PingOne Advanced Services

June 11, 2025

PINGONE ADVANCED SERVICES

Table of Contents

PingOne Advanced Services

PingOne Advanced Services

PingOne Advanced Services is a powerful solution that simplifies identity management for enterprise organizations by providing them with full cloud services, without compromising security or system performance.

Release Notes

- Release notes

Get Started with PingOne Advanced Services

- Introduction to PingOne Advanced Services
- Comparison: PingOne Advanced Services and PingOne Cloud Platform
- Environments
- Network guide
- Limitations guide
- Monitoring and logging
- Penetration and load testing policy

Use PingOne Advanced Services

- How PingOne Advanced Services works
- Signing on to the platform
- Configuring connections for SSO
- Renewing Let's Encrypt certificates
- PingOne Advanced Services task summary table
- Self-service
- Service requests

PingOne Advanced Services

Learn More

- PingOne Platform
- PingOne Advanced Services Community

PingOne Advanced Services Release Notes

Review release notes for PingOne Advanced Services.

May 2025

Platform version: 2.1.0. Updated May 22, 2025.

In this platform version:

- PingAccess deploys with version 8.2.0 instead of 8.0.6. You can find details regarding this release in the PingAccess 8.2.0 release notes.
- PingCentral deploys with version 2.2.0 instead of 2.0.2. You can find details regarding this release in the PingCentral 2.2.0 release notes.

These applications are also included:

- PingFederate 12.1.6
- PingDirectory 10.0.0.4
- PingDataSync 10.0.0.2
- Delegated Admin 5.0.0

Use OAuth to access the PingAccess Admin API

New

You can configure the PingAccess Admin API so that administrators can access it using OAuth. The API requires a JWT Bearer token for authenticating the requests. This token can be retrieved using either an authorization code flow or a client credentials flow.

Learn more about setting up these flows in Setting up OAuth to access the PingAccess Admin API. If you choose to use a client credentials flow, connections must be correctly configured for self-managing administrator accounts. Learn more in Configuring connections for SSO.

> **Note**
>
> For improved security, basic authentication for the PingAccess Admin API has been deprecated and will be removed in PingOne Advanced Services version 2.2.

LDAPS custom domains now supported

Improved

PingDirectory LDAPS URLs are now routed through NGINX, which has improved system flexibility and supports custom domains.

Automated certificates for global DNS domains now available

Improved

Those using Let's Encrypt certificates to ensure that communications between PingOne Advanced Services products and services remain encrypted and secure (used by default), can now create automated certificates for global DNS domains.

Logging improvements

Improved

Internal log pipeline stability improvements have been made, which will further help you observe and maintain your system.

April 2025

Platform version: 2.0.1. Updated April 30, 2025.

In this platform version:

- PingFederate deploys with version 12.1.6 instead of 12.1. You can find details regarding this release in the PingFederate 12.1.6 release notes.
- PingAccess deploys with version 8.0.6 instead of 8.0.4. You can find details regarding this release in the PingAccess 8.0.6 release notes.
- PingDirectory deploys with version 10.0.0.4 instead of 10.0.0.2. You can find details regarding this release in the PingDirectory 10.0.0.4 release notes.

These applications are also included:

- PingDataSync 10.0.0.2
- Delegated Admin 5.0.0
- PingCentral 2.0.2

December 2024

Platform version: 2.0.0. Updated December 20, 2024.

In this platform version, PingFederate deploys with version 12.1 instead of 11.3.8. You can find details regarding this release in the PingFederate 12.1 release notes.

These applications are also included:

- PingAccess 8.0.4
- PingDirectory 10.0.0.2
- PingDataSync 10.0.0.2
- Delegated Admin 5.0.0
- PingCentral 2.0.2

Self-service API Beta now available

New

You and your administrators can now create and update virtual host certificates and TLS configurations yourselves through a self-service API. Configurations are automatically replicated to child regions in PingOne Advanced Services for the following applications:

- PingFederate
- PingFederate Admin API
- PingAccess
- PingAccess Admin API
- PingAccess Agents
- PingDirectory
- Delegated Admin

Learn more in Creating and updating virtual hosts.

If you don't want to create or update virtual hosts yourself, you can still submit a service request. Select **Advanced/Other** as your requested capability, provide a detailed description of your needs, and submit your request to the Support team.

Note that if you've already configured connections for SSO, you'll need to add the **SelfService** attribute. Learn more in Creating custom user attributes. Then, update the application with the appropriate attribute mappings.

November 2024

Platform version: 1.19.2.0. Updated November 21, 2024.

In this platform version:

- PingAccess deploys with version 8.0.4 instead of 8.0.3. You can find details regarding this release in the PingAccess 8.0.4 release notes.
- PingCentral deploys with version 2.0.2 instead of 2.0.1. You can find details regarding this release in the PingCentral 2.0.2 release notes.

These applications are also included:

- PingFederate 11.3.8
- PingDirectory 10.0.0.2
- PingDataSync 10.0.0.2
- Delegated Admin 5.0.0

Indexed log file retention policy change

Info

With the release of platform version 1.19.0.0, we announced that we've replaced Elasticsearch with OpenSearch because OpenSearch provides a larger and more innovative feature set. As part of the 1.19.2.0 log adjustments, we will now have indexed logs available for a rolling 30-day window. This change will be rolled out to all platform versions of P1AS starting on Feb 1st. Log files older than 30 days will be unavailable and will remain in our internal archive.

Many of you have your own Security Information and Event Management (SIEM) systems and your own ways of storing, indexing, and searching your log files, so you won't be affected by this change. The same is true if you receive a copy of your logs through a customer endpoint. Your log files can remain on your endpoint systems for the amount of time specified in your retention policies.

Otherwise, this change in policy means that:

- If you're upgrading to version 1.19.2.0, your Elasticsearch data will not be directly migrated into OpenSearch. Instead, only new logs will be processed after the upgrade and be available in your new OpenSearch dashboard when the upgrade is complete.
- If you're using platform version 1.19.0.0, this change will occur on February 1, 2025. On that day, you'll notice that your Kibana or OpenSearch dashboards will only display indexed log files for a rolling 30-day window.

If you want to have indexed log files for more than 30 days, we recommend that you add your own customer-managed endpoint, or use your own SIEM system to store and manage your log files.

To have your logs sent to a SIEM system or other customer endpoint, submit a service request through the Support Portal. Learn more about submitting this type of request in Platform service requests > SIEM integration.

September 2024

Platform version: 1.19.1.0. Updated September 11, 2024.

In this platform version:

- PingFederate deploys with version 11.3.8 instead of 11.3.6. You can find details in the PingFederate 11.3.8 release notes.
- PingAccess deploys with version 8.0.3 instead of 8.0.1. You can find details regarding this release in the PingAccess 8.0.3 release notes.
- OpenSearch and OpenSearch Dashboards were also upgraded from version 2.8.0 to 2.11.1. You can find details in the OpenSearch and OpenSearch Dashboards 2.11.1 release notes.

These applications are also included:

- PingDirectory 10.0.0.2
- PingDataSync 10.0.0.2
- Delegated Admin 5.0
- PingCentral 2.0.1

Administrators can self-service their administrator SSO accounts

New

You can now set up and configure connections between environments that will allow your administrators to use single sign-on (SSO) to access the PingOne Advanced Services platform and the appropriate admin consoles. Learn more in Configuring connections for SSO.

May 2024

Platform version: 1.19.0.0. Updated May 6, 2024.

In this platform version:

- PingAccess deploys with version 8.0.1 instead of 7.07. You can find details regarding this release in the PingAccess 8.0.1 release notes.
- PingDirectory deploys with version 10.0.0.2 instead of 9.2.0.4. You can find details regarding this release in the PingDirectory 10.0.0.2 release notes.
- PingCentral deploys with version 2.0.1 instead of 1.10.1. You can find details regarding this release in the PingCentral 2.0.1 release notes.

These applications are also included:

- PingFederate 11.3.5
- PingDataSync 10.0.0.1
- Delegated Admin 5.0

Elasticsearch replaced by OpenSearch

Improved

After careful consideration over several years, PingOne Advanced Services has replaced Elasticsearch with OpenSearch, an open source branch of Elasticsearch. OpenSearch provides a much larger and innovative feature set that enables a better path forward for continuing to provide log indexing, search, alerting, single sign-on (SSO), custom dashboards, and role-based access.

Elasticsearch data will not be directly migrated into OpenSearch. Instead, only new logs will be processed during the upgrade to platform version 1.19.0.0 and will be available in your new OpenSearch dashboards. We retain 13 months worth of raw log files, and can reprocess up to 3 months of these files into OpenSearch to allow indexed searches of limited historical data, upon request.

This change should not affect logs sent to your SIEM systems, such as Splunk. Log processing pipelines for your endpoints will remain the same, and logs sent to these endpoints will remain in a raw format for you to process.

Kibana Data Views have also been expanded. Each log generated by an app will now have its own data view, which makes it much easier to know where your logs are based on the name of the log file generated by the app. Custom dashboards will need to be exported as JSON files before the upgrade, and after the upgrade, imported into OpenSearch Dashboards and updated to reflect the changes in the new data views. The change to the data views might also require that you update the dashboard panels with the name of the new data view that previously contained the logs of interest.

PingDirectory improvements

Improved

Several improvements were made to PingDirectory:

- You can now enable database cache sharing for deployments with multiple backend databases. You can find details in the PingDirectory 10.0.0.0 release notes.
- When deployed with multiple backend databases, PingDirectory now performs better than before because preloading has been disabled.
- PingDirectory pod IPs availability and propagation to DNS have been improved for multi-region support.
- PingDirectory pods graceful shutdown has been improved and now uses an on-premise software-aligned stop-server script to terminate pods.

OnePingLogin

Improved

The PingFederate admin console, PingAccess admin console, ArgoCD, and OpenSearch SSO has been improved to reduce the number of multi-factor authentications.

CAP permissions have also been improved to support additional fine-grained controls over user permissions. Now, users sign on using SSO to access their OpenSearch, PingFederate, or PingAccess environments. The tasks they can perform depend on the administrative roles they are assigned. By default, CAP users will not have any PingFederate or PingAccess roles assigned to them and must submit a service request to request the appropriate roles and permissions.

> **Note**
>
> This authentication experience is configured in the PingAccess and PingFederate authentication settings. Changing these settings to use a non-default token provider might delay support because it introduces additional authentication steps for Ping Identity operations resources to review.

PingFederate and PingAccess administrator roles provide fine-grained access to features that allow them to perform specific tasks.

PingFederate administrator roles

- **User Admin**: Those with this role can add and remove users, change and reset passwords, and install replacement license keys.
- **Admin**: Those with this role can configure partner connections and most system settings, but they cannot manage local accounts or handle local keys and certificates.
- **Expression Admin**: Those with this role can map user attributes using Object-Graph Navigation Language (OGNL).

> **Note**
>
> Only administrators who have both the Admin role and the Expression Admin role can be granted:
> - The User Admin role. This restriction prevents non-Expression Admins from granting themselves the Expression Admin role.
> - Write access to the file system or directory where PingFederate is installed. This restriction prevents a non-Expression Admin user from placing a `data.zip` file containing expressions into the `<pf_install>/pingfederate/server/default/deploy` directory, which would introduce expressions into PingFederate.]

- **Crypto Admin**: Those with this role manage local keys and certificates.
- **Auditor**: Those with this role have view-only privileges.

PingAccess administrator roles

- **Administrator**: Those with this role can access all features unless someone is assigned the Platform Administrator role. If that role is assigned, the Administrators can't update authorization, user, or environment settings, but can access everything else.
- **Platform Administrator**: Those with this role can access everything that an Administrator can access, but they can also update authorization, user, and environment settings and configurations. Use this role in conjunction with the Administrator role to prevent accidental lockouts.
- **Auditor**: Those with this role have view-only privileges.

March 2024

Platform version 1.18.2.0. Updated May 23, 2024.

Product versions:

- In this platform version, PingFederate deploys with version 11.3.6 instead of 11.3.5. You can find details regarding the release in the PingFederate 11.3.6 release notes.
- In this platform version, PingAccess deploys with version 7.0.7 instead of 7.0.5. You can find details regarding this release in the PingAccess 7.0.7 release notes.

These applications are also included:

- PingDirectory 9.2.0.4 suite of products
- PingCentral 1.10

Platform version: 1.18.1.0. Updated March 27, 2024.

In this platform version, PingFederate deploys with version 11.3.5 instead of 11.3.3. You can find details regarding this release in the PingFederate 11.3.5 release notes.

These applications are also included:

- PingDirectory 9.2.0.4 suite of products
- PingAccess 7.0.5

- PingCentral 1.10

December 2023

Platform version: 1.18.0.0

In this platform version:

- PingFederate deploys with version 11.3.3 instead of 11.1.8. You can find details regarding this release in the PingFederate 11.3.3 release notes.
- The PingDirectory suite of products deploys with version 9.2.0.4 instead of 9.2.0.2. You can find details regarding this release in the PingDirectory 9.2.0.4 release notes.

These applications are also included:

- PingAccess 7.0.5
- PingCentral 1.10
- Delegated Admin 4.10

Delegated Admin

New

Administrators can now upload and download user reports.

Prometheus

New

You can now access Prometheus metrics through a private link or VPN.

PingDirectory

Improved

Several improvements were made to PingDirectory:

- Backend priming no longer occurs when PingDirectory is started, which decreases PingDirectory startup time.
- PingDirectory restarts have also been enhanced with increased health checking to reduce the chance of data inconsistencies within the cluster.
- Backup and restore now occurs within its own `PersistentVolume`. Learn more in Backing up and restoring data in the PingDirectory documentation.

PingFederate

Improved

Kerberos authentication will no longer support RC4 encryption due to the use of the new 11.0.21 JDK version (which does not support this weak cipher). Any use of RC4 will need to be replaced with AES256 encryption.

Parsing improvement

Improved

Multi-line logs generated from `server.log` (PingFederate) now appear in Kibana as a single document.

ElasticSearch

Improved

A horizontal pod autoscaler was added and Logstash performance has improved. The number of warm nodes available has also been increased, which has improved performance and survives AZ failures.

Fluent Bit

Improved

Now leverages IMDSv2 security instead of IMDSv1.

Grafana

Improved

User authorization now displays in separate customer and internal teams views. Logging and alert metrics are also now available, but only to internal Ping Identity teams.

Storage class provisioner and EBS volume type changes

Improved

The StorageClass provisioner was changed to CSI, and the EBS volume type was changed to GP3, which will improve performance and stability.

Log file handling

Info

Our legacy logging mode (sending log files to Cloudwatch) has been removed, and log files are now sent to our internal ELK (Elasticsearch, Logstash, Kibana) stack or to a customer endpoint.

Kibana (1.18 only)

Info

Kibana logs older than 90 days must be dropped for the migration to the new StorageClass provisioner. However, raw PROD logs from this time period are still available in S3 but can be restored to Kibana via a service request after the upgrade. When searching indexes, results contain the same fields and data, regardless of which index is chosen. For example, `pf-audit*` and `logstash*` return the same results.

Argo CD

Info

Argo CD is now only deployed to the one per-region customer hub managing the development, staging, testing, and production environments.

October 2023

Platform version: 1.17.3.0.

The PingDirectory suite of products deploys with version 9.2.0.2 instead of 9.2. You can find details regarding this release in the PingDirectory 9.2.0.2 release notes.

These applications are also included:

- PingAccess 7.0.5
- PingCentral 1.10
- Delegated Admin 4.10
- PingFederate 11.1.8

September 2023

Platform version: 1.17.2.0.

PingFederate deploys with version 11.1.8 instead of 11.1.7. You can find details regarding this release in the PingFederate 11.1.8 release notes.

These applications are also included:

- PingAccess 7.0.5
- PingCentral 1.10
- PingDataSync 8.2.0.6
- Delegated Admin 4.10
- PingDirectory 9.2

July 2023

Platform version: 1.17.1.0.

PingFederate deploys with version 11.1.7 instead of 11.1.5. You can find details regarding this release in the PingFederate 11.1.7 release notes.

These applications are also included:

- PingAccess 7.0.5
- PingCentral 1.10
- PingDataSync 8.2.0.6
- Delegated Admin 4.10
- PingDirectory 9.2

March 2023

Platform version: 1.17.0.0.

PingDirectory deploys with version 9.2 instead of 9.0.0.2. You can find details regarding this release in the PingDirectory 9.2 release notes.

These applications are also included:

- PingAccess 7.0.5
- PingCentral 1.10
- PingDataSync 8.2.0.6
- Delegated Admin 4.10
- PingFederate 11.1.5

Dashboard consolidation

Improved

The PingOne Advanced Services dashboard has been enhanced. Not only does it provide a consolidated view of key indicators, metrics, and data regarding the health of your infrastructure, but you can now access all of your environments from this location instead of using separate URLs.

User interface updates

Improved

The PingOne Advanced Services user interface has also been updated to more closely match the look and feel of PingOne, which smooths the transition between the two.

November 2022

Platform version: 1.16.5.0.

These applications are included:

- PingAccess 7.0.5
- PingCentral 1.10
- PingDataSync 8.2.0.6
- Delegated Admin 4.10
- PingDirectory 9.0.0.2
- PingFederate 11.1.5

Provision and deprovision users for SaaS applications

New

Using PingOne Advanced Services, PingFederate administrators can now provision and deprovision users to the following software as a service (SaaS) applications:

- Slack
- Udemy
- Zscaler
- SCIM
- PingOne MFA

> **Note**
>
> In a multi-region deployment, SaaS provisioning is deployed to a single region, which is your primary region, and will not be deployed to your secondary region.

Performance metrics

Improved

You can now access up to 13 months of performance data that will help you better understand the activities occurring within your PingOne Advanced Services environments.

PingFederate patches now automatically updated

Improved

PingFederate patch versions are now automatically updated in PingOne Advanced Services.

September 2022

Platform version: 1.16.2.0.

PingOne Advanced Services deploys with PingFederate 11.1.5 instead of version 11.1.0. You can find details in the PingFederate 11.1.5 release notes.

These applications are also included:

- PingAccess 7.0.5
- PingCentral 1.10
- PingDataSync 8.2.0.6
- Delegated Admin 4.10
- PingDirectory 9.0.0.2

Kerberos gateway is also now supported.

Password policy added for topology administrators

Fixed

Having a password policy specifically for topology administrators prevents them from being affected when password expiration policies are applied to non-administrator accounts.

PingFederate dashboard revisions

Fixed

PingFederate **Failed SSO** and **Failed Authentication** dashboards have been revised to adjust to PingFederate 11.1 changes.

- The **Failed SSO** dashboard will not contain data if the **Fail Authentication on Account Lockout** option is disabled in PingFederate, which is the default.
- The **Failed Authentication** dashboard will not distinguish between SSO authentication requests and other types of authentication requests.

Additional time series data now available

Improved

Up to 13 months of Prometheus time series data is now available for you to compare current performance metrics with historical data to better understand their environments. Contact your Ping Identity representative for additional information about this option.

Active user numbers now available

Improved

The number of active users in each environment now displays on Grafana dashboards.

July 2022

Platform version: 1.16.1.1.

These applications are included:

- PingAccess 7.0.5
- PingCentral 1.10
- PingDataSync 8.2.0.6
- Delegated Admin 4.10
- PingDirectory 9.0.0.2
- PingFederate 11.1

Use PingCentral to configure PingFederate and PingAccess environments

New

PingCentral is now deployed with PingFederate and PingAccess environments. All of your development environments, (development, testing, staging, and production) will be configured for you and accessible from PingCentral.

Use PingFederate Admin API to create password credential validator and LDAP client manager

Fixed

You can now use the PingFederate Admin API to create the PingDirectory password credential validator and the LDAP client manager instead of using static XML. If the credential validator or client manager already exists, they will not be overwritten.

Hot and warm Elasticsearch index tiers added

Improved

Elasticsearch index lifecycle management (ILM) policies have been created, and a hot-warm-cold architecture has been implemented to improve performance and resiliency.

The indexer handles indexed data in a way that ages the data through several states. When the data is first indexed, it's added to a hot data tier and remains there for 90 days. Data nodes that are not actively written to are moved to a warm data tier, where they remain for 180 days. Data not accessed for more than 180 days is not indexed.

Health check services added

Improved

Health check services, which provide operational status and performance data, were recently added to monitor internal APIs and clusters.

Configurable log-streaming pipeline added

Improved

You can now use a variety of different security analytics services and customize the ways log data is streamed. You can filter streamed data by application, log, and keywords, and modify JSON files. Available security analytics services include:

- Customer S3 bucket
- Customer Cloudwatch ingestion
- Syslog
- IBM QRadar

May 2022

Platform version: 1.16.1.0.

These applications are included:

- PingAccess 7.0.5
- PingCentral 1.10
- PingDataSync 8.2.0.6
- Delegated Admin 4.10
- PingDirectory 9.0.0.2
- PingFederate 11.1

Synchronize all of your data sources into one source of truth

New

The PingDataSync Server is now available to synchronize the data from your on-premise and cloud-based data sources into PingDirectory, a high-performance, extensible LDAP directory that serves as the single source of identity truth.

PingOne LDAP gateway connectivity

New

PingOne LDAP gateway connectivity is now supported in the PingOne Advanced Services Simple Network option, which is significantly less time-consuming to deploy than the Advanced Network option that used to be required for LDAP connectivity.

RADIUS ports are now configured by default

Improved

Having these ports configured by default eliminates the need for our partners and professional services teams to manually configure them after deployment.

PingFederate thread usage auto-tuning enhanced

Improved

The PingFederate server thread usage auto-tuning feature has been enhanced to improve the user experience and reduce the need for manual tuning.

Custom password policies are now available through the admin portal

Improved

Now, not only can you request custom password policies through a service request form, but you can also request them through the admin portal.

JVM metrics are now available for PingFederate and PingAccess

Improved

The PingFederate and PingAccess tenant dashboards now display Java Virtual Machine (JVM) metrics, which you can use to optimize system performance.

March 2022

Platform version: 1.16.0.1.

These applications are included:

- PingAccess 7.0.5
- PingCentral 1.10
- PingDataSync 8.2.0.6
- Delegated Admin 4.9
- PingFederate 11.1.10

Web application firewall offers additional protection

Security

A Signal Sciences Web Application Firewall (WAF) was added to the platform to protect environments against vulnerabilities and mitigate DoS and DDoS attacks.

Log4j and Log4Shell security fixes

Security

This release contains several updates that address and remediate Log4j and Log4Shell vulnerabilities.

Updated Nginx ingress controller

Improved

The Nginx ingress controller was updated to the latest version, which provides access to the latest network security and performance functionality.

Updated dashboard and monitoring tools

Improved

NewRelic agent, Kibana, ElasticSearch, Logstash were updated to the latest versions available.

Added OpenToken Adapter

New

The OpenToken Adapter Kit was added to the PingFederate default profile.

Introduction to PingOne Advanced Services

PingOne Advanced Services is a powerful solution that simplifies identity management for enterprise organizations.

This solution provides organizations with full cloud services, without compromising security or system performance. Each organization has its own dedicated cloud environment in which all resources are isolated and only available to them. Their administrators can focus on configuring access policies to meet the organization's needs, while Ping Identity monitors and maintains the underlying platform and infrastructure.

By moving their resources to this powerful cloud solution, organizations can quickly:

- Provide secure seamless sign-on experiences — Having a highly customizable global authentication authority in place ensures that customers and workforce have simple, secure, and consistent sign-on experiences to their applications and resources.
- Comply with regulations — Many organizations handle confidential information, such as medical records, financial documents, and other sensitive data, and having a dedicated cloud infrastructure helps them comply with cloud-first and cloud-only mandates.
- Cut costs — Not only do organizations avoid large, upfront capital expenditures and lengthy procurement cycles for infrastructure and platform resources, but they also avoid paying for unused computing capacity and pay a fixed fee for their scalable service.
- Realize additional benefits — Designed with identity management best practices in mind, PingOne Advanced Services leverages cloud automation tools and capabilities, and allows organizations to automatically scale workloads to respond to business growth or surges in traffic without sacrificing performance. It also offers organizations the flexibility to determine which resources they will move to the cloud, and when migrations will occur.

Most importantly, this solution was designed for hybrid IT enterprise environments and can connect to everything, which makes it easy to migrate to PingOne Advanced Services. It uses open identity standards, like SAML, OAuth, and OpenID Connect (OIDC) to quickly onboard applications and can connect to legacy systems based on proprietary standards. This solution can also integrate with on-premise data or authentication sources, and act as either an identity provider or a service provider, which makes complex authentication flows possible and ecosystems even more secure.

Comparison: PingOne Advanced Services and PingOne Cloud Platform

As you're transitioning to the cloud, you might wonder which Ping Identity solution will best meet your needs. This comparison shows the differences between our two cloud platforms and is designed to help you select the best solution for your organization.

PingOne Cloud Platform	PingOne Advanced Services
With the PingOne Cloud Platform, your users access applications on a subscription basis and never have to download, install, or upgrade applications. PingOne is a software as a service (SaaS) solution that resides on a remote cloud network and can be accessed through the platform or APIs. The platform has a multi-tenancy SaaS architecture, which means that single instances of software and their supporting infrastructure serve multiple customers. It uses an organization-based model to define tenant accounts and their related entities within the platform and cannot be deployed as a single tenant. PingOne solutions can include any of these Ping Identity SaaS services: • PingOne SSO • PingDirectory • PingOne MFA / PingID • PingOne • PingOne Authorize (includes PingAccess capabilities) • PingOne Protect • PingIntelligence for APIs Adopting a cloud-first or cloud-only strategy also helps you comply with rapidly changing electronic data handling regulations, especially in heavily regulated industries such as healthcare and financial services. You also trade capital costs, such as those associated with physical servers and data centers, for variable expenses with a pay-as-you-go system. Whether you just want single sign-on (SSO), or a risk-based, adaptive authentication authority, starting off with a PingOne solution package lets you only pay for what you need and gives you room to grow.	PingOne Advanced Services has a single-tenancy architecture and provides you with your own virtual private cloud (VPC) network that you define. This virtual network can connect to any data source and closely resembles the network that you operate in your data centers, but in a scalable, secure, cloud environment. This network is hosted by Amazon Web Services (AWS) and isolated from other virtual networks. Your development environments are also isolated from each other within the network and communicate with each other through a central hub. This hub not only facilitates communication, but it also collects data from across your accounts and environments and helps you identify trends and potential threats. PingOne Advanced Services includes: • PingFederate • PingDirectory • PingDirectory/ Delegated Admin • PingAccess • PingCentral • PingDataSync These services can also be integrated with the PingOne Advanced Services, but are not deployed with the platform by default: • PingOne MFA/ PingID • PingOne • PingOne Authorize • PingOne Protect • PingIntelligence for APIs Most importantly, PingOne Advanced Services can connect to anything and everything, including legacy systems based on proprietary standards. This solution can also integrate with on-premise data or authentication sources, and act as either an identity provider (IdP) or a service provider (SP), which makes complex authentication flows possible.

Deployment models

Both platforms are built on Amazon Web Services (AWS), which hosts resources in multiple locations worldwide.Each AWS region is isolated from other AWS regions and contains between two and five availability zones.Each zone is supported by at least one physical data center in that region.Although a single availability zone can span multiple data centers, to reduce the likelihood of two zones failing simultaneously, no two zones share a data center.

You have one region with the PingOne Cloud Platform, and you can have between one and three different regions with PingOne Advanced Services. All regions guarantee uptimes of 99.99%:

- With the PingOne Cloud Platform, your region can be in the United States, Canada, EMEA (Germany or Ireland), or Australia.
- With PingOne Advanced Services, your regions can be in North America (US-West, US-East, or Canada), in EMEA (Germany or Ireland), or in APAC (Australia or Singapore).

PingOne SaaS services can be replicated within their geographic region, and PingOne Advanced Services can be replicated across all regions and across all availability zones within a region.

Both of these solutions are deployed using active-active configurations, which means the database contains at least two active nodes that share data and write to the database. If one connection becomes unavailable, all traffic is routed through the other connection.

Having this type of configuration in place improves application availability, scalability, security, and performance, and reduces, if not eliminates, downtime from new application deployments or database upgrades and patching.

Admin experience

With the PingOne Cloud Platform, you can manage all of your organization's environments and the users, applications, connections, and experiences within them, directly from the PingOne admin console. Applications are accessible from a catalog.

An administrative console is not yet available for PingOne Advanced Services, but admin consoles are available for PingFederate and PingAccess. These consoles allow you to manage your applications, authentication policies, and data sources yourself. For tasks that you can't complete yourself, submit a service request. See the Task summary table for a complete list of these tasks.

PingCentral is also included in PingOne Advanced Services to help you manage your applications across your environments.

PingOne Cloud Platform	PingOne Advanced Services
The PingOne Cloud Platform also includes: • A self-service admin portal for end users to update their profiles, passwords, and authentication methods. • The ability to change the look and feel of your registration pages, sign-on pages, and verification pages to match your organization's branding. • OpenID Connect (OIDC) scope and grant administration capabilities. • Customizable domain names and notifications. Notification templates are included to help you get started. • Agreements that users must consent to during the sign-on process. You can present these agreements in different languages and for different locales.	With the PingOne Advanced Services, you work with our Professional Services team to design your virtual network. This virtual network can connect to any data source and can closely resemble the network you operate in your data centers, but in a scalable, secure, cloud environment. Connections can be made using integration kits, or you can use customized integrations to connect to the resources you need. You can also: • Bulk import and export JSON files. • Import and export SAML metadata. • Import and export configuration archive `.ZIP` files and even automatically create backup files.

Authentication

Authentication is the process of determining whether someone, or something, is who or what they say they are. The ways in which users prove their identities often depend on the sensitivity of the data and digital resources involved. Learn more about how it works in Authentication in Identity Fundamentals.

Both the PingOne Cloud Platform and PingOne Advanced Services support a variety of authentication standards, adapters, and policies, which makes it possible to provide a wide variety of authentication experiences to your customers and workforce.

See the following:

With both platforms, you can use OIDC and SAML 2.0 to design SSO authentication experiences for your customers. PingOne Advanced Services also supports SAML 1.X. These experiences can include any of these features:

- Email verification
- Passive profiling
- Changing and resetting passwords
- Unlocking accounts
- Account linking
- Self-service account management

With PingOne Advanced Services, you can also provide a way for your customers to recover their usernames, and use CAPTCHA for challenge-response authentication.

Both platforms also support SSO experiences for your employees, partners, and vendors, and can include:

- Browser-based SSO

- Single logout (SLO)
- IdP discovery
- Attribute mapping

With PingOne SaaS products, attribute manipulation can be performed using the Spring Expression Language (SpEL).With PingOne Advanced Services, attribute manipulation is done using Object-Graph Navigation Language (OGNL), which is an open-source expression language for Java.

PingOne Advanced Services also supports WS-Trust, an OASIS standard that directs web service clients and providers to interact with the Security Token Service (STS) to issue, renew, and validate security tokens so that a trusted connection can be established. If the receiving entity successfully validates the security token from the requesting entity, the connection is established. If it's unsuccessful, the request is denied.

The PingOne Cloud Platform and PingOne Advanced Services support a wide variety of adapters to connect your authentication applications and services to the platform:

- **Identifier-first login**: Authenticates users in two separate steps, which is useful if you need to display a separate, branded sign-on page based on an email address or user domain. It can also be used to trigger additional security mechanisms based on user IDs or email addresses.
- **Social login**: Authenticates users by using existing sign-on information from a social network provider like Facebook, Twitter, or Google to sign on to a third-party website instead of creating a new account specifically for that website.
- **External IdPs**: Authenticates users using SAML or OIDC and your external databases, applications, and services.
- **Active Directory (AD)** or another identity repository authenticates users in those databases using LDAP or RADIUS gateways.
- **Kerberos**: Authenticates users and client-server applications using time-limited secret-key cryptography, multiple secret keys, and a third-party service.
- **PingOne MFA or PingID**: Authenticates users after they present at least two pieces of evidence that they are who they claim to be.

PingOne Advanced Services also supports the OpenToken adapter, the Agentless Integration Kit, and Microsoft Entra certificate-based authentication (CBA), which enables users to authenticate directly with client certificates (X.509) against Microsoft Entra ID.

Authentication policies determine the order and conditions in which various authentication mechanisms are used to successfully authenticate a user:

- With the PingOne Cloud Platform, you can configure sign-on policies, PingOne policies, and authentication API policies.
- With PingOne Advanced Services, not only can you configure sign-on, include::partial$common_product_keydefs.adoc[tags=singularkey], and API policies, but you can also use authentication selectors, reusable policy fragments, and policy builders to design unique authentication experiences for your users.

Authorization

With the PingOne Cloud Platform, you can manage all of your organization's environments and the users, applications, connections, and experiences within them, directly from the PingOne admin console. Applications are accessible from a catalog.

An administrative console is not yet available for PingOne Advanced Services, but admin consoles are available for PingFederate and PingAccess. These consoles allow you to manage your applications, authentication policies, and data sources yourself. For tasks that you can't complete yourself, submit a service request. See the Task summary table for a complete list of these tasks.

PingCentral is also included in PingOne Advanced Services to help you manage your applications across your environments.

PingOne Cloud Platform	PingOne Advanced Services
The PingOne Cloud Platform also includes: • A self-service admin portal for end users to update their profiles, passwords, and authentication methods. • The ability to change the look and feel of your registration pages, sign-on pages, and verification pages to match your organization's branding. • OpenID Connect (OIDC) scope and grant administration capabilities. • Customizable domain names and notifications. Notification templates are included to help you get started. • Agreements that users must consent to during the sign-on process. You can present these agreements in different languages and for different locales.	With the PingOne Advanced Services, you work with our Professional Services team to design your virtual network. This virtual network can connect to any data source and can closely resemble the network you operate in your data centers, but in a scalable, secure, cloud environment. Connections can be made using integration kits, or you can use customized integrations to connect to the resources you need. You can also: • Bulk import and export JSON files. • Import and export SAML metadata. • Import and export configuration archive `.ZIP` files and even automatically create backup files.

Identity federation

Federated identity management (FIM) is a system that allows users in separate organizations to access the same networks, applications, and resources using one set of credentials. Each organization maintains their own identity management systems, which are linked to a third-party Idp that stores user credentials and authenticates users across organizations.

Both the PingOne Cloud Platform and PingOne Advanced Services support a variety of functions that help ensure communication between federated entities remains secure:

- Metadata URL consuming and publishing, which provides additional information about a site that's embedded into its code.
- OAuth redirect URI validation, which helps ensure users are directed to appropriate locations after they successfully sign-on.
- SSL and TLS encryption, which helps ensure that communications between a client and server are secure.
- Key rotation policies, which define when a signing key should be retired and replaced with a new cryptographic key.
- Self-signed certificates. PingOne Advanced Services supports both signed and self-signed certificates. There is no cryptographic difference between the two as they use the same algorithm and have the same key length, but some partners might not support unanchored trust models.

PingOne Advanced Services also supports:

- Mutual TLS authentication, where the two parties authenticate each other using the TLS protocol.

- The certificate revocation list (CRL), which is a list of revoked certificates downloaded from the certificate authority (CA), and Online Certificate Status Protocol (OCSP), which is used to check revocation of a single certificate interactively using an online service called an OCSP responder.

Monitoring and logging

Both the PingOne Cloud Platform and PingOne Advanced Services have a variety of monitoring and logging tools to help you stay informed about the health of your network and to help you troubleshoot issues if they arise:

- With the PingOne Cloud Platform, you use webhooks, also known as subscriptions, to monitor events in PingOne.You can retrieve logs through the admin console or through the API.Audit logs, which record all actions performed in the admin console and in PingDirectory, are also available.Learn more in PingOne Platform logging and reporting in the PingOne documentation.
- With PingOne Advanced Services, your organization has its own dedicated cloud network that you define, without having to manage cloud resources, containers, networking, scaling, healing, and backup and restoration.

  Our Support team and our Site Reliability Engineers proactively monitor your infrastructure and deployments and attempt to address issues before they become problems. If outages occur, we'll notify you using standard support methods.

  You are responsible for monitoring your Ping applications and configurations, but we will stream log files to you, which will help you identify, monitor, and resolve any issues you might encounter. You can also subscribe to receive alerts from PingOne Advanced Services, which will notify you of events occurring within your network. Learn more in the Monitoring and logging section of this guide.

Provisioning

Provisioning is a process for creating, updating, and deleting users and accounts across your IT infrastructure. In any enterprise, users access many different applications and resources daily.

Managing accounts and permissions across a variety of systems for a large number of users might seem like a daunting task. Fortunately, automated provision is available in both PingOne and PingOne Advanced Services.

Using automated user and account provisioning ensures that your users can access the applications, files, and other resources they need while minimizing the need for system administrators to be involved.

- With PingOne SaaS, inbound and outbound AD and LDAP directory synchronization is performed using the PingOne gateway.
- With PingOne Advanced Services, inbound and outbound synchronization is performed using either PingFederate or PingDataSync.

PingOne Directory

Both PingOne SaaS and PingOne Advanced Services use PingDirectory as the identity repository for their platforms. Not only does PingDirectory simplify administration, reduces costs, and secures information in systems that scale for large numbers of users, but it also acts as your single source of identity truth across your organization.

Although both cloud solutions use PingDirectory, the ways in which it can be used differ between them.See the following for details regarding those differences.

Data modeling is a process that you use to define the structure of a database before implementing it. The database can simply store information about customers and products, or it could be used for something much more complicated, such as tracking sales and trends across a global network of stores.

- PingOne SaaS uses PingDirectory as its database, which is only used to manage user identities.
- With PingOne Advanced Services, you can use data modeling to manage:
  - Structured and unstructured data
  - Any type of object, such as devices, tokens, and consents
  - Custom data requests

Schemas are sets of rules that define the directory structures, which guarantee that new data entries and modifications meet and conform to these predetermined rules and definitions:

- PingOne SaaS comes with a standard extendable schema for all of your environments, which you can build upon and customize to meet your needs.

  You can add single-valued, multivalued, and custom attributes, which are all validated, including regex and enumerated values. Learn more about schemas in About the schema in the PingDirectory documentation.
- The PingOne Advanced Services schema uses LDAP v3. Schemas and global ACIs, which are completely customizable.

  Submit a Schema - attribute type, a Schema - objectClass, or ACI service request to your Ping Identity support team, who will build the schema and customize global ACIs to best meet your needs.

In each PingOne Saas environment, you can have a maximum of:

- Twenty million identities without incurring additional costs
- One hundred declared attributes (200 attributes by the end of Q2, 2023)
- 100 JSON attributes

With PingOne Advanced Services, there is no limit to the number of identities or attributes you can have in each environment. The largest number of identities currently supported is 170 million.

With PingOne SaaS, you can manage your users, user groups, and attributes through the administrative console or through the REST or Identity Access APIs.

PingOne DaVinci, an orchestration platform that lets you create flows to guide users through defined tasks, can be connected to PingOne.

An administrative console is not available for PingOne Advanced Services, but Delegated Admin is.

You can also use LDAP to directly manage your users, groups, and attributes within the directory, and submit a PingDirectory service request to request additional customization.

PingOne DaVinci can also be connected to PingOne using an LDAP gateway.

Password policies are sets of rules that user passwords must adhere to. For example, a password policy might require that passwords contain at least five characters and include at least one special character. With PingDirectory, you can also specify:

- Whether passwords should expire

- Whether users are allowed to modify their own passwords
- Whether too many failed authentication attempts should result in an account lockout

To help get you started quickly, PingDirectory provides three different out-of-the-box password policies that you can apply to your entries or as templates for configuring customized policies. Learn more about these policies in Viewing password policies in the PingDirectory documentation.

- With PingOne SaaS, password policies are highly customizable and assigned at the population level. These policies can also be used with a wide variety of password validators, except Regex.
- PingOne Advanced Services provides more flexibility and can be assigned at the group or user level.

  Not only can this platform be integrated with most password validators, such as Dictionary, Haystack, and Regex, it can also be integrated with Have I Been Pwned?. This application allows users to check and see if their personal data has been compromised in a data breach.

Passthrough authentication allows your users to sign on to both on-premises and cloud-based applications using the same passwords. This feature provides your users a better experience because there's one less password to remember, which reduces IT help desk costs.

With PingOne SaaS, passthrough authentication is performed using either:

- PingOne SSO
- PingOne gateways

With PingOne Advanced Services, passthrough authentication can be performed using either:

- PingOne SSO
- Active Directory
- Custom authentication plugins

Replication is a data synchronization mechanism that ensures that updates made to a database are automatically duplicated to other servers. Replication improves data availability when unforeseen or planned outages occur and improves search performance by allowing client requests to be distributed across multiple servers.

With PingOne SaaS, PingDirectory handles replication and redundancy, but with PingOne Advanced Services, you can use any replication system you choose.

Data synchronization is the ongoing process of synchronizing data between two or more devices and updating changes automatically between them to maintain consistency between systems.

Synchronization and replication are not the same thing. With replication, exact replicas of the data are created and stored in a variety of different locations. Synchronization can:

- Transform data between two different directory information tree (DIT) structures.
- Map attribute types.
- Synchronize subsets of branches and specific object classes.

With PingOne SaaS, inbound and outbound AD and LDAP directory synchronization is performed using the PingOne gateway.

With PingOne Advanced Services, inbound and outbound synchronization is performed using PingDataSync.

Encryption is a way of scrambling data so that only authorized parties can understand the information, which is standardized across PingOne SaaS and PingOne Advanced Services environments. Entry and attribute-level encryption is also available with PingOne Advanced Services.

- PingOne SaaS uses the standard hashing algorithm, SSHA-512, to ensure that the data is stored in a scrambled state, so it's harder to steal.

  A variety of other password hashing algorithms can also be used, but are rehashed after the initial authentication.

- PingOne Advanced Services supports additional password hashing algorithms including SSHA, PBKDF2, bcrypt, msCrypto, and Argon2.

Environments

With PingOne Advanced Services, you have one production environment and a variety of non-production environments that you can use to develop and test your code and configurations.

Items of note include:

- Automation is used to build and deploy PingOne Advanced Services into AWS so that all environments follow the same generic footprint.
- Each environment has data storage limits, which are important to consider when configuring your platform. See Data storage considerations for details.
- PingOne Advanced Services comes with a number of URLs to access different services, such as PingFederate and PingAccess runtime endpoints. Do not use these URLs for users accessing your production environment. Instead, provide a TLS certificate and key so that it can be branded to your domain.

Production environment

The production environment (Prod) is where the latest versions of software, products, or updates are pushed live to their intended users.

With PingOne Advanced Services, the production environment is:

- Built to support the predicted load for each customer, based on their licensed identity count.
- The only environments that are subject to Ping Identity's uptime and Severity 1 and 2 service level agreements.

With multi-region deployments, production environments use active-active clustering configurations to achieve load balancing.

Non-production environments

Non-production environments provide you with a way to develop and test your code and configurations using smaller sets of representative data, and then perform final testing and load testing in accordance with Ping Identity's load testing policies. Development and testing environments cannot be revised once they are created and remain static throughout their existence.

- **Development environments (Dev)**

  Each PingOne Advanced Services deployment includes one development environment by default. Development environments are used to create and test code without interfering with the content on live sites.

  Keep the following in mind:

  - These environments should not be used for performance or load testing.
  - They do not scale and are always deployed in a single-region model.
  - With multi-region deployments, development environments only exist in the primary region.
  - The Dev environment is provisioned with 8GB of RAM and 40 GB of disk space.
  - These environments are not subject to Ping Identity's uptime and Severity 1 and 2 service level agreements.

- **Testing (Test)**

Testing environments are replicas of the Dev environments and are optional add-ons with PingOne Advanced Services. Testing environments are used to quality-check applications and perform user acceptance testing.

Keep the following in mind:

- These environments should not be used for performance or load testing.
- With multi-region deployments, testing environments only exist in the primary region.
- The Test environment is provisioned with 8GB of RAM and 40 GB of disk space.
- These environments are not subject to Ping Identity's uptime and Severity 1 and 2 service level agreements.

- **Staging (Stage)**

Staging environments are replicas of the production environment and are optional add-ons with PingOne Advanced Services. They can be used for performance and load testing, and for final testing before changes are released to the live site.

Keep the following in mind:

- With multi-region deployments, the staging environment clustering configuration matches the production environment configuration.
- The Staging environment is provisioned with the same RAM and disk space as your production environment.
- These environments are not subject to Ping Identity's uptime and Severity 1 and 2 service level agreements.

> **Note**
>
> A staging environment is required for multi-region clustered deployments, even if one is not purchased. The environment will be present, but turned off, so be sure to account for the /22 RFC1918 IP space required to house it.

- **Customer hub**: This environment is deployed in every region that your solution is deployed in, and serves as a central data store for cluster configuration code and product integration kits. PingCentral also runs here, which allows you to delegate common application configuration and deployment tasks to application owners. See Introduction to PingCentral for details.

Data storage considerations

Data is measured in entries. An entry could be a user account, the grants associated with that user, or any data associated with that user. The total number of entries is also known as the total number of objects.

The amount of data that can be loaded to an environment depends on the size of each entry, the amount of memory required to store it, and the amount of storage available. As the schema for an entry is customized for each customer, there is no single calculation that can be made to determine how much memory and storage a customer will require.

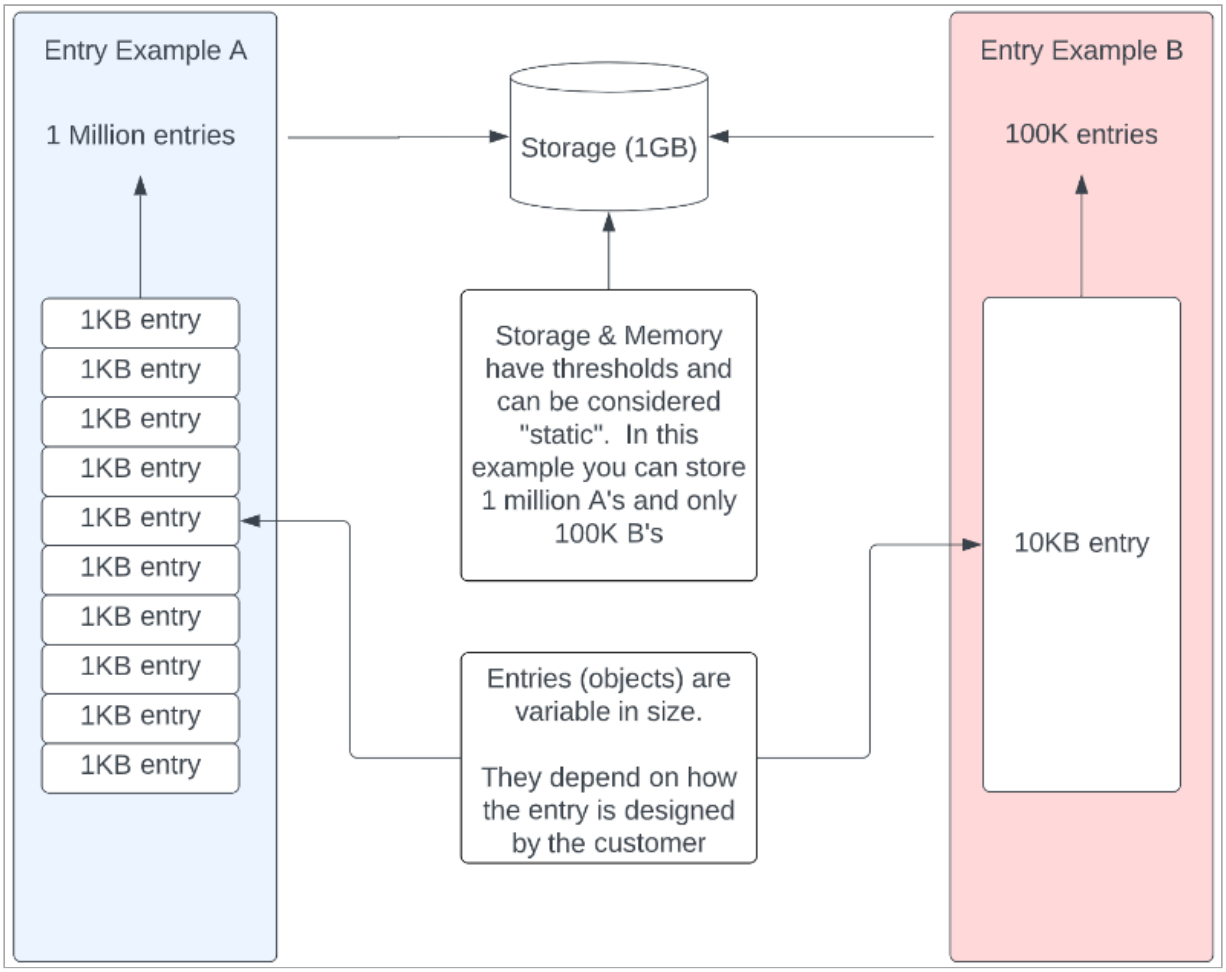
In these examples, we illustrate how data storage is calculated using two different entry sizes.

- If the average size of each entry is 1 KB, and 1 GB can store 1 million KB:

  1 KB per entry * 1 million entries = 1 GB of storage needed.

- If the average size of each entry is larger, the number of entries that can be stored in each GB will be smaller. For example, if the average size of each entry is 10 KB, you can only store about 100,000 entries:

  10 KB per entry * 100,000 entries = 1 GB of storage needed.



Remember that Development and Testing environments are provisioned with 8 GB of RAM and 40 GB of disk space and are not intended for load testing. You can load a portion of your data into those environments to quality-check your applications and perform user acceptance testing, and then move all of your data to the Staging environment for performance and load testing.

Network guide

PingOne Advanced Services provides you with your own virtual private cloud (VPC) network that you define. This virtual network can connect to any data source and closely resembles the network you operate in your data centers, but in a scalable, secure, cloud environment with data and resource isolation.

This guide describes each of the network options available for PingOne Advanced Services and the regions and deployment models available. Review this information to become familiar with your options, and work with your Ping Identity team members to select the options that are right for you.

Learn more:

- Regions and deployment models
- Network options:
  - Internet-only network
  - Simple network
  - Advanced network
- Setup considerations

> **Note**
>
> With this platform, request headers are passed from the client to the AWS Network Load Balancer and through the ingress controller unchanged, but the `X-Forwarded-For` and `X-Real-IP` headers have the client IP address added to the header value.

Items not supported

Although PingOne Advanced Services is hosted in AWS, it doesn't have all the features and functionality available with AWS. Much of the network is automated, so PingOne Advanced Services only supports items and settings that its automation supports.

The PingOne Advanced Services customer hub can only be connected to a single network. The platform does not allow for a production/non-production split.

Nor does it support:

- Authenticated BGP for AWS Site-to-Site VPN tunnels.
- Split DNS Forwarders to on-premise DNS servers (production or non-production, or by environment).
- Private endpoint cross-region redundancy.

Private endpoints cannot be accessed within the cluster due to a NAT loopback limitation with the AWS Network Load Balancer (NLB). For example, PingFederate should not connect to the PingDirectory private ingress, but rather the PingDirectory internal cluster name.

Limitations guide

Many of you have used on-premise versions of Ping Identity products, such as PingFederate, PingAccess, PingCentral, and the PingDirectory suite of products. Many of you have also used a variety of different cloud services, including Amazon Web Services (AWS).

However, it's important to understand that some of the product features and configuration options that you might be accustomed to using are not available with PingOne Advanced Services. Even if you're an experienced AWS user, PingOne Advanced Services has a variety of infrastructure and networking requirements that you should be aware of.

This guide lists the product features that are not available in PingOne Advanced Services, and explains how the product log files differ from the on-premise versions. It also outlines our data loading and access policies.

Refer to the following for details:

- Infrastructure
- Product features and configurations
- Observability and logging
- Data loading and access

Infrastructure

Items to keep in mind regarding PingOne Advanced Services infrastructure:

- The PingOne Advanced Services SaaS platform is built on AWS, which hosts resources in multiple locations worldwide. No other cloud provider is supported.

  > **Important**
  >
  > PingOne Advanced Services is built on AWS, but because it is a SaaS platform, it does not provide access to the features and tools that you might be accustomed to using in AWS.

- Multi-cloud deployments are not supported.
- A Simple Mail Transfer Protocol (SMTP) server is not included. If one is needed and because AWS blocks port 25 outbound by default, Simple Mail Transfer Protocol Secure (SMTPS) must be used.
- Each AWS region is isolated from other AWS regions, and each zone is supported by at least one physical data center in that region. Although a single availability zone can span multiple data centers, no two zones share a data center to reduce the likelihood of two zones failing simultaneously.

  The following table lists the regions supported:

Region group	Code (region)	Name
Asia	ap-Southeast-1 (url region "sg1")	Asia Pacific (Singapore)
	ap-Southeast-2 (url region "au1")	Asia Pacific (Sydney)
	ap-Southeast-4 (url region "au2")	Asia Pacific (Melbourne)

Region group	Code (region)	Name
Canada	ca-Central-1 (url region "ca1")	Canada (Central)
Europe	eu-Central-1 (url region "eu1")	Europe (Frankfurt)
	eu-West-1 (url region "eu2")	Europe (Ireland)
United States	us-East-2 (url region "us1")	US East (Ohio)
	us-West-2 (url region "us2")	US West (Oregon)

You have one region with the PingOne Cloud Platform and can have between one and three different regions with PingOne Advanced Services. All regions guarantee uptimes of 99.99%.

> **Note**
>
> Session migration on inter-regional fail-over is only supported if the products are properly configured, and should be addressed during the system planning and design phase.

- You have one production environment and up to three non-production environments (Dev, Test, and Stage) that you can use to develop and test your code and configurations. Dev and Test environments:
  - Are provisioned with 8GB of RAM and 40GB of disk space.
  - Do not auto-scale resources for the number of pods needed.
  - Only exist in the primary region for multi-region deployments.
  - Support a limited number of identities or objects:
    - The limit of identities or objects in Dev and Test is 10,000.
    - More identities or objects can be loaded, however, doing so is at your own risk.
    - Performance or stability issues might be encountered if the limit is exceeded.

The staging environment is a replica of the production environment infrastructure but is not subject to Ping Identity's uptime and Severity 1 and 2 service level agreements.

Load and performance testing is not permitted on the Dev or Test environments.

See Environments for additional information about each of these environments.

> **Note**
>
> Determine which types of non-production environments you want to use upfront, as it's arduous to add environments after PingOne Advanced Services is deployed.

Product features and configurations

Although most functionality available in the on-premise products is also available in PingOne Advanced Services, some features and configurations are not.

For example, heartbeat health checks are not available for our products and services. However, you can submit a service request and ask for health checks to be run on the staging server.

The following sections list some of the product-specific features and configurations you should keep in mind.

PingFederate

- Integration kits that add an application (war file) are not supported, however, JavaScript or other scripts are allowed.
- PingFederate provisioning is only available from the primary region with no fail-over.
- The PingFederate Agentless Integration Kit cannot use dots in header names (only dashes).
- The OAuth Playground is not supported in Production environments.
- The persistent session datastore for PingFederate can only be PingDirectory.
- The X509/mTLS uses the alternate Hostname format, (not the alternate port format).
- There is no self-service report or way to view administrator-level permissions (roles) for admin users.
- An administrator audit log file is not available.
- When configuring CRL checking, the **Treat Unretrievable CRLs as Revoked** option cannot be used with PingOne Advanced Services. As soon this option is selected in PingFederate and the configuration is replicated to the engines, the outage starts. After PingFederate is restarted with the option selected, a support ticket is required, as PingFederate will no longer start.

> **Important**
>
> If changes to the PingFederate `config-store` are needed, you must make them yourself using an API call or the API interactive documentation. Your organization owns the data in both `config-store` and `config-archive`, and our Support team isn't allowed to make updates.

PingDirectory

- The number of customer-specific directory backends is limited to five.
- HSMs that require extra libraries are not supported.
- Automatic certificate management in a truststore is not supported.
- Certain privileges are not available to PingOne Advanced Services, including config-read, and bypass-acl.
- There is no access to backends other than customer backends and no privileges or configuration changes that would impact those backends, (e.g., no access to the default password policy or virtual attributes that impact non-customer backends).

- No changes can be made to root users or root privileges.
- PingDataSync only supports LDAP-to-LDAP sync pipes.
- PingDataSync is unable to make outbound connections to Kafka.

Important

If you are a PingDirectory administrator, be aware that using static groups, especially large groups with more than 1000 members, can significantly impact performance. Also, if you make changes to a large static group, manually or through the referential integrity plugin, PingDirectory server performance can be significantly affected and outages could occur. Ensure that your administrators and application developers work together to minimize the potential impact on the user experience.
This is one of the many reasons it's recommended not to use static groups. Dynamic groups or inverted static groups that use an attribute of the user entry to determine the user's membership, are recommended instead.
However, if you can't avoid using large, static groups, here are a few recommendations that could help improve performance:

- Don't directly update the static group for each user record. Instead, collect the changes and create a single operation that adds or removes many users using a single group modify operation.
- Set the referential integrity plugin update interval to a non-zero value. Note that this only delays the effort that the directory servers must take.
- Modify the replication assurance policies to exclude group operations so that they don't require local assurance. Note that this also only delays the effort the directory servers must take.
- Increase the new generation memory to reduce the risk of premature promotion and the number of young generation collections. By default, 2G is provided.

PingAccess

- This product cannot be used as a proxy for PingFederate.
- There is no self-service report or way to view administrator-level permissions (roles) for admin users.
- An administrator audit log file is not available.
- Customers can only use port 443 for PingAccess-protected application URLs (virtual hosts).

General platform features

- Customer-managed PingFederate and PingAccess admin accounts are not supported.
- If you have many internal certificate authorities (CAs), more than 20 virtual hosts must be created in PingOne Advanced Services. Application code will also need to be updated to reflect the virtual hosts for agentless drop-off and pick-up.

Observability and logging

Our Support team and the Site Reliability Engineers proactively monitor your infrastructure and deployments and attempt to address issues before they become problems. If outages occur, we'll notify you using standard support methods.

You are responsible for monitoring your Ping applications and configurations, but we will stream log files to you, which will help you identify, monitor, and quickly resolve any issues you might encounter. You can also subscribe to receive alerts from PingOne Advanced Services, which will notify you of events occurring within your network.

See Monitoring and logging for additional information.

Although the on-premise products you might be accustomed to using allow you to customize your log files, the log files in PingOne Advanced Services are limited.

Items to keep in mind regarding PingOne Advanced Services observability and logging:

- Log fields cannot be customized.
- Debugging is turned off for the production and Stage environments, but can be turned on for brief periods of time for troubleshooting purposes.
- Only the default product logs are available.
- If integration kits are used with PingOne Advanced Services, they must be provided by Ping Identity product or engineering teams. Kits created by customers or other third parties are not allowed.
- Parsed log files are available (on a best-effort basis) in OpenSearch for 30 days (subject to change).
- S3 Log Replay is an internal tool used only by internal teams for troubleshooting purposes.
- Customer-requested log replay isn't available for either OpenSearch or customer endpoints.

The log names that you might be used to seeing in PingFederate, PingAccess, and the PingDirectory suite of products might be different in the PingOne Advanced Services log files. These differences are listed here by product.

PingFederate

On-premise log name	PingOne Advanced Services log name
server.log	pf-server-*
audit.log	pf-audit-*
transaction.log	pf-transaction-*
provisioner.log	pf-provisioner-*
provisioner-audit.log	pf-provisioner-audit-*
<date.>request.log	pf-request-*
admin.log	pf-admin-log-*
admin-event-detail.log	pf-admin-event-detail-*
admin-api.log	pf-admin-api-*
runtime-api.log	pf-runtime-api-*

On-premise log name	PingOne Advanced Services log name
init.log	pf-init-*
jvm-garbage-collection.log	pf-jvm-garbage-collection-*

PingAccess

On-premise log name	PingOne Advanced Services log name
pingaccess.log	pa-pingaccess-*
pingaccess_engine_audit.log	pa-engine-audit-*
pingaccess_agent_audit.log	pa-agent-audit-*
pingaccess_api_audit_har.log	pa-api-audit-har-*
pingaccess_api_audit.log	pa-api-audit-log-*
pingaccess_sideband_audit.log	pa-sideband-audit-*
pingaccess_sideband_client_audit.log	pa-sideband-client-audit-*
pingaccess.log	pa-was-pingaccess-*
audit.log	pa-was-engine-audit-*
pingaccess_was_api_audit_har.log	pa-was-api-audit-har-*
pingaccess_was_api_audit.log	pa-was-api-audit-log-*
pingaccess_was_sideband_audit.log	pa-was-sideband-audit-*
pingaccess_was_sideband_client_audit.log	pa-was-sideband-audit-*

PingAccess Web Application Security (WAS)

On-premise log name	PingOne Advanced Services log name
pingaccess.log	pa-was-system*
audit.log	pa-was-audit*
pingaccess_engine_audit.log	pa-was-audit*
pingaccess_api_audit.log	pa-was-audit*
pingaccess_agent_audit.log	pa-was-audit*

On-premise log name	PingOne Advanced Services log name
pingaccess_sideband_audit.log	pa-was-audit*
pingaccess_sideband_client_audit.log	pa-was-audit*
pingaccess.log	pa-was-admin-system*
audit.log	pa-was-admin-audit*
pingaccess_engine_audit.log	pa-was-admin-audit*
pingaccess_api_audit.log	pa-was-admin-audit*

PingDirectory

On-premise log name	PingOne Advanced Services log name
access	pd-access-*
errors	pd-errors-*
server.out	pd-server-*
replication	pd-replication-*
failed-ops	pd-failed-ops-*
expensive-write-ops	pd-expensive-write-ops-*
http-detailed-access	pd-http-detailed-access-*

PingDataSync

On-premise log name	PingOne Advanced Services log name
access	pds-access-*
errors	pds-errors-*
server.out	pds-server-*
failed-ops	pds-failed-ops-*

Data loading and access

When transitioning to PingOne Advanced Services, you'll need to load your existing data from your legacy systems into your PingOne Advanced Services deployment.

For security reasons, Ping Identity will not, and should not, have access to your data.

However, our Professional Services team will work closely with you to ensure the transition is as painless as possible. We'll discuss the methods we'll use during the system planning and design phase.

These methods include but are not limited to:

- Importing an LDIF file remotely through an LDAP browser
- Using PingDataSync

If you intend to use NGINX or PingAccess, request sizes cannot be larger than 1 MB.

Web servers and Ingress

Web servers proxies HTTP requests to web application servers, while Ingress exposes HTTP and HTTPS routes from outside the cluster to services within the cluster. Traffic routing is controlled by rules defined on the Ingress resource.

PingOne Advanced Services is deployed with a variety of hostname URLs by default, but it's important that you use your own hostname URLs. Using the default URLs can cause issues for your users if you have a multi-region deployment, or plan to in the future.

The pre-authorized ciphers are:

- ECDHE-ECDSA-AES128-GCM-SHA256:
- ECDHE-RSA-AES128-GCM-SHA256:
- ECDHE-ECDSA-AES256-GCM-SHA384:
- ECDHE-RSA-AES256-GCM-SHA384:
- ECDHE-ECDSA-CHACHA20-POLY1305:
- ECDHE-RSA-CHACHA20-POLY1305:
- DHE-RSA-AES256-GCM-SHA384:
- ECDHE-RSA-AES256-SHA384:
- ECDHE-RSA-AES128-SHA256:
- ECDHE-ECDSA-AES256-GCM-SHA384:

Monitoring and logging

With PingOne Advanced Services, your organization has its own dedicated cloud network that you can define, without having to manage cloud resources, containers, networking, scaling, healing, and backup and restoration.

Our Support team and the Site Reliability Engineers proactively monitor your infrastructure and deployments and attempt to address issues before they become problems. If outages occur, we'll notify you using standard support methods.

You are responsible for monitoring your Ping applications and configurations. You can either use the built-in log aggregation tool, OpenSearch, or you can stream the log files yourself using Amazon S3 Bucket, Generic HTTP or Webhook, IBM QRadar, Splunk HTTP Event Collector (HEC), or Syslog. These files can help you identify, monitor, and quickly resolve any issues you might encounter. You can also subscribe to receive alerts from PingOne Advanced Services, which will notify you of events occurring within your network.

See the following for details:

- Platform monitoring
- Application monitoring and alerts
- Logging
- Product-specific logs
- Updating your log-streaming services

Platform monitoring

The PingOne Advanced Services platform is built on AWS, so we leverage their tools to monitor and support the platform.

These tools include:

- Amazon CloudWatch, which is used for real-time monitoring of the AWS platform and our applications leveraging the platform.
- GuardDuty, which is used for intelligent threat detection.

We also use New Relic, an observability platform used to log, track, and analyze data from any digital source in real time.

You are not responsible for monitoring the platform or its infrastructure, so you won't see any of the alerts sent from these services, but rest assured that we will notify you if your network is affected.

You can also access the Ping Identity status page to see service interruption information, or subscribe to receive alerts regarding particular products or services.

Application monitoring and alerts

Since you are responsible for monitoring your applications, you can subscribe to receive a variety of different alerts regarding the health of your network. You can also work with your Ping Identity support teams to customize the alerts you receive and display them on Kibana dashboards.

Some of the most common PingFederate alerts and PingDirectory alerts are listed and described here.

PingFederate alerts

If more than one error occurs within one minute, alerts will be sent to those who subscribe to them. Alerts that PingFederate administrators often subscribe to include:

Error alerts	Description
Fatal or critical errors	These errors were not discovered by other filters and likely require immediate attention.
Connectivity errors	These errors can occur for a variety of reasons and often indicate that cluster members cannot communicate with components, either within or outside of PingOne Advanced Services, or with each other. PingFederate connectivity alerts are: • PF LDAP Connection Lost • PF PingID Connection Lost
Authentication flow errors	These errors indicate that the authentication flow contains errors, which are often **HandleAuthNRequest** errors. PingFederate authentication flow alerts are: • PF Unexpected Runtime Error • PF Auth Exception
Invalid action errors	These errors indicate that a large number of unexpected invalid calls or actions were detected. The PingFederate invalid action error is: • PF Invalid Request Parameter
Decoding errors	These errors indicate that a large number of token decoding errors were detected. The PingFederate decoding error is: • PF Profile Message Missing ID

PingDirectory alerts

If more than one error occurs within one minute, alerts will be sent to those who subscribe to them. Alerts that PingDirectory administrators often subscribe to include:

Error alerts	Description
Fatal or critical errors	These errors were not discovered by other filters and likely require immediate attention. The PingDirectory critical error is: • PD Critical
General errors	These errors indicate that issues within the application might negatively affect the user experience. PingDirectory general alerts are: • PD Major • PD Third Party Extension Exception
Connectivity errors	These errors can occur for a variety of reasons and often indicate that cluster members cannot communicate with components, either within or outside of PingOne Advanced Services, or with each other. The PingDirectory connectivity error is: • PD LDAP Connection Handler Startup Error
Replication errors	These errors indicate that data consistency issues exist. PingDirectory replication alerts are: • PD Failed Mirror Configuration • PD Replication Backlogged • PD Replication Changelog Failure • PD Replication Missing Changes • PD Replication Replay Operation Failed • PD Replication Server Failure Alarm • PD Unresolved Replication Conflict
Performance errors	These errors indicate that performance has fluctuated more than it normally does. The PingDirectory performance alert is: • PD Worker Threads Terminated
Garbage collection errors	These errors indicate that garbage collection processes are occurring more frequently, or are taking longer than expected. The PingDirectory garbage collection filter alert is: • PD Continuous Garbage Collection Filter

Logging

Event logs contain valuable information regarding possible security threats, outages, and metrics that can help troubleshoot issues.

You can either use the built-in log aggregation tool, OpenSearch, or you can stream the log files yourself using Amazon S3 Bucket, Generic HTTP or Webhook, IBM QRadar, Splunk HTTP Event Collector (HEC), or Syslog.

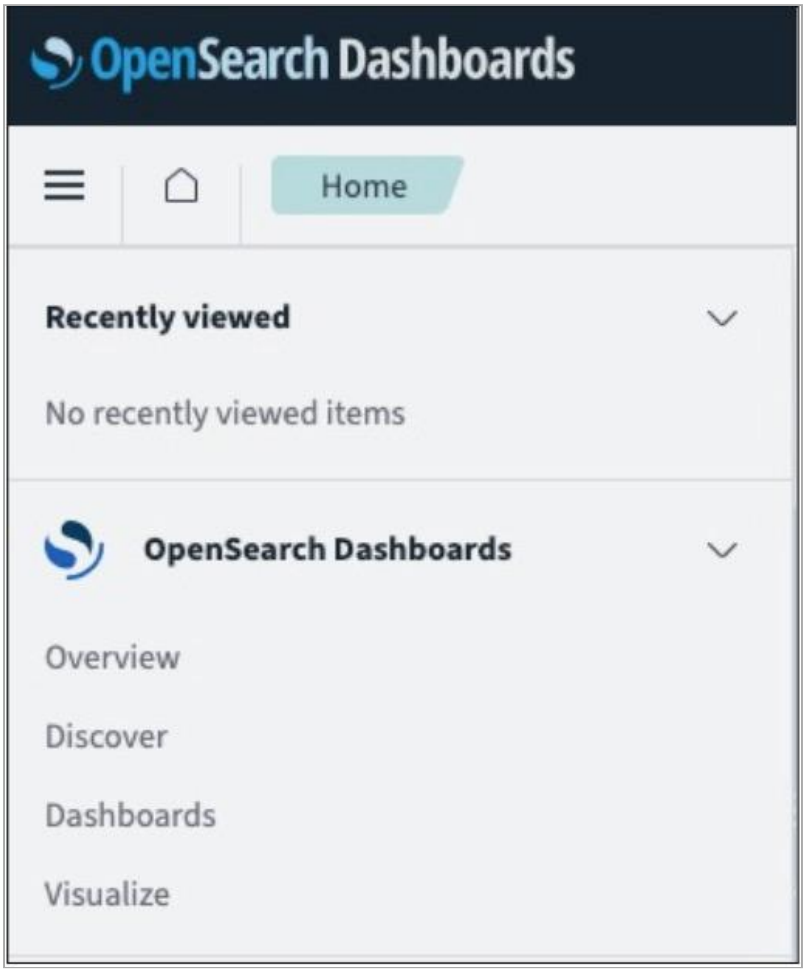
- Using OpenSearch
- Streaming log files

Using OpenSearch

PingOne Advanced Services has built-in log aggregation. Standard logs from Ping Identity products are streamed to OpenSearch, where you can review the data in a variety of different dashboards.

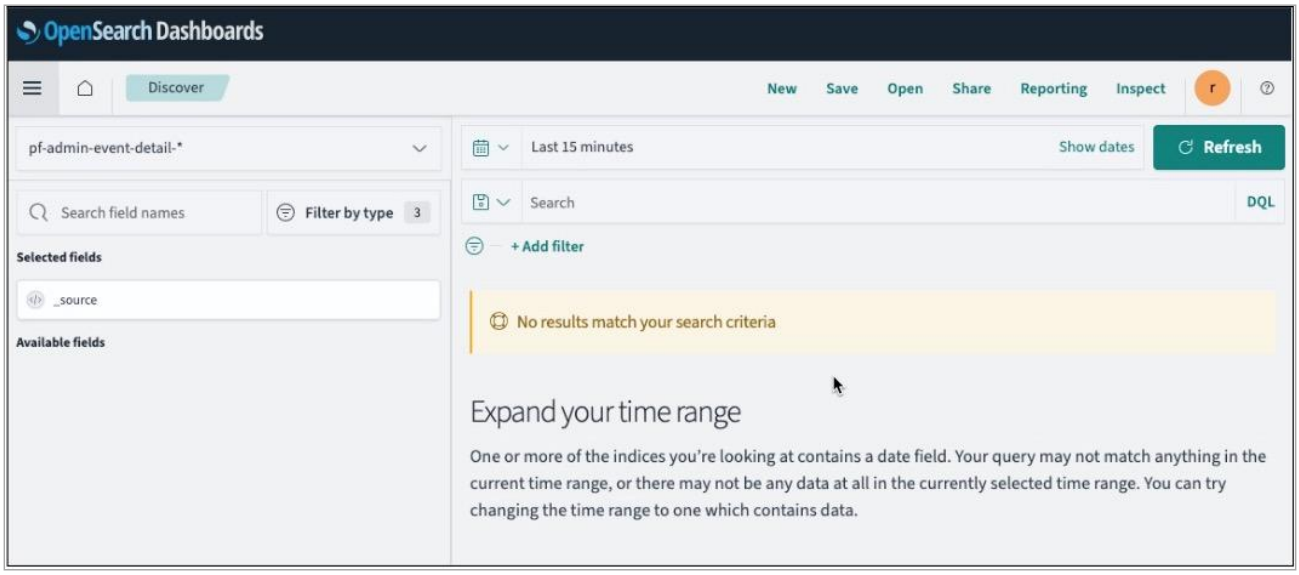
1. Go to https://logs.<env>-<stub>.<primary-region>.ping.cloud to access OpenSearch.
2. Click **Log in with single sign-on**.
3. On the **Select your tenant** page, select **Global** and click **Confirm**.

   The OpenSearch Dashboards modal opens.

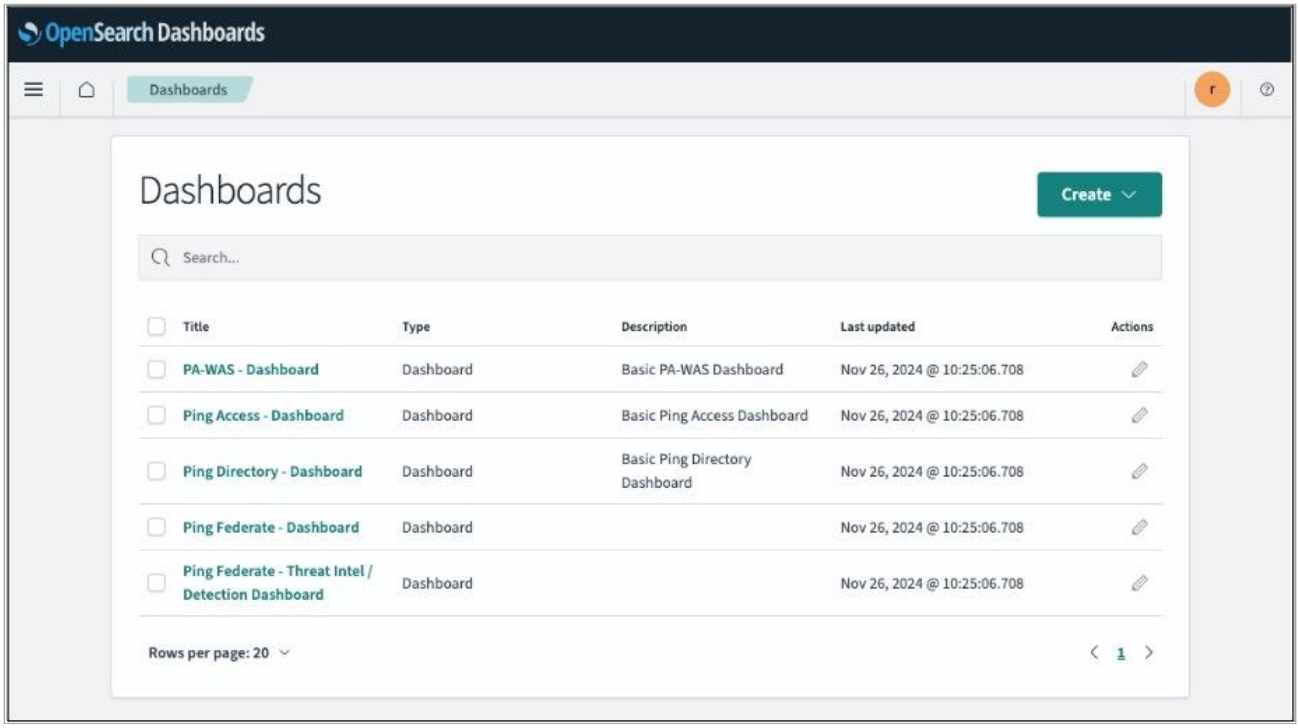


4. Expand the **OpenSearch Dashboards** list select the appropriate application:

    - **Discover** gives you access to data from each Ping Identity product log. You can analyze your data by querying and filtering, viewing results, and drilling down to examine specific documents. You can also create histograms to display your data. Learn more about Discover in Using the Discover application in the OpenSearch documentation.



- **Dashboards** provides you with pre-built dashboard templates for PingOne Advanced Services, which allow you to visualize your data. Learn more about Using the Dashboards application in the OpenSearch documentation.



Streaming log files

You can stream your log files near real-time for all Ping Identity products in your PingOne Advanced Services cloud network using one of the log aggregation tools listed here.

You can either set up this process when you initially access your applications or submit a service request at any time. In your request, make sure that you include the pertinent information listed here regarding your aggregation tool.

Refer to the following for details about each logging tool:

To export log files with an Amazon S3 bucket, include the following information in your request:

- Your AccountID
- AWS key and secret
- Bucket name

To export log files with a generic HTTP or webhooks, include the following information in your request:

- Endpoint URL
- HTTP method used to send data
- An authorization token or key (optional)

QRadar uses the syslog output with a JSON encoding. To export log files, include the destination host and port in your request.

Splunk HEC only supports RAW Endpoint. To export log files, include the following information in your request:

- Splunk HEC Endpoint URL
- Splunk API Key

To export log files with Syslog, include the destination host and port in your request.

If you want to use a logging tool not listed, reach out to your account team.

Product-specific logs

Detailed information regarding product log files is available in the product documentation:

PingFederate:

- PingFederate log files
- Runtime transaction logging
- Security audit logging
- Administrator audit logging

PingDirectory:

- Managing logging
- Access and audit log

PingAccess:

- Logging configuration

Updating your log-streaming services

In the July 2022 release, PingOne Advanced Services added a configurable log-streaming pipeline, which made it possible to customize the ways log data is streamed. You can filter streamed data by application, log, and keywords, and modify JSON files.

If you have not yet migrated to the new streaming processes, be aware that streaming formatting changes need to occur and are outlined here. This format is based on logstash output filters and can be customized to meet your needs.

Here is an example of a log event at the input:

```
{"@timestamp":"2022-07-14T12:00:10.728763Z",
"message":"All pods in namespace ingress-nginx-public are running              |
PASS |\n",
"log_type":"customer_out",
"time":"2022-07-14T12:00:04.314969694Z",
"kubernetes":
{"container_hash":"public.ecr.aws/r2h3l6e4/pingcloud-services/robot-framework@sh
a256:e64b3beb9c23d655f8542e685f0c68c01178498f4b226294f36773832dd1cb48",
"container_image":"public.ecr.aws/r2h3l6e4/pingcloud-services/robot-framework:v1
.3.0",
"docker_id":"9944534ac7556566a40a9f40331e5d07b0cf4244cca2a5a07e6f4b83d0de69a9",
"labels":
{
"app":"ping-cloud",
"controller-uid":"ea007809-075f-4cd6-9955-ad69c94ae190",
"job-name":"healthcheck-cluster-health-27630000"
},
"container_name":"healthcheck-cluster-health",
"host":"ip-10-254-1-222.us-west-2.compute.internal",
"pod_id":"05dc5c68-852e-40f9-93a8-13a24502d545",
"namespace_name":"ping-cloud-antonklyba",
"pod_name":"healthcheck-cluster-health-27630000-4fztv"},
"host":"10.254.12.248",
"@version":"1",
"stream":"stdout",
"log_group":"application"
}
```


This file contains the following information:

- **@timestamp**: Indicates when logstash processed the event.
- **log or message**: Ping Identity applications generate logs and all other types of applications and sidecars.
- **log_type**: Provides internal labels for all events sent to the pipeline.
- **time**: Date and time when the log was captured, which could be different from the date and time it was generated.
- **kubernetes**: The nested JSON object with kubernetes metadata.
- **host**: The internal IP address of a fluent-bit pod sent to logstash.
- **@version**: This internal logstash field will always be “1”.
- **stream**: The name of the stream where the log was captured, and will either be stdout (standard output) or stderr (standard error).
- **log_group**: This internal label will always be “application”.

If you do not apply filters and opt to use the default output configuration, a variety of differences exist:

- If you are exporting log files with Amazon CloudWatch or generic HTTP, you will receive a JSON file similar to the example.

- If you are exporting log files to an Amazon S3 Bucket:
  - Ensure that the S3 output is appropriately configured. Use `'codec ⇒ "json"'` to create a JSON file similar to the example. The S3 output is useless when filters are not applied or this setting is not established because it only obtains **@timestamp**, **host**, and **message** fields from the event.
  - By default, the following line will be written to text files named `'ls.s3.${randomUUID}.${currentTime}.${tags}.${part}.txt`

```
${timestamp} ${host} ${message}(e.g "2022-07-14T12:00:04.314969694Z 10.254.12.248 All pods in
namespace ingress-nginx-private are running | PASS |")
```

> **Note**
>
> Filenames within S3 buckets can be prefixed to create directories, but the filenames are hardcoded and cannot be changed.

- If you are exporting log files to Syslog, it uses the rfc3164 format, by default:

```
${timestamp} ${host} ${process}: ${message} (e.g. "Jul 14 12:00:04 10.254.12.248 LOGSTASH[-]: All pods in
namespace ingress-nginx-private are running              |PASS |")
```

Ensure that Syslog output is appropriately configured. Either use `'codec ⇒ "json"'` to send the whole JSON object in a **${message}** field, or configure the **message** property to include specific fields.

Penetration and load testing policy

Penetration testing is a simulated attack designed to find and exploit vulnerabilities in a system's defenses that attackers could take advantage of, while load testing determines if the system will perform as intended under normal conditions.

Our policies regarding these tests were created to:

- **Preserve platform stability**: Unplanned testing can interfere with our ability to effectively support all of our customers. Since some tests are initially indistinguishable from denial-of-service (DoS) attacks or other serious issues, they can:
    - Set off alarms
    - Cause service shutdowns
    - Add services and IPs to deny lists
    - Prevent our Support teams from taking the appropriate remedial actions.

      This type of disruption can also disproportionately occupy our Support teams, which will delay our response to other customers.
- **Regulate testing**: When you request a load test, we ask that you provide us with your load testing plan, origin of testing information, and the name and contact information for members of your testing team. That way, we can schedule the tests and help ensure that your testing approach is realistic, manageable, and provides meaningful results.
- **Avoid unnecessary testing**: At Ping Identity, we test all of our infrastructure and applications for you using code scans and automated load tests, which ensures that testing methods are consistent and can be compared over time. A third party performs penetration testing.

Penetration and load testing policy

With PingOne Advanced Services, penetration testing is performed by a third party, which is an industry best practice. We can share the results of these tests with you at any time. Our engineers review the test results, eliminate false positives, and perform in-depth analysis regarding the security of your infrastructure and applications.

Regarding load testing, you can:

- Indirectly test Ping infrastructure and applications, as part of a wider test of your own infrastructure and applications, on your staging environment. Load testing is not permitted on your development, test, and production environments.
- Specify the number of identities you intend to create and the throughput levels you intend to simulate, which should not exceed the number of licenses you have.

You cannot:

- Directly test Ping-hosted infrastructure and applications. This specifically applies to DoS or DDoS attacks. Ping Identity already does this testing on your behalf.
- Authorize a third party to perform load testing without Ping's prior written consent. To perform load testing, we must receive your request in writing at least 2 weeks prior to the proposed test date.

Load testing requests

When requesting a load test, we ask that you provide us with your:

- **Load testing plan**: Describe the strategy you intend to follow when testing your own infrastructure and applications.

  Indicate the number of identities you intend to create, and the throughput levels you intend to simulate. These should align with the number of identities and throughput level you agreed upon Ping when you purchased the service, and should not exceed the following thresholds:

  - Agreed number of identities +25%
  - Agreed throughput +50%

  This plan should also avoid unrealistic patterns, such as the setup and tear down of many identities for each load test, and instantaneous user actions, such as changing the password and simultaneously attempting to use the new password.

- **Origin of testing documentation**: Specify whether the testing will originate from an external source over the internet or from an internal source within your organization. If it's originating from an external source, you must also supply IP addresses.

- **Contact name**: Provide the name of a member of your testing team and their contact information in case we have questions or need to stop the testing for any reason.

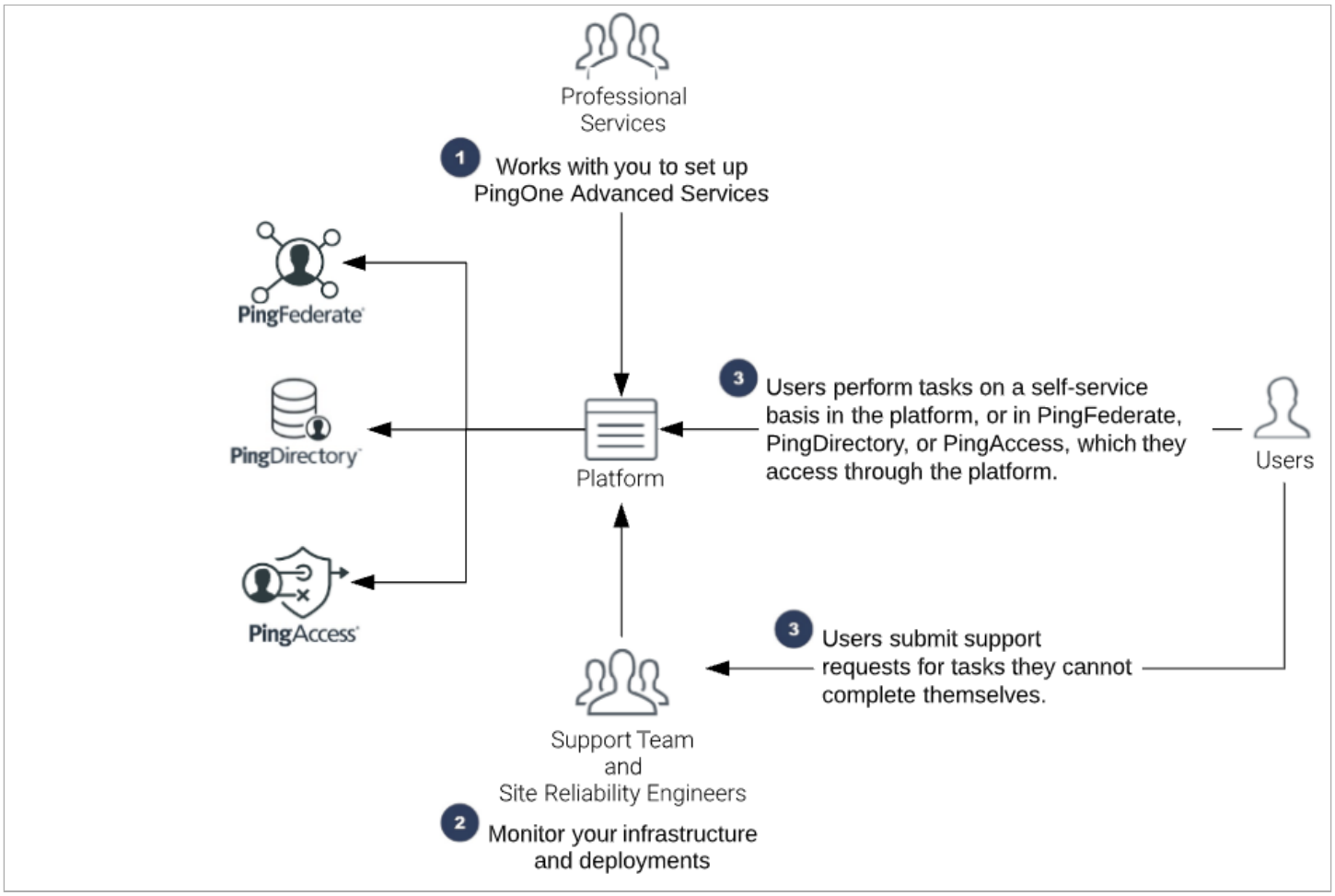
In the unlikely event that a vulnerability is discovered in the Ping infrastructure or applications, we also need you to attest, in writing, that you will not test the vulnerability further than the point of discovery, and that you will immediately report the issue to us.

How PingOne Advanced Services works

PingOne Advanced Services is a hosted service on Amazon Web Services (AWS) that makes it possible for you to manage your service yourself without having to also manage cloud resources, containers, networking, scaling, healing, and backup and restoration.

Diagram that shows how PingOne Advanced Services works

This diagram shows how it works. The Ping Identity Professional Services team works with you to set up the platform, and when it's available, you can perform tasks yourself through the platform or submit support tickets for tasks you can't complete yourself.



1. The Professional Services team works with you to initially set up PingOne Advanced Services.

   The team connects to your on-premise infrastructure and configures your data sources, environments, authentication and password policies, and ensures the platform is working correctly. Ping follows industry best practices and deploys its products using Kubernetes and Docker.

2. The Support team and the site reliability engineers proactively monitor your infrastructure and deployments and attempt to address issues before they become problems. They don't monitor your product configurations. Learn more in the Monitoring and logging section of this guide.

3. When the IAM service is available:
    - You can perform a variety of tasks on a self-service basis in the platform, or in PingFederate or PingDirectory, which you can access from the platform. Learn more about the tasks you can perform yourself in the Self-service tasks section of this guide.
    - There are also a variety of different tasks you cannot complete yourself, so we ask that you submit a service request. These requests are sent to our Support and Professional Services teams, who continually monitor the request queues and will work closely with you to complete the request. Learn more about submitting service requests in the Service requests section of this guide.

All self-service tasks and service requests are also listed and grouped by product in the Task summary table. The table contains links to instructions for completing each task.

Important

Remember that a service request is just a way to initiate a conversation about your needs. The more detail you provide in the request, the better equipped we'll be to help you and appropriately respond.

Signing on to the platform

Click the link you are provided to sign on to the platform.

Steps

1. On the sign on screen, enter your username in the **Username** field.
2. Click **Forgot Password** and then **Submit**.

   You are emailed a password reset code to complete the multi-factor authentication process.
3. Enter the recovery code in the **Recovery Code** field and create a new password. Enter the new password in the **Enter New Password** and **Verify New Password** fields and click **Save**.
4. The first time you log in, you will be prompted to read the End User License Agreement (EULA). Review this agreement and click **Accept** to continue.

   The system displays a green check mark when your authentication is complete. The dashboard opens and displays information about your environments, as shown in the following example. You will likely not see any environments listed the first time you log into the platform.

   In the future, if you forget your password or want to reset it, repeat this process.

Configuring connections for SSO

To allow administrators to use single-sign on (SSO) to access PingOne Advanced Services and the appropriate admin consoles, configure the connections.

> **Note**
>
> PingOne Advanced Services version 1.19.1 is required to configure a connection to PingOne.

Before you begin

Ensure that:

- Your PingOne environment is provisioned.
- You have administrator credentials to sign on to the environment.
- You have the region domain and environment ID for the PingOne Advanced Services environment, which you can get from your Ping Identity team members.

Regardless of which method you choose, you'll need to complete these steps:

Steps

1. Create custom attributes to authenticate users when they sign on.
2. Create an OIDC application and configure it to connect the PingOne environment to the PingOne Advanced Services environment.
3. Configure the identity provider. There are a variety of ways the identity provider (IdP) can be configured.

   Users can be managed:

   1. In the same PingOne environment that contains the OIDC application connection to PingOne Advanced Services, which is the default.
   2. In a PingOne environment that does not contain the OIDC application connection.
   3. By another identity provider who uses OIDC.
4. If you have the Postman application, you can validate the configuration by running a Postman collection.
5. Submit a service request to the Support and Professional Services teams to provide them with details regarding the OIDC application and the name that should display when users sign on.

> **Note**
>
> If users report that they can't access the admin consoles, see Troubleshooting, which provides step-by-step instructions for troubleshooting the connections.

Creating custom user attributes

Create custom user attributes that you will use to authenticate users. You can use the **P1AS Customer Tenant Configuration Postman** collection, or add the attributes manually.

If you're using Postman

Steps

1. Navigate to the first step in the collection: **P1AS Customer Tenant Configuration → Tenant Configuration → Step 1. Create User Custom Attributes**.
2. Drag and drop the step into the **Run order** window.
3. Click **Run** and determine if issues exist.

If you're creating the application manually

Steps

1. Go to **Applications → Applications**.
2. Click the **+** icon.
3. Complete the following fields:
    1. **Application Name**: Enter the name of the application.
    2. **Description**: Enter a meaningful description for the application.
    3. **Application Type**: Select **OIDC Web App**.
4. Click **Save**.
5. On the **Configuration** tab, enter the appropriate URL in the **Redirect URIs** field using the following format:

    ```
    https://auth.pingone.com/<REGION_ID>/rp/callback/openid_connect
    ```

    Use the REGION_ID provided by your Ping Identity team members.
6. Click **Save**.
7. Add an MFA (multi-factor authentication) policy to the application. Learn more in Adding an MFA policy in the PingOne documentation.

    > **Note**
    >
    > Adding this additional layer of security is highly recommended if your users are created and stored in your PingOne environment. If your users are created and stored in an external IdP, we recommend configuring an MFA policy in the third-party OIDC application that is connected to the external IdP.

8. On the **Attribute Mappings** tab, enter the following mappings:

```
“sub” = “User ID”
“email” = “Email Address”
“familyName” = “Family Name”
“givenName” = “Given Name”
“username” = “Username”
“p1asArgoCDRoles” = “P1AS ArgoCD Roles”
"p1asGrafanaRoles” = “P1AS Grafana Roles”
“p1asOpensearchRoles” = “P1AS Opensearch Roles”
“p1asPingAccessRoles” = “P1AS PingAccess Roles”
“p1asPingFederateRoles” = “P1AS PingFederate Roles”
“p1asPrometheusRoles” = “P1AS Prometheus Roles”
"p1asSelfServiceRoles" = "P1AS Self-Service Roles"
```

9. Click **Save** and click the toggle switch to enable the application.

Creating an OIDC application

Now, create an OpenID Connect (OIDC) application and configure it to connect the PingOne environment to the PingOne Advanced Services environment.

You can use the **P1AS Customer Tenant Configuration Postman collection**, or create the application manually.

If you’re using Postman

Steps

1. Navigate to the second step in the collection: **P1AS Customer Tenant Configuration → Tenant Configuration → Step 2. Create OIDC Application**.
2. Drag and drop the step into the **Run order** window.
3. Click **Run** and determine if issues exist.
4. Add an MFA (multi-factor authentication) policy to the application. For instructions, see Adding an MFA policy in the PingOne documentation.

> **Note**
>
> Adding this additional layer of security is highly recommended if your users are created and stored in your PingOne environment. If your users are created and stored in an external IdP, we recommend configuring an MFA policy in the third-party OIDC application that is connected to the external IdP.

If you’re creating the application manually

Steps

1. Go to **Applications → Applications**.
2. Click the **+** icon.

3. Complete the following fields:
    1. **Application Name**: Enter the name of the application.
    2. **Description**: Enter a meaningful description for the application.
    3. **Application Type**: Select **OIDC Web App**.
4. Click **Save**.
5. On the **Configuration** tab, enter the appropriate URL in the **Redirect URIs** field using the following format:

```
https://auth.pingone.com/<REGION_ID>/rp/callback/openid_connect
```

   Use the REGION_ID provided by your Ping Identity team members.

6. Click **Save**.
7. Add an MFA (multi-factor authentication) policy to the application. Learn more in Adding an MFA policy in the PingOne documentation.

> **Note**
>
> Adding this additional layer of security is highly recommended if your users are created and stored in your PingOne environment. If your users are created and stored in an external IdP, we recommend configuring an MFA policy in the third-party OIDC application that is connected to the external IdP.

8. On the **Attribute Mappings** tab, enter the following mappings:

```
“sub” = “User ID”
“email” = “Email Address”
“familyName” = “Family Name”
“givenName” = “Given Name”
“username” = “Username”
“p1asArgoCDRoles” = “P1AS ArgoCD Roles”
"p1asGrafanaRoles” = “P1AS Grafana Roles”
“p1asOpensearchRoles” = “P1AS Opensearch Roles”
“p1asPingAccessRoles” = “P1AS PingAccess Roles”
“p1asPingFederateRoles” = “P1AS PingFederate Roles”
“p1asPrometheusRoles” = “P1AS Prometheus Roles”
"p1asSelfServiceRoles" = "P1AS Self-Service Roles"
```

9. Click **Save** and click the toggle switch to enable the application.

Configuring the identity provider

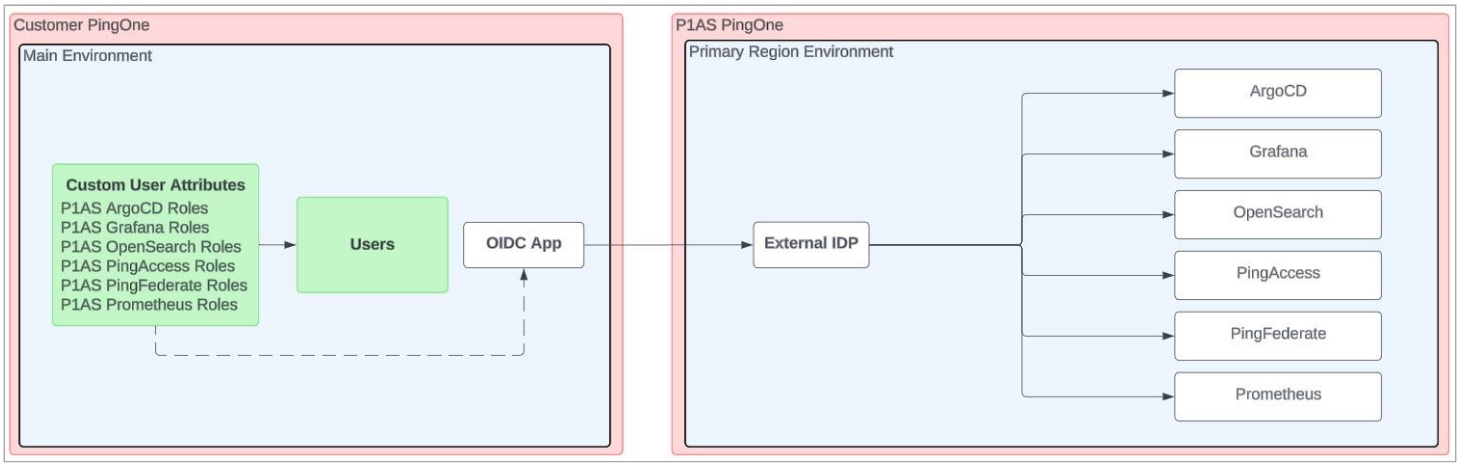
There are a variety of ways the identity provider can be configured:

- Users are managed in the same environment that contains the OIDC application that connects to PingOne Advanced Services.
- Users are managed in an environment that does not contain the OIDC application.

- Users are managed by another identity provider.

Users are managed in the same environment that contains the OIDC application

In this configuration, which is the default, users are managed in the same environment as the OIDC application, which connects to PingOne Advanced Services, as shown in the diagram.

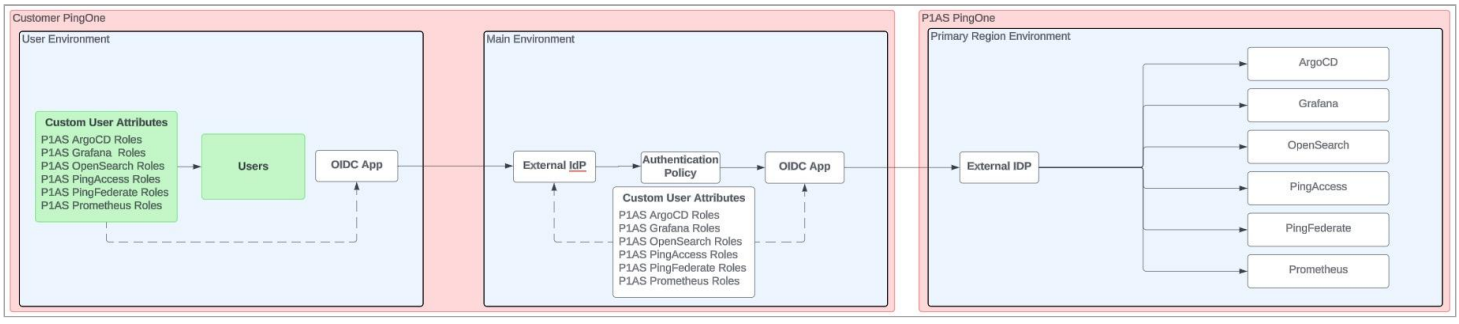


If you have this type of configuration, most of your work is done.

1. First, submit a service request to the Support and Professional Services teams to provide them with details regarding the OIDC application and the name that should display when users sign on.
2. Then, you can begin adding users to this environment and assigning roles. You can find a complete list of PingOne Advanced Services attribute mappings for each administrator role and the permissions each role is assigned in the administrative role mappings.

Users are managed in an environment that does not contain the OIDC application

In this configuration, users are managed in a PingOne environment that does not contain the OIDC application that connects to PingOne Advanced Services, as shown in the diagram.



If you have this type of configuration, you need to configure a connection from the environment containing your users to the environment containing the OIDC application that connects to PingOne Advanced Services:

1. Access the PingOne environment that contains your users and complete the steps listed here.
2. Access the PingOne environment that contains the OIDC application, which connects to PingOne Advanced Services, and complete the steps listed here.

3. Access the PingOne environment that contains your users and complete the process.

1. Access the PingOne environment that contains your users

1. Ensure that the custom user attributes are defined, as described in Creating custom user attributes.
2. Create a new OIDC application to connect these environments. Learn how to create this application in Creating an OIDC application.
3. Copy and save the application client ID, client secret, and OIDC Discovery Endpoint URL, which you'll need to provide in the next task.

2. Access the PingOne environment that contains the OIDC application, which connects to PingOne Advanced Services

1. Access the appropriate PingOne environment.
2. Create an external IdP to configure a connection to the user environment:
    1. Go to **Integrations → External IdPs**.
    2. Click **+ Add Provider**.
    3. Click **OpenID Connect**.
    4. On the **Create Profile** page, enter the following:
        - **Name**: A unique identifier for the IdP.
        - **Description** (optional): A brief description of the IdP.
        - **Icon** (optional): An image to represent the identity provider. Use a file up to 1 MB in JPG, JPEG, GIF, or PNG format. Use a 90 X 90 pixel image.
        - **Login button** (optional): An image to use for the login button displayed to the end user. Use a 300 X 42 pixel image.
    5. Click **Continue**.
    6. Enter the connection and discovery details you copied and saved in step 3 of the previous task:
        - **Client ID**: Enter the client ID for the OIDC application you just created.
        - **Client secret**: Enter the client secret generated for the OIDC application.
        - **Discovery document URI**: Enter the OIDC Discovery Endpoint URL from the OIDC application, and then click **Use Discovery document** to populate the remaining settings. Learn more in Discovery document URI in the PingOne documentation.
    7. Click **Save and Continue**.
    8. On the **Map Attributes** page enter the following mappings:

```
“Username” = “providerAttributes.username”
“External ID” = “providerAttributes.sub”
“Email” = “providerAttributes.email”
“Family Name” = “providerAttributes.familyName”
“Given Name” = “providerAttributes.givenName”
“P1AS ArgoCD Roles” = “providerAttributes.p1asArgoCDRoles
“P1AS Grafana Roles” = “providerAttributes.p1asGrafanaRoles”
“P1AS Opensearch Roles” = “providerAttributes.p1asOpensearchRoles”
“P1AS PingAccess Roles” = “providerAttributes.p1asPingAccessRoles”
“P1AS PingFederate Roles” = “providerAttributes.p1asPingFederateRoles”
“P1AS Prometheus Roles” = “providerAttributes.p1asPrometheusRoles”
"P1AS Self-Service Roles" = "providerAttributes.p1asSelfServiceRoles"
```

9. Click **Save and Finish**.
10. Locate the new external IdP in the list, expand it, and click the **Connections** tab.
11. Copy and save the **Callback URL** to use in a later step.
12. Click the toggle switch to enable the application.

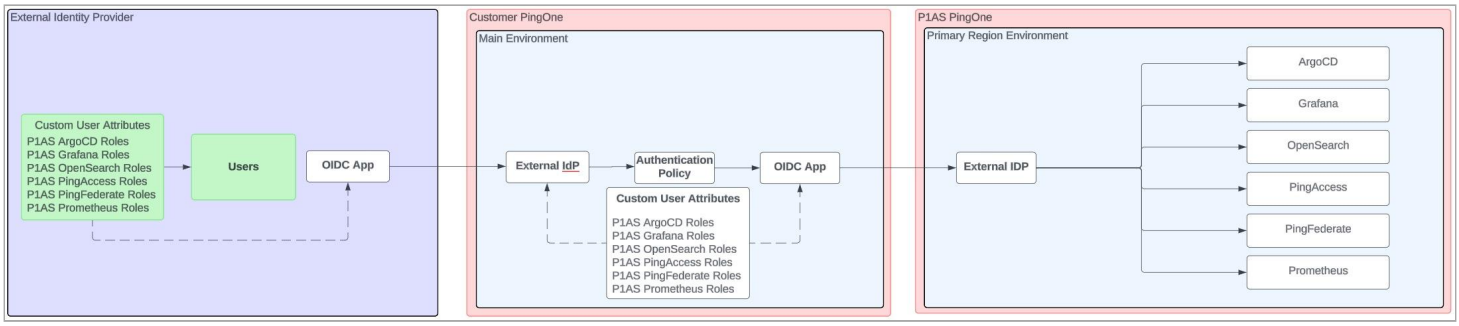
3. Create an authentication policy for the external IdP:
    1. Go to **Authentication → Authentication**.
    2. Click **+ Add Policy**.
    3. Enter a policy name.
    4. From the**Step Type** list, select **External identity provider**.
    5. From the **External identity provider** list, select the external provider you just configured and click **Save**.
4. Add the authentication policy to the OIDC application:
    1. Go to **Applications → Applications**, and select the OIDC application you created in the previous step.
    2. Select the **Policies** tab and click **+ Add Policies**.
    3. Select the authentication policy you created in the previous step and click **Save**.

3. Access the PingOne environment that contains your users

1. Go to **Applications → Applications**, and select the new OIDC application.
2. Click the **Configuration** tab and then click the **Pencil** icon.
3. In the **Redirect URIs** field, enter the **Callback URL** you copied and saved in the previous task and click **Save**.
4. Submit a service request to the Support and Professional Services teams to provide them with details regarding the OIDC application and the name that should display when users sign on.
5. Now, you can begin adding users to this environment and assigning roles. You can find a complete list of PingOne Advanced Services attribute mappings for each administrator role and the permissions each role is assigned in Administrative role mappings.

Users are managed by another identity provider

In this configuration, users are managed in your PingOne environment that does not contain the OIDC application connection, as shown in the diagram.



If you have this type of configuration, you need to configure a connection from the external identity provider that manages your users to the PingOne environment that contains the OIDC application that connects PingOne to PingOne Advanced Services.

1. Access the external identity provider environment that contains your users and complete the steps listed here.
2. Access the PingOne environment that contains the OIDC application and complete the steps listed here.
3. Access the external identity provider environment that contains your users and complete the process.

1. Access the external identity provider environment that contains your users

1. Ensure that the custom user attributes are defined as described in Creating custom attributes.
2. Create a new OIDC application to connect these environments.
    1. Go to **Applications → Applications**.
    2. Complete the following fields:
        - **Application Name**: Enter the name of the application.
        - **Description**: Enter a meaningful description for the application.
        - **Application Type**: Select **OIDC Web App**.
    3. On the **Configuration** tab, click the **Pencil** icon, select the following options, and click **Save**.
        - In the **Response Type** field, select **Code**.
        - In the **Grant Type** field, select **Authorization Code**.
        - In the **Token Auth Method** field, select **Client Secret Basic**.
    4. Add a multi-factor authentication (MFA) policy to the application. Refer to your external identity provider documentation for instructions on adding an MFA policy.
    5. Click the **Attribute Mappings** tab and enter the following mappings:

```
“sub” = “User ID”
“email” = “Email Address”
“familyName” = “Family Name”
“givenName” = “Given Name”
“username” = “Username”
“p1asArgoCDRoles” = “P1AS ArgoCD Roles”
“p1asGrafanaRoles” = “P1AS Grafana Roles”
“p1asOpensearchRoles” = “P1AS Opensearch Roles”
“p1asPingAccessRoles” = “P1AS PingAccess Roles”
“p1asPingFederateRoles” = “P1AS PingFederate Roles”
“p1asPrometheusRoles” = “P1AS Prometheus Roles”
"p1asSelfServiceRoles" = "P1AS SelfService Roles"
```

6. Click the toggle switch to enable the application.
7. Copy and save the application client ID, client secret, and OIDC Discovery Endpoint URL, which you'll need to provide in the next step.

2. Access the PingOne environment that contains the OIDC application

1. Access the appropriate PingOne environment.
2. Create an external IdP to configure a connection to the user environment:
    1. Go to **Integrations → External IDPs**.
    2. Click **+ Add Provider**.
    3. Click **OpenID Connect**.
    4. On the **Create Profile** page, enter the following:
        - **Name**: A unique identifier for the IdP.
        - **Description** (optional): A brief description of the IdP.
        - **Icon** (optional): An image to represent the identity provider. Use a file up to 1 MB in JPG, JPEG, GIF, or PNG format. Use a 90 X 90 pixel image.
        - **Login button** (optional): An image to use for the login button displayed to the end user. Use a 300 X 42 pixel image.
    5. Click **Continue**.
    6. Enter the connection and discovery details you copied and saved in step 2 of the previous task:
        - **Client ID**: Enter the client ID for the OIDC application you just created.
        - **Client secret**: Enter the client secret generated for the OIDC application.
        - **Discovery document URI:** Enter the OIDC Discovery Endpoint URL from the OIDC application, and then click **Use Discovery document** to populate the remaining settings. Learn more in Discovery document URI in the PingOne documentation.
    7. Click **Save and Continue**.

8. On the **Map Attributes** page enter the following mappings:

```
“Username” = “providerAttributes.username”
“External ID” = “providerAttributes.sub”
“Email” = “providerAttributes.email”
“Family Name” = “providerAttributes.familyName”
“Given Name” = “providerAttributes.givenName”
“P1AS ArgoCD Roles” = “providerAttributes.p1asArgoCDRoles
“P1AS Grafana Roles” = “providerAttributes.p1asGrafanaRoles”
“P1AS Opensearch Roles” = “providerAttributes.p1asOpensearchRoles”
“P1AS PingAccess Roles” = “providerAttributes.p1asPingAccessRoles”
“P1AS PingFederate Roles” = “providerAttributes.p1asPingFederateRoles”
“P1AS Prometheus Roles” = “providerAttributes.p1asPrometheusRoles”
"P1AS SelfService Roles" = "providerAttributes.p1asSelfServiceRoles"
```

9. Click **Save and Finish**.
10. Locate the new external IdP in the list, expand it, and click on the **Connections** tab.
11. Copy and save the **Callback URL** to use in a later step
12. Click the toggle switch to enable the application.

3. Create an authentication policy for the external IdP:
    1. Go to **Authentication → Authentication**.
    2. Click **+ Add Policy**.
    3. Enter a policy name.
    4. From the **Step Type** list, select **External identity provider**.
    5. From the **External identity provider** list, select the external provider you just configured and click **Save**.
4. Add an authentication policy to the OIDC application:
    1. Go to **Applications → Applications**, and select the OIDC application you created in the previous step.
    2. Select the **Policies** tab and click **+ Add Policies**.
    3. Select the authentication policy you created in the previous step and click **Save**.

3. In the external identity provider environment that contains your users

1. Go to **Applications → Applications** and select the new OIDC application.
2. Click the **Configuration** tab and then click the **Pencil** icon.
3. In the **Redirect URIs** field, enter the **Callback URL** you copied and saved in the previous task and click **Save**.
4. Submit a service request to the Support and Professional Services teams to provide them with details regarding the OIDC application and the name that should display when users sign on.

5. Now, you can begin adding users to this environment and assigning roles. You can find a complete list of PingOne Advanced Services attribute mappings for each administrator role and the permissions each role is assigned in Administrative role mappings.

Validating the configuration

If you have Postman, you can validate the configuration by running Postman collections.

To validate the custom user attributes that you created:

1. Navigate to the following folder:

   P1AS Customer Tenant Configuration → Tenant Validation → Validate User Attributes

2. Drag and drop the step into the **Run order** window.
3. Click **Run** and determine if issues exist.

To validate the OIDC application that you created:

1. Navigate to the following folder:

   P1AS Customer Tenant Configuration → Tenant Validation → Validate OIDC application

2. Drag and drop the step into the **Run order** window.
3. Click **Run** and determine if issues exist.

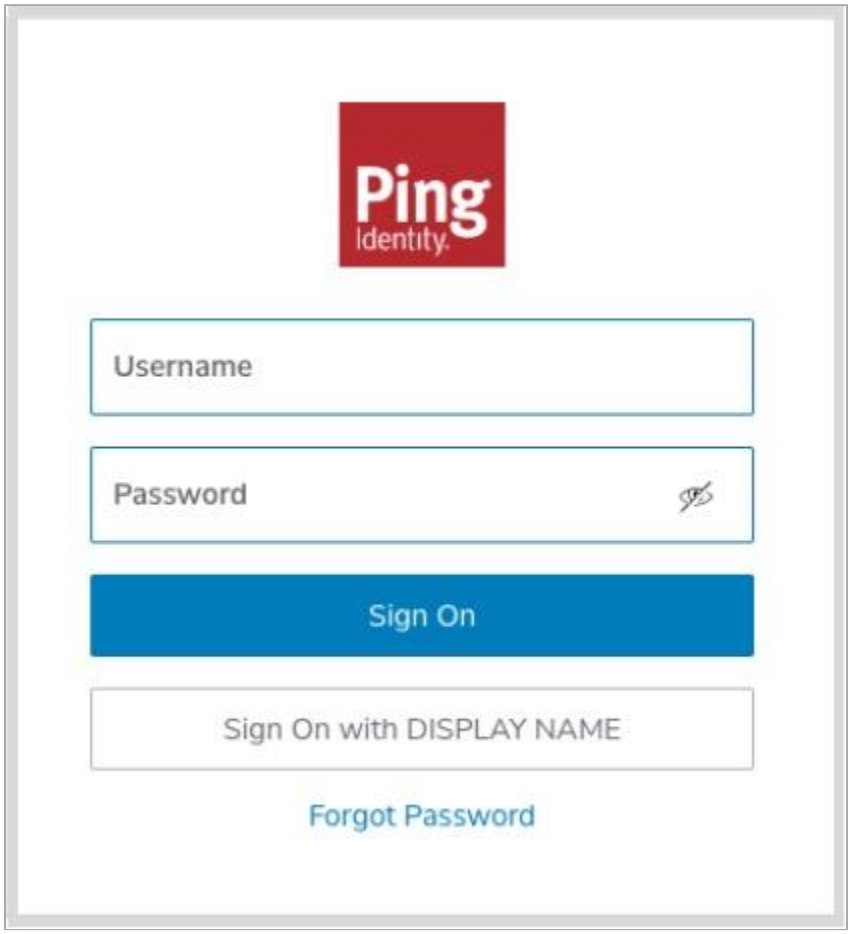
Submitting a service request

To complete the connection, submit a service request through the Support Portal.

Steps

1. Complete the following fields:
   - **Subject**: Enter a description of your request, including the action to be taken.
   - **Environment Type**: Specify the type of environment affected by this request.
   - **Proposed Change Window**: Specify the dates or times in which you want the work complete.
2. In the **Capability** list, select **Advanced/Other**.
3. In the **Business Priority** list, select the appropriate description:
   - Change needed by deadline to avoid business impact
   - Change modifies existing functionality
   - Change adds new functionality
4. In the **Description** field, provide the following information regarding the OIDC application you created:
   - The **Client ID**, which displays on the **OIDC application Overview** page.

- The **Client Secret,** which also displays on the **OIDC application Overview** page.
- The **Issuer URL**, which displays on the **OIDC application Configuration** page, in the URLs section.
- The **Display Name**, which is the name that you want displayed to your users when they sign on, as shown here.



5. If you are tracking your request within your organization, enter the tracking ID or ticket number associated with it in the **Customer Tracking ID** field.
6. To submit your request, click **Save**.

Configuring Postman

If you plan to use Postman to configure your connections, you'll need to ensure that several collection variables are set and that Postman is correctly configured. You'll also need to download the collection. Learn more in Download the Postman collection.

Steps

1. Add the API domain for your PingOne region to the collection variable *apiPath*, and then add the auth domain for the region to the collection variable *authPath*. Learn more in API requests in the PingOne Developers documentation.
2. Get an access token from a worker application. You can use an existing worker application or create a new one.

   Either way, ensure that the **Environment Admin** and **Client Application Developer** roles are assigned. Learn more in Create an admin Worker app connection in the PingOne Developers documentation.

Then, get the token. Learn more in Get a PingOne admin access token in the PingOne Developers documentation.

To get a token from a different worker application in a different sandbox environment, run the token request endpoint using the client ID and client secret of the worker application to authenticate the request. Learn more in Worker applications in the PingOne Developers documentation.

Add the access token to the collection variable *accessToken*.

3. Choose the PingOne environment that will act as the OIDC identity provider, which will connect to the PingOne Advanced Services environment.
4. Add the environment ID to the collection variable *envID*.
5. Request the region domain and environment ID for your primary region from PingOne Advanced Services.
6. Add the auth domain for the PingOne Advanced Services environment to the collection variable *p1asAuthPath*.
7. Add the environment ID for the PingOne Advanced Services tenant to the collection variable *p1asEnvID*.

Download the Postman collection

There are two different methods you can use to retrieve a Postman collection into your workspace:

1. Fork the collection into your workspace. The Postman application retains an association between the source and your fork. If Ping Identity changes the source collection, you can pull those changes into the fork in your workspace.
2. Import the collection into your workspace. This is a one-time transfer and retains no association to the source collection.

Steps

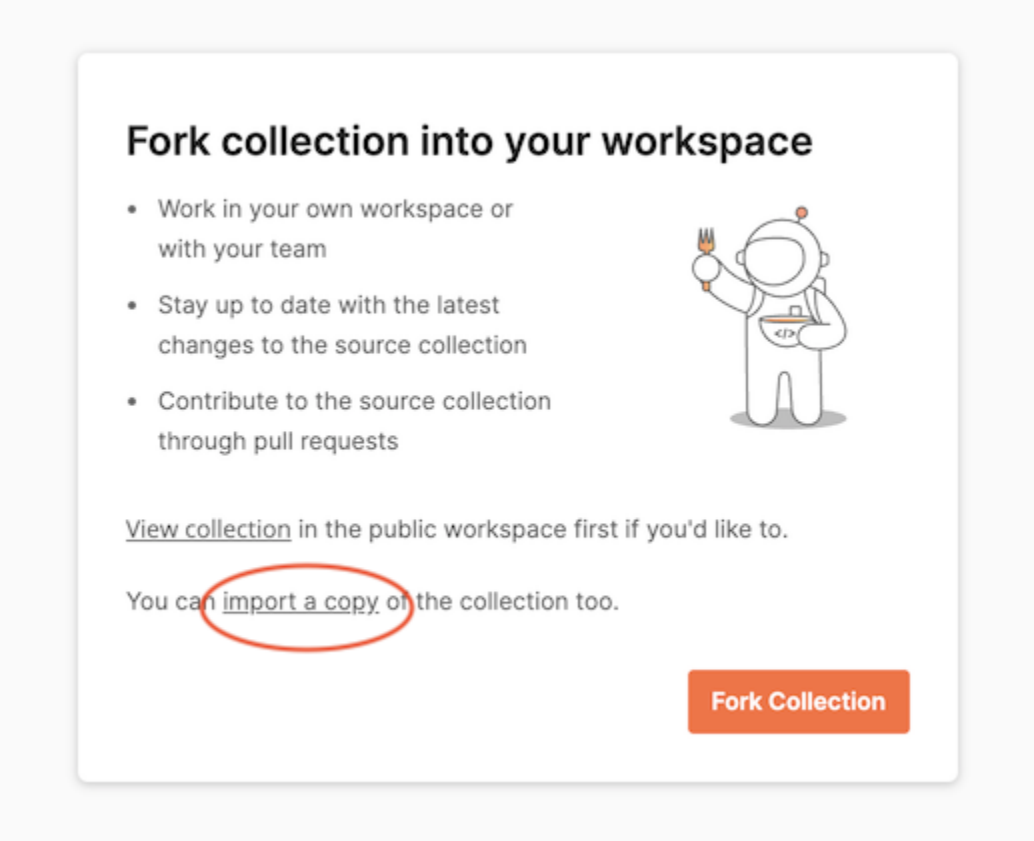
To retrieve the collection:

1. Click **Run in Postman**.

   Run in Postman

2. At the prompt, click **Fork Collection** at the bottom of the dialog or click **import a copy** near the bottom of the dialog.

> **Note**
>
> You must be signed on to your Postman account to retrieve the collection.



3. Follow the on-screen instructions to fork or import the collection. You might be prompted to open your Postman app and to select a Postman workspace for the retrieved collection.

When you fork a Postman collection, you create a copy of it in a different workspace. Forking a collection creates a linked version that synchronizes with its source collection.

You'll see this synchronization when you click the ellipsis icon on the forked collection. If changes are available, the context menu displays a **Pull changes** button, which you can click to compare the fork to the source collection and pull changes into your fork. You can also watch the collection so that you are notified when the source changes.

If you import a collection, a copy is created with no link back to the source. The collection is static, which might be useful in some situations. For example, if you intend to keep and consume only portions of the collection, a link back to the source is not needed.

But you don't have to choose between these two methods. You can fork a copy to track the source *and* import a copy for experimentation.

The environment downloaded with the collection of requests contains every variable used in the collection. Each request that creates a new object with an ID has a script that:

1. If not available, create an environment variable unique to that service.
2. Assigns the id of the newly created object to that environment variable.

Troubleshooting

If your users are having trouble accessing their admin consoles, determine where the users are managed and complete the appropriate set of steps:

- Users are managed in a PingOne environment
- Users are managed by an external identity provider

Users are managed in a PingOne environment

If your users are managed in a PingOne environment, test the connection between that environment and the environment containing the OIDC application that connects to PingOne Advanced Services.

About this task

To test this connection, create a test user in the environment and use the new user credentials to sign on to the appropriate console.

Steps

Use Postman to create the test user, or create the user manually.

If you're using Postman:

1. Navigate to the following step in the collection:

   P1AS Customer Tenant Configuration → Troubleshooting → Create Test User to Validate P1AS Connection.

2. Drag and drop the step into the **Run order** window.
3. Click **Run** and determine if issues exist.

If you're creating a test user manually:

1. Ensure that the user is added to the appropriate population and that the appropriate IdP is selected. For instructions, see Adding a user in the PingOne documentation.
2. Assign the user the appropriate roles and user attributes. You can find a complete list of PingOne Advanced Services attribute mappings for each administrator role, and the permissions each role is assigned, in Administrative role mappings.
3. Use the appropriate console URL and the new test user's credentials to sign on.

   If you're able to sign on, that means that the connection works and the issue likely involves users' roles, permissions, or the user attributes assigned.

4. If you're not able to sign on, access the user's profile and determine if they have the appropriate roles and user attributes assigned.

Users are managed by an external identity provider

If your users are managed by an external identity provider, test the connections between the environments.

About this task

There are two different connections to test:

- The connection between the environment containing the users and the environment containing the OIDC application. To test this connection, complete the troubleshooting steps outlined in Users are managed in a PingOne environment.
- The connection between the external IdP and the environment that contains the OIDC application.

To test this connection, attempt to access the admin consoles from the external identity provider:

Steps

1. Get the username and password for the user.
2. Open a browser window and enter the admin console URL.
3. Enter the username and password and click **Sign On**.
    - If you're able to sign on, that means that the connection works.
    - If you're not redirected to the external identity provider, ensure that the authentication policy that the OIDC application is using includes the external identity provider:
        - If you're using login authentication, ensure that the external identity provider is added as a **Presented identity provider**. To learn more, see Adding a login authentication step in the [pingone] documentation.
        - If you're using identifier-first authentication, ensure that the external IdP is added as a rule or as a **Presented identity provider**. To learn more, see Adding an identifier-first authentication step.
        - If you're using external identity provider authentication policies, ensure that the external IdP is added as an **External identity provider**. To learn more, see Adding an external identity provider sign-on step.
    - If you receive an error message regarding missing roles:
        - Ensure that the user has the appropriate roles and attributes assigned.
        - Ensure that the custom user attributes are correctly defined and mapped.

Administrative role mappings

Refer to the following:

- Argo CD roles
- Grafana roles
- OpenSearch roles
- PingAccess roles
- PingFederate roles
- Prometheus roles
- Self-Service roles

Argo CD roles

Attribute mapping	Permissions
argo-configteam	Argo CD restart statefulset access for the Dev and Test environments.

Grafana roles

Attribute mapping	Permissions
dev-graf-editor	Grafana editor access for the Dev environment.
test-graf-editor	Grafana editor access for the Test environment.
stage-graf-editor	Grafana editor access for the Stage environment.
prod-graf-editor	Grafana editor access for the Prod environment.

OpenSearch roles

Attribute mapping	Permissions
os-configteam	OpenSearch admin access for all environments.

PingAccess roles

Attribute mapping	Permissions
dev-pa-admin	PingAccess admin access for the Dev environment.
dev-pa-audit	PingAccess audit access for the Dev environment.
dev-pa-platform	PingAccess platform access for the Dev environment.
test-pa-admin	PingAccess admin access for the Test environment.
test-pa-audit	PingAccess audit access for the Test environment.
test-pa-platform	PingAccess platform access for the Test environment.
stage-pa-admin	PingAccess admin access for the Stage environment.
stage-pa-audit	PingAccess audit access for the Stage environment.
stage-pa-platform	PingAccess platform access for the Stage environment.

Attribute mapping	Permissions
prod-pa-admin	PingAccess admin access for the Prod environment.
prod-pa-audit	PingAccess audit access for the Prod environment.
prod-pa-platform	PingAccess platform access for the Prod environment.

PingFederate roles

Attribute mapping	Permissions
dev-pf-audit	PingFederate audit access for the Dev environment.
dev-pf-crypto	PingFederate crypto access for the Dev environment.
dev-pf-expression	PingFederate expression access for the Dev environment.
dev-pf-roleadmin	PingFederate role admin access for the Dev environment.
dev-pf-useradmin	PingFederate user admin access for the Dev environment.
test-pf-audit	PingFederate audit access for the Test environment.
test-pf-crypto	PingFederate crypto access for the Test environment.
test-pf-expression	PingFederate expression access for the Test environment.
test-pf-roleadmin	PingFederate role admin access for the Test environment.
test-pf-useradmin	PingFederate user admin access for the Test environment.
stage-pf-audit	PingFederate audit access for the Stage environment.
stage-pf-crypto	PingFederate crypto access for the Stage environment.
stage-pf-expression	PingFederate expression access for the Stage environment.
stage-pf-roleadmin	PingFederate role admin access for the Stage environment.
stage-pf-useradmin	PingFederate user admin access for the Stage environment.
prod-pf-audit	PingFederate audit access for the Prod environment.
prod-pf-crypto	PingFederate crypto access for the Prod environment.
prod-pf-expression	PingFederate expression access for the Prod environment.
prod-pf-roleadmin	PingFederate role admin access for the Prod environment.

Attribute mapping	Permissions
prod-pf-useradmin	PingFederate user admin access for the Prod environment.

Prometheus roles

Attribute mapping	Permissions
prom	Prometheus admin access for all environments.

Self-Service roles

Attribute mapping	Permissions
dev-tls-audit	TLS read-only access for the Dev environments.
dev-tls-admin	TLS admin access for the Dev environment.
test-tls-audit	TLS read-only access for the Test environment.
test-tls-admin	TLS admin access for the Test environment.
stage-tls-audit	TLS read-only access for the Stage environment.
stage-tls-admin	TLS admin access in the Stage environment.
prod-tls-audit	TLS read-only access for the Prod environment.
prod-tls-admin	TLS admin access for the Prod environment.
all-tls-audit	TLS read-only audit access for all environments.
all-tls-admin	TLS admin access for all environments.

Renewing Let’s Encrypt certificates

To ensure that communications between PingOne Advanced Services products and services remain encrypted and secure, Let's Encrypt certificate chains are used by default. These chains verify that the sender and all certificate authority (CA) certificates in the chain are trustworthy. Learn more about how these certificate chains work in How it Works in the Let's Encrypt documentation.

For PingOne Advanced Services, the Let's Encrypt certificate chain consists of three different certificates:

The Advanced Services end-entity certificate

The chain begins with an RSA 2048-bit end-entity certificate issued by Let's Encrypt, which is signed by the intermediate CA.

This certificate expires every 90 days, but PingOne Advanced Services rotates every 60 days to avoid expiration overlap, by default. Avoid adding this certificate to your truststore because it rotates so often.

The R10 or R11 intermediate CA

This certificate, next in the chain, is signed by the root CA.

These certificates expire every 3 years. Avoid adding them to your truststore as well. Because they sign the end-entity certificate, and that certificate rotates every 60 days, you would have to maintain both versions of the certificates for the chain to work.

The ISRG Root X1 root CA

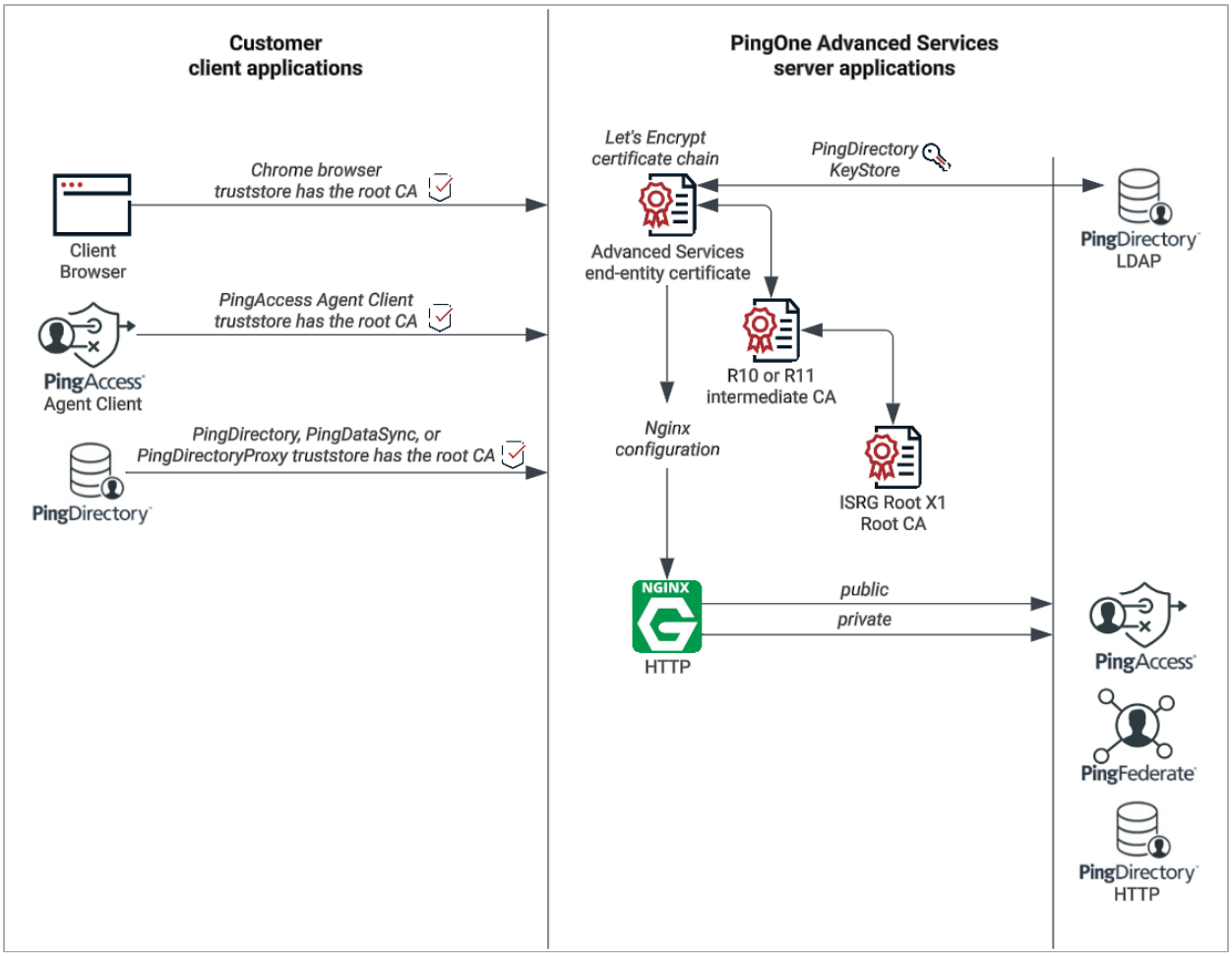
The chain ends with the root CA certificate, which is self-signed.

This certificate will expire in 2035, and every 20 years after that, so you don't need to worry about renewing it for several years.

> **Note**
>
> You'll receive many updates regarding the ISRG Root X1 Root CA before it expires in 2035.

You must add the root CA to your client truststore for the certificate chain to work. You can find instructions below.

Learn more about how these certificates keep customer client applications and PingOne Advanced Services server applications secure in this network diagram:



Adding the root CA to the client truststore

Add the root CA to your client truststore to ensure the certificate chain will work.

On-premise, non-Ping Identity client applications

To add the root CA to your on-premise, non-Ping Identity client application:

1. Download the ISRG Root X1 Certificate from Let's Encrypt.
2. Add the root CA to your truststore. Refer to your application documentation for instructions.

On-premise PingDirectory, PingDirectoryProxy, and PingDataSync

To add the root CA to your on-premise PingDirectory application and its PingDirectory instance clients, open a terminal window and enter the following:

```
# 1) Download "ISRG Root X1" Root CA from Let's Encrypt to /tmp directory
$ curl https://letsencrypt.org/certs/isrgrootx1.pem -o /tmp/pingone-advanced-services-root-ca.pem
# 2) Add "ISRG Root X1" Root CA to truststore
$ bin/manage-certificates \
  import-certificate \
  --keystore config/truststore \
  --keystore-password-file config/truststore.pin \
  --alias "pingone-advanced-services-isrg-root-x1-ca-expires-2035" \
  --certificate-file /tmp/pingone-advanced-services-root-ca.pem --no-prompt
# 3) Remove "ISRG Root X1" Root CA resource from server /tmp directory
$ rm -o /tmp/pingone-advanced-services-root-ca.pem
```

On-premise PingAccess Agent

To add the root CA to your on-premise, PingAccess Agent application:

1. Download the ISRG Root X1 Certificate from Let's Encrypt.
2. Add the root CA to your truststore. You can find instructions in Rotating a CA in the PingAccess documentation.

Task summary table

The following table lists the tasks that users can perform on a self-serve basis and the tasks for which they must submit service requests to the Support team. These tasks are grouped by product and link to instructions on how to complete each task.

Keep in mind that the Professional Services team helps with initial setup including:

- Deployment
- Authentication policies
- Application onboarding

Additional projects can be arranged at any time for additional use cases or complicated tasks, including:

- Custom integration kits
- Custom data sources
- Migration projects
- Application onboarding
- Significant changes to the original setup

Self-service

Users can perform these tasks themselves through the product consoles.

Platform	PingAccess	PingDirectory	PingFederate
Users can manage administrators themselves in the platform.	Users can manage a variety of access management features for each environment using PingAccess, which is accessible through the platform.	Users can modify data objects using their preferred LDAP browser.	Users can manage applications, authentication policies, and data sources using the PingFederate admin console, which is accessible through the platform.
• Manage administrators • View the platform activity log • Creating and updating virtual hosts	• Manage applications • Manage authentication requirements • Manage identity mappings • Manage rules • Manage web sessions	• Manage entries	• Manage applications • Manage authentication policies • Manage data sources

Service requests

Our support teams will perform these tasks on your behalf, in accordance with Support guidelines.

Platform	PingAccess	PingDirectory	PingFederate
Users submit service requests for additional platform tasks.	Users submit service requests for file system changes.	Users submit service requests for data server configuration changes.	Users submit service requests for file system changes.
• Administrator MFA • Approve merge request • Restore from a backup • Creating and updating virtual hosts • Enable outbound provisioning • Load or performance test • PingDirectory truststore certificate import • SIEM integrations • Rollback SIEM • Subscribe to SNS alerts • Update TLS certificate • Upgrades	• Enable debug logger • Integration kits • Update templates • Virtual hosts	• ACIs • Email templates • Indexes • JSON field constraints • Password policies • Plugins • Schema - attribute type • Schema - objectClass • Virtual attribute	• Elevate admin • Enable debug logger • Password rules • Integration kits • Update templates

Self-service

You can complete a variety of tasks yourself, either directly in the platform, or using PingAccess, PingDirectory, or PingFederate, which are accessible from the platform.

Refer to the following:

- Platform self-service
- PingAccess self-service
- PingDirectory self-service
- PingFederate self-service

Platform self-service

In the PingOne Advanced Services platform, you can:

- Manage administrators
- View platform activity log
- Creating and updating virtual hosts

Managing administrators

If you are an administrator, you can view a list of administrators who share the same customer with you, add and remove additional administrators from the system, and update their information anytime it changes.

Steps

1. To add a new administrator:
    1. To access the **Administrators** page, click **Administrators**.

       You see a list of the administrators with whom you share customers. Clicking the expandable icon associated with each administrator reveals their first and last names, contact phone number, contact email address, and role.
    2. To add an administrator, click **Add Administrator**.
    3. Enter the new administrator's first name, last name, phone number, and email address in the appropriate fields and click **Save**.

       The resulting text provides new administrators with the sign-on URL, their user name, and instructions for using a recovery code to complete the initial sign-on process. The new user's user name is automatically created and cannot be changed.

       If the new administrator is not authorized to access customer information, or if the new administrator has the same first and last name as another administrator for the same customer, you can't add the new administrator to the system.
    4. To inform the new IAM administrator that you have provisioned their account, copy and paste the text into an email and send it to the new administrator.
2. To edit an administrator's information or your own:
    1. Click the **Pencil** icon.

       All of the editable information, which is obtained from the PingOne database, shows on one page.
    2. Update this information as necessary and click **Save**.
    3. Inform the administrator that you updated the information.
3. To delete an administrator, click its associated **Delete** icon.

> **Important**
>
> Understand that if you delete an administrator from the platform, they will not be able to sign on to the PingFederate or PingAccess consoles.
> You cannot delete yourself.

The administrator is removed from the platform and the PingOne database.

Viewing the platform activity log

The activity log displays PingOne administrator sign-on information.

Steps

1. To view the activity log, click **Activity Log** on the left side of the page.

   Result:

   This log provides a timestamp of the date and time the activity occurred, the environment or user affected, the action taken, and the user who performed the action.

2. Use this information to troubleshoot platform-related issues.

Creating and updating virtual hosts

You and your administrators can create and update virtual host certificates and TLS configurations yourselves. Configurations are automatically replicated to child regions in PingOne Advanced Services for the following applications:

- PingFederate
- PingFederate Admin API
- PingAccess

- PingAccess Admin API
- PingAccess Agents
- PingDirectory
- Delegated Admin

Supported functions include:

- Create/List/Update/Delete configurations

> **Note**
>
> With the CREATE certificates route, the certificate and key must be formatted into a single line with line-break characters.
> Linux/Unix:
> `awk 'NF {sub(/\r/, ""); printf "%s\\n",$0;}' "cert_or_pkey.pem" | pbcopy`
> Windows PowerShell or PowerShell Core:
> `(Get-Content -Raw -Path "cert_or_pkey.pem") -replace "`r?`n", '\n' | Set-Clipboard`

> **Note**
>
> The GET certificates route does not return the certificate's fullchain and private key. It is up to the user to keep track of that information.

Also note that after you create or update a configuration, it will take some time for the virtual host to become available.

- Rollback configurations

> **Note**
>
> Configurations can only be rolled back once. Then the configuration needs to be updated again at least once before rollback will succeed again.

Rollback routes also support an optional `dry_run` query parameter. Setting it to `true` in a request gets the expected version after rollback, but does not do the rollback.

Limitations include:

- You cannot currently create or update the following items yourself. Submit a service request instead.
  - MTLS configurations
  - Configurations that need custom annotations, such as "cors-all-origin"
  - Private Ingress configurations
  - EC or ECC TLS certificates
- You cannot currently create or update PingFederate Admin UI or the PingAccess Admin UI in PingOne Advanced Services.

About this task

The API requires a JWT Bearer token for authenticating the requests. This token can be retrieved using user credentials or client credentials.

- Authenticate using user credentials
- Authenticate using client credentials

The API also includes interactive documentation for both developers and non-developers to explore the API endpoints, view documentation for the API, and experiment with API calls. You can make API calls from an interactive user interface, custom applications, or from command line tools such as cURL.

The Swagger UI component that displays the Self-Service admin API documentation uses OpenAPI specification (OAS) 3.1. Access to these specifications simplifies the process of integrating the **Self-Service** API with modern API clients, such as Postman.

Learn more in Accessing the API interactive documentation.

Accessing the API interactive documentation

To access the administrative API documentation:

1. Start a web browser.
2. Browse to the URL:

```
https://self-service-api.<environment>-<customer>.<region>.ping.cloud/docs
```

> **Note**
>
> The API is also documented in the OpenAPI Specification, previously known as the Swagger Specification. Go to:

```
https://self-service-api.<environment>-<customer>.<region>.ping.cloud/api/v1/openapi.json
```

Authenticate using user credentials

To authenticate using user credentials, you'll use the Swagger UI to generate an access token.

Before you begin

To access the API using user credentials, ensure that users are assigned the **P1AS Self-Service** role. To assign these roles, you must be a PingOne Identity Data Admin. To learn more, access the instructions in Assigning self-service roles.

Steps

1. Navigate to the interactive documentation. You can find instructions in Accessing the interactive documentation.
2. Click **Get Token** at the top of the page.

   A new tab opens and redirects you to the sign-on page.
3. Enter your credentials and click **Submit**.

   If authentication is successful, you're redirected to the **Success** page and a **Copy Token** button displays.

4. Click **Copy Token**.
5. From there, you can use the token in different ways. You can:
    - Use the Swagger UI.
        1. Click **Authorize**, which is next to **Get Token**.
        2. Paste the token in the input field, and **Authorize**, and then click **Close**. All API requests that come from Swagger UI will now be authenticated.
    - Query the API directly using other tools, such as Postman or cURL, and include the bearer token in the headers.

      Example

      ```
      {"Authorization": "Bearer {TOKEN}"}
      ```

Authenticate using client credentials

To authenticate using client credentials, create a client credentials application in your PingOne environment and then generate an access token.

To set this up, you'll need to:

- Create the client credentials application
- Generate the token

You should also restrict access to this application to PingOne administrators. Learn more in Restricting access to the application.

> **Note**
>
> In addition to the JWT Bearer token, the API uses role-based access control, as described in Administrative role mappings. The roles assigned to the accounts affect the results of the API calls.

Creating the client credentials application

Start by creating an OIDC application in PingOne.

Steps

1. Go to **Applications** > **Resources**.
2. Click the **+** icon.
3. Create the resource by completing these fields:
    - **Resource name**: A unique identifier for the resource.
    - **Description** (optional): A brief characterization of the resource that helps identify it.
4. Click **Next**.

5. On the **Attributes** page, click **Add** to add a new attribute.
6. Name the new attribute `groups`.

   Set the value to a hardcoded list of valid **Self-Service** roles. For example, `{“dev-tls-admin”, “prod-tls-audit”}`. You can find a complete list of these roles in Administrative role mappings.

   > **Note**
   >
   > The **Self-Service** attribute must be set up for it to display in the list. You can find instructions on adding this attribute in Creating custom attributes.

7. Click **Next**.
8. On the **Scopes** page, add a new scope to map the **Self-Service** role to the new application. Click **Add Scope** and complete the following fields:
   - **Scope name**: A unique identifier for the scope.
   - **Description** (optional): A brief characterization of the scope that helps identify it.
9. Click **Save**.
10. Now, add the OIDC application. Go to **Applications** > **Applications**.
11. Click the **+** icon.
12. Complete the following fields:
    - **Application name**: A unique identifier for the application.
    - **Description** (optional): A brief characterization of the application that helps identify it.
    - **Icon** (optional): A graphic representation of the application. Use a file up to 1 MB in JPG, JPEG, GIF, or PNG format.
13. In the list of available application types, select **OIDC Web App**. Click **Save**.
14. On the **Configuration** tab, click the **Pencil** icon to edit the configuration.
    - Change the **Response Type** to none by clearing all the options.
    - Change the **Grant Type** to **Client Credentials**.
15. Click **Save**.
16. On the **Resources** tab, click the **Pencil** icon to add the scope you added in step 8 to the application.
17. Click **Save** and click the toggle to enable the application.

Generating the token

Access the new application in the PingOne console to generate an access token.

Steps

1. Follow the steps outlined in Getting an access token in the PingOne documentation.
2. Include the bearer token in the headers.

   Example

   ```
   {"Authorization": "Bearer {TOKEN}"}
   ```

Restricting access to the application

To ensure that only administrators can generate access tokens, restrict access to it.

Steps

1. Select the application, click the **Access** tab, and then the **Pencil** icon.
2. Select the **Admin Only Access** checkbox and click **Save**.

Assigning Self-Service roles

Assign users the appropriate PingOne Advanced Services Self-Service roles on the **Users** page in the directory. To assign these roles, you must be assigned the PingOne Identity Data Admin role.

Steps

1. Go to **Directory** > **Users** and browse or search for the users that you want to assign the role to.
2. Click the user entry to open the user details panel, and then click the **Pencil** icon in the profile.
3. On the bottom of the page, in the **Custom Attributes** list, select **P1AS Self-Service Roles**.
4. Click **Save**.

PingAccess self-service

PingAccess is an identity-enabled access management product that protects web applications and APIs by applying security policies to client requests. You can connect to PingAccess directly from the platform and complete a variety of tasks, described here.

To access the administrative console through the Customer Portal, click the **Expand** icon associated with the environment and select the appropriate PingAccess link. You can also set up OAuth to connect to the PingAccess Admin API. Learn more in Setting up OAuth to access the PingAccess Admin API.

In PingAccess, you can:

Manage applications

Applications represent the protected web applications and APIs to which client requests are sent. Applications are composed of one or more resources, have a common virtual host and context root, and correspond to a single target site. Applications can be protected by the PingAccess Gateway or PingAccess Agent. In a gateway deployment, the target application is specified as a site. In an agent deployment, the application destination is an Agent.

Manage authentication

Authentication requirements are policies that dictate how users must authenticate before access is granted to protected web applications. Authentication methods are string values and ordered in a list by preference. At runtime, the type of authentication attempted is determined by the order of the authentication methods.

Manage identity mappings

Identity mappings make user attributes available to backend sites that use them for authentication. There are multiple types of identity mappings, each with different behavior and a distinct set of fields to specify the identity mapping behavior.

Manage rules

Rules are the building blocks for access control and request processing. There are many types of rules, each with different behavior and a distinct set of fields to specify the rule behavior. Rule sets allow you to group multiple rules into re-usable sets, which can be applied to applications and resources. Rule set groups can contain rule sets or other rule set groups, allowing you to create hierarchies of rules to any level of depth. Rule sets and rule set groups can be applied to applications and resources, as required.

Manage web sessions

Web sessions define the policy for web application session creation, lifetime, timeouts, and scope. Multiple web sessions can be configured to scope the session to meet the needs of a target set of applications. This strategy improves the security model of the session, as it prevents unrelated applications from impersonating an end user.

Setting up OAuth to access the PingAccess Admin API

You can configure the PingAccess Admin API so that administrators can access it using OAuth. The API requires a JWT Bearer token for authenticating the requests. This token can be retrieved using either an authorization code flow or a client credentials flow.

- Authenticate using an authorization code flow
- Authenticate using a client credentials flow

Authenticate using an authorization code flow

The API supports the authorization code flow, which gets access tokens by securely redirecting users to the authorization server for authentication.

Before you begin

After user accounts are created, you can assign the appropriate user access control roles and permissions. Users can then get an access token to use with API calls. Learn more about these roles and permissions in PingAccess roles.

Steps

1. Go to the PingOne Advanced Services login URL:

```
https://self-service-api.<environment>-<customer>.<region>.ping.cloud/api/v1/login/pingaccess
```

2. Enter your credentials and click **Submit**.

   If authentication is successful, you're redirected to the **Success** page and a **Copy Token** button displays.

3. Click **Copy Token**.

4. Query the API directly using tools such as Postman or cURL, and include the bearer token in the headers.

   Example

   ```
   {"Authorization": "Bearer {TOKEN}"}
   ```

Authenticate using a client credentials flow

The API supports the client credentials flow, designed for machine-to-machine (M2M) interactions, which allows applications to access system resources without involving a user.

> **Note**
>
> This type of flow can only be used if connections are correctly configured for self-managing administrator accounts. Learn more in Configuring connections for SSO.

To set this up, you'll need to:

- Create a client credentials application in your PingOne environment
- Generate the token

You should also restrict access to this application to PingOne administrators. Learn more in Restricting access to the application.

> **Note**
>
> In addition to the JWT Bearer token, the API uses role-based access control, as described in Administrative role mappings. The roles assigned to the accounts affect the results of the API calls.

Creating the client credentials application

Start by creating an OpenID Connect (OIDC) application in PingOne.

Steps

1. Go to **Applications > Resources**.
2. Click the **+** icon.
3. Create the resource by completing these fields:
   - **Resource name**: A unique identifier for the resource.
   - **Description** (optional): A brief characterization of the resource that helps identify it.

4. Click **Next**.
5. On the **Attributes** page, click **Add**.
6. Name the new attribute `groups`.

   Set the value to a hardcoded list of valid **PingAccess** roles. For example, `{"dev-pa-admin", "prod-pa-audit"}`. You can find a complete list of the PingAccess roles and permissions in PingAccess administrative role mappings.

   > **Note**
   >
   > The **PingAccess** attribute must be set up for it to display in the list. You can find instructions on adding this attribute in Creating custom user attributes.

7. Click **Next**.
8. On the **Scopes** page, add a new scope to map the **PingAccess** role to the new application. Click **Add Scope** and complete the following fields:
   - **Scope name**: A unique identifier for the scope.
   - **Description** (optional): A brief characterization of the scope that helps identify it.
9. Click **Save**.
10. Now, add the OIDC application. Go to **Applications** > **Applications**.
11. Click the **+** icon.
12. Complete the following fields:
    - **Application name**: A unique identifier for the application.
    - **Description** (optional): A brief characterization of the application that helps identify it.
    - **Icon** (optional): A graphic representation of the application. Use a file up to 1 MB in JPG, JPEG, GIF, or PNG format.
13. In the list of available application types, select **OIDC Web App**. Click **Save**.
14. On the **Configuration** tab, click the **Pencil** icon to edit the configuration.
    - Change the **Response Type** to none by clearing all the options.
    - Change the **Grant Type** to **Client Credentials**.
15. Click **Save**.
16. On the **Resources** tab, click the **Pencil** icon to add the scope you added in step 8 to the application.
17. Click **Save** and click the toggle for the application.

Generate the token

Access the new application in the PingOne console to generate an access token.

Steps

1. Follow the steps outlined in Getting an access token in the PingOne documentation.
2. Include the bearer token in the headers.

   Example

   ```
   {"Authorization": "Bearer {TOKEN}"}
   ```

Restricting access to the application

To ensure that only administrators can generate access tokens, restrict access to it.

Steps

1. Select the application, click the **Access** tab, and then the **Pencil** icon.
2. Select the **Admin Only Access** checkbox and click **Save**.

PingDirectory self-service

PingDirectory is a scalable directory used to store identity and rich profile data. Enterprises use it to securely store and manage sensitive customer, partner and employee data, including credentials, profiles, preferences and privacy choices. You can connect to PingDirectory directly from the platform.

To connect to PingDirectory through the portal, click the expandable icon associated with the appropriate environment, click the **Products** tab, and click the **LDAPS** link.

In PingDirectory, you can change user and group objects through your preferred LDAP browser. Learn more in Managing entries in the PingDirectory documentation.

PingFederate self-service

PingFederate is an enterprise federation server that enables user authentication and single sign-on (SSO). It serves as a global authentication authority that allows employees, customers and partners to securely access all the applications they need from any device. You can connect to PingFederate directly from the platform and complete a variety of tasks, described here.

To connect to PingFederate through the portal, click the expandable icon associated with the environment and select the appropriate PingFederate link.

In PingFederate, you can:

Manage applications

Create and modify SAML connections, OAuth and OpenID Connect (OIDC) clients, and other integrations with resources you are protecting through PingFederate as authentication service.

Manage authentication policies

Combine adapters, selectors, and policy contracts in a logical tree to define the end user authentication experience when accessing a protected resource.

Manage data sources

Source and map user attribute data from anywhere using LDAP, REST, Java Database Connectivity (JDBC), and other data types.

PingFederate: Manage applications

You can configure a wide variety of applications in PingFederate and set up single sign-on (SSO) to other Ping products and applications.

See the following:

- Configuring a SAML application in PingFederate
- Setting up an OIDC application in PingFederate
- Configuring federation with SharePoint server
- Configuring Workday SSO with PingOne or PingFederate
- Integrating CyberArk with Ping products for SSO and authentication
- Using Palo Alto Networks Next-Generation Firewall with Ping products

PingFederate: Manage authentication policies

Authentication policies are processes used to verify that those attempting to access services and applications are who they claim to be. Administrators can configure these policies in an infinite number of ways, using a wide variety of authentication sources, to meet your needs.

Learn more in the following:

- Authentication policies
- Defining authentication_policies
- Adapter mappings
- Register Azure AD devices automatically through PingFederate for Windows 10 devices
- Integrating MFA with SSO (PingID with PingFederate)
- Configuring medium-grained application access control through Azure AD, PingFederate, and PingAccess Connecting PingFederate to PingAccess
- Connecting PingFederate to PingAccess
- Protecting PingAccess resources through external IdPs with PingFederate acting as an SP (leveraging FedHub)

PingFederate: Manage data sources

Most customers using PingFederate as an identity provider has at least one connection to an external data source. Active Directory is the most common data source used to connect to PingFederate, but other options are available.

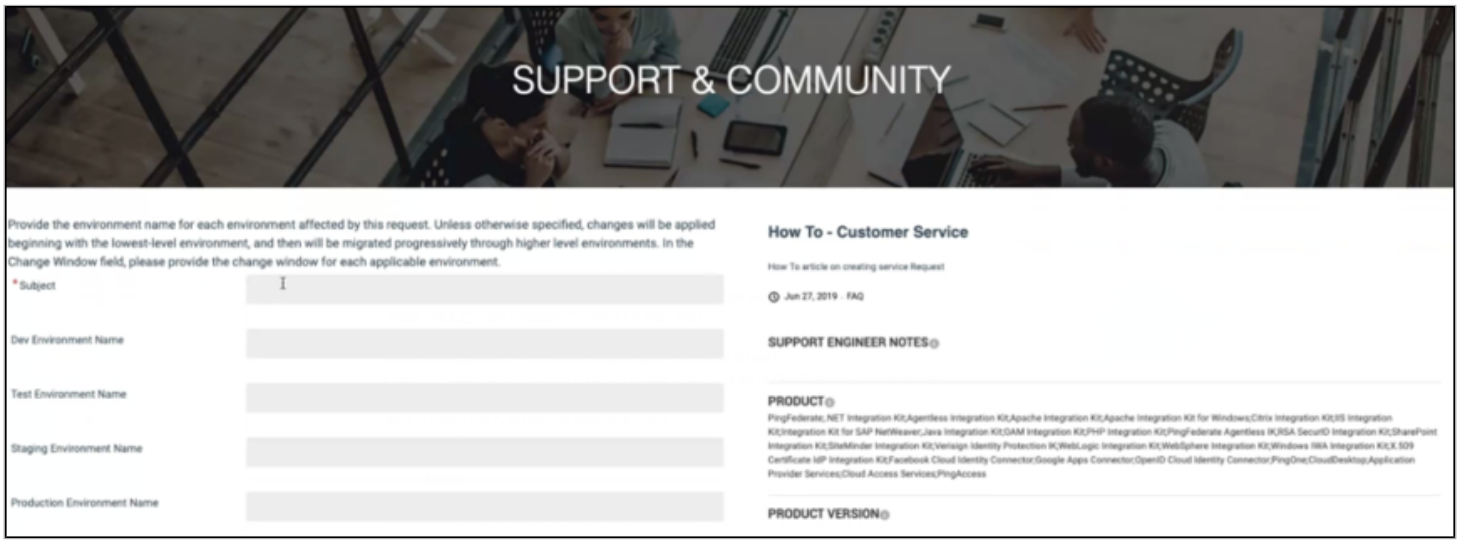
See the following:

- Datastores
- Configuring the Active Directory environment
- Configuring offline MFA with PingID

Service requests

For the tasks that you can't complete yourself, submit a service request through the Support Portal.

To access this page, go to the Ping Identity home page and select **Support → Get Support**. Click **Sign On** and enter your credentials to access your account.



To ensure your request is processed as quickly as possible, follow the instructions provided for each type of request. Common service requests are categorized and listed below.

> **Note**
>
> Our average turnaround time for most service requests is 2 business days.

PingAccess service requests	PingDirectory service requests	PingFederate service requests	Platform service requests
• Enable debug logger • Integration kits • Update templates • Virtual hosts	• ACIs • Email templates • Indexes • JSON field constraints • Password policies • Plugins • Schema - attribute type • Schema - objectClass • Virtual attribute	• Elevate admin • Enable debug logger • Password rules • Integration kits • Update templates	• Administrator MFA • Approve merge request • Restore from a backup • Creating and updating virtual hosts • Enable outbound provisioning • Load or performance test • PingDirectory truststore certificate import • SIEM integrations • Rollback SIEM • Subscribe to SNS alerts • Update TLS certificate • Upgrades

If the type of request you want to submit is not listed, select **Advanced/Other** as your requested capability, provide a detailed description of your needs, and submit your request to the Support team.

PingAccess service requests

For PingAccess tasks you can't complete yourself, submit a service request.

To ensure your service requests are processed as quickly as possible, follow the instructions provided for each type of request:

- Enable debug logger
- Integration kits
- Update templates
- Virtual hosts

> **Note**
>
> Our average turnaround time for most service requests is 2 business days.

If the type of request you want to submit is not listed, select **Advanced/Other** as your requested capability, provide a detailed description of your needs, and submit your request to the Support team.

Enable debug logger

PingAccess generates logs that record server events. To enable the standard debug logger or request a non-standard debug level, submit a service request through the Support Portal.

Steps

1. Complete the following fields:
    - **Subject**: Enter a description of your request, including the action to be taken.
    - **Environment Type**: Specify the type of environment affected by this request.
    - **Proposed Change Window**: Specify the dates or times in which you want the work complete.
2. In the **Capability** list, select **PingAccess service requests → Enable Debug Logger**.
3. Select the **Standard Debug?** field to configure the log level to `DEBUG`. See Configuring log levels for details.
4. If you're requesting a non-standard debug level, specify the targets that you want configured from the `log4j2.xml` file in the **Debug Targets** fields.

   Then, specify the appropriate debug level for each target listed in the **Debug Level** fields.
5. In the **Business Priority** list, select the appropriate description:
    - Change needed by deadline to avoid business impact
    - Change modifies existing functionality
    - Change adds new functionality
6. In the **Description** field, enter a description of your request.
7. If you are tracking your request within your organization, enter the tracking ID or ticket number associated with it in the **Customer Tracking ID** field.
8. To submit your request, click **Save**.

Integration kits

To install a new integration kit or upgrade an existing kit, submit a request through the service request form on the Support Portal.

Steps

1. Complete the following fields:
    - **Subject**: Enter a description of your request, including the action to be taken.
    - **Environment Type**: Specify the type of environment affected by this request.
    - **Proposed Change Window**: Specify the dates or times in which you want the work complete.
2. In the **Capability** list, select **PingAccess service requests → Integration Kits**.

3. In the **Integration Kit Type** field, select **Non-Standard** if the kit is provided by the Professional Services team. Otherwise, select **Standard**.
4. In the **Integration Kit Name** field, provide the name of the kit you're requesting.
5. In the **Version** field, provide the version of the kit you're requesting.
6. In the **Business Priority** list, select the appropriate description:
    - Change needed by deadline to avoid business impact
    - Change modifies existing functionality
    - Change adds new functionality
7. In the **Description** field, indicate whether the request is for a new integration kit or an upgrade to an existing kit.
8. If you are tracking your request within your organization, enter the tracking ID or ticket number associated with it in the **Customer Tracking ID** field.
9. To submit your request, click **Save**.

Update templates

PingAccess supplies templates to provide information to end users. To update these templates, submit a service request through the Support Portal.

Steps

1. Complete the following fields:
    - **Subject**: Enter a description of your request, including the action to be taken.
    - **Environment Type**: Specify the type of environment affected by this request.
    - **Proposed Change Window**: Specify the dates or times in which you want the work complete.
2. In the **Capability** list, select **PingAccess service requests → Update Templates**.
3. In the **Template Type** field, select the type of template that you want to update. If you want to update both user-facing screen templates and localized messages, select **Other**.
4. In the **Business Priority** list, select the appropriate description:
    - Change needed by deadline to avoid business impact
    - Change modifies existing functionality
    - Change adds new functionality
5. In the **Description** field, enter a description of your request.
6. If you are tracking your request within your organization, enter the tracking ID or ticket number associated with it in the **Customer Tracking ID** field.
7. To submit your request, click **Save**.

Virtual hosts

Although you can set the hostname in PingAccess, this request sets the hostname in the platform. Submit a request through the Support Portal.

Steps

1. Complete the following fields:
    - **Subject**: Enter a description of your request, including the action to be taken.
    - **Environment Type**: Specify the type of environment affected by this request.
    - **Proposed Change Window**: Specify the dates or times in which you want the work complete.
2. In the **Capability** list, select **PingAccess service requests → Virtual hosts**.
3. In the **AWS Region** field, select the primary region of your P1AS environment (US1, EU1, AU1, etc.)
4. In the **Environment** field, select the environment this applies to (Dev, Test, Stage, or Prod).
5. In the **Target Application** field, select the product this hostname will point to.
6. In the **Virtual Host Name** field, provide the desired hostname for the target application.
7. In the **Business Priority** list, select the appropriate description:
    - Change needed by deadline to avoid business impact
    - Change modifies existing functionality
    - Change adds new functionality
8. In the **Description** field, enter a description of your request.
9. If you are tracking your request within your organization, enter the tracking ID or ticket number associated with it in the **Customer Tracking ID** field.
10. To submit your request, click **Save**.

PingDirectory service requests

For PingDirectory tasks you can't complete yourself, submit a service request.

To ensure your service requests are processed as quickly as possible, follow the instructions provided for each type of request:

- ACIs
- Email templates
- Indexes
- JSON field constraints
- Password policies

- Plugins
- Schema - attribute type
- Schema - objectClass
- Virtual attribute

> **Note**
>
> Our average turnaround time for most service requests is 2 business days.

If the type of request you want to submit is not listed, select **Advanced/Other** as your requested capability, provide a detailed description of your needs, and submit your request to the Support team.

ACIs

To add, modify, or remove access control instructions (ACIs), submit a request through the service request form, accessible from the Support Portal.

About this task

Global ACIs are a set of ACIs that can apply to entries anywhere in the server, but they can also be scoped so that they only apply to a specific set of entries. These ACIs work in conjunction with access control rules stored in user data and provide a convenient way to define ACIs that span disparate portions of the DIT (Directory Information Tree).

You can apply Global ACIs to administrator access, anonymous and authenticated access, delegated access to a manager or for proxy authorization. The following table includes access control components, descriptions, and the syntax used for each component.

Access Control Components	Description	Syntax
targets	This component specifies the set of entries or attributes that the access control rule applies to.	Syntax: `(target keyword = || != expression)`
name	This component specifies the name of the ACI.	
permissions	This component specifies the type of operations to which an access control rule might apply.	Syntax: `allow||deny (permission)`
bind rules	This component specifies the criteria that indicate whether an access control rule should apply to a given requester.	Syntax: `bind rule keyword = ||!= expression;` The bind rule syntax requires that it be terminated with a ";".

For additional information, see Defining global ACIs in the*PingDirectory Server Administration Guide*.

Steps

1. Complete the following fields:
    - **Subject**: Enter a description of your request, including the action to be taken.
    - **Environment Type**: Specify the type of environment affected by this request.
    - **Proposed Change Window**: Specify the dates or times in which you want the work complete.
2. In the **Capability** list, select **PingDirectory service request → ACIs**.
3. If you want to use an ACI that you constructed, select the **Do you have ACI already?** option.
4. In the **Base DN that ACI applies to** field, select the parent Base DN that the ACI should apply to. Note that this ACI will apply to all subtrees below this Base DN.
5. In the **Attributes(s) to apply to (comma separated)** field, provide a comma-separated list of attributes that should be allowed or denied by this ACI.
6. In the **DN of user or group** field, provide the User DN or Group DN that the ACI will apply to, which will determine who is allowed or denied access.
7. In the **Is the target a user or group?** field, indicate whether the target is a user or a group based on the DN provided in the previous step.
8. In the **Does this ACI allow or deny access?** field, indicate whether the ACI should allow access to users with the selected attribute or deny access.
9. In the **Permissions** field, select the permissions you want to grant or deny to the target users or groups.
10. If you have a complete ACI, paste it into the **Advanced (supply a raw ACI)**field.
11. In the **Business Priority** list, select the appropriate description:
    - Change needed by deadline to avoid business impact
    - Change modifies existing functionality
    - Change adds new functionality
12. In the **Description** field, provide a description of the request.
13. If you are tracking your request within your organization, enter the tracking ID or ticket number associated with it in the **Customer Tracking ID** field.
14. To submit your request, click **Save**.

Email templates

To modify email templates, submit a service request through the Support Portal.

About this task

You can use PingDirectory email templates in a variety of ways. An example email template is provided in the **Delegated Admin** package at the top level in the `delegated-admin-account-created.template` file. This template provides a multipart text and HTML email to the user with their username and initial password, along with a self-service link they can use to sign on to PingFederate and change their password and profile information.

For additional information, see Edit and copy the email template to PingDirectory Server in the *PingDirectory Server Administration Guide*.

Steps

1. Complete the following fields:
    - **Subject**: Enter a description of your request, including the action to be taken.
    - **Environment Type**: Specify the type of environment affected by this request.
    - **Proposed Change Window**: Specify the dates or times in which you want the work complete.
2. In the **Capability** list, select **PingDirectory service requests → Email templates**.
3. In the **Specify email handler type** field, specify whether a standard email notification handler or a multipart email status notification handler will be used.
4. In the **Business Priority** list, select the appropriate description:
    - Change needed by deadline to avoid business impact
    - Change modifies existing functionality
    - Change adds new functionality
5. In the **Description** field, enter a description of your request.
6. If you are tracking your request within your organization, enter the tracking ID or ticket number associated with it in the **Customer Tracking ID** field.
7. Click **Save**.
8. Click the **Attachments** tab and upload a `.zip` file that contains all files in the template directory you are updating.

> **Note**
>
> If necessary, request the latest instance of these files before making your update.

Indexes

Submit your index change requests through the service request form on the Support Portal.

About this task

Indexes improve database search performance and provide consistent search rates, regardless of the number of database objects stored in the directory information tree (DIT) and are associated with attributes within your schema. To add an index, attributes must already exist in the schema defined for your directory. To delete an index, ensure that data is removed from user entries prior to it being deleted or data modification issues and application errors will exist.

For additional information, see Working with indexes in the *PingDirectory Server Administration Guide*.

Steps

1. Complete the following fields:
    - **Subject**: Enter a description of your request, including the action to be taken.
    - **Environment Type**: Specify the type of environment affected by this request.
    - **Proposed Change Window**: Specify the dates or times in which you want the work complete.
2. In the **Capability** list, select **PingDirectory service requests → Indexes**.
3. In the **Attribute to index** field, provide the attribute that will be indexed.
4. In the **Index type(s)** field, select the index types that you want to create. See Index types for a list of PingDirectory server index types.

   If you're unsure of which index types you should select, provide your own filter to specify how the index should be applied. For example, "(cn=smith)" would apply the index to users whose common name is Smith.
5. If you selected a subtree index and expect that strings might have more than 4,000 matches, you can specify a higher limit in the **Substring index entry limit** field.
6. If you expect a search to match more than 4,000 values, you can specify a higher limit in the **Index entry limit** field. Searches that exceed this value will be unindexed and are only allowed upon request.
7. In the **Business Priority** list, select the appropriate description:
    - Change needed by deadline to avoid business impact
    - Change modifies existing functionality
    - Change adds new functionality
8. In the **Description** field, enter a description of your request.
9. If you are tracking your request within your organization, enter the tracking ID or ticket number associated with it in the **Customer Tracking ID** field.
10. To submit your request, click **Save**.

JSON field constraints

Submit your requests to define JSON field constraints through the service request form on the Support Portal.

About this task

You can define a number of constraints for the fields included in JSON objects stored in values of a specified attribute type. For example, you can require that a field value is a specific data type, specify whether a field is required or optional, or restrict values of string fields to a predefined set of values.

For additional information, see About managing JSON attribute values in the *PingDirectory Server Administration Guide*.

Steps

1. Complete the following fields:
    - **Subject**: Enter a description of your request, including the action to be taken.
    - **Environment Type**: Specify the type of environment affected by this request.
    - **Proposed Change Window**: Specify the dates or times in which you want the work complete.
2. In the **Capability** list, select **PingDirectory service requests → JSON field constraints**.
3. In the **JSON attribute** field, specify the JSON attribute for which a field will be created.
4. Select the **Allow unnamed fields** option if you want to allow attributes that are not explicitly defined in the constraints.
5. In the **JSON field name** field, specify a field name to add to the JSON attribute
6. In the **Value type** field, specify the value type of the JSON.
7. Select the **Is required** option if this field should be required.
8. In the **Is array** field, specify whether the field should hold an array (required), can hold an array (optional) or cannot hold an array (prohibited).
9. Select the **Allow null value** option if you want to allow nun values in the field.
10. Select the **Allow empty object** option to allow empty objects in the field.
11. Select the **Index values** option to create an index for this field.
12. In the **Business Priority** list, select the appropriate description:
    - Change needed by deadline to avoid business impact
    - Change modifies existing functionality
    - Change adds new functionality
13. In the **Description** field, enter a description of your request.
14. If you are tracking your request within your organization, enter the tracking ID or ticket number associated with it in the **Customer Tracking ID** field.
15. To submit your request, click **Save**.

Password policies

Password policies contain configurable properties for password expiration, failed sign on attempts, account lockout and other aspects of password and account maintenance. Submit your password policy requests through the service request form on the Support Portal.

About this task

For more information, see About the password policy properties in the *PingDirectory Server Administration Guide*.

Steps

1. Complete the following fields:
    - **Subject**: Enter a description of your request, including the action to be taken.
    - **Environment Type**: Specify the type of environment affected by this request.
    - **Proposed Change Window**: Specify the dates or times in which you want the work complete.
2. In the **Capability** list, select **PingDirectory service requests → Password policies**.
3. In the **Password policy name** field, provide the name of the password policy you want to add, modify or delete.
4. If you want to add a new policy, select the **New Policy** option. If you want to modify or delete an existing policy, leave this field blank.
5. In the **Default password storage scheme** field, provide the scheme. The default is `Salted SHA-256`, but you can specify another supported scheme. See Supported password storage schemes for a complete list.
6. In the **Password validators** field, provide the names of the password validators you want to use with this policy. See Password validators for a complete list.
7. In the **Password history count** field, specify the number of passwords that users must have before a password can be reused.
8. In the **Password history duration** field, specify the amount of time that must pass before a password can be reused.
9. In the **Min age** field, specify the minimum amount of time that a user must wait to change their password after a prior password change.
10. In the **Max age** field, specify the amount of time that can pass before the password must be changed.
11. In the **Expiration warning interval (0 if expire without warning)** field, specify the amount of time prior to a password expiring that the server will warn users about the expiry, or select 0 if you want passwords to expire without warning.
12. In the **Lockout failure count** field, specify the number of incorrect passwords that users can enter before they are locked out.
13. In the **Lockout duration** field, specify the amount of time an account will remain locked out.
14. Select the **Force change on add** option if you want to force users to change their passwords following an administrator reset.
15. In the **Business Priority** list, select the appropriate description:
    - Change needed by deadline to avoid business impact
    - Change modifies existing functionality
    - Change adds new functionality
16. In the **Description** field, enter a description of your request.
17. If you are tracking your request within your organization, enter the tracking ID or ticket number associated with it in the **Customer Tracking ID** field.
18. To submit your request, click **Save**.

Plugins

Only out-of-the-box plugins that are part of the PingDirectory default deployment are currently supported. To have one or more of these plugins enabled, or to submit other types of plugin requests, submit your request through the service request form on the Support Portal.

Steps

1. Complete the following fields:
    - **Subject**: Enter a description of your request, including the action to be taken.
    - **Environment Type**: Specify the type of environment affected by this request.
    - **Proposed Change Window**: Specify the dates or times in which you want the work complete.
2. In the **Capability** list, select **PingDirectory service requests → Plugins**.
3. In the **Choose common plugin** field, choose the plugin that you want to have created. Each plugin has different requirements.
4. In the **Attribute mapper - source attribute** field, specify the attribute you want to transform.
5. In the **Attribute mapper - target attribute** field, specify what the source attribute will transform into.
6. In the **Composed attribute - attribute** field, specify the attribute to be created on an entry.
7. In the **Composed attribute - value pattern** field, specify the value pattern for this field. See Composed attribute plugin configuration properties for additional information.
8. In the **DN mapper - source DN** field, specify the DN that you want to transform.
9. In the **DN mapper - target DN** field, specify the transformed value of the specified DN.
10. In the **Unique attribute - attribute** field, specify the attribute that should be unique in the environment.
11. In the **Business Priority** list, select the appropriate description:
    - Change needed by deadline to avoid business impact
    - Change modifies existing functionality
    - Change adds new functionality
12. In the **Description** field, enter a description of your request.
13. If you are tracking your request within your organization, enter the tracking ID or ticket number associated with it in the **Customer Tracking ID** field.
14. To submit your request, click **Save**.

Schema - attribute type

To add, modify, or delete attribute types within the schema, submit a service request through the Support Portal.

Steps

1. Complete the following fields:
    - **Subject**: Enter a description of your request, including the action to be taken.
    - **Environment Type**: Specify the type of environment affected by this request.
    - **Proposed Change Window**: Specify the dates or times in which you want the work complete.
2. In the **Capability** list, select **PingDirectory service requests → Schema - attribute type**.
3. In the **Attribute Name** field, enter the name of the attribute that you want to add, modify, or delete.
4. In the **Syntax** field, specify the name or OID of the syntax that you want to use. See Attribute Indexes for additional information.
5. Select the **Multi-valued** option if the attribute should allow multiple values on a single entry.
6. Select the **Unique** option if the attribute values should be unique across all server entries.
7. In the **Business Priority** list, select the appropriate description:
    - Change needed by deadline to avoid business impact
    - Change modifies existing functionality
    - Change adds new functionality
8. In the **Description** field, enter a description of your request.
9. If you are tracking your request within your organization, enter the tracking ID or ticket number associated with it in the **Customer Tracking ID** field.
10. To submit your request, click **Save**.

Schema - objectClass

To add, modify, or delete objectClass attributes, submit a service request through the Support Portal.

Steps

1. Complete the following fields:
    - **Subject**: Enter a description of your request, including the action to be taken.
    - **Environment Type**: Specify the type of environment affected by this request.
    - **Proposed Change Window**: Specify the dates or times in which you want the work complete.
2. In the **Capability** list, select **PingDirectory service requests → Schema - objectClass**.
3. In the **Parent objectClass** field, specify the name of the class in which the objectClass attribute resides.
4. In the **Type** field, select the objectClass type. See Object Classes for additional information.
5. In the **Required attributes** field, provide a comma-separated list of attributes that the attribute will require.

6. In the **Optional attributes** field, provide a comma-separated list of the attributes that are allowed, but not required, by the objectClass.
7. In the **Business Priority** list, select the appropriate description:
    - Change needed by deadline to avoid business impact
    - Change modifies existing functionality
    - Change adds new functionality
8. In the **Description** field, enter a description of your request.
9. If you are tracking your request within your organization, enter the tracking ID or ticket number associated with it in the **Customer Tracking ID** field.
10. To submit your request, click **Save**.

Virtual attribute

To add, modify, or delete virtual attributes, submit a service request through the Support Portal.

Steps

1. Complete the following fields:
    - **Subject**: Enter a description of your request, including the action to be taken.
    - **Environment Type**: Specify the type of environment affected by this request.
    - **Proposed Change Window**: Specify the dates or times in which you want the work complete.
2. In the **Capability** list, select **PingDirectory service requests → Virtual Attribute**.
3. In the **Attribute name** field, enter the name of the virtual attribute that you want to add, modify, or delete. This attribute must exist in the schema.
4. In the **Value Pattern** field, specify the logic that will be used when constructing values. See Composed attribute plugin configuration properties for additional information.
5. In the **Base DN** field, specify Base DNs that the virtual attribute should apply to.
6. In the **Group DN** field, specify groups that the virtual attribute should apply to.
7. To apply this virtual attribute to a specific group of users, create a filter to identify these groups.
8. To apply this
9. In the **Business Priority** list, select the appropriate description:
    - Change needed by deadline to avoid business impact
    - Change modifies existing functionality
    - Change adds new functionality
10. In the **Description** field, enter a description of your request.

11. If you are tracking your request within your organization, enter the tracking ID or ticket number associated with it in the **Customer Tracking ID** field.
12. To submit your request, click **Save**.

PingFederate service requests

For PingFederate tasks you can't complete yourself, submit a service request.

To ensure your service requests are processed as quickly as possible, follow the instructions provided for each type of request:

- Elevate admin
- Enable debug logger
- Password rules
- Integration kits
- Update templates

> **Note**
>
> Our average turnaround time for most service requests is 2 business days.

If the type of request you want to submit isn't listed, select **Advanced/Other** as your requested capability, provide a detailed description of your needs, and submit your request to the Support team.

Elevate admin

To modify the permissions your administrators have, such as managing certificates or users, submit a service request through the Support Portal.

Steps

1. Complete the following fields:
    - **Subject**: Enter a description of your request, including the action to be taken.
    - **Environment Type**: Specify the type of environment affected by this request.
    - **Proposed Change Window**: Specify the dates or times in which you want the work complete.
2. In the **Capability** list, select **PingFederate service requests → Elevate admins**.
3. In the **Admin Permissions to Add** field, select all the permissions that you want your administrators to have.

    > **Note**
    >
    > If you want administrators to be granted different permissions, submit separate requests for each.

4. In the **Admins to change** field, provide the names of the administrators who you want to be granted the requested permissions.

5. In the **Description** field, enter a description of your request.
6. If you are tracking your request within your organization, enter the tracking ID or ticket number associated with it in the **Customer Tracking ID** field.
7. To submit your request, click **Save**.

Enable debug logger

PingFederate generates logs that record server events. To enable the standard debug logger or request a non-standard debug level, submit a service request through the Support Portal.

About this task

Log files are written to the PingFederate log directory, located in the following directory by default: `<pf_install>/pingfederate/log`.

Steps

1. Complete the following fields:
   - **Subject**: Enter a description of your request, including the action to be taken.
   - **Environment Type**: Specify the type of environment affected by this request.
   - **Proposed Change Window**: Specify the dates or times in which you want the work complete.
2. In the **Capability** list, select **PingFederate service requests → Enable debug logger**.
3. Select the **Standard Debug?** field to configure the log level to `DEBUG`.
4. If you're requesting a non-standard debug level, specify the targets that you want configured from the `log4j2.xml` file in the **Debug Targets** fields. See Log4j 2 logging service and configuration for additional information.

   Then, specify the appropriate debug level for each target listed in the **Debug Level** fields.
5. In the **Business Priority** list, select the appropriate description:
   - Change needed by deadline to avoid business impact
   - Change modifies existing functionality
   - Change adds new functionality
6. In the **Description** field, enter a description of your request.
7. If you are tracking your request within your organization, enter the tracking ID or ticket number associated with it in the **Customer Tracking ID** field.
8. To submit your request, click **Save**.

Password rules

PingFederate applies a configurable policy to passwords, pass phrases, and shared secrets defined by administrators in the administrative console. To update password rules, submit a request through the service request form on the Support Portal.

Steps

1. Complete the following fields:
    - **Subject**: Enter a description of your request, including the action to be taken.
    - **Environment Type**: Specify the type of environment affected by this request.
    - **Proposed Change Window**: Specify the dates or times in which you want the work complete.
2. In the **Capability** list, select **PingFederate service requests → Password rules**.
3. In the **Password rule to update** field, specify which rule you want to update.

   Default policy settings include:
    - **requireMixedCase**: Default is true
    - **minLength**: Default is 8
    - **minNumeric**: Default is 1
    - **minAlpha**: Default is 2
    - **minSpecial**: Default is 0
    - **specialChars**: Default is !$%^&*()_+\|~-=\`\{}[]:";'<>?,/.
4. In the **Business Priority** list, select the appropriate description:
    - Change needed by deadline to avoid business impact
    - Change modifies existing functionality
    - Change adds new functionality
5. In the **Description** field, enter a description of your request.
6. If you are tracking your request within your organization, enter the tracking ID or ticket number associated with it in the **Customer Tracking ID** field.
7. To submit your request, click **Save**.

Integration kits

To install a new integration kit, or upgrade an existing integration kit, submit a service request through the Support Portal.

Steps

1. Complete the following fields:
    - **Subject**: Enter a description of your request, including the action to be taken.
    - **Environment Type**: Specify the type of environment affected by this request.
    - **Proposed Change Window**: Specify the dates or times in which you want the work complete.
2. In the **Capability** list, select **PingFederate service requests → Integration Kits**.
3. In the **Integration Kit Type** field, select **Non-Standard** if the kit is provided by the Professional Services team. Otherwise, select **Standard**.
4. In the **Integration Kit Name** field, provide the name of the kit you're requesting.
5. In the **Version** field, provide the version of the kit you're requesting.
6. In the **Business Priority** list, select the appropriate description:
    - Change needed by deadline to avoid business impact
    - Change modifies existing functionality
    - Change adds new functionality
7. In the **Description** field, indicate whether the request is for a new integration kit or an upgrade to an existing kit.
8. If you are tracking your request within your organization, enter the tracking ID or ticket number associated with it in the **Customer Tracking ID** field.
9. To submit your request, click **Save**.

Update templates

PingFederate supplies templates to provide information to end users. To update these templates, submit a service request through the Support Portal.

Steps

1. Complete the following fields:
    - **Subject**: Enter a description of your request, including the action to be taken.
    - **Environment Type**: Specify the type of environment affected by this request.
    - **Proposed Change Window**: Specify the dates or times in which you want the work complete.
2. In the **Capability** list, select **PingFederate service requests → Update Templates**.
3. In the **Template Type** field, select the type of template that you want to update. If you are uploading a variety of different template types, select **Other**.
4. In the **Merge request URL** field, provide the URL of the merge request.

5. In the **Business Priority** list, select the appropriate description:
    - Change needed by deadline to avoid business impact
    - Change modifies existing functionality
    - Change adds new functionality
6. In the **Description** field, enter a description of your request.
7. If you are tracking your request within your organization, enter the tracking ID or ticket number associated with it in the **Customer Tracking ID** field.
8. To submit your request, click **Save**.

Platform service requests

For platform tasks you can't complete yourself, submit a service request.

To ensure your service requests are processed as quickly as possible, follow the instructions provided for each type of request:

- Administrator MFA
- Approve merge request
- Restore from a backup
- Enable outbound provisioning
- Load or performance test
- PingDirectory truststore certificate import
- SIEM integration
- Rollback SIEM
- Subscribe to SNS alerts
- Update TLS certificate
- Upgrades

> **Note**
>
> Our average turnaround time for most service requests is 2 business days.

If the type of request you want to submit is not listed, select **Advanced/Other** as your requested capability, provide a detailed description of your needs, and submit your request to the Support team.

Administrator MFA

Submit your requests to manage customer IAM Administrator multi-factor authentication (MFA) through the service request form on the Support & Community page.

Steps

1. Complete the following fields:
    - **Subject**: Enter a description of your request, including the action to be taken.
    - **Environment Type**: Specify the type of environment affected by this request.
    - **Proposed Change Window**: Specify the dates or times in which you want the work complete.
2. In the **Capability** list, select **Platform service requests → Administrator MFA**.
3. In the**Administrator(s)** field, enter the administrator name.
4. In the **Desired MFA setting** field, indicate whether you want to enable or disable MFA.
5. In the **MFA contact method** field, indicate whether the MFA contact method will be email or phone number.
6. In the **MFA contact info** field, provide the MFA information (email address or phone number).
7. In the **Business Priority** list, select the appropriate description:
    - Change needed by deadline to avoid business impact
    - Change modifies existing functionality
    - Change adds new functionality
8. In the **Description** field, enter a description of your request.
9. If you are tracking your request within your organization, enter the tracking ID or ticket number associated with it in the **Customer Tracking ID** field.
10. To submit your request, click **Save**.

Approve merge request

To approve a merge request, submit a service request through the Support Portal.

Steps

1. Complete the following fields:
    - **Subject**: Enter a description of your request, including the action to be taken.
    - **Environment Type**: Specify the type of environment affected by this request.
    - **Proposed Change Window**: Specify the dates or times in which you want the work complete.
2. In the **Capability** list, select **Platform service requests → Approve Merge Request**.
3. In the **Merge request URL** field, provide the URL for the request.
4. In the **Business Priority** list, select the appropriate description:
    - Change needed by deadline to avoid business impact

- Change modifies existing functionality
- Change adds new functionality

5. In the **Description** field, enter a description of your request.
6. If you are tracking your request within your organization, enter the tracking ID or ticket number associated with it in the **Customer Tracking ID** field.
7. To submit your request, click **Save**.

Restore from a backup

To request that a product be restored from a backup, submit a service request through the Support Portal.

Steps

1. Complete the following fields:
   - **Subject**: Enter a description of your request, including the action to be taken.
   - **Environment Type**: Specify the type of environment affected by this request.
   - **Proposed Change Window**: Specify the dates or times in which you want the work complete.
2. In the **Capability** list, select **Platform service requests → Restore from a backup**.
3. In the **Product** field, indicate whether your request is regarding PingAccess, PingDirectory, or PingFederate.
4. In the **Date and time to restore to** field, provide the date and time that you want the product to be restored from a backup. The Support team will use the most recent backup available that is earlier than the date you requested.
5. In the **Business Priority** list, select the appropriate description:
   - Change needed by deadline to avoid business impact
   - Change modifies existing functionality
   - Change adds new functionality
6. In the **Description** field, enter a description of your request.
7. If you are tracking your request within your organization, enter the tracking ID or ticket number associated with it in the **Customer Tracking ID** field.
8. To submit your request, click **Save**.

Enable debug logging

To enable the debug logger on an environment or application, submit a service request through the Support Portal.

Steps

1. Complete the following fields:
    - **Subject**: Enter a description of your request, including the action to be taken.
    - **Environment Type**: Specify the type of environment affected by this request.
    - **Proposed Change Window**: Specify the dates or times in which you want the work complete.
2. In the **Capability** list, select **Platform service requests → Enable debug logger**.
3. In the **AWS Region** field, select the region of your P1AS environment (US1, EU1, AU1, etc.) that you want to update.
4. In the **Targeted application** field, specify the application that the hostname will point to.
5. In the **Business Priority** list, select the appropriate description:
    - Change needed by deadline to avoid business impact
    - Change modifies existing functionality
    - Change adds new functionality
6. In the **Description** field, enter a description of your request.
7. If you are tracking your request within your organization, enter the tracking ID or ticket number associated with it in the **Customer Tracking ID** field.
8. To submit your request, click **Save**.

Enable outbound provisioning

To enable outbound provisioning, submit a service request through the Support Portal.

Steps

1. Complete the following fields:
    - **Subject**: Enter a description of your request, including the action to be taken.
    - **Environment Type**: Specify the type of environment affected by this request.
    - **Proposed Change Window**: Specify the dates or times in which you want the work complete.
2. In the **Capability** list, select **Platform service requests → Enable outbound provisioning**.
3. In the **AWS Region** field, select the region of your P1AS environment (US1, EU1, AU1, etc.) that you want to update.
4. In the **Business Priority** list, select the appropriate description:
    - Change needed by deadline to avoid business impact
    - Change modifies existing functionality
    - Change adds new functionality

5. In the **Description** field, enter a description of your request.
6. If you are tracking your request within your organization, enter the tracking ID or ticket number associated with it in the **Customer Tracking ID** field.
7. To submit your request, click **Save**.

Load or performance test

To request a load or performance test, submit a service request through the Support Portal.

Steps

1. Complete the following fields:
    - **Subject**: Enter a description of your request, including the action to be taken.
    - **Environment Type**: Specify the type of environment affected by this request.
    - **Proposed Change Window**: Specify the dates or times in which you want the work complete.
2. In the **Capability** list, select **Platform service requests → Load/performance test**.
3. In the **Date needed** field, enter the date that you want to perform the load test. Note that this date must be at least two weeks after the request is submitted.
4. In the **Summary of plan** field, provide a summary of the activities that will be performed during testing.
5. In the **What is the success criteria?** field, list the requirements that will determine how the system performed during testing.
6. In the **Business Priority** list, select the appropriate description:
    - Change needed by deadline to avoid business impact
    - Change modifies existing functionality
    - Change adds new functionality
7. In the **Description** field, enter a description of your request.
8. If you are tracking your request within your organization, enter the tracking ID or ticket number associated with it in the **Customer Tracking ID** field.
9. To submit your request, click **Save**.

PingDirectory truststore certificate import

To request a PingDirectory truststore certificate import, submit a service request through the Support Portal.

Steps

1. Complete the following fields:
    - **Subject**: Enter a description of your request, including the action to be taken.

- **Environment Type**: Specify the type of environment affected by this request.
- **Proposed Change Window**: Specify the dates or times in which you want the work complete.

2. In the **Capability** list, select **Platform service requests → PingDirectory truststore certificate import**.
3. In the **Certificate** field, provide the text of the `.crt` public key to trust.
4. In the **Business Priority** list, select the appropriate description:
   - Change needed by deadline to avoid business impact
   - Change modifies existing functionality
   - Change adds new functionality
5. In the **Description** field, enter a description of your request.
6. If you are tracking your request within your organization, enter the tracking ID or ticket number associated with it in the **Customer Tracking ID** field.
7. To submit your request, click **Save**.

SIEM integration

To integrate SIEM data, submit a service request through the Support Portal.

Steps

1. Complete the following fields:
   - **Subject**: Enter a description of your request, including the action to be taken.
   - **Environment Type**: Specify the type of environment affected by this request.
   - **Proposed Change Window**: Specify the dates or times in which you want the work complete.
2. In the **Capability** list, select **Platform service requests → SIEM Integration**.
3. In the **Type of Integration** field, select the type of integration that you want to use. The Support team will reach out to you to gather details about the integration after the case is created.
4. In the **Business Priority** list, select the appropriate description:
   - Change needed by deadline to avoid business impact
   - Change modifies existing functionality
   - Change adds new functionality
5. In the **Description** field, enter a description of your request.
6. If you are tracking your request within your organization, enter the tracking ID or ticket number associated with it in the **Customer Tracking ID** field.
7. To submit your request, click **Save**.

Rollback SIEM

To request a SIEM rollback, submit a service request through the Support Portal.

Steps

1. Complete the following fields:
    - **Subject**: Enter a description of your request, including the action to be taken.
    - **Environment Type**: Specify the type of environment affected by this request.
    - **Proposed Change Window**: Specify the dates or times in which you want the work complete.
2. In the **Capability** list, select **Platform service requests → Rollback SIEM**.
3. In the **AWS Region** field, select the region of your PingOne Advanced Services environment (US1, EU1, AU1, etc.) that you want to update.
4. In the **Business Priority** list, select the appropriate description:
    - Change needed by deadline to avoid business impact
    - Change modifies existing functionality
    - Change adds new functionality
5. In the **Description** field, enter a description of your request.
6. If you are tracking your request within your organization, enter the tracking ID or ticket number associated with it in the **Customer Tracking ID** field.
7. To submit your request, click **Save**.

Subscribe to SNS alerts

To subscribe to SNS alerts, submit a service request through the Support Portal.

Steps

1. Complete the following fields:
    - **Subject**: Enter a description of your request, including the action to be taken.
    - **Environment Type**: Specify the type of environment affected by this request.
    - **Proposed Change Window**: Specify the dates or times in which you want the work complete.
2. In the **Capability** list, select **Platform service requests → Subscribe to SNS alerts**.
3. In the **AWS Region** field, select the region of your P1AS environment (US1, EU1, AU1, etc.) that you want to update.
4. In the **Customer AWS account ID** field, enter the ID for the account that will receive alerts.
5. In the **Subscription type** field, specify how the alert will be delivered (either email, HTTP, or SQS).

6. In the **Business Priority** list, select the appropriate description:
    - Change needed by deadline to avoid business impact
    - Change modifies existing functionality
    - Change adds new functionality
7. In the **Description** field, enter a description of your request.
8. If you are tracking your request within your organization, enter the tracking ID or ticket number associated with it in the **Customer Tracking ID** field.
9. To submit your request, click **Save**.

Update TLS certificate

To update TLS certificates, submit a service request through the Support Portal.

Steps

1. Complete the following fields:
    - **Subject**: Enter a description of your request, including the action to be taken.
    - **Environment Type**: Specify the type of environment affected by this request.
    - **Proposed Change Window**: Specify the dates or times in which you want the work complete.
2. In the **Capability** list, select **Platform service requests → Update TLS certificate**.
3. In the **Virtual Hostname** field, provide the name of the host that will be updated with this certificate.
4. In the **Business Priority** list, select the appropriate description:
    - Change needed by deadline to avoid business impact
    - Change modifies existing functionality
    - Change adds new functionality
5. In the **Description** field, enter a description of your request.
6. If you are tracking your request within your organization, enter the tracking ID or ticket number associated with it in the **Customer Tracking ID** field.
7. To submit your request, click **Save**.

Upgrades

Product upgrades can be performed on request. Upgrades are provided once per year, and security patches are applied when they are available. Additional upgrades might require a fee for Professional Services assistance. Submit your upgrade requests through the service request form on the Support & Community page.

Steps

1. Complete the following fields:
    - **Subject**: Enter a description of your request, including the action to be taken.
    - **Environment Type**: Specify the type of environment affected by this request.
    - **Proposed Change Window**: Specify the dates or times in which you want the work complete.
2. In the **Capability** list, select **Platform service requests → Upgrades**.
3. In the **Product to upgrade** field, indicate whether this request is regarding PingAccess, PingDirectory, or PingFederate.
4. In the **Version** field, indicate the version to which you want to upgrade.
5. In the **Business Priority** list, select the appropriate description:
    - Change needed by deadline to avoid business impact
    - Change modifies existing functionality
    - Change adds new functionality
6. In the **Description** field, enter a description of your request.
7. If you are tracking your request within your organization, enter the tracking ID or ticket number associated with it in the **Customer Tracking ID** field.
8. To submit your request, click **Save**.