configuration.

These items include:

- How to modify configuration files post installation.
- How to uninstall Mac Workstation Authentication.

Modify configuration files post installation

When Mac Workstation Authentication is installed, configurations are set at the system level, and when user(s) enable Mac Workstation Authentication on their account, at the user level. **Do not modify** the configurations after the installation.

Copyright © 2025 Ping Identity Corporation

> **Caution**
>
> If you need to modify the xml file for Mac Workstation Authentication, run the `.pkg` file over the existing installation. Do not uninstall Mac Workstation Authentication as this would require the end users to re-enable Mac Workstation Authentication.

Instead, install Mac Workstation Authentication over the existing installation:

1. Configure the xml file.
2. Reinstall Mac Workstation Authentication following the steps in Install Mac Workstation Authentication.

> **Note**
>
> For larger deployments, utilize a deployment tool, such as Jamf to update the xml file.

Uninstall Mac Workstation Authentication

To uninstall the client:

1. Click the Ping icon in the top right of the menu bar and click **Open Workstation Authentication Preferences...**.

   > **Note**
   >
   > You can also access the **Workstation Authentication** application by opening it in **Finder**.

2. Click **Help**.
3. In the **Uninstall** section, click **Uninstall**.
4. Enter an administrator's credentials to uninstall.

Copyright © 2025 Ping Identity Corporation

Enterprise Connect Passwordless overview

Add-on

Ping Enterprise Connect Passwordless is an add-on capability available for purchase for PingOne Advanced Identity Cloud and self-managed versions of PingAM. Contact your Ping representative for more details on how this capability can enhance your organization's security posture.

Note

For more information on concepts and high-level information, refer to passwordless overview.

Ping Enterprise Connect Passwordless enables your organization to move towards passwordless in a conscious, phased-approach.

Enterprise Connect Passwordless is developed through Ping's strategic partnership with Secret Double Octopus (SDO).

When integrated into PingOne Advanced Identity Cloud/Ping Identity Platform, it:

- Protects the most commonly used and vulnerable organization resources such as servers, workstations, remote desktops, and VPNs.
- Helps large enterprises proactively defend against cyber-attacks, and unauthorized access by providing a passwordless experience to legacy applications, systems and services.

This can be through one or a combination of the following:

- Passwordless factor - Use a passwordless method, such as a push notification or a one-time passcode (OTP), as an additional authentication factor beyond a password. This is also referred to as a second-factor or multi-factor authentication.
- Passwordless experience - Remove the password from the user experience and perform any password-based authentication securely in the background.

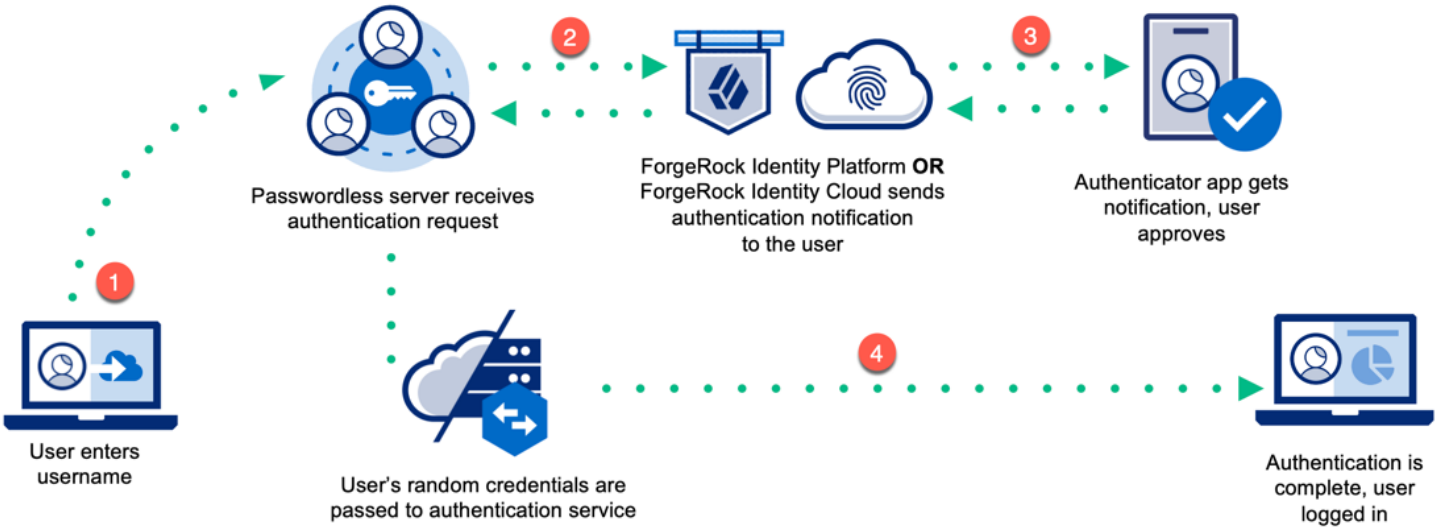
  For example, your legacy system may require passwords for authentication, or they cannot accommodate the new technologies/protocols a complete passwordless state needs. In this scenario, opting for the passwordless experience is what you need. Using Enterprise Connect Passwordless's passwordless experience, the passwords rotate securely in the background, without the user needing to know their password. This improves the user experience while increasing the overall security of your organization and allows you to continue on the journey of passwordless using Enterprise Connect Passwordless.
- Complete passwordless - Eliminate the need for passwords completely by authenticating users using passwordless factors or private-key cryptography.

Copyright © 2025 Ping Identity Corporation

Most organizations find themselves using a combination of all three authentication methods. Enterprise Connect Passwordless gives you the tools to achieve passwordless every step of the way.

In many scenarios, this means using the passwordless experience for managed devices.

The following is a typical scenario of Enterprise Connect Passwordless, focusing on the passwordless experience.



Copyright © 2025 Ping Identity Corporation

Implement Enterprise Connect Passwordless

Enterprise Connect Passwordless uses various systems and process to operate.

Typical steps are:

- Installation of the management console (MC) servers
- Installation of authentication server(s) (AS)
- Configuration of the servers.
- Connection and use of a user store, such as Active Directory (AD) or PingOne Advanced Identity Cloud for the AS to sync identities with.
- Connection to and use of an PingOne Advanced Identity Cloud tenant or PingAM environment.

To use Enterprise Connect Passwordless, you must:

1. Install the Enterprise Connect Passwordless Servers.
2. Configure the Enterprise Connect Passwordless Servers.
3. Configure Ping journeys to use with passwordless.

   The journeys you configure correspond to the Ping specific configurations when you configure the Enterprise Connect Passwordless Servers (step 2) or when you configure the passwordless agents (step 4).

   There are sample journeys defined in the Enterprise Connect Windows Workstation Authentication documentation. These journeys are specific to Enterprise Connect Windows Workstation Authentication; however, they can be used as a reference when creating your journeys. Depending on your deployment, additional integration patterns such as Ping pass-through authentication could be required. For more information, refer to Create authentication journey(s).

   For more information on journeys for PingOne Advanced Identity Cloud, refer to PingOne Advanced Identity Cloud journeys.

   For more information on journeys for PingAM, refer to PingAM journeys.
4. Configure any of the following passwordless agents for managed devices:
   - Enterprise Connect Passwordless Windows Agent (ECP Windows Agent)
   - Enterprise Connect Passwordless Mac Agent (ECP Mac Agent)
5. Deploy the agent(s) using your preferred software to managed devices.

Copyright © 2025 Ping Identity Corporation

Servers

Install Enterprise Connect Passwordless Servers

Enterprise Connect Passwordless requires you install servers on-premise.

These servers include:

- **Management Console server (MC)** - An administrative console that:
  - Provides a place for configurations and the management of users and devices
  - Communicates with the authentication server

  When created, it can contain its own local database or you can connect your own.
- **Authentication server (AS)** - Deployed on the enterprise domain. It is configured to access the directory service (user store) and work with relying parties. It is configured through the MC.
- **Authentication server in DMZ (DMZ)** - The Authentication Server DMZ may be required in the DMZ if there are configurations where users need authentication to services while outside the enterprise's network, and you do not want to use a VPN connection.

  In this installation option, you must have two or more Authentication Servers inside your network and at least one server in the DMZ.
- **All-in-One server (AIO)** - Use the AIO server option **only** for proof-of-concept (POC) environments. This option installs the MC, an AS, and a database in a single installation process.

For production deployments, install the MC and AS separately. The database may be created as part of the MC installation, or it can be configured later by the administrator as the first step of the MC configuration.

> **Note**
>
> For larger scale deployments, install each component on a separate server. Make sure to use distributed architecture where each component is installed twice on at least two servers. This supports high availability in case of failure of one of the components.

Guides

For installation instructions of the Enterprise Connect Passwordless Servers, refer to the following table:

Version	PDF
Enterprise Connect Passwordless Server 5.8.2	5.8.2 install guide

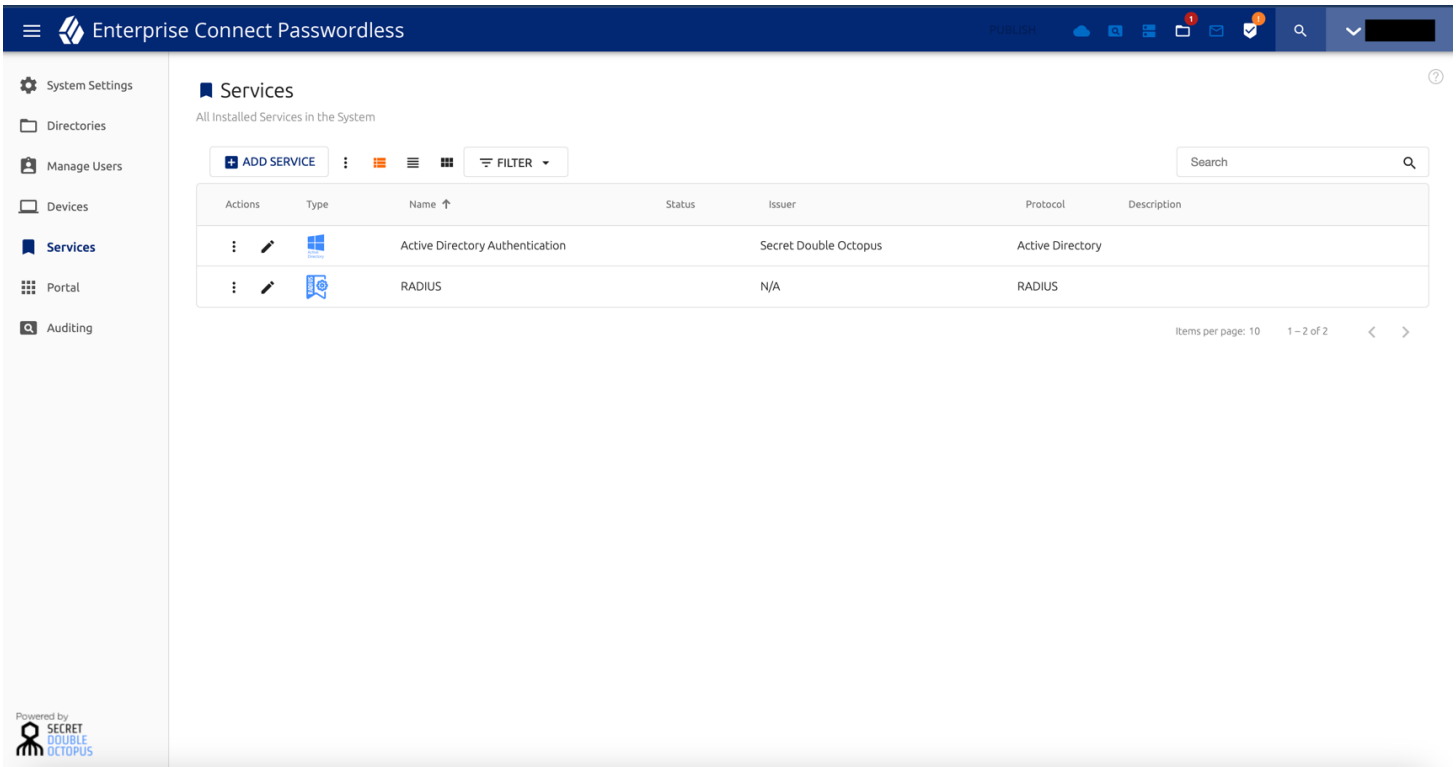
Copyright © 2025 Ping Identity Corporation

Version	PDF
Enterprise Connect Passwordless Server 5.4.8	5.4.8 install guide
Enterprise Connect Passwordless Server 5.4.4	5.4.4 install guide

Configure the management console

The management console (MC) is the central place to manage settings, devices, and users for Enterprise Connect Passwordless.

> **Note**
>
> For information on installing the management console server, refer to Install Enterprise Connect Passwordless Servers.



It enables you to configure and manage:

- System settings: Enables you to view and update system configuration settings, such as authenticators, mail server settings, and more.
- Directories: Allows you to integrate corporate directories with the system and configure settings for each directory.
- Manage users: Lists your users according to their associated directories and enables you to add, remove, and perform other administrative actions on users.
- Devices: Lists the workstations in the system, provides detailed information about them and allows you to perform administrative operations on them.

Copyright © 2025 Ping Identity Corporation

- Services: Lists the services integrated with the MC and enables you to add and update services.
- Portal: Allows you to control settings for the user portal.
- Auditing: Displays a log of every administrative action performed by the system or by users.

Guides

For configuration instructions of the MC, refer to the following table:

Version	PDF
Enterprise Connect Passwordless Server 5.8.2	5.8.2 MC guide
Enterprise Connect Passwordless Server 5.4.8	5.4.8 MC guide
Enterprise Connect Passwordless Server 5.4.4	5.4.4 MC guide

Upgrade Enterprise Connect Passwordless Servers

To upgrade from a previous version of Enterprise Connect Passwordless Servers to 5.4.8, refer to page 20 in the 5.4.8 install guide.

Copyright © 2025 Ping Identity Corporation

ECP Windows Agent

You must install and configure Enterprise Connect Passwordless Servers before you can configure and deploy the Enterprise Connect Passwordless Windows Agent.

Ping and SDO replace passwords altogether with a high assurance, password-free authentication paradigm.

Using Enterprise Connect Passwordless Windows Agent (ECP Windows Agent) Windows Credential Provider in conjunction with standard interfaces to Active Directory (AD), the password-free solution seamlessly replaces AD passwords with a stronger, more secure alternative. As a result, the security posture of the AD domain is enhanced, user experience and productivity improve, and password management costs are dramatically lowered.

Guides

For installation instructions of the ECP Windows Agent, refer to the following table:

Version	PDF
Enterprise Connect Passwordless Windows Agent 3.9.3	3.9.3 install guide
Enterprise Connect Passwordless Windows Agent 3.8.4	3.8.4 install guide
Enterprise Connect Passwordless Windows Agent 3.8.2	3.8.2 install guide

Copyright © 2025 Ping Identity Corporation

ECP Mac Agent

You must install and configure Enterprise Connect Passwordless Servers before you can configure and deploy the Enterprise Connect Passwordless Mac Agent.

Using the Enterprise Connect Passwordless Mac Agent (ECP Mac Agent) authentication provider in conjunction with standard interfaces to Active Directory (AD), this password free solution seamlessy replaces AD passwords with a stronger, more secure alternative.

As a result, you can do the following:

- Enhance the security posture
- Improve user experience
- Improve productivity
- Lower password management costs

Guides

For installation instructions of the ECP Mac Agent, refer to the following table:

Version	PDF
Enterprise Connect Passwordless Mac Agent 2.7.1	2.7.1 install guide
Enterprise Connect Passwordless Mac Agent 2.6.7	2.6.7 install guide

Copyright © 2025 Ping Identity Corporation