Anyware Manager (Installable) Administrators Guide

24.03

Table of Contents

Anyware Manager 24.03 7

Where Do I Begin? 7

Where Do I Install Anyware Manager? 8

Ports and Connections 12

What Deployment Topology Can I Use? 12

Single Host Deployment 12

Two/Three Host Deployment 13

Five or more Hosts Deployment 14

How Do I Install Anyware Manager? 15

Using a Default Database and Secret Storage 16

Using an External Database and Secret Storage 16

Installation and Upgrade 17

Prerequisites 17

Anyware Manager System Requirements 17

Installing Anyware Manager - Default Configuration 20

Installing Anyware Manager 20

Installing the Anyware Connector 29

Installing Anyware Manager - External Configuration 30

Preparing an External Database and Secret Storage 30

Installing Anyware Manager 33

Installing the Connector 45

Installing Anyware Manager - Darksite Installation 46

Download and Transfer Dependencies 46

Upgrading Anyware Manager (Online Upgrade) 50

Which Option Should I Choose? 50

Running an In-Place Upgrade 51

Installing Anyware Manager on a new Virtual Machine 53

Removing the Anyware Manager Virtual Machine 54

Upgrading Anyware Manager (Darksite Upgrade) 55

Download and Transfer Dependencies 55

Customizing Anyware Manager 59

Configuration Template Files and Parameters 59

Configuration Template Files 59

Configuration Parameters 60

Configuring Custom TLS Certificates 63

Internal TLS Certificates 63

Configuring Timezone 66

Multi-Admin Support 68

Multi-Admin Support 68

Configuring the Active Directory for Anyware Manager 72

AWS Configuration 74

Admin Console 77

Overview 77

Connecting to the Admin Console 78

Connecting to Anyware Manager 78

Connecting to Anyware Manager as a Service 78

Admin Console Dashboard 80

Configuring the Admin Console 80

Sessions History 82

Data Source and Data Retention 82

Filtering 84

Columns Description 85

Session States Lifecycle 86

Session state transitions 88

Managing Deployments 90

- Cloud Service Accounts 91
- Editing an Existing Deployment 94

Editing a Anyware Connector 96

Provisioning a Remote Workstation 97

- Provisioning a Remote Workstation 99

Workstation Pools 102

- Creating Workstation Pools 102
- Floating Workstation Assignments 112

Workstation Profiles 114

- Creating a Workstation Profile 114
- Deploying a Remote Workstation with a Workstation Profile 115

Workstation Status in Anyware Manager 117

- Types of Errors 117

SAML Configuration with Anyware Manager 118

- What is SAML? 118
- Anyware Manager Initiated SAML Authentication Flow 119
- Configure Anyware Manager as a SAML Service Provider to Enable Multi-Admin 120

Service Account and API Access 123

Federated Authentication 126

- OAuth 126
- Single Sign-On 140
- Troubleshooting Federated Authentication 168

Remote Workstations 173

- Adding a Remote Workstation 173
- Editing a Remote Workstation 175
- Viewing Remote Workstation Users 177
- Updating Cloud Provider Information 178
- AMT Power Management in Anyware Manager 179

System Alerts 187

Anyware Monitor 190

Using Anyware Monitor 190

Installing/Uninstalling Anyware Monitor 202

Troubleshooting Anyware Monitor 211

HP ZCentral Hardware Monitor 215

HP ZCentral Hardware Monitor-Installation 215

HP ZCentral Hardware Monitor-Troubleshooting 220

Admin Console Configuration 223

Setting Time and Date 223

Activity Log 224

Reference 225

Preparing a Secret Storage Application 225

Preparing Azure Key Vault 225

Preparing Hashicorp Vault 225

Configuring a Secret Storage Application 229

Configuring Azure Key Vault 229

Configuring Hashicorp Vault 230

Connecting to a Vault server with Self-Signed TLS Certificates 231

Vault Token Auto-Renewal 232

Vault Data Migration 233

Backing up and Restoring Anyware Manager Data 234

Backing up Anyware Manager Data 234

Restoring Anyware Manager Data 235

Moving Anyware Manager Data 236

Migrating from a Default to External Configuration 238

Prerequisites for Migrating Anyware Manager Data 238

Migrating Internal MongoDB Data 239

Migrating Internal Vault Data 242

- Proxy Configuration for Anyware Manager 248
- Troubleshooting 250
  - Anyware Manager Support Bundle 250
    - Support Bundle Information and Logs 250
  - Anyware Manager Health Status 253
  - Vault Issues 255
  - Repository Management 256
- Logging 257
  - Adding a Sumo Logic Log Collector 257
- Getting Support 260
  - Contacting Support 260
  - The HP Community Forum 260
- Release Notes 261

Anyware Manager 24.03

Anyware Manager is a HP management plane enabling users to configure, manage and monitor brokering of remote workstations. Anyware Manager enables highly-scalable and cost-effective Anyware Software deployments by managing cloud compute costs by brokering PCoIP connections to remote workstations, see Anyware Software for supported hosts.

Anyware Manager is offered in 2 variants – as an HP managed Service, and as an installable instance deployed and managed by the users in their on-premises or cloud environments.

This document covers the installable instance variant of Anyware Manager.

For information on Anyware Manager as a Service, see Anyware Manager as a Service.

Where Do I Begin?

Anyware Manager is a collection of microservices, and each microservice operates from its own docker container. These container images are deployed on a local lightweight Kubernetes (k3s) cluster, on a virtual machine. This cluster is set up on the virtual machine as part of the installation.

Before you begin installing Anyware Manager, it is important to understand what other components are required to enable end to end brokering:

HP Components:

- HP Anyware Connector
- HP PCoIP Registration Key
- HP PCoIP Client
- HP PCoIP Agent

Third-party Components:

- MongoDB
    - Internal: MongoDB
    - External: MongoDB compatible provider

- Vault
    - Internal: Hashicorp Vault
    - External: Azure Key Vault

MongoDB is the data store that hosts all Anyware Manager information, configurations and settings.

Hashicorp Vault is the secret storage where Anyware Manager can store and encrypt all the secrets and keys.

Azure Key Vault is the cloud service from Microsoft that enables the secure storage of, and access to, secrets.

Anyware Connector is an access hub that facilitates PCoIP connections to remote desktops and workstations by providing user authentication, entitlement, and security gateway services. It is installed on a separate Virtual Machine that resides in your environment. Based on your requirements, you may need multiple Connectors. Please ensure you have read all the installation guidelines and prerequisites in the Anyware Connector System Requirements Section[add link when document is published].

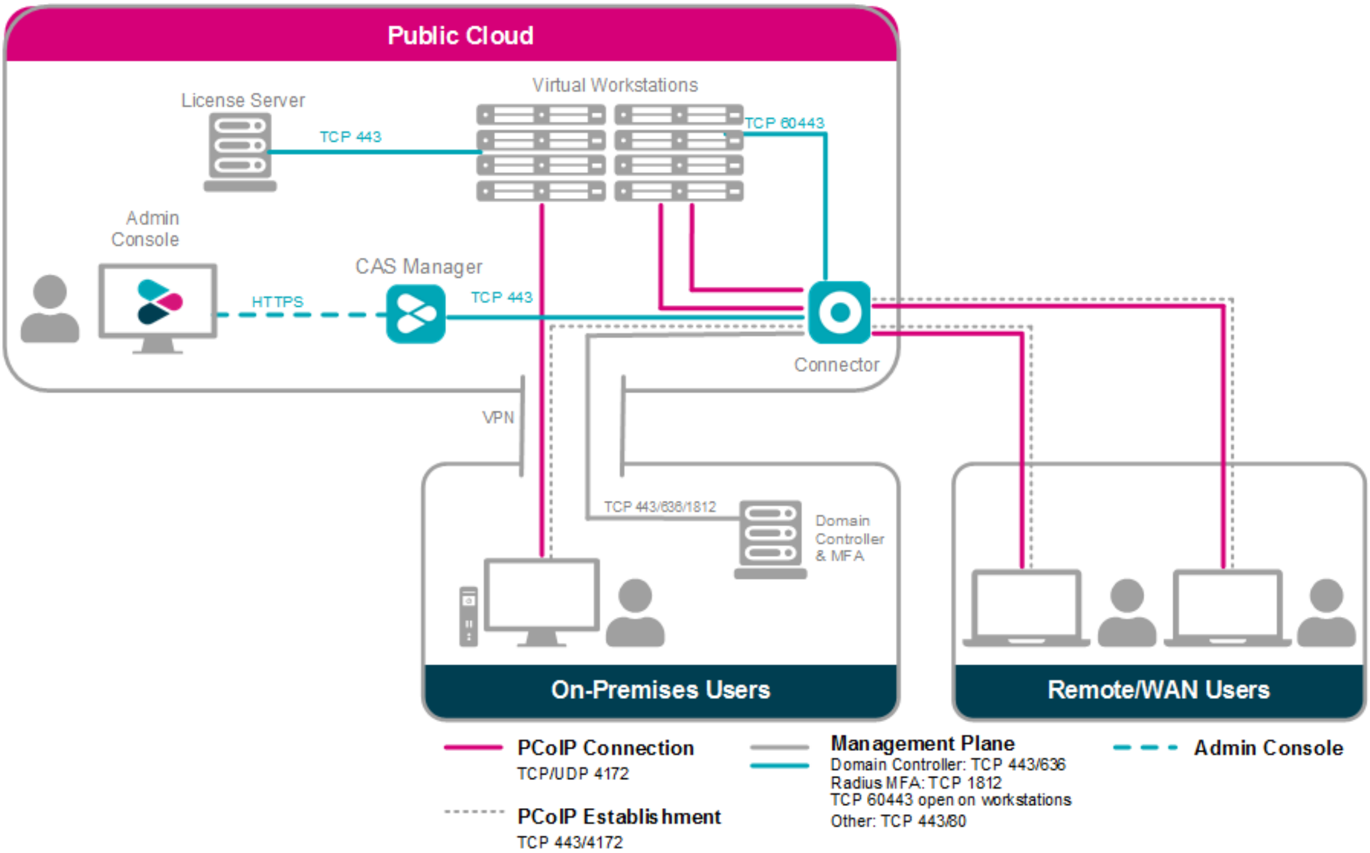
Where Do I Install Anyware Manager?

The following architectural diagrams depict where Anyware Manager can be installed in multiple infrastructures – be it the Public Cloud, On-Premises or a Hybrid deployemnt.

Please pay close attention to the number of Connectors required based on your setup, and the ports you may need to configure to allow PCoIP traffic (pre-session and in-session). These ports are outlined in the Ports and Connections table.

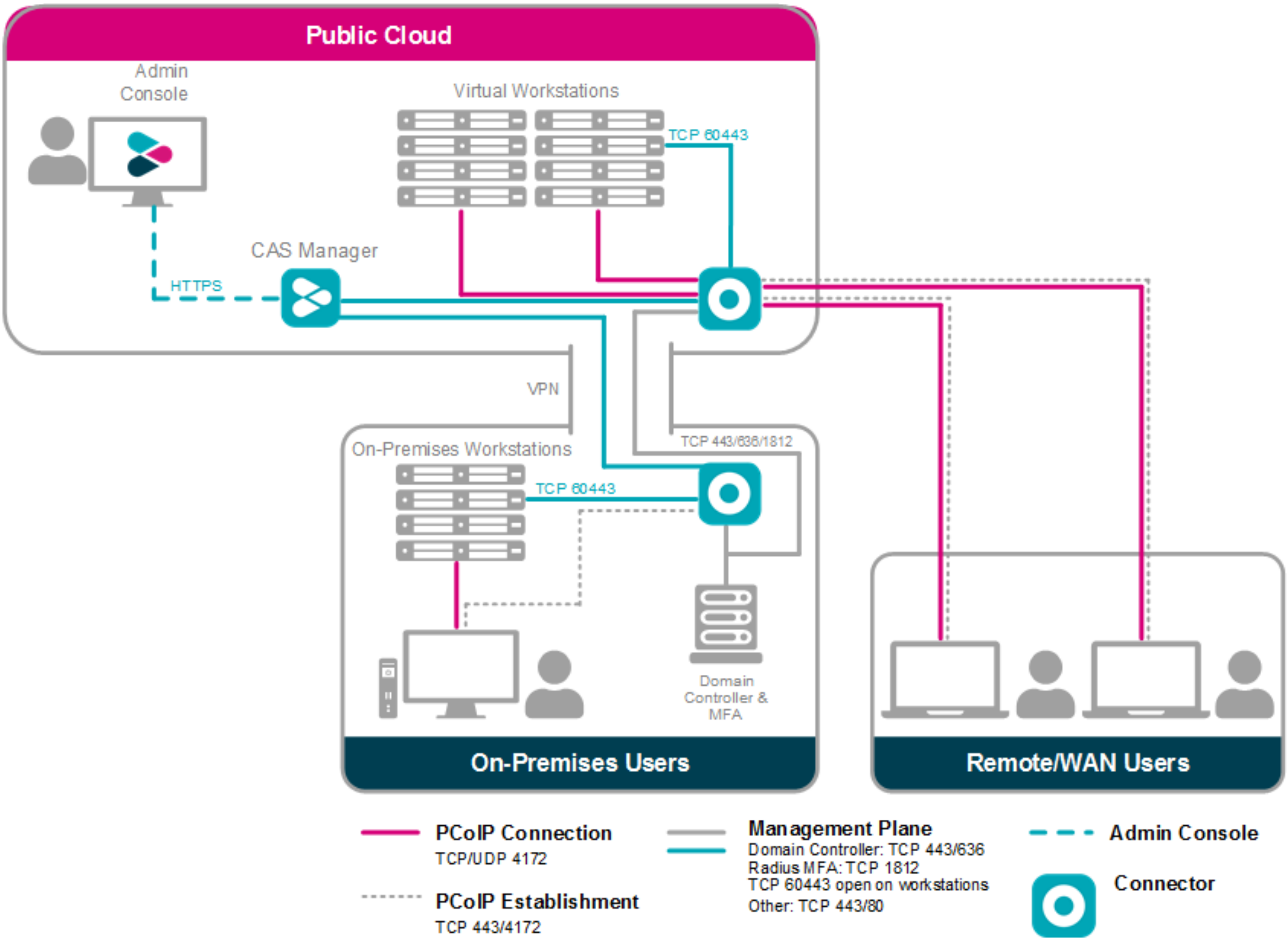
Public Cloud Deployment

The following diagram illustrates a public cloud deployment with Anyware Manager.



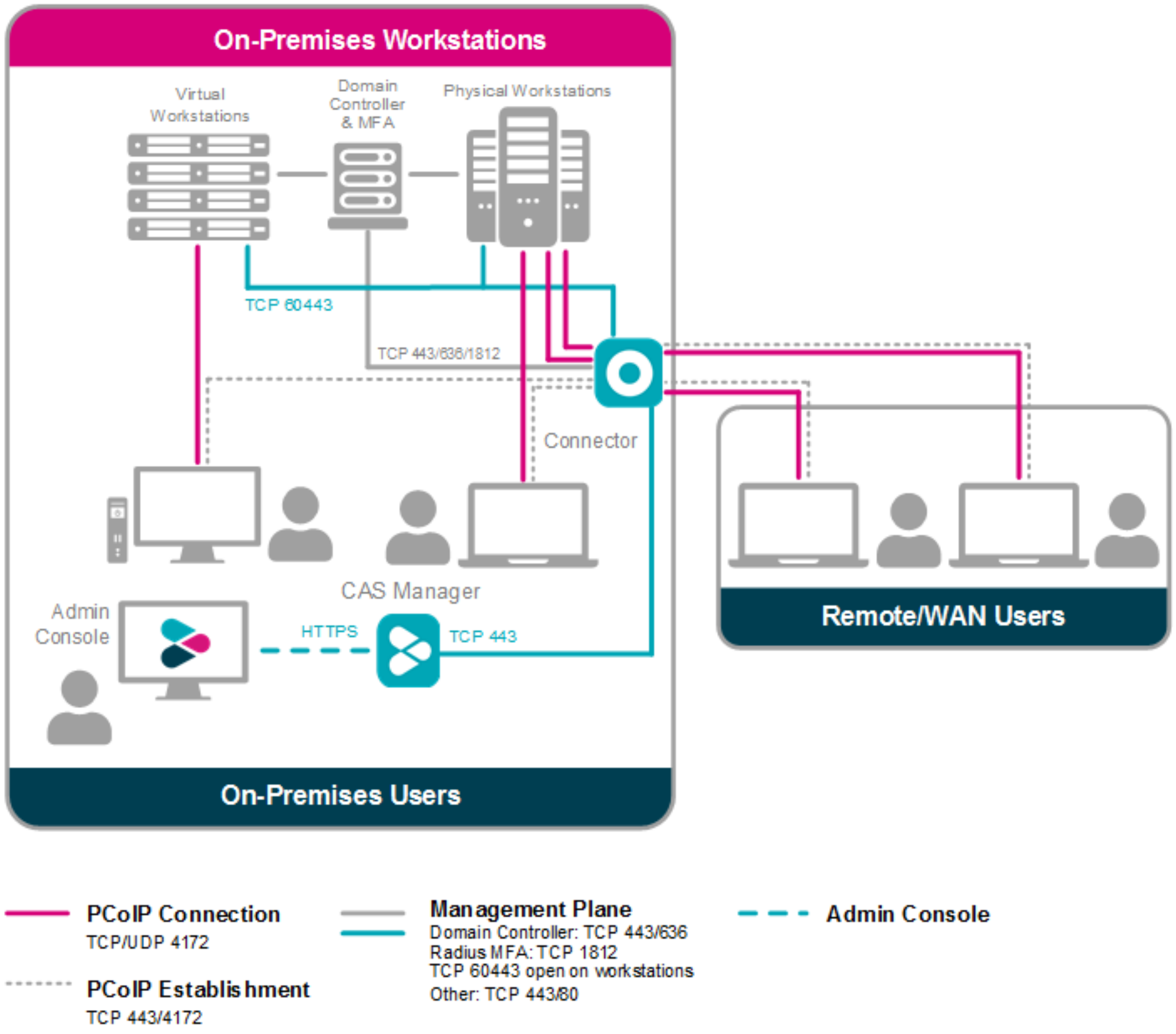
Hybrid Deployment

The following diagram illustrates a hybrid deployment where Anyware Manager is deployed in the Public Cloud.



On-Premises Deployment

The following diagram illustrates an on-premises deployment with Anyware Manager.


On-Premises Workstations
Virtual Workstations
Domain Controller & MFA
Physical Workstations
TCP 60443
TCP 443/636/1812
Connector
CAS Manager
Admin Console
HTTPS
TCP 443
On-Premises Users
Remote/WAN Users
PCoIP Connection
TCP/UDP 4172
PCoIP Establishment
TCP 443/4172
Management Plane
Domain Controller: TCP 443/636
Radius MFA: TCP 1812
TCP 60443 open on workstations
Other: TCP 443/80
Admin Console

Ports and Connections

Anyware Manager requires certain ports to be open to enable connections between the other components such as Connector, MongoDB, Vault etc. The following table outlines the required ports and connections for Anyware Manager:

Component	Allow	Port/ Protocol	Source/Destination Component	Description
Anyware Manager	Inbound	443/TCP	From administrative web browsers, HTTP request clients and Connector.	To enable access to Anyware Manager.
Anyware Manager	Outbound	443/TCP	To the public license server.	Validates the CAS registration code.
Anyware Manager	Outbound	8200/TCP	To external Vault.	Stores Anyware Manager secrets.
Anyware Manager	Outbound	27017/ TCP	To external MongoDB.	Stores Anyware Manager data.
Anyware Manager	Outbound	636/TCP	To Domain Controller.	Authenticates users to Anyware Manager.
Anyware Manager	Outbound	53/UDP	To DNS.	Domain name resolution.

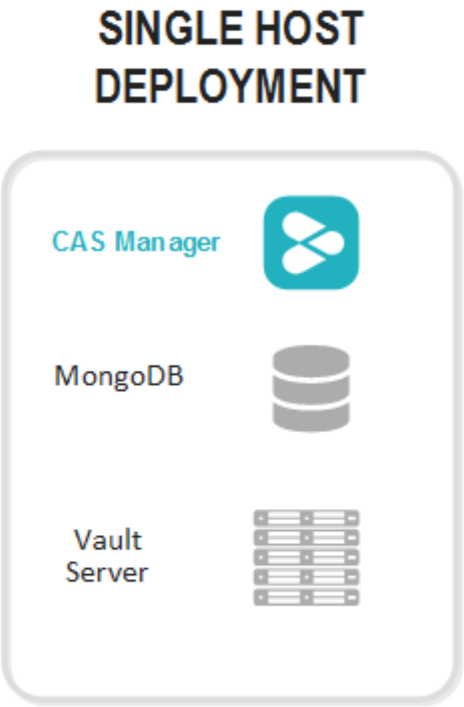
What Deployment Topology Can I Use?

In terms of deployment topologies and scenarios, Anyware Manager is flexible and can be deployed in a single host, or with multiple hosts, depending on your organization's network environment and operational requirements. The possible deployment topologies are outlined below. Connector(s) are not included in these diagrams, they are deployed on additional host(s) separately.

Single Host Deployment

This deployment configuration is when Anyware Manager and MongoDB and Vault server are running on a single host, it can be deployed on a virtual machine on any cloud or on-premise. It should be used for getting started with Anyware Manager for initial prototyping or smaller scale production deployments. If you use this configuration for production environment you must ensure there is a backup and restore process in place. This is necessary to minimize the loss of data and to minimize down time.

For information on installing Anyware Manager as part of a single host deployment, see Installing Anyware Manager - Default Configuration.

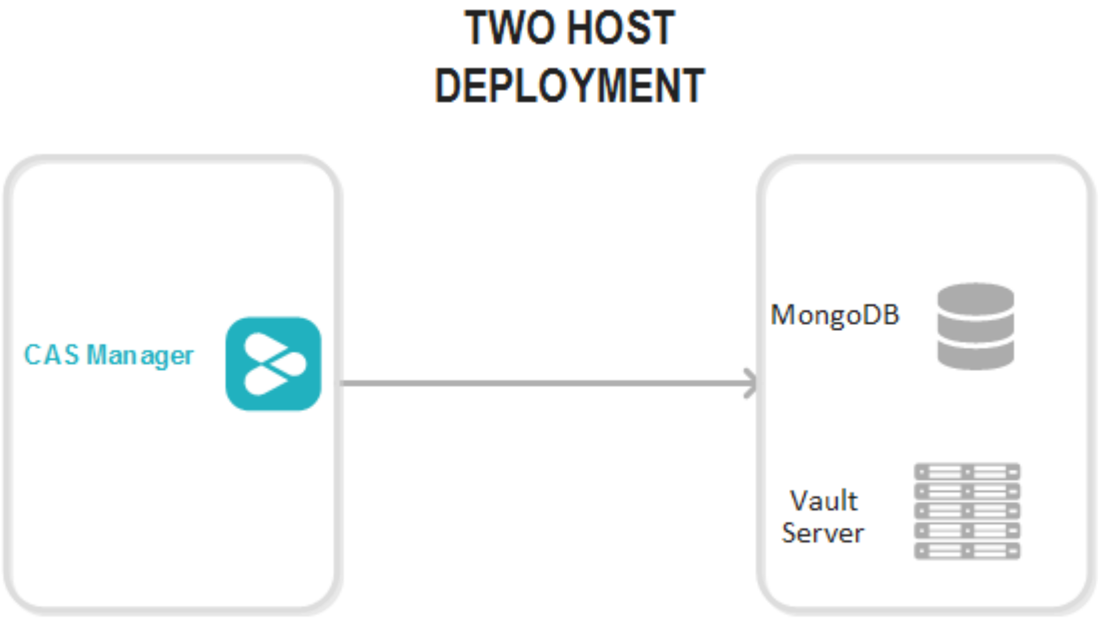


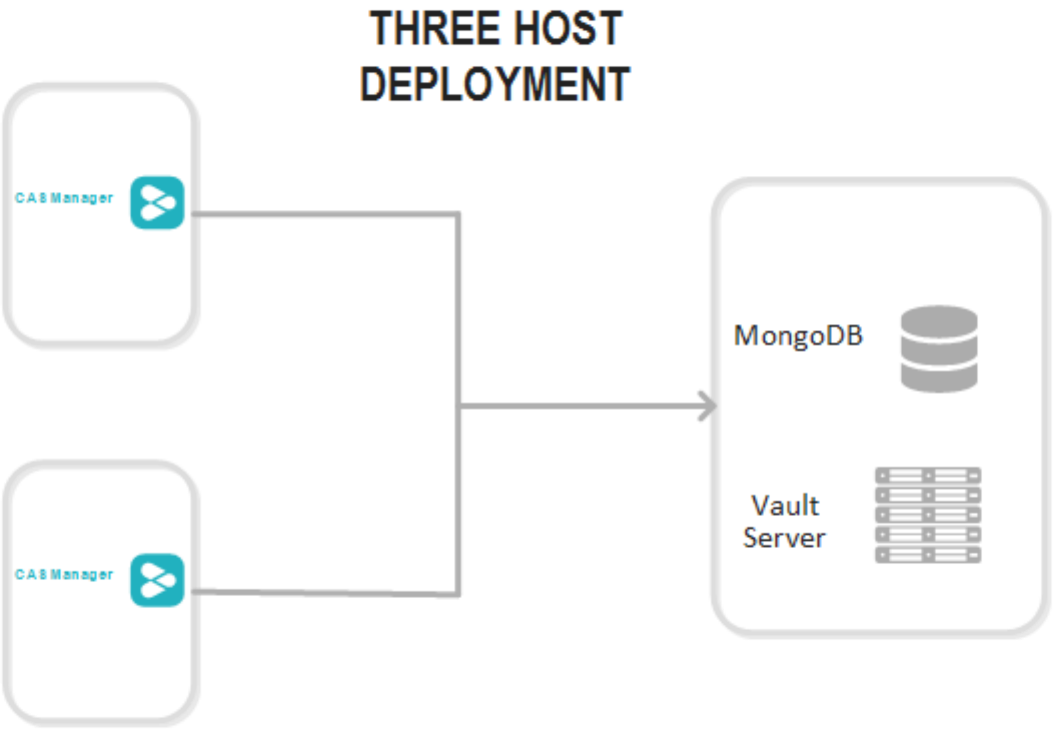
Two/Three Host Deployment

This deployment configuration is when Anyware Manager, MongoDB and Vault server are running on separate hosts. By hosting the database and secret storage on a separate machine, it reduces the risk of data loss in the case of Anyware Manager server failure. This configuration enables high-availability and scalability for Anyware Manager by deploying multiple instances of Anyware Manager. This configuration has the following limitations:

- With only one instance of MongoDB and Vault deployed, high-availability is not available to the data persistence layer, and a backup and restore process must be in place for the server hosting MongoDB and Vault to minimize data loss.
- You can configure this deployment on virtual machines hosted on-premises or on any cloud.
- This configuration requires a certain level of technical knowledge around MongoDB and Vault to properly deploy and operate these external components. For detailed deployment instructions on installing and configuring MongoDB and Vault in a single virtual machine to be used by Anyware Manager, see the following Knowledge Base article.

For information on installing Anyware Manager as part of a two/three host deployment, see Installing Anyware Manager - External Configuration.

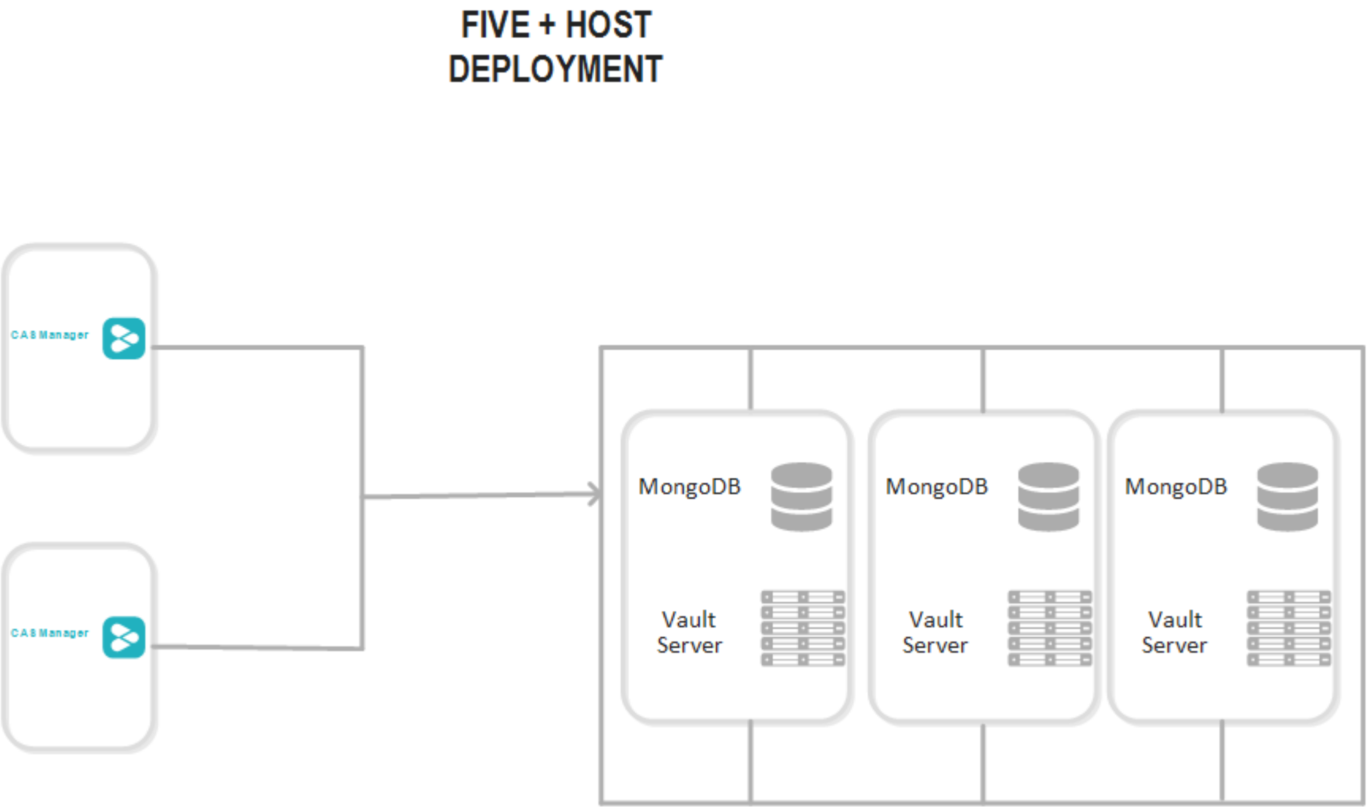




Five or more Hosts Deployment

This deployment configuration provides high-availability for Anyware Manager, MongoDB, and Vault server that are on separate hosts. In this configuration, two or more Anyware Manager instances provide high-availability using a load balancer. The hosts that contain the MongoDB and Vault server provide a basic high-availability for data persistence with a failure tolerant of 1. This is a complex environment and requires you to have working knowledge of installing, configuring, and operating the MongoDB and Vault server services in a high-availability setup. Visit MongoDB and Hashicorp Vault official documentation sites for detailed instructions on how to carry out these steps.

For information on installing Anyware Manager as part of a five or more host deployment, see [Installing Anyware Manager - External Configuration](#).



How Do I Install Anyware Manager?

You need to setup and install a dedicated virtual machine that can host Anyware Manager. This virtual machine needs to meet certain system requirements which are outlined in the sections below. If you are using an external MongoDB and secret storage you need to prepare these components before installing Anyware Manager, and then configure them afterwards. The available configurations are outlined below.

⚠ **Connector Installation**

Once you have installed Anyware Manager using either of the configurations below, you need to install the Connector. This should take roughly **1 hour** to complete.

Using a Default Database and Secret Storage

This is the default installation of Anyware Manager where an instance of MongoDB and Vault is deployed as part of the installation. Installation of these components is seamlessly built into the Anyware Manager installer. This configuration does not scale beyond a single Anyware Manager instance and does not support high availability. For more information on this configuration, see Installing Anyware Manager - Default Configuration.

⚠ **Installation Time**

Installing Anyware Manager with the default database and secret storage should take roughly **45 minutes** to complete. It should take a further **1 hour** to install the Connector.

Using an External Database and Secret Storage

With Anyware Manager you can prepare and install your own instances of MongoDB and Vault, or you can use an Azure Key Vault service, on a different virtual machine, by following the guidelines in the installation section. This enables you to upgrade or re-install Anyware Manager, and makes a high-availability service available. For more information on this configuration, see Installing Anyware Manager - External Database and Secret Storage Configuration.

⚠ **Production Environments**

Installing Anyware Manager with an external database and secret storage should take roughly **2 hours** to complete. It should take a further **1 hour** to install the Connector.

Installation and Upgrade

Prerequisites

Anyware Manager System Requirements

Before installing Anyware Manager you need to prepare your system as per the recommended configuration, configure system firewall and proxy settings on the Anyware Manager virtual machine.

System Requirements

Your virtual machine must have the following configuration:

- Operating System: RHEL 8 and Rocky Linux 8.
- 8 GB RAM (Minimum)
- 4 CPU
- 60 GB Storage: If you are using LVM and /var is mounted on a separate volume, that volume must have 30GB or more in order for the installation to succeed and for Anyware Manager to function properly.
- Active Directory permissions set to **List contents** and **Read all properties**. If you do not set these permissions you are not able to connect to a specific remote workstations.
- The VM's hostname should be as per standards defined in **RFC1123** and it must:
    - Contain only 253 characters.
    - Contain only lowercase alphanumeric characters, '-' or '.'.
    - Start with an alphanumeric character.
    - End with an alphanumeric character.

Firewall Configuration

The firewall on the Anyware Manager Virtual machine must be configured as follows:

Enable Port 443

Ensure port 443 is enabled in the firewall rules for the Anyware Manager Virtual Machine.

1. Login to the Anyware Manager Virtual Machine by ssh from a bash shell as root.
2. Confirm if firewall is active by running this command: `sudo systemctl status firewalld`.
3. If `firewalld` is active, Run the following commands to configure the firewall:

```
sudo firewall-cmd --permanent --add-port=6443/tcp # virtual network flannel
sudo firewall-cmd --permanent --zone=trusted --add-source=10.42.0.0/16 #
This subnet is for the pods
sudo firewall-cmd --permanent --zone=trusted --add-source=10.43.0.0/16 #
This subnet is for the services
sudo firewall-cmd --reload
```

If `firewalld` is inactive, and your organization does not require firewall on the Anyware Manager Virtual Machine, then skip the firewall configuration.

Proxy Configuration

If you are using HTTP/HTTPS proxy, you must configure it. For NO_PROXY, provide the specific IP addresses or domain names for internal services. The IP address range such as "10.0.0.0/8" does not work; you should add the exact IP address or domain name for the traffic routing through proxy. Configure the following variables in the `/etc/environment` file:

1. Run this command to edit the `/etc/environment/` file in vim. You could also use vim or nano: `sudo vi /etc/environment`.
2. Update the file to include the following environment variables:

```
HTTPS_PROXY="http://hostname_of_proxy:port"
HTTP_PROXY="http://hostname_of_proxy:port"
NO_PROXY=[list of all host names that should not go through the proxy,
such as: localhost, 127.0.0.1, 0.0.0.0, ip_address_of_mongo]
ALL_PROXY="http://hostname_of_proxy:port"
https_proxy="http://hostname_of_proxy:port"
http_proxy="http://hostname_of_proxy:port"
no_proxy=”=[list of all host names that should not go through the proxy,
such as: localhost, 127.0.0.1, 0.0.0.0, ip_address_of_mongo]
all_proxy="http://hostname_of_proxy:port"
```

3. Save the file. When you install Anyware Manager, you can configure the file to use the proxy configuration. From this new terminal, proceed with the installation steps. The proxy configuration is implemented when Anyware Manager is installed.

Anyware Software Registration Code

When you have a HP Anyware Software subscription, an email with the registration code is sent to you. To contact sales and enquire about attaining a Anyware Software subscription, contact our Sales Team.

Installing Anyware Manager - Default Configuration

For the Anyware Manager installation, you should configure a repository to download and save configuration files, configure SELinux policies, and run the installation package. Anyware Manager can be installed and configured along with a default or an external database. This section outlines the default installation method for Anyware Manager.

Installation Time

The default configuration of Anyware Manager uses an internal Vault and MongoDB. It takes approximately **45 minutes** to complete the installation.

Data Migration

Anyware Manager does not do any data migration when configuring your database and secret storage application. Any data stored when Anyware Manager is used with the default database and secret storage configuration is not transferred if the same Anyware Manager instance is re-configured to run with an external database and secret storage.

Firewall and Load Balancing Considerations

For information on firewall and load balancing ports connected to Anyware Manager and Connector, see Firewall and Load Balancing Considerations

Installing Anyware Manager

The following section outlines how to install Anyware Manager with the default database and secret storage. These steps should be performed on the target machine by connecting via SSH or console.

⚠ **Before you begin**

Follow the prerequisite steps in the Anyware Manager System Requirements section to prepare your target machine. It is important to read and address all the prerequisites outlined. Once you have completed these steps and prepared the target machine, return to this page and continue with the installation.

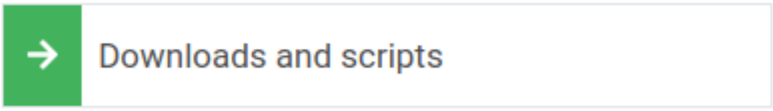
1. Add Anyware Manager Repository

The virtual machine you are adding the repo to must have access to the internet to be able to download and install the required files.

Anyware Manager Repositories

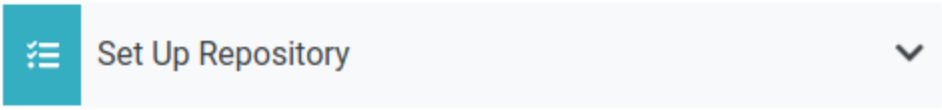
The new repository `teradici-anyware-manager` is introduced. If you currently have `teradici-cas-manager` repository, you must remove it. See Repository Management to remove them. Once the unwanted repos are removed, you can proceed with the installation process below.

To access the scripts and to configure and add the RHEL and Rocky Linux repository, select the **Downloads and scripts** option from the
Anyware Manager support site.



If you see a login button instead, click it to log into the site and then proceed.

Accept the End User License Agreement, then click **Set Up Repository**.



The window expands and displays the setup scripts for each supported operating system. Copy the command for your system to the clipboard.

Paste command on the target machine where you wish to install Anyware Manager and press `Enter`.

The command fetches a configuration script from our servers and runs it locally, setting up and configuring the repository on the local machine.

Run the following command to confirm `teradici-anyware-manager` repos were added into dnf repo.

```
dnf repolist --enabled teradici-anyware-manager*
```

The output from this command should list the repo id, names as outlined in the example below:

```
repo id                                                     repo name
teradici-anyware-manager-beta                               teradici-anyware-manager-
beta
teradici-anyware-manager-beta-noarch                        teradici-anyware-manager-
beta-noarch
teradici-anyware-manager-beta-source                        teradici-anyware-manager-
beta-source
```

2. SELinux Configuration

SELinux policies are required for persistent storage and container logging on Anyware Manager. If SELinux policies are not found, data stored in Anyware Manager is lost when the Anyware Manager Machine is shut down.

Once configured, and the installation has verified SELinux, all Anyware Manager related data persists when the target machine hosting Anyware Manager is re-booted. To check if SELinux is already installed on your system, run the following command:

```
sudo dnf list installed | grep anyware-manager-selinux
```

The output from this command notifies if you if `selinux` is already running on your system. If it is not then you need to run the following commands to install the SELinux policies:

Run the following command to install the SELinux policies and set the basic framework for persistent database and Vault:

Run the following command to install a specific version of SELinux that has been tested for K3s:

Run the following command to install SELinux from the Anyware Manager repo:

Install Command Alias

The older command `sudo dnf install -y cas-manager` works as an alias for Anyware Manager installation.

3. Install Anyware Manager

Installation Commands Updated

Anyware Manager installation requires two commands comparing to previous version where only one command is required. If you have automated the installation in scripting, make sure the script is updated accordingly.

Run the following command to install Anyware Manager RPM:

```
sudo dnf install -y anyware-manager
```

The installer installs Anyware Manager, as well as all external components required.

These external components are:

- k3s
- MongoDB (data store)
- Vault (secret store from HashiCorp)
- A self-signed SSL certificate for HTTPS access

Run the following command to install Anyware Manager with the appropriate flags suits your needs, see "Installation Flags and Options" for all supported flags. The command example below installs Anyware Manager with self-signed certificate from teradici-anyware-manager* repo added in the pervious steps. Debug level log is displayed to help troubleshooting.:

```
sudo /usr/local/bin/anyware-manager install --accept-policies --self-signed --debug
```

PASSWORD CONFIGURATION

You need to configure a password to install Anyware Manager instance on your system. The password adds a layer of protection to the system and is required when accessing the Web Admin Console. To meet the security standards, the password should be 8 characters in length with minimum 1 uppercase, 1 lowercase, 1 number and 1 special character.

> **Password Special Character**
>
> The `%` character and whitespaces are not supported.

Anyware manager installer requires Web Admin password and prompts for it, if this behavior is not preferred the password could be passed to the install command using:

```
--manager-admin-password
```

In case you forget the password, you can reset it using the following flag with the `configure` command:

```
--reset-admin-password
```

> **Password File**
>
> The `/opt/teradici/casm/temp-creds.txt` file that has the ability to store Anyware Manager password is not created any more by the installer. If you forget your password, you need to reset it using the `--reset-admin-password` flag.

INSTALLATION FLAGS AND OPTIONS

For detailed information on the installation flags and the configuration file parameters that you can pass during installation, see the table outlined below:

Flags	Example	Description
`--accept-policies`	sudo /usr/local/bin/anyware-manager install --accept-policies	If this flag is set, the installer does not prompt for accepting policies. This flag is optional
`--clear`	sudo /usr/local/bin/anyware-manager install --clear	This flag Removes data and files of an existing or previous Anyware Manager instance.
`--manifest`	sudo /usr/local/bin/anyware-manager install --manifest	This flag is set to provide a path for manifest files. This flag is optional.
`--self-signed`	sudo /usr/local/bin/anyware-manager install --self-signed	This flag is set to Automatically generate self-signed TLS cert and key. Setting this flag ignores `--tls-key` and `--tls-cert` flags.
`--tls-key`	sudo /usr/local/bin/anyware-manager install --tls-key	If this flag is set, it requires the full path and filename of the TLS key to use with the Anyware Manager.
`--tls-cert`	sudo /usr/local/bin/anyware-manager install --tls-cert	If this flag is set,it requires the full path and filename of the TLS certificate to use Anyware Manager.
`--registry`	sudo /usr/local/bin/anyware-manager install --registry	This flag is used to specify the container registry from which the Anyware Manager pulls container images.
`--registry-username`	sudo /usr/local/bin/anyware-manager install --registry-username	This flag is used to authenticate Anyware Manager username to the registery and to pull container images.
`--registry-password`	sudo /usr/local/bin/anyware-manager install --registry-password	This flag is used to authenticate Anyware Manager password to the registry to pull container images.
`--manager-admin-password`	sudo /usr/local/bin/anyware-manager install --manager-admin-password	This flag is used to create a new password for Anyware Manager during installation.
`--reset-admin-password`	sudo /usr/local/bin/anyware-manager configure --reset-admin-password	This flag is used to reset the password for Anyware Manager.

```
sudo dnf install -y anyware-manager-selinux
sudo dnf install -y https://github.com/k3s-io/k3s-selinux/releases/download/
v1.1.stable.1/k3s-selinux-1.1-1.el8.noarch.rpm
```

```
sudo dnf install -y selinux-policy-base container-selinux
```

Vault Data Encryption

The Vault data that is installed as part of the Anyware Manager installation, is installed on the Anyware Manager virtual machine, and is encrypted at rest. It is recommended that you take appropriate measures to secure access to the filesystem. For information on this, see the Filesystem Storage Backend section of the HashiCorp Vault guide.

The installation process takes 5-10 minutes to complete, depending on your network connection speed and other environment variables. During this process, Anyware Manager is running a health check every 15 seconds to confirm that all required services are deployed and running successfully before reporting that the installation is complete.

Once the installation has been successful you should see a message stating **Anyware Manager installation complete**. The IP address and the version of your Anyware Manager instance isdisplayed.

If the installation appears unhealthy, you should generate a support bundle and send this to HP for investigation. For more information on generating a support bundle, see Support Bundle. For more information on monitoring and assessing the health status of Anyware Manager, see Health Status.

Generated Self-Signed Certificates

The installer automatically generates several certificates to ensure that internal communication within the Anyware Manager and communication to the Anyware Manager itself are done over encrypted TLS connections. These certificates are automatically generated as needed when Anyware Manager is initially installed or when upgrades are done. If you do not wish to upgrade, certificates must be periodically renewed, see TLS Certificates for steps on how to do this.

4. Configure Anyware Manager to use Proxy

The following section outlines the steps involved in enabling the proxy configuration with Anyware Manager:

1. If the proxy environment variables were not set before installing Anyware Manager, please see the Proxy Configuration Variables section above for the steps involved in setting these variables. If you already have these variables set, continue to step 2.
2. Establish a new ssh/shell session.
3. Configure Anyware Manager to use the proxy configuration by running the following command:

```
sudo /usr/local/bin/anyware-manager configure --enable-proxy
```

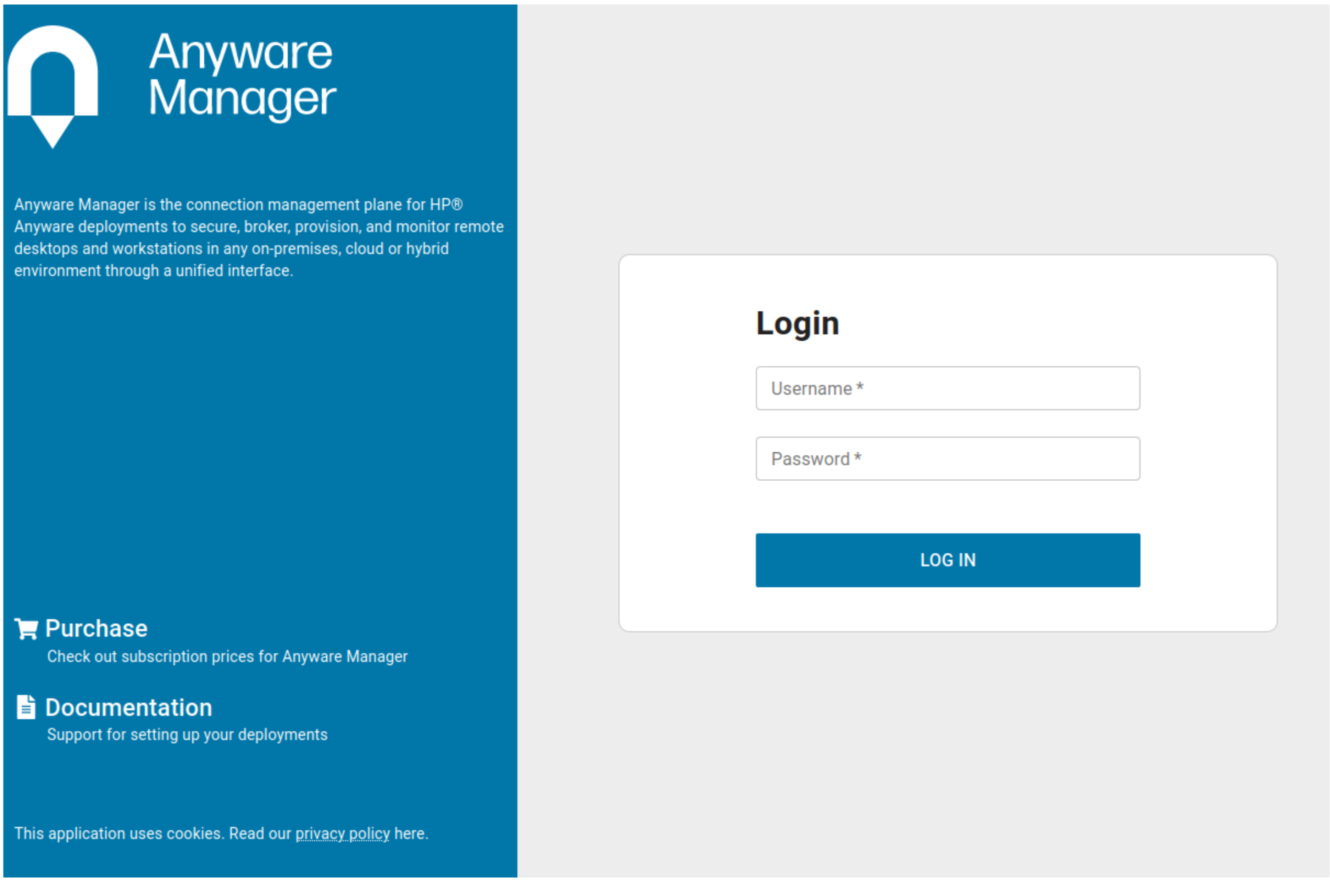
5. Access the Admin Console

The following section outlines how to access and unlock the Anyware Manager Admin Console.

1. Open a web browser and go to https://{ip-address-or-dns-name-of-anyware-manager}. This is the IP address of the target machine where Anyware Manager is installed.
2. When presented with the Anyware Manager Login page, use the following credentials to begin using Anyware Manager:

   username: adminUser

   password: The password that is configured during Anyware Manager installation.



Anyware Manager

Anyware Manager is the connection management plane for HP® Anyware deployments to secure, broker, provision, and monitor remote desktops and workstations in any on-premises, cloud or hybrid environment through a unified interface.

Purchase
Check out subscription prices for Anyware Manager

Documentation
Support for setting up your deployments

This application uses cookies. Read our privacy policy here.

Login

Username *

Password *

3. Click **Login**.

You are now able to use Anyware Manager as the **adminUser** user.

To unlock the Admin Console enter your Anyware Software registration code into the Unlock dialog that appears when you first log-in. Anyware Manager verifies the registration code and then create a new deployment on your behalf. For further information on using the Admin Console, see Admin Console.

6. Anyware Manager dnf Repo Management

By default, Anyware Manager installs any updates that are available, when you update all managed packages with the following command:

```
dnf upgrade anyware-manager
```

or

```
dnf update anyware-manager
```

This system wide update includes any new Anyware Manager version updates. If you do not want this system wide update, the Anyware Manager repo(s) should be disabled once installation is complete.

LOCKING ANYWARE MANAGER VERSION IN THE DNF REPO

The following section outlines how to lock the Anyware Manager in the dnf repo:

1. Run this command: `sudo dnf config-manager --set-disabled teradici-anyware-manager*`.
2. To confim the settings, run this command: `dnf repolist teradici-anyware-manager*`.

The output from this command should list the repo id, names and their status, as outlined in the example below:

```
repo id                                         repo
name                                       status
teradici-anyware-manager                            teradici-anyware-
manager                            disabled
teradici-anyware-manager-noarch                     teradici-anyware-manager-
noarch                     disabled
teradici-anyware-manager-source                     teradici-anyware-manager-
source                     disabled
```

Installing the Anyware Connector

Once you have installed the Anyware Manager you can install Anyware Connector(s) by following the instructions outlined in the Installing the Connector section.

Installing Anyware Manager - External Configuration

For the Anyware Manager external installation, you should configure an external database and secret storage, a repository to download and save configuration files, configure SELinux policies, and run the installation package. Anyware Manager can be installed and configured along with a default or an external database. This section outlines the external configuration installation method for Anyware Manager.

Installation Time

The default configuration of Anyware Manager uses an internal Vault and MongoDB. It takes approximately **45 minutes** to complete the installation.

Data Migration

Anyware Manager does not do any data migration when configuring your database and secret storage application. Any data stored when Anyware Manager is used with the default database and secret storage configuration is not transferred if the same Anyware Manager instance is re-configured to run with an external database and secret storage.

Firewall and Load Balancing Considerations

For information on firewall and load balancing ports connected to Anyware Manager and Connector, see Firewall and Load Balancing Considerations

By default, Anyware Manager installs a database and secret storage on the same virtual machine. If you want to use an external database and secret storage, which we recommend for scaling, continue with the steps outlined below to prepare the external database and secret store.

Preparing an External Database and Secret Storage

The following sections outline how to prepare a secret storage application and MongoDB that can be configured to work with Anyware Manager.

Verified Versions

The table below outlines the versions of MongoDB and Vault that are verified with Anyware Manager:

Anyware Manager Version	Vault Version	MongoDB Version
22.01	1.7.1	4.2.14
22.04	1.7.1	4.2.14
22.09	1.7.10	4.2.14
23.01	1.7.10	4.2.14
23.04	1.11.6	4.2.14

Preparing a Secret Storage Application

It is possible to use either Hashicorp Vault or Azure Key Vault, depending on your environment and needs, for secret and key encryption and storage with Anyware Manager. Once you have successfully installed Anyware Manager you need to configure Anyware Manager to use the defined secret store. Please be aware that you can only configure one secret storage option with Anyware Manager.

The sections below outline the prerequisite steps required to prepare these secret stores:

- Preparing Azure Key Vault
- Preparing Hashicorp Vault

You can't configure the secret storage application to work with Anyware Manager until you have successfully installed Anyware Manager. Please complete the installation and then perform the required configurations.

Preparing an External Database

The following section provides guidelines and best practices involved when preparing and deploying a production MongoDB solution with Anyware Manager.

Reference Instructions for MongoDB and Vault Configuration

For detailed deployment instructions on installing and configuring MongoDB and Vault in a single virtual machine to be used by Anyware Manager, see the following Knowledge Base article. This article outlines in detail how to install and configure an instance of MongoDB and an instance of Vault on the same virtual machine. This KB article should be used in conjunction with the installation steps outlined in this section.

Reference Steps Only

All configuration steps outlined should be used as a reference only. For specific details, visit the vendor's official documentation and knowledge base. For information on the main reference list for MongoDB, see https://docs.mongodb.com/manual/administration/.

GUIDELINES AND BEST PRACTICES

The following are some of the guidelines and best practices that We encourage when deploying a MongoDB to work with Anyware Manager:

- Ensure the machine is deployed in a secure subnet with no public facing access.
- Ensure that the host firewalls are leveraged to control inbound and outbound traffic.
- MongoDB only needs to be accessible to the Anyware Manager and to administrators so it is better to be overly restrictive when granting access, and follow the rules of granting least privilege access.
- Anyware Manager cannot connect to an external MongoDB from behind a proxy.
- Remote desktop or SSH access to the system should be disallowed altogether if possible - realistically this is highly unlikely - or heavily restricted to essential users only, with a security-conscious configuration (e.g. add certificates for RDP, use passphrase-protected SSH keys and disallow password based authentication, change default SSH port, etc).
- Keep the host OS patched and up to date to ensure security fixes are deployed.
- It is best to use the latest stable version of MongoDB to ensure there are as few vulnerabilities, bugs, and issues as possible.
- It is best to maintain a regular update cadence for both MongoDB and the host machine in order to maintain latest security fixes.
- It is best to run MongoDB on a Long Term Support variant of Linux (ex, RHEL x86_64 or Ubuntu x86_64) VM.

- In order to maintain data integrity, it is best to run Mongo with Journaling enabled (enabled by default) in a geographically distributed replica set.
- Regular backups are also important to ensure Anyware Manager can be restored in case of a crash. To keep MongoDB secure, it is important to create the appropriate admin accounts for granting access and ensuring that all communication is done over a secured TLS connect. Details for creating an appropriate service account can be found in the official MongoDB documentaton, as well as:
    - Details for enabling data encryption at rest.
    - How to enable TLS on the MongoDB server.
    - Additional tips for hardening the system.

Installing Anyware Manager

The following section outlines how to install Anyware Manager with the default database and secret storage. These steps should be performed on the target machine by connecting via SSH or console.

⚠ Before you begin

Follow the prerequisite steps in the Anyware Manager System Requirements section to prepare your target machine. It is important to read and address all the prerequisites outlined. Once you have completed these steps and prepared the target machine, return to this page and continue with the installation.

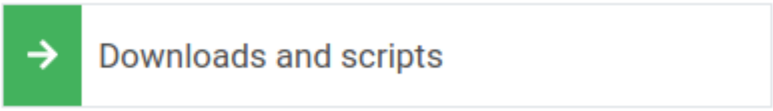
1. Add Anyware Manager Repository

The virtual machine you are adding the repo to must have access to the internet to be able to download and install the required files.

Anyware Manager Repositories

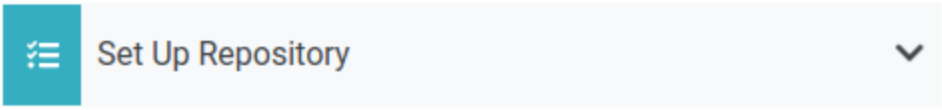
The new repository `teradici-anyware-manager` is introduced. If you currently have `teradici-cas-manager` repository, you must remove it. See Repository Management to remove them. Once the unwanted repos are removed, you can proceed with the installation process below.

To access the scripts and to configure and add the RHEL and Rocky Linux repository, select the **Downloads and scripts** option from the
Anyware Manager support site.



If you see a login button instead, click it to log into the site and then proceed.

Accept the End User License Agreement, then click **Set Up Repository**.



The window expands and displays the setup scripts for each supported operating system. Copy the command for your system to the clipboard.

Paste command on the target machine where you wish to install Anyware Manager and press `Enter`.

The command fetches a configuration script from our servers and runs it locally, setting up and configuring the repository on the local machine.

Run the following command to confirm `teradici-anyware-manager` repos were added into dnf repo.

```
dnf repolist --enabled teradici-anyware-manager*
```

The output from this command should list the repo id, names as outlined in the example below:

```
repo id                                                    repo name
teradici-anyware-manager-beta                              teradici-anyware-manager-
beta
teradici-anyware-manager-beta-noarch                       teradici-anyware-manager-
beta-noarch
teradici-anyware-manager-beta-source                       teradici-anyware-manager-
beta-source
```

2. SELinux Configuration

SELinux policies are required for persistent storage and container logging on Anyware Manager. If SELinux policies are not found, data stored in Anyware Manager is lost when the Anyware Manager Machine is shut down.

Once configured, and the installation has verified SELinux, all Anyware Manager related data persists when the target machine hosting Anyware Manager is re-booted. To check if SELinux is already installed on your system, run the following command:

```
sudo dnf list installed | grep anyware-manager-selinux
```

The output from this command notifies if you if `selinux` is already running on your system. If it is not then you need to run the following commands to install the SELinux policies:

Run the following command to install the SELinux policies and set the basic framework for persistent database and Vault:

Run the following command to install a specific version of SELinux that has been tested for K3s:

Run the following command to install SELinux from the Anyware Manager repo:

Install Command Alias

The older command `sudo dnf install -y cas-manager` works as an alias for Anyware Manager installation.

3. Install Anyware Manager

Installation Commands Updated

Anyware Manager installation requires two commands comparing to previous version where only one command is required. If you have automated the installation in scripting, make sure the script is updated accordingly.

Run the following command to install Anyware Manager RPM:

```
sudo dnf install -y anyware-manager
```

The installer installs Anyware Manager, as well as all external components required.

These external components are:

- k3s
- MongoDB (data store)
- Vault (secret store from HashiCorp)
- A self-signed SSL certificate for HTTPS access

Run the following command to install Anyware Manager with the appropriate flags suits your needs, see "Installation Flags and Options" for all supported flags. The command example below installs Anyware Manager with self-signed certificate from teradici-anyware-manager* repo added in the pervious steps. Debug level log is displayed to help troubleshooting.:

```
sudo /usr/local/bin/anyware-manager install --accept-policies --self-signed --
debug
```

PASSWORD CONFIGURATION

You need to configure a password to install Anyware Manager instance on your system. The password adds a layer of protection to the system and is required when accessing the Web Admin Console. To meet the security standards, the password should be 8 characters in length with minimum 1 uppercase, 1 lowercase, 1 number and 1 special character.

Password Special Character

The `%` character and whitespaces are not supported.

Anyware manager installer requires Web Admin password and prompts for it, if this behavior is not preferred the password could be passed to the install command using:

```
--manager-admin-password
```

In case you forget the password, you can reset it using the following flag with the `configure` command:

```
--reset-admin-password
```

⚠ Password File

The `/opt/teradici/casm/temp-creds.txt` file that has the ability to store Anyware Manager password is not created any more by the installer. If you forget your password, you need to reset it using the `--reset-admin-password` flag.

INSTALLATION FLAGS AND OPTIONS

For detailed information on the installation flags and the configuration file parameters that you can pass during installation, see the table outlined below:

Flags	Example	Description
`--accept-policies`	sudo /usr/local/bin/anyware-manager install --accept-policies	If this flag is set, the installer does not prompt for accepting policies. This flag is optional
`--clear`	sudo /usr/local/bin/anyware-manager install --clear	This flag Removes data and files of an existing or previous Anyware Manager instance.
`--manifest`	sudo /usr/local/bin/anyware-manager install --manifest	This flag is set to provide a path for manifest files. This flag is optional.
`--self-signed`	sudo /usr/local/bin/anyware-manager install --self-signed	This flag is set to Automatically generate self-signed TLS cert and key. Setting this flag ignores `--tls-key` and `--tls-cert` flags.
`--tls-key`	sudo /usr/local/bin/anyware-manager install --tls-key	If this flag is set, it requires the full path and filename of the TLS key to use with the Anyware Manager.
`--tls-cert`	sudo /usr/local/bin/anyware-manager install --tls-cert	If this flag is set,it requires the full path and filename of the TLS certificate to use Anyware Manager.
`--registry`	sudo /usr/local/bin/anyware-manager install --registry	This flag is used to specify the container registry from which the Anyware Manager pulls container images.
`--registry-username`	sudo /usr/local/bin/anyware-manager install --registry-username	This flag is used to authenticate Anyware Manager username to the registery and to pull container images.
`--registry-password`	sudo /usr/local/bin/anyware-manager install --registry-password	This flag is used to authenticate Anyware Manager password to the registry to pull container images.
`--manager-admin-password`	sudo /usr/local/bin/anyware-manager install --manager-admin-password	This flag is used to create a new password for Anyware Manager during installation.
`--reset-admin-password`	sudo /usr/local/bin/anyware-manager configure --reset-admin-password	This flag is used to reset the password for Anyware Manager.

```
sudo dnf install -y anyware-manager-selinux
sudo dnf install -y https://github.com/k3s-io/k3s-selinux/releases/download/
v1.1.stable.1/k3s-selinux-1.1-1.el8.noarch.rpm
```

```
sudo dnf install -y selinux-policy-base container-selinux
```

The external components are:

- k3s
- A self-signed SSL certificate for HTTPS access

The installation process takes 5-10 minutes to complete, depending on your network connection speed and other environment variables. During this process, Anyware Manager is running a health check every 15 seconds to confirm that all required services are deployed and running successfully before reporting that the installation is complete.

Once the installation has been successful you should see a message stating **Anyware Manager installation complete**. The IP address and the version of your Anyware Manager instance isdisplayed.

If the installation appears unhealthy, you should generate a support bundle and send this to HP for investigation. For more information on generating a support bundle, see Support Bundle. For more information on monitoring and assessing the health status of Anyware Manager, see Health Status.

Generated Self-Signed Certificates

The installer automatically generates several certificates to ensure that internal communication within the Anyware Manager and communication to the Anyware Manager itself are done over encrypted TLS connections. These certificates are automatically generated as needed when Anyware Manager is initially installed or when upgrades are done. If you do not wish to upgrade, certificates must be periodically renewed, see TLS Certificates for steps on how to do this.

4. Configure Anyware Manager to use Proxy

The following section outlines the steps involved in enabling the proxy configuration with Anyware Manager:

1. If the proxy environment variables were not set before installing Anyware Manager, please see the Proxy Configuration Variables section above for the steps involved in setting these variables. If you already have these variables set, continue to step 2.

2. Establish a new ssh/shell session.
3. Configure Anyware Manager to use the proxy configuration by running the following command:

```
sudo /usr/local/bin/anyware-manager configure --enable-proxy
```

5. Configure Anyware Manager to use a Secret Storage Application

Once you have successfully installed Anyware Manager you must configure it to use the secret store you prepared in the prerequisite steps prior to installing Anyware Manager. You need to have prepared the selected secret storage application before installing Anyware Manager, as outlined in the Preparing a Secret Storage Application section above. For information on how to configure Anyware Manager to work with these secret stores, see the following sections based on what type of secret storage you prepared:

- Configuring Anyware Manager with Azure Key Vault
- Configuring Anyware Manager with Hashicorp Vault

6. Configure Anyware Manager to use MongoDB

Once you have successfully installed Anyware Manager you must configure it to use the external MongoDB you prepared in the prerequisite steps prior to installing Anyware Manager.

The following section outlines how to configure Anyware Manager to use MongoDB:

1. SSH to your target machine where you installed Anyware Manager.
2. Create a file that contains the following data:

```
{
"db-connection-string": "mongodb://<username>:<password>@<address>/
<db_name>",
"db-enable-tls": true,
"db-skip-verify-cert": false
}
```

⚠ URL Encoding

If the username or password contain any of the following special characters: **/**, **?**, **#**, **[]**, **@**, **%**, those characters must be converted using URL encoding in the MongoDB connection string. For example, if you defined user 'awmuser' with password 'Password%' in MongoDB, then in Anyware Manager the `db-connection-string` for MongoDB would look like this:

```
mongodb://awmuser:Password%25@ip_of_mongodb:27017/name_of_mongodb
```

If you require more characters to be encoded, or want to test encoding or decoding your data, see https://www.urlencoder.org/.

3. Replace the following place holders with your own values:
   - username: Username of the MongoDB user that Anyware Manager authenticates MongoDB requests.
   - password: Password for the MongoDB user referenced in "username".
   - address: Address to the MongoDB server.
   - db_name: Name of the MongoDB database that Anyware Manager can use. Note that if no db name is specified, the db named "test" is used.
4. Run the following command to configure Anyware Manager to use MongoDB:

```
sudo /usr/local/bin/anyware-manager configure --config-file path-to-your-config-file
```

⚠ MongoDB Database Name

If no database name is provided as part of the connection string, a default name "test" is used instead, for example:

db-connection-string:"mongodb://user:pass@mongo:27017/ results in the creation of a database with the name "test".

If you provide a database name, for example:

db-connection-string:"mongodb://user:pass@mongo:27017/awm_db. Then the name "awm_db" is used as the database name.

After running this command, Anyware Manager validates the configuration by attempting to query the MongoDB server. If the request is successful, then Anyware Manager is configured to use this MongoDB. The configure command should only take a few minutes to complete.

Here's an example of creating a user for the Anyware Manager Database "awm_db":

```
use awm_db
db.createUser(
  {
    user: "anyware",
    pwd: passwordPrompt(), // or cleartext password
    roles: [ {db: "awm_db", role:"readWrite"} ], // user only needs readWrite
Access to awm DB,
    authenticationRestrictions: [
        {
          clientSource: [
            "<AWM-IP>", // IP address of the AWM Host
            "10.42.0.0/24" // Subnet for the AWM pods
          ],
          serverAddress: ["<MongoDB IP>"] // IP for the MongoDB server
        }
     ],
  }
)
```

The connection string for this user would be:

```
mongodb://anyware-manager:<password>@<MongoDB IP>/awm_db
```

Configuration Templates

HP provides configuration template files and parameters that can be generated and used when configuring your MongoDB, see Configuration Templates.

6.1 CONNECTING A MONGODB WITH SELF-SIGNED TLS CERTIFICATES

Anyware Manager allows for the option to provide a database connection string, a flag to enable/disable TLS, a flag to enabled/disable TLS cert validation, and also provide a custom Certificate Authority certificate for the MongoDB Server certificate. This is only recommended during proof-of-concept testing. In this mode, TLS must be enabled and certificate validation must be carried out. A server certificate signed by a public Certificate Authority is also highly recommended.

⚠ **Tested on CentOS Only**

The following steps have been tested on CentOS. These steps may not work, or work differently, on different systems.

The following steps outline how to connect a MongoDB that uses self-signed TLS certificates:

1. SSH to your target machine where you installed Anyware Manager.
2. Create a file that contains the following data:

```
{
    "db-connection-string": "mongodb://<username>:<password>@<address>/
<db_name>",
    "db-enable-tls": true,
    "db-ca-cert-file": "/path/to/mongo/TLS/custom/certificate/authority",
    "db-skip-verify-cert": false
}
```

3. Replace the following place holders with your own values:
   - "db-connection-string": Follow the same guidelines as mentioned above.
   - "db-ca-cert-file": Path to MongoDB's custom Certificate Authority's public certificate, in PEM format, if one is used. This is only required to validate self-signed certificates or certificates signed by a non-public Certificate Authority.
4. Run the following command to configure Anyware Manager to use MongoDB:

```
sudo /usr/local/bin/anyware-manager configure --config-file path-to-your-
config-file
```

1. If you want to skip certificate verification, include `"db-skip-verify-cert": true` in your configuration file. Please note that this is not secure and is not recommended for production use cases:

```
{
    "db-connection-string": "mongodb://<username>:<password>@<address>/
<db_name>",
    "db-enable-tls": true,
    "db-ca-cert-file": "/path/to/mongo/TLS/custom/certificate/authority",
    "db-skip-verify-cert": true
}
```

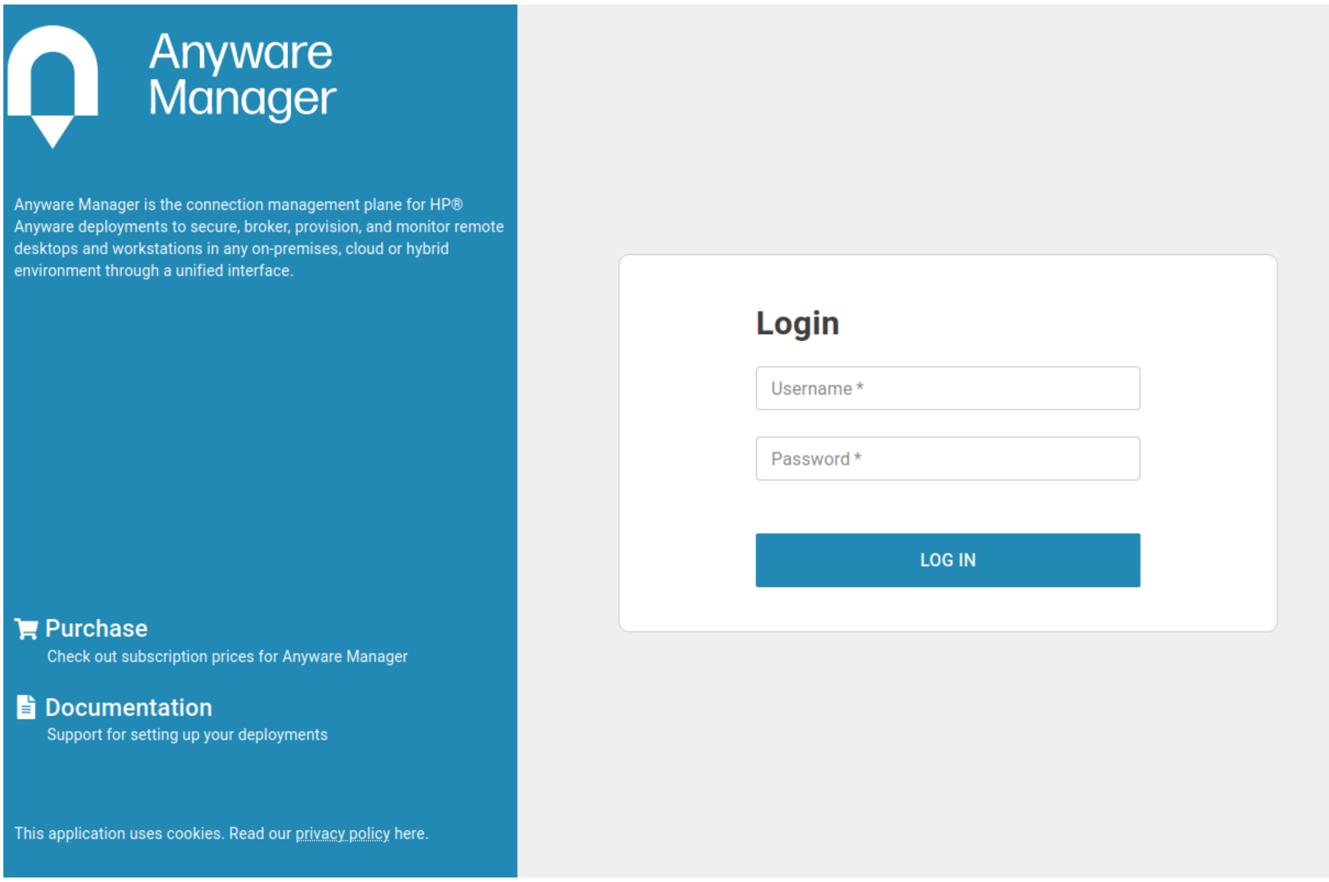
7. Accessing the Admin Console

The following section outlines how to access and unlock the Anyware Manager Admin Console.

1. Open a web browser and go to https://{ip-address-or-dns-name-of-anyware-manager}. This is the IP address of the target machine where Anyware Manager is installed.
2. When presented with the Anyware Manager Login page, use the following credentials to begin using Anyware Manager:

   username: adminUser

   password: The password that is configured during Anyware Manager installation.

   Anyware Manager is the connection management plane for HP® Anyware deployments to secure, broker, provision, and monitor remote desktops and workstations in any on-premises, cloud or hybrid environment through a unified interface.

   Anyware Manager
Purchase
Check out subscription prices for Anyware Manager
Documentation
Support for setting up your deployments
This application uses cookies. Read our privacy policy here.
Login
Username *
Password *
LOG IN

3. Click **Login**.

You are now able to use Anyware Manager as the **adminUser** user.

To unlock the Admin Console enter your Anyware Software registration code into the Unlock dialog that appears when you first log-in. Anyware Manager verifies the registration code and then create a new deployment on your behalf. For further information on using the Admin Console, see Admin Console.

8. Anyware Manager dnf Repo Management

By default, Anyware Manager installs any updates that are available, when you update all managed packages with the following command:

```
dnf upgrade anyware-manager
```

or

```
dnf update anyware-manager
```

This system wide update includes any new Anyware Manager version updates. If you do not want this system wide update, the Anyware Manager repo(s) should be disabled once installation is complete.

LOCKING ANYWARE MANAGER VERSION IN THE DNF REPO

The following section outlines how to lock the Anyware Manager in the dnf repo:

1. Run this command: `sudo dnf config-manager --set-disabled teradici-anyware-manager*`.
2. To confim the settings, run this command: `dnf repolist teradici-anyware-manager*`.

The output from this command should list the repo id, names and their status, as outlined in the example below:

```
repo id                                         repo
name                                       status
teradici-anyware-manager                            teradici-anyware-
manager                            disabled
teradici-anyware-manager-noarch                     teradici-anyware-manager-
noarch                     disabled
teradici-anyware-manager-source                     teradici-anyware-manager-
source                     disabled
```

Installing the Connector

Once you have installed the Anyware Manager you can install Connector(s) by following the instructions outlined in the Installing the Connector section.

Installing Anyware Manager - Darksite Installation

In cases where Anyware Manager needs to be installed in a **darksite** (ie, an environment where there is no internet access, also known as **airgap** or **offline** environment) you must download the darksite dependency files, transfer them to the target darksite machine, and then run the darksite installation script.

Legacy Scripts and Tarball Files

Before you install a new darksite version of Anyware Manager, you must remove all legacy Anyware Manager scripts and tarball files.

RHEL/Rocky Linux OS version

For Anyware Manager Darksite installation, the minimum RHEL/Rocky Linux operating system version is 8.7.

Before you begin

Follow the prerequisite steps in the Anyware Manager System Requirements section to prepare your target machine. It is important to read and address all the prerequisites outlined. Once you have completed these steps and prepared the target machine, return to this page and continue with the installation.

Download and Transfer Dependencies

Once you have addressed all the prerequisite steps, you need to download and transfer the dependencies files.

The combined dependencies takes up 2.2 GB approximately. You must ensure you have a media device that can transfer all required components to the target darksite virtual machine; these components can be removed from the target virtual machine once installation is complete. The required packages and dependencies to complete a darksite installation are:

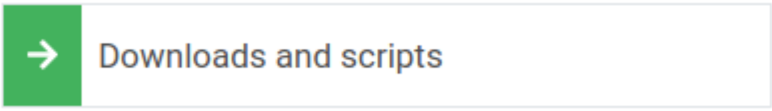
- Darksite installation bash script: A bash script that will set up and install required components as well as the Anyware Manager.
- RedHat Package Manager (RPM) dependencies: A yum repo that contains all RPM dependencies required to install Anyware Manager. Only the dependencies that are missing will be installed but this package contains all system requirements.
- Anyware Manager container images: A `.tar.gz` file containing all Anyware Manager container images required for running the Anyware Manager to be loaded onto the system.

All of the packages and dependencies are bundled in a tar archive file.

1. Downloading the File

Once you have access to a virtual machine with internet access follow the steps below:

1. To download the Anyware Manager installation package, select the **Downloads and scripts** option from the Anyware Manager support site.

   If you see a login button instead, click it to log into the site and then proceed.
2. Read and accept the HP End User License Agreement.
3. To download the darksite package, click **Download linux** Under **Darksite packages**.

2. Transferring the File

Once you have downloaded the `.tar.gz` file, transfer it to the target darksite machine.

To transfer the file you can copy it onto a media device, such as a USB drive or a DVD, and then connect that device to the target darksit machine. You can also connect the target darksite machine to another machine via SSH or FTP, and complete a network file transfer. This method may not be viable for some darksite networks.

3. Extracting the File

Run the following command to extract the downloaded `.tar.gz` file on the target darksite machine:

```
sudo tar xzvf anyware-manager-offline_Linux.tar.gz
```

That creates a new folder called `anyware-manager-offline_VERSION_linux`.

Change drive on the command prompt into the new folder. You can see two files, one is the dependency tarball file and the other is the install bash script file.

4. Install Anyware Manager Darksite

Checking and Removing Anyware Manager Repository Files

Anyware Manager Darksite doesn't need to download images from online repository, this usually works as expected on a clean VM without additional step here. However, if there is repository set by the flags or repository file, the installer will try to download from what the target is set to. To avoid this you must make sure the relevant repository files are removed from the VM.

- To check if the repository present in the system, run `sudo ls -la /etc/yum.repos.d`
- If you have any repository name that start from *teradici-anyware-manager*, you need to remove them by running `sudo rm /etc/yum.repos.d/NAME_OF_THE_REPO`.

Run the following command for the installation:

```
sudo ./install.sh
```

Enter Admin Password

After executing this command, please enter the admin password for Anyware Manager When prompted.

This installs the Anyware Manager and all the other dependencies.

The command above replaces steps 1-3 in either the External Configuration or Default Configuration installation steps. Please follow the steps after this with the configuration you want to use.

⚠ **Installation Errors**

The Darksite installation could fails due to a package conflicting or checksum error if there is an existing package already present on the target machine. To resolve this, you need to delete the conflicting package and re-run the installation script.

5. Upgrading Anyware Manager to version 23.01 and later (Optional)

If you have Anyware Manager 22.09 installed then upgrading to Anyware Manager 23.01 and later, requires you to perform a series of additional steps. They are as follows:

1. Perform all actions in step 1 to step 4 mentioned above.

   Installation Warning Message

   After performing step 4, the system displayed a warning message that says *An instance of Anyware Manager is installed or previous data is still on disk, if you would like to upgrade you need to run the upgrade command instead, but if you would like to remove and install a new instance you will need to pass `--clear` to the install command.*

2. To complete the installation process, run the `anyware-manager upgrade` command.

The upgrade and install is now successful.

Upgrading Anyware Manager (Online Upgrade)

When upgrading Anyware Manager there are two options available.

1. **In-place upgrade within the maintenance window:** You can run an in-place upgrade through dnf for Anyware Manager. Depending on the configuration you implemented, this will mean a period of downtime which can range from a few seconds to a few minutes.
2. **Zero downtime upgrade via a new VM**. The second option involves installing Anyware Manager on a new virtual machine, and configuring it to connect to the same external database and secret storage. If done correctly this can result in zero downtime.

The steps involved in both options are outlined below.

Which Option Should I Choose?

The upgrade option you choose depends on the amount of downtime you are willing to experience and how your Anyware Manager instance has been deployed and setup. The following are some use cases that outline which option to use:

- If you have a single Anyware Manager server connecting to external database and secret storage, it is recommended to install Anyware Manager on a new virtual machine. If you don't have a new virtual machine then run the in-place upgrade on the existing virtual machine with the understanding that there will be some downtime during this upgrade.
- If you have multiple Anyware Manager servers connecting to the same external database and secret storage, it is recommended to run an in-place upgrade on each Anyware Manager server, one at a time. There should not be any downtime as long as one Anyware Manager server is up and running.
- If the database and secret storage is on the same virtual machine as Anyware Manager, you must run an in-place upgrade. This is to ensure that the data persists after the upgrade has been completed. There will be some downtime during this upgrade.

Running an In-Place Upgrade

Anyware Manager Downtime

The Anyware Manager virtual machine that is undergoing an in-place upgrade will not be available during the upgrade. This can take anywhere from a few seconds to a few minutes, depending on the number of services that need to be upgraded and the speed of download when retrieving new versions from the repo. If this is the only Anyware Manager server you have, the new connections will not be established until the upgrade is completed successfully.

Anyware Manager Repositories

The new repository `teradici-anyware-manager` is introduced. If you currently have `teradici-cas-manager` repository, you must remove it. See [Repository Management]() to remove them. Once the unwanted repos are removed, you can proceed with the update process.

1. Add Anyware Manager dnf Repository

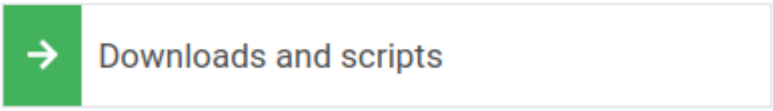
1. SSH to the Anyware Manager virtual machine.
2. Remove the existing dnf repo for previous CAS Manager with the following command.

   ```
   sudo rm /etc/yum.repos.d/teradici-anyware-manager.repo
   ```

3. Check that the repos are removed

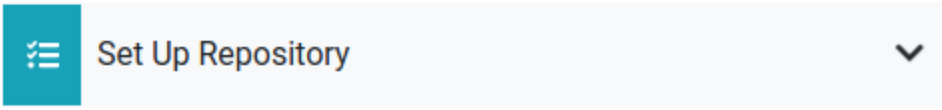
   ```
   dnf repolist --enabled teradici-anyware-manager*
   ```

4. To access the scripts and to configure and add the RHEL and Rocky Linux repository, select the **Downloads and scripts** option from the [Anyware Manager support site]().

   If you see a login button instead, click it to log into the site and then proceed.

5. Accept the End User License Agreement, then click **Set Up Repository**.



6. The window expands and displays the setup scripts for each supported operating system. Copy the command for your system to the clipboard.
7. Paste command on the target machine where you wish to install Anyware Manager and press `Enter`.

The command fetches a configuration script from our servers and runs it locally, setting up and configuring the repository on the local machine.

Run the following command to confirm `teradici-anyware-manager` repos were added into dnf repo.

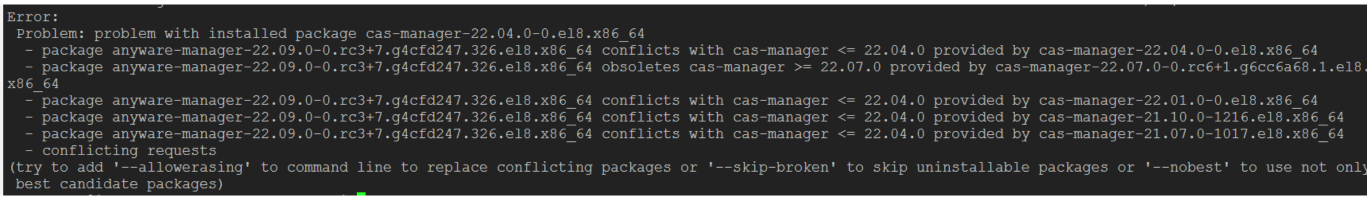
```
dnf repolist --enabled teradici-anyware-manager*
```

The output from this command should list the repo id, names as outlined in the example below:

```
repo id                                                   repo name
teradici-anyware-manager-beta                                 teradici-anyware-
manager-beta
teradici-anyware-manager-beta-noarch                          teradici-anyware-
manager-beta-noarch
teradici-anyware-manager-beta-source                          teradici-anyware-
manager-beta-source
```

2. Upgrade Anyware Manager via dnf

To upgrade CAS Manager 22.04 or prior to Anyware Manager, transitional steps are required so that Anyware Manager can recognize CAS Manager as the predecessor instead of thinking Anyware Manager is in conflict. Otherwise, you would see an error message as shown below:



```
Error:
 Problem: problem with installed package cas-manager-22.04.0-0.el8.x86_64
  - package anyware-manager-22.09.0-0.rc3+7.g4cfd247.326.el8.x86_64 conflicts with cas-manager <= 22.04.0 provided by cas-manager-22.04.0-0.el8.x86_64
  - package anyware-manager-22.09.0-0.rc3+7.g4cfd247.326.el8.x86_64 obsoletes cas-manager >= 22.07.0 provided by cas-manager-22.07.0-0.rc6+1.g6cc6a68.1.el8.
x86_64
  - package anyware-manager-22.09.0-0.rc3+7.g4cfd247.326.el8.x86_64 conflicts with cas-manager <= 22.04.0 provided by cas-manager-22.01.0-0.el8.x86_64
  - package anyware-manager-22.09.0-0.rc3+7.g4cfd247.326.el8.x86_64 conflicts with cas-manager <= 22.04.0 provided by cas-manager-21.10.0-1216.el8.x86_64
  - package anyware-manager-22.09.0-0.rc3+7.g4cfd247.326.el8.x86_64 conflicts with cas-manager <= 22.04.0 provided by cas-manager-21.07.0-1017.el8.x86_64
  - conflicting requests
(try to add '--allowerasing' to command line to replace conflicting packages or '--skip-broken' to skip uninstallable packages or '--nobest' to use not only
 best candidate packages)
```

Please follow the steps below to upgrade from CAS Manager 22.04 or prior versions:

1. Upgrade CAS Manager 22.04 RPM or prior to CAS Manager 22.07.0 RPM, which is the transitional version, by running the following command:

   ```
   sudo dnf install cas-manager-22.07.0
   ```

2. Install latest version of Anyware Manager RPM by running the following command:

   ```
   sudo dnf install anyware-manager
   ```

3. Upgrade to Anyware Manager by running the following command:

   ```
   sudo /usr/local/bin/anyware-manager upgrade
   ```

If you want to use a different manifest than the default one, please add `--manifest` and the path to your manifest.

For EX: `sudo /usr/local/bin/anyware-manager upgrade --manifest path-to-manifest.tar.gz`

Installing Anyware Manager on a new Virtual Machine

The following steps outline how to install Anyware Manager on a new virtual machine, and configure it to connect to the same external database and secret storage application:

1. Before performing an upgrade you should backup the database and secret storage application you used when installing Anyware Manager. If you intend to install Anyware Manager on a new virtual machine, backup the configuration file so that it can be used on the Anyware Manager instance.
2. Follow the installation steps outlined here to install a new instance of Anyware Manager in a new virtual machine to replace the existing one. You must configure it to be identical to the old Anyware Manager instance. It needs to connect to the same MongoDB, and secret storage application, as well as having the same certificate and network configurations.
3. Change your DNS to point to the new Anyware Manager instance.

4. Reconfigure your Connector to connect to the new Anyware Manager if necessary:
    - If you installed your Connector with `--manager-url=https://Fully-Qualified-Domain-Name-of-Anyware-manager`:
        - Change your DNS entry for the FQDN to point to the new Anyware Manager's static IP.
        - In the Connector virtual machine, flush the DNS cache to use the latest DNS. This ensures that there will be zero downtime as the Connector will be able to connect to the new Anyware Manager instance:

          ```
          sudo systemd-resolve --flush-caches
          ```

    - If you installed your Connector with `--manager-url=https://ip-address-of-anyware-manager`:
        - Update your Connector to use the latest Anyware Manager's IP address.
        - Log into the Connector virtual machine and run the following command to update the Anyware Manager IP:

          ```
          sudo usr/sbin/cloud-access-connector update --manager-url https://
          <New Anyware-Manager IP>
          ```

5. In the Connector, ping the FQDN to verify it can find the new Anyware Manager instance.
6. Remove the old Anyware Manager virtual machine.

Removing the Anyware Manager Virtual Machine

The following steps outline how to remove the Anyware Manager virtual machine:

1. Save the configuration setting files used in the current version of Anyware Manager. For example, save them as a *all-configurations.json* file. If the current Anyware Manager has proxy configured, save all the proxy environment variables also.
2. Run the following commands to remove the Anyware Manager.

   ```
   sudo dnf remove -y anyware-manager-selinux anyware-manager
   sudo rm -rf /opt/teradici/casm     # Remove the cas-manager files
   ```

3. Delete the Anyware Manager VM.

Upgrading Anyware Manager (Darksite Upgrade)

In cases where Anyware Manager needs to be updated in a **darksite** (ie, an environment where there is no internet access, also known as **airgap** or **offline** environment) you will need to download the darksite dependency files, transfer them to the target darksite machine, and then run the darksite installation script.

✎ **Legacy Scripts and Tarball Files**

Before you upgrade to a new darksite version of Anyware Manager, you must remove all legacy Anyware Manager scripts and tarball files.

✎ **RHEL/Rocky Linux OS version**

For Anyware Manager Darksite installation, the minimum RHEL/Rocky Linux operating system version is 8.5.

⚠ **Before you begin**

Follow the prerequisite steps in the Anyware Manager System Requirements section to prepare your target machine. It is important to read and address all the prerequisites outlined. Once you have completed these steps and prepared the target machine, return to this page and continue with the installation.

Download and Transfer Dependencies

Once you have addressed all the prerequisite steps, you need to download and transfer the dependencies files.

The combined dependencies takes up 2.2 GB approximately. You must ensure you have a media device that can transfer all required components to the target darksite virtual machine; these components can be removed from the target virtual machine once installation is complete. The required packages and dependencies to complete a darksite installation are:

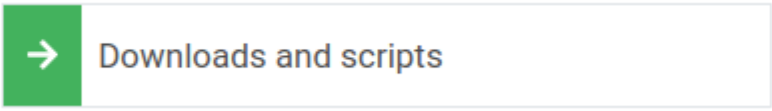
- Darksite installation bash script: A bash script that will set up and install required components as well as the Anyware Manager.
- RedHat Package Manager (RPM) dependencies: A yum repo that contains all RPM dependencies required to install Anyware Manager. Only the dependencies that are missing will be installed but this package contains all system requirements.
- Anyware Manager container images: A `.tar.gz` file containing all Anyware Manager container images required for running the Anyware Manager to be loaded onto the system.

All of the packages and dependencies are bundled in a tar archive file.

1. Downloading the File

Once you have access to a virtual machine with internet access follow the steps below:

1. To download the Anyware Manager installation package, select the **Downloads and scripts** option from the Anyware Manager support site.

   If you see a login button instead, click it to log into the site and then proceed.
2. Read and accept the HP End User License Agreement.
3. To download the darksite package, click **Download linux** Under **Darksite packages**.

2. Transferring the File

Once you have downloaded the `.tar.gz` file, transfer it to the target darksite machine.

To transfer the file you can copy it onto a media device, such as a USB drive or a DVD, and then connect that device to the target darksit machine. You can also connect the target darksite machine to another machine via SSH or FTP, and complete a network file transfer. This method may not be viable for some darksite networks.

3. Extracting the File

Once the .tar.gz file has been transferred to the target darksite machine, extract the downloaded file by running the following command:

```
sudo tar xzvf anyware-manager-offline_Linux.tar.gz
```

That creates a new folder called `anyware-manager-offline_VERSION_linux`.

Change drive on the command prompt into the new folder. You can see two files, one is the dependency tarball file and the other is the install bash script file.

4. Upgrade using Anyware Manager Darksite

4.1 UPGRADE FROM CAS MANAGER TO ANYWARE MANAGER

> **Updating from CAS Manager to Anyware Manager**
>
> This step is only required when updating from an older CAS Manager version to a new Anyware Manager version. You can skip this step if it does not match your use case.

1. Unpack the `anyware-manager-offline-deps.tar.gz` by running the following command in order to run the transitional commands:

```
sudo tar zxvf anyware-manager-offline-deps.tar.gz
```

1. Run the installation of the transition CAS Manager in the following order:

```
sudo dnf install -y --disablerepo=* anyware-manager/cas-manager-k3s.rpm
sudo dnf install -y --disablerepo=* anyware-manager/cas-manager-selinux.rpm
sudo dnf install -y --disablerepo=* anyware-manager/cas-manager.rpm
```

4.2 INSTALL ANYWARE MANAGER DARKSITE

Checking and Removing Anyware Manager Repository Files

Anyware Manager Darksite doesn't need to download images from online repository, this usually works as expected on a clean VM without additional step here. However, if there is repository set by the flags or repository file, the installer will try to download from what the target is set to. To avoid this you must make sure the relevant repository files are removed from the VM.

- To check if the repository present in the system, run `sudo ls -la /etc/yum.repos.d`
- If you have any repository name that start from `_teradici-anyware-manager_`, you need to remove them by running `sudo rm /etc/yum.repos.d/NAME_OF_THE_REPO`.

Run the following command for the installation:

```
sudo ./install.sh
```

Enter Admin Password

After executing this command, please enter the admin password for Anyware Manager When prompted.

This sets up the Anyware Manager and all the other dependencies.

Run the following command to update Anyware Manager:

```
sudo /usr/local/bin/anyware-manager upgrade
```

The command above replaces steps 1-3 in either the External Configuration or Default Configuration installation steps. Please follow the steps after this with the configuration you want to use.

Customizing Anyware Manager

Configuration Template Files and Parameters

The following section outlines the configuration template files and parameters available with Anyware Manager.

Configuration Template Files

To generate template files that can be used to fill in various Anyware Manager configurations, do the following:

1. SSH to your machine where you installed Anyware Manager.
2. Run one of the following commands listed in the code block below to generate configuration template files:

```
# Generate the following config templates: mongo-template.json
sudo /usr/local/bin/anyware-manager generate --mongo

# Generate the following config templates: tls-template.json
sudo /usr/local/bin/anyware-manager generate --tls

# Generate the following config templates: vault-template.json
sudo /usr/local/bin/anyware-manager generate --vault

# Generate the following config templates: all-templates.json, mongo-template.json, tls-template.json, vault-template.json
sudo /usr/local/bin/anyware-manager generate --all-templates
```

Configuration Parameters

The following table contains all of the parameters that can be used in a configuration file to configure Anyware Manager.

Parameter	Type	Description	Required
vault-type	string	Specifies the type of secret store that Anyware Manager should use. Currently, "vault" is the only supported value for this parameter.	Required for updating Vault configuration.
vault-url	string	URL of the Vault server.	Required for updating Vault configuration.
vault-secret-path	string	Vault secret path where secrets are stored.	Required for updating Vault configuration.
vault-token	string	Token used to authenticate requests to the Vault server.	Required for updating Vault configuration.
vault-ca-cert-file	string	Path to the file containing a PEM-formatted CA certificate that is used to validate the Vault server's certificate.	Required if the Vault server is using self-signed certificates.
vault-skip-verify-cert	boolean	If true, Anyware Manager does not validate the Vault server's TLS certificate. This is not secure and is not recommended for production deployments.	Not required. Defaults to "false".
db-connection-string	string	URL of the MongoDB server.	Required for updating MongoDB configuration.
db-enable-tls	boolean	If false, requests to MongoDB are not encrypted. Setting this parameter to false is not secure and is not recommended for production deployments.	Not required. Defaults to "true".
db-skip-verify-cert	boolean	If true, Anyware Manager does not validate the MongoDB server's TLS certificate. This is not secure and is not recommended for production deployments.	Not required. Defaults to "false".
db-ca-cert-file	string	Path to the file containing a PEM-formatted CA certificate that is used to validate the MongoDB server's certificate.	Required if the MongoDB server is using self-signed certificates.

Parameter	Type	Description	Required
tls-key-file	string	Path to the file containing a PEM-formatted TLS key that is used by Anyware Manager.	Required for updating TLS certificates used by Anyware Manager.
tls-cert-file	string	Path to the file containing PEM-formatted TLS certificate that is used by Anyware Manager.	Required for updating TLS certificates used by Anyware Manager.
skip-validate-reg-code	boolean	If true, skip validating PCoIP registration code when creating or updating a deployment.	Not required unless Anyware Manager is blocking all internet traffic. Defaults to "false".

Configuring Custom TLS Certificates

By default, Anyware Manager is deployed using self-signed TLS certificates. We recommend using a custom TLS certificate for using Anyware Manager in production. You should renew and maintain these certificates as required. Anyware Manager supports X509 certificates in PEM format, the certificate file must only include a single certificate, the CA bundle is not supported. The TLS key must not require Password.

To configure Anyware Manager to use custom TLS certificates, or to update Anyware Manager to use a new TLS certificate, follow the steps outlined below:

1. Create a file called *tls-config.json* with the following contents:

```
{
  "tls-key-file": "<path to a file containing your TLS certificate key>",
  "tls-cert-file": "<path to a file containing your TLS certificate>"
}
```

2. Update the TLS configuration by running the following command:

```
sudo /usr/local/bin/anyware-manager configure --config-file tls-config.json
```

   This command updates the Anyware Manager services automatically.

Internal TLS Certificates

When you are using internal MongoDB and Vault for data storage, in order to keep Anyware Manager's internal communication secure, the installer also generates a set of self-signed TLS certificates to be used for encrypting internal communication within Anyware Manager. By default these certificates expire 2 years from when they are generated.

In order to ensure that the Anyware Manager uptime is not interrupted unexpectedly it is important to ensure that these certificates do not expire. This can be done by:

- Upgrading Anyware Manager regularly. These certificates are regenerated by the installer during the upgrade process if they are close to expiring so upgrading at a regular cadence (eg, once or twice a year) ensures everything remains operational.

- If you do not want to upgrade Anyware Manager and only want to use a version that you have qualified yourself, and that may exceed the TLS certificates expiration time, you can either:
    - Periodically re-deploy the Anyware Manager instance you are running so that new certificates are generated regularly.
    - Run the command to re-generate certificates periodically. See Internal Certificate Generation below for steps on how to do this.
- Monitor when the certificates are going to expire and plan to regenerate them beforehand. You can do this by either running the Anyware Manager diagnose command or checking the Anyware Manager health probe's logs. Run the following command to generate this health check:

```
/usr/local/bin/anyware-manager diagnose --health
```

This health check assesses the Mongo Database and Vault connections. A warning message is logged if the certificates are close to expiring and an error is logged if they have expired. For example,

```
...
INFO .. Connections:
INFO .... MongoDB=Healthy
WARN ...... Mongo Certificate Valid From=2021-08-17 19:35:42 Mongo
Certificate Valid Until=2021-09-18 19:35:42
INFO .... vault=Healthy
WARN ...... Vault Certificate Valid From=2021-08-17 19:35:42 Vault
Certificate Valid Until=2021-09-18 19:35:42
...
```

In order to check the logs for the Anyware Manager health probe, run

```
/usr/local/bin/kubectl get jobs -o jsonpath='{.items[?
(@.spec.template.metadata.labels.name=="manager-health-
probe")].metadata.name}' --sort-by=.metadata.creationTimestamp | rev | cut -
d' ' -f 1 | rev | xargs -I % /usr/local/bin/kubectl logs jobs/%
```

This command returns the last completed Anyware Manager health probe's logs and states when the certificates are expiring. For example:

```
Secret Provider type is Vault
Vault certificate is valid from Tue Aug 17 19:35:42 2021 until Sat Sep 18
19:35:42 2021
Vault status - Initialized: True, Sealed: False
Vault is healthy
MongoDB certificate is valid from Tue Aug 17 19:35:42 2021 until Sat Sep 18
19:35:42 2021
MongoDB is healthy
Manager is healthy
```

These commands show the expiration date for the Mongo Database and Vault in both the default MongoDB/Vault mode or external MongoDB/Vault mode. For external MongoDB/Vault modes, you need to manually change the certificates yourself on the external instances since Anyware Manager does not have the necessary permissions or functionality to do that for you.

Internal Certificate Generation

In the case where the certificate has expired or is about to expire, and you do not wish to upgrade your Anyware Manager instance, you can generate internal certificates by running the following command:

```
/usr/local/bin/anyware-manager configure --generate-certs
```

Once you have run this command, check the output of the diagnostics health command or the Anyware Manager health probe as shown in point 3 above. Please note that this only updates the certificates within Anyware Manager, so if you are using an external MongoDB and/or external Vault with TLS enabled, this command does not affect the external Database or Vault's certificates.

Configuring Timezone

The following section outlines steps to configure the timezone in Anyware Manager.

1. Run the following commands on your workstation where you have Anyware Manager installed.

   ```
   sudo timedatectl set-ntp on
   timedatectl status
   ```

   After you execute the command above, the command line displays the following message:

   ```
   Local time: Wed 2023-01-11 16:39:43 KST
   Universal time: Wed 2023-01-11 07:39:43 UTC
   RTC time: Wed 2023-01-11 07:39:43
   Time zone: Asia/Seoul (KST, +0900)
   System clock synchronized:
   ```

2. If you wish to manually configure the desired timezone, run the following command:

   ```
   sudo timedatectl set-timezone Asia/Seoul
   ```

   Run the following command:

   ```
   $ timedatectl status
   ```

   After you execute the command above, the command line displays the following message:

   ```
   Local time: Wed 2023-01-11 13:06:16 IST
   Universal time: Wed 2023-01-11 07:36:16 UTC
   RTC time: Wed 2023-01-11 07:36:16
   Time zone: Asia/Kolkata (IST, +0530)
   System clock synchronized:
   ```

3. After `System clock synchronized:`, say `yes` and press enter.

   The command line displays:

   ```
   NTP service: active
   RTC in local TZ: no
   ```

Network Time Protocol

Ensure that Network Time Protocol (NTP) is set as 'active' so that the system time doesn't change to UTC by default.

The desired timezone is now configured.

Multi-Admin Support

Multi-Admin Support

Once Anyware Manager is installed, a local **adminUser** user is created to manage Anyware Manager. Optionally, Active Directory or SAML integration can be configured to support additional admin users. If you don't configure either of these integrations, **adminUser** is the only admin user.

Active Directory Integration

The Active Directory used to enable multi-admin in Anyware Manager does not need to be the same Actve Directory that was used by the Connector to manage the users for the remote workstation.

The Active Directory Domain Controller machine must be accessible from the target machine that Anyware Manager is installed on over the LDAPS port (TCP 636). Typically, this is only the case if both machines are on the same LAN.

To enable multiple users to manage Anyware Manager, an Active Directory LDAPS configuration must be added in the Active Directory as outlined here.

⚠ **Anyware Manager Integration**

The following steps are applicable for configuring an Active Directory with Anyware Manager only. They are not applicable to integrating with Anyware Manager as a Service.

⚠ **Active Directory Configuration Permissions**

Only the **adminUser** has the permissions to configure the Active Directory with Anyware Manager from the Anyware Manager Admin Console.

DNS and Name Resolution

You must ensure that you can resolve your AD domain and controller. For information on how to install and edit resolve.conf, and configure DNS name resolution, see Configuring DNS Name Resolution.

The following steps outline how to configure Active Directory integration in the Anyware Manager Admin Console:

1. Go to the Anyware Manager Admin Console and log-in using your Anyware Manager admin credentials.
2. Click on **adminUser** from the user account tab and then click on **Multi-Admin Settings**.
3. Click on the **Active Directory Configuration** tab.
4. Enter the Active Directory configuration information:
   - Domain Controller URL: This is the URL where your domain controller is hosted, for example ldaps://dc.example.com. You can also use the Fully qualified domain name (FQDN) of the Domain Controller if you do not know the LDAP address.
   - Admin Connection DN: This is the distinguished name (DN) of a user within your AD that is able to search for users. Microsoft AD supports using UPN format for logging in. For example cn=manager_admin,cn=Users,dc=example,dc=com or manager_admin@example.com.
   - Admin Password: This is the password for the admin user defined by "Admin connection DN".
   - Manager group DN: This is the DN of a group in your AD. Only users that belong to this group is able to authenticate to Anyware Manager. For example, cn=Manager Admins,cn=Users,dc=example,dc=com.
   - Search Base DN: This is the DN of the container in your AD where you search for user's to authenticate. For example, cn=Users,dc=example,dc=com
5. Click **SAVE** to save the configuration.

User's from the Active Directory belonging to the Manager group is able to navigate to the Anyware Manager Admin Console login page and authenticate using their Active Directory credentials.

SAML Integration

If the Active Directory Domain Controller cannot be accessed, you can alternatively enable Active Directory users to login by enabling the Admin Console's SAML integration.

The following steps outline how to enable SAML integration and configuration of IDP settings, admins and groups access and general configuration information:

1. Go to the Admin Console.
2. Log-in using your Anyware Manager admin credentials.
3. After logging into the Admin Console click on **adminUser** from the user account tab and then click on **Multi Admin settings** to open the preferences page.
4. Click on the **SAML** tab.
5. Enter the SAML configuration information:
    - The first section contains auto-generated information about the login URLs and IDP:
        - **Anyware Manager login page**: A link to the page for multi-administrator login to the Admin Console
        - **Direct login via identity provider**: An endpoint to which multi-admin sign-in requests can be sent
        - **Assertion Consumer Service URL**: The callback URL provided to the IDP to which user information is sent once the IDP has authorized the user
        - **Audience URL**: The entity ID that the IDP can use to identify the Admin Console
    - The second section contains IDP settings that can be updated to manage the SAML configuration within the Anyware Manager:
        - **Identity Provider Login URL**: The IDP endpoint to which SAML authentication requests are sent
        - **Identity Provider Certificate**: The public certificate of the IDP used to verify the signature of the IDP. You can also upload a .xml file that contains your IDP information.
    - The third section enables you to add new admins as well as displaying all existing admins that are allowed to login via an IDP. To enable the access for a single user, visit the **Allowed admins** tab, enter their e-mail, and click the **Add Admin** button.
    - The fourth section enables you to add new groups as well as displaying all existing groups that are allowed to login via an IDP. To enable the access for a group of users, visit the **Allowed groups** tab, enter the claim type and group claim and click **Add Group**. The claim type informs Anyware Manager how the group is returned in the SAML assertion by your IDP. The group claim matches against the group either in the Group Name claim or in the Group ID claim returned in the SAML assertion for a user based on the claim type defined for the group.

   A user's access via SAML can be enabled or disabled on either the **Allowed admins** or **Allowed groups** tabs.

Configuring the Active Directory for Anyware Manager

Anyware Manager uses Lightweight Directory Access Protocol (LDAP) or Secure Lightweight Directory Access Protocol (LDAPS) with Active Directory servers for user authentication. LDAPS is recommended to give you a more secure environment, through the use of an Active Directory Certificate, which should be available before activating the Active Directory configuration.

The following section details how to configure and add an existing Active Directory with Anyware Manager. You must have an existing Active Directory to use with Anyware Manager.

Test LDAPS

The first step is to test LDAPS. For information on adding a self-signed certificate to enable LDAPs, see How to create and install a self-signed certificate on a Windows 2016 Active Directory server to enable LDAPS in our Knowledge Base.

The following command outlines how to test LDAPS through PowerShell as an Admin. Enter the name of your domain controller in place of `dc1.example.com`:

```
openssl s_client -connect "dc1.example.com":636
```

If you see a certificate successfully returned, then LDAPS for the Active Directory is configured and functioning.

Configure Active Directory for Anyware Manager

The following steps outline how to configure the Active Directory for Anyware Manager:

1. Open the system Control Panel and select **Administrative Tools**.
2. Click **Active Directory Users and Computers** from the list of options. If you don't have an Active Directory installed, then this option does not appear.
3. Create the following groups and users within the *Users* folder:

   New Group: **TESTGROUP** New User: **testUser**

   The group and user names used above are just examples and can be replaced with any names you choose.

4. Once you have created this new group and user you need to access the Anyware Manager Admin Console and configure the Active Directory. For information on how to do this, see Multi-Admin Support.

If you are using the Anyware Manager as a simple broker without power management, the Active Directory user you select must have read permission to query the Active Directory. A simple Domain Users group should suffice. If you are using the Anyware Manager with power management features enabled, please see the following section of the Anyware Manager Administrator's guide, here.

AWS Configuration

The following page outlines how to enable AWS features through the AWS management console on Anyware Manager. The first step is to create a policy that can be attached to a service account. This service account allows Anyware Manager to manage resources within the provided AWS account.

Roles and Permissions for AWS

Prior to creating and assigning a permissions policy, you need to ensure that it contains the following permissions:

- **Service**: EC2
- **Actions**:
  - List: DescribeInstances
  - Write: RebootInstances StartInstances StopInstances TerminateInstances

There are additional permissions needed to verify that the policy has all the required permissions before being added to a deployment:

- **Service**: IAM
- **Actions**:
  - List: ListAttachedUserPolicies ListUserPolicies
  - Read: GetUser GetUserPolicy GetPolicy GetPolicyVersion SimulatePrincipalPolicy

If the user tries to add an AWS policy that doesn't have these permissions, Anyware Manager adds the policy but does not validate that it has the required permissions.

Please note the permissions required for AWS configuration with Anyware Manager as a Service are different to the permissions required for Anyware Manager. See AWS Permissions Policies for Anyware Manager as a Service for information on these permissions. Currently, the permissions required for Azure and GCP configuration are the same between Anyware Manager and Anyware Manager as a Service.

Create a Anyware Manager Policy in AWS

The following steps outline how to create the required AWS policy that you can attach to a AWS User to manage AWS resources:

1. Go to the IAM Management page in the AWS management console.
2. From the sidebar, click **Policies**.
3. Click **Create policy**.
4. For **Service** click **EC2** from the list of services.
5. Under **Access level** expand the **List** section and select **DescribeInstances**.
6. Under **Access level** expand the **Write** section and select the following permissions:
    - **RebootInstances**
    - **StartInstances**
    - **StopInstances**
    - **TerminateInstances**
7. For **Service** click **IAM** from the list of services.
8. Under **Access level** expand the **Read** section and select the following permissions:
    - **GetUser**
    - **SimulatePrincipalPolicy**
9. For **Resources** click **All resources**.
10. Leave **Request conditions** blank and click **Review policy**.
11. Give the newly created policy a name and click **Create policy**.

Create Anyware Manager Service Account for AWS

This service account has the ability to perform required actions in AWS. This lets the service account manage resources that the user has access to.

The following steps outline how to create the CAM service account:

1. Go to the IAM Management page in the AWS management console.
2. From the sidebar, click **Users**.
3. Click **Add user**.

4. Give the user a name and select **Programmatic access** as the Access type.
5. Click **Next: Permissions**.
6. Click **Attach existing policies directly** and search for the policy you created above that has EC2 permissions and select it. Optionally, you can add a tag to this role.
7. Click **Next:Review**.
8. Click **Create user**
9. Copy the **User name**, **Access key ID** and **Secret access key** credentials and save them to a secure location.

Add the AWS Service Account to a Anyware Manager Deployment

The next step requires you to add the AWS service account you have created from the previous steps in the AWS management console to Anyware Manager. This service account will have the CAM policy created in the previous step.

The following steps outline how to add the information to Anyware Manager:

1. Log in to Anyware Manager.
2. Select the Anyware Manager deployment ou want to add the AWS service account to.
3. Click **Edit Deployment**.
4. Click the **Cloud service accounts** tab and open the AWS container.
5. Enter the **User name**, **Access key ID** and **Secret access key** values that you saved previously in the AWS form.
6. Click **Submit**.

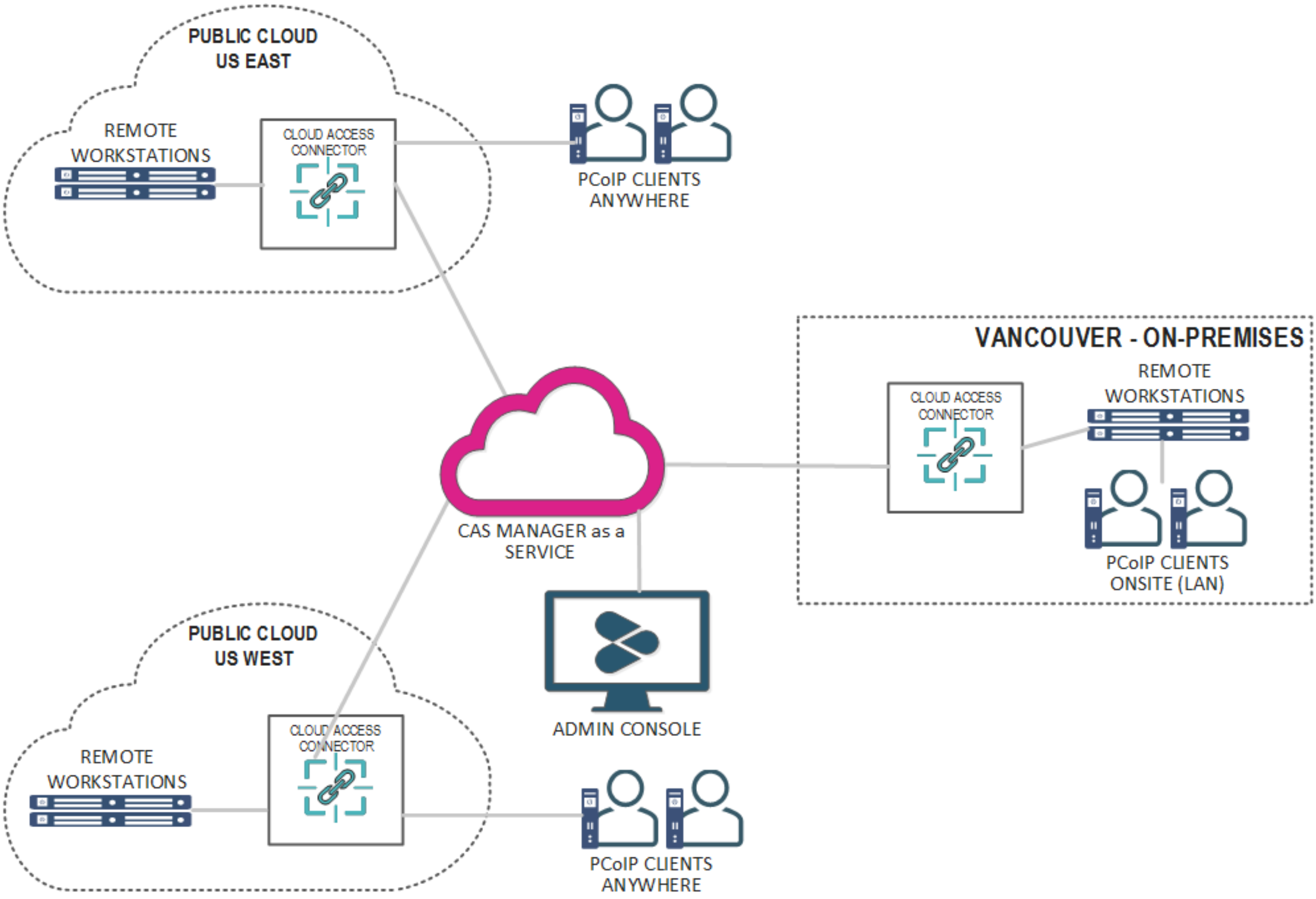
Anyware Manager should be able to manage AWS machines that get added to this deployment.

Admin Console

Overview

The Admin Console enables you to create deployments, connectors and remote workstations all within a single console and from a single interface (UI). You can track all these components from the interface of the console, as well as monitor and manage all aspects of your deployment infrastructure. You can access support, release notes and get service status information from the Admin Console also. The Admin Console works with both Anyware Manager, and Anyware Manager as a Service.

The diagram below outlines a connection workflow for a cloud deployment using the Admin Console with Anyware Manager as a Service.



Connecting to the Admin Console

The following section outlines how to access and connect to the Admin Console for Anyware Manager and Anyware Manager as a Service.

Connecting to Anyware Manager

Once you have unlocked the Admin Console, open a web browser and go to https://public-or-private-ip-address-of-cas-manager to login with the default "adminUser". If you have configured multi-admin support, login with your enterprise identity provider account that has the required admin permission for Anyware Manager.

Connecting to Anyware Manager as a Service

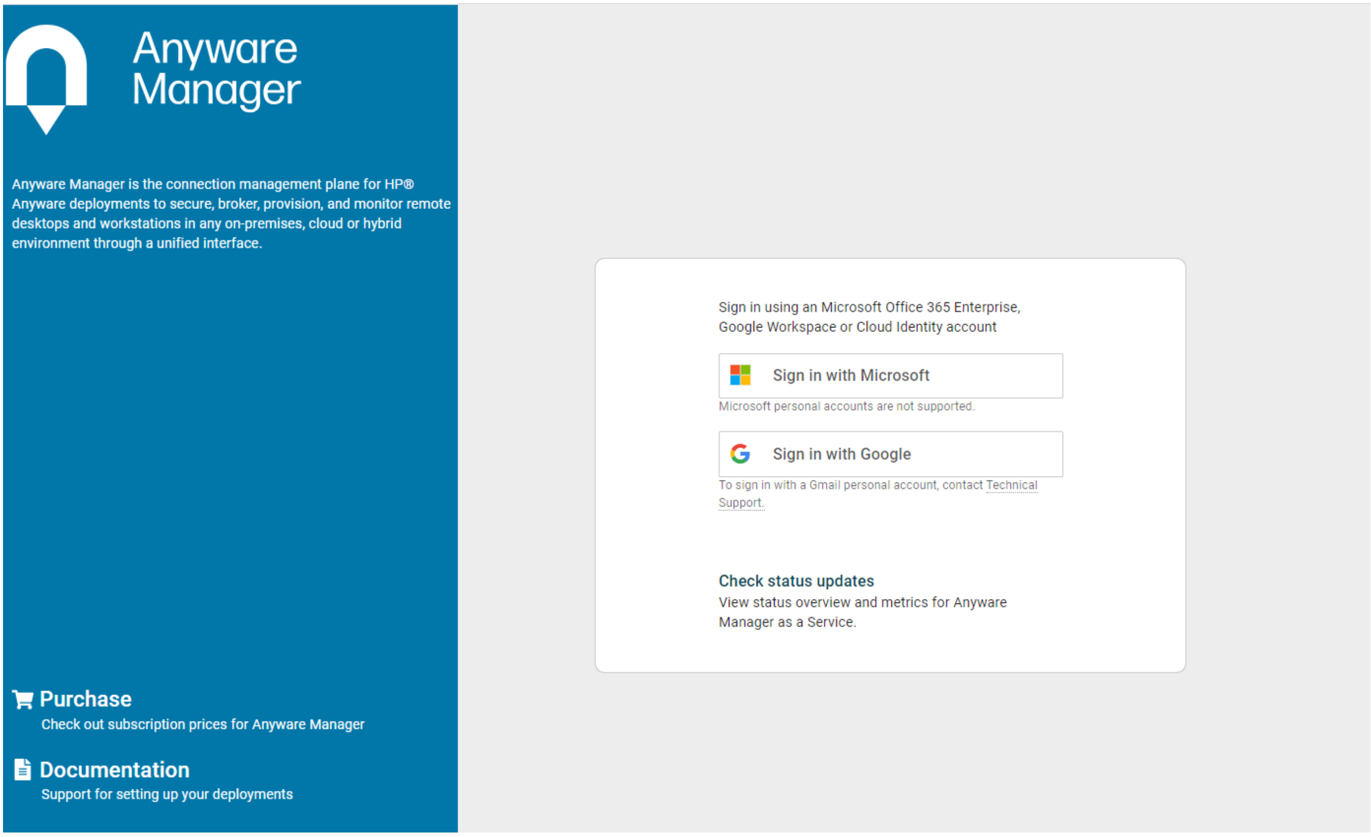
Go to the Admin Console login page and log in with your Enterprise Microsoft Azure account, or if you are logging in through Google, a G Suite or Cloud Identity account. Enter your credentials to access the Admin Console.

Email Account Support with Anyware Manager

Anyware Manager supports two types of email accounts:

- Company email accounts registered with Google G Suite.
- Company email accounts registered with Microsoft Azure Active Directory services. For more information on this account type, see Microsoft Azure Active Directory Authentication.

Personal Gmail accounts are not supported by default and need to be approved by HP before being used. For access to Anyware Manager with a personal Gmail account, contact HP support. Anyware Manager as a Service does not support Microsoft personal email accounts.



Anyware Manager is the connection management plane for HP® Anyware deployments to secure, broker, provision, and monitor remote desktops and workstations in any on-premises, cloud or hybrid environment through a unified interface.

Sign in using an Microsoft Office 365 Enterprise, Google Workspace or Cloud Identity account

Microsoft personal accounts are not supported.

To sign in with a Gmail personal account, contact Technical Support.

Check status updates

View status overview and metrics for Anyware Manager as a Service.

Purchase

Check out subscription prices for Anyware Manager

Documentation

Support for setting up your deployments

If you encounter issues logging into the Admin Console, it could be for one of the following reasons:

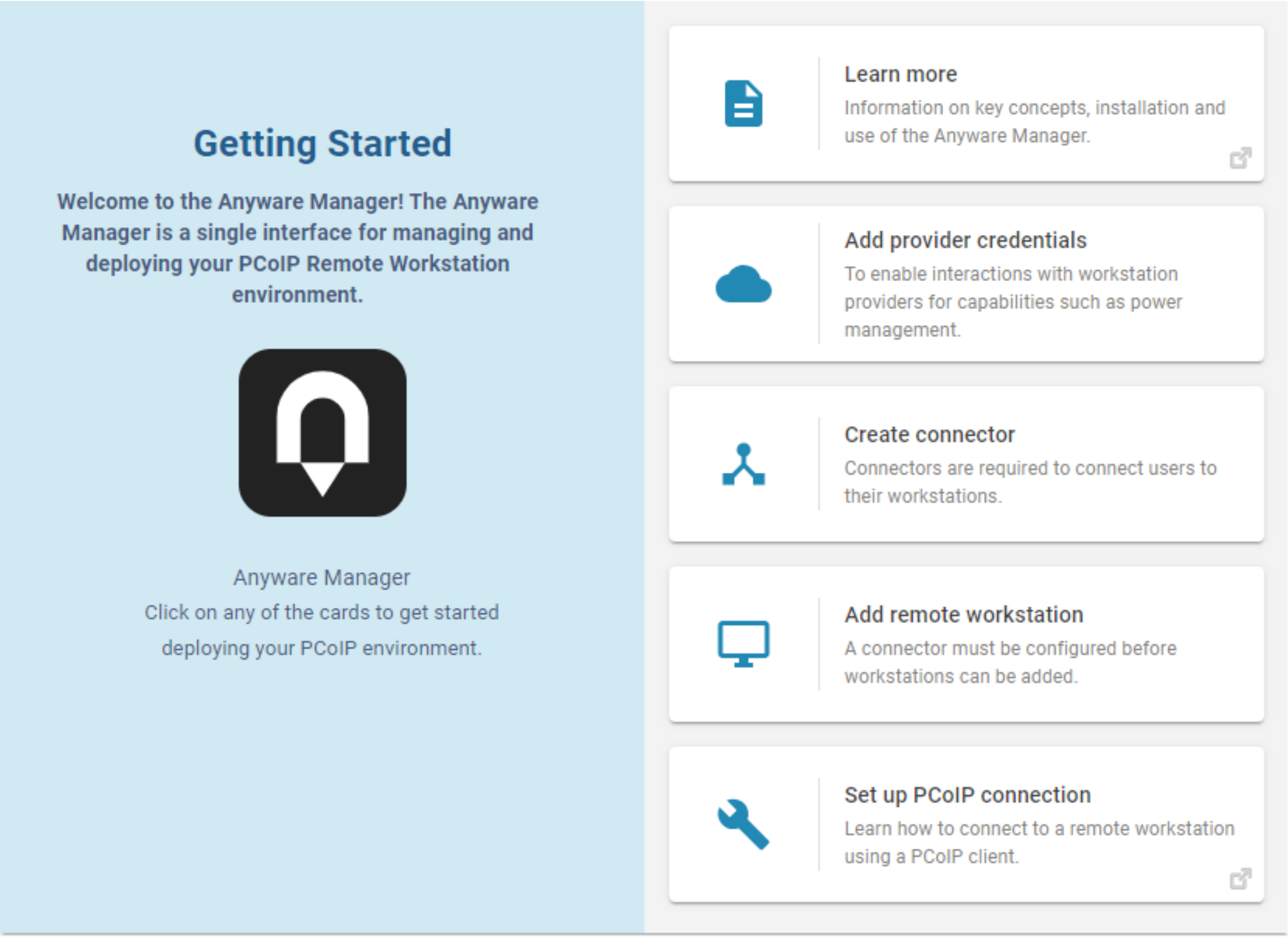
- The account being used is a personal account and has not been approved by HP.
- Cookies have been blocked on https://cam.teradici.com/.
- Pop-ups have been blocked on https://cam.teradici.com/.

If you continue to experience issues logging into the Admin Console, contact HP Support.

Admin Console Dashboard

Once you log into the Admin Console you should see the dashboard page. This dashboard acts as a quick-start guide which points to where you can create deployments, create Connectors, add remote workstations as well as provide links to useful information within the Anyware Manager documentation.

You can return to the dashboard page at any time by clicking the **Dashboard** option from the console sidebar.



Getting Started

Welcome to the Anyware Manager! The Anyware Manager is a single interface for managing and deploying your PCoIP Remote Workstation environment.

Anyware Manager
Click on any of the cards to get started deploying your PCoIP environment.

Learn more
Information on key concepts, installation and use of the Anyware Manager.

Add provider credentials
To enable interactions with workstation providers for capabilities such as power management.

Create connector
Connectors are required to connect users to their workstations.

Add remote workstation
A connector must be configured before workstations can be added.

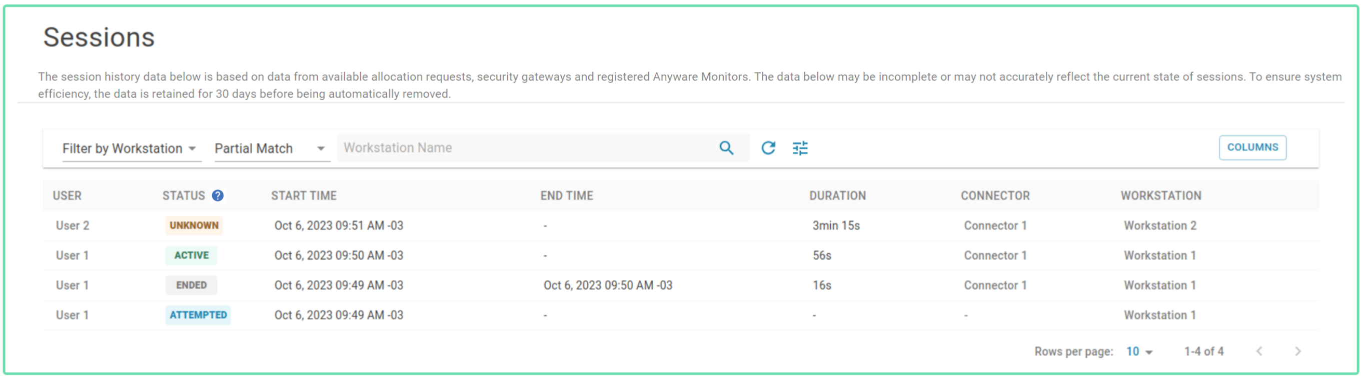
Set up PCoIP connection
Learn how to connect to a remote workstation using a PCoIP client.

Configuring the Admin Console

On the **Deployments**, **Connectors** and **Remote Workstations** pages you can control which columns are visible and in which order they appear for the listed resources. To change your column options, select **COLUMNS** from the page heading and select which columns you wish to make visible. The format you select is preserved when you log back into the Admin Console.

Sessions History

The Session History feature provides the ability to view both past and currently active sessions. This table provides valuable information about session establishment, including entity names and IDs associated with the session (such as users, workstations, and connectors), session status, and various time metrics (start time, end time, duration, etc).



Sessions

The session history data below is based on data from available allocation requests, security gateways and registered Anyware Monitors. The data below may be incomplete or may not accurately reflect the current state of sessions. To ensure system efficiency, the data is retained for 30 days before being automatically removed.

USER	STATUS	START TIME	END TIME	DURATION	CONNECTOR	WORKSTATION
User 2	UNKNOWN	Oct 6, 2023 09:51 AM -03	-	3min 15s	Connector 1	Workstation 2
User 1	ACTIVE	Oct 6, 2023 09:50 AM -03	-	56s	Connector 1	Workstation 1
User 1	ENDED	Oct 6, 2023 09:49 AM -03	Oct 6, 2023 09:50 AM -03	16s	Connector 1	Workstation 1
User 1	ATTEMPTED	Oct 6, 2023 09:49 AM -03	-	-	-	Workstation 1

Data Source and Data Retention

The session history data presented in the table is collected from the connector, monitor and security gateway. Each session is represented as a single row, which presents an accumulation of all of the data about a session from the sources reporting on it. Please note that this data may be incomplete and may not accurately reflect the real-time state of sessions. To ensure system efficiency, the data is retained for 30 days before being automatically removed.

The following table provides more details about the current data sources, including which sessions a source impacts, the source's update frequency, and the source's possible affect on session state:

Data Source	Applies To	Update Interval	Effect (States Changed)
Anyware Manager	All sessions initiated through a connector	Single time per session	ATTEMPTED
Security Gateway	All sessions being brockered by a security gateway if Session Tracking is enabled in connector settings	5 minutes	ACTIVE ENDED
Anyware Monitor	All sessions in workstations that have Anyware Monitor installed	When session state changes occur, otherwise every 5 minutes	ACTIVE ENDED
Manager Session Cleaning Service	Sessions that left ATTEMPTED state and stopped receiving updates from other sources	1 min	UNKNOWN ENDED

Note

Anyware Monitor and PCoIP Agent versions 23.12 and higher are required to receive session state updates from the Monitor.

Explanation of Table Columns:

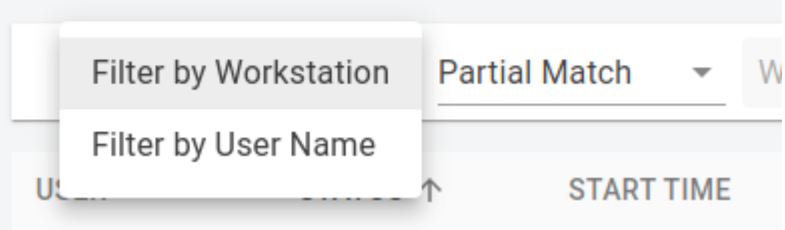
- **Data Source**: The source of data that contributes to the session history.
- **Applies To**: Which sessions the data source applies to.
- **Update Interval**: The frequency at which the data source is updated or polled.
- **Effect (States Changed)**: The session states that can be changed or updated by each data source.

Session Status

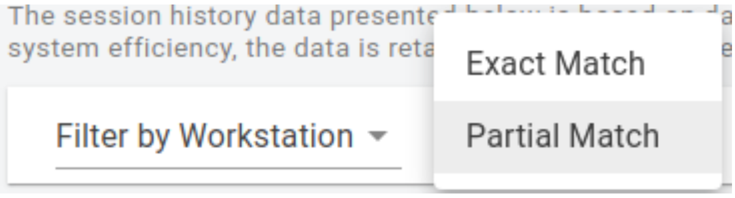
Attempted: Indicates that the session establishment was initiated
Active: The session is currently active
Unknown: Indicates that the session has stopped receiving updates
Ended: The session has ended

Filtering

Similar to other tables in the Admin Console, you can use the input field to filter the session history based on specific criteria. On the session history page, you have the option to filter by workstation or username.



Furthermore, you can choose to apply exact or partial matching filters.



The session history data presente

system efficiency, the data is reta

✎ **Note**

Partial matches may take longer to process.

Columns Description

The following table provides a description of the available columns in the session history table:

Name	Description	Data Type	Visible by Default	Sortable
Session ID	Unique identifier of the session	String	No	No
User	User responsible for establishing the session	String (with link)	Yes	No
User Guid	Globally Unique Identifier (GUID) of the user	String	No	No
Detected Users	Logged in desktop users detected by the operating system at any point during the session	String	No	No
Status	Current status of the session	Icon representing the session status (Refer to the note below for possible session statuses)	Yes	No
Start Time	Date and time when the session started	Date	Yes	Yes
Last Update Time	Date and time of the last collected telemetry	Date	No	No
End Time	Date and time when the session ended	Date	Yes	No
Duration	Total duration of the session	String	Yes	No
Connector	Connector used to establish the connection (if one was used at all)	String (with link)	Yes	No
Connector ID	Identifier of the connector used for the connection	String (with link)	No	No
Workstation	Name of the workstation used for the session	String (with link)	Yes	No
Machine ID	Identifier of the workstation used for the session	String	No	No

GUID

GUID (or UUID) stands for "Globally Unique Identifier" (or "Universally Unique Identifier"). It is a 128-bit integer number used to uniquely identify resources.

Session States Lifecycle

This section provides an overview of the lifecycle of session states and describes the associated time metrics during state transitions.

ATTEMPTED

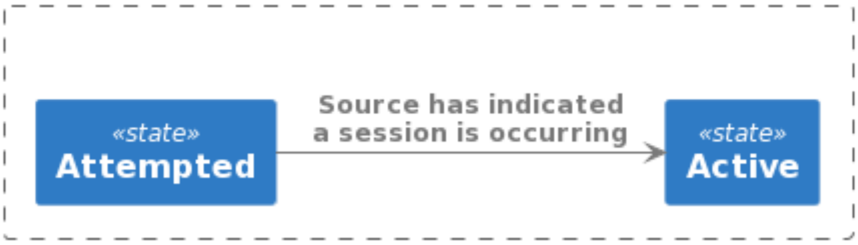
Sessions may start in the attempted state. In this state, the session has the following time metrics:

- Start Time
- Last Updated Time (same as the start time)
- Session End (empty)
- Duration (empty)

ATTEMPTED TO ACTIVE

During this transition, the session exhibits the following time metrics:

- Last Updated Time reflects the most recent update
- Session Duration reflects the most recent update
- Session End (empty)

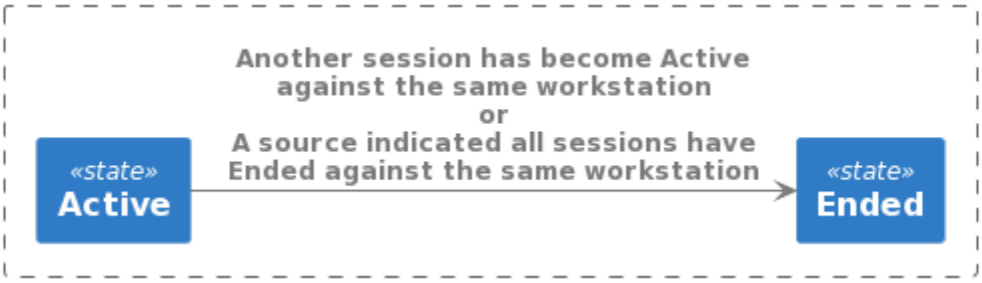


ACTIVE TO ENDED

When the session transitions from Active to Ended, the time metrics are as follows:

- Last Updated Time reflects the most recent update time

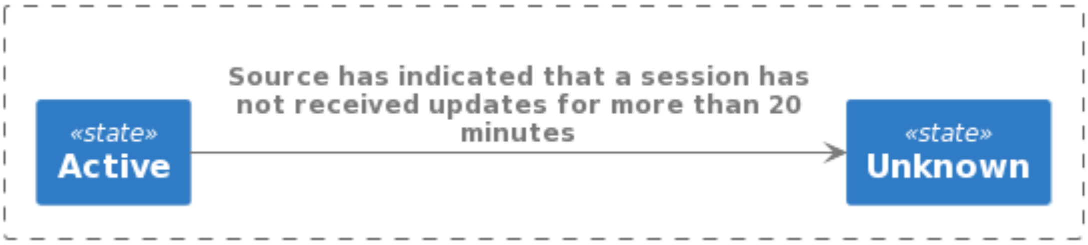
- Session End (populated)
- Duration reflects the most recent update


«state»
Active
Another session has become Active against the same workstation
or
A source indicated all sessions have Ended against the same workstation
«state»
Ended

ACTIVE TO UNKNOWN

When a session is without updates for 20 minutes, the time metrics are as follows

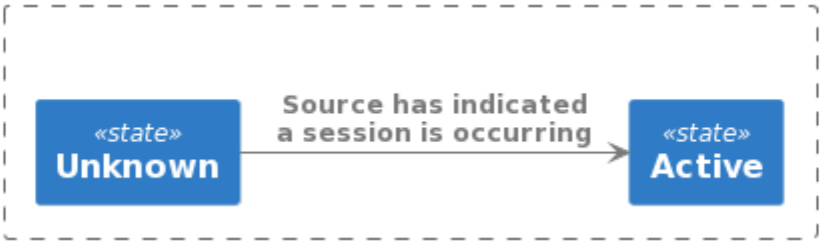
- Last Updated Time reflects the most recent update and indicates the "staleness" of information
- Duration reflects the most recent update
- Session End (empty)


«state»
Active
Source has indicated that a session has not received updates for more than 20 minutes
«state»
Unknown

UNKNOWN TO ACTIVE

During the transition from unknown to Active, the time metrics are as follows:

- Last Updated Time reflects the most recent update
- Duration reflects the most recent update
- Session End (empty)



UNKNOWN TO ENDED

This transition occurs based on three different source behaviors:

1. When 24 hours have passed since the start of the last session
2. When another session becomes Active against the same workstation, indicating previous sessions have ended
3. When a source indicates all sessions have Ended against the same workstation

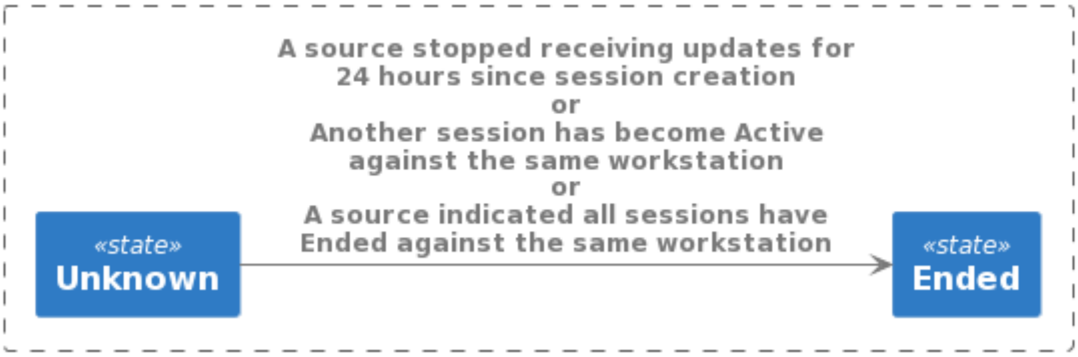
Each behavior has different time metrics.

For the first behavior:

- Last Updated Time reflects the most recent update and potentially indicates the "staleness" of information
- Duration (unchanged)
- Session End populated with the last updated time

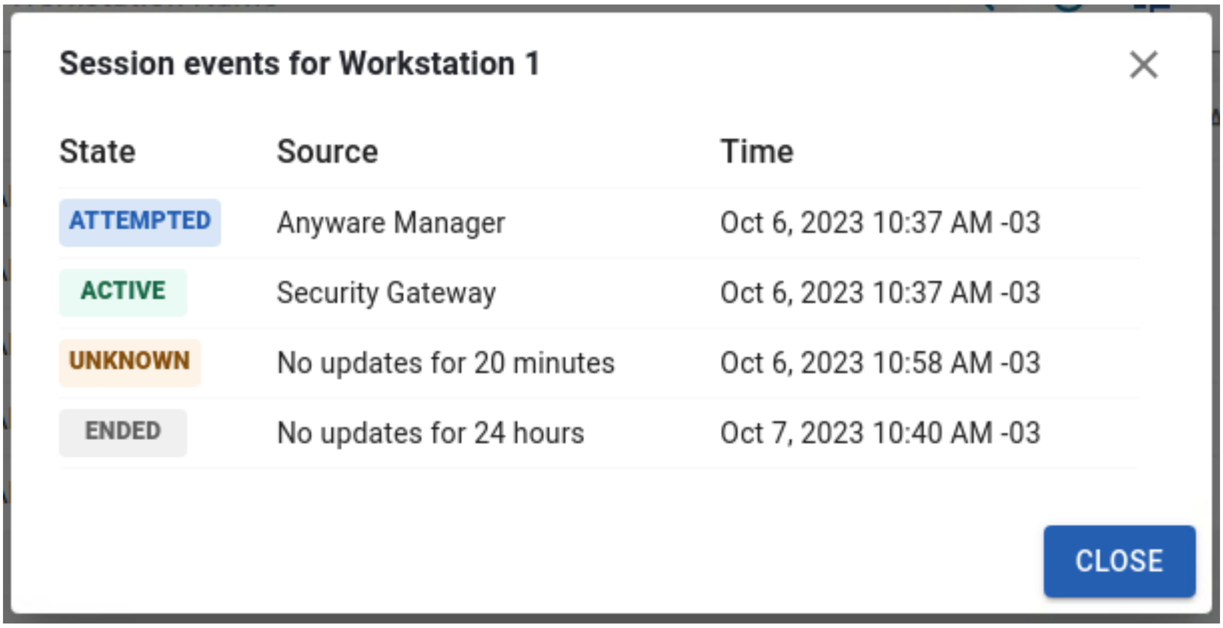
For the second and third behaviors:

- Last Updated Time reflects the most recent update
- Duration reflects the most recent update
- Session End (populated)


A source stopped receiving updates for
24 hours since session creation
or
Another session has become Active
against the same workstation
or
A source indicated all sessions have
Ended against the same workstation
«state»
Unknown
«state»
Ended

Session state transitions

By clicking on a session's status, a modal is shown that displays the session's state progression along with the time the status changed and the source or reason for the change.



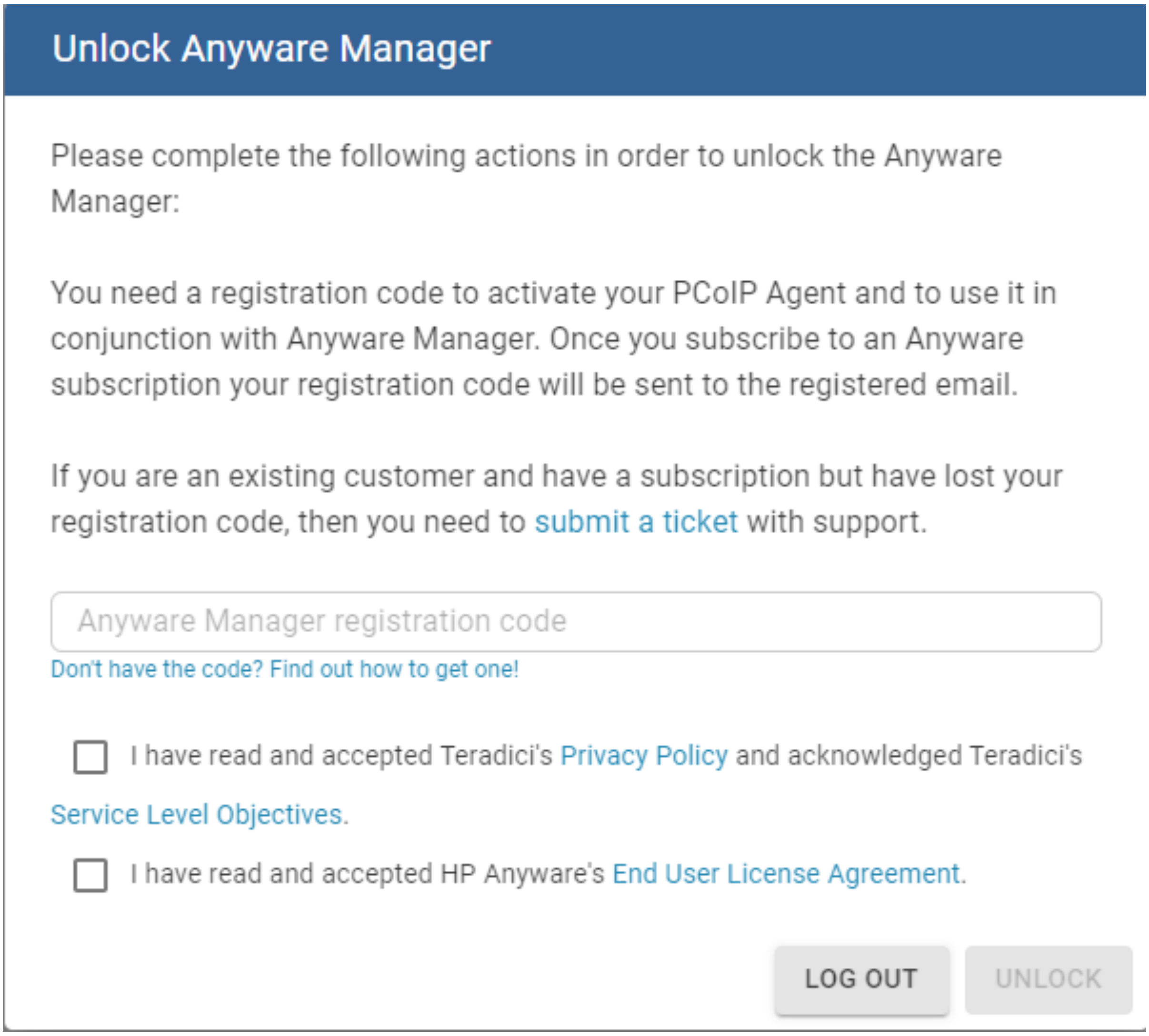
Session events for Workstation 1

State	Source	Time
ATTEMPTED	Anyware Manager	Oct 6, 2023 10:37 AM -03
ACTIVE	Security Gateway	Oct 6, 2023 10:37 AM -03
UNKNOWN	No updates for 20 minutes	Oct 6, 2023 10:58 AM -03
ENDED	No updates for 24 hours	Oct 7, 2023 10:40 AM -03

Managing Deployments

The following section outlines how to create a deployment using the Admin console:

1. If you do not have any existing deployments (first time log-in) you are prompted to enter your Anyware Software registration code. Once you enter the code it automatically generates your first deployment and take you to the **Edit Deployment** page.



Unlock Anyware Manager

Please complete the following actions in order to unlock the Anyware Manager:

You need a registration code to activate your PCoIP Agent and to use it in conjunction with Anyware Manager. Once you subscribe to an Anyware subscription your registration code will be sent to the registered email.

If you are an existing customer and have a subscription but have lost your registration code, then you need to submit a ticket with support.

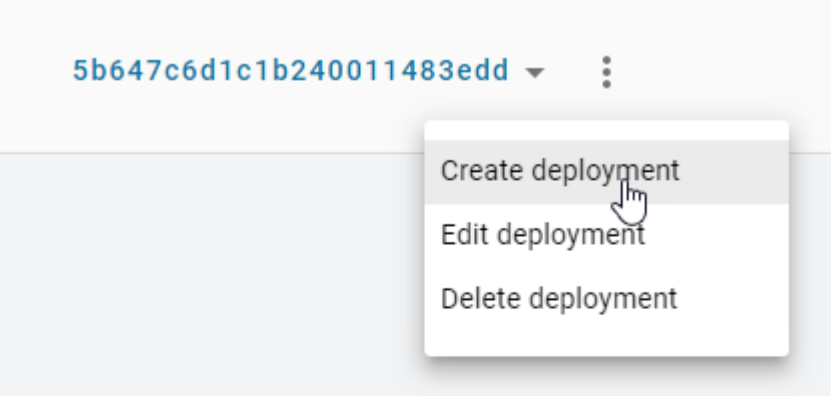
Anyware Manager registration code

Don't have the code? Find out how to get one!

□ I have read and accepted Teradici's Privacy Policy and acknowledged Teradici's Service Level Objectives.

□ I have read and accepted HP Anyware's End User License Agreement.

2. If you have existing deployments you can click **Create deployment** from the kebab options at the top of the page to take you to the **Create Deployment** page.



3. Enter the following information:
   - Enter the deployment name.
   - Enter your PCoIP registration code. Please store this code in a secure location as it cannot be retrieved later.
4. Click **CREATE**.

The deployment has now been created and you can edit the deployment by configuring deployment service accounts, cloud service accounts and Connector settings.

Cloud Service Accounts

You can now enter cloud service account credentials for AWS, Azure and GCP if you are working in those environments and want to enable Anyware Manager to perform certain functions, such as power management. If you are not using AWS, Azure, and GCP then you do not need to enter this information.

> **Cloud Service Account Credentials**
>
> These credentials are used in places where the Anyware Manager as a Service interacts with your cloud environment to perform actions such as powering a remote workstation on or off. If credentials are not provided, remote workstations in that cloud can still be added to Anyware Manager as a Service and users can still be entitled to the remote workstation and start a PCoIP session, but Anyware Manager as a Service cannot perform functions such as power on and off.

Entering these credentials is optional and enables you to access extra functionality and control over the remote workstations within the deployment on the cloud provider of your choice.

> ⚠ **Domain Controllers in a Single Deployment**
>
> You cannot deploy multiple Connectors against different Domain Controllers within the same deployment. This causes the Connectors to crash.

AWS Cloud Credentials

The following sections outline how to managed and configure AWS cloud information for Anyware Manager and Anyware Manager as a Service. Please note the permissions required for Anyware Manager as a Service are different to the permissions for Anyware Manager.

AWS CLOUD CREDENTIALS FOR ANYWARE MANAGER

To configure AWS Cloud Credentials for Anyware Manager, see the AWS Configuration section.

AWS CLOUD CREDENTIALS FOR ANYWARE MANAGER AS A SERVICE

Through the Admin Console you can generate a Anyware Manager Account ID and External ID that can be used when creating an AWS role through the AWS Management Console. The following steps outline how to generate a Anyware Manager Account ID and External ID:

1. In the Admin Console select the deployment you wish to use.
2. Click **Edit Deployment**.
3. Click **Cloud Service Accounts**.
4. Select AWS and click **Generate**. Ensure you copy the Anyware Manager Account ID and External ID and save them to your clipboard.

> ⚠ **AWS Role Creation and Permission Policy**
>
> You must create a role in your AWS account which Anyware Manager as a Service is able to assume. You must use the Account ID and External IDs when creating the AWS role. For more information on creating roles in AWS, see here.

Once you have entered the Anyware Manager Account ID and External ID and created the AWS role, you need to create a permissions policy for Anyware Manager as a Service that contains the following permissions:

- **Service**: EC2

- **Actions**:
    - List: DescribeInstances
    - Write: RebootInstances StartInstances StopInstances TerminateInstances

There are additional permissions needed to verify that the role has all the required permissions before being added to a deployment:

- **Service**: IAM
- **Actions**:
    - Read: GetUser SimulatePrincipalPolicy

The following is an example of how the permissions set should look in a JSON format:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "ec2:RebootInstances",
                "ec2:DescribeInstances",
                "ec2:TerminateInstances",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "iam:GetUser",
                "iam:SimulatePrincipalPolicy"
            ],
            "Resource": "*"
        }
    ]
}
```

If the user tries to add an AWS role that doesn't have these permissions, Anyware Manager as a Service adds the role but does not validate that it has the required permissions. You can now associate a permissions policy to this role.

1. Once you have created the role in AWS, copy and paste the role ARN and enter it into the Role ARN field in the Admin Console.
2. Click **Submit**.

For information on the AWS Service Account roles and permission policies with Anyware Manager as a Service, see here.

Azure Cloud Credentials

For Azure you need to enter the Tenant ID, Subscription ID, Client ID and Client Secret.

For information on how to create a new Client Secret from Azure, see here.

> ⚠ **Azure Client Secret**
>
> Once you generate the client secret you need to copy it as it is not available again from Microsoft. If you have an expired client secret you need to delete it and then create a new secret and assign it to that deployment.

For information on the Azure Service Account and permission requirements with Anyware Manager, see here.

GCP Cloud Credentials

You can enable GCP cloud credentials by entering the GCP client email, Project ID and Private Key and clicking **Submit**. You can also upload the JSON Key file with the GCP cloud credentials.

For more information on GCP Cloud Service Accounts with Anyware Manager, see here.

Editing an Existing Deployment

The creation date, computer and users DNs and the interval time in minutes that it syncs with the Active Directory for the deployment are also displayed when you go to edit a specific deployment.

You can search for specific deployments by name by using the search bar in the table toolbar.

You can edit the deployment name, update the registration code and GCP or Azure cloud service account credentials of an existing deployment through the Admin Console. A menu item has been added to the table toolbar that enables you to create, edit, delete and view all existing deployments:

1. Click the dropdown menu from the top of the page and select the deployment.

2. Select the deployment and click the kebab option under the **ACTIONS** column to edit the deployment.
3. Update the deployment name, registration code, GCP or Azure credentials and then click **SAVE**.

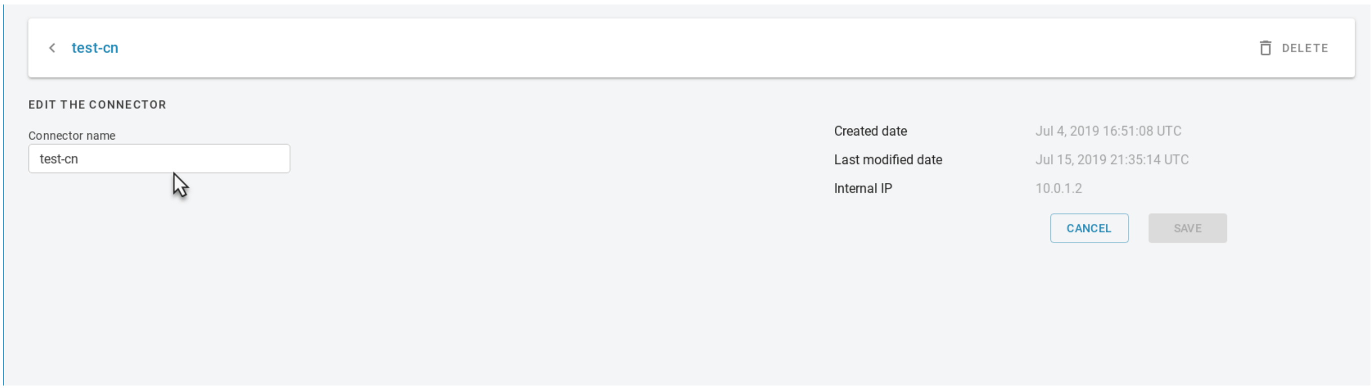
The updated information and credentials are now associated with this deployment.

Editing a Anyware Connector

Once you have created a Connector you can edit its name by clicking on the Connector directly from the **Connectors** page or by clicking on **Edit** from the kebab associated with it on the **Connectors** page.

You can search for specific Connectors by name by using the search bar in the table toolbar.

Enter the new name and click **Save**.



EDIT THE CONNECTOR

Connector name: test-cn

Created date: Jul 4, 2019 16:51:08 UTC

Last modified date: Jul 15, 2019 21:35:14 UTC

Internal IP: 10.0.1.2

Domain Controller Certificates

If all DC certificates have expired, the Anyware Connector stops working. An error indicator is displayed on the **Connectors** page when a Anyware Connector has a Domain Controller with expired certificates.

A warning indicator that details the current state of the Domain Controller certificates is displayed on the same page when a Anyware Connector has a certificate that less than a week away from expiring.

Provisioning a Remote Workstation

The following section outlines how to provision a remote workstation using the Admin Console.

Pre-Defined Images and Templates

If you wish to use your own custom images or templates, you must create and manage those outside of Anyware Manager and create your remote workstation outside of Anyware Manager also. Once you have created a remote workstation you can add it to your deployment in Anyware Manager for brokering and management.

Before provisioning a remote workstation you need to ensure that the Active Directory domain is correctly configured. This should be a different AD Service Account to the account used when installing the Connector. The AD Service Account needs to have the following permissions:

- Create Computer Objects
- Delete Computer Objects

The permissions on the Computer Objects must be set to:

- Read All Properties
- Write All Properties
- Read Permissions
- Modify Permissions
- Change Passwords
- Reset User Passwords
- Validated write to DNS host name
- Validate write to service principal name

These permissions are required so that the remote workstations are able to join the domain account. Without these permissions the remote workstation is provisioned, but there could be an issue when adding it to the domain.

Permissions to Create and Delete Computer Objects

The following section outlines how to add permissions to create and delete computer objects through the OU permissions dialog:

1. Go to the security tab of the OU you want to give permissions to.
2. Right-click the relevant OU and click **Properties**.
3. Go to the security tab and click **Advanced**.
4. Click **Add** and browse to your user account. As stated above you need to add the user account to the OU.
5. Select **This object and all descendant objects** and select the following permissions:
    - Create Computer Objects
    - Delete Computer Objects
6. Click **OK**.

Permissions on the Computer Objects

The following section outlines how to select permissions on the computer objects through the OU permissions dialog:

1. Go to the security tab of the OU you want to give permissions to.
2. Right-click the relevant OU and click **Properties**.
3. Go to the security tab and click **Advanced**.
4. Click **Add** and browse to your user account. As stated above you need to add the user account to the OU.
5. Limit the **Apply Onto** scope to **Descendant Computer objects** and select the following settings:
    - Read All Properties
    - Write All Properties
    - Read Permissions
    - Modify Permissions
    - Validated write to DNS host name
    - Validated write to service principal name
6. Click OK.

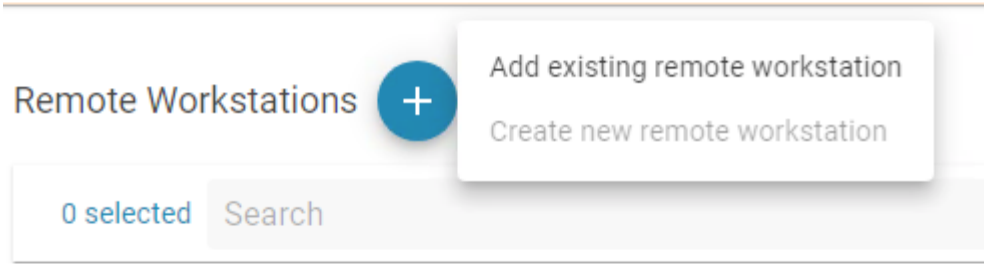
The validated write to DNS host and service principal name permissions are required so that the DNS record for a remote workstation can be created after it is domain joined.

For information on which Cloud Service accounts can perform certain features, please consult the Service Account Requirements section.

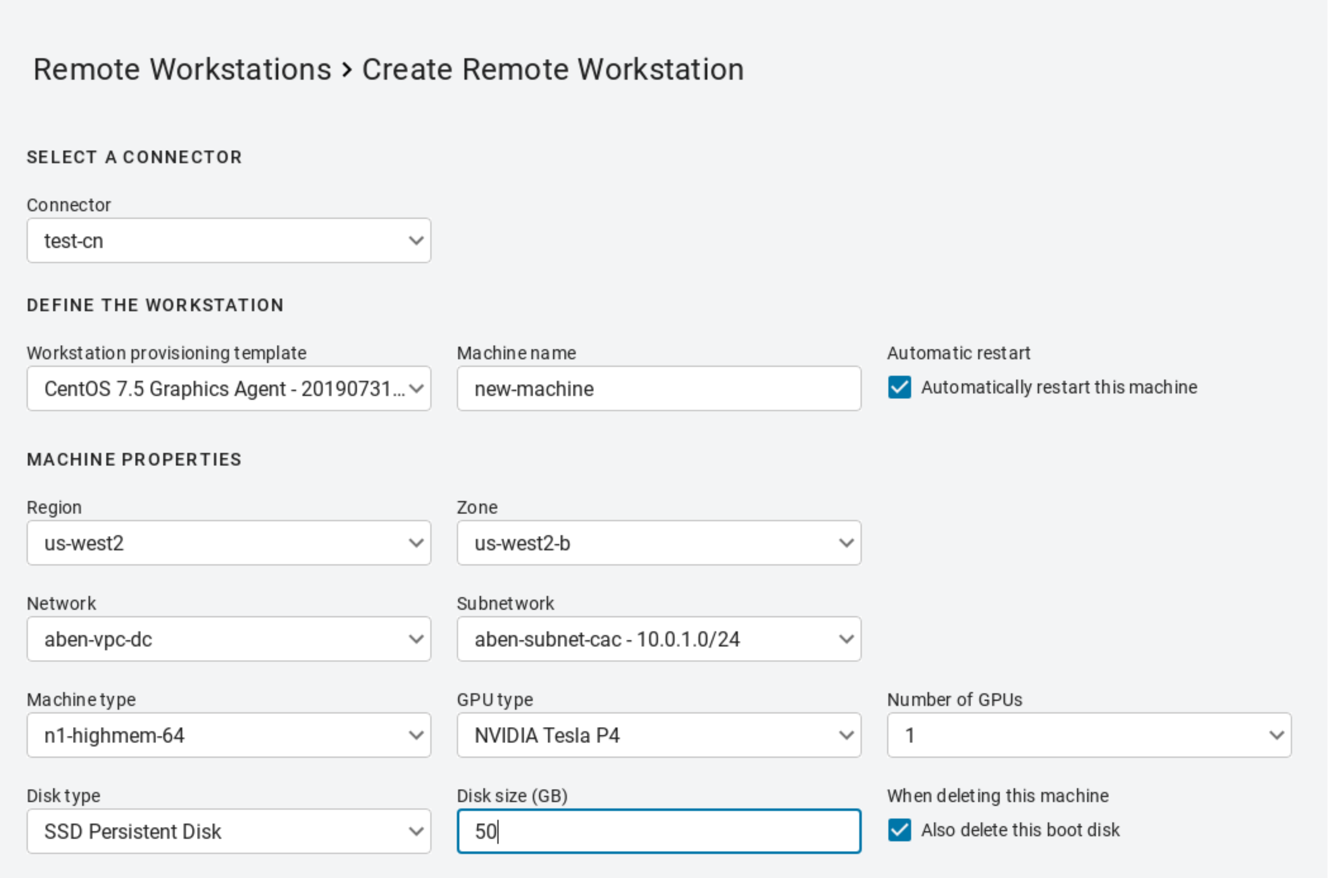
Provisioning a Remote Workstation

You must have a valid cloud service account to enable this feature. The following steps outline how to provision a remote workstation:

1. Click **Workstations** from the Admin Console sidebar.
2. Click **Create new remote workstation** from the add remote workstation icon.


Remote Workstations
+
Add existing remote workstation
Create new remote workstation
0 selected
Search

3. Select an existing Connector from the dropdown menu.
4. Select a provisioning template from the dropdown menu and give your remote workstation a machine name. You can also choose whether you want to enable an automatic restart of the workstation. Compute engine can automatically restart remote workstation instances if they are terminated for non- user intitiated reasons, such as maintenance events, hardware failures, software failures, etc.
5. Enter the remote workstations network, region and disk properties. An example of what this information may look like is shown below:



Remote Workstations > Create Remote Workstation

SELECT A CONNECTOR

Connector: test-cn

DEFINE THE WORKSTATION

Workstation provisioning template: CentOS 7.5 Graphics Agent - 20190731...

Machine name: new-machine

Automatic restart: ☑ Automatically restart this machine

MACHINE PROPERTIES

Region: us-west2

Zone: us-west2-b

Network: aben-vpc-dc

Subnetwork: aben-subnet-cac - 10.0.1.0/24

Machine type: n1-highmem-64

GPU type: NVIDIA Tesla P4

Number of GPUs: 1

Disk type: SSD Persistent Disk

Disk size (GB): 50

When deleting this machine: ☑ Also delete this boot disk

⚠ Public IP or Cloud NAT Requirement

Provisioning fails unless the machine has a public IP or Cloud NAT.

⚠ Remote Workstation Machine Name

Due to NetBIOS and a Windows limitation, the remote workstations machine name must be 15 characters or less. Failure to do this may result in issues with your remote workstation connection.

6. Enter the Active Directory information for the remote workstation. The service account must have permission to join computers to the domain.
7. Once you have entered all required information, click **CREATE**.

The remote workstation appears in the table of available machines on the **Workstations** page.

Active Directory Information

Active Directory information is only used during provisioning to join the remote workstation in question to the domain. This information is not saved by the Anyware Manager. The remote workstation is joined to the active directory domain configured in the Connector.

Metadata Retrieval and Storage Information

All provisioned remote workstations have `--metadata enable-guest-attributes=TRUE` set. This is set to facilitate the passing of data at provisioning time. For more information, see https://cloud.google.com/compute/docs/storing-retrieving-metadata.

IdleShutDown Agent Configuration

IdleShutDown Agent is configured so that the remote workstation shuts down when it is idle. For more information on installing and configuring this feature, see Configuring Idle Shutdown.

Workstation Pools

Creating Workstation Pools

You can create workstation pools within the Anyware Manager Admin Console. A workstation pool is a group of remote workstations. To simplify user access management, a user group or individual users can simply be assigned to a workstation pool.

A floating pool is a remote workstation pool that uses a **floating workstation assignment policy**. With this pool, a user is entitled to a pool and its remote workstations rather than a single remote workstation. When a user is assigned a remote workstation, this assignment is ephemeral. Once the user disconnects from the remote workstation there is a holding time where it is assigned to that user. This holding time can be configured by an admin user. Once this holding period expires, the user is unassigned to the remote workstation and it is added back to the pool and is available for re-assignment.

Once you log in to the Anyware Manager Admin Console, you are automatically assigned a remote workstation within the pool, depending on the assignment policy of the pool. When creating a remote workstation pool, the assignment policy can be selected.

Use Cases for Floating Workstation Assignment Policy

The following section outlines potential use cases for the floating workstation assignment policy:

Two user's and two Windows workstations

- User 1 attempts to log in with a PCoIP Client.
- Windows workstation 1 is successfully assigned to User 1.
- User 2 attempts to log in with a PCoIP Client.
- Windows workstation 2 is successfully assigned to User 2.

Two user's and a single Windows workstation

- User 1 attempts to log in with a PCoIP Client.
- Windows workstation 1 is successfully assigned to User 1.

- User 1 closes the PCoIP Client.
- User 2 then attempts to log in and is presented with an error message stating "Resource does not exist in CAM Service".
- User 2 attempts to log in 25 minutes later. The assignment holding time for this example is 20 minutes, which is the default minimum assignment holding.
- Windows workstation 1 is successfully assigned to User 2. The Windows session is taken over by User 2.

These use cases also apply for RHEL/CentOS workstations.

The following section outlines how to create a floating workstation pool from the Anyware Manager Admin Console:

Creating a Workstation Pool

You can add multiple workstation pools to specific deployments. Each workstation pool lists the remote workstations, users and user groups within that pool. The following steps outline how to create a workstation pool, and choose the floating pool assignment policy:

1. Click on **Workstation Pools** from the Anyware Manager Admin Console sidebar.
2. Click the **+** icon to create a new workstation pool.
3. Name the pool and choose the **Floating** option for the workstation assignment policy. The workstation assignment policy determines how workstations belonging to the workstation pool are assigned to users when they log in. This assignment policy can not be modified after the workstation pool has been created.
4. Enable **Session Tracking** by selecting the toggle.
5. Add the workstation holding time in minutes. Once this holding period expires, the user is unassigned to the remote workstation and it is added back to the pool and is available for re-assignment.
6. Name the pool and click **CREATE**.

There are two possible options for the workstation assignment policy:

Persistent: This is the default policy. Once a user logs in they are automatically and persistently assigned a remote workstation within the pool.

Floating: With the floating policy, once a user disconnects their PCoIP session, the remote workstation is automatically unassigned from the user, and the remote workstation becomes available for other users to connect to.

Adding Remote Workstations to a Workstation Pool

Remote workstations and users within a workstation pool are a subset of the available remote workstations and users within a specific deployment. As a result of this, you can add remote workstations and users that have already been created in Anyware Manager.

The following steps outline how to add remote workstations to a workstation pool:

1. Click on **Workstation Pools** from the Anyware Manager Admin Console sidebar.
2. Select the workstation pool you created in the previous section to display the edit pools page.
3. Click **Add Remote Workstations** and add remote workstations to the pool.

Adding Users to a Workstation Pool

Only specified users can establish PCoIP sessions to remote workstations in the workstation pool. If a remote workstation is available (not assigned to a user) it is automatically assigned to the user. The following steps outline how to add users to a workstation pool:

1. Select the workstation pool and click **Add Users/Add Groups**.
2. Search for the users you want to add, select them and click **SAVE**.

Once users and remote workstations are added to the workstation pool, users from the workstation pool get available workstations upon log in. Once the PCoIP Session is disconnected, the remote workstation is automatically available for future connections or continue to be assigned to the user depending on the workstation pool assignment policy.

Features and Known Limitations

There are certain limitations associated with this feature, as outlined in the following list:

- This feature is only supported in Connector(s) version 78 or higher.
- If all remote workstations have been assigned, and no remote workstations are available, users can see the following error during session establishment "Resource does not exist on CAM Service".

- Remote workstations remain assigned to a user for approximately 20 minutes after the PCoIP session has been disconnected by default. This time period is configurable through assignment holding time, and has to be longer than 20 minutes.
- The current limit is 200 remote workstations in a floating pool. The feature works with a larger number of remote workstations, but the assignment timing may vary.
- **Limited support for Linux Agents**: When establishing a PCoIP session to Linux Agents, the session must be logged off before another user can connect. If the session is not logged off, a 6604 error message is displayed. To resolve this error reboot the remote workstation. This issue is being worked on.
- When connecting to a PCoIP Agent for Windows, if a previous user has been connected, the other user can see the Windows Switch Users screen. They are prompted to enter their credentials again before accessing the desktop.
- For Windows remote workstations that are power managed through Anyware Manager, the Idle Shutdown Service for the PCoIP Agent can be installed and configured. Once this service is installed, the remote workstation automatically shuts off after the PCoIP session has been disconnected. During PCoIP session establishment, the remote workstation is powered on. For information on installing and configuring the Idle Shutdown Service, see below.

Idle Shutdown Service

The following section outlines the steps to install and configure the Idle Shutdown Service for each Windows remote workstation:

1. Connect to the remote workstation via the PCoIP Client. Ensure you have admin permissions.

2. Copy the following PowerShell script:

```
$idleTimerRegKeyValue = <idle-time-in-minutes>
$enableAutoShutdown = <$true-or-$false>

# Detect agent type
$is64 = $false
$serviceName = "CAMIdleShutdown"
$path = "C:\Program Files (x86)\Teradici\PCoIP Agent\bin"
if (!(Test-Path -path $path))  {
    $path = "C:\Program Files\Teradici\PCoIP Agent\bin"
    $is64 = $true
}
cd $path

# Install Service
$ret = .\IdleShutdownAgent.exe -install
# Check for success
if( !$? ) {
    $msg = "Failed to install {0} because: {1}" -f $serviceName, $ret
    Write-Host $msg
    throw $msg
}

# Configure Service
$idleTimerRegKeyPath =
"HKLM:SOFTWARE\WOW6432Node\Teradici\CAMShutdownIdleMachineAgent"
if ($is64) {
    $idleTimerRegKeyPath =
"HKLM:SOFTWARE\Teradici\CAMShutdownIdleMachineAgent"
}
$idleTimerRegKeyName = "MinutesIdleBeforeShutdown"
if (!(Test-Path $idleTimerRegKeyPath)) {
    New-Item -Path $idleTimerRegKeyPath -Force
}
New-ItemProperty -Path $idleTimerRegKeyPath -Name $idleTimerRegKeyName -
Value $idleTimerRegKeyValue -PropertyType DWORD -Force

# Disable service if desired
$svc = Get-Service -Name $serviceName
if (!$enableAutoShutdown) {
    $msg = "Attempting to disable {0} service" -f $serviceName
    Write-Host $msg
    try {
        if ($svc.Status -ne "Stopped") {
            Start-Sleep -s 15
            $svc.Stop()
            $svc.WaitForStatus("Stopped", 180)
        }
        Set-Service -InputObject $svc -StartupType "Disabled"
        $status = if ($?) { "succeeded" } else { "failed" }
        $msg = "Disabling {0} service {1}" -f $svc.ServiceName, $status
        Write-Host $msg
    }
    catch {
        throw "Failed to disable CAMIdleShutdown service."
    }
}
```

If the remote workstation was provisioned by Anyware Manager then the `idle timer` is already configured. In this case the `Install Service` section of the above commands can be skipped.

3. Set `$idleTimerRegKeyValue` to be between 5 and 10000, this is the number of minutes before the remote workstation is considered idle after the last PCoIP session was disconnected.
4. Set `$enableAutoShutdown` to `$true`.
5. Save the PowerShell script with a *.ps1* file extension and run the script. After the script has been successfully executed, the idle shutdown timer should be running. The remote workstation shuts down after the specified number of minutes of inactivity, as configured in step 3, once the user disconnects.

For more information on the Idle Service Shutdown, see Installing and Configuring Anyware Manager as a Service in the Anyware Manager as a Service guide.

Auto Log-Off Service

When a user disconnects their PCoIP session from a Linux PCoIP Agent, a different user is unable to connect unless the existing remote workstation user session is terminated. This results in the remote workstation being locked, and unusable in a floating pool assignment, since a different user cannot log-in.

The auto log-off service enables you to bypass this issue by terminating a user session after the PCoIP session has been terminated. The auto log-off service monitors the **pcoip-server** process every minute. If it is not an active process then it samples the CPU load involved and if it is below a certain level for a certain amount of minutes, the script terminates the **pcoip-desktop-child** process which emulates a user logging off.

The auto log-off service disconnects a user if following criteria are met:

- No active PCoIP session detected (**pcoip-server** process is terminated).
- CPU utilization is less than 20% (`CPUUtilizationLimit`) for over 20 minutes (`MinutesIdleBeforeLogOff`).

- Sampling rate is 1 minute (`OnUnitActiveSec`).

INSTALLING AND CONFIGURING THE AUTO LOG-OFF SERVICE

You must have a CentOS/RHEL 7.8 virtual machine or Ubuntu virtual machine installed in order to run this service.

CentOS/RHEL Virtual Machine

- Run the following command to install the `pcoip-agent-autologoff` service on a CentOS/RHEL virtual machine:

```
sudo yum install pcoip-agent-autologoff
```

Ubuntu Virtual Machine

- Run the following command to install the `pcoip-agent-autologoff` service on a Ubuntu virtual machine:

```
sudo apt-get install pcoip-agent-autologoff
```

Once you have installed the service you can manage it via the `pcoip-agent-autologoff-mgmt` script. This script is located in */opt/teradici/pcoip-agent-autologoff/pcoip-agent-autologoff-mgmt*. The following commands must be executed either from the script path, or using the full path of the script.

The following table outlines the options you can use to manage the auto log-off service:

Option	Description
`--enable`	Enable the service.
`--disable`	Disable the service.
`--change-params`	Modify CPU utilization limit (CPUUtilizationLimit) and Idle time before logging off (MinutesIdleBeforeLogOff).
`--change-timer`	Modify polling interval (OnUnitActiveSec). This value sets how often the service runs.
`--show-logs`	Shows last 100 log messages.
`--follow-logs`	Shows live log messages.
`--help`	Shows the tool help page.

The default settings are shown in the table below. It is possible to modify these settings after the auto log-off service has been installed and configured:

Setting	Default	Description
`MinutesIdleBeforeLogOff`	20 minutes	Number of minutes the remote workstation must be considered idle before it logs a user off. The timer only starts when a user is not in PCoIP session.
`CPUUtilizationLimit`	20%	Value between 0 and 100 representing CPU utilization percentage. If average CPU utilization is below this value, the machine is considered idle, and logs off if maintained for `MinutesIdleBeforeLogOff`.
`OnUnitActiveSec`	1 Minute	Polling interval in minutes for checking the CPU utilization.

ENABLING THE AUTO LOG-OFF SERVICE

The following section outlines how to enable the auto log-off service.

1. To enable the service run the following command:

```
sudo pcoip-agent-autologoff-mgmt --enable
```

2. To disable the service run the following command:

   ```
   sudo pcoip-agent-autologoff-mgmt --disable
   ```

UPDATING THE AUTO LOG-OFF SERVICE CONFIGURATION

The following section outlines how to update the auto log-off service configuration.

- Run the following command to change `MinutesIdleBeforeLogOff` or `CPUUtilizationLimit`:

  ```
  sudo pcoip-agent-autologoff-mgmt --change-params

  # follow the prompt to apply changes to the service
  ```

- Run the following command to change `OnUnitActiveSec`:

  ```
  sudo pcoip-agent-autologoff-mgmt --change-timer

  # follow the prompt to apply changes to the service
  ```

- Run the following command to show the log history:

  ```
  sudo pcoip-agent-autologoff-mgmt --show-logs
  ```

- Run the following command to follow the logs:

  ```
  sudo pcoip-agent-autologoff-mgmt --follow-logs
  ```

- Run the following command to display help information:

  ```
  sudo pcoip-agent-autologoff-mgmt --help
  ```

Floating Workstation Assignments

Floating workstation assignments is a feature of the Connector v78 or higher, which enables a user's entitlement to a workstation to be temporary. The remote workstation can be used by multiple users. Floating workstation assignments enables remote workstations that are part of a Remote Workstation Pool, to be assigned to a user for the duration of the PCoIP session. Once this session has been disconnected, the remote workstation are automatically unassigned, and are available for other users to connect.

This feature is useful for managing persistent remote workstations that are shared by multiple users and that have expensive software and applications, such as video editing, video proofing, etc. Multiple users can access the same remote workstation and utilize these applications. It can be used for project based remote workstations, where remote workstations are associated with projects instead of users. Teams can log into the project and access a specific remote workstation for that project. This also enables organizations to enforce logical separation of remote workstations.

The following sections outlines the steps involved in enabling this feature.

Create a Floating Pool

The next step is to create a floating pool group from the Admin Console.

1. Open the **Workstations Pools** page and click the **+** icon to create a new pool.
2. Select **Floating** for the workstation assignment policy, name the pool and click **CREATE**.
3. Click on the newly created pool from the Pools menu.
4. Click **ADD REMOTE WORKSTATIONS** to add workstations to the pool and click **SAVE**.

Remote Workstation Limit

There is a limit of 200 remote workstations in a floating pool. This feature works with a larger number of remote workstations, but assignment timing may vary as a result.

Assign Users to the Pool

Once you have enabled session tracking and created and added remote workstations to your pool, you now need to add specific users. Only specified users can establish PCoIP sessions to remote workstations in the pool.

1. Click on the newly created pool from the Pools menu.
2. Click **ADD USERS** from the top menu, select the users you want to add and click **SAVE**.

Once you have completed these steps any user from the pool is able to get any available remote workstation from the same pool on login. Once the PCoIP session has been disconnected, the remote workstation automatically becomes available for future connections.

Session Disconnection

Please note that remote workstations remains assigned to a user for **approximately 25 minutes** after the PCoIP session has been disconnected.

Limited Support for PCoIP Agents for Linux

PCoIP sessions to PCoIP Agents for Linux must be logged off before another user can connect. If the session is not logged off, a 6604 Error is displayed. If you observe this error, reboot the remote workstation.

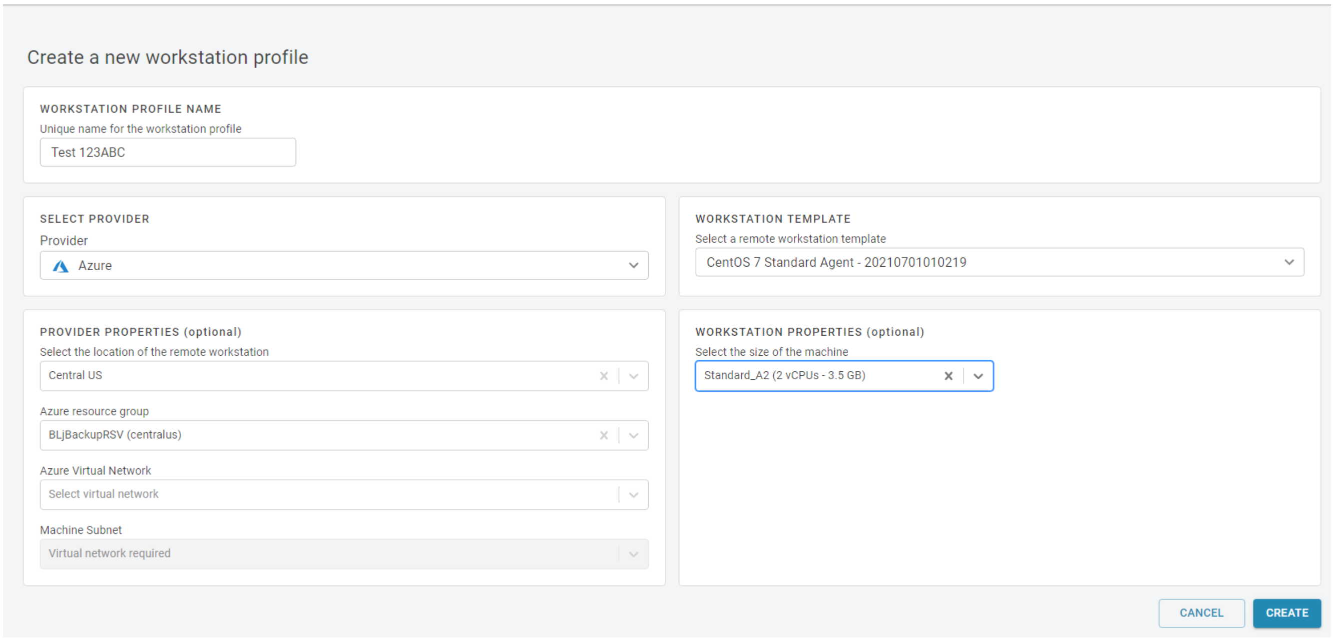
Workstation Profiles

Workstation profiles logically group remote workstation provisioning information. Profiles define a set of workstation deployment settings that are shared by any workstation deployed from this profile. This feature enables administrators to streamline deploying workstations and improves the experience of deploying a large number of identical remote workstations.

Creating a Workstation Profile

The following steps outlines how to create a workstation profile from the Admin Console. Once you have created a workstation profile, you can use it to deploy a remote workstation.

1. Click on **Workstation Profiles** from the Admin Console sidebar.
2. Click the **+** icon to create a new workstation profile.
3. Enter a unique name for the workstation profile.
4. Select the cloud provider you wish to use. Currently Azure and GCP are supported.
5. Select a remote workstaion template. The remote workstation template defines the base OS and provisioning steps for the remote workstation you want to deploy. The only required field is the **Resource template ID** parameter.



Create a new workstation profile

WORKSTATION PROFILE NAME
Unique name for the workstation profile
Test 123ABC

SELECT PROVIDER
Provider
Azure

WORKSTATION TEMPLATE
Select a remote workstation template
CentOS 7 Standard Agent - 20210701010219

PROVIDER PROPERTIES (optional)
Select the location of the remote workstation
Central US

Azure resource group
BLjBackupRSV (centralus)

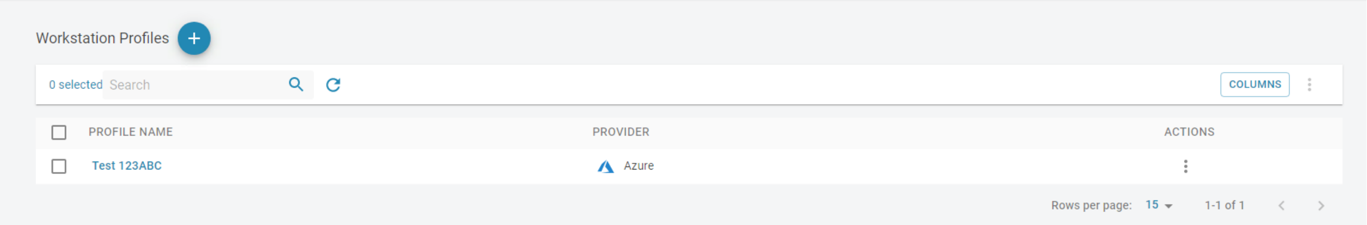
Azure Virtual Network
Select virtual network

Machine Subnet
Virtual network required

WORKSTATION PROPERTIES (optional)
Select the size of the machine
Standard_A2 (2 vCPUs - 3.5 GB)

6. Once you entered all the required information, click **CREATE**.

The workstation profile you created is visible in the list of workstation profiles. You can delete any workstation profiles from this view.



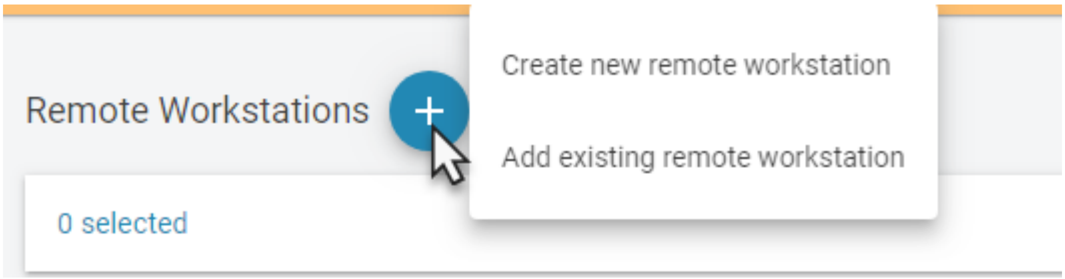
□	PROFILE NAME	PROVIDER	ACTIONS
□	Test 123ABC	Azure	⋮

Rows per page: 15 1-1 of 1

Deploying a Remote Workstation with a Workstation Profile

Once you have created a workstation profile you can use it to populate the **Create Workstation** page. The following steps outline how to use the workstation profile when creating a new remote workstation:

1. Click **Workstations** from the Admin Console sidebar.
2. Click **Create new remote workstation** from the add remote workstation icon.


Remote Workstations
0 selected
Create new remote workstation
Add existing remote workstation

3. Select the cloud provider you wish to use. This must be the same cloud provider you entered when you created the workstation profile.
4. From the **WORKSTATION PROFILE** tab select the workstation profile you created to auto-fill the page with the provider properties, workstation template and workstation properties.
5. If you chose Azure as your cloud provider, enter the remote workstation username and password.
6. Enter the Active Directory account and password. The Active Directory information is only used during provisioning to join the remote workstation to the domain. This information is not saved by the Anyware Manager or Admin Console.
7. Click **DEPLOY**.

The remote workstation is now created and deployed and is visible on the **Workstations** page. Using a specific workstation profile ensures that the identical information is used for all remote workstations created.

Workstation profile checkbox

If you deploy a remote workstation and do not use a workstation profile, you are prompted by a message asking if you want to use this configuration as a workstation profile. You can select to not show this message again, are not prompted again to create a workstation profile for future deployments.

Workstation Status in Anyware Manager

Anyware Manager helps you monitor the status and health of each Workstation available in your deployment. Each Workstation has a status that is affected by any errors detected by the Anyware Manager. If no errors are detected, the status column on the Workstations page for a specific Workstation contains a green check mark. When errors are detected, the column displays a red warning icon. Clicking on the icon displays a list of the errors affecting the Workstation status. You can sort the status column by clicking on the column header to locate all Workstations with errors.

Types of Errors

Anyware Manager Errors

Anyware Manager Errors are detected internally and can affect the ability to connect to Workstations. They are depicted by the following icon:

⚠

System Errors

System Errors can be of two types and are issued by Intel® AMT. They are as follows:

- **System Boot:** Anyware Manager can detect initialization errors from Workstations that support AMT 9 or later.
- **Power Supply:** Anyware Manager can detect Power Supply errors for HP ZCentral 4R Workstations.

They are depicted by the following icon:

▣

For more information, see System Alerts for more details.

SAML Configuration with Anyware Manager

What is SAML?

SAML stands for Security Assertion Markup Language (SAML) and is a standard which Identity Providers use to communicate authorization credentials to different Service Providers. This enables users to manage one set of credentials to authenticate with different services.

SAML enables federated login to several services by passing authorization credentials between services. A SAML flow has three main roles:

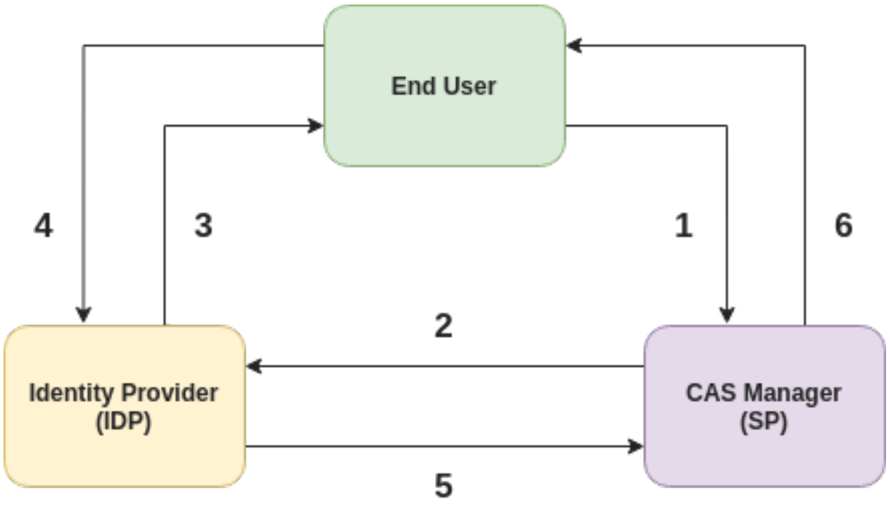
- **End User**: A user who is trying to access a service using federated login credentials
- **Identity Provider (IDP)**: An identity provider performs the authentication about the end users identity and sends the necessary data to the service provider along with any other access control data in the form of **SAML Assertions**. Popular examples are Azure Active Directory and Okta.
- **Service Provider (SP)**: A service provider is the system that requests authentication from an identity provider to authorize an end user. **Anyware Manager plays the role of a SP**

SAML Assertions

SAML Assertions are XML documents that the IDP sends to a given SP to validate user authorization. There are three different types of SAML Assertions:

- **Authentication**: This assertion provides user identity and the time at which a user was authenticated and the method of authentication that was used.
- **Attribute**: This assertion passes the SAML attributes about the user to the service provider. There can be more than one attribute assertions in a SAML response.
- **Authorization**: This assertion is the decision that determines if the user was successfully authorized to access the service or not by the IDP. Most common causes of failed authorization are incorrect password and/or insufficient access to the service the end user tried to access.

Anyware Manager Initiated SAML Authentication Flow



In the diagram above the following is happening

1. An end user wants to login to Anyware Manager. The user uses the SSO link for Anyware Manager.
2. Anyware Manager requests the configured IDP for the SAML response for the user.
3. IDP requests the user to login and verifies credentials.
4. User logs in with the desired credentials to IDP.
5. The IDP now sends a SAML response to Anyware Manager based on the user provided credentials.
6. Anyware Manager validates the SAML response and *SAML Attribute Assertions for Anyware Manager* received from the IDP, and then grants access to the end user.

SAML Attribute Assertions for Anyware Manager

Anyware Manager checks for the following attributes in the SAML response received from the configured IDP:

- **NameID**: Anyware Manager verifies the NameID attribute, which is used to uniquely identify a user. The NameID value is typically a user's UPN or email.
- **Group Attributes**: Anyware Manager can also verify a user's group membership from properties in the AttributeStatement of the SAML Assertion. The *Group attribute name* (configured in the *Allowed Groups* tab on the *Multi Admin Setting* page of the Admin Console) specifies the name of the Attribute where the groups are returned. The AttributeValue can match either a *Group ID* or *Group Name* based on how an Allowed Group was created in the Multi-Admin Settings page.

Anyware Manager allows access to a user through a SAMl configuration if the user is in the list of **Allowed Admins** in Anyware Manager or the user is a member of one or more of the **Allowed Groups** in your IDP. Hence if you need to revoke a user's access to Anyware Manager through a SAMl configuration, you need to remove the user from the **Allowed Admins** list in Anyware Manager and remove the user's membership from any **Allowed Groups** through your IDP.

Configure Anyware Manager as a SAML Service Provider to Enable Multi-Admin

The following section outlines the steps to setup and configure SAML for Anyware Manager using the Anyware Manager Admin Console:

1. From the account icon click **Multi Admin Settings** to create a new multi-admin configuration.
2. Register Anyware Manager as a SP with your IDP. You can obtain the **Assertion Consumer Service URL** and **Audience URL** from the **Configuration Info** section. This information should be used to configure your IDP to recognize Anyware Manager as a SP.
3. Configure Anyware Manager to be able to connect to your IDP. Obtain the **Identity Provider Login URL** and **Identity Provider Certificate** from your IDP and configure the **IDP Settings** section accordingly. Alternatively you can also upload an *IDP XML Metadata* file in the **IDP Settings** section.
4. Enable Multi-Admin configuration to use configured IDP. Make sure that your configuration is enabled by toggling the switch at the bottom of the **Configuration Info** section and confirm that you see the *Configuration is enabled* message.
5. Configure Anyware Manager Assertion Attributes:
    - To allow individual user as admin, go to the **Allowed Admins** section and add the UPN associated to that user. Anyware Manager validates the UPN against the **NameId** SAML assertion attribute in the SAML response received from the IDP.
    - To allow user groups. Go to the **Allowed Groups** section and configure the **Group Attributes** accordingly. This configures Anyware Manager to validate the **Group Name** and/or **Group ID** SAML attribute assertions in the SAML response received from the IDP.
    - You can configure either **Allowed Admins** or **Allowed Groups** or both in the **Multi-Admin Settings**.
6. Allowed users can now access Anyware Manager by opening the **Anyware Manager login page** URL which is available in the **Configuration Info** section. Alternatively, users can also directly login

via the IDP using the **Direct login via identity provider** URL also available on the **Configuration Info** section.

Configuration Information

This section contains auto-generated information about the login URLs and IDP:

- **Anyware Manager login page**: A link to the page for multi-administrator login to the Admin Console. This is the SSO link used by the end user in **Step 1** of SAML auth flow diagram
- **Direct login via identity provider**: An endpoint to which multi-admin sign-in requests can be sent. This is the login page for the configured IDP.
- **Assertion Consumer Service URL**: The callback URL provided to the IDP to which user information is sent once the IDP has authorized the user. This is the Anyware Manager endpoint that the IDP sends the SAML response to in **Step 5** of the SAML auth flow diagram
- **Audience URL**: The entity ID that the IDP can use to identify the Admin Console.

IDP Settings

This section contains IDP settings that can be updated to manage the SAML configuration within Anyware Manager:

- **Identity Provider Login URL**: The IDP endpoint to which SAML authentication requests are sent. This endpoint is the one that Anyware Manager sends the SAML login request to in **Step 2** of SAML authentication flow diagram above.
- **Identity Provider Certificate**: The public certificate of the IDP used to verify the signature of the IDP.

You can also upload a .xml file that contains your IDP information.

Allowed Admins

This section enables you to add new admins and displays all existing admins that are allowed to login via your IDP. To add a new admin, enter their e-mail, and click the **Add Admin** button.

Allowed Groups

This section enables you to add new groups and displays all existing groups that are allowed to login via your IDP. To enable the access for a group of users, enter the *claim type* and *group claim* and click **Add Group**.

- The *claim type* informs Anyware Manager how the group is returned in the SAML attribute assertions in the SAML response received from your IDP.
- The *group claim* matches against the group either in the **Group Name** claim or in the **Group ID** claim received in the SAML attribute assertions for a user based on the *claim type* defined for the group.

Service Account and API Access

Anyware Manager as a Service provides direct API access in the Anyware Manager as a Service service. API's are an advanced way of interacting with the service, which enables you to integrate it into your business systems or to automate your use of the service for your specific needs.

> **HP Advantage Partner Program**
>
> To access and use the Anyware Manager as a Service APIs, you must be a member of the HP Advantage Partner Program or have been pre-approved by HP. Contact HP here for more information.

Service Accounts: There are two types of service accounts that you can create with the Admin Console:

Anyware Manager Service Accounts

The Anyware Manager service account is an account that is created from the Admin Console for the purpose of creating future deployments and deployment service accounts through the Anyware Manager as a Service APIs. The Anyware Manager service account cannot perform any actions within a deployment, and so further actions to a deployment require the deployment service account, which is outlined below. For information on creating a Anyware Manager service account, see here.

Deployment Service Accounts

Deployment service accounts are specific accounts that can only perform actions against the deployment, such as adding remote workstations. The deployment in this case is the deployment the service account is created within. They cannot perform actions against any other deployment. For information on creating a deployment service account, see here.

API Access Token

The API Access Token can be used to enable a user to operate at a level above deployments, such as creating a new deployment. The API Access Token is only valid for a limited period of time. This token also acts as an authorization token that can be used when performing an account ownership transfer, as outlined in the Account Ownership section of the Anyware Manager as a Service guide.

For more detailed information on accessing the Anyware Manager as a Service APIs, see Anyware Manager APIs.

Creating Anyware Manager Service Account

You can create a Anyware Manager service account from within the Admin Console. The following steps outline how to create a Anyware Manager service account.

1. Click on your account name and select **Anyware Manager service account**.
2. Click the **+** icon from the Anyware Manager service account page and name your new account.
3. Once you have created the Anyware Manager service account download the JSON file or copy the key id. Ensure that you store the file securely as this key cannot be recovered if lost.
4. Go to the Service Account Keys section of the Anyware Manager as a Service API documentation for the required APIs to use this key to create a deployment.

Creating and Assigning a Deployment Service Account

You can create and assign a deployment service account to a deployment through the **Deployments** option within the Anyware Manager as a Service Admin Console. The following steps outline how to add a deployment service account to an existing deployment:

1. Click on your deployment from the console dropdown to display your existing deployments.
2. Click the kebab icon and click **Edit deployment** to display the deployment properties page.
3. Under the **Deployment Service Accounts** tab click the **+** sign to create a service account.
4. Once the service account has been created it returns service account information. This information should be saved as a JSON file in a secure location, as it can only be retrieved once. It returns a Anyware Manager as a Service API token that you can use to query the Anyware Manager as a Service APIs. This token is only authorized to access resources associated to the deployment that service account is associated with.

All deployment service accounts associated with a specific deployment is listed on the deployment page. You can delete deployment service accounts from this page. For information on using the deployment service accounts and deployment service keys with the Anyware Manager as a Service APIs, see here.

Obtaining a Anyware Manager as a Service API Access Token

API access tokens permit you to enable other tools and applications to interact with Anyware Manager as a Service through public APIs. The access token has tenant level permissions, which enables you to access all of a user's resources from any deployment.

To obtain a Anyware Manager as a Service API Access token:

- Click **Get API token** from the user account icon within the Admin Console. You receive the following message:

"You need to copy the token as it will expire after a period of time."

HP Advantage Partner Program

To access and use the Anyware Manager as a Service APIs, you must be a member of the HP Advantage Partner Program (HPAA) or have been pre-approved by HP. Contact HP here for more information.

Federated Authentication

OAuth

Federated Authentication Overview

Federated User Authentication enables organizations to use their own Identity Provider (IDP) as the source to verify the identity and to authenticate a user before permitting them to select a remote workstation. Once the desired workstation is selected, the user needs to provide the username and password to authenticate at the remote workstation.

PREREQUISITES

To use the Federated Authentication Functionality, you must meet the following criteria:

- Anyware Manager 23.04 or later
- HP PCoIP Client version 23.01.0 or later
- An Identity Provider that supports OAuth2
- Ubuntu Connector v147 or later with access to an Identity Provider

POST CONFIGURATION USER WORKFLOW

After completing the Federated Authentication configuration, the user workflow is as follows:

- You can open the PCoIP Client and select a Connector or a broker from the list of connections.
- The default web browser opens to a login page for the respective Identity Provider for user authentication.
- The user gets a list of remote desktops or pools to select.
- The user gets prompted within the client to authenticate. This credential is used to log the user into the desktop itself.
- The PCoIP Session is initiated with the remote desktop.

Federated Authentication Workflow

When you connect to a remote desktop using a PCoIP client earlier than 23.01 or a zero client and Federated Authentication has been configured there are one of two possible outcomes:

- **Multi-Factor Authentication is not configured at the connector**: The PCoIP client is unable to proceed and may produce an error or warning.
- **Multi-Factor Authentication is configured at the connector**: The system asks for a username/ password and prompts for an MFA token for authentication.

Configuring Okta IDP

Okta is a third-party identity provider (IdP) that can be configured to work with Anyware Manager. This permits Okta to be used as the source of authentication for any user attempting to connect to a connector in order to get a list of remote workstations to connect to.

When configured, a user attempting to connect to a Connector instance is prompted to log in at the organization's Okta login page. After this login is completed, the user is presented with their list of pools or desktops. After selecting a desktop or pool to connect to, the user is prompted in the PCoIP client for their username and password, and these last credentials are used at the remote workstation to log the user in.

⚠ **Okta Documentation Reference**

The configuration steps listed below a produced using Okta and their documentation. The Okta system and documentation are outside the control of HP and may change over time and may potentially not match the instructions here. For more information or the most recent documentation see Okta Documentation.

⚠ **IDP Configuration Subject to Change**

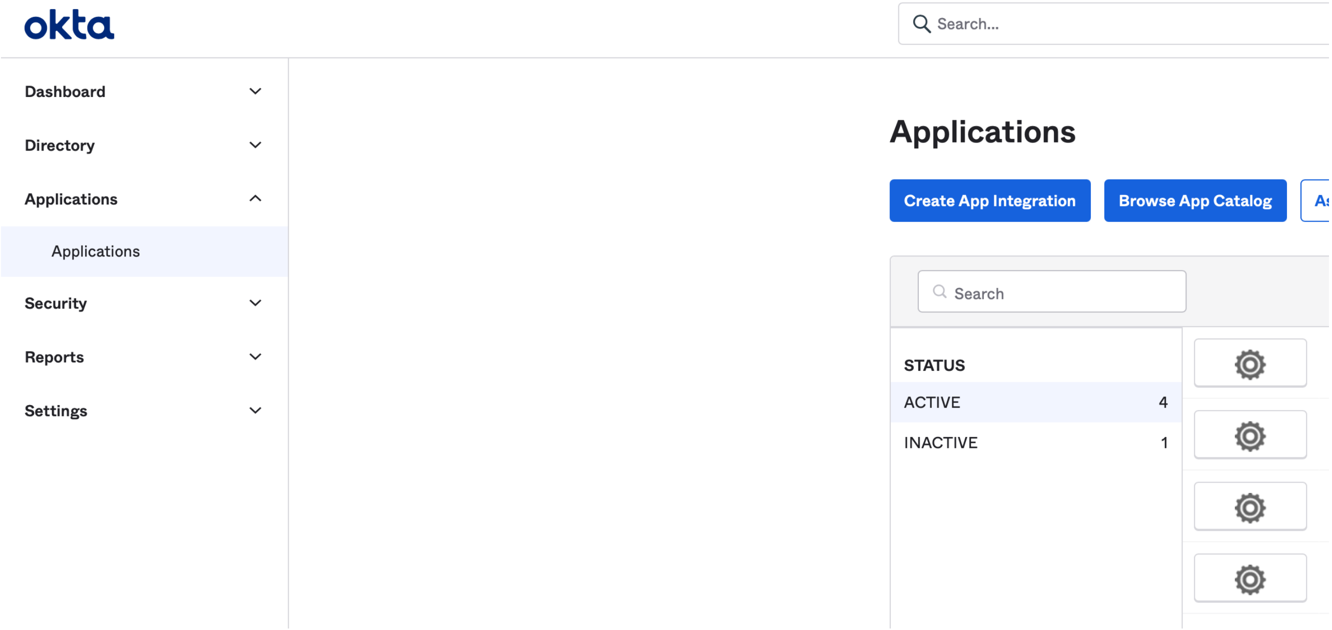
The configuration instructions below are provided as an example with Okta IDP. They are provided as-is. The method of configuration could change outside of the control of HP. Additionally, other IdPs could have different steps required and may use different terms to describe the requirements.

After completing the setup within your IdP, you must have the following information for future configurations:

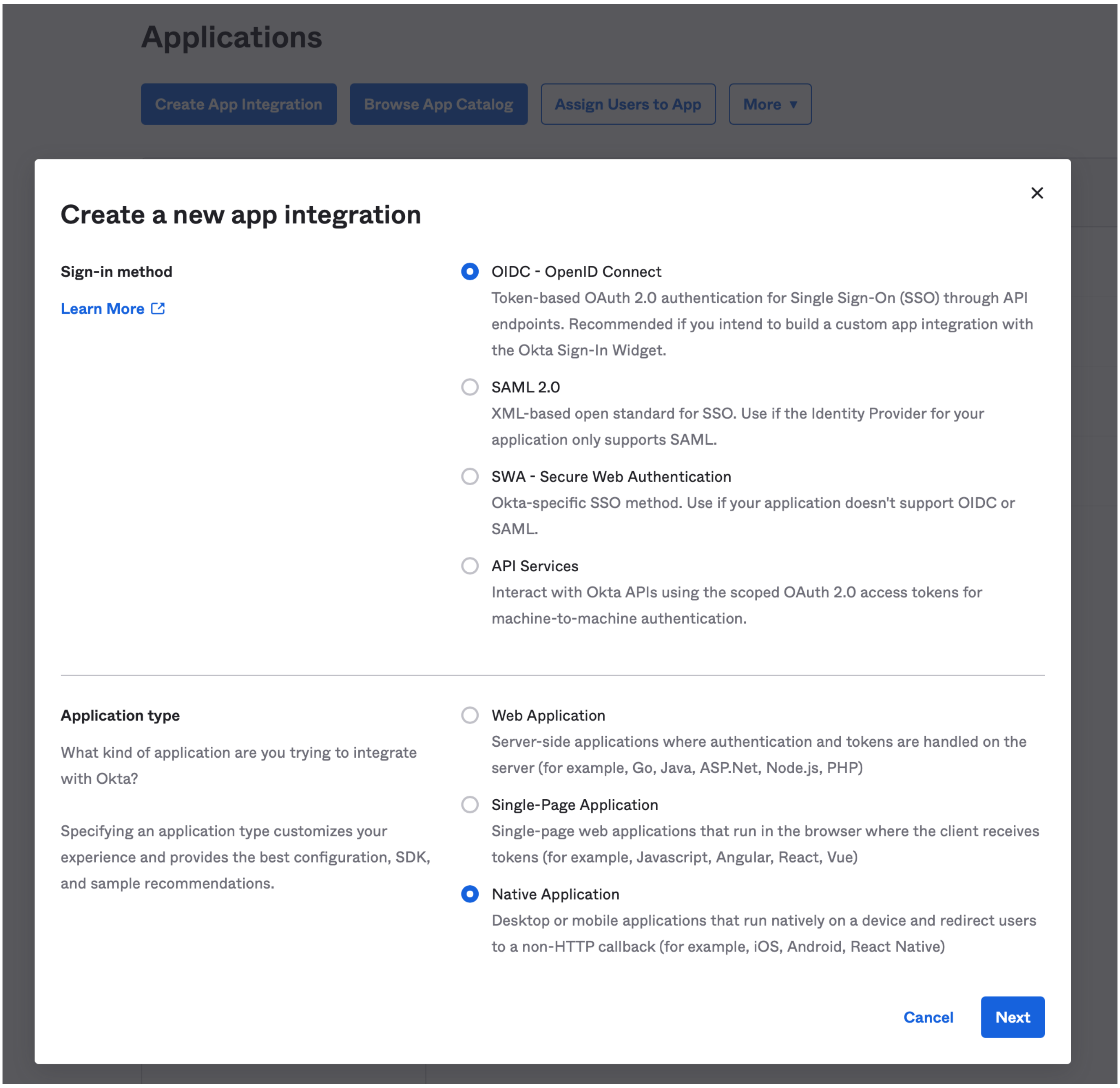
- The authorization URL of your identity provider
- A Client ID

TO CONFIGURE OKTA

1. Login to Okta on the link here.
2. Go to **Applications** section on the left pane and select **Create App Integration**.



3. In the **Create a new app integration** window, select **OIDC-OpenID Connect** as the sign-in method and **Native Application** as the Application type.



Create a new app integration

Sign-in method

Learn More

● OIDC - OpenID Connect
Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.

○ SAML 2.0
XML-based open standard for SSO. Use if the Identity Provider for your application only supports SAML.

○ SWA - Secure Web Authentication
Okta-specific SSO method. Use if your application doesn't support OIDC or SAML.

○ API Services
Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.

Application type

What kind of application are you trying to integrate with Okta?

Specifying an application type customizes your experience and provides the best configuration, SDK, and sample recommendations.

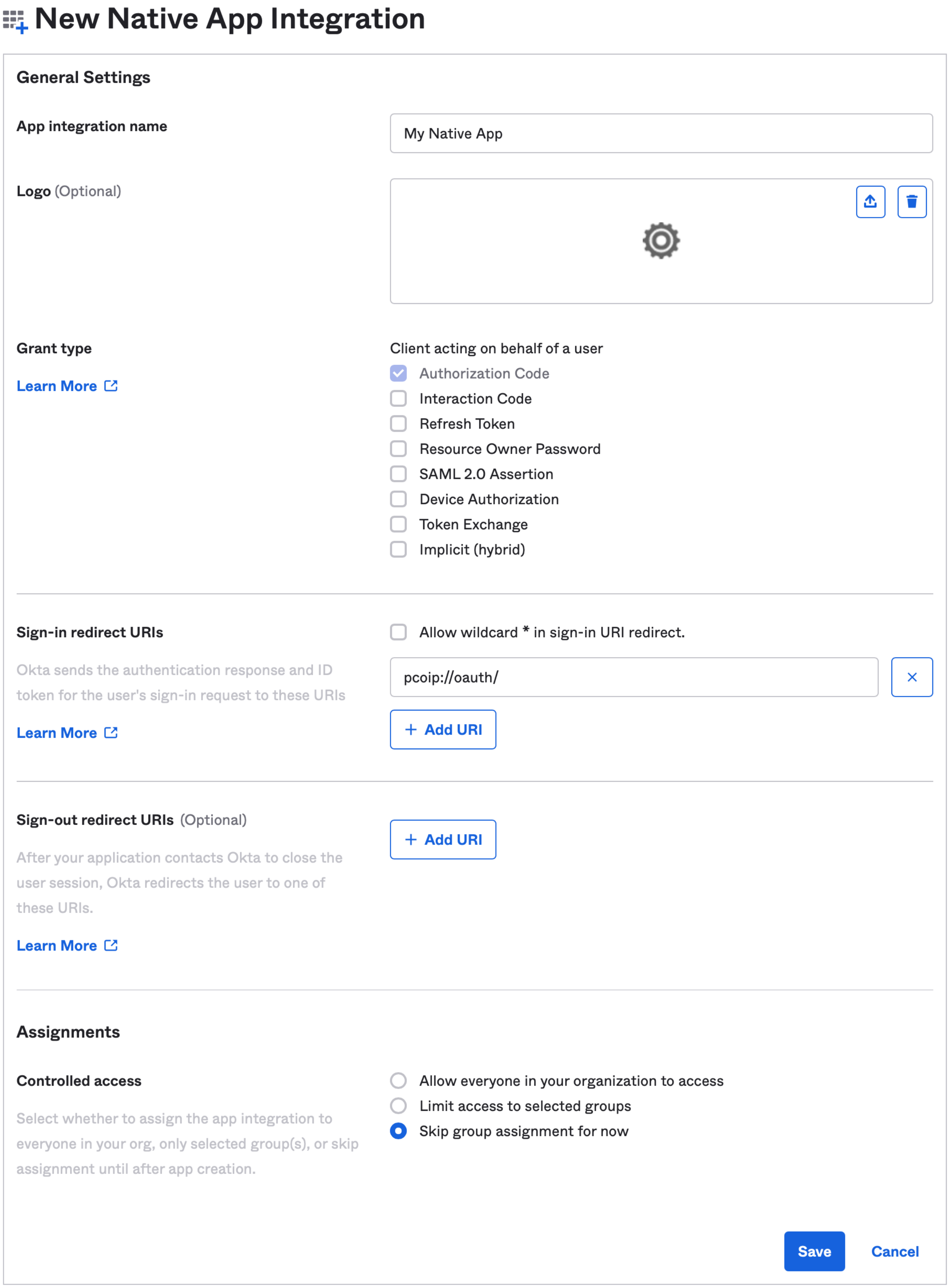
○ Web Application
Server-side applications where authentication and tokens are handled on the server (for example, Go, Java, ASP.Net, Node.js, PHP)

○ Single-Page Application
Single-page web applications that run in the browser where the client receives tokens (for example, Javascript, Angular, React, Vue)

● Native Application
Desktop or mobile applications that run natively on a device and redirect users to a non-HTTP callback (for example, iOS, Android, React Native)

4. Click **Next**.

5. In the **New Native App Integration** window, enter a name in the **App integration name** field.



New Native App Integration

General Settings

App integration name: My Native App

Logo (Optional)

Grant type

Learn More

Client acting on behalf of a user

☑ Authorization Code
□ Interaction Code
□ Refresh Token
□ Resource Owner Password
□ SAML 2.0 Assertion
□ Device Authorization
□ Token Exchange
□ Implicit (hybrid)

Sign-in redirect URIs

Okta sends the authentication response and ID token for the user's sign-in request to these URIs

Learn More

□ Allow wildcard * in sign-in URI redirect.

pcoip://oauth/

+ Add URI

Sign-out redirect URIs (Optional)

After your application contacts Okta to close the user session, Okta redirects the user to one of these URIs.

Learn More

+ Add URI

Assignments

Controlled access

Select whether to assign the app integration to everyone in your org, only selected group(s), or skip assignment until after app creation.

○ Allow everyone in your organization to access
○ Limit access to selected groups
● Skip group assignment for now

6. Check the **Authorization Code** option as Grant type.
7. Enter `pcoip://oauth/` as the **Sign-in redirect URLs**.

8. In the **Assignments** section, select the **Skip group assignment for now** option.
9. Click **Save**.

Okta IDP is now Configured.

HP Anyware supports other IDPs

It may be possible to use these instructions as a guide for configuring other identity providers that support OAuth2. However, those other IdPs may use different terminology and the method of configuration may differ, it is also possible that they may not be compatible.

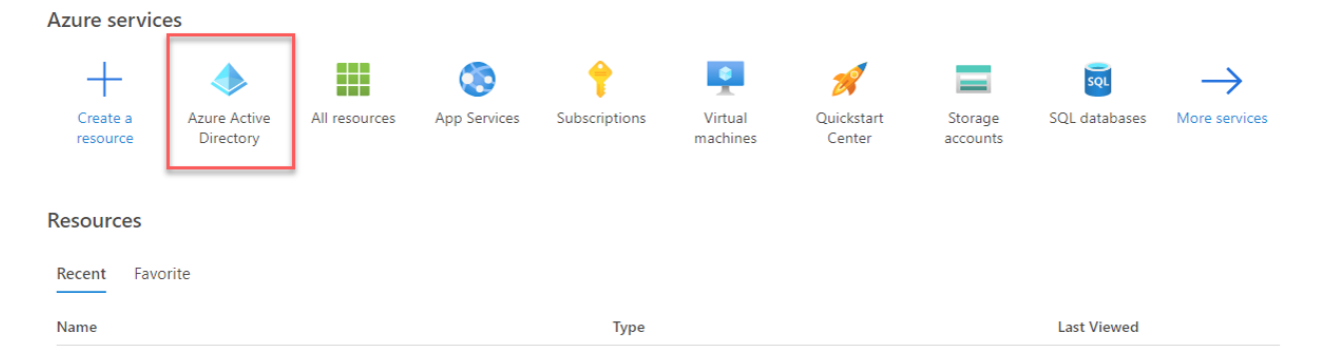
Configuring Azure Active Directory

Azure Active Directory is a third-party identity provider (IdP) that can be configured to work with Anyware Manager. This permits Azure to be used as the source of authentication for any user attempting to connect to a connector in order to get a list of remote workstations to connect to.

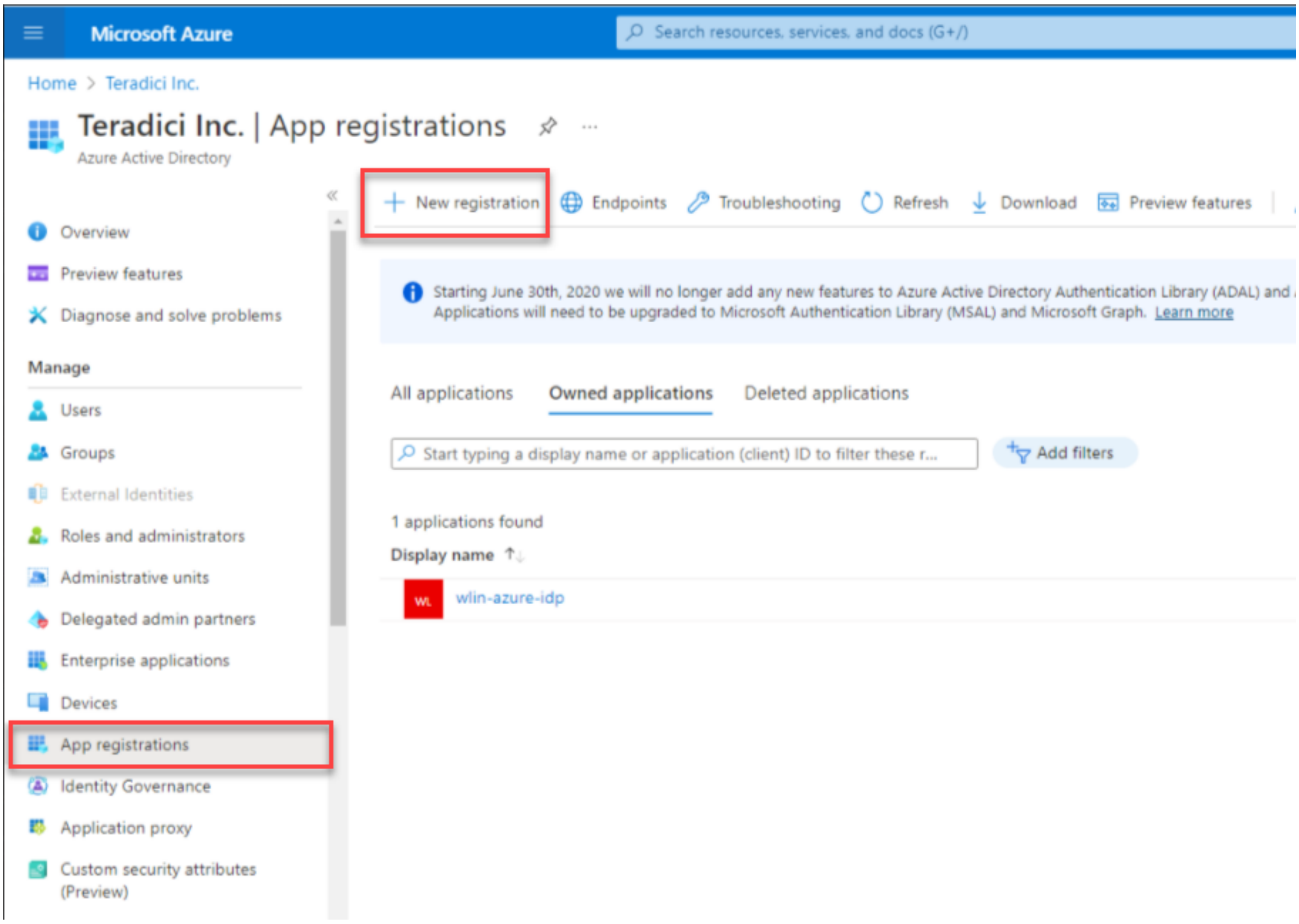
CONFIGURE AZURE ACTIVE DIRECTORY

To configure:

1. Login to Microsoft Azure and Select the **Azure Active Directory** component.



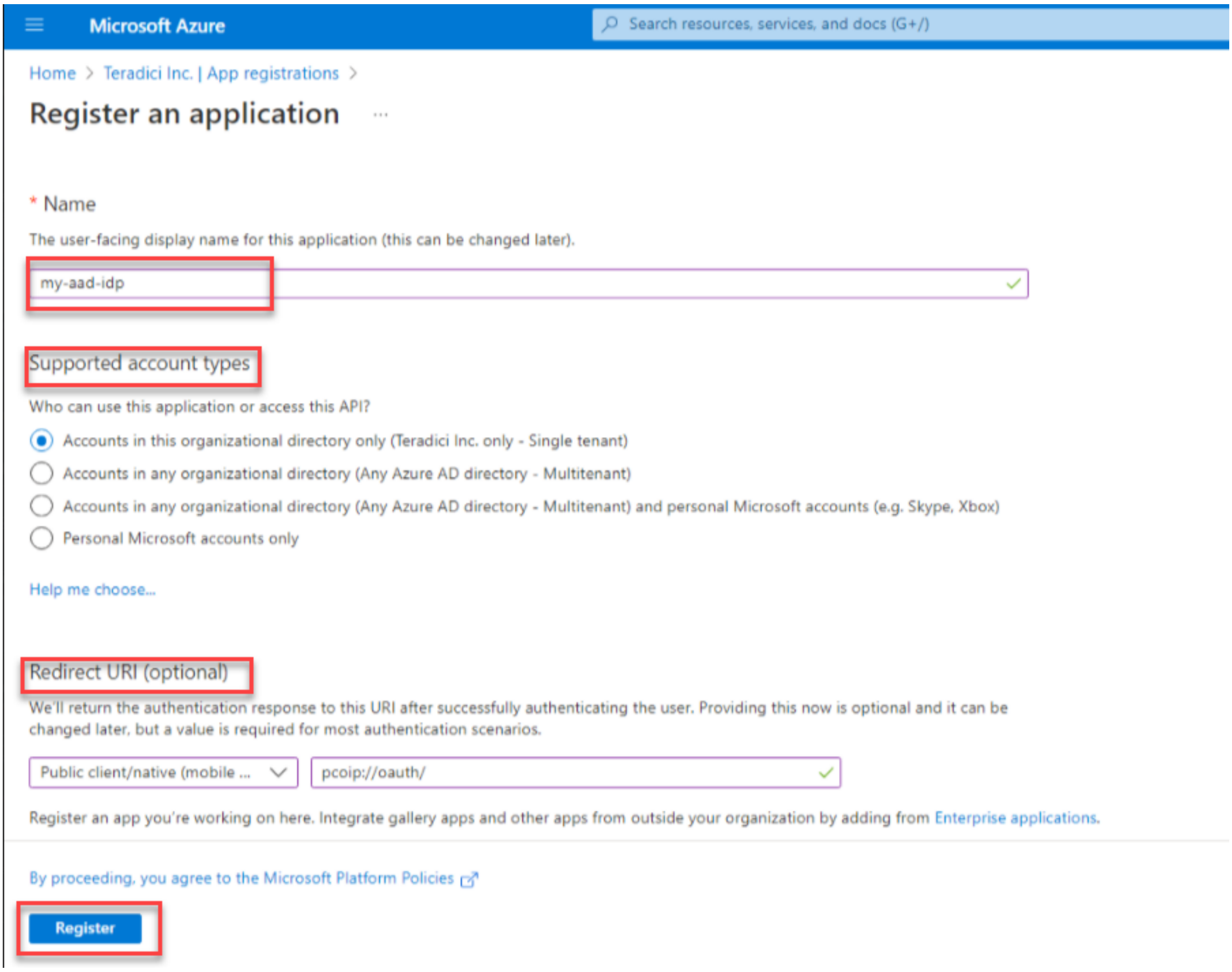
2. From the left pane, select **App registrations** and click **New registration**.



Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

3. Enter the application name, supported account types, and the redirect URL (optional).

4. Click **Register**.



Microsoft Azure
Search resources, services, and docs (G+/)
Home > Teradici Inc. | App registrations >

Register an application

* Name

The user-facing display name for this application (this can be changed later).

my-aad-idp ✓

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (Teradici Inc. only - Single tenant)

○ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

○ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

○ Personal Microsoft accounts only

Help me choose...

Redirect URI (optional)

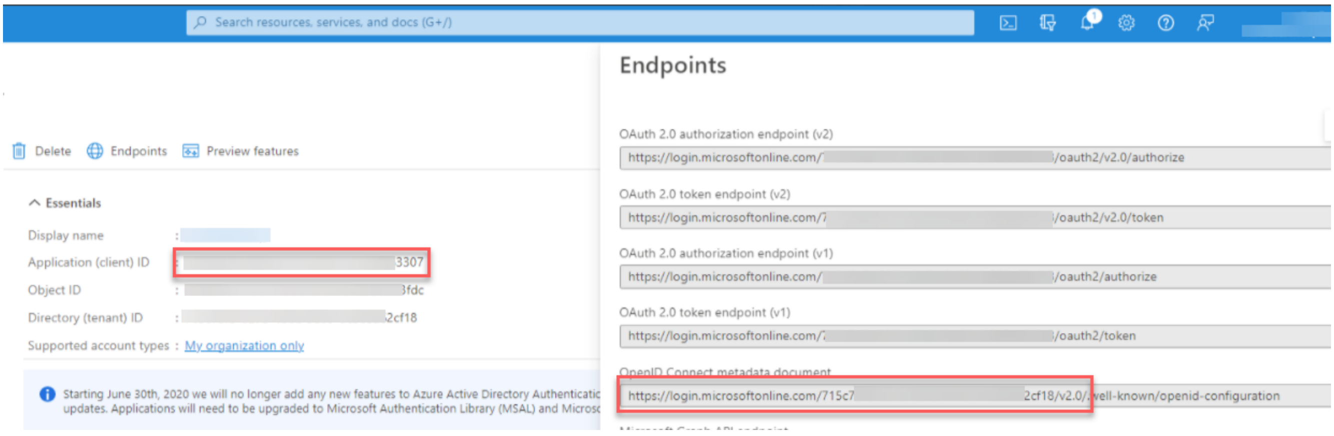
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Public client/native (mobile ... | pcoip://oauth/ ✓

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from Enterprise applications.

By proceeding, you agree to the Microsoft Platform Policies

5. In the **App registrations** page, Click **Endpoints** and make a note of the client ID and the IDP URL for future configurations.



Essentials

Display name : [redacted]

Application (client) ID : [redacted]3307

Object ID : [redacted]3fdc

Directory (tenant) ID : [redacted]2cf18

Supported account types : My organization only

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authenticatic updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsc

Endpoints

OAuth 2.0 authorization endpoint (v2)
https://login.microsoftonline.com/[redacted]/oauth2/v2.0/authorize

OAuth 2.0 token endpoint (v2)
https://login.microsoftonline.com/7[redacted]/oauth2/v2.0/token

OAuth 2.0 authorization endpoint (v1)
https://login.microsoftonline.com/[redacted]/oauth2/authorize

OAuth 2.0 token endpoint (v1)
https://login.microsoftonline.com/7[redacted]/oauth2/token

OpenID Connect metadata document
https://login.microsoftonline.com/715c7[redacted]2cf18/v2.0/.well-known/openid-configuration

Enable Federated Authentication for Anyware Manager

To use the Federated Authentication feature seamlessly you must have the lastest versions of all the HP Anyware software component such as the **Software Client**, **Software Agent**, and the **Anyware Manager** installable. This is not applicable if you are using **Anyware Manager as a Service**. When Federated Authentication is configured, you should enable it from the **Admin Console**.

This has been tested against Okta and ADFS. In most IdPs, the settings include terms like:

- Creating an App Integration
- OAuth2 or OIDC or OpenId Connect sign-in method
- Native Application application type
- The Grant type is Authorization Code
- And the redirect URL would be: pcoip://oauth/

TO ENABLE FEDERATED AUTHENTICATION:

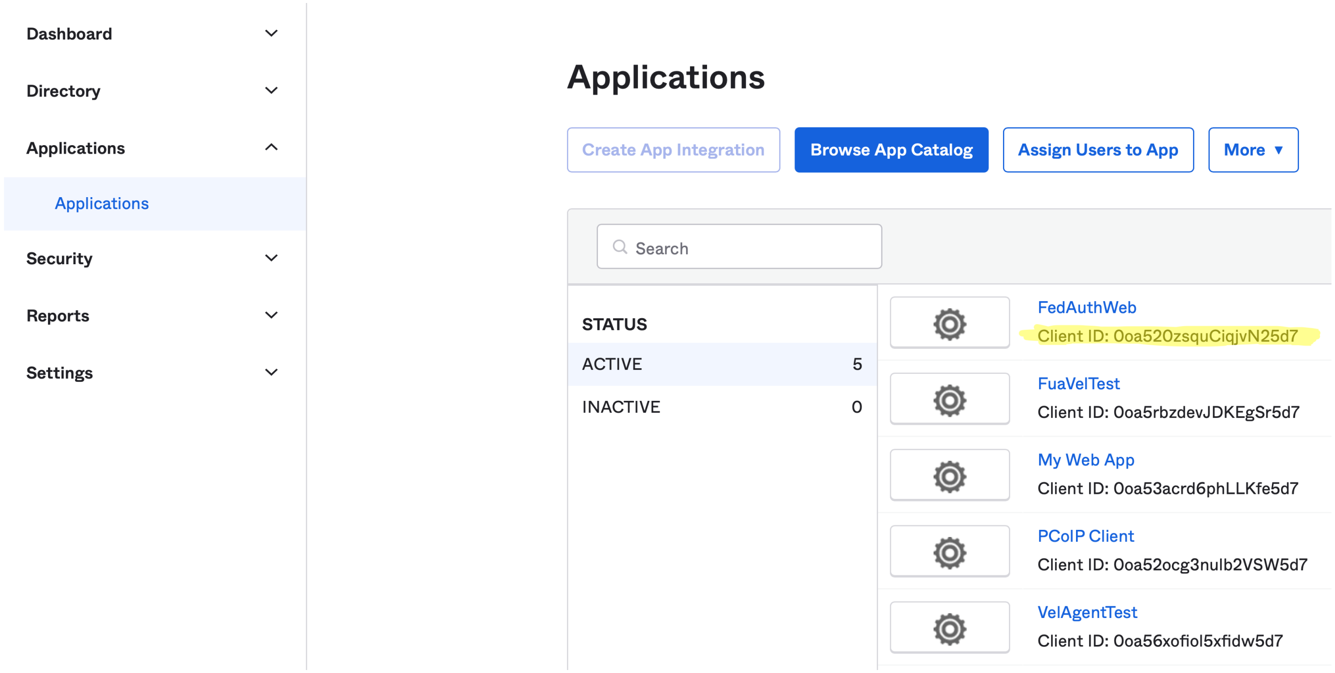
There are two methods of configuring Federated User Authentication in Anyware Manager, through the Admin Console, or the Connector installer. Configuring via the admin console simplifies the connector install flags necessary, and makes it easier to pull the same configuration down to every connector and can be used to override single connectors. Configuring at the connector can be used to have scripted configurations that may change per connector, or when testing the feature out to avoid changing the whole environment.

1. Admin Console configuration

Global Configuration

Federated Authentication can be configured for your entire deployment using the Global configuration method. The steps are:

1. Open the Anyware Manager Admin Console.
2. Select your deployment from the drop down, click the kebab (3 vertically stacked circles) next to your deployment's name and select **Edit deployment**.
3. Open the **Deployment Settings** section and select **Connector Settings**.
4. Enable **OAuth Authentication** and enter in authentication URL and client ID. To obtain the OAuth client ID, you need to login into Okta IDP and navigate to the **Applications** tab from the left pane. Please refer the highlighted area in the image below:



FedAuthWeb
Client ID: 0oa520zsquCiqjvN25d7

FuaVelTest
Client ID: 0oa5rbzdevJDKEgSr5d7

My Web App
Client ID: 0oa53acrd6phLLKfe5d7

PCoIP Client
Client ID: 0oa52ocg3nulb2VSW5d7

VelAgentTest
Client ID: 0oa56xofiol5xfidw5d7

5. Click **Save Configuration**.

Disabling OAuth for a Connector

This enables OAuth Authentication for all Connectors in the deployment. To enable/disable OAuth for a specific connector, please use the following flags during installing/updating the Connector:

```
cloud-access-connector install <other configuration> --id-provider-url
<authorization_url> --enable-oauth <true or false> --oauth-client-id
<client id>
```

Per Connector Configuration

Federated User Authentication can be configured on a per connector basis. This permits you to try it out on a single connector to start to minimize impact to your deployment or to have specific connectors that are used for Federated User Authentication:

1. Select your deployment from the Deployment drop down option.
2. Click **Connectors** from the left pane and select the connector you wish to modify from the table.
3. Select the **Connector Settings** tab and click **Enabled** under OAuth Authentication.
4. Enter the following information into the interface that you obtained from your Identity Provider configuration:
    - Authorization URL

- Client ID

5. Click **Save Configuration**.

After configured the setting in admin console, run the following commands in Connector to apply the setting. - To update a connector to use this setting: - Log into the connector using SSH - Run the command: `sudo cloud-access-connector update <any other configuration flags you use> --pull-connector-config` - To deploy a new connector to use this setting: - Log into the connector using SSH - Run the command: `sudo cloud-access-connector install <any other configuration flags you use> --pull-connector-config`

2. OAuth Configuration for Connectors

You can configure your environment at the connector using the command line interface (CLI) on each connector in your environment. You can choose this option if you are scripting connector deployments or if you wish to avoid storing your identity provider information in the Anyware Manager service.

If you are installing a new connector:

- `sudo cloud-access-connector install […other settings...] --enable-oauth true --id-provider-url https://id.provider.com --oauth-client-id XXXXXXXXX`

If you are configuring an existing connector:

- `sudo cloud-access-connector update […other settings...] --enable-oauth true --id-provider-url https://id.provider.com --oauth-client-id XXXXXXXXX`

Installation Flags

Flag	Type	Description
`--enable-oauth`	Boolean	Enables Oauth authentication. (Default=False)
`--id-provider-url`	String	Sets the identity provider URL. Example: `--id-provider-url https://provider-1234567890.okta.com`. This flag is required if `--enable-oauth is true`.
`--oauth-client-id`	String	Gets the Client ID from the Identity Provider. This flag is required if `--enable-oauth is true`.
`--fa-url`	String	The Federated Auth Broker URL. for example https://cac-vm-fqdn:port
`--oauth-flow-code`	String	Specify the oauth flow / grant type (default "OAUTH_FLOW_CODE_WITH_PKCE"). "OAUTH_FLOW_CODE_WITH_PKCE" is the only supported oauth flow for now
`--enable-entitlements-by-upn`	Boolean	Enables/Disables searching entitlements by UPN. This flag is required to be true, if `--enable-oauth is true`.

Single Sign-On

Single Sign-On Overview

Federated User Authentication with Single Sign-On enables organizations to use their own Identity Provider (IDP) as the source to verify the identity and to authenticate a user before permitting them to select remote workstation. Once the desired workstation is selected, the user does not need to authenticate and directly connects to the remote workstation.

This has been tested against Okta and ADFS. In most IDPs, the settings include terms like:

- Creating an App Integration
- OAuth2 or OIDC or OpenId Connect sign-in method
- Native Application application type
- The Grant type is Authorization Code
- And the redirect URL would be: pcoip://oauth/

PREREQUISITES

To use the Federated Authentication Functionality, you must meet the following criteria:

- Anyware Manager 23.04 or later
- HP PCoIP Client version 23.01.0 or later
- HP PCoIP Windows Agent 23.01.0 or later (SSO is not supported on Linux or MacOS in 23.01)
- An Identity Provider that supports OAuth2
- Ubuntu Connector v147 or later with access to an Identity Provider

POST CONFIGURATION USER WORKFLOW

After completing the Federated Authentication configuration, the user workflow is as follows:

- You can open the PCoIP Client and select a Connector or a broker from the list of connections.
- The default web browser opens to a login page for the respective Identity Provider for user authentication.
- The PCoIP Client requests another layer of user authentication to display the list of available remote workstations.

- The PCoIP Client presents the user with their list of desktops or pools to select from.
- The user enters their PCoIP session with their remote desktop.
- The PCoIP Session is initiated with the remote desktop.

⚠ **Configuring IDP for Single Sign-On**

Before you start preparing for Single Sign-On, ensure that you configure an IDP to enable Federated Authentication. We recommend configuring Okta or Azure Active Directory as your identifty provider.

- For more information on Okta IDP configuration, see Configuring Okta IDP.
- For more information on Azure Active Directory configuration, see Configuring Azure Active Directory.

SSO for Anyware Manager

Single Sign-On supports alternative credential. Should the PCoIP Agent not support Federated User Authentication, user is prompted to enter username and password. Single Sign-On is not publicly available and we anticipate the configuration method to change significantly in future version.

Preparing for Single Sign-On

Configuring Single Sign-On enables a user to connect into their desktop having only authenticated once, and that authentication is used to provide them both their list of desktops and to log into the remote workstation.

> ⚠ **Certificate Authority required for Single Sign-On**
>
> The instructions assume you have a Certification Authority (CA) in your environment and your remote workstations use it to verify certificates. If you do not have a Certification Authority, See https://learn.microsoft.com/en-us/windows-server/networking/core-network-guide/cncg/server-certs/install-the-certification-authority. Instructions for generating a signed intermediate certificate and private key can vary from CA to CA, or even between versions of the same CA. Please reference your CA documentation for further instructions.

ENROLLMENT OPTIONS

In order to support Single Sign-On, the Connector must be able to obtain or generate a certificate to provide to the PCoIP Agent to log the user in. Two methods are available to enable this:

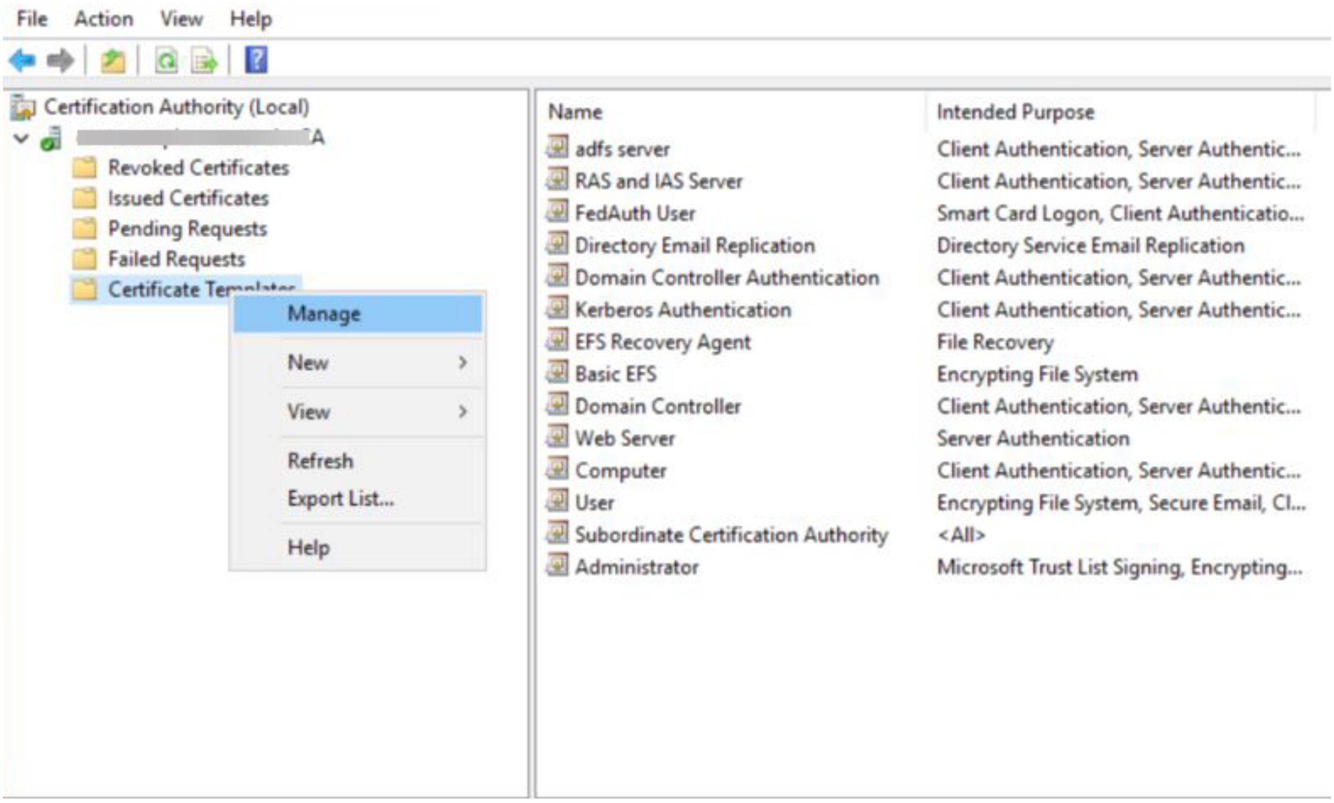
- By Active Directory Certification Authority Web Enrollment
- By private key and certificate of the Certification Authority

By Active Directory Certification Authority Web Enrollment

> **Note: The CA certificate and key could be used by malicious actors to impersonate valid devices on your network, impacting confidentiality, and integrity. We recommend following the Active Directory Certification Authority Web Enrollment method if your connector has an external IP address. If you export your domain's CA certificate and key, ensure you keep all copies secure (including local).**

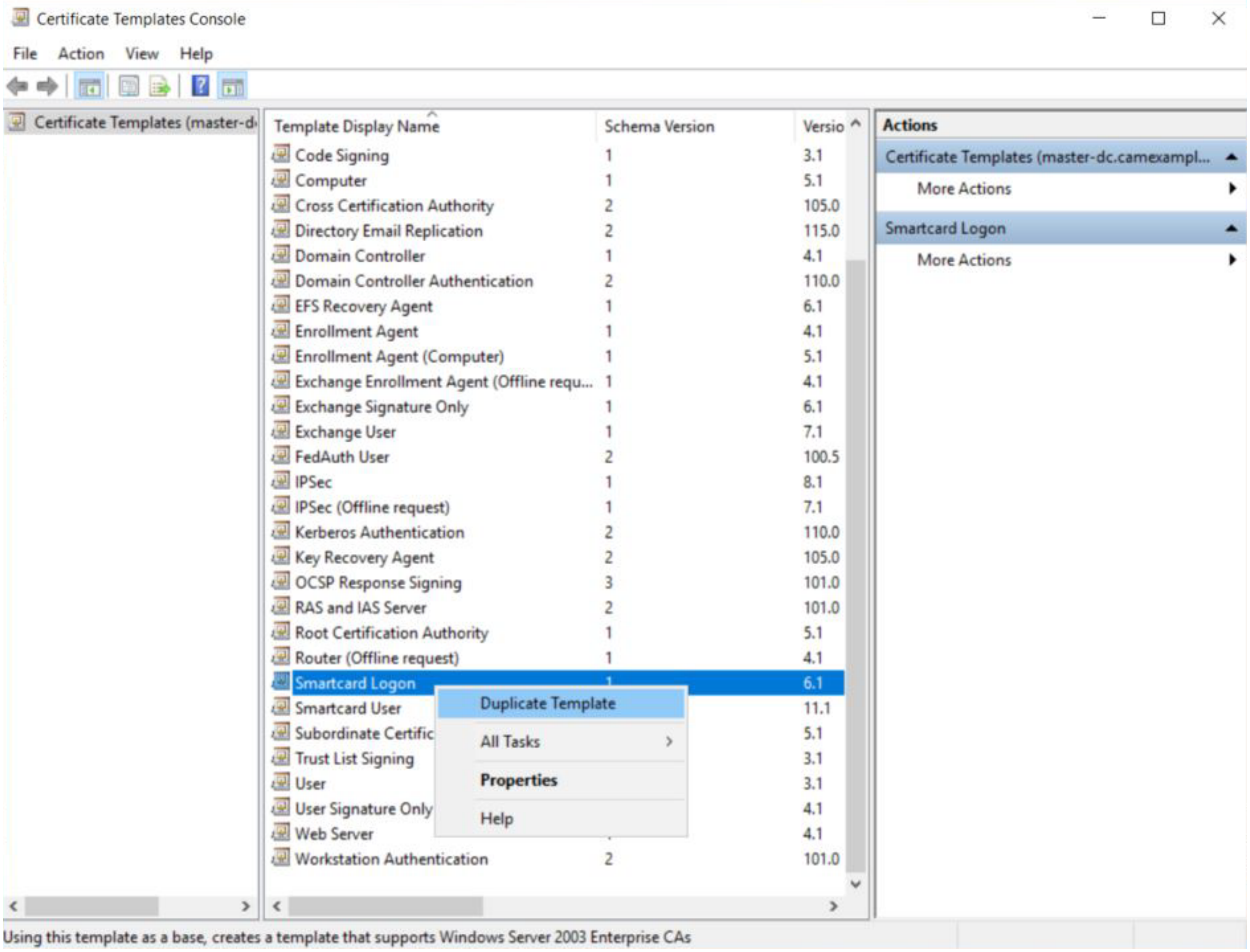
Create Certificate Authority Template

1. Log on to the Certificate Authority resource.
2. Open Certificate Authority MMC (`certsrv.msc`).
3. Right click the **Certificate Templates** and select **Manage**.



Name	Intended Purpose
adfs server	Client Authentication, Server Authentic...
RAS and IAS Server	Client Authentication, Server Authentic...
FedAuth User	Smart Card Logon, Client Authenticatio...
Directory Email Replication	Directory Service Email Replication
Domain Controller Authentication	Client Authentication, Server Authentic...
Kerberos Authentication	Client Authentication, Server Authentic...
EFS Recovery Agent	File Recovery
Basic EFS	Encrypting File System
Domain Controller	Client Authentication, Server Authentic...
Web Server	Server Authentication
Computer	Client Authentication, Server Authentic...
User	Encrypting File System, Secure Email, Cl...
Subordinate Certification Authority	<All>
Administrator	Microsoft Trust List Signing, Encrypting...

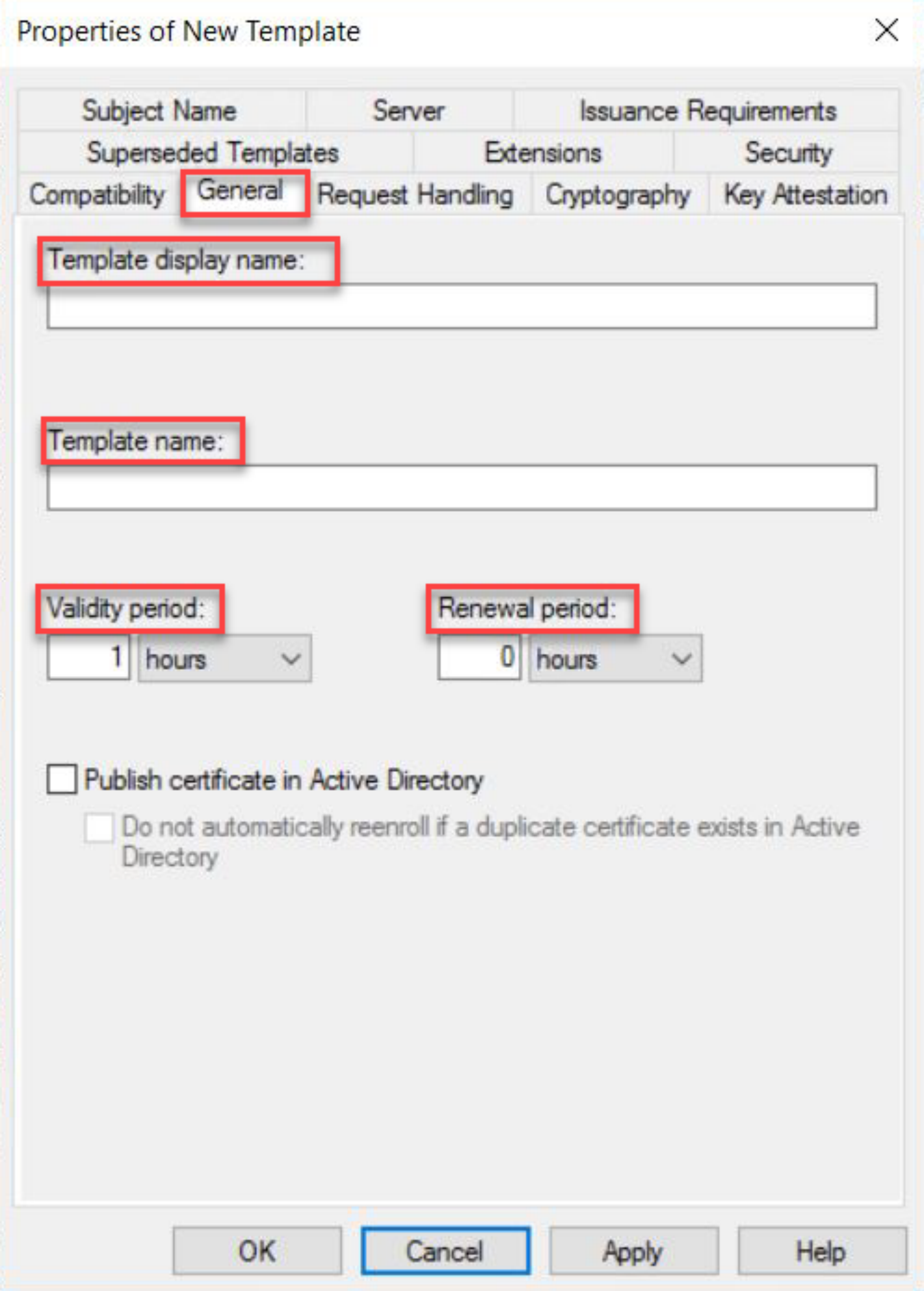
4. **Certificates Templates Console** window is now open. Right click **Smartcard User** and select **Duplicate Template**.



Template Display Name	Schema Version	Versio
Code Signing	1	3.1
Computer	1	5.1
Cross Certification Authority	2	105.0
Directory Email Replication	2	115.0
Domain Controller	1	4.1
Domain Controller Authentication	2	110.0
EFS Recovery Agent	1	6.1
Enrollment Agent	1	4.1
Enrollment Agent (Computer)	1	5.1
Exchange Enrollment Agent (Offline requ...	1	4.1
Exchange Signature Only	1	6.1
Exchange User	1	7.1
FedAuth User	2	100.5
IPSec	1	8.1
IPSec (Offline request)	1	7.1
Kerberos Authentication	2	110.0
Key Recovery Agent	2	105.0
OCSP Response Signing	3	101.0
RAS and IAS Server	2	101.0
Root Certification Authority	1	5.1
Router (Offline request)	1	4.1
Smartcard Logon	1	6.1
Smartcard User		11.1
Subordinate Certific		5.1
Trust List Signing		3.1
User		3.1
User Signature Only		4.1
Web Server		4.1
Workstation Authentication	2	101.0

Using this template as a base, creates a template that supports Windows Server 2003 Enterprise CAs

5. Navigate to the **General** tab and rename the template to a desired name and take note of the name as it is required during Connector installation. Change the **Validity Period** and **Renewal Period** to minimum such as 1 hours and 0 hours respectively.



Template display name:

Template name:

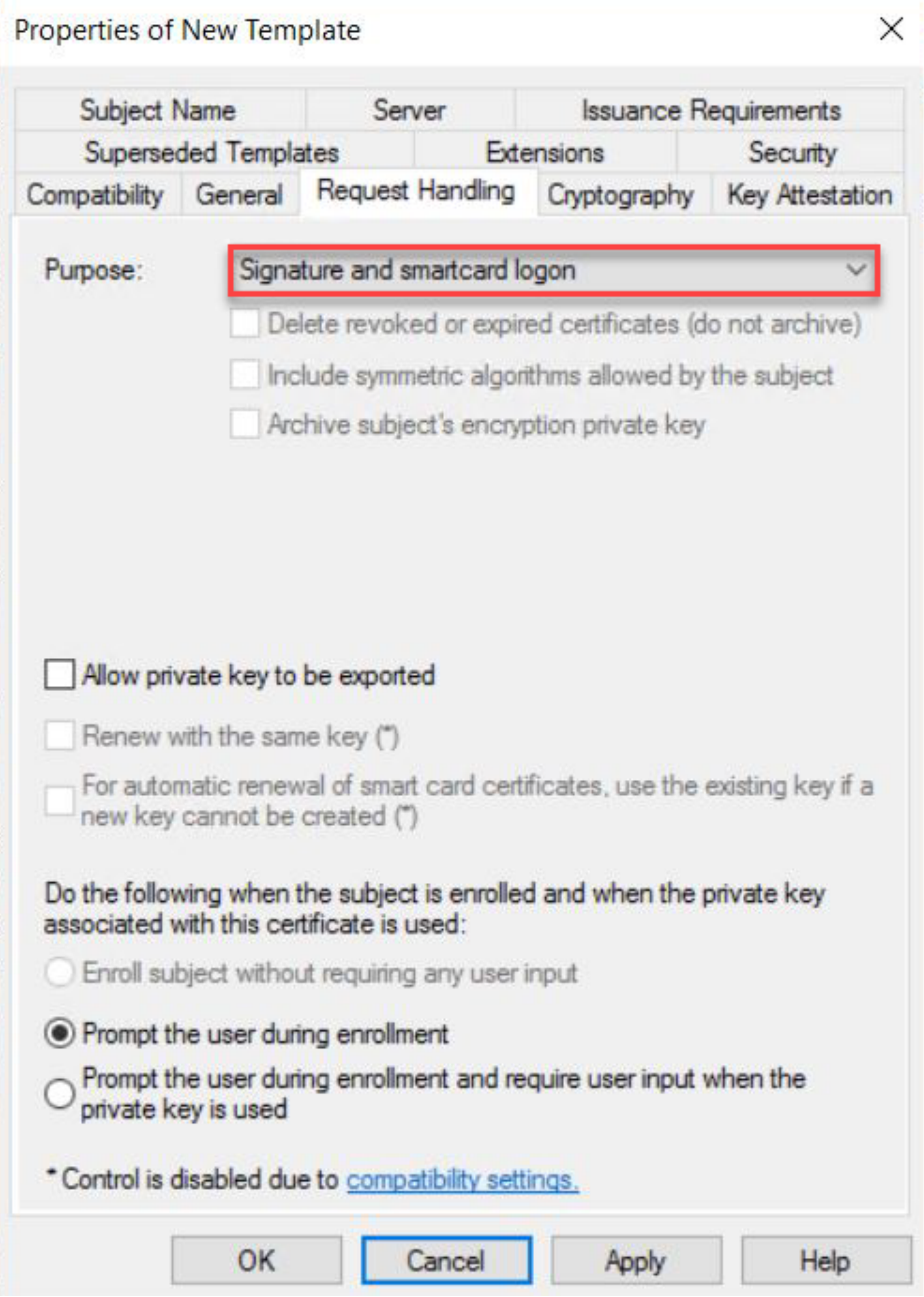
Validity period: 1 hours

Renewal period: 0 hours

□ Publish certificate in Active Directory

□ Do not automatically reenroll if a duplicate certificate exists in Active Directory

6. Navigate to **Request Handling** tab and change the purpose to **Signature and smartcard logon**. The **Certificate Templates** information box appears. Click **Yes** to close it.



Properties of New Template

Purpose: Signature and smartcard logon

□ Delete revoked or expired certificates (do not archive)

□ Include symmetric algorithms allowed by the subject

□ Archive subject's encryption private key

□ Allow private key to be exported

□ Renew with the same key (*)

□ For automatic renewal of smart card certificates, use the existing key if a new key cannot be created (*)

Do the following when the subject is enrolled and when the private key associated with this certificate is used:

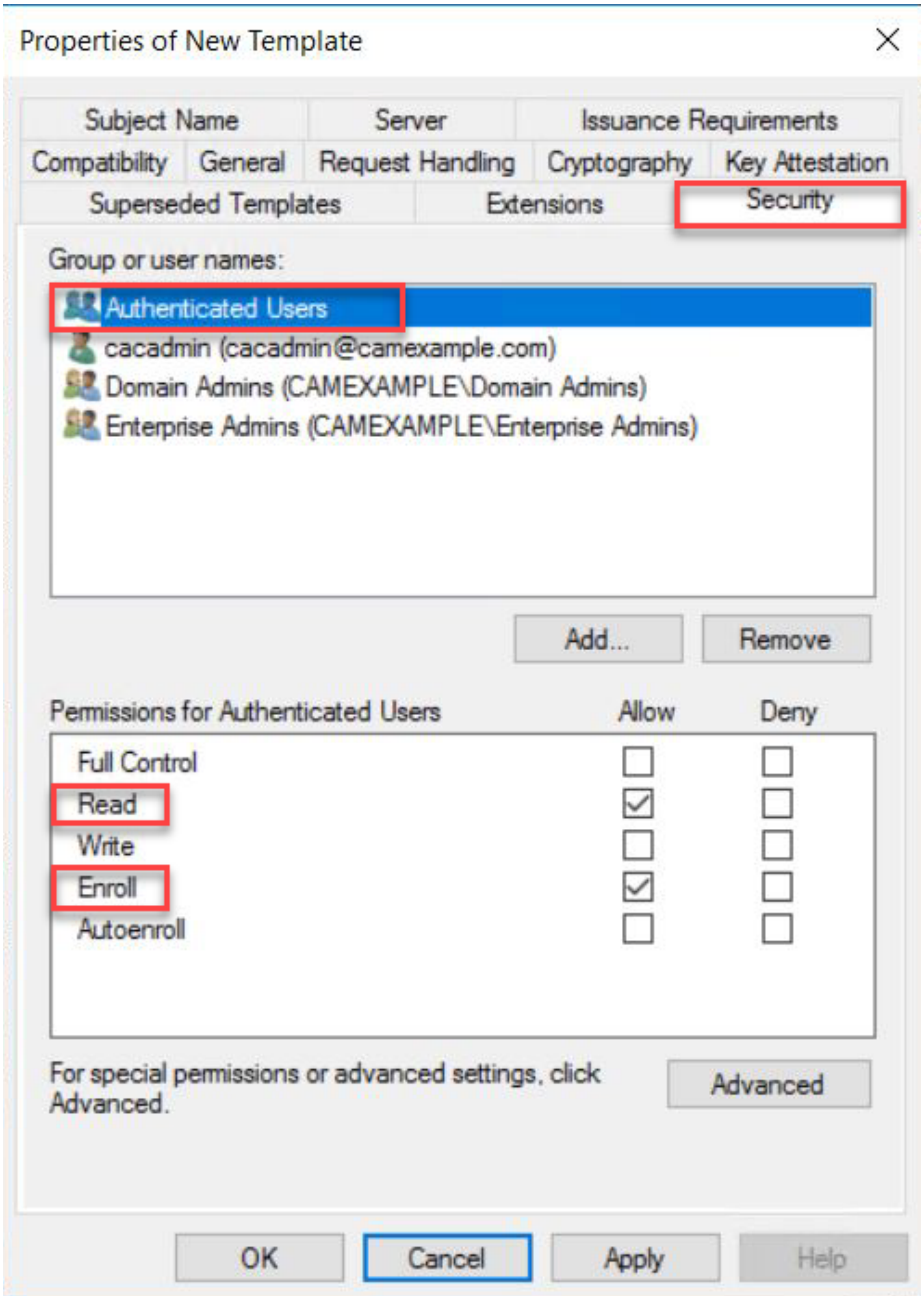
○ Enroll subject without requiring any user input

● Prompt the user during enrollment

○ Prompt the user during enrollment and require user input when the private key is used

* Control is disabled due to compatibility settings.

7. Navigate to **Security** tap and select **Read** and **Enroll** as **Allow** for **Authenticated Users**.



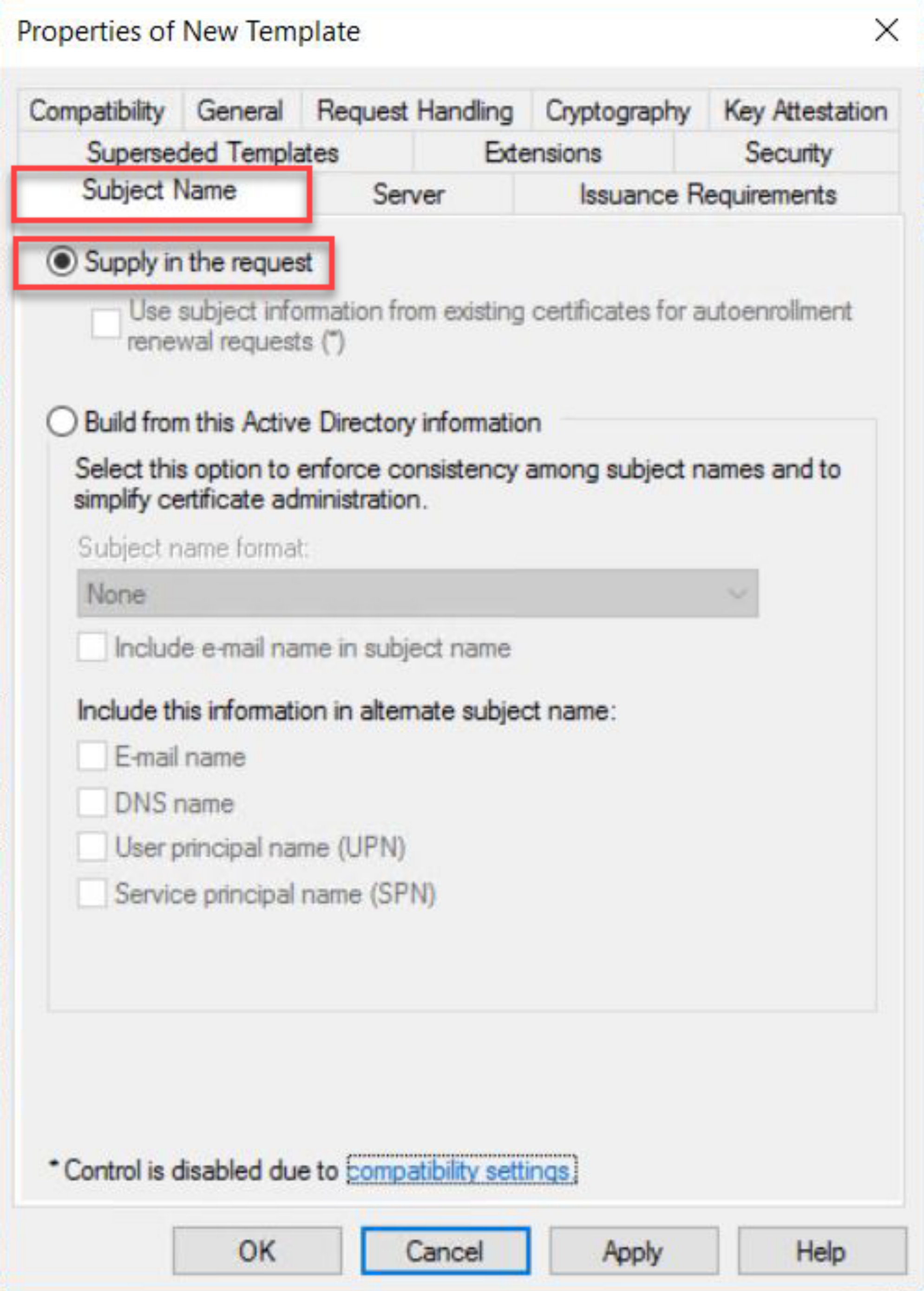
Group or user names:

- Authenticated Users
- cacadmin (cacadmin@camexample.com)
- Domain Admins (CAMEXAMPLE\Domain Admins)
- Enterprise Admins (CAMEXAMPLE\Enterprise Admins)

Permissions for Authenticated Users	Allow	Deny
Full Control	□	□
Read	☑	□
Write	□	□
Enroll	☑	□
Autoenroll	□	□

For special permissions or advanced settings, click Advanced.

8. Navitage to **Subject Name** tab and select **Supply in the request**. A warning text box appears and click **OK** to close the warning text box.



● Supply in the request

□ Use subject information from existing certificates for autoenrollment renewal requests (*)

○ Build from this Active Directory information

Select this option to enforce consistency among subject names and to simplify certificate administration.

Subject name format:

None

□ Include e-mail name in subject name

Include this information in alternate subject name:

□ E-mail name

□ DNS name

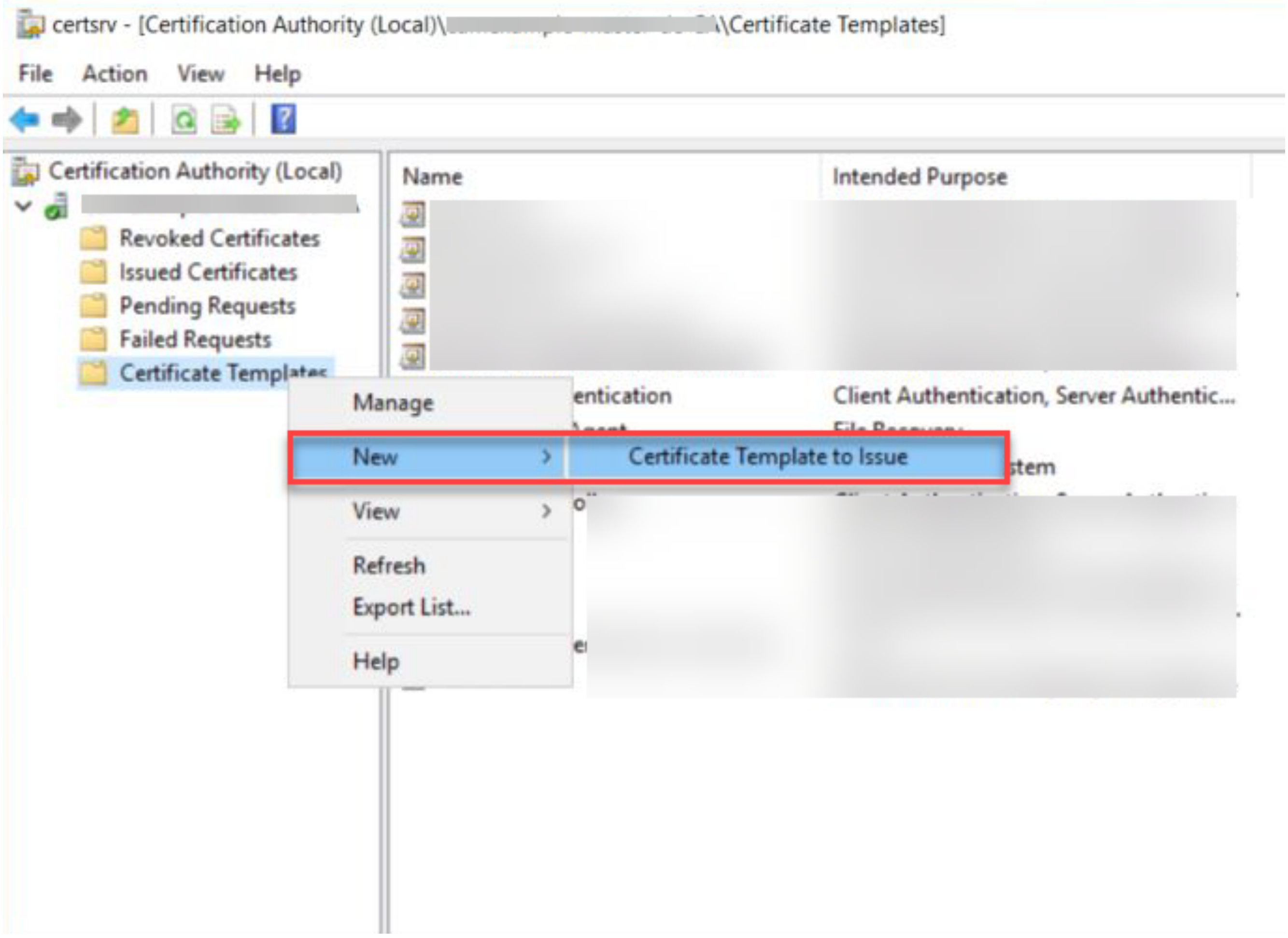
□ User principal name (UPN)

□ Service principal name (SPN)

* Control is disabled due to compatibility settings.

9. Click **Apply** and then **OK** to finish creating the template.

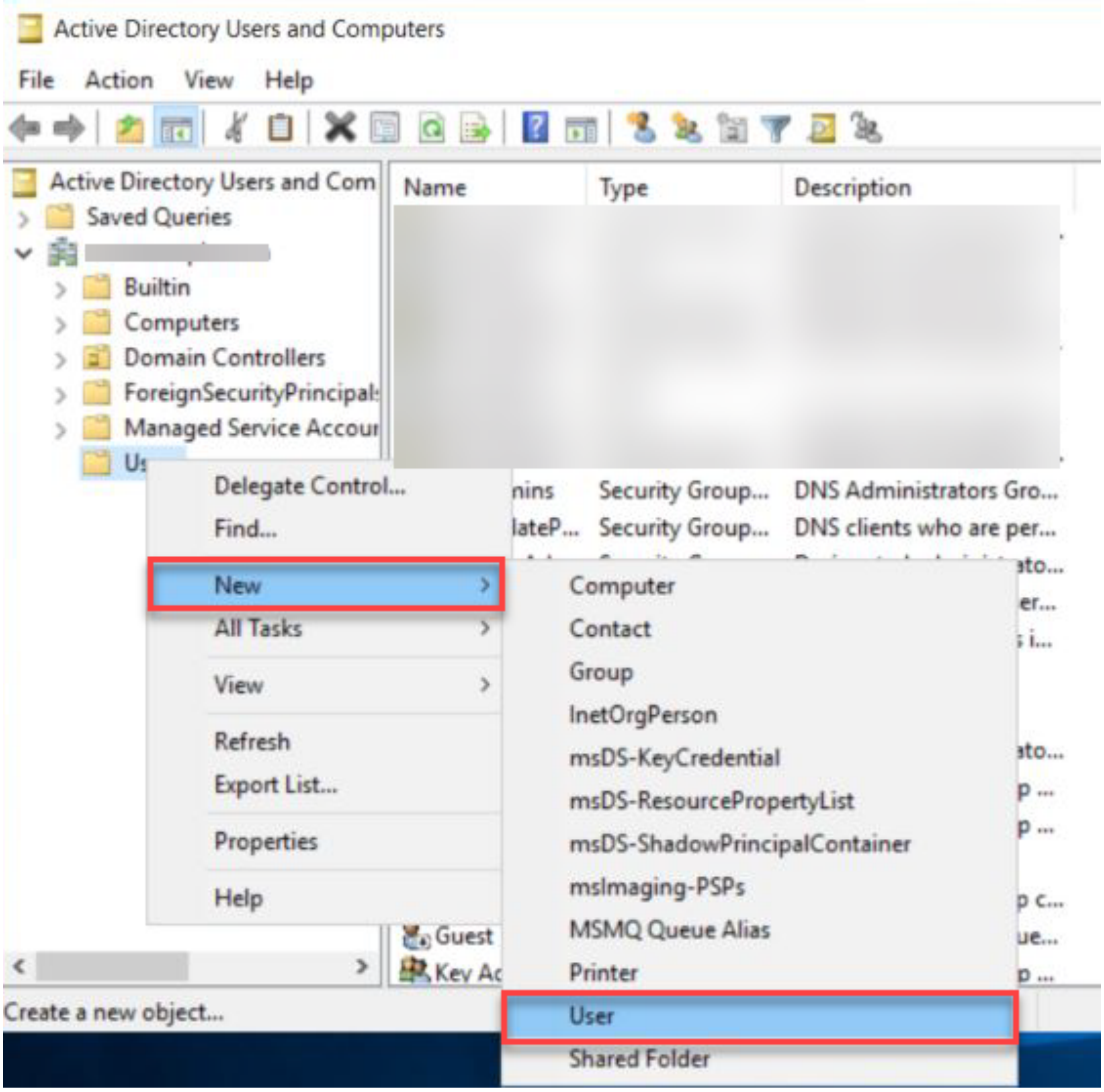
10. Right click the **Certificate Templates**, select **New** and click **Certificate Template to Issue**.



11. Select the template created above and click **OK** to add the template to CA.

Create a user who will have the permission to request Certificate

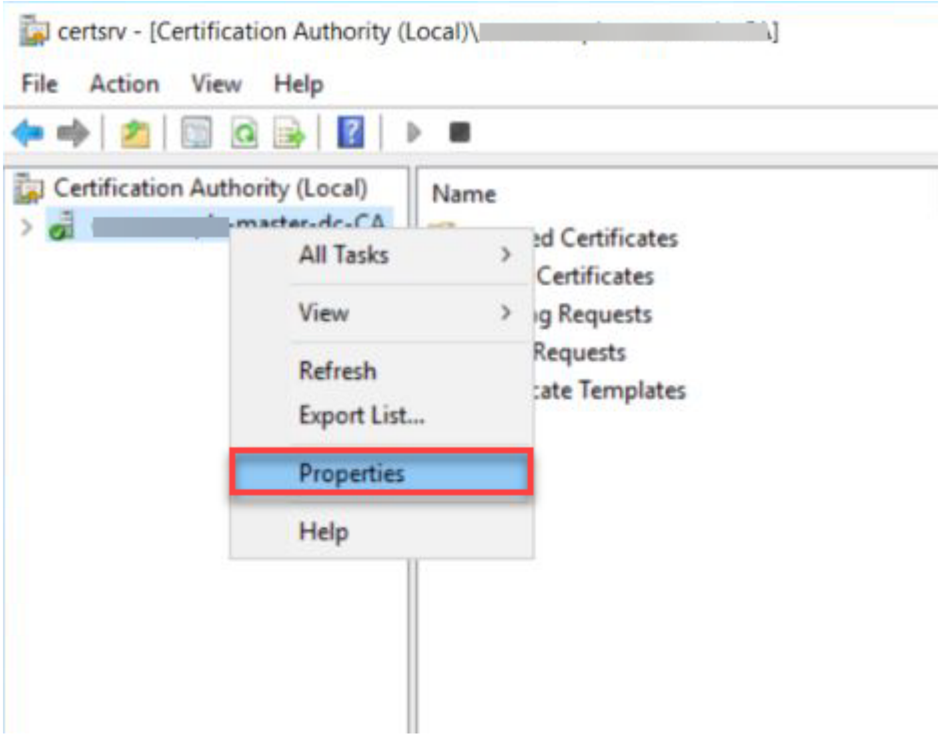
1. Logon to Domain Controller, open **Active Directory Users and Computers**.
2. Go to **$Domain** and select **Users**.
3. Right click **Users** select **New** and click **Use**.



4. Enter the required information such as First name, Last name, User Logon name ...etc and click on **Next**.
5. Enter the Password for the user and click **Next**.
6. Note the username and password as it is required during Connector installation.
7. Click on **Finish** to create the user.

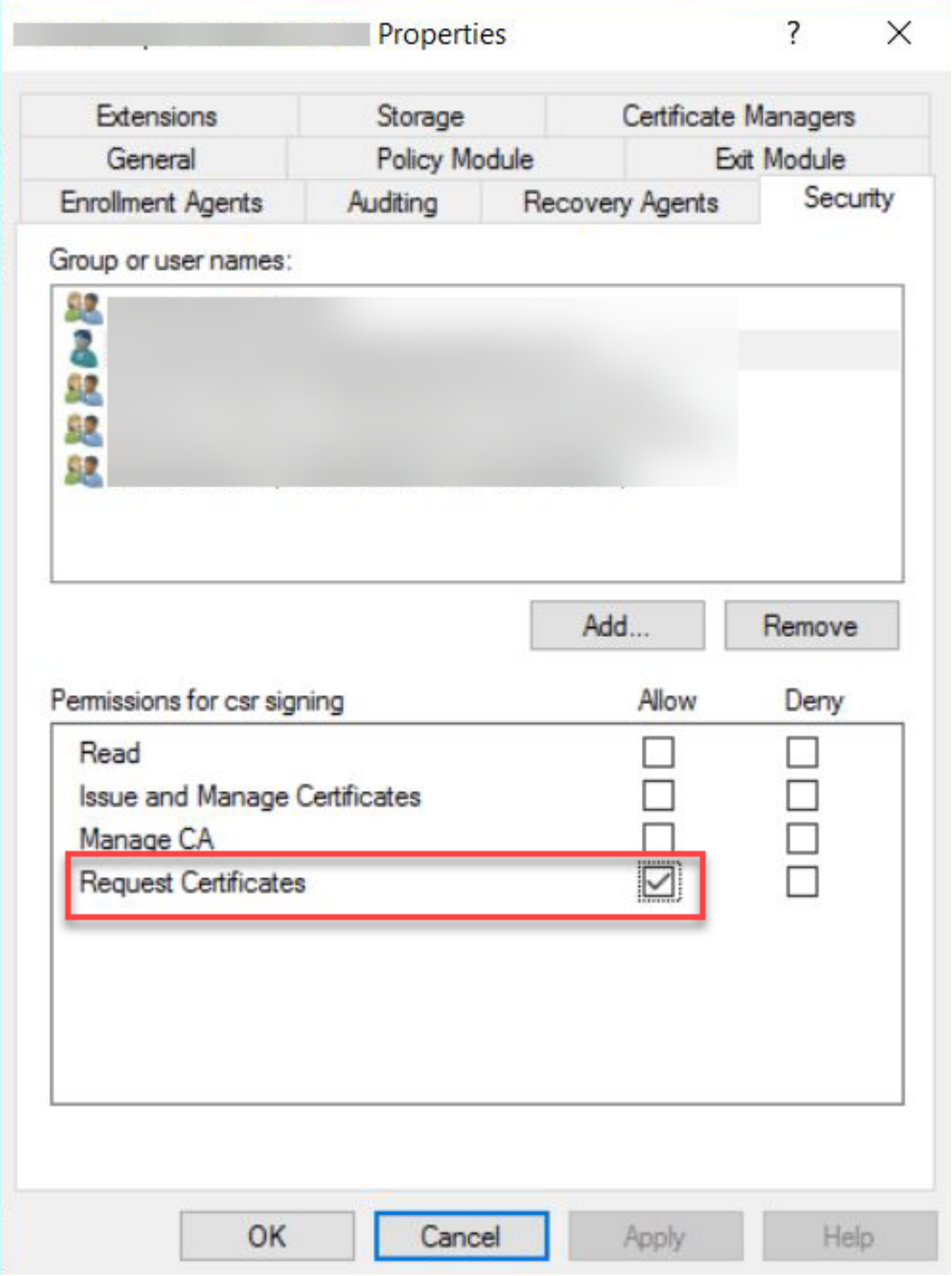
Grant user the permission to request Certificate

1. Log on to the Certificate Authority machine
2. Open Certificate Authority MMC (`certsrv.msc`)
3. Right click the CA and select **Properties**.



4. Navigate to **Security** tab and click **Add...** and add the user created above.

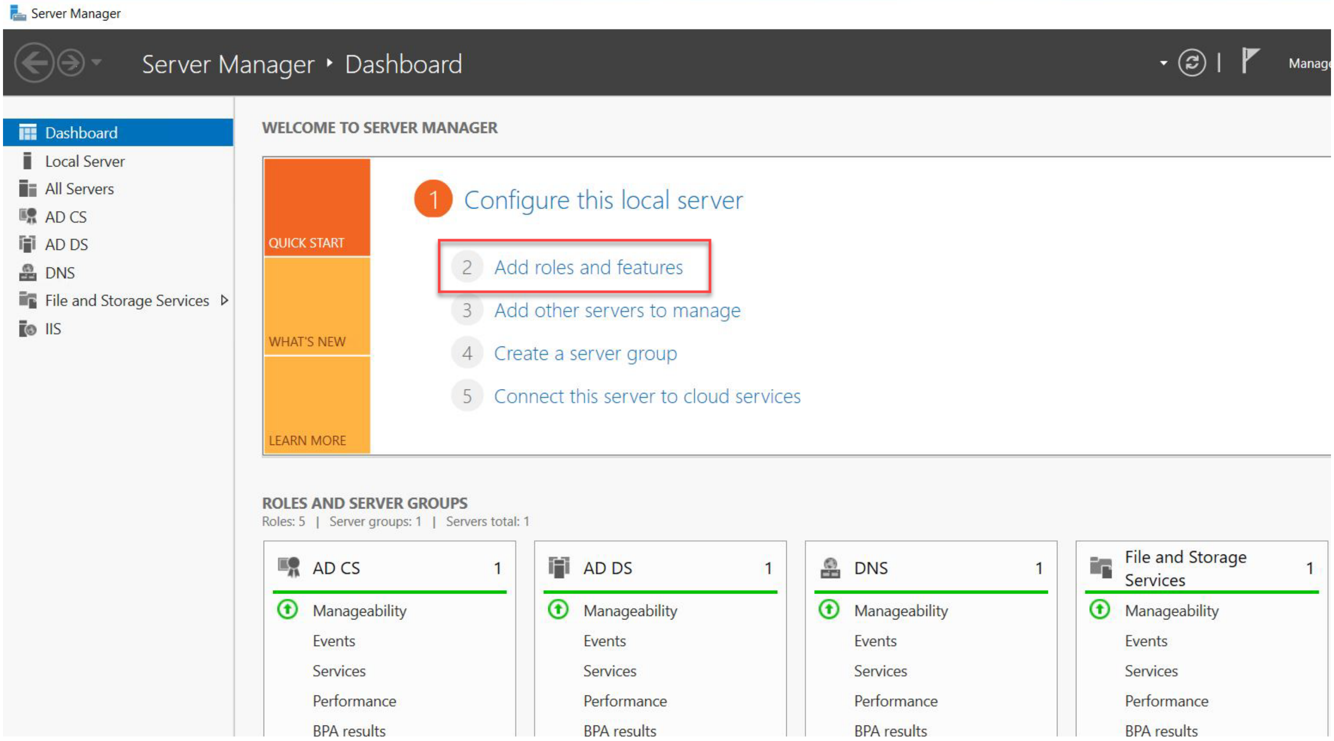
5. Ensure the user added is allowed to **Request Certificates**.



Permissions for csr signing	Allow	Deny
Read	□	□
Issue and Manage Certificates	□	□
Manage CA	□	□
Request Certificates	☑	□

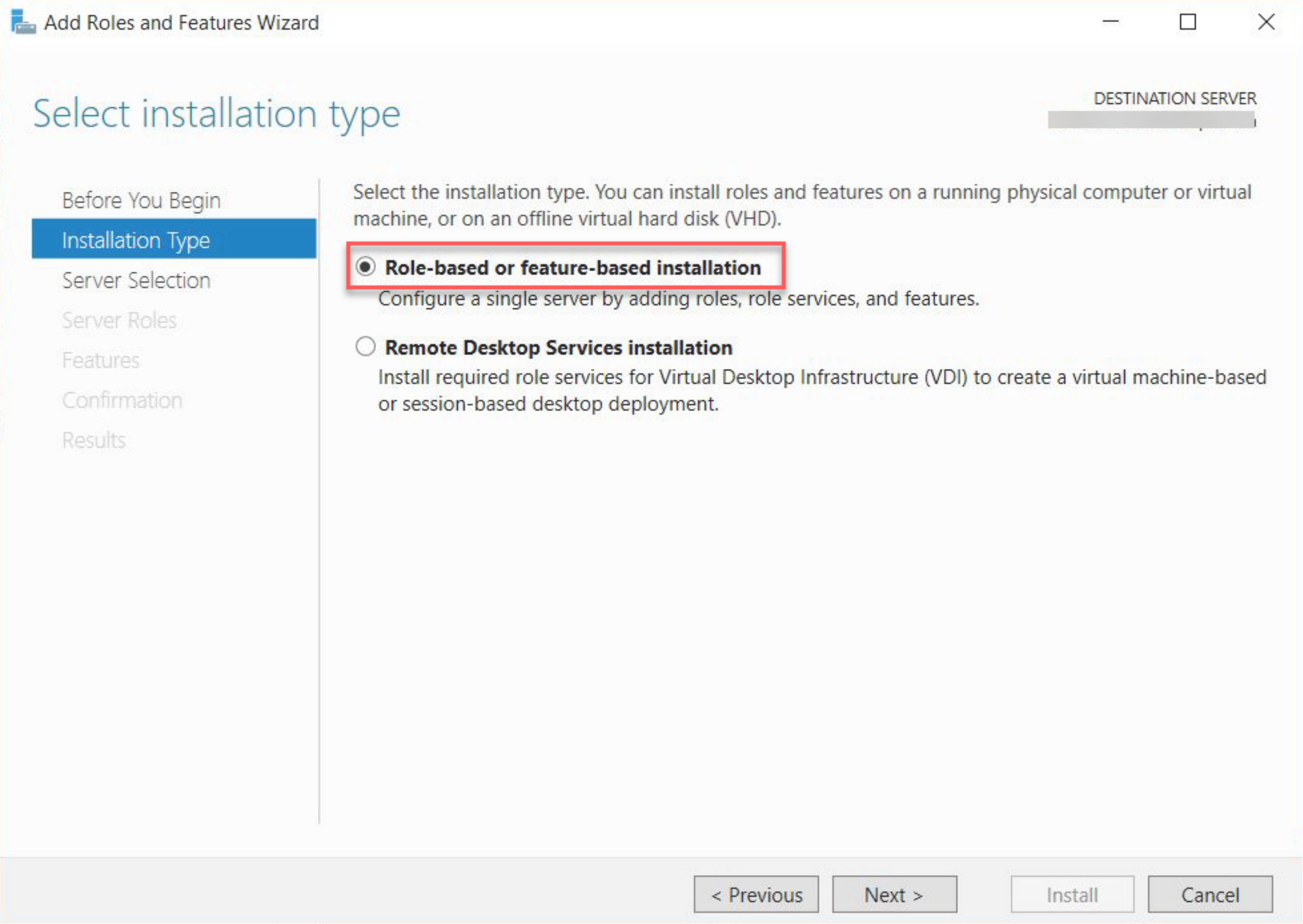
Set up Active Directory Certification Authority Web Enrollment

1. On a Windows Server machine where the Certification Authority is installed, select **Add roles and features** on the Server Manager window.



2. Click **Next** on the **Before you begin** window.

3. Select **Role-based or feature-based installation** on the **Installation Type** page.



[redacted]

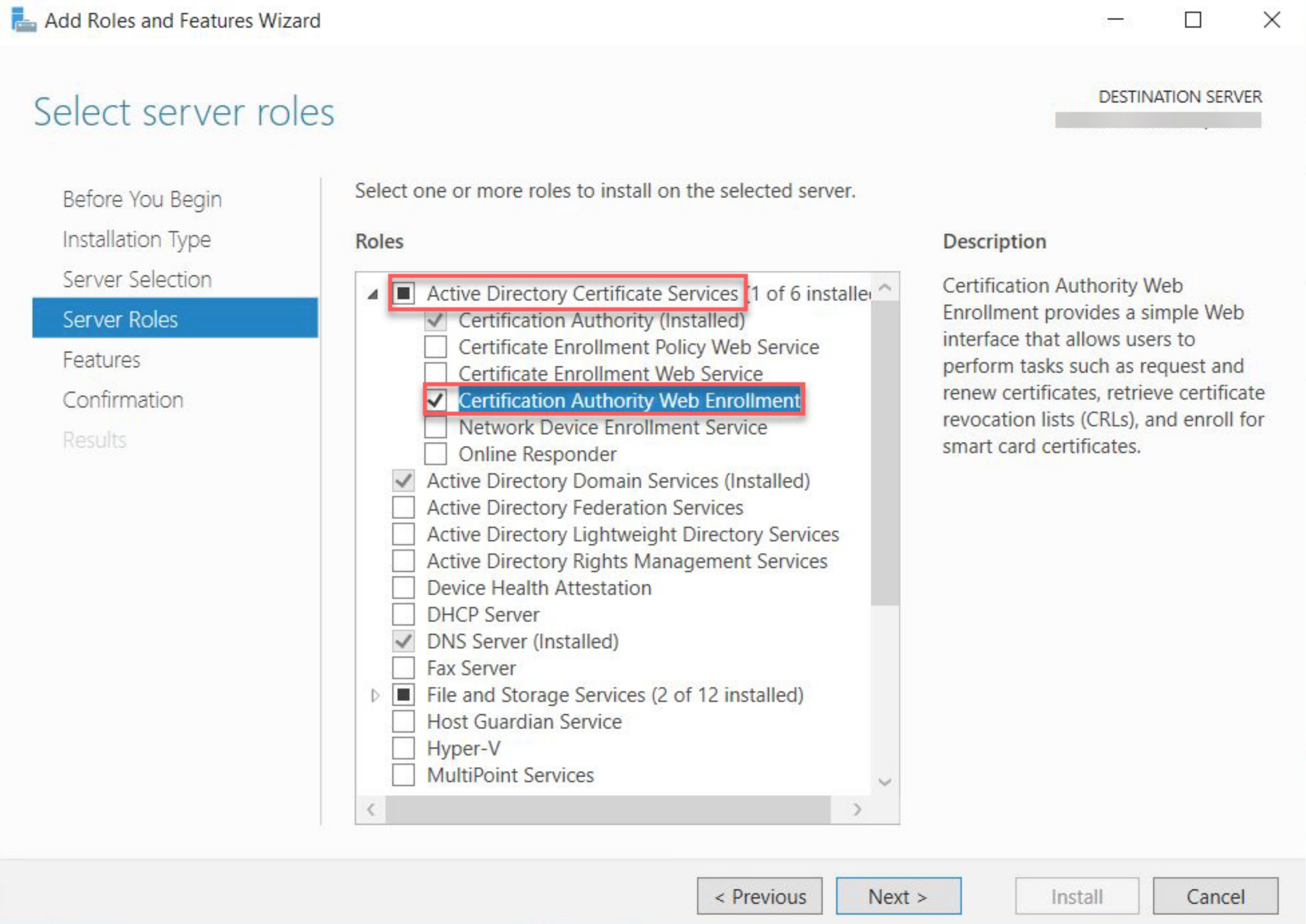
Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

● **Role-based or feature-based installation**
Configure a single server by adding roles, role services, and features.

○ **Remote Desktop Services installation**
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

4. Select a server from the server pool and press **Next**.

5. On the **Server Roles** page, expend **Active Directory Certificate Services** section, and select **Certificate Authority Web Enrollment**. Click **Next**.



[redacted]

Select one or more roles to install on the selected server.

Roles

- ■ Active Directory Certificate Services (1 of 6 installe
  - ☑ Certification Authority (Installed)
  - □ Certificate Enrollment Policy Web Service
  - □ Certificate Enrollment Web Service
  - ☑ Certification Authority Web Enrollment
  - □ Network Device Enrollment Service
  - □ Online Responder
- ☑ Active Directory Domain Services (Installed)
- □ Active Directory Federation Services
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Device Health Attestation
- □ DHCP Server
- ☑ DNS Server (Installed)
- □ Fax Server
- ■ File and Storage Services (2 of 12 installed)
- □ Host Guardian Service
- □ Hyper-V
- □ MultiPoint Services

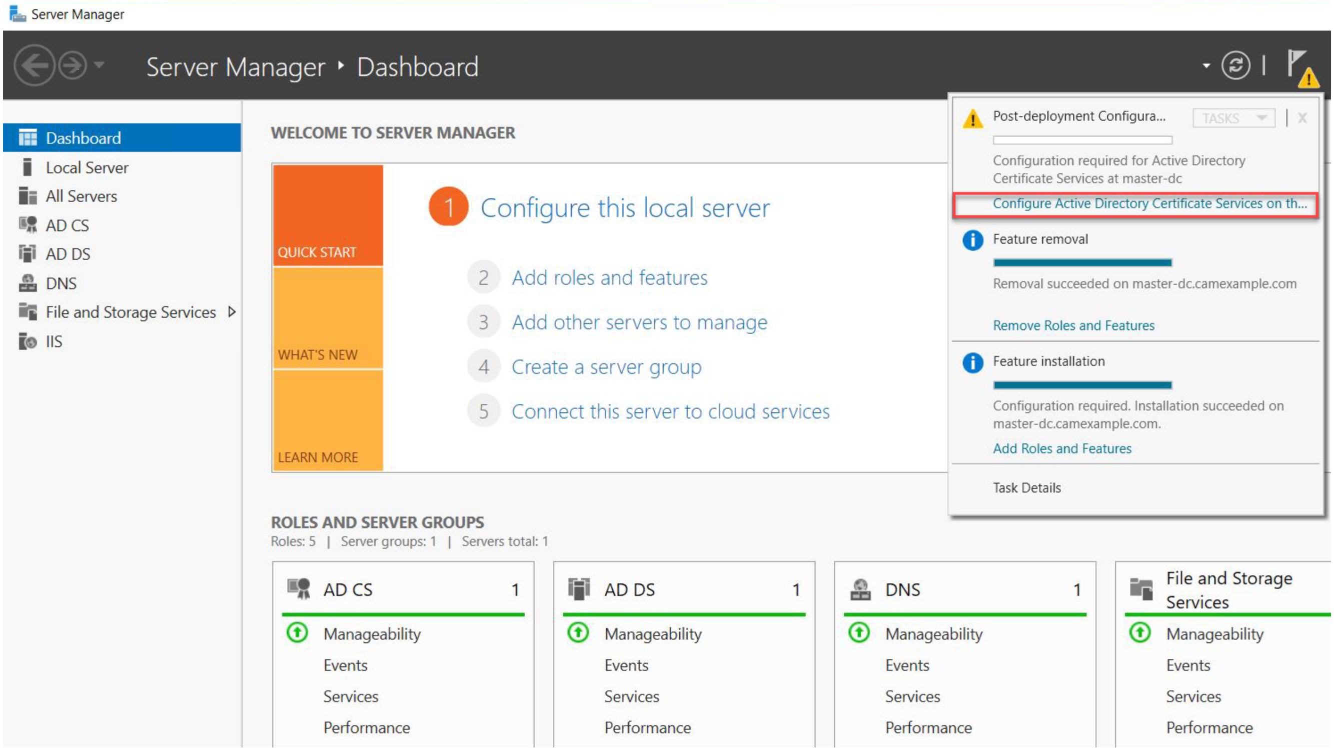
Description

Certification Authority Web Enrollment provides a simple Web interface that allows users to perform tasks such as request and renew certificates, retrieve certificate revocation lists (CRLs), and enroll for smart card certificates.

6. On the **Features** page, Click **Next**.

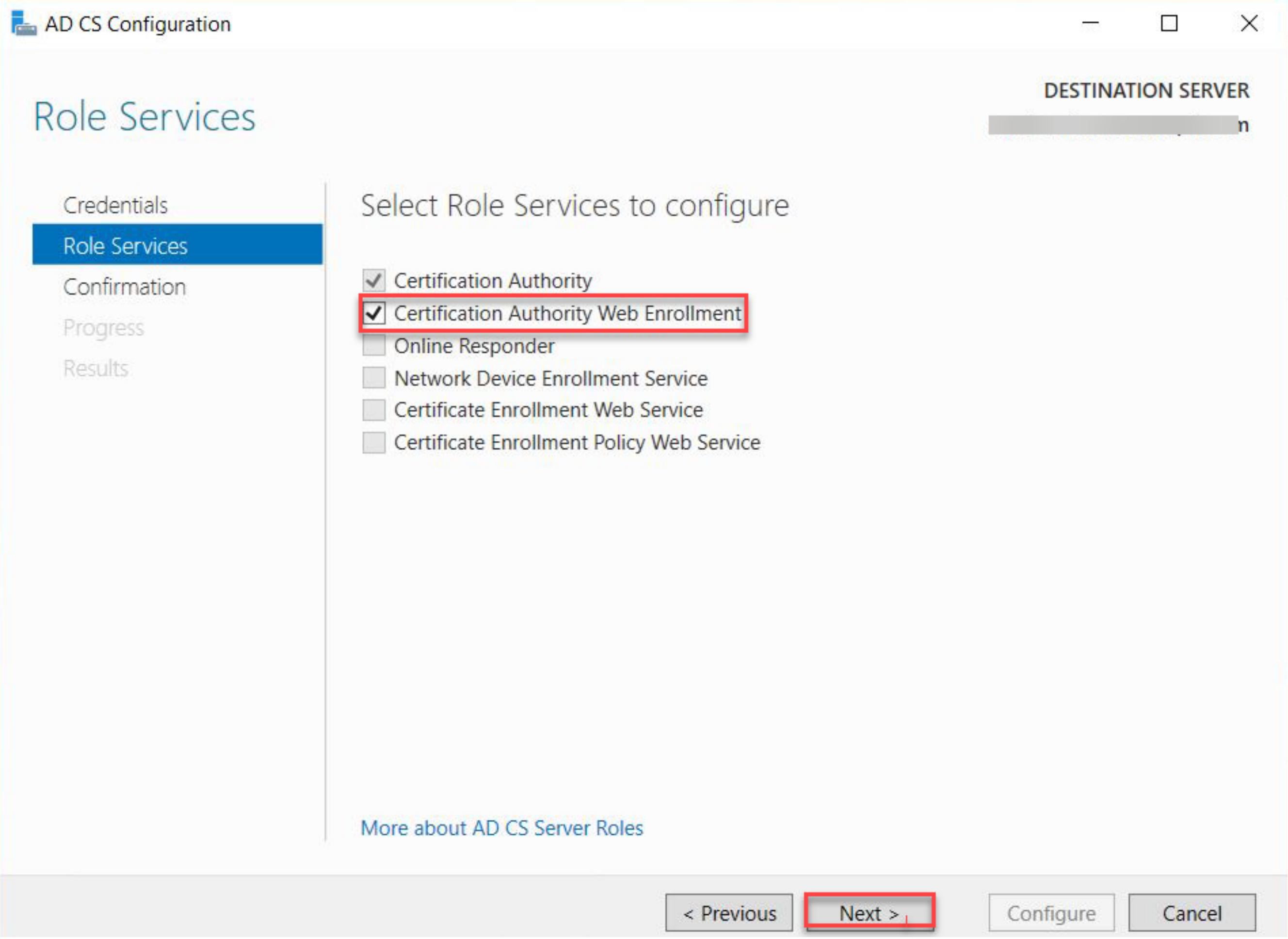
7. On the **Confirmation** page, select **Restart the destination server automatically if required** and press **Install**.

8. After installation, go to the **notification** tab and click **Configure Active Directory Certificate Services**.


Server Manager
Server Manager ‣ Dashboard
Dashboard
Local Server
All Servers
AD CS
AD DS
DNS
File and Storage Services
IIS
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
5 Connect this server to cloud services
ROLES AND SERVER GROUPS
Roles: 5 | Server groups: 1 | Servers total: 1
AD CS 1
AD DS 1
DNS 1
File and Storage Services
Manageability
Events
Services
Performance
Post-deployment Configura...
TASKS
Configuration required for Active Directory Certificate Services at master-dc
Configure Active Directory Certificate Services on th...
Feature removal
Removal succeeded on master-dc.camexample.com
Remove Roles and Features
Feature installation
Configuration required. Installation succeeded on master-dc.camexample.com.
Add Roles and Features
Task Details

9. On the **Credentials** page, input the Credentials and click **Next**.

10. On the **Role Services** page, select **Certification Authority Web Enrollment** and Click **Next**.



DESTINATION SERVER
[redacted]

Role Services

Select Role Services to configure

☑ Certification Authority
☑ Certification Authority Web Enrollment
□ Online Responder
□ Network Device Enrollment Service
□ Certificate Enrollment Web Service
□ Certificate Enrollment Policy Web Service

11. On the **Confirmation** page, click **Configure** to finish configuration.

Single Sign-On is now configured.

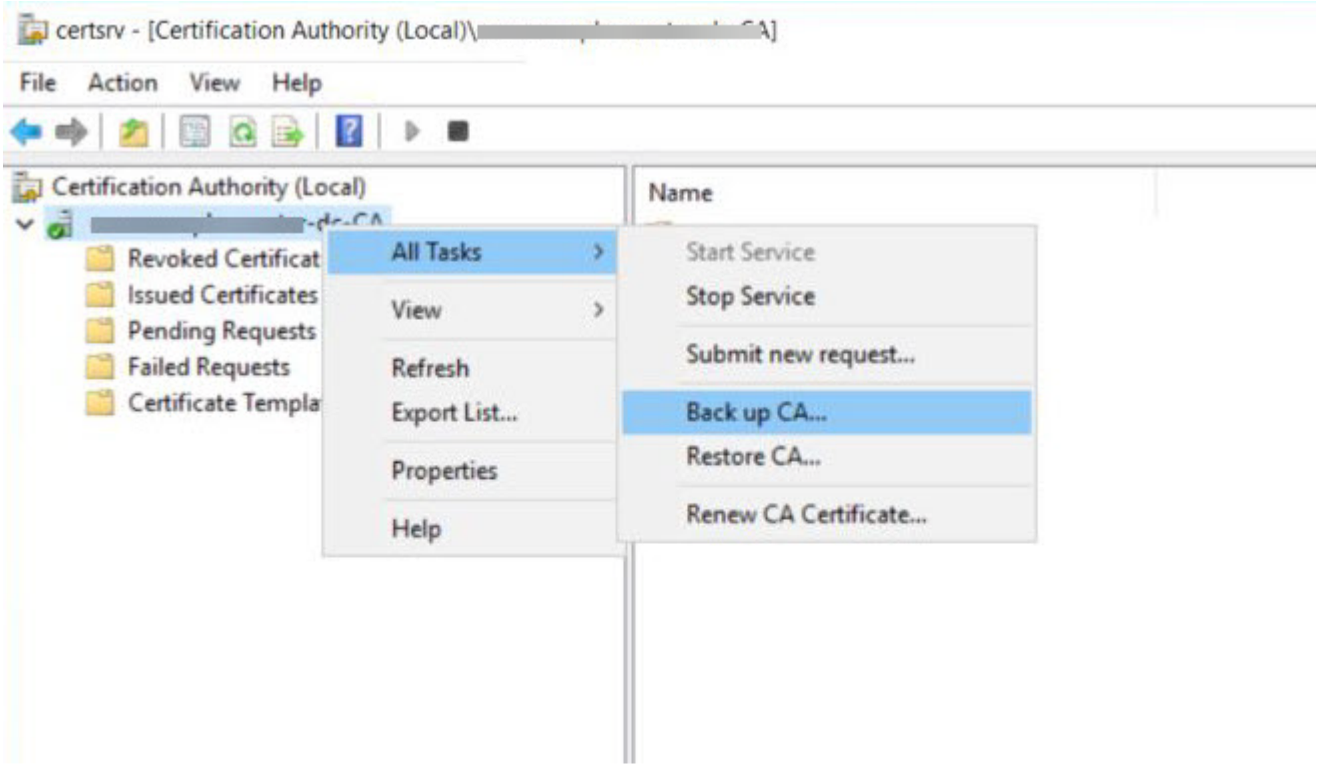
By private key and certificate of the Certification Authority

Working with your Certification Authority (CA) you will need to obtain:

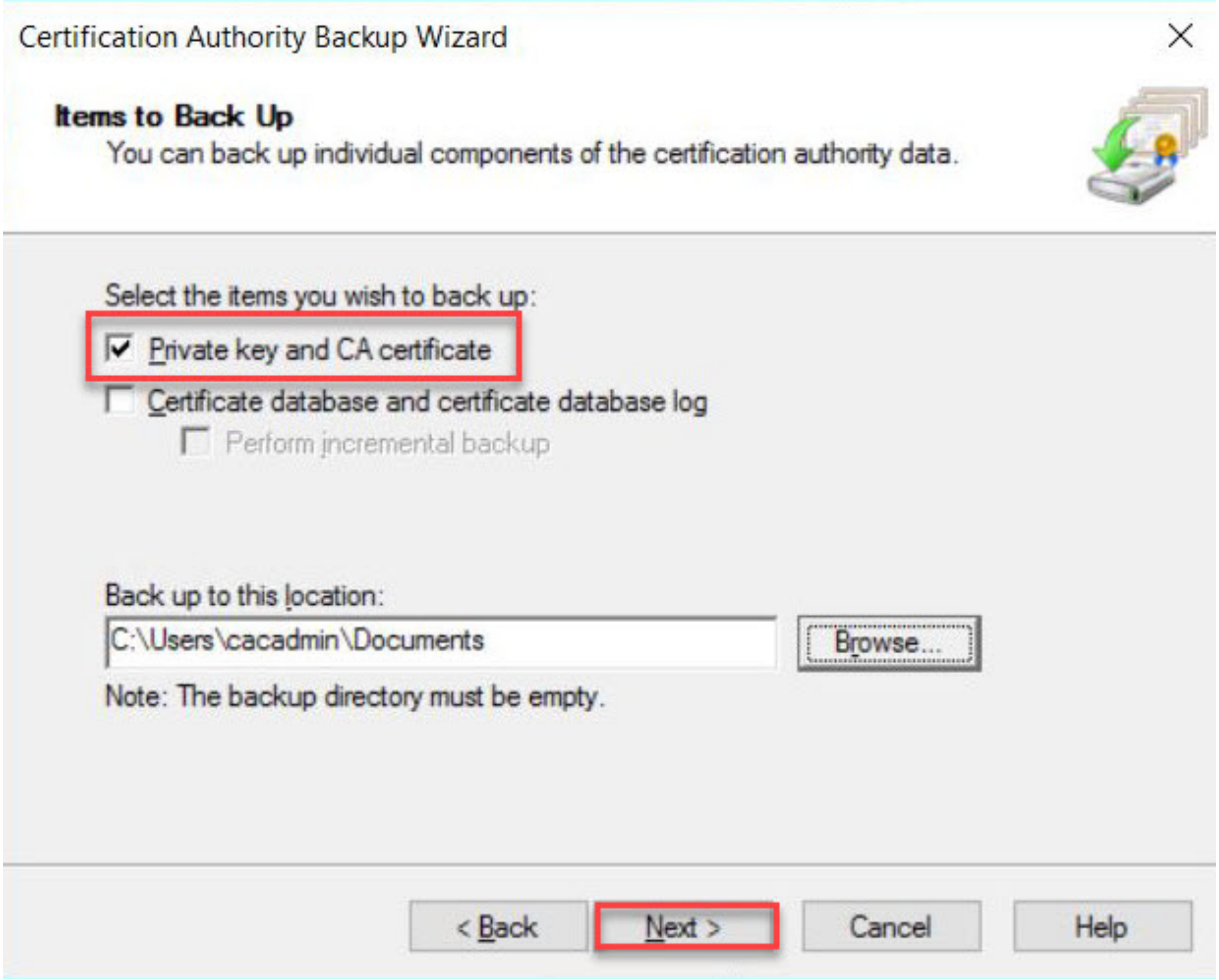
- Certificate of Intermediate CA
- Private Key of Intermediate CA
- Certificate Revocation List (CRL) file of the Intermediate CA

Export private key and certificate of the Intermediate Windows CA (Microsoft Windows Server 2019 Datacenter)

1. Log on to the Certificate Authority resource.
2. Open Certificate Authority MMC (`certsrv.msc`).
3. Right-click the CA in the tree, select **All Tasks** and click **Back up CA...**.



4. In the **Certification Authority Backup Wizard** window, click **Next**.
5. In the **Items to Back Up** section, select **Private key and CA certificate** and click on **Browse...** to choose a location to save the file. Click on **Next** to go to next step.



Certification Authority Backup Wizard

Items to Back Up

You can back up individual components of the certification authority data.

Select the items you wish to back up:

☑ Private key and CA certificate

□ Certificate database and certificate database log

□ Perform incremental backup

Back up to this location:

C:\Users\cacadmin\Documents

Note: The backup directory must be empty.

6. Click **Finish** to finish exporting the private key and certificate of the CA. **Note:** The private key and certificate are in a single `p12` file.

Extract the private key and certificate from `p12` file:

On a resource such as Linux VM that has `openssl` available:

1. Export and copy the `p12` file to a virtual machine that has the Connector/Connection Manager installed. You can transfer the file using a USB flash drive or SCP.
2. Run the following commands:
   - Extract private key with `openssl`. Run the following command and enter password when prompted:

```
openssl pkcs12 -in <your .p12 file name>.p12 -nocerts -nodes -out <your
private key file name>.key
```

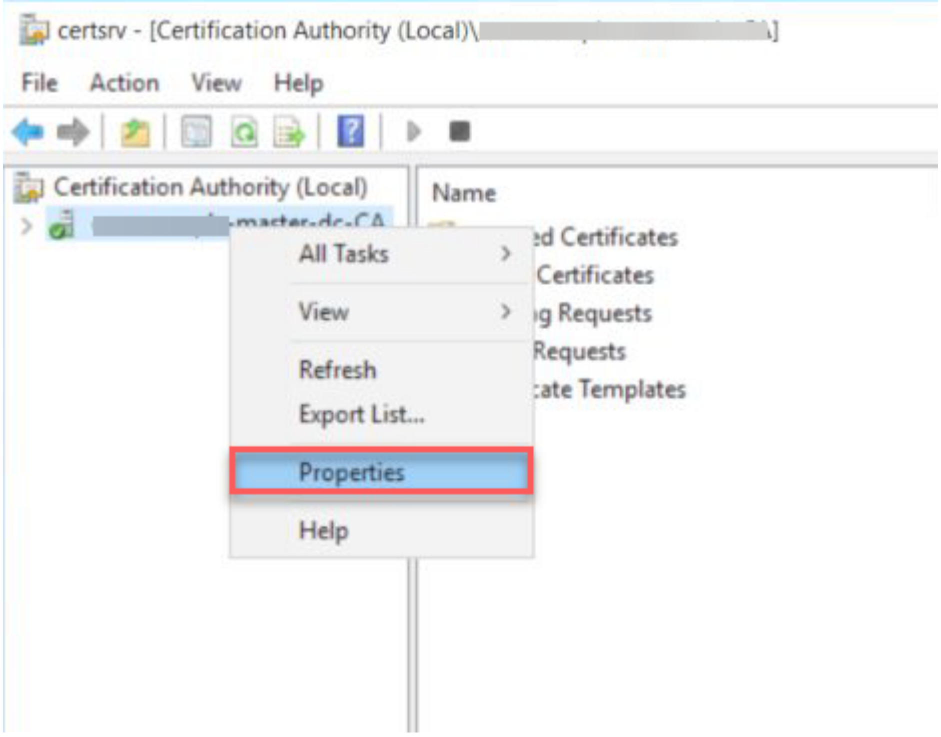
- Extract certificate with `openssl`. Run the following command and enter password when prompted:

```
openssl pkcs12 -in <your .p12 file name>.p12 -clcerts -nokeys -out
<your certificate file name>.crt
```

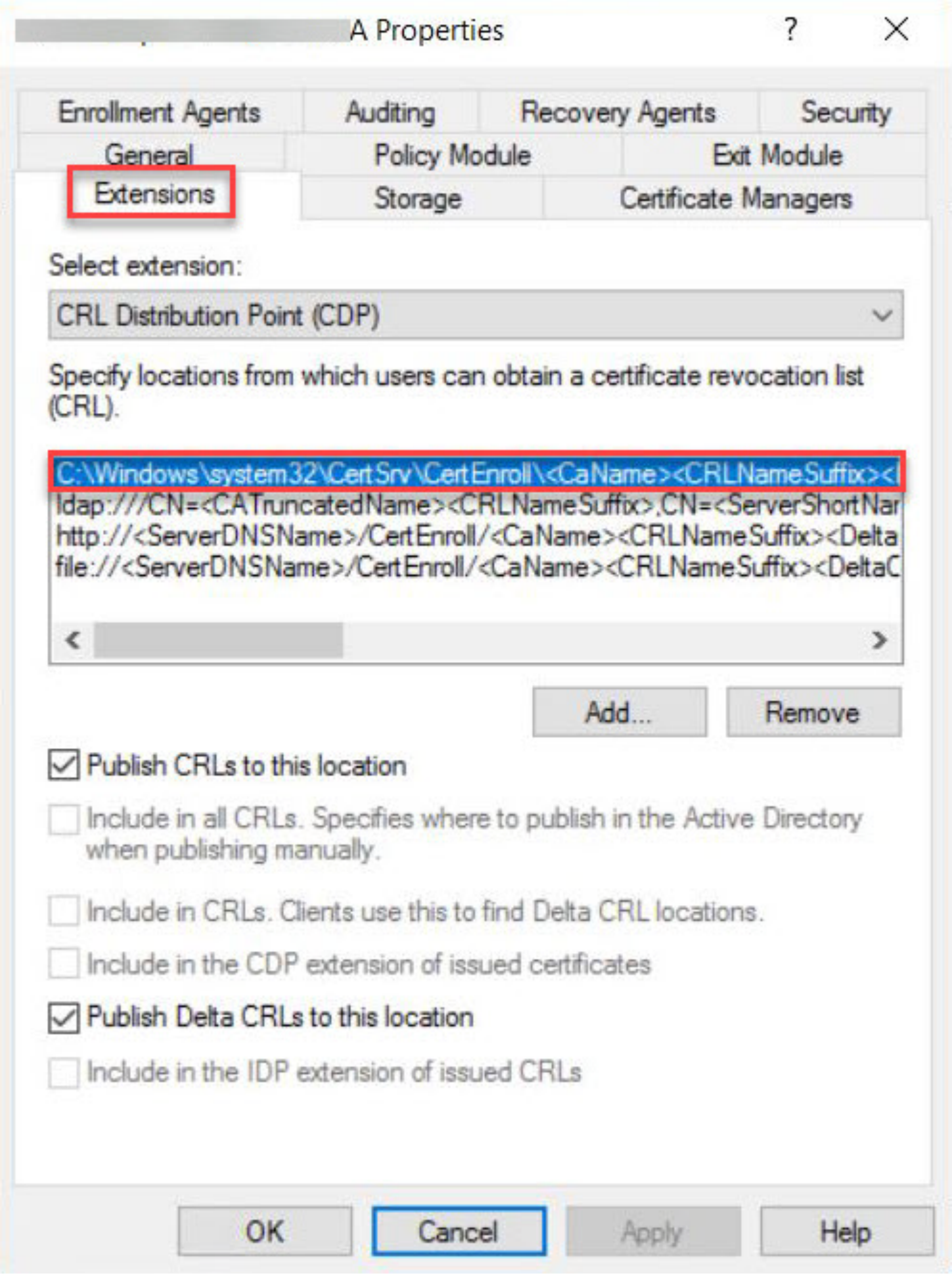
Locate Certificate Revocation List (CRL) file of the Intermediate Windows CA (Microsoft Windows Server 2019 Datacenter)

Perform the following steps:

1. Log on to the Certificate Authority resource, run `certsrv.msc` from command line to launch Certification Authority.
2. Right click the CA name and select **Properties**.



3. Select the **Extensions** tab, and take note of the `.crl` path. In this example, it is `C:\Windows\System32\CertSrv\CertEnroll\<CA name>.crl`.



[redacted]A Properties

Select extension:

CRL Distribution Point (CDP)

Specify locations from which users can obtain a certificate revocation list (CRL).

```
C:\Windows\system32\CertSrv\CertEnroll\<CaName><CRLNameSuffix><
ldap:///CN=<CATruncatedName><CRLNameSuffix>,CN=<ServerShortNar
http://<ServerDNSName>/CertEnroll/<CaName><CRLNameSuffix><Delta
file://<ServerDNSName>/CertEnroll/<CaName><CRLNameSuffix><DeltaC
```

☑ Publish CRLs to this location

□ Include in all CRLs. Specifies where to publish in the Active Directory when publishing manually.

□ Include in CRLs. Clients use this to find Delta CRL locations.

□ Include in the CDP extension of issued certificates

☑ Publish Delta CRLs to this location

□ Include in the IDP extension of issued CRLs

After you have obtained the files, they should be uploaded via SFTP (using a tool such as SCP) to your Connector and ensure that they are available for future configurations.

Enable Federated Authentication for Anyware Manager with SSO

To use the Federated Authentication feature seamlessly you must have the lastest versions of all the HP Anyware software component such as the **Software Client**, **Software Agent**, and the **Anyware Manager** installable. This is not applicable if you are using **Anyware Manager as a Service**. When Federated Authentication is configured, you should enable it from the **Admin Console**.

TO ENABLE FEDERATED AUTHENTICATION:

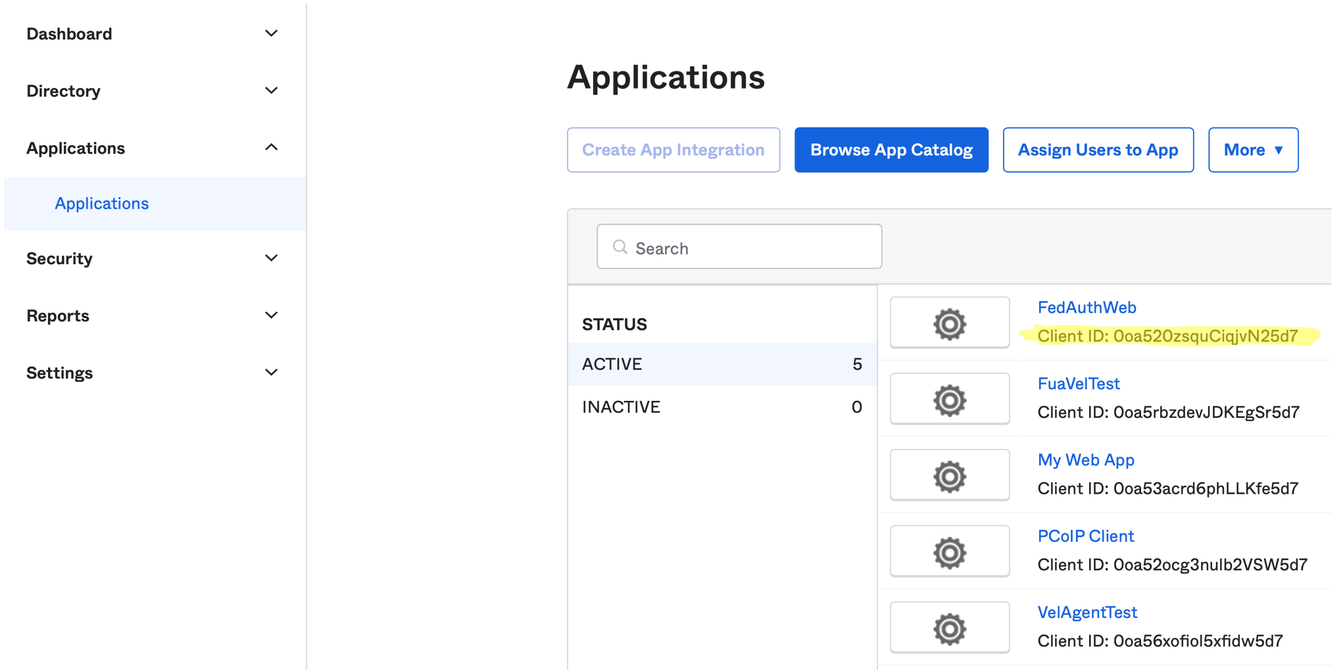
There are two methods of configuring Federated User Authentication in Anyware Manager, through the Admin Console, or the Connector installer.

1. Admin Console configuration

Global Configuration

Federated Authentication can be configured for your entire deployment using the Global configuration method. The steps are:

1. Navigate to https://cas.teradici.com and open the web console.
2. Enable the **Beta** toggle to turn on Beta mode, near the top of the interface. Select **Yes, I am in!** in the dialog box.
3. Select your deployment from the drop down, click the kebab (3 vertically stacked circles) next to your deployment's name and select **Edit deployment**.
4. Open the **Deployment Settings** section and select **Connector Settings**.
5. Enable **OAuth Authentication** and enter in authentication URL and client ID. To obtain the OAuth client ID, you need to login into Okta IDP and navigate to the **Applications** tab from the left pane. Please refer the highlighted area in the image below:



STATUS	
ACTIVE	5
INACTIVE	0

FedAuthWeb
Client ID: 0oa520zsquCiqjvN25d7

FuaVelTest
Client ID: 0oa5rbzdevJDKEgSr5d7

My Web App
Client ID: 0oa53acrd6phLLKfe5d7

PCoIP Client
Client ID: 0oa52ocg3nulb2VSW5d7

VelAgentTest
Client ID: 0oa56xofiol5xfidw5d7

6. Click **Save Configuration**.

Federated Authentication is now configured.

Per Connector Configuration

Federated User Authentication can be configured on a per connector basis. This permits you to try it out on a single connector to start to minimize impact to your deployment or to have specific connectors that are used for Federated User Authentication:

1. Select your deployment from the Deployment drop down option.
2. Click **Connectors** from the left pane and select the connector you wish to modify from the table.
3. Select the **Connector Settings** tab and click **Enabled** under OAuth Authentication.
4. Enter the following information into the interface that you obtained from your Identity Provider configuration:
    - Authorization URL
    - Client ID
5. Click **Save Configuration**.

Federated Authentication is now configured.

After configured the setting in admin console, run the following command in connector to apply the setting:

Private Key and CA requirement

Ensure that you have the PEM files for the signed certificate, private key and certificate revocation list from the above instructions on Preparing for Single Sign-On, and have uploaded them via sftp to each Connector.

1. To enroll by the private key and certificate of the Certification Authority (available in 23.01 and later):
    - To update a Connector to use this setting:
        - Log into the Connector using SSH.
            - Run the command: `sudo cloud-access-connector update <any other configuration flags you use> --pull-connector-config --sso-signing-csr-ca <path to pem> --sso-signing-csr-key <path to pem> --sso-signing-crl <path to crl> --sso-enrollment-url "" --sso-enrollment-domain "" --sso-enrollment-username "" --sso-enrollment-password "" --sso-enrollment-certificate-template-name ""`.
    - To deploy a new Connector to use this setting: - Log into the Connector using SSH. - Run the command: `sudo cloud-access-connector install <any other configuration flags you use> --pull-connector-config --sso-signing-csr-ca <path to pem> --sso-signing-csr-key <path to pem> --sso-signing-crl  <path to crl>`.
2. To enroll via Active Directory Certification Authority Web Enrollment (available in 23.01 and later):
    - To update a Connector to use this setting:
        - Log into the Connector using SSH.
        - Run the command: `sudo cloud-access-connector update <any other configuration flags you use> --pull-connector-config --sso-enrollment-url "$Enrollment_URL" --sso-enrollment-domain "$Domain" --sso-enrollment-username "$User_Name" --sso-enrollment-password "$Password" --sso-enrollment-certificate-template-name "$Template_Name"--sso-signing-csr-ca "" --sso-signing-csr-key "" --sso-signing-crl ""`.
    - To deploy a new Connector to use this setting:
        - Log into the Connector to using SSH.
        - Run the command: `sudo cloud-access-connector install <any other configuration flags you use> --pull-connector-config --sso-enrollment-url`

`"$Enrollment_URL" --sso-enrollment-domain "$Domain" --sso-enrollment-username "$User_Name" --sso-enrollment-password "$Password" --sso-enrollment-certificate-template-name "$Template_Name"`.

2. OAuth Configuration for Connectors

You can configure your environment at the connector using the command line interface (CLI) on each connector in your environment.

To enroll by the private key and certificate of the Certification Authority:

Private Key and CA requirement

Ensure that you have the PEM files for the signed certificate, private key and certificate revocation list from the above instructions on Preparing for Single Sign-On, and have uploaded them via sftp to each Connector.

Passphrase Protection

Passphrase protection for CA certificates is not supported.

If you are installing a new connector:

- Run this command: `sudo cloud-access-connector install […other settings...] --enable-oauth true --id-provider-url https://id.provider.com --oauth-client-id XXXXXXXXX --enable-sso true --sso-signing-csr-ca <path to pem> --sso-signing-csr-key <path to pem> --sso-signing-crl  <path to crl>`.

If you are configuring an existing connector:

- Run this command (for 23.01 or later): `sudo cloud-access-connector update […other settings...] --enable-oauth true --id-provider-url https://id.provider.com --oauth-client-id XXXXXXXXX --enable-sso true --sso-signing-csr-ca <path to pem> --sso-signing-csr-key <path to pem> --sso-signing-crl <path to crl> --sso-enrollment-url "" --sso-enrollment-domain "" --sso-enrollment-username "" --sso-enrollment-password "" --sso-enrollment-certificate-template-name ""`.

To enroll via Active Directory Certification Authority Web Enrollment (available in 23.01 and later):

If you are installing a new connector:

- Run this command: `sudo cloud-access-connector install […other settings...] --enable-oauth true --id-provider-url https://id.provider.com --oauth-client-id XXXXXXXXX --enable-sso true --sso-enrollment-url "$Enrollment_URL" --sso-enrollment-domain "$Domain" --sso-enrollment-username "$User_Name" --sso-enrollment-password "$Password" --sso-enrollment-certificate-template-name "$Template_Name"`.

If you are configuring an existing connector:

- Run this command: `sudo cloud-access-connector update […other settings...] --enable-oauth true --id-provider-url https://id.provider.com --oauth-client-id XXXXXXXXX --enable-sso true --sso-enrollment-url "$Enrollment_URL" --sso-enrollment-domain "$Domain" --sso-enrollment-username "$User_Name" --sso-enrollment-password "$Password" --sso-enrollment-certificate-template-name "$Template_Name" --sso-signing-csr-ca "" --sso-signing-csr-key "" --sso-signing-crl ""`.

Installation Flags

Flag	Type	Description
`--enable-oauth`	Boolean	Enables Oauth authentication. (Default=False)
`--id-provider-url`	String	Sets the identity provider URL. Example: `--id-provider-url https://provider-1234567890.okta.com`. This flag is required if `--enable-oauth is true`.
`--oauth-client-id`	String	Gets the Client ID from the Identity Provider. This flag is required if `--enable-oauth is true`.
`--fa-url`	String	The Federated Auth Broker URL. for example https://cac-vm-fqdn:port
`--oauth-flow-code`	String	Specify the oauth flow / grant type (default "OAUTH_FLOW_CODE_WITH_PKCE"). "OAUTH_FLOW_CODE_WITH_PKCE" is the only supported oauth flow for now
`--enable-entitlements-by-upn`	Boolean	Enables/Disables searching entitlements by UPN. This flag is required to be true, if `--enable-oauth is true`.
`--sso-signing-csr-ca`	String	Path to copy intermediate CA Certificate.
`--sso-signing-csr-key`	String	Path to the intermediate key.
`--sso-signing-crl`	String	Path to a certificate revocation list.
`--sso-enrollment-url`	String	Gets the URL to the Active Directory Certification Authority Web Enrollment Service.
`--sso-enrollment-domain`	String	Domain of the user to access Active Directory Certification Authority Web Enrollment Service.
`--sso-enrollment-username`	String	Username for accessing Active Directory Certification Authority Web Enrollment Service.
`--sso-enrollment-password`	String	Password for the username to access Active Directory Certification Authority Web Enrollment Service.
`--sso-enrollment-certificate-template-name`	String	Name of the certificate template that Active Directory Certificate Services (AD CS) uses to sig CSR.

After Completion of Testing

After you have completed trying the feature our, or testing it. We recommend you revoke the Intermediate Signed Certificate and Private Key you generated to enable SSO.

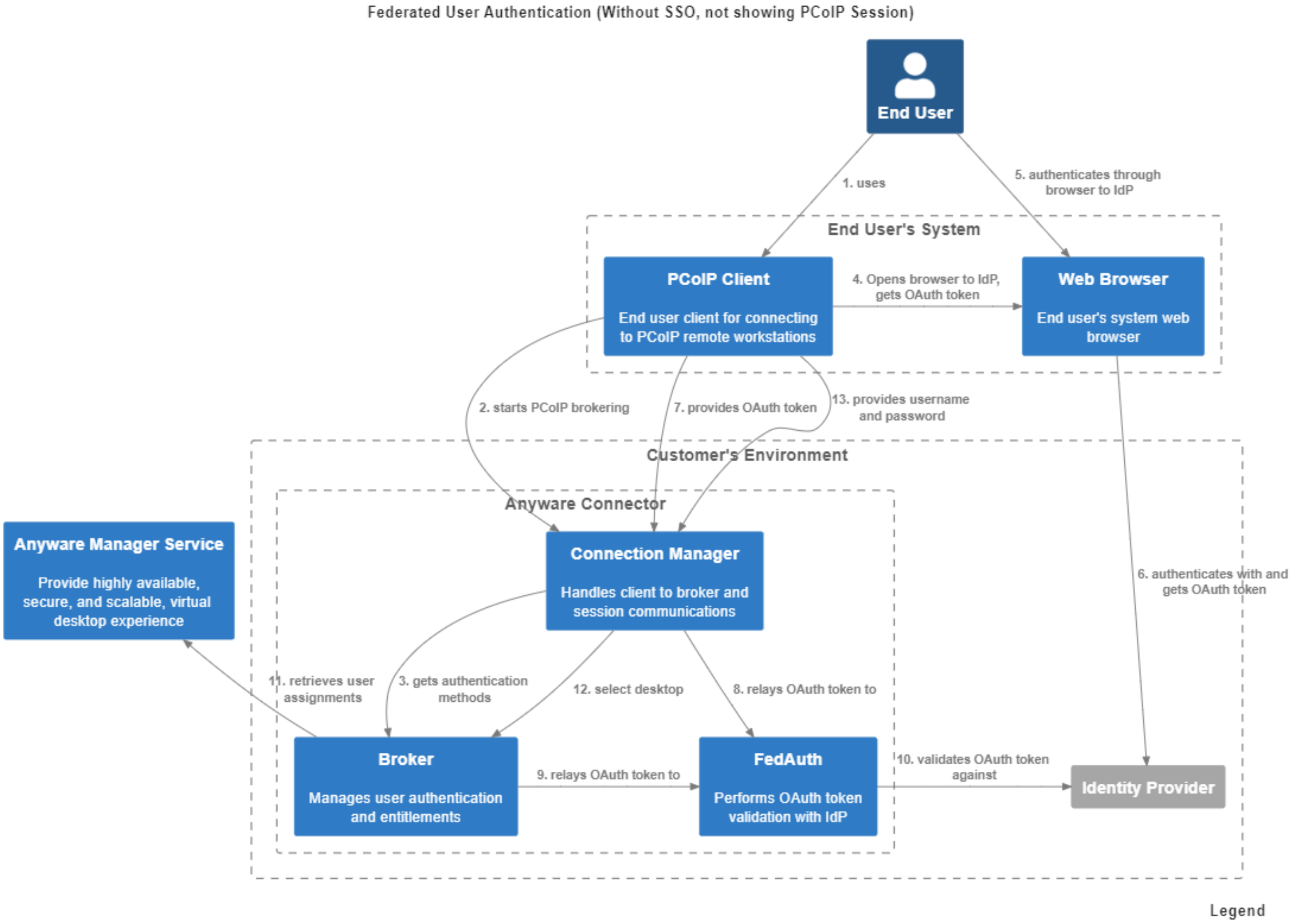
If you had configured this in production Connectors you need to turn off SSO. This can be done using the instructions above from the Admin Console and switching Enable Single Sign-On (SSO) so that it is disabled, or from the command line for each connector using:

- Run the command: `sudo cloud-access-connector update […other settings...] --enable-sso false`.

Troubleshooting Federated Authentication

Federated Authentication Process Overview

The diagram below describes the components and steps that occur when a user authenticates to a Connector using Federated User Authentication up to the point where the user has selected the desktop they want to connect to. The diagram is numbered, and the flow can be followed by the numbers to determine which components are in use at any given step in the process, and instructions are provided for how to obtain logs from those components if a failure occurs. .


Federated User Authentication (Without SSO, not showing PCoIP Session)
End User
1. uses
5. authenticates through browser to IdP
End User's System
PCoIP Client
End user client for connecting to PCoIP remote workstations
4. Opens browser to IdP, gets OAuth token
Web Browser
End user's system web browser
2. starts PCoIP brokering
7. provides OAuth token
13. provides username and password
Customer's Environment
Anyware Connector
Anyware Manager Service
Provide highly available, secure, and scalable, virtual desktop experience
Connection Manager
Handles client to broker and session communications
6. authenticates with and gets OAuth token
11. retrieves user assignments
3. gets authentication methods
12. select desktop
8. relays OAuth token to
Broker
Manages user authentication and entitlements
9. relays OAuth token to
FedAuth
Performs OAuth token validation with IdP
10. validates OAuth token against
Identity Provider
Legend

OBTAINING LOGS

The table above describes the components that may contain logs to describe errors if a failure occurs. This section provides information or references to how to obtain logs for each HP provided component:

- **PCoIP Client**
    - Windows: https://www.teradici.com/web-help/pcoip_client/windows/current/support/logs/
    - Linux: https://www.teradici.com/web-help/pcoip_client/linux/current/support/logs/
    - MacOS: https://www.teradici.com/web-help/pcoip_client/mac/current/support/logs/
- **Connector**
    - Overview: https://www.teradici.com/web-help/cas_manager_as_a_service/troubleshooting/troubleshooting_logs/
    - Connection Manager:
        - client inside the corporate network: `sudo docker service logs connector_cm`
        - client outside the corporate network: `sudo docker service logs connector_cmsg`
    - Federated Auth service:
        - client inside the corporate network: `sudo docker service logs connector_brokerinternal`
        - client outside the corporate network: `sudo docker service logs connector_brokerexternal`
    - Broker: `sudo docker service logs connector_fa`
- **PCoIP Agent**
    - Windows Standard Agent: https://www.teradici.com/web-help/pcoip_agent/standard_agent/windows/current/admin-guide/diagnostics/locating-log-files/
    - Windows Graphics Agent: https://www.teradici.com/web-help/pcoip_agent/graphics_agent/windows/current/admin-guide/diagnostics/locating-log-files/

POTENTIAL ISSUES

Step	Visual	Description	Potential Types of Failures	Components Involved
1	Alt Text	The user opens up the PCoIP Client from their computer.	Client failures, such as crashing.	PCoIP Client
2	Alt Text	From the list of configured connections, the user selects the connector configured for Federated User Authentication.	- Networking errors between the client and connector. - Connector is misconfigured or failing	- PCoIP Client - Connection Manager
3	Alt Text	The connector instructs the PCoIP Client to perform Federated User Authentication and the user's web browser is opened to the organization's Identity Provider.	- No browser is opened: Connector misconfigured for federated authentication. Check Connector Configuration - Connector was configured with an incorrect client ID. (See step 5 in Admin Console configuration section.) Alt Text - Networking errors between the user's computer and the Identity Provider.	- PCoIP Client Connection Manager, Federated Authentication Service - Identity Provider.
4	Alt Text Alt Text	The user provides their credentials or any other authentication means to the Identity Provider.	Incorrect credentials. Alt Text	Identity Provider.
5	NA	The user returns to their PCoIP Client and the client provides the user's proof of authentication to the connector. The connector validates that authentication against the Identity Provider.	- - Incorrectly configured redirect URL in the Identity Provider see, step 5 in Configuring Okta IDP and step 4 in Configuring Azure Active Directory. - Untrusted certificate between the connector and Identity Provider.	- PCoIP Client - Connector (Connection Manager, Broker, Federated Authentication Service) - Identity Provider
6	Alt Text	Connector obtains the user's list of desktops (or pools) and returns them to the client to be displayed to the user.	- Network failures between the connector and Anyware Manager. - Revoked or invalid credentials within the connector to Anyware Manager. - User is not configured in Anyware Manager or has no	- PCoIP Client - Connection Manager - Third-Party Broker

Step	Visual	Description	Potential Types of Failures	Components Involved
			desktops or pools entitled to them Alt Text	
7	Alt Text	The user selects a desktop (or pool).	Desktop fails to start Alt Text	- PCoIP Client - PCoIP Agent - Connector (Connection Manager, Broker)
8	Alt Text	The user is prompted at the PCoIP Client to enter their username and password.	- User provides incorrect credentials. - PCoIP Agent is unable to authenticate the user using the credentials.	- PCoIP Client - Connector (Connection Manager, Broker) - PCoIP Agent
Single Sign-On				
Step	Visual	Description	Potential Types of Failures	Components Involved
1	Alt Text	The user is prompted to enter their username and password.	- SSO is not supported by the Agent. - SSO is disabled (see `--enable--sso` flag, check current configuration)	- Connector (Connection Manager, Broker) - PCoIP Agent
2	Alt Text	The user connects to a session and is presented with the login screen.	- Certificate issue. Connector may have been configured with incorrect certificate files. Agent was not able to login with the certificate (Check `--sso-signing-*` or `--sso-enrollment-*` installation flags, check current configuration).	- PCoIP Agent - Connector (Connection Manager, Broker)

Remote Workstations

Adding a Remote Workstation

You can add an existing remote workstation you created within the Admin Console, or one created in your cloud environment to a deployment. You can also view and add available resource groups if the remote workstation has valid cloud credentials. The remote workstation must have a PCoIP Agent installed on it and be visible to the Connector. You must have a valid Anyware Software registration code and the remote workstation, and user, must be part of the deployments active directory domain. Any remote workstations that have a PCoIP Agent installed must be domain joined.

The following steps outlines how to add an existing remote workstation to your deployment using the Admin Console:

1. Click **Workstations** from the console sidebar.
2. Click the Add Remote Workstation button and click **Add existing remote workstation** to display the Add a Remote Workstation panel.
3. Select a Cloud Services Provider.
    - If your remote workstation has AWS credentials select the AWS region.
    - If your remote workstation has Azure credentials you can view and select available resource groups from the resource groups tab.
    - If your remote workstation has GCP credentials select the GCP region where your remote workstation resides, as well as the GCP zone.
    - If your remote workstation is on the Private Cloud you can search for, and add, these remote workstations. They must be domain joined and have a PCoIP Agent installed. If you want to add remote workstations that are not domain joined, you can click DEFINE YOUR OWN MACHINES and enter the name of the remote workstation and add it. The Connector can connect to this remote workstation by a FQDN or an IP address. If you are using an IP address, ensure it is static or persistently assigned to the remote workstation in question.
4. Select the remote workstations you want to add.
5. Select how you want to manage adding users to these remote workstations. You can individually select users, add users later or use workstations pools.

6. Click **SAVE**.

The remote workstation should now appear on the **Workstations** page.

Editing a Remote Workstation

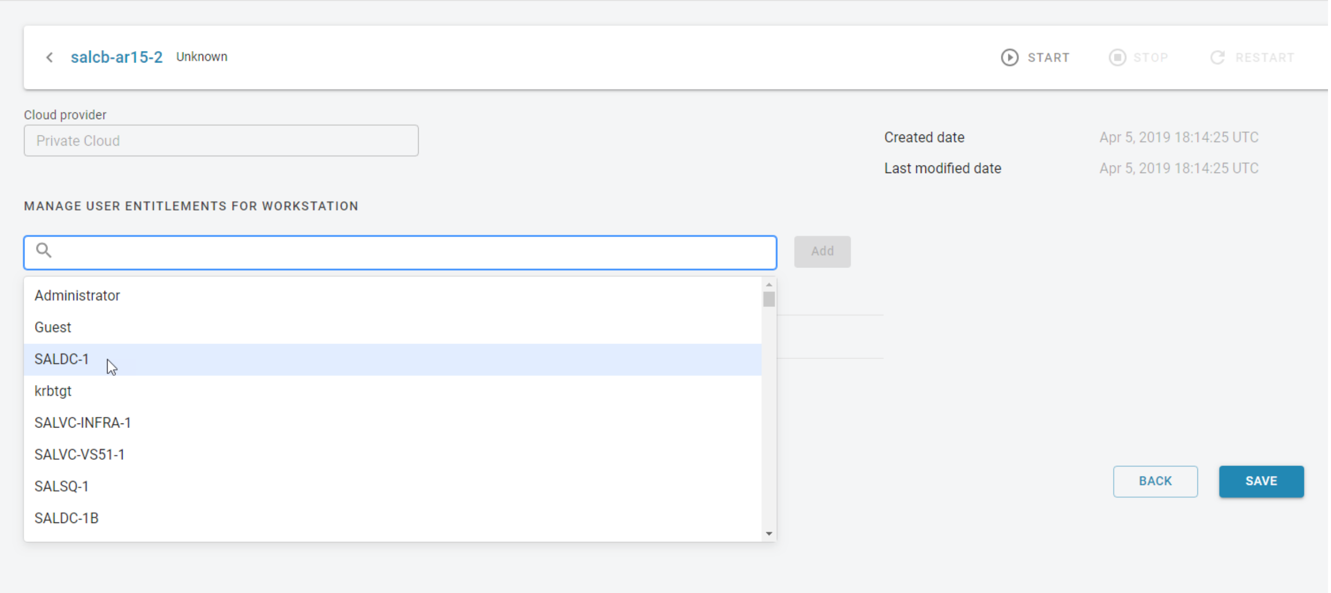
Once you have created a remote workstation within the Admin Console you can manage and reconfigure it directly from the **Remote Workstations** page.

You can search for specific remote workstations by name by using the search bar in the table toolbar.

Entitling Users

Once you have created a remote workstation you can entitle users from the active directory account to specific remote workstations. The following section outlines how to entitle users:

1. Click the kebab option under the **ACTIONS** column to edit the desired remote workstation.
2. Click **Edit**.
3. Select the search bar and select the user you want to entitle:



salcb-ar15-2 Unknown

Cloud provider: Private Cloud

Created date: Apr 5, 2019 18:14:25 UTC

Last modified date: Apr 5, 2019 18:14:25 UTC

MANAGE USER ENTITLEMENTS FOR WORKSTATION

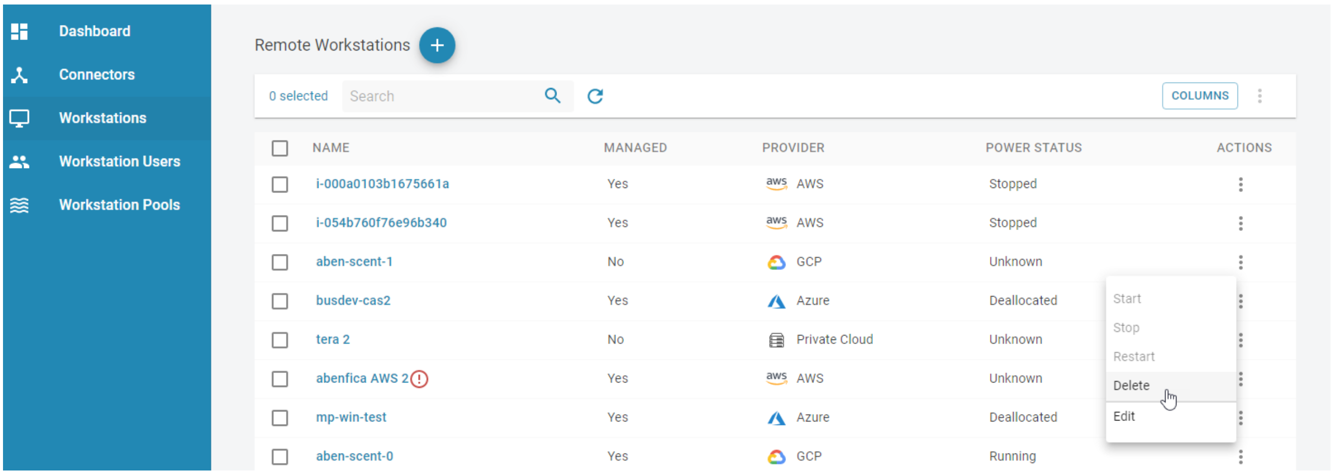
4. Click **Add** and then **SAVE**.

The user you entitled appears in the *USER* column on the Remote Workstations page for that particular remote workstation.

Deleting Remote Workstations from the Public Cloud

You can delete existing remote workstations from AWS, Azure, and GCP from thes Admin Console. Only remote workstations that exist in AWS, Azure, and GCP and are part of deployments that have valid cloud credentials can be deleted.

1. Click **Workstations** from the console sidebar to display your existing remote workstations.
2. Click the kebab option under the **ACTIONS** column.
3. Click **Delete**.



NAME	MANAGED	PROVIDER	POWER STATUS	ACTIONS
i-000a0103b1675661a	Yes	AWS	Stopped	⋮
i-054b760f76e96b340	Yes	AWS	Stopped	⋮
aben-scent-1	No	GCP	Unknown	⋮
busdev-cas2	Yes	Azure	Deallocated	⋮
tera 2	No	Private Cloud	Unknown	⋮
abenfica AWS 2	Yes	AWS	Unknown	⋮
mp-win-test	Yes	Azure	Deallocated	⋮
aben-scent-0	Yes	GCP	Running	⋮

4. Click **CONFIRM** from the resulting pop-up message.

The process for deleting the remote workstation has now begun. It is also possible to bulk delete more than one remote workstation at a time by selecting multiple remote workstations to delete from the Admin Console.

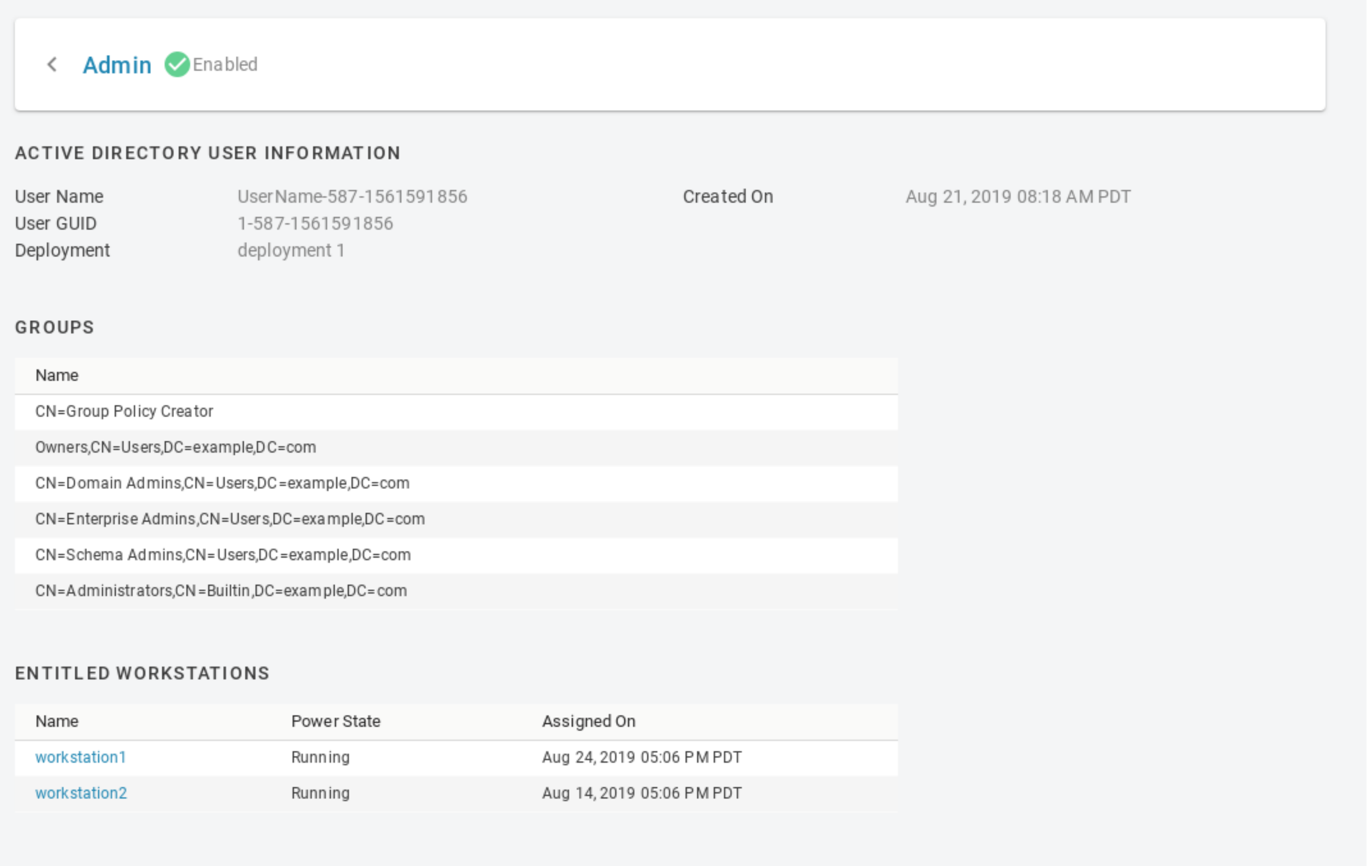
The remote workstation disappears immediately from the Admin Console and can take 5-10 minutes to be deleted from the Anyware Manager and public cloud. You should monitor the workstation in your cloud provider to ensure a successful completion.

Viewing Remote Workstation Users

You can view all available Workstation users in your active directory by selecting the **Workstation Users** page. You can search for specific users by name with the search field in the toolbar. You can obtain the following user information for specific users:

- User Name
- User GUID
- Deployment
- Directory status
- User Groups
- Date of creation

When you select a specific user, you can see all the user groups and entitled remote workstations associated with this user:



< Admin ✓ Enabled

ACTIVE DIRECTORY USER INFORMATION

User Name	UserName-587-1561591856	Created On	Aug 21, 2019 08:18 AM PDT
User GUID	1-587-1561591856		
Deployment	deployment 1		

GROUPS

Name
CN=Group Policy Creator
Owners,CN=Users,DC=example,DC=com
CN=Domain Admins,CN=Users,DC=example,DC=com
CN=Enterprise Admins,CN=Users,DC=example,DC=com
CN=Schema Admins,CN=Users,DC=example,DC=com
CN=Administrators,CN=Builtin,DC=example,DC=com

ENTITLED WORKSTATIONS

Name	Power State	Assigned On
workstation1	Running	Aug 24, 2019 05:06 PM PDT
workstation2	Running	Aug 14, 2019 05:06 PM PDT

This gives your an overview of a specific user's entitlements and deployment information and can be useful for troubleshooting issues.

Updating Cloud Provider Information

Remote workstations that have been added into Anyware Manager, or created by Anyware Manager, can be associated to a cloud provider. This enables Anyware Manager to use the credentials for that cloud provider to access the remote workstation and enable power management. The cloud provider in which the remote workstation resides in can be changed. This can be done if either the remote workstation has been moved, or if the workstation was set to the Private Cloud, and you want to update it and assign it to the actual cloud provider.

Editing the cloud provider and zone information does not change the location of the remote workstation. This feature enables Anyware Manager to point to a different location to verify the remote workstation exists in the specified zone. If you do not have valid cloud credentials for a cloud provider you are not able to change the remote workstation cloud provider.

The following section outlines how to update a remote workstation on the private cloud and associate it to a workstation in a public cloud:

1. Click the kebab option under the **ACTIONS** column to edit the desired remote workstation.
2. Click **Edit**.
3. From the **CLOUD INFORMATION** panel click **EDIT PROVIDER**.
4. Select the cloud provider the remote workstation belongs to.
5. Select the region, resource group and zone, depending on the cloud provider, the remote workstation resides in.
6. Select the remote workstation and update the provider.

If you enter the correct cloud provider and zone for the remote workstation you should receive a notification regarding successful update. The new zone, cloud provider and information is also listed on this page.

If you enter an incorrect zone, you receive an error message stating that the remote workstation does not exist in the entered zone.

AMT Power Management in Anyware Manager

Anyware Manager can use Intel® AMT to remotely power operate physical workstations. To be controlled remotely, a physical workstation within a deployment must have Intel AMT provisioned.

Provisioning Intel® AMT for Workstations

To use Intel® AMT, physical access to the workstation is required in order to perform manual provisioning and each workstation needs to be provisioned for Intel® AMT. Support for AMT power operations is not limited to workstations made by HP. Support for AMT version 12 is provided by default. AMT versions as low as AMT 9 are also supported with the selection of the **Enable support for AMT 11 or lower** toggle in the UI that allows communication via the less secure TLS 1.1 protocol.

⚠ **Transport Layer Security(TLS) Configuration Required**

Only TLS connections are supported by the Anyware Manager to communicate with Intel® AMT devices. Non TLS or Mutual TLS (mTLS) connections are not supported. As the network traffic is unencrypted before setting up TLS, HP recommends performing manual provisioning and configuration in a closed network.

PROVISIONING INTEL® AMT

A brief overview of provisioning HP Workstations is available in the Setting up and configuring Intel® AMT in HP Business Notebooks, Desktops, and Workstations white paper provided by HP. For more detailed information about provisioning AMT, please refer to the documentation provided by Intel: Intel® Active Management Technology Implementation.

Perform the following steps to enable and provision Intel® AMT for interoperation with HP Anyware Manager:

1. Power on the workstation.
2. During POST press F6 or Ctrl+P to enter the MEBx setup menu (this depends on the model of the workstation).
3. Select **MEBx Login** and enter the default password “admin”.

4. Create a new password. For best practices regarding AMT passwords, refer to the Setting up and configuring Intel® AMT in HP Business Notebooks, Desktops, and Workstations white paper provided by HP.
5. Select **Intel® AMT Configuration**.
6. Select **Power Control**.
7. In **Host Sleep States** section, ensure that the **Intel® AMT ON** option is set to *On* in S0, and *ME Wake* in S3 and S4-5.
8. Press **Esc** key to go back to the previous menu.
9. Select **Activate Network Access**.
10. Press **Y** to activate network access.
11. Exit the MEBx setup menu.

Intel® AMT provisioning setup is now completed. To verify the provisioning is correctly configured, open a web browser and go to `http://<hostname>:16992` and sign-in in with the username “admin” and the password that was created above.

> **Enterprise Provisioning**
>
> Enterprise provisioning is not currently supported in the Anyware Manager.

Communication Security

TLS

Transport Layer Security(TLS) is required by the Anyware Manager to communicate with the Intel® AMT device in an encrypted form. The AMT device holds a server certificate that must be trusted by the Manager to establish a connection. To avoid name mismatch errors, the FQDN/IP used for the workstation by the Manager must match the Common Name or a Subject Alternative Name of the certificate.

DIGEST

The Manager uses a digest username and password to connect to an AMT device. The username and password must be saved in the Manager for each workstation to which the Manager connects via AMT. The passwords used for AMT are encrypted when stored by the Manager.

Password Tip

Consider using different passwords for each AMT device as this reduces the area of attack if a single password is compromised.

Configuring Transport Layer Security(TLS) for Anyware Manager

TLS can be configured using MeshCommander, an open source Intel® AMT management console. Click here to download and install MeshCommander. The steps to configure TLS using MeshCommander are as follows:

1. Open MeshCommander.
2. If you do not already have a Root Certificate configured, follow these steps:
    a. Open the **Certificate Manager** tab.
    b. Create a Root Certificate.
    c. View the new Root Certificate and save the `.pem` file.
    d. Import the public key of the `.pem` file to the **Provider Service Accounts** page of the Anyware Manager.
        - The Manager service needs to trust this certificate.
        - This single trusted Root certificate should be used to issue TLS certificates for each workstation going forward.
3. Open MeshCommander and click the **Computer Management** tab.
4. Add the provisioned workstation.
5. Connect to the workstation.
6. Open the **Security Settings** tab.
7. Click **Add Certificate** and add the root certificate as a **Trusted Root Certificate**.
8. Click **Issue Certificate** and use the root certificate to issue a TLS Server (HTTPS) certificate.
9. Ensure that the common name matches the FQDN/IP you intend to use for connecting the workstation to the Anyware Manager.
10. Click **link next** to *Remote TLS Security*.
11. Select the newly issued certificate and Server-auth TLS only.
12. Click **OK**.

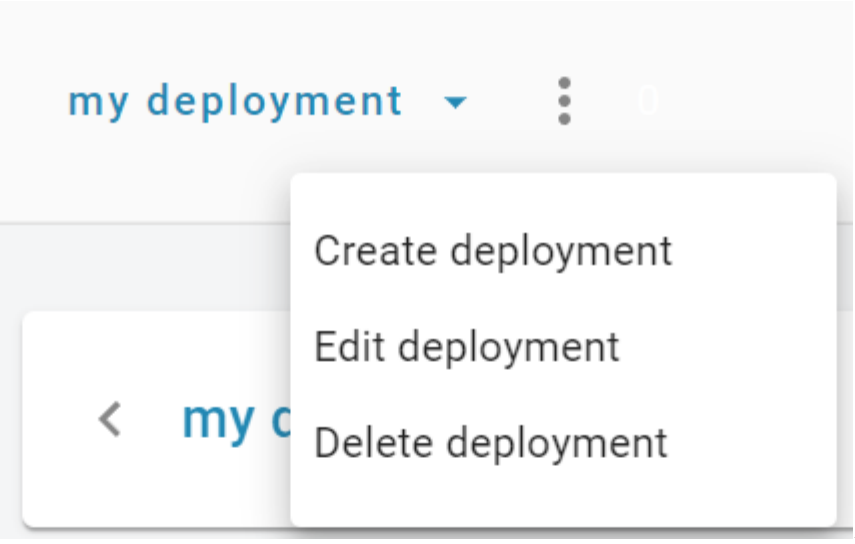
13. Reconnect with the workstation with TLS connection.

TLS connection is configured with the workstation. When TLS is enabled, you can access the web interface hrough `https://<hostname>:16993`.

> **Root certificate for TLS**
>
> When enabling TLS through MeshCommander, a Root Certificate and private key can be imported from the file system. This process needs to be done for each workstation individually.

Creating Intel® AMT Workstations in Anyware Manager

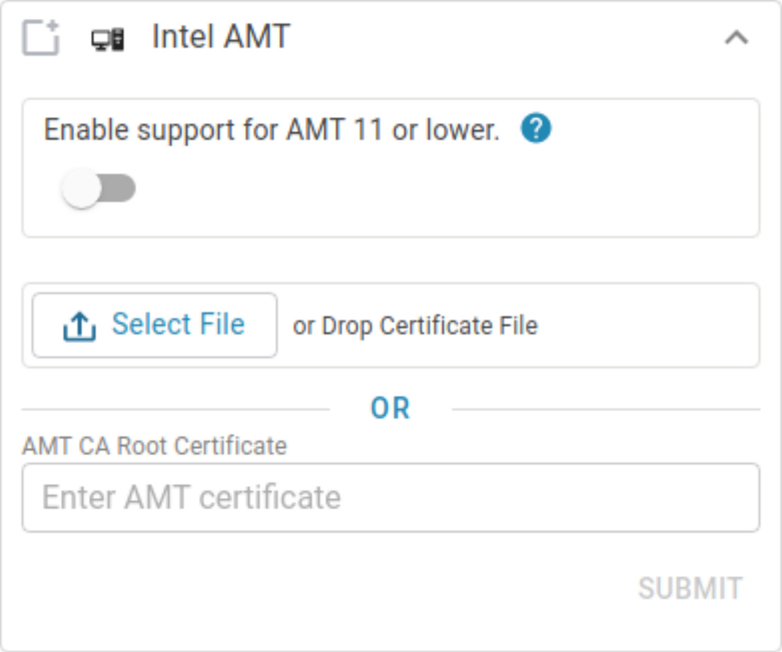
When Intel® AMT provisioning and TLS configuration is complete, workstations can then be added to the Anyware Manager administrative console. You need to edit an existing deployment in order to add workstations. If you do not have an existing deployment, you have to create one. For detailed steps, See Managing Deployment. To create Intel® AMT workstations, do the following:

1. In Anyware Manager, click **Edit deployment** from the kebab option to edit your deployment to provide the trusted Root Certificate to the Intel® AMT Provider Service Account 

.

2. Under **Provider Service Accounts** open the Intel® AMT account box.

3. Click **Select File**, browse and upload a Root Certificate public key file in the `.pem` format from your system. You can also copy and paste contents from the Root Certificate public key file to the **AMT CA Root Certificate** section.



Intel AMT

Enable support for AMT 11 or lower. ?

Select File or Drop Certificate File

OR

AMT CA Root Certificate

Enter AMT certificate

SUBMIT

4. Click **Submit**.
5. If you do not have an existing Connector, you should create one. For detailed steps, Click [here](#).
6. Add workstations for the Intel® AMT service provider. Make sure to use the same FQDN/IP For each workstation that matches the Common Name or Subject Alternative Name of the workstation's AMT server certificate. For detailed steps, see [Adding a Remote Workstation](#).

> **Authorized Access**
>
> You can set up authorized access to the workstations for individual users or pools. Authorized access can be configured at any time.

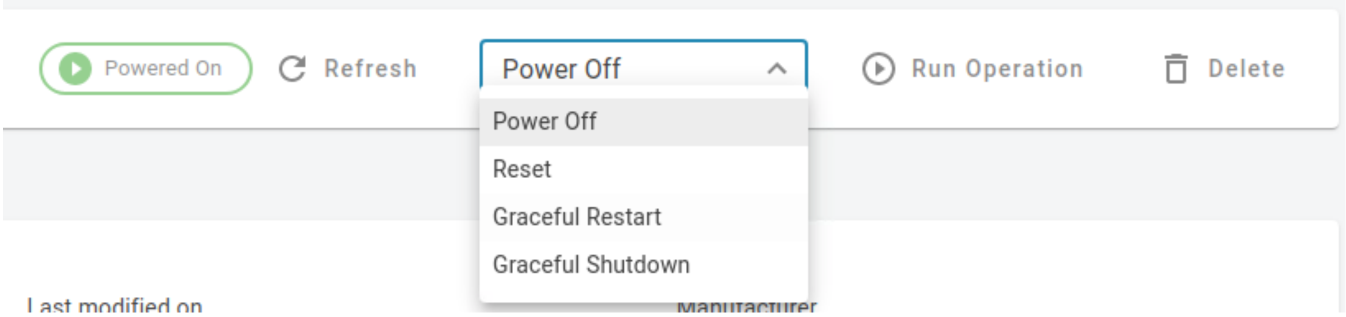
7. Open the workstation added for Intel® AMT. Under the **Provider Information** section, enable the **Managed by Anyware Manager** toggle. If the credentials are not entered an error message *This workstation cannot be managed by Intel AMT without administrator credentials* is displayed.
8. If the AMT network interface is not the same as the LAN IP/FQDN, use the Alternate AMT IP/FQDN field to specify the AMT network interface reachable by the Manager.
9. Populate the digest username and digest password for the workstation in the Intel® AMT Username and Intel AMT Password fields and click **Save Credentials**. It validates with AMT that the digest credentials are correct, even if the **Managed by Anyware Manager** toggle is off.

Workstation configuration for Intel® AMT is complete.

Intel® AMT Power Operations

Once the workstations are added and the Intel® AMT configuration is completed, you can manage power operations for each workstation in the **Workstations** or **Workstations Pools** page:

- Open a desired workstation.
- The current available power operations are shown in the drop-down menu. To change the power state, select the desired operation from the drop-down menu and click **Run Operation**.

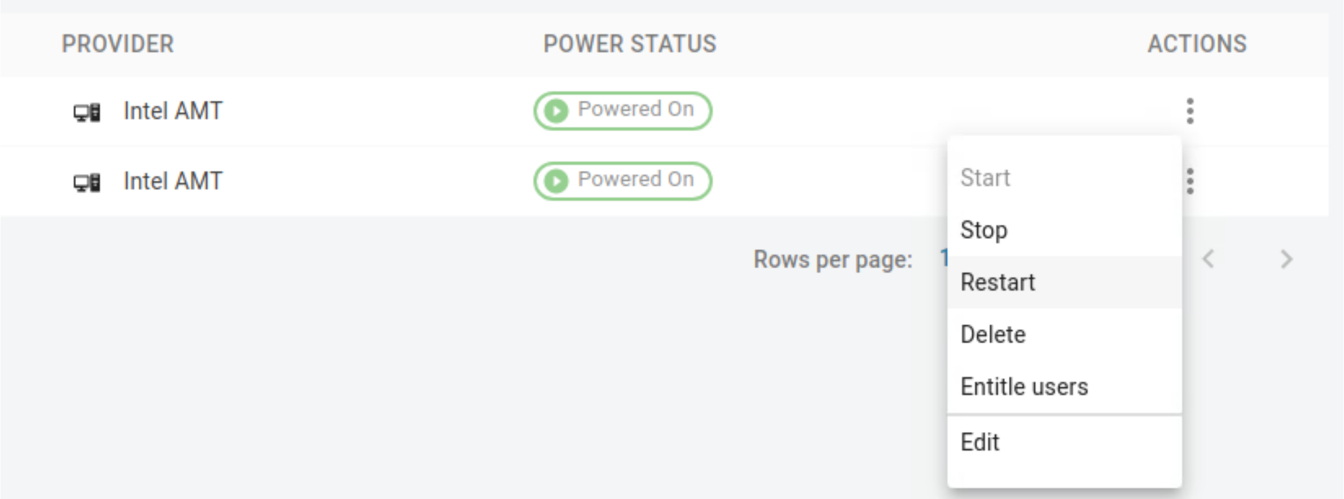


  - Available remote power operations are:
    - Power On
    - Power Off
    - Graceful Shutdown
    - Reset
    - Graceful Restart

> **Graceful Power Options**
>
> Intel® Management and Security Application Local Management is required to support graceful power operations. Graceful Shutdown requires Intel® AMT version 9 or greater and Graceful Restart requires Intel AMT version 10 or greater.

You can also execute power operations on a single workstation or on multiple workstations from the **Workstations** or **Workstations Pools** page:

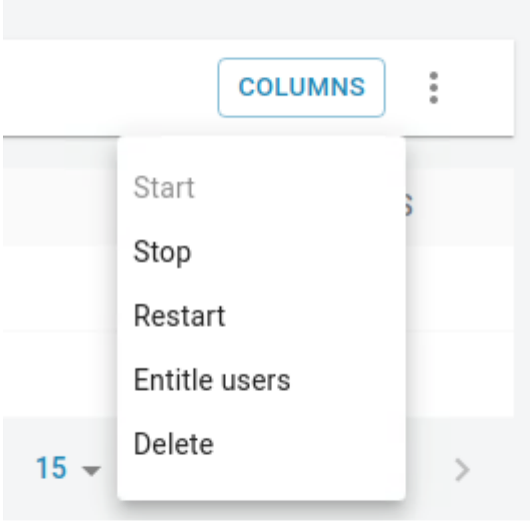
- Under the **ACTIONS** section, click the kebab option to select the desired power operation.



PROVIDER	POWER STATUS	ACTIONS
Intel AMT	Powered On	⋮
Intel AMT	Powered On	⋮

  - Available remote power operations are:
    - Start (Power On)
    - Stop (Power Off)
    - Restart (Reset)

To execute power operations on multiple workstations, select the desired workstations using the checkbox column on the leftmost side of the table and then select the kebab option on the top right next to the **COLUMNS** button and choose the desired power option.



For a Pool of workstations follow the same steps as above from the **Workstations Pools** page.

Power Operation Cooling time

Once a power operation is triggered, the Manager does not permit another power operation to be sent for 20 seconds in order to protect the AMT device.

Intel® AMT Troubleshooting Errors

When interacting with an Intel® AMT workstation in Anyware Manager, some errors can occur. Reference the following table for more information on these errors.

Error Message	Interpretation
Network timeout occurred	A network timeout occurred when trying to reach the workstation on the provided FQDN/IP. The workstation could not be reached.
FQDN/IP does not match AMT certificate subject	The certificate representing the individual AMT workstation did not have a Common Name or Subject Alternative Name matching the FQDN/IP provided in the Manager to connect to the workstation. These fields must match in order for the Manager to have confirmation it is interacting with the intended workstation.
AMT root certificate does not match Intel provider CA certificate	The root certificate which signed the individual AMT workstation certificate does not match the root certificate which was entered into the Intel Provider Service Account page. The root certificate present in the chain of the workstation certificate is not trusted.
Error validating management credentials:	There was an error while trying to verify digest credentials for the workstation with AMT. See error text for details.
No credentials found.	No digest credentials have been saved for the workstation, so the Manager cannot interact with AMT.

System Alerts

Anyware Manager System Alerts

Anyware Manager monitors all workstations in your deployment managed by Intel® AMT for system alerts. The alerts in the AMT log appear as errors on Workstations in the Anyware Manager console until they are resolved.

There are some prerequisites for enabling systems alerts. They are:

- Workstations should be Intel® AMT provisioned.
- Workstations should be managed by Intel® AMT Provider in Anyware Manager.
- For HP ZCentral 4R Workstations, the ZCentral Hardware Monitor package should be installed to detect Power Supply alerts.

Supported System Alert Events

Following system alert events are supported for all Workstations that meet the prerequisite criteria:

System Boot Errors

For all AMT Management enabled Workstations:

- **Host OS shut down unexpectedly:** This error occurs if the Operating System has a critical failure. In Windows Systems this is usually seen as a *Blue Screen* error. Resetting the Host is a way to recover from this error, but further maintenance could be required if the problem persists.
- **Host failed to boot to the OS:** This error occurs if the Host is unable to boot the operating system in a timely manner or when there's an issue during the POST action. Resetting the Host is a way to recover from this error, but further maintenance could be required if the problem persists.

Power Supply Errors

For HP ZCentral 4R Workstations with AMT Management enabled:

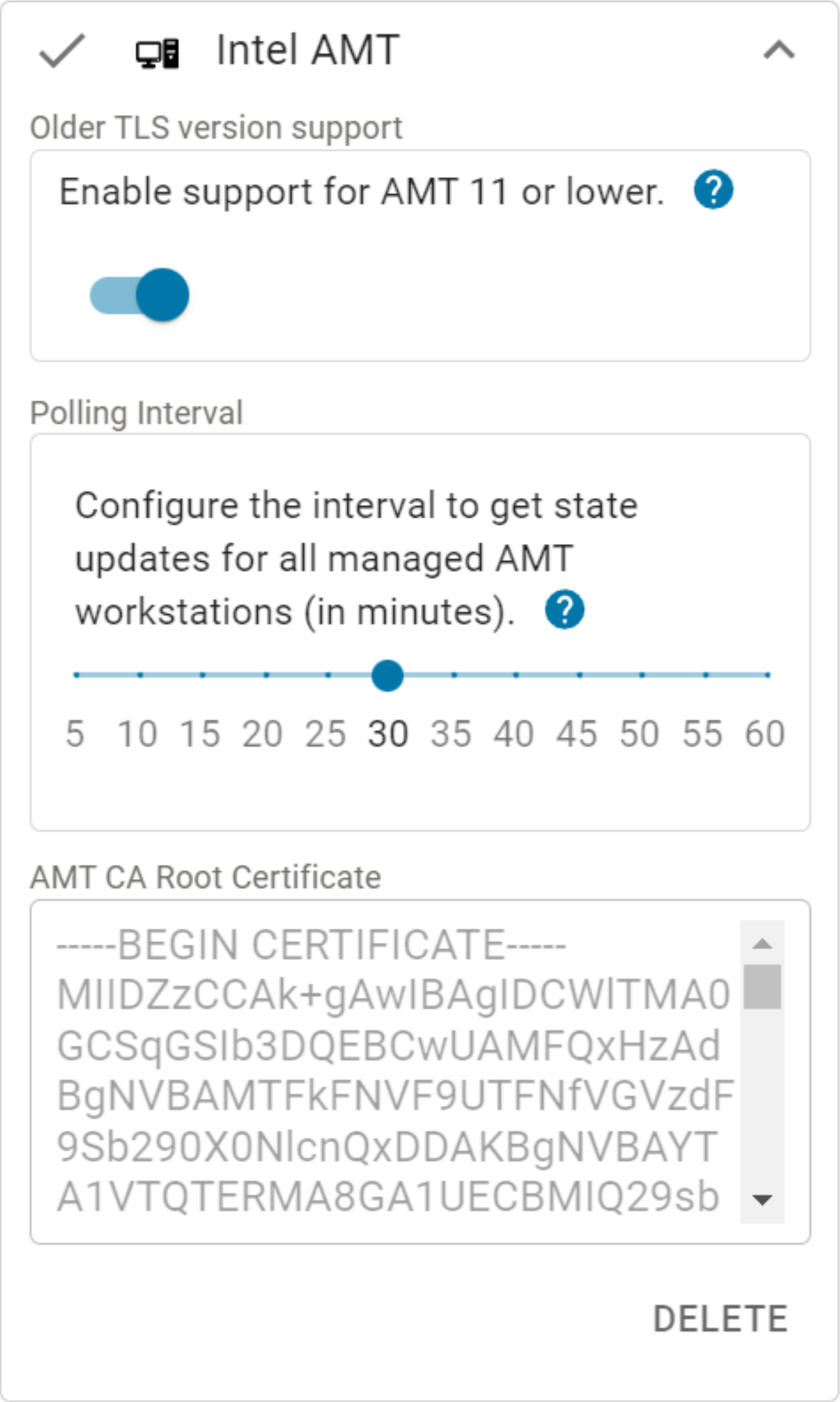
- **Two Power Supply Units installed in Redundant Mode (one Power Supply Unit is offline. Thus, no redundancy):** This error occurs when the Workstation detects one of its power supplies is offline. In this case, the power supply redundancy is compromised. There could be a problem with the Power Supply.
- **Two Power Supply Units installed in Non-Redundant Mode (one Power Supply Unit is offline. System is in a lower power configuration):** This error occurs when the Workstation detects one of

its power supply is offline. In this case, the power supplies power output is compromised. There could be a problem with the Power Supply.

Configure System Alert checks

Anyware Manager checks for system alerts on all AMT managed Workstations at a regular interval. Workstations that are actively being viewed in the Admin Console can be expected to be polled more frequently than the configured polling interval. The Interval can be configured as follows:

1. In **Admin Console**, navigate to the **PROVIDER SERVICE ACCOUNTS**.
2. Ensure a CA Root Certificate is uploaded. If not, paste or upload a CA Root Certificate and click **Submit**.
3. When the certificate is submitted, you can see a slider. Move the slider to adjust the system alert time interval.



✓ Intel AMT

Older TLS version support

Enable support for AMT 11 or lower. ?

Polling Interval

Configure the interval to get state updates for all managed AMT workstations (in minutes). ?

5 10 15 20 25 **30** 35 40 45 50 55 60

AMT CA Root Certificate

```
-----BEGIN CERTIFICATE-----
MIIDZzCCAk+gAwIBAgIDCWlTMA0
GCSqGSIb3DQEBCwUAMFQxHzAd
BgNVBAMTFkFNVF9UTFNfVGVzdF
9Sb290X0NlcnQxDDAKBgNVBAYT
A1VTQTERMA8GA1UECBMIQ29sb
```

The polling interval for system alerts is now configured.

Anyware Monitor

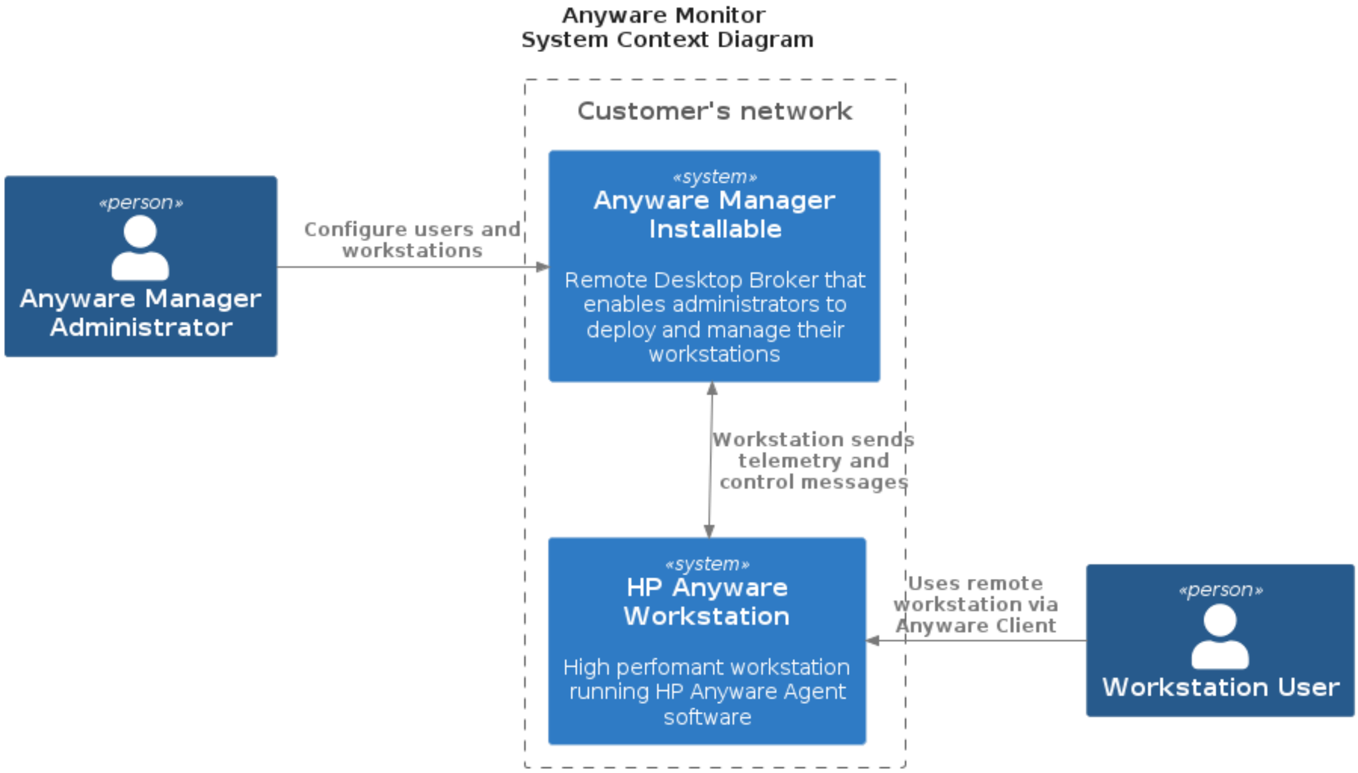
Using Anyware Monitor

Anyware Monitor enables you to review and monitor the connection health and general information regarding the remote workstations configured in your deployment. The Monitor also allows you to monitor connection status, manage sessions with remote workstations, log off users from remote workstations, and send notifications to the remote workstation.

Anyware Monitor Architecture

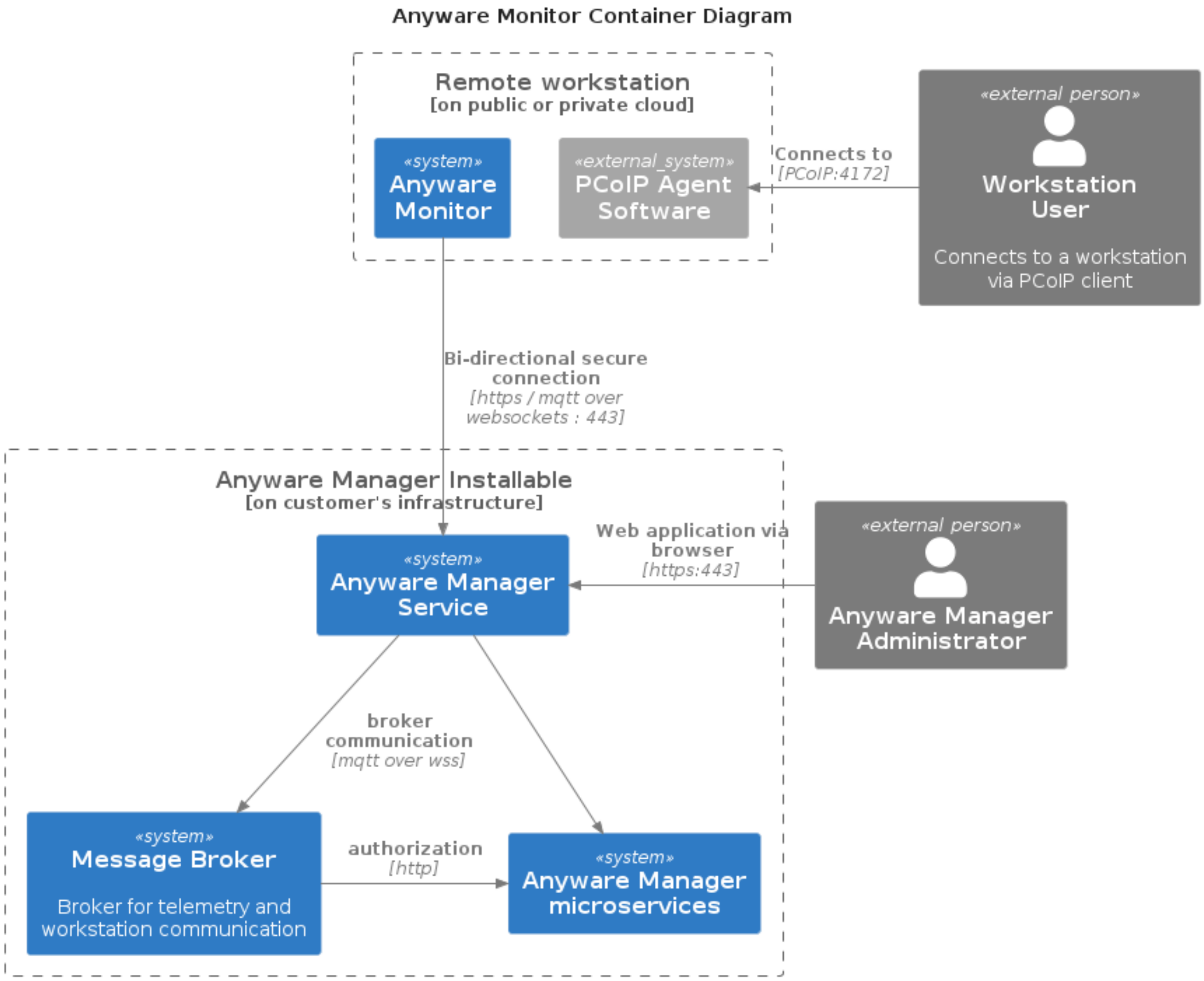
Anyware Monitor System Context

The following diagram provides the context of the overall Anyware infrastructure and the actors that are involved in it. The Anyware Manager Administrators can configure the users and the corresponding workstations using Anyware Manager and users can connect to those workstations remotely using a PCoIP Client.


Anyware Monitor
System Context Diagram
Customer's network
«person»
Anyware Manager Administrator
Configure users and workstations
«system»
Anyware Manager Installable
Remote Desktop Broker that enables administrators to deploy and manage their workstations
Workstation sends telemetry and control messages
«system»
HP Anyware Workstation
High perfomant workstation running HP Anyware Agent software
Uses remote workstation via Anyware Client
«person»
Workstation User

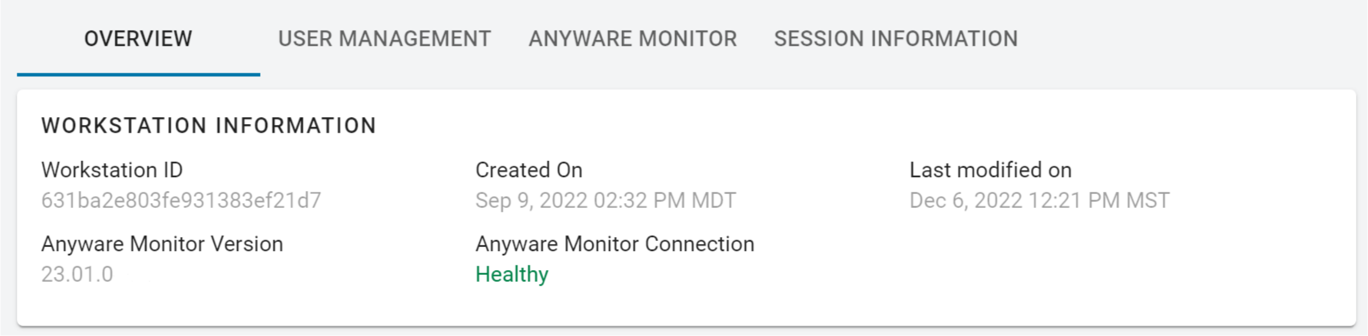
Anyware Monitor Container Diagram

The following diagram depicts the various components and the role of Anyware Monitor in the HP Anyware architecture.


Anyware Monitor Container Diagram
Remote workstation
[on public or private cloud]
«system»
Anyware Monitor
«external_system»
PCoIP Agent Software
Connects to
[PCoIP:4172]
«external_person»
Workstation User
Connects to a workstation via PCoIP client
Bi-directional secure connection
[https / mqtt over websockets : 443]
Anyware Manager Installable
[on customer's infrastructure]
«system»
Anyware Manager Service
Web application via browser
[https:443]
«external_person»
Anyware Manager Administrator
broker communication
[mqtt over wss]
«system»
Message Broker
Broker for telemetry and workstation communication
authorization
[http]
«system»
Anyware Manager microservices

Anyware Monitor Connection Status

The status of the Anyware Monitor on a workstation can be viewed by selecting the applicable workstation from the **Workstation Management** page. The overview and Anyware Monitor tab reports the connection status.



WORKSTATION INFORMATION

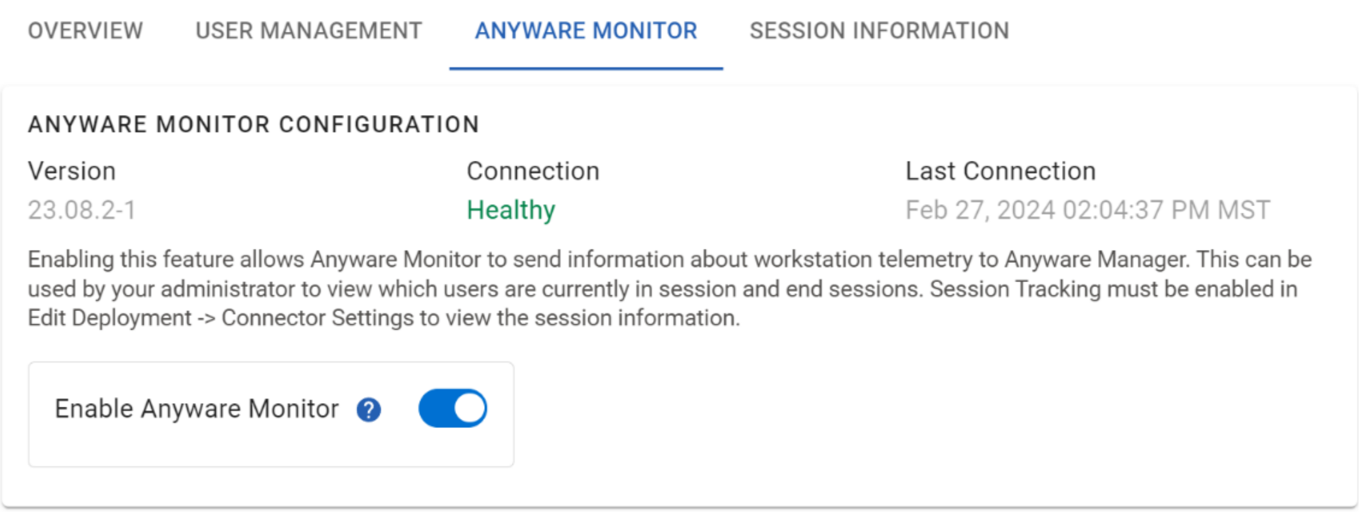
Workstation ID: 631ba2e803fe931383ef21d7

Created On: Sep 9, 2022 02:32 PM MDT

Last modified on: Dec 6, 2022 12:21 PM MST

Anyware Monitor Version: 23.01.0

Anyware Monitor Connection: Healthy



ANYWARE MONITOR CONFIGURATION

Version: 23.08.2-1

Connection: Healthy

Last Connection: Feb 27, 2024 02:04:37 PM MST

Enabling this feature allows Anyware Monitor to send information about workstation telemetry to Anyware Manager. This can be used by your administrator to view which users are currently in session and end sessions. Session Tracking must be enabled in Edit Deployment -> Connector Settings to view the session information.

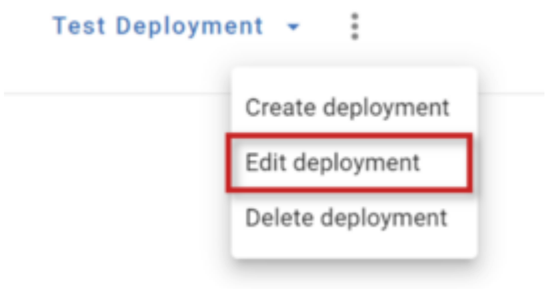
Enable Anyware Monitor: on

Session Tracking

ENABLING SESSION TRACKING

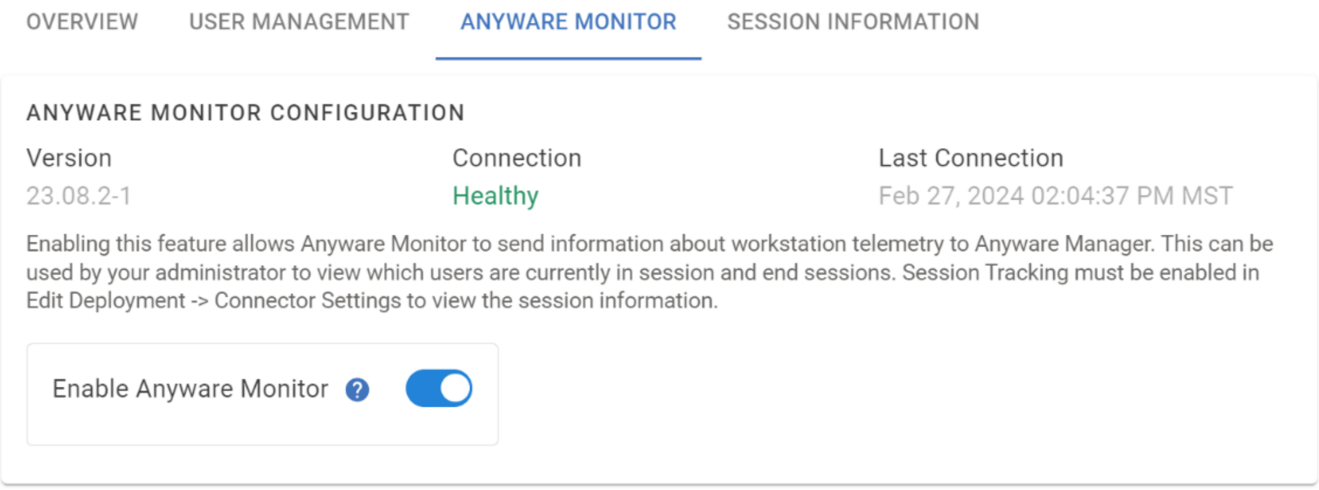
To configure the Monitor for session status tracking, the deployment Connector settings must be enabled:

1. In the Admin Console, click the kebab option in the dashboard and select **Edit Deployment**.



2. Navigate to the **Connector Settings** and enable the **Session Tracking** Toggle.

3. Navigate to the **Anyware Monitor** section in the **Workstations** tab and enable the **Enable Anyware Monitor** toggle.



ANYWARE MONITOR CONFIGURATION

Version	Connection	Last Connection
23.08.2-1	Healthy	Feb 27, 2024 02:04:37 PM MST

Enabling this feature allows Anyware Monitor to send information about workstation telemetry to Anyware Manager. This can be used by your administrator to view which users are currently in session and end sessions. Session Tracking must be enabled in Edit Deployment -> Connector Settings to view the session information.

Enable Anyware Monitor ? ●

The Anyware Monitor Session tracking is now enabled.

SESSION TRACKING

When the Monitor is enabled and is in a **Healthy** state, session information can be viewed in the Workstation's **Session Information** tab or in the **Session** column in the **Remote Workstations** table.

The Monitor reports the username in session with the following session states:

- In Session - A user is logged into a desktop session.
- Ending Session - A pending state while the monitor attempts to log users off.
- No active users found for this workstation - No users are logged into a desktop session.

> **In the Remote Workstations tables' session column, the session state can be viewed by hovering over the username.**

> **Note**
>
> The Monitor reports a user In Session when it detects any user(s) logged into a desktop session, and is not limited to PCoIP sessions.

LOG OFF WORKSTATION SESSION

When managing session tracking, the Anyware Monitor provides the ability to log users off of workstations. This gives the benefit of releasing PCoIP connections to free up licenses as well as cleaning up the workstation for next user.

To disable this feature on an individual workstation, disable the **Enable Anyware Monitor** toggle within the Workstation's Anyware Monitor tab.

Scope of Log Out

This action only logs out users logged into a desktop session, not a tty session.

There are four ways users can be logged out from a session with a workstation.

Floating pool log out user when floating assignment is ended

When the user's floating assignment with a workstation in the floating pool is ended, the user is logged off to free up the PCoIP session and free up the workstation to other users who can access the pool.

Persistent Pool log out user when user is unassigned

When a user is unassigned from a workstation in a persistent pool, the user is logged off to clean up the workstation. Similarly, if you assign a new user to a workstation that is already assigned to a current user, the current user is logged off to clean up the workstation.

Removing user assignment from workstation

In the Workstation's **User Management** page, when a user is unassigned from a workstation, that user is logged off to free up the workstation for another assignment.

Admin manually logs out user in a session

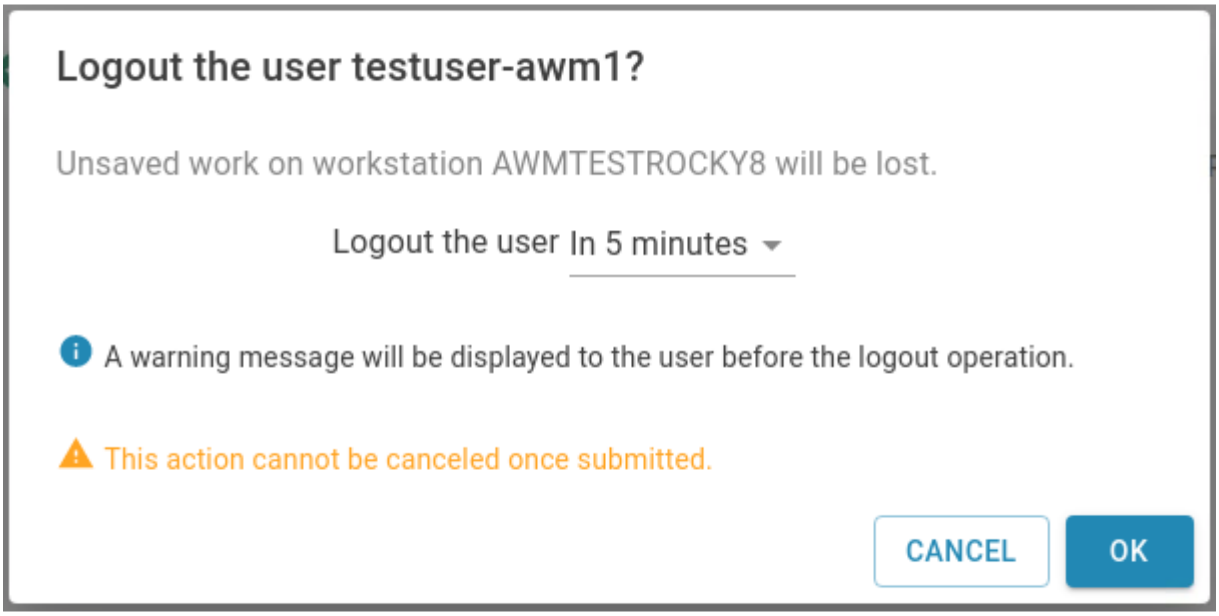
You can manually log off a PCoIP session to free up the workstation for a new user.

There are three ways to manually log out users:

- In the Workstation's **Session Information** tab, select the **logout** icon under the Actions column.
- In the **Session** column of the **Remote Workstations** table, click the username of the user to be logged out.

- In the actions column of the **Remote Workstations** table, click the actions button and click "Logout users". This method logs out all users from the selected workstation.

Select a timespan in which to log out the user and confirm the action.



Logout the user testuser-awm1?

Unsaved work on workstation AWMTESTROCKY8 will be lost.

Logout the user In 5 minutes ▾

ⓘ A warning message will be displayed to the user before the logout operation.

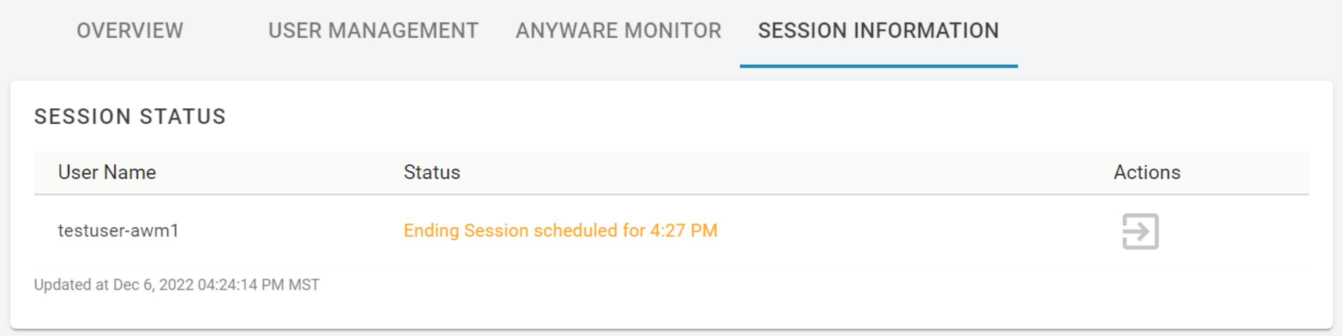
⚠ This action cannot be canceled once submitted.

Anyware Monitor Manual Log out

This action is possible for any workstation regardless of its Pool association, and only logs out users in a desktop session, not a tty session.

For logouts that are not immediate, the admin console shows the time at which the logout occurs:

- **Session Information** tab shows the logout time in the **Status** column

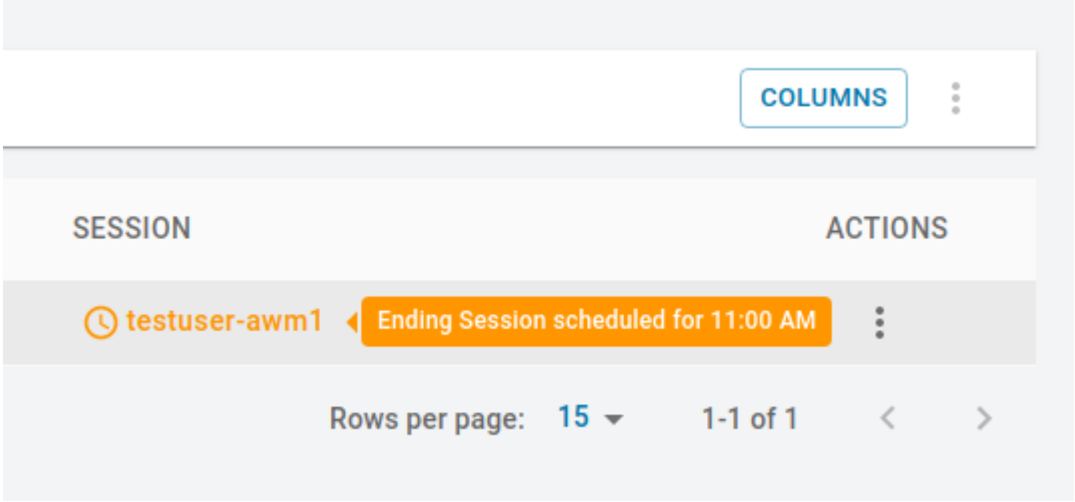


SESSION STATUS

User Name	Status	Actions
testuser-awm1	Ending Session scheduled for 4:27 PM	

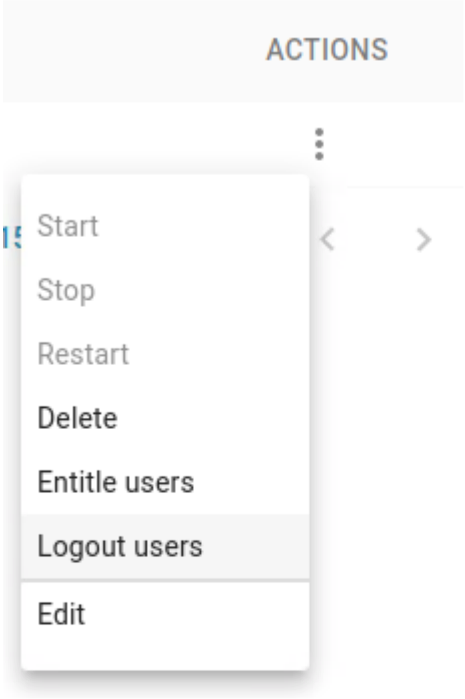
Updated at Dec 6, 2022 04:24:14 PM MST

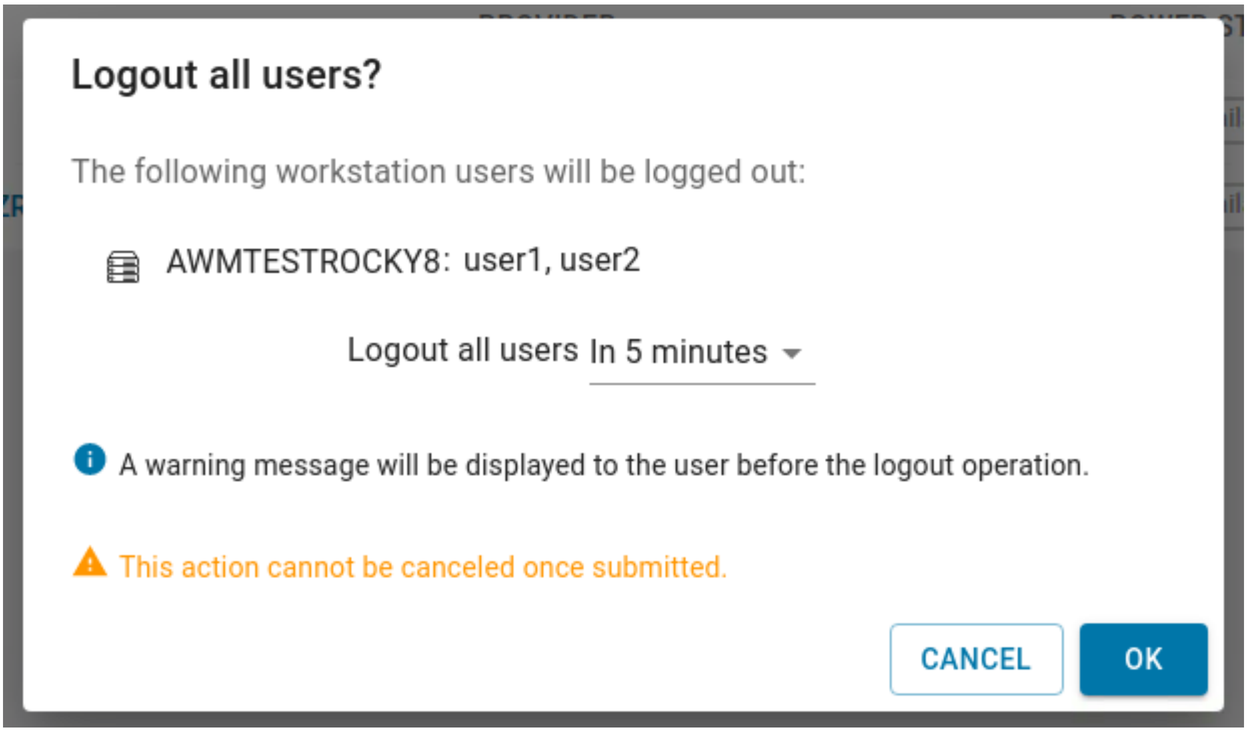
- **Session** column of the **Remote Workstations** table shows the logout time upon hovering over the username



Multiple users logout

If you have more than one user logged into a remote workstation, you can log them out by clicking in the actions column of the **Remote Workstations** table





Logout all users?

The following workstation users will be logged out:

AWMTESTROCKY8: user1, user2

Logout all users In 5 minutes

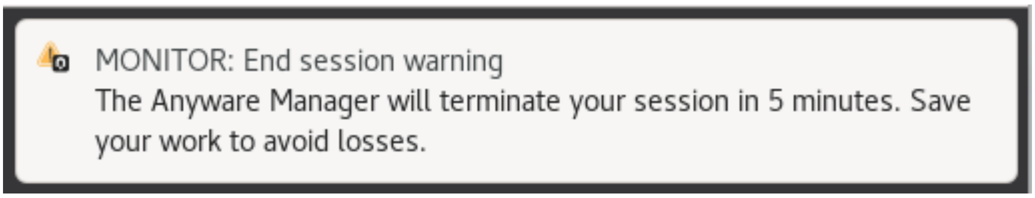
A warning message will be displayed to the user before the logout operation.

This action cannot be canceled once submitted.

NOTIFICATIONS

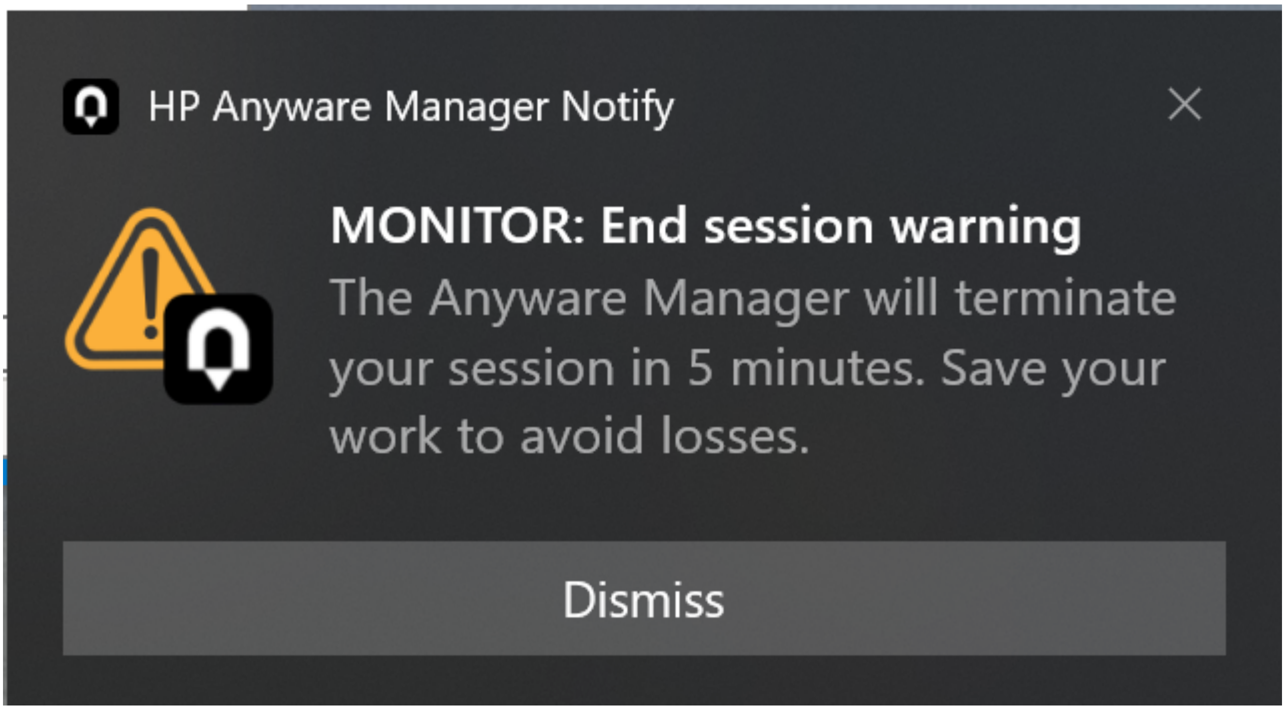
When a logout is scheduled, a notification warning is displayed that a logout occurs approximately 5 minutes before the scheduled logout time. For immediate logouts, there is no logout notification.

- Example of logout warning notification on Linux



MONITOR: End session warning
The Anyware Manager will terminate your session in 5 minutes. Save your work to avoid losses.

- Example of logout warning notification on Windows



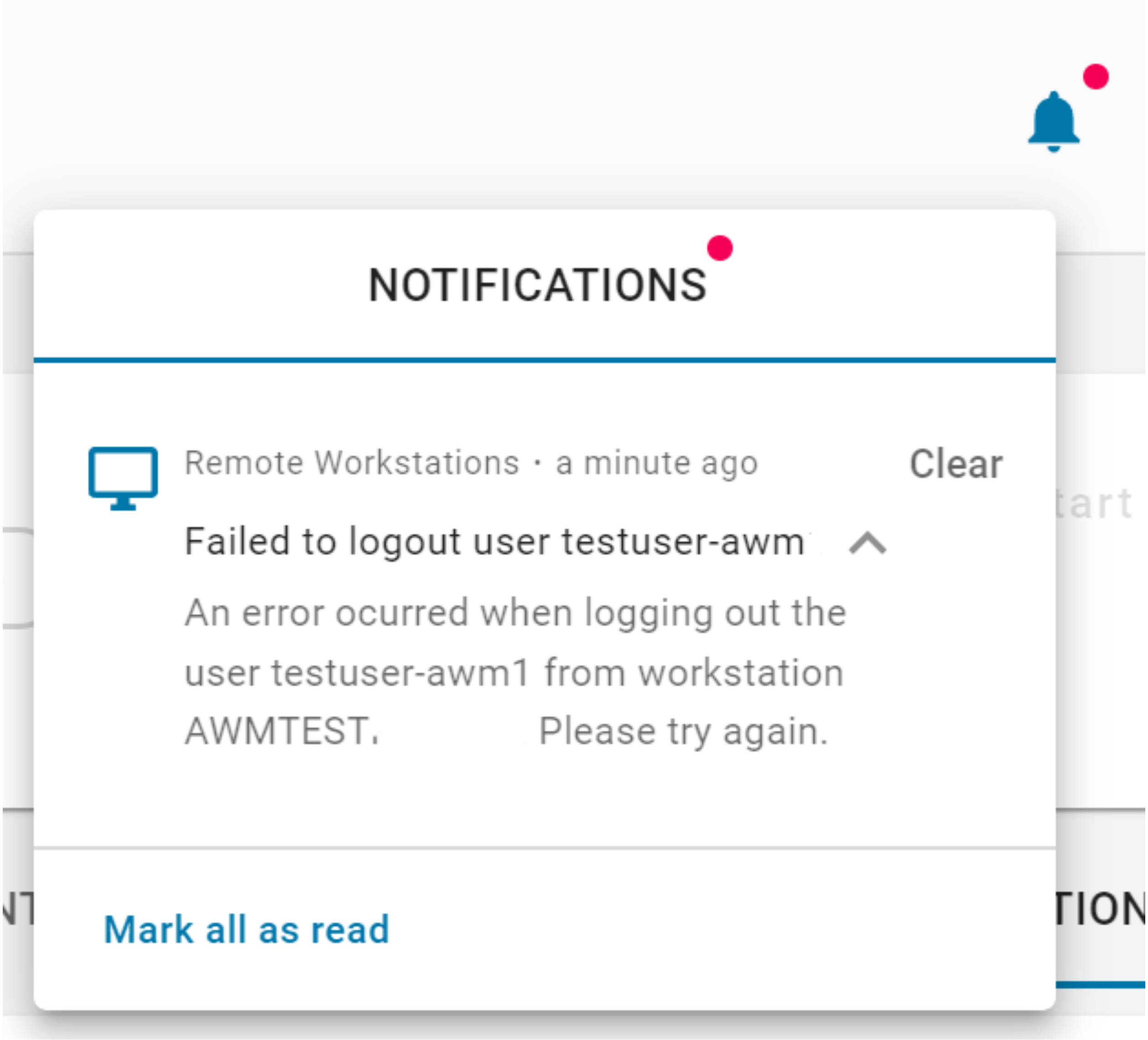
HP Anyware Manager Notify

MONITOR: End session warning

The Anyware Manager will terminate your session in 5 minutes. Save your work to avoid losses.

Log out Attempt

If the user is not logged out due to network errors, the notification center warns the admin that the log out attempt was unsuccessful.



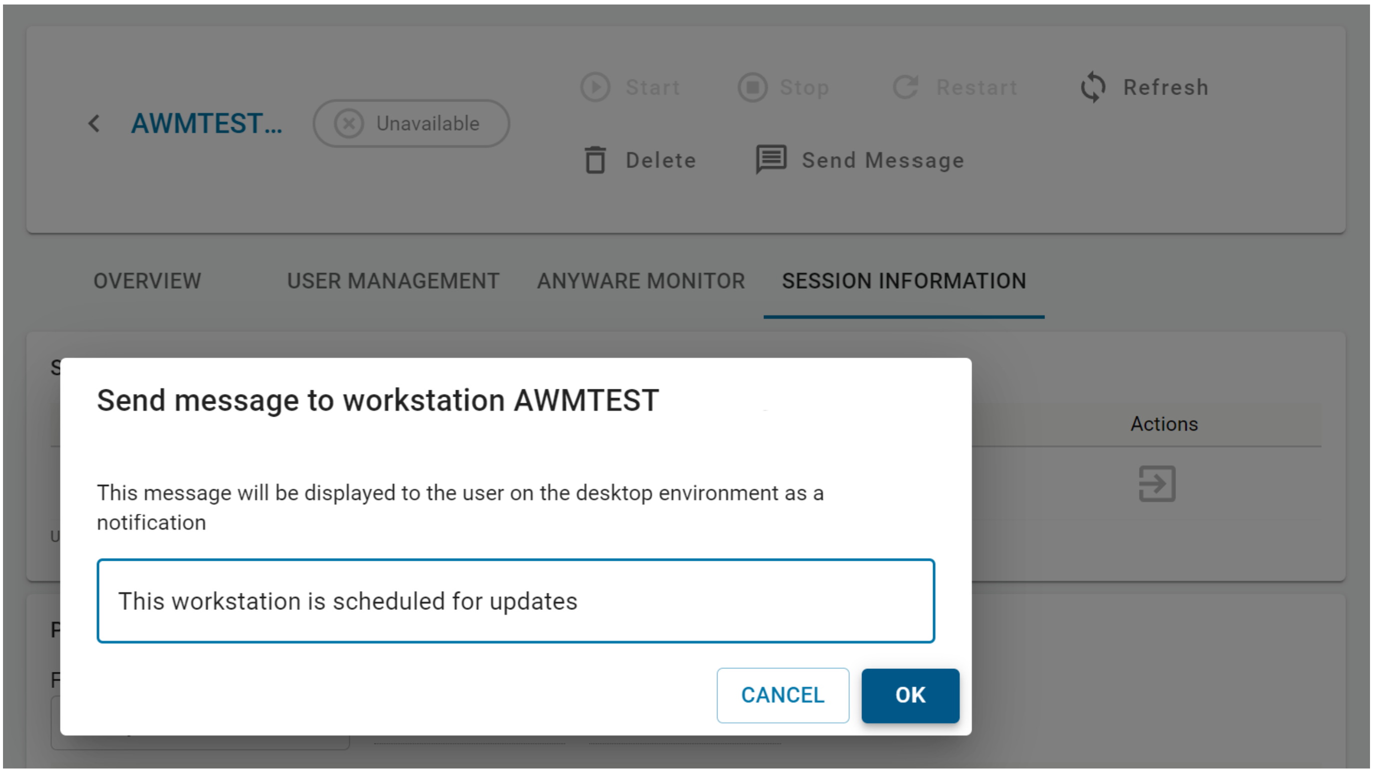
Failed to logout user testuser-awm

An error ocurred when logging out the user testuser-awm1 from workstation AWMTEST. Please try again.

Manual Notifications

You can send a notification to the workstation with any message of your choosing.

In the **Workstation** page, select **Send Message**, fill in message, and select **OK**.



Send message to workstation AWMTEST

This message will be displayed to the user on the desktop environment as a notification

This workstation is scheduled for updates

The workstation displays the message to any currently logged in users of a desktop session.

Notifications on Windows workstations

Notifications must be enabled on Windows to show Monitor Notifications. Instructions to enable notifications can be found in Enabling notifications on Windows 10 and 11.

Notification Support for Linux

Notifications are not currently supported on Wayland Display server on Linux, so if you are using a version of Linux that uses Wayland by default (Ubuntu 18.04 or later, CentOS / RHEL 8 and later), you need to disable it, and use the Xorg server instead.

If you have already installed a PCoIP Agent, the installer disables Wayland for you. If not, follow the steps below to disable it:

1. Locate the correct configuration file for your OS.
   - Ubuntu- `/etc/gdm3/custom.conf`
   - CentOS/RHEL- `/etc/gdm/custom.conf`
2. Open the file with `sudo/root privileges` command.

3. Uncomment `WaylandEnable=false` by deleting the `#` at the beginning of the line.
4. For the changes to take effect, choose from one of the following methods:
   - Reboot the system
   - In the terminal, run the command `sudo systemctl restart gdm`

Restarting the gdm will close all open applications and log out all logged in users.

Installing/Uninstalling Anyware Monitor

Anyware Monitor is an official component of the HP Anyware Software that can be installed on remote workstations, and you can enable it from the **Admin Console**.

Installing Anyware Monitor

Anyware Monitor is supported on the following operating systems:

- Windows 10 Professional 22H2
- Windows 10 Enterprise 21H2, 22H2
- Windows 11 Professional 22H2
- Windows 11 Enterprise 21H2, 22H2
- Windows Server 2019, 2022
- Ubuntu 22.04 LTS
- RHEL 8
- Rocky Linux® 8

To install **Anyware Monitor**:

1. Open the Admin Console, and navigate to the **Workstations Management** page.
2. From the list of all active remote workstations, select the workstation on which you wish to install the Anyware Monitor.
3. Select the **Anyware Monitor** tab.
4. If the End user license agreement (EULA) is present, read and accept the EULA.

> **Once accepted, End user license agreement (EULA) for Anyware Monitor does not appear again unless it is updated.**

Anyware Monitor Functionality

On accepting the EULA, the Anyware Monitor defaults to enabled, but can be toggled at any time. Disabling the Anyware Monitor stops the Monitor from sending telemetry data to the Anyware Manager and disables session tracking and logout functionality.

5. Choose a TLS validation level.

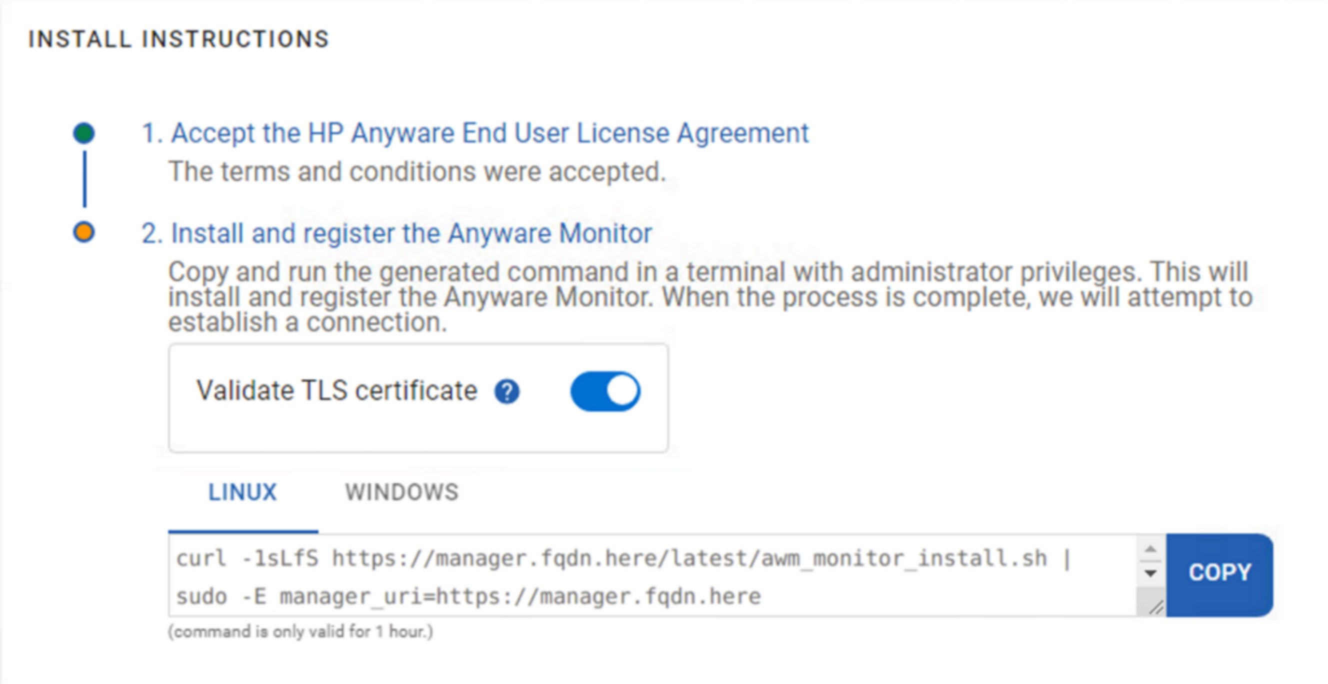
   The Anyware Monitor installer automatically generates certificates to ensure that communication to the Anyware Manager is done over encrypted TLS connections. No validation of any certificate will occur when the "Validate TLS certificate" toggle is switched off. This toggle should be switched off if the Anyware Manager is using its default certificates.

   When choosing the default option to verify the TLS certificate, the Anyware Manager needs to be configured with a valid TLS certificate issued by a certificate authority, and the Anyware Monitor host operating system needs to trust this certificate. For more information regarding how to configure the Anyware Manager to use a custom TLS certificate, see Configuring Custom TLS Certificates.

Anyware Monitor Downloads

Downloads for Anyware Monitor are serviced by dl.anyware.hp.com. If the download command fails to reach dl.anyware.hp.com, downloads are serviced by the Manager. This allows installation and registration for dark sites.

6. Copy the following operating system specific command as shown in the image below:



INSTALL INSTRUCTIONS

1. Accept the HP Anyware End User License Agreement
The terms and conditions were accepted.

2. Install and register the Anyware Monitor
Copy and run the generated command in a terminal with administrator privileges. This will install and register the Anyware Monitor. When the process is complete, we will attempt to establish a connection.

Validate TLS certificate ●

```
curl -1sLfS https://manager.fqdn.here/latest/awm_monitor_install.sh |
sudo -E manager_uri=https://manager.fqdn.here
```

(command is only valid for 1 hour.)

Running this command on Workstations downloads the Anyware Monitor and its dependencies, installs the Monitor, and registers the Workstation with the Anyware Manager.

> ⚠ **Anyware Manager Installation Token**
>
> For each Workstation, you need to generate a token using a new command by following steps 1 to 5. The command carries an unique token used to identify the Workstation inside the Anyware Manager and should not be reused on different Workstations. For installing on multiple workstations with the same command, see Anyware Monitor Bulk Installation.

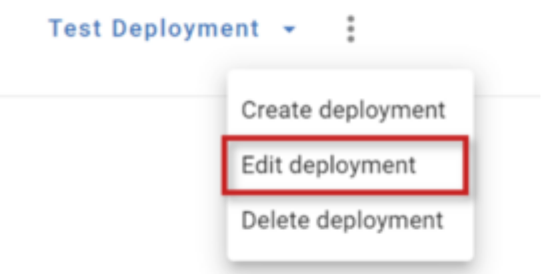
7. Run the command inside a terminal from your chosen workstation with administrative privileges.
8. Once the installation and registration has succeeded, you can see your Workstation with a connection status of Healthy. The Anyware Monitor feature is ready to use.
9. Repeat steps 1 to 8 for installing Anyware Monitor on each subsequent workstation added in Anyware Manager.

Anyware Monitor Bulk Installation

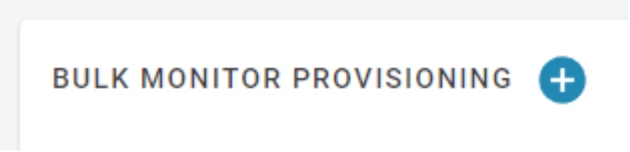
To expedite the deployment of several monitor installations, a bulk enrollment option is available. This option uses a single command that can be passed to any number of machines to start an automated process of installation and registration. It should be noted that machines do not need to be added to the **Workstations** page prior to bulk installation of the Monitor; for your convenience, the bulk installation process automatically adds new Workstations where the Monitor has been installed as long as the enrollment request is approved. For darksite installations, please see more information about the concurrent download limit below.

To facilitate Anyware Monitor Bulk installation:

1. Open the Admin Console and click the kebab option in the dashboard and select **Edit Deployment**.



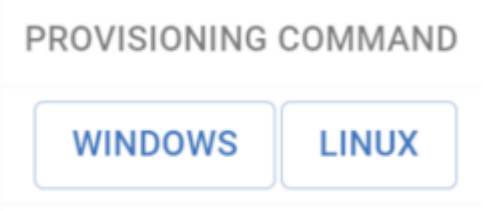
2. Navigate to the **Anyware Monitor** section in the **Workstations** tab, click "+" next to **Bulk Monitor Provisioning** and enter a Command Name.



3. If the End user license agreement (EULA) is present, read and accept it.

> **Once accepted, End user license agreement (EULA) for Anyware Monitor does not appear again unless it is updated.**

4. Choose a TLS validation level. See step 5 in Installing Anyware Monitor for details on TLS validation level.
5. Select an Operating System between **Windows** and **Linux** to generate a command that is copied to your clipboard.



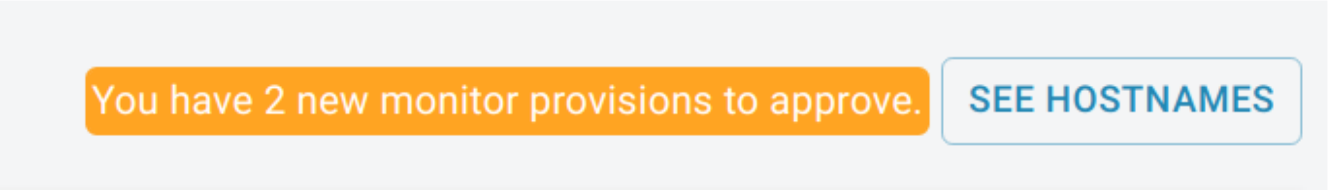
6. Run the copied command with administrator privileges on all the machines on which you want to install the Monitor.

   > ✎ **The machines do not need to be added in the workstation page before this step**

7. After the command successfully completes, Anyware Monitor is installed, but must be approved to complete registration.

   > ✎ **There is a very generous time limit on approving pending Monitor registration requests (currently set to three years, but could be subject to change in the future). As long as the enrollment account key has not been revoked, pending Monitor registration requests can be approved. This permits delayed installation of the Anyware Monitor in cases where it is desired.**

8. Navigate to the **Workstation Management** page and click on **SEE HOSTNAMES** to navigate to the Pending Monitor Provisions page.



You have 2 new monitor provisions to approve.

9. Choose one of the following actions for each machine:

ADD - Indicates that the machine has not yet been added to the Anyware Manager. Sends a message to the Anyware Monitor and gives it permission to proceed and complete registration, and adds this machine to the Workstations Page.

LINK - Indicates that the machine was already added to the Anyware Manager. Sends a message to the Anyware Monitor and gives it permission to proceed and complete registration.

REJECT - Sends a message to the Anyware Monitor that it should not proceed with registration. Once this action is selected, this machine needs to be re-enrolled or re-registered to enable Anyware Monitor.

UPDATE - Indicates that there was a mismatch between when Anyware Monitor was enrolled and the current machine was added or deleted from the workstation page. Once this action is selected, the mismatch is fixed and it is possible to either add or link. By hovering over the warning icon in the **Host Name** column, the reason for the need to update is displayed.

A healthy monitor status indicates registration was a success.

> ⚠ **Concurrent Installations on Dark sites**
>
> The Anyware Manager on a dark site can support up to 50 concurrent installs from Anyware Monitors at a time. If your deployment plan for installing Monitors requests more than 50 concurrent Monitor installs at a time, it is recommended to spread them out either consecutively or in batches of no more than 50 at a time. Failure to do so may cause moderate lag on the UI, and possible failed installations and registrations with the Manager.

Revoking Tokens

ENROLLMENT ACCOUNTS

The Key used in the Provisioning Command for Bulk Enrollment can be revoked. Once this action is completed, the generated command is no longer authorized to initiate bulk enrollment on any new workstations. Any workstations that used this token and already approved the enrollment and completed registration successfully are able to authenticate and communicate with the Manager. However, any workstations that is still pending enrollment lose the ability to complete the registration process.

To revoke an enrollment account key:

1. In the Admin Console, click the kebab option in the dashboard and select **Edit Deployment**.
2. Navigate to the **Anyware Monitor** section in the **Workstations** tab.
3. Under **Bulk Monitor Provisioning**, chose the command you want to revoke the key for, and click the trash icon under the Revoke column.

WORKSTATION ACCOUNTS

When the Anyware Monitor is installed and registered with the Anyware Manager, a service account is created that authorizes communication between the Monitor and the Manager. These service accounts are visible by navigating to the Deployment's edit page and navigating to the **Anyware Monitor** tab. This service account can be deleted.

To revoke a workstation's service account:

1. In the Admin Console, click the kebab option in the dashboard and select **Edit Deployment**.
2. Navigate to the **Anyware Monitor** tab.

3. Under **Approved Monitor Installations**, choose the workstation you want to revoke the service account for, and click on the trash icon under the Delete column.

> **Deleting Workstation Service Accounts**
>
> This action is permanent. To reestablish communication, repeat the install process to register the workstation again.

Proxy Configuration

If your machines are connected through a Proxy Server, there are two ways to add the Proxy details to the Anyware Monitor:

- By adding proxy configuration during the bulk enrollment process.
- By running the Monitor Config executable to add proxy details to the Settings File.

ADDING PROXY CONFIGURATION IN THE ANYWARE MONITOR BULK INSTALLATION PROCESS

Copy the provisioning command from the bulk installation page for the selected operating system. (See Anyware Monitor Bulk Installation)

Edit the script adding the Proxy URI after the manager URI, like the following examples:

Linux

```
curl -1sLfS https://dl.anyware.hp.com/token/anyware-manager/raw/names/anyware-monitor-sh/versions/latest/anyware-monitor_latest.sh | sudo -E manager_uri=https://mymanagerfqdn proxy_uri=https://myproxyserver:port  token=enrollment_token mode=enroll channel=stable download_token=token bash
```

Windows

```
powershell.exe -noexit ". { Set-Variable ProgressPreference SilentlyContinue; Invoke-WebRequest -useb https://mymanagerfqdn/anyware-monitor/versions/latest/anyware-monitor_latest.ps1 } | Invoke-Expression; install -manager_uri https://mymanagerfqdn -proxy_uri https://myproxyserver:port -token enrollment_token  -mode enroll -channel stable -download_token token;exit"
```

Your commands may look different if you choose to disable TLS validation when generating your command.

ADDING THE PROXY SERVER ADDRESS TO THE MONITOR SETTINGS FILE

If the Monitor is already installed and registered, you can run the Monitor Config executable to add the proxy server address.

Linux

Run the following command and replace the Proxy URI with your Proxy address: `sudo /opt/awm-monitor/awm_monitor_config configure-settings --proxy-uri=https://myproxyserver:port`

Windows

Using a terminal with administrator privileges, navigate to the Anyware Monitor install folder (default path):

`%PROGRAMFILES%\HP\Anyware Manager Monitor`

Then run the following command and replace the Proxy URI with your Proxy Server address:

`awm_monitor_config.exe configure-settings --proxy-uri https://myproxyserver:port`

REMOVING PROXY CONFIGURATION FROM ANYWARE MONITOR

If you are no longer running a proxy server and wish to remove the Proxy configuration from the Anyware Monitor, it can be easily done.

Linux

Run the following command:

`sudo /opt/awm-monitor/awm_monitor_config reset-settings --proxy-uri`

Windows

Navigate to the Anyware Monitor install folder using a terminal with administrator privileges: Program Files > HP > Anyware Manager Monitor

Run the following command: `awm_monitor_config.exe reset-settings --proxy-uri`

Removing HP Anyware Monitor

If you do not require the Anyware Monitor, it can be easily removed/uninstalled.

For Windows OS:

1. Navigate to **Add or Remove Programs** in the Windows settings.
2. Locate the HP Anyware Monitor instance and click **Uninstall**.

For Linux OS:

Use the package manager to remove the `awm-monitor` package. You can run the following commands:

Example for Ubuntu:

With apt:

```
sudo apt remove awm-monitor
```

Example for RHEL:

With yum:

```
sudo yum remove awm-monitor
```

With dnf:

```
sudo dnf remove awm-monitor
```

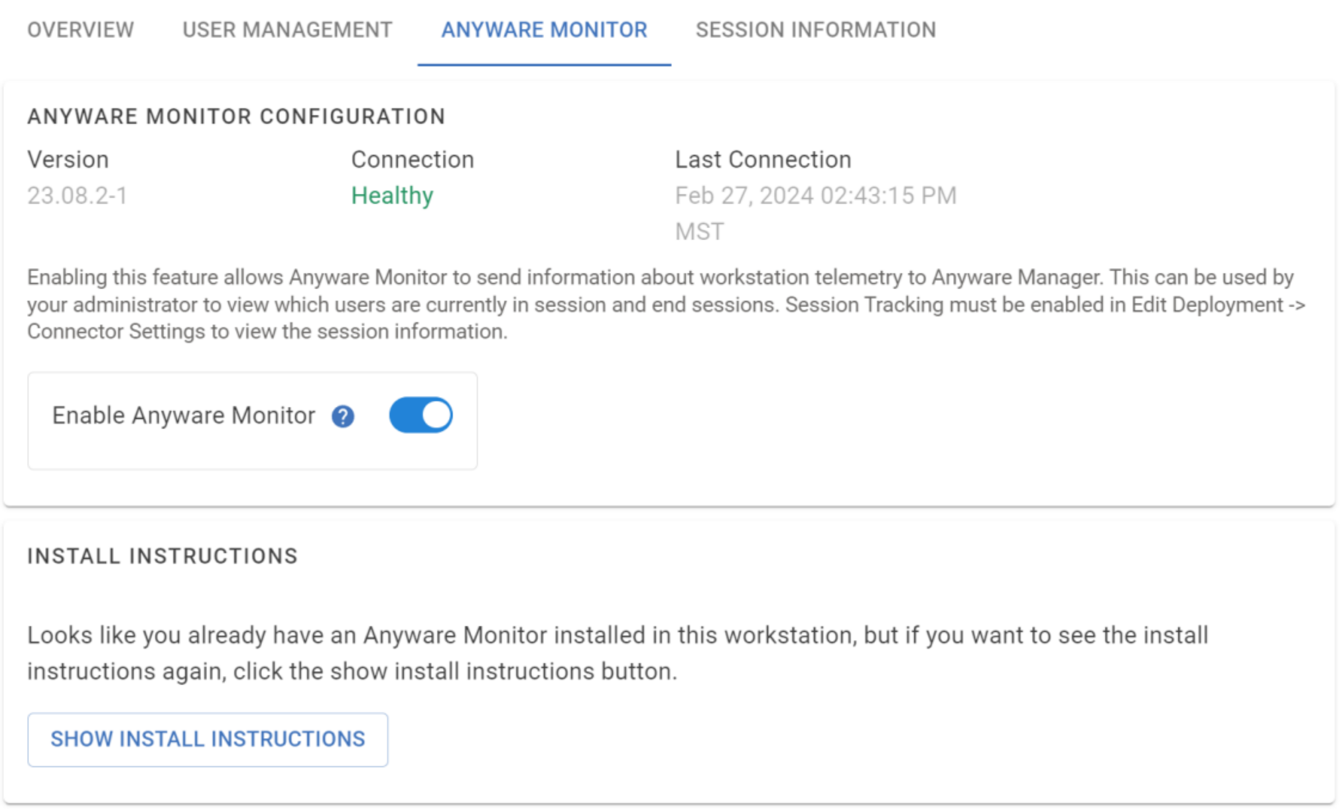
Troubleshooting Anyware Monitor

In the event that there is an issue with the Anyware Monitor, the following rectification steps may be useful to help fix the issue. Some of the known issues with the Anyware Monitor are:

REGISTRATION FAILS AFTER INSTALLATION OR MONITOR FAILS TO START AFTER INSTALLATION

Occasionally the network may fail during registration process or it is possible that the authorization token that the script carries has expired. If the registration fails and the token is less than one hour old, run the install script again.

> **If the registration fails and the token is more than one hour old, generate a new script command with a refreshed token by navigating to the Workstation's Anyware Monitor tab and select Show Install Instructions for a refreshed command and try again.**



ANYWARE MONITOR CONFIGURATION

Version: 23.08.2-1

Connection: Healthy

Last Connection: Feb 27, 2024 02:43:15 PM MST

Enabling this feature allows Anyware Monitor to send information about workstation telemetry to Anyware Manager. This can be used by your administrator to view which users are currently in session and end sessions. Session Tracking must be enabled in Edit Deployment -> Connector Settings to view the session information.

Enable Anyware Monitor: On

INSTALL INSTRUCTIONS

Looks like you already have an Anyware Monitor installed in this workstation, but if you want to see the install instructions again, click the show install instructions button.

WORKSTATION IS UNEXPECTEDLY MARKED AS UNHEALTHY

Restart the service using your operating system service tool:

- On Windows, click on the **Start** Menu and type `services.msc` to open the **Windows Services list**. Navigate to the HP Anyware Monitor service, select and restart it using the left pane menu.
- On Linux®, open a terminal and run the command: `systemctl restart awm-monitor`.

Ensure system clocks are synced The Anyware Monitor health status, displayed in the Anyware Manager, relies on regular time-stamped messages coming from the Monitor. If the system clocks are off by more than a minute, the Manager may report that the Monitor status is unknown. To prevent this, ensure both the Monitor and Manager system clocks are in sync.

NOTIFICATIONS DO NOT APPEAR IN A WORKSTATION AS EXPECTED

Ensure that your machine has PCoIP Agent installed on it:

- On Windows, ensure that notifications are enabled. For more information, see Enabling notifications on Windows 10 and 11.
- On Linux, ensure that you have it configured to not use Wayland display server. For more information, see Manual Notifications.

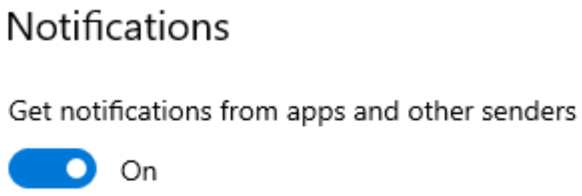
There is a known issue in Linux machines where notifications may not be displayed to the user. While most supported Linux desktop configurations are expected to work, there are rare instances where the system is unable to identify the user's desktop session id required to issue a notification.

In this case, a default location is used. If a Linux system is not showing notifications, the log may state "Using default dbus address". This location is not guaranteed to be present either, resulting in the system incapable of rendering a notification.

ENABLING NOTIFICATIONS ON WINDOWS 10 AND 11

You can enable notifications by performing the following steps:

1. Navigate to **Start** menu and click **Settings**.
2. Click the **System** tab and select **Notifications & actions**.
3. Enable the **Notifications** toggle.



Notifications

Get notifications from apps and other senders

On

You can also enable notifications by editing Windows Registration using a PowerShell Command and restarting the workstation.

Run the following command:

```
Set-ItemProperty -Path "HKCU:
\Software\Microsoft\Windows\CurrentVersion\PushNotifications" -Name
"ToastEnabled" -Type DWord -Value 1
```

These actions only enable notifications for the current user. This can be further automated to apply the setting for multiple users.

BULK ENROLLMENT FAILURES

Running the command outputs a TLS/SSL error

- Check the configuration of certificates on the machines, or disable the certificate validation toggle for the bulk provisioning command and run again.

Enrollment Fails with exit error code of 1

- The console should output error messages that can help determine the root cause. When in doubt, generating a new command and trying again should help to resolve the issue.

Enrollment fails with error: "The Anyware Monitor was unable to detect a hostname or IP address required for Bulk Enrollment."

- Bulk Enrollment requires a hostname or IP address. The system will try to detect this. In the rare event that the system cannot detect a hostname or IP address, one of the following options is recommended:
  - Ensure that the machine's hostname is configured properly.
  - Register this machine independently. For more information, see Installing/Uninstalling Anyware Monitor.

After Adding or Linking the machine, the machine does not show as Healthy after some time

- The Monitor tries to proceed with registration when you choose the **ADD** or **LINK** option for a machine during installation. If there is a temporary network issue, the message may not be received or there may be an issue with registration. To help determine root cause, inspect the Monitor logs. For more information, see Anyware Monitor Logs.

ANYWARE MONITOR LOGS

For information and diagnostic purposes, Anyware Monitor records logs internally to a file.

- In the affected Workstation, navigate to the folder where HP Anyware Monitor is installed:
  - On Windows (by default): `%PROGRAMFILES%\HP\Anyware Manager Monitor`
  - On Linux: `/opt/awm-monitor`
- Open the file log4net.config using a Text Editor.
  - Change the line <level value="INFO"> to <level value="DEBUG">.
  - Save the changes you have made to the file.
- Restart the HP Anyware Monitor service:
  - On Windows, click on the Start Menu and type `services.msc` to open the Windows Services list. Scroll down to the HP Anyware Monitor service, click on it and restart using the left side menu.
  - On Linux®, open a terminal and run the command: `systemctl restart awm-monitor`
- Reproduce the issue that you are facing.
- Navigate to the following folder to view the content of the log file:
  - On Windows: `%PROGRAMDATA%\HP\Anyware Manager Monitor`
  - On Linux®: `/var/log/awm-monitor`

> **Viewing Log content on Linux**
>
> On Linux, the log content can also be viewed realtime by running the command `sudo journalctl -u awm-monitor -f`.

HP ZCentral Hardware Monitor

HP ZCentral Hardware Monitor-Installation

The **HP ZCentral Hardware Monitor** is an optional ZCentral software component that enhances the System Alerts experience. When installed, Anyware Manager can monitor the state of Power Supply units for ZCentral 4R systems and display alerts as errors on the Anyware Manager console.

System Requirements

1. A supported hardware platform (Currently only HP ZCentral 4R workstations are supported).
2. The most up-to-date Intel® AMT Firmware.
3. Supported operating systems such as:
    - Windows 10
    - Red Hat Enterprise 7
    - Red Hat Enterprise 8
    - Ubuntu 18.04
    - Ubuntu 20.04

When installing on Windows the following are also required:

```
- Intel® Management Engine Interface Driver (Intel® Management Engine
Software [Chipset Driver] softpaq from the HP Drivers website)
- Microsoft Visual C++ 2015-2019 Redistributable
```

HP ZCentral Hardware Monitor Installation

To install the Hardware Monitor, download and run the installer package for one of the following supported platforms, which is available on the Installers page of the Anyware Manager console:

- Windows
- Red Hat 7, Red Hat 8

- Ubuntu-18.04, Ubuntu-20.04

The package includes the Hardware Monitor installer and an install script.

Install Scripts

The installer packages come with an installation script (`install.cmd` for Windows and `install.sh` for Linux) that determines the platform support for HP ZCentral Hardware Monitor. If supported, then the Hardware Monitor is installed. The installers can be executed manually if required.

- **Linux Script:** To upgrade a package, instead of performing a fresh install, the script can be passed the `--upgrade` argument. This ensures that the rpm uses the upgrade command on a Red Hat Linux OS. On a Debian OS the `dpkg` command does not change.
- **Windows Script:** By default, the script only calls *msiexec /i MSI*. Any arguments should be additionally passed to the script. This can be done for both installers or individually. Run `install.cmd` with `--help` to view the available arguments.

SIGNATURE VERIFICATION

Hardware Monitor installation packages are digitally signed to ensure security and integrity of the package upon download. You can verify these digital signatures to ensure sanctity of the installation package before installing them on your system.

A gpg key indicates who signed the package. Details for the hardware monitor gpg signature key can be found below.

- Download the public key from the link that says **Download signature key** on the installation page of the Anyware Manager console. This link becomes visible when a platform is selected from the operating system dropdown field.
- Key ID: HP ZCentral Connect hpss-admin@hp.com
- Fingerprint: 66CF 5025 AA35 1EB7 CC78 136F C75F B106 E198 51F0

You can verify *gpg* signatures using a *gpg* key. Files such as `.tar.gz`, `zip`, `.deb` have a gpg signature. The `.msi` Windows installer file has a Windows operating system signature that can be viewed by right-clicking the file and examining its security properties.

VERIFY DIGITAL SIGNATURES ON `.TAR.GZ`, `.ZIP`, `.DEB` FILES

> **Verify Signature on Windows OS**
>
> To verify gpg signatures on a Windows OS, a 3rd party tool such as **GPG4Win** is required to add GPG support.

To verify the signature:

1. Import the public key to the *gpg* key ring by running the following command:

```
gpg --import GPG-KEY-hpzcentralconnect
```

After executing this command, the output on the command line should be as follows:

```
gpg: key E19851F0: public key "HP ZCentral Connect <hpss-admin@hp.com>"
imported
gpg: Total number processed: 1
gpg: imported: 1  (RSA: 1)
```

1. Verify the signature of the `.deb`, `.tar.gz` or `.zip` file by passing the corresponding signature file (the signature file ends in the `.asc` extension) with the file to be verified. Run the following command:

```
gpg --verify hp_zcentral_hardware_monitor_rhel.tar.gz.asc
hp_zcentral_hardware_monitor_rhel.tar.gz
```

After executing this command, the output on the command line should be as follows:

```
gpg: Signature made XXX XX XXX 2020 XX:XX:XX XX MST using RSA key ID E19851F0
gpg: Good signature from "HP ZCentral Connect <hpss-admin@hp.com>"
gpg: WARNING: This key is not certified with a trusted signature!
gpg: There is no indication that the signature belongs to the owner.
Primary key fingerprint: 66CF 5025 AA35 1EB7 CC78  136F C75F B106 E198 51F0
```

Trusted Signature

If you want to remove the trusted signature warning message, you can instruct the gpg tool to trust the key by using the following commands:

```
gpg --edit-key "HP ZCentral Connect"
gpg> trust
gpg> <Select your level of trust>
gpg> quit
```

VERIFY DIGITAL SIGNATURES ON `.RPM` FILES

To verify the signature:

1. Import the public key to the `.rpm` key ring by running the following command:

```
rpm --import GPG-KEY-hpzcentralconnect
```

1. Verify the signature of the `.rpm` file by running the following:

```
rpm --checksig hpzcentralconnecthardwaremonitor.rpm
```

After executing this command, the output on the command line should be as follows:

```
hpzcentralconnecthardwaremonitor.rpm: rsa sha1 (md5) pgp md5 OK
```

Supported Events

The ZCentral Hardware Monitor scans the health of the Power Supply Units on HP ZCentral 4R workstations while the OS is running. The dual Power Supply Units (PSUs) on a 4R are each in 1 of 3 states: 1. Uninstalled. 2. Installed and Providing Power. 3. Installed and Not Providing Power.

Additionally, when 2 Power Supply Units are installed, they are configured in Redundant or Non-redundant (Aggregate) mode depending on the workload of the workstation. This configuration is done through BIOS and the Hardware Monitor gathers this information during start-up.

The following is a list of states that the Hardware Monitor is aware of:

- 2 Power Supplies installed and providing power running in redundant mode. (Good State)

- 2 Power Supplies installed and providing power running in non-redundant mode. (Good State)
- 1 Power Supply installed and providing power. (Good State)
- 2 Power Supplies installed but only 1 providing power running in redundant mode. (Error State)
- 2 Power Supplies installed but only 1 providing power running in non-redundant mode. (Error State)

HP ZCentral Hardware Monitor-Troubleshooting

In case the HP ZCentral Hardware Monitor fails or malfunctions, you should undertake the following corrective and review measures:

HP ZCENTRAL HARDWARE MONITOR LOGS

The logs for ZCentral Hardware Monitor are available in the following locations:

- On Windows: `%PROGRAMDATA%\HP\ZCentralConnectHardwareMonitor\HardwareMonitor.log`.
- On Linux®: `/var/log/hpzcentralconnecthardwaremonitor/HardwareMonitor.log`.

To change the level of information displayed in the log files, edit the `log4net.config` file and change the line to DEBUG. The `log4net.config` file is available in the following locations:

- On Windows (by default): `%PROGRAMFILES%\HP\ZCentralConnectHardwareMonitor\bin\log4net.config`.
- On Linux®: `/opt/hp/zcentralconnecthardwaremonitor/log4net.config`.

The Hardware Monitor also logs to the **Windows Event Log** under **Application logs** on a Windows OS.

HP ZCENTRAL HARDWARE MONITOR INSTALLATION ERRORS AND WARNINGS

Errors: *This application requires Microsoft Visual C++ 2015-2019 Redistributable.* - The Windows installer and the Hardware Monitor require the Visual C++ 2015-2019 Redistributable for the installation. The installation fails without it. The `vc_redist.x64.exe` package should be downloaded from Microsoft and installed before reattempting installation.

Warning: *HP ZCentral Hardware Monitor requires the Intel® Management Engine Interface driver to be installed.* - Without the Intel® Management Engine Interface driver, the Hardware Monitor service is unable to start, but it is installed. The driver can be installed by installing the Intel® Management Engine Software (Chipset Driver) softpaq for the platform. It is available for download on the HP Drivers website (https://www.hp.com/drivers). Once the driver is installed the service can be started.

HP ZCENTRAL HARDWARE MONITOR ERRORS

Error Code	Error Message	Resolution
2	Logger could not be configured. Ensure log4cpp.config is present and correctly formatted.	Ensure the file exists and has not been corrupted. To recreate this file, please reinstall the Hardware Monitor.
3	Unable to access SMBIOS information.	Ensure service is running with administrator permissions and BIOS is up to date.
4	SMBIOS does not contain System Info (Type 1) table.	Ensure the most current version of the supported BIOS is in use.
5	SMBIOS does not contain Power Supply (Type 39) table.	Ensure the most current version of the supported BIOS is in use.
6	The number of Power Supply (Type 39) SMBIOS tables is not expected.	Ensure the most current version of the supported BIOS is in use.
7	The Unit Group values of the power supplies do not match.	Ensure the most current version of the supported BIOS is in use.
9	Power supply monitoring is not supported on this platform. Initialization failed.	Ensure platform is a ZCentral 4R workstation.
10	The SWTools Driver failed to be initialized.	Ensure service is running with administrator permissions.
11	The Power Supply Monitor was unable to be initialized.	Ensure service is running with administrator permissions.
12	The Power Supply Monitor was unable to map physical memory.	Ensure service is running with administrator permissions.
13	The Power Supply Monitor was unable to unmap physical memory.	Ensure service is running with administrator permissions.
14	The Power Supply Monitor Driver was unable to be cleaned up.	Ensure service is running with administrator permissions.
15	HP ZCentral Hardware Monitor is not supported on the current platform.	Ensure platform is a ZCentral 4R workstation.
16	Failed to enumerate installed drivers.	Ensure service is running with administrator permissions.
17	The Intel® Management Engine Interface driver is not installed. The Intel® Management Engine Software (Chipset Driver) softpaq for this platform can be downloaded from the HP Drivers website (https://www.hp.com/drivers).	Install Intel® Management Engine Software (Chipset Driver) softpaq.

Admin Console Configuration

Setting Time and Date

You can configure the time zone, time format and date format within the **Admin Console**. This enables you to ensure the time zone is set to your local time zone or else to the time zone into which your remote workstations are deployed. The current date and time format provided by the web browser is the default preference used.

The following steps outline how to set date and time preferences:

1. Click **Preferences** from the user account icon within the Admin Console.
2. Select the desired Date format, Time zone and Time format.
3. Click **SAVE**.

The new date and time preferences are applied globally where applicable across the entire Admin Console.

Activity Log

The Anyware Manager activity log enables you to view a record of all activity and operations performed in your Anyware Manager environment. You can choose whether to show all records or just the records from a selected deployment. To view the activity log from the Admin Console:

1. Click the user account icon within the Admin Console.
2. Click **Activity Log** to display the activity log for that deployment.

The logs show the date, user account, source and activity details.

You can search for logs based on specific operations that occured. You can download all the logs available in Anyware Manager by clicking the **Download CSV** button. For information on Anyware Manager levels and how they impact the activity log, see Anyware Manager.

Activity Log Expiration Timeframe

The Activity Log in the Admin Console contains short-term data, up to 7 days. After 7 days the log data expires. To maintain your long term storage Teradici recommends downloading the .csv file regularly.

Accessing the Activity Log through Anyware Manager APIs

Anyware Manager offers a RESTful API as an alternative to using the Admin Console. It allows for programmatic management and automation of resources in Anyware Manager deployments.

The following API page details how you can obtain these Activity Logs using the Anyware Manager APIs: https://cam.teradici.com/api/docs#tag/Activity-Logs

The Get activity logs and download activity logs API calls enable users to get the logs and download them as a .csv file.

Reference

Preparing a Secret Storage Application

The following section outlines the steps involved in preparing specific secret storage applications prior to installing Anyware Manager. Once you have Anyware Manager installed, you can configure the secret storage application to work with Anyware Manager.

Preparing Azure Key Vault

The following section outlines how to prepare Azure Key Vault for key and secret encryption and storage with Anyware Manager.

Before configuring Anyware Manager to use the Azure Key Vault you need to complete the following steps:

1. Create an Azure service principal that is able to read, write and delete secrets from/to the Azure Key Vault. For information on how to create this service principal, see App Objects and Service Principals.
2. Create an Azure Key Vault. For information on how to create an Azure Key Vault, see Quickstart: Create a key vault using the Azure Portal.

Once you have completed the pre-requisite steps above, return to the Installing Anyware Manager - External Database and Secret Storage Configuration and complete the installation of Anyware Manager.

Preparing Hashicorp Vault

The following section outlines how to prepare Vault for key and secret encryption and storage with Anyware Manager.

Deploying Vault with Consul and Integrated Storage (Raft)

For information on setting up a Vault server using Consul as a storage backend, see Hashicorp's official deployment guide see Vault using Consul. This guide demonstrates how to deploy a Vault in a high availability mode.

HashiCorp's recommendations for a production level deployment of Vault can be found here Production Level Deployment.

Hashicorp's official deployment guide for setting up a Vault server using Integrated Storage (Raft) as a storage backend can be found here Vault with Raft Storage.

Reference Instructions for MongoDB and Vault Configuration

For detailed deployment instructions on installing and configuring MongoDB and Vault in a single virtual machine to be used by Anyware Manager, see the following KB article. This KB article outlines in detail how to install and configure an instance of MongoDB and an instance of Vault on the same virtual machine. This KB article should be used in conjunction with the installation steps outlined in this section.

All configuration steps outlined should be used as a reference only. For specific details user's should visit the vendors official documentation and knowledge base.

The following steps outline how to prepare Vault to be used by Anyware Manager. You can skip these steps if you have setup Vault and prepared it by following the KB article linked above. If you have not gone through the KB above and have already installed and configured the Vault server, following the vendors official documentation site, follow the steps below to add specific Vault configurations required for Anyware Manager:

1. Initialize the Vault. For information on initializing the Vault, see Initializing the Vault.
2. Unseal the Vault. For information on sealing and unsealing the Vault, see Seal/Unseal.
3. Enable the secrets path expected by Anyware Manager by running the following command:

```
vault login
vault secrets enable -version=2 -path=secret/ kv
```

4. Create a Vault policy called "manager-policy":

```
vault policy write manager-policy - << EOF
path "secret/data/*" {
  capabilities = ["create", "update", "read", "delete", "list"]
}
EOF
```

The output for this command should be:

```
Success! Uploaded policy: manager-policy
```

You can validate the policy by running the following command:

```
vault policy read manager-policy
```

5. Create a role to be used by Anyware Manager by running the following command:

```
vault write auth/token/roles/manager-role allowed_policies="manager-
policy" period="768h"
```

This command creates a token role with the manager policy created above. Any token created using this role is valid for 32 days, if not renewed. If the token is renewed, then its validation period is reset back to 32 days. This period should be set in accordance with your security guidelines and should be configured to be as low as possible. The output of this command should be:

```
Success! Data written to: auth/token/roles/manager-role
```

6. Create a periodic token to be used by Anyware Manager by running the following command:

```
vault token create -role=manager-role -orphan
```

This command creates a periodic token which are useful when the token in question is intended to be used by a long-running process or application. For more information on creating Vault tokens, see Vault Tokens. The output of this command should be:

```
Key                    Value
---                    -----
token                  <your token is here>
token_accessor         <your token accessor is here>
token_duration         768h
token_renewable        true
token_policies         ["manager" "default"]
identity_policies      []
policies               ["manager" "default"]
```

Once you have completed the pre-requisite steps above, return to the Installing Anyware Manager - External Database and Secret Storage Configuration and complete the installation of Anyware Manager.

Configuring a Secret Storage Application

The following section outlines the steps involved in configuring specific secret storage applications to work with Anyware Manager. You should prepare the secret storage applications prior to installing Anyware Manager.

> ⚠ **Data Migration between Secret Stores Prohibited**
>
> Anyware Manager does not support any data migration between secret stores. If Anyware Manager is originally configured with another secret store application, for example Hashicorp Vault, and is then configured to use Azure Key Vault, Anyware Manager does not have access to the data stored in the original Vault. Anyware Manager does not be able to retrieve any stored passwords, so login requests fail. Teradici recommends using the same secret store throughout the lifetime of a Anyware Manager instance.

Configuring Azure Key Vault

Follow the steps below to configure Anyware Manager to use the Azure Key Vault as its secret storage application. Anyware Manager must be installed before the command can be run:

1. SSH to the target machine where you installed Anyware Manager.
2. Create a config file that contains the following parameters and information:

   ```
   {
   "vault-type": "azure",
   "key-vault-url": "<URL of Azure Key Vault>",
   "azure-client-id": "<client id of Azure service principal>",
   "azure-client-secret": "<client secret of Azure service principal>",
   "azure-tenant-id": "<tenant id of Azure service principal>"
   }
   ```

3. Run the following command to implement the config file:

   ```
   sudo /usr/bin/local/anyware-manager configure --config-file <config file
   name>
   ```

Configuring Hashicorp Vault

Follow the steps below to configure Anyware Manager to use Hashicorp Vault as its secret storage application. Anyware Manager must be installed before the command can be run:

1. SSH to the target machine where you installed Anyware Manager.
2. Create a file that contains the following data:

```
{
        "vault-type": "vault",
        "vault-url": "https://<vault_address>",
        "vault-token": "<vault_token>",
        "vault-secret-path": <in this example: secret/data>
}
```

3. Replace the following place holders with your own values:
   - vault_address: IP address or domain name of the Vault server.
   - vault_token: The access token generated on the Vault server that is used by Anyware Manager to access the Vault.
4. Run the following command to configure Anyware Manager to use Vault:

```
sudo /usr/local/bin/anyware-manager configure --config-file path-to-your-config-file
```

   After running this command, Anyware Manager validates the configuration by attempting to query the Vault's health status. If the request is successful, then Anyware Manager is configured to use this Vault. The configure command should only take a few minutes to complete. To verify that the connection to the Vault is healthy, run the following command:

```
sudo /usr/local/bin/anyware-manager diagnose --health

## It will show the following if Vault is healthy:
[2021-01-25T22:49:02Z]  INFO .. Connections:
[2021-01-25T22:49:02Z]  INFO .... Vault=Healthy

## It will show the following if Vault is unhealthy:
[2021-01-26T01:47:10Z]  INFO .. Connections:
[2021-01-26T01:47:10Z] ERROR .... Vault=Vault service is unreachable
[2021-01-26T01:47:10Z] ERROR .. Overall Health=Anyware Manager is in Unhealthy state because Vault is unhealthy
```

Connecting to a Vault server with Self-Signed TLS Certificates

⚠ Tested on CentOS Only

The following steps have been tested on CentOS. These steps may not work, or work differently, on different systems.

The following steps outline how to connect to a Vault server that uses self-signed TLS certificates:

1. Create a file called *vault-config.json* that contains the following:

```
{
        "vault-type": "vault",
        "vault-url": "https://<vault_address>",
        "vault-token": "<vault_token>",
        "vault-ca-cert-file": "<vault_ca_cert_file>",
        "vault-skip-verify-cert": false,
        "vault-secret-path": "secret/data"
}
```

2. Replace the following place holders with your own values:
    - vault_address (string): IP address or domain name of the Vault server.
    - vault_token (string): The access token generated on the Vault server that is used by Anyware Manager to access the Vault.
    - vault_ca_cert_file (string): The path to the file containing the CA certificate for your self-signed certificate.
3. Run the following command to update Anyware Manager to use Vault:

```
sudo /usr/local/bin/anyware-manager configure --config-file path-to-your-config-file
```

4. If you want to skip certificate verification, include `"vault-skip-verify-cert":true` in your configuration file. Please note that this is not secure and is not recommended for production use cases:

```
{
        "vault-type": "vault",
        "vault-url": "https://<vault_address>",
        "vault-token": "<vault_token>",
        "vault-ca-cert-file": "<vault_ca_cert_file>",
        "vault-skip-verify-cert": true,
        "vault-secret-path": "secret/data"
}
```

Vault Token Auto-Renewal

Anyware Manager does not renew the Vault token by default. You can manually set-up auto-renewal by configuring the `vault-config.json` file. For more information on renewing Vault tokens, see Vault Token Renewal.

Anyware Manager can automatically renew the Vault token. You need to enable the setting in the `vault-config.json` file, and set the interval you wish the token to renew at. To enable this feature, add the Vault token auto-renew settings as follows:

1. Edit the `vault-config.json` file with the following settings:

```
{
        "vault-type": "vault",
        "vault-url": "https://<vault_address>",
        "vault-token": "<vault_token>",
        "vault-secret-path": <in this example: secret/data>
        "vault-enable-token-renew": true,
        "vault-token-renew-interval": "<crontab expression: eg @hourly,
@daily, @weekly, @monthly>"
}
```

2. Set the auto-renew token setting appropriately. The `vault-token-renew-interval` is a cron tab string. It can either be in a descriptor format as outlined in the above example, or you can set it to

your own custom cron tab expression. The cron tab expression needs to be in the following format:

```
"<minute> <hour> <day-of-month> <month> <day-of-week>"
```

Vault Token Renewal Interval

To ensure that the Vault token is kept alive, the renewal needs to be able to occur multiple times before the token expires. If the token expires in a week, then you need to renew at least twice a week, if it expires every day, it needs to be renewed every few hours.

Vault Data Migration

Anyware Manager does not do any data migration between different Vault configurations. If Anyware Manager is updated to use a new Vault configuration, it is no longer be able to access the data from the previous configuration. If the admin user's password had been updated using a prior Vault configuration, you no longer be able to login. To fix this, do one of the following:

- If you have access to the old Vault, migrate the data from the old Vault to the new Vault.
- Find the key that Anyware Manager is using to look for the admin password in the Vault and then manually store the password in the Vault at that location. To find the key, stream the logs for the secretmgmt service by running the following command:

  ```
  /usr/local/bin/kubectl logs -l app=secretmgmt -f
  ```

  Log in to Anyware Manager using the adminUser account and look for the log that includes the route `/internal/secrets/admin-XXX`. The password is expected to be at `<secret path>/admin-XXX` in the Vault, where *secret path* is the path defined by "vault-secret-path" in your Anyware Manager config-file.
- Update to use a new MongoDB, or drop the `standaloneAdmins` collection in your MongoDB. **WARNING: this causes you to lose all of your Anyware Manager data.**

Backing up and Restoring Anyware Manager Data

The following sections outline the steps to backup the data stored using in-cluster data storage applications, and used by Anyware Manager. It also outlines how to restore this data from the created archive, as well as how to then migrate this data to another virtual machine.

Backing up Anyware Manager Data

The following section outlines how to back up the data stored and used by Anyware Manager, by creating an encrypted archive of the data.

> ⚠ **Backup Command for In-Cluster Storage Only**
>
> The backup command can only be run if Anyware Manager is using in-cluster data storage for both Vault and MongoDB. This command does not work if Anyware Manager is using an external Vault or MongoDB.

To backup the data run the following command in an SSH terminal:

```
sudo /usr/local/bin/anyware-manager backup
```

This creates an encrypted archive of the Vault and MongoDB data used by Anyware Manager. If successful, the backup archive file and decryption key file locations are displayed in the terminal.

The backup archive file is stored in the `/opt/teradici/casm/backups/` directory. The decryption key is stored in the `/opt/teradici/casm/.private/backup.key`. Anyware Manager only creates a new decryption key if one does not already exist. If there is an existing decryption key then it continues to use it.

Once the file and key has been created, you need to change the ownership of the file to the SSH user using the `chown` command. You can move the files to a specific directory, change the owner, and the correct permissions are assigned. The following script is an example of this command:

```
ssh user1@machine1
sudo mv /opt/teradici/casm/backups/<archive_name> ~/backup.tar
sudo chown user1:user1 ~/backup.tar
exit

ssh user2@machine2
scp user1@machine1:~/backup.tar .
```

You need to copy the decryption key and change its ownership. The following script is an example of this command:

```
ssh user1@machine1
sudo cp /opt/teradici/casm/.private/backup.key ~/
sudo chown user1:user1 ~/backup.key
exit

ssh user@machine2
scp user1@machine1:~/backup.key .
```

Restoring Anyware Manager Data

Once you have backed up the data to the encrypted archive, you need to restore this data. If the restore command fails, Anyware Manager attempts to try and restore using a backup archive that is automatically created right after the restore command has been run. If this is successful, Anyware Manager has the same data as before the restore was attempted. To skip the rollback feature, add `--skip-rollback` to the arguments of the restore function.

⚠ **Restore Command for In-Cluster Storage Only**

The restore command can only be run if Anyware Manager is using in-cluster data storage for both Vault and MongoDB. This command does not work if Anyware Manager is using an external Vault or MongoDB.

To restore the data run the following command in an SSH terminal:

```
sudo /usr/local/bin/cas-manager restore --archive <path to archive file>  --
key <path to key file>
```

If you do not specify a key, Anyware Manager attempts to restore using the key found at `/opt/teradici/casm/.private/backup.key`.

Moving Anyware Manager Data

It is possible to backup data on one Anyware Manager virtual machine, and then restore the resulting archive on a separate Anyware Manager virtual machine. Once you have backed up the data successfully on the first Anyware Manager virtual machine, you can move the encrypted archive to another virtual machine.

You must ensure you have a machine that has SSH access to the virtual machines that host each of the Anyware Manager instances. You must first copy the encrypted archive and decryption key to this machine, then you can move the data from this intermediary machine to the new Anyware Manager virtual machine.

The following steps outline how to move Anyware Manager data:

1. Run the following command to copy the encrypted archive to a machine that has SSH access to the Anyware Manager instance:

   ```
   scp <username>@<manager1_URL>:/opt/teradici/casm/backups/<archive_name>
   <path on machine that contains manager backups>
   ```

2. Run the following command to copy the decryption key to the same machine that has SSH access to the Anyware Manager instance:

   ```
   scp <username>@<manager1_URL>:/opt/teradici/casm/.private/backup.key <path
   on machine that contains manager backup keys>
   ```

3. Run the following command to move the encrypted archive file from the machine to the host of the new Anyware Manager virtual machine:

   ```
   scp <path on machine that contains manager backups>/<archive_name>
   <username>@<manager2_URL>:<path on manager2 host that contains backups>
   ```

4. Run the following command to move the decryption key file from the machine to the host of the new Anyware Manager virtual machine:

   ```
   scp <path on machine that contains manager backup keys>/backup.key
   <username>@<manager2_URL>:<path on manager2 host that contains backup keys>
   ```

Migrating from a Default to External Configuration

The following section outlines the steps involved in migrating the data stored in the internal data storage applications as part of a default configuration of Anyware Manager, to MongoDB and Vault instances in the external configuration mode.

Prerequisites for Migrating Anyware Manager Data

> ⚠ **Migration Commands are for Internal Storage Only**
>
> The migration commands can only be run if Anyware Manager is using internal data storage for Vault or MongoDB as part of the default configuration. The Vault migration commands does not work if Anyware Manager is already using an external Vault. The MongoDB commands does not work if Anyware Manager is already using an external MongoDB.

1. Create the configuration files for the target MongoDB and Vault you are migrating Anyware Manager data to. To create blank configuration files run the following command in an SSH terminal:

   ```
   /usr/local/bin/anyware-manager generate --vault --mongo
   ```

   This creates `mongo-template.json` and `vault-template.json` files which that are created in the `config-templates/` directory within the current directory. The commands output contains the full path to the files for reference.

2. Input the required parameters for the configuration file by following the instructions here.
3. In order for our migration scripts to be able to read from these files, please install the `jq` utility by running the following command in an SSH terminal:

   ```
   sudo dnf install -y jq
   ```

Migrating Internal MongoDB Data

The following steps outline how to migrate the internal MongoDB data to the external MongoDB instance as part of an external configuration of Anyware Manager.

⚠ **Migration Commands are for Internal Storage Only**

The migration commands can only be run if Anyware Manager is using internal data storage for MongoDB. This command does not work if Anyware Manager is using an external MongoDB instance.

Once you have configured the `config-templates/mongo-template.json`, you can run the following commands to migrate the data from the internal storage to the external MongoDB instance.

1. Run the following command in an SSH terminal to set the configuration for where to migrate the data to:

    ```
    # Set path to Mongo Configuration file
    export PATH_TO_MONGO_CONFIG='config-templates/mongo-template.json'
    ```

2. Run the migration script. Ensure that the `DEST_MONGO_DB` is set correctly. It should match the database specified by the MongoDB connection string in the configuration file.

```
# Run Commands to migrate MongoDB data from internal MongoDB to external
MongoDB
/usr/local/bin/kubectl exec -it deployments/mongo -- bash -c "
#!/bin/sh
set -e

# If destination DB is different from default (managerdb), set it
accordingly.
export DEST_MONGO_DB='managerdb';

# Get connection string from mongo configuration file.
export DEST_MONGO_CONNECTION_STRING=$(jq '."db-connection-string"' $
{PATH_TO_MONGO_CONFIG});

# Check if TLS is enabled for external MongoDB
if [[ $(jq '."db-enable-tls"' ${PATH_TO_MONGO_CONFIG}) == 'true' ]]; then
    export MONGO_TLS='--ssl --tlsInsecure'
fi

# Get internal MongoDB's credentials
export MONGO_ADMIN=$(/usr/local/bin/kubectl get secrets/mongo-secret --
template={{.data.username}} | base64 -d);
export MONGO_DB=$(/usr/local/bin/kubectl get secrets/mongo-secret --
template={{.data.dbname}} | base64 -d);
export MONGO_PWD=$(/usr/local/bin/kubectl get secrets/mongo-secret --
template={{.data.password}} | base64 -d);

$(cat << 'EOF'
# Check if TLS is enabled for internal MongoDB. This file is volume mounted
in K8S manifest when TLS is required for mongo.
if [[ -f /certs/tls_combined.crt ]]; then
    export INTERNAL_MONGO_TLS='--ssl --tlsInsecure'
fi
rm -rf /export/
mkdir -p /export/

# Dump data from internal MongoDB
mongodump ${INTERNAL_MONGO_TLS} -u $MONGO_ADMIN -p $MONGO_PWD --db
$MONGO_DB --gzip --archive=/export/mongo.archive
# Restore dumped data to external MongoDB instance
mongorestore ${MONGO_TLS} --uri="${DEST_MONGO_CONNECTION_STRING}" --drop --
gzip --nsInclude=$MONGO_DB.* --nsFrom=$MONGO_DB.* --nsTo=$DEST_MONGO_DB.*
--archive=/export/mongo.archive

# Clean up
rm -rf /export/
EOF
)"
```

Once this command is complete, the last line logged by `mongorestore` displays a message similar to the following:

```
6 document(s) restored successfully. 0 document(s) failed to restore.
```

3. Run the following command to apply the external MongoDB configuration to complete the migration:

```
# Point Anyware Manager instance to External MongoDB
/usr/local/bin/anyware-manager configure --config-file $
{PATH_TO_MONGO_CONFIG}
```

After running this command, there may be some momentary down time as the database is switched over. Once the command is complete, Anyware Manager should be functional. If for whatever reason you need to re-run the migration commands, you need to run the following command to start the internal MongoDB:

```
/usr/local/bin/kubectl scale deployments/mongo --replicas=1
```

Common issue are that the `DEST_MONGO_DB` environment variable set in the script and the database specified by the external MongoDB connection string in the configuration file do not match, or there are permissions issues with the credentials in the connection string. Applying the MongoDB configuration again disables the internal MongoDB.

Migrating Internal Vault Data

The following steps outline how to migrate the internal Vault data to the external Vault instance as part of an external configuration of Anyware Manager.

> ⚠ **Migration Command is for Internal Storage Only**
>
> The migration commands can only be run if Anyware Manager is using internal data storage for Vault. This command does not work if Anyware Manager is using an external Vault instance.

Once you have configured the `config-templates/vault-template.json`, you can run the following commands to migrate the data from the internal storage to the to the external Vault instance.

1. Run the following command in an SSH terminal to set the configuration for where to migrate the data to:

   ```
   # Set path to Vault Configuration file
   export PATH_TO_VAULT_CONFIG='config-templates/vault-template.json'
   ```

2. Create a backup of the internal Vault's token:

   ```
   # Create backup of internal vault's token in case something fails
   /usr/local/bin/kubectl create secret generic clustervaulttoken --from-literal=token="$(/usr/local/bin/kubectl get secret vault-secret --template={{.data.roottoken}} | base64 -d)" --from-literal=address="$(/usr/local/bin/kubectl get secrets app --template={{.data.VAULT_ADDRESS}} | base64 -d)"
   ```

3. Run the migration script:

```
# Run Commands to migrate Vault data from internal Vault to external Vault
/usr/local/bin/kubectl exec -it deployments/vault -- sh -c "
#!/bin/sh
set -e

# Get target Vault settings from configuration file.
export DEST_VAULT=$(jq '."vault-url"' ${PATH_TO_VAULT_CONFIG});
export DEST_VAULT_TOKEN=$(jq '."vault-token"' ${PATH_TO_VAULT_CONFIG});
export DEST_SECRET_PATH=$(jq '."vault-secret-path"' $
{PATH_TO_VAULT_CONFIG});

# Set existing vault settings
export VAULT_ADDR=$(/usr/local/bin/kubectl get secret clustervaulttoken --
template={{.data.address}} | base64 -d);
export VAULT_TOKEN=$(/usr/local/bin/kubectl get secret clustervaulttoken --
template={{.data.token}} | base64 -d);
export VAULT_SECRET_PATH='secret/';
export VAULT_SKIP_VERIFY='true';

# Dump secrets in json format
$(cat << 'EOF'
rm -rf /export/
mkdir -p /export/
for key in $( vault kv list ${VAULT_SECRET_PATH} | tail +3  )
do
    dest=/export/$key.json
    # Don't copy sub-folders
    if [[ $(echo $key | grep -E '/\s*$') ]]
    then
        continue;
    fi
    mkdir -p /export/${key%/*}
    echo \"get ${VAULT_SECRET_PATH}$key\"
    vault kv get -format=json -field=data  ${VAULT_SECRET_PATH}$key >
$dest;
done

# Copy secrets to destination vault
export VAULT_ADDR=${DEST_VAULT}
export VAULT_TOKEN=${DEST_VAULT_TOKEN}
export DEST_SECRET_PATH=$(echo ${DEST_SECRET_PATH} | sed -e 's|\(.*\)data|
\1|g')
for secret_file in $( ls /export/*.json   ); do
    key_file_name=$(basename -- \"$secret_file\")
    key_name=${key_file_name%%.*}
    echo \"put ${DEST_SECRET_PATH}$key_name\"
    vault kv put ${DEST_SECRET_PATH}$key_name @$secret_file;
done
# Clean up
rm -rf /export/
EOF
)"
```

On successful completion, the output displays a message similar to the following:

```
"get secret/60f9f0455234e00881fd00a2"
"get secret/admin-60f9f0365234e066b4fd00a1"
"get secret/secret-management-service-health"
"put secret/60f9f0455234e00881fd00a2"
Key                Value
---                -----
created_time       2021-07-22T22:27:59.961440121Z
deletion_time      n/a
destroyed          false
version            1
"put secret/admin-60f9f0365234e066b4fd00a1"
Key                Value
---                -----
created_time       2021-07-22T22:28:00.088969023Z
deletion_time      n/a
destroyed          false
version            1
"put secret/secret-management-service-health"
Key                Value
---                -----
created_time       2021-07-22T22:28:00.207620136Z
deletion_time      n/a
destroyed          false
version            1
```

4. Run the following command to apply the external Vault configuration to complete the migration:

```
# Point Anyware Manager instance to External Vault
/usr/local/bin/anyware-manager configure --config-file $
{PATH_TO_VAULT_CONFIG}
```

After running this command, there may be some momentary down time as the vault is switched over. Once the command is complete, Anyware Manager should be functional. If for whatever reason you need to re-run the migration commands, run the following command to start the internal Vault:

```
/usr/local/bin/kubectl scale deployments/vault --replicas=1
/usr/local/bin/kubectl patch cronjobs vaultunseal -p '{"spec" :
{"suspend" : false }}'
sleep 60
```

A common issue is that the destination secret path is incorrect or the Vault has been sealed. If there is a problem please check the configuration and try again.

5. If everything is okay, delete the backup of the internal Vault's token by running the following command:

```
/usr/local/bin/kubectl delete secret clustervaulttoken
```

Once this is deleted you are no longer able to access data from the internal Vault.

Proxy Configuration for Anyware Manager

Enable Proxy Configurating for Installation

If HTTP/HTTPS proxy is used, then `HTTP_PROXY`, `HTTPS_PROXY` and `NO_PROXY` must be set. For `NO_PROXY`, specific IP addresses or domain names of service that are internal must be added. IP address ranges like "10.0.0.0/8" does not work; exact IP addresses or domain names must be used for `NO_PROXY` for the traffic to be routed through the proxy to work properly. The outlined variables need to be set in the `/etc/environment` file.

The following steps outline how to modify this file to add these variables:

1. Run the following command to edit the `/etc/environment/` file in vi. You could also use vim or nano:

   ```
   sudo vi /etc/environment
   ```

2. Update the file to include the following environment variables.

   ```
   HTTPS_PROXY="http://hostname_of_proxy:port"
   HTTP_PROXY="http://hostname_of_proxy:port"
   NO_PROXY=[list of all host names that should not go through the proxy,
   such as: localhost, 127.0.0.1, 0.0.0.0, ip_address_of_mongo]
   ALL_PROXY="http://hostname_of_proxy:port"
   https_proxy="http://hostname_of_proxy:port"
   http_proxy="http://hostname_of_proxy:port"
   no_proxy=”=[list of all host names that should not go through the proxy,
   such as: localhost, 127.0.0.1, 0.0.0.0, ip_address_of_mongo]
   all_proxy="http://hostname_of_proxy:port"
   ```

3. Save the file. Once you install Anyware Manager you can configure it to use the proxy configuration. From this new terminal, proceed with the installation steps. The proxy configuration is implemented when Anyware Manager is installed.

Disable Proxy Configuration

Once all installations and configurations are done, If Anyware Manager run into issues related to proxy, you can disable proxy on the Anyware Manager server to confirm if that's the cause. To disable proxy:

1. Check the proxy settings saved in the cluster:

   ```
   sudo /usr/local/bin/kubectl edit secret proxysettings -o yaml
   ```

2. Look for strings such as `HTTP_PROXY`, `HTTPS_PROXY`, `NO_PROXY`.
3. Press the letter "i" to edit the keys to set them to empty string by doing the following:

   ```
   HTTP_PROXY: ""
   HTTPS_PROXY: ""
   NO_PROXY: ""
   ```

   if you do not see one of those strings change the rest to empty string "".

4. Save the new configuration by pressing "ESC" then ":" then "wq".

Troubleshooting

Anyware Manager Support Bundle

If you encounter an issue installing the Anyware Manager or with the application itself, it is possible to generate a support bundle that can be sent to the HP support team to investigate and resolve.

To generate the support bundle, run the following command:

```
sudo /usr/local/bin/anyware-manager diagnose --support-bundle
```

If this command is successful, a `.tar.gz` file is located under the */tmp* folder with a name formatted as follows:

/tmp/anyware-manager-support-bundle-yyyymmddThhmmssZ.tar.gz

yyyymmddThhmmssZ represents the date and time the support bundle was created.

Support Bundle Information and Logs

The support bundle collects the various information from the system and then zip the files into a `.tar.gz` file in the */tmp* directory.

Once you unzip the file the structure is as follows:

- **files/etc** folder contains files with OS level information:
  - **issue** file contains a copy of all contents from the */etc/issue* file.
  - **os-release** file contains all operating system identification data that was found in the */usr/lib/os-release* file.
  - **/systemd/system/k3s.service** folder contains the information about `k3s.service` configuration.
- **files/var/log/anyware-manager** folder collects all of the Anyware Manager log files, for example generate, configure, diagnose, install logs.

The **out** folder collects outputs from running various commands to expose the details of relevant system information and Anyware Manager backend services, as outlined below:

- **os** folder contains the following files:
    - **dmesg.out** file contains the output of command `dmesg`.
    - **ls_-l@var@crash.out** file contains the output of the command `ls -l /var/crash`.
    - **pgrep_-l_k3s.out** file contains the output of the command `pgrep -l k3s`.
    - **ps_wwauxfx.out** file contains the output of the command `ps wwauxfZ`.
    - **ss-aux.out** file contains the output of the command `ss -ax`.
    - **who.out** file contains the output of the command `who`.
    - **dnf_list_--installed_--disablerepo=*.out** file contains the packages that are currently installed on the system and their versions.
- The **firewall** folder contains the outputs of the command `firewall-cmd --list-services`.
- The **network** folder displays the following network files:
    - **netstat_-Wnap.out** file contains the output of the command `netstat -Wnap`.
    - **ip_add.out** file contains the output of the command `ip add`.
    - **selinux** folder contains the following files:
        - **semodule_-l.out** file contains the output of the command `semodule -l`.
        - **sestatus.out** file contains the output of the command `sestatus`.
- The **deployments** folder contains the following files:
    - **kubectl_get_deployment.out** file is the output of the command `kubectl get deployments` that lists the status of all deployments for Anyware Manager services.
    - The description of the deployment for each of the deployments through the output of the command `kubectl describe`.
    - The deployments information is retrieved from the following namespaces: `kube-system`, `kube-public`, `kube-node-lease`, `connector`, `logging`, and `ingress-nginx`.
- The **pods** folder contains the following files:
    - **kubectl_get_pods.out** file is the output of the command `get pods` that lists the status of all pods for Anyware Manager services.
    - The description of a pod for each of the pods through the output of the command `kubectl describe pod`

    - The pod information is retrieved from the following namespaces: `kube-system`, `kube-public`, `kube-node-lease`, `connector`, `logging`, and `ingress-nginx`.

- **logs** folder contains the following files:
    - The log files for each pod.
    - The logs files are retrieved from the following namespaces: `kube-system`, `kube-public`, `kube-node-lease`, `connector`, `logging`, and `ingress-nginx`.
- The **services** folder contains the following files:
    - **kubectl_get_services.out** file is the output of the command `get services` that lists the status of all services for Anyware Manager services.
    - The description of a service for each of the services through the output of the command `kubectl describe services`
    - The services information is retrieved from the following namespaces: `kube-system`, `kube-public`, `kube-node-lease`, `connector`, `logging`, and `ingress-nginx`.
- **secrets** folder displays the output of the command `kubectl get secrets` and displays the following files:
    - **kubectl_get_secrets.out** file is the output of the command `get secrets` that lists the status of all services for Anyware Manager services.
    - The description of a secrets through the output of the command `kubectl describe secrets`.
    - The secrets information is retrieved from the following namespaces: `kube-system`, `kube-public`, `kube-node-lease`, `connector`, `logging`, and `ingress-nginx`.

Anyware Manager Health Status

In the case that there is an issue with Anyware Manager, the diagnose health command provides an overview of Anyware Manager's health. The following command provides a list of services that are in healthy and unhealthy state. The command allows the user to determine the services that are unhealthy and run more specific diagnosis on the unhealthy service:

```
sudo /usr/local/bin/anyware-manager diagnose --health
```

Anyware Manager Proxy Configuration

When using a proxy, the diagnose health command could time out when trying to reach the vault. Add the vault IP address seen in the error to the no_proxy and NO_PROXY environment configuration.

The diagnose command lists all Anyware Manager services, but not all services are essential. The essential services for Anyware Manager are listed below. If any of these services are in an unhealthy state, the overall health status is unhealthy:

- "activitylog"
- "activitylogconsumer"
- "authorization"
- "camadminconsolega"
- "connectors"
- "connectorsworker"
- "deploymentmgmt"
- "deploymentworker"
- "docs"
- "kafka"
- "machinemgmt"
- "machinemgmtdeleteworker"

- "machinemgmtworker"
- "machinemonitor"
- "machinemonitorworker"
- "poolmgmt"
- "poolmgmtworker"
- "secretmgmt"
- "redis"
- "resourcetemplates"
- "resourcetemplatestore"
- "userentitlement"
- "userentitlementworker"

Vault Issues

If you suddenly start getting errors when using Anyware Manager features, it is possible the Vault token used in your Anyware Manager deployment has expired. To diagnose, try the following options:

1. Run the following command to follow the logs for the secret management service:

   ```
   kubectl logs -l app=secretmgmt -f
   ```

2. While streaming the secretmgmt logs, try logging in to Anyware Manager. If you see the following message in the logs, your Vault token may have expired:

   ```
   {"message":"Permission denied","level":"error"}
   ```

3. To confirm that the Vault token has expired, run the following command in the location you have the Vault CLI installed:

   ```
   vault token lookup <your Anyware Manager Vault token>
   ```

4. If you get the following message after running this command, then your Anyware Manager token has expired or become invalid:

   ```
   Error looking up token: Error making API request.

   URL: POST https://<your Vault address>/v1/auth/token/lookup
   Code: 403. Errors:

   * bad token
   ```

To fix this issue, create a renewable token and update your Anyware Manager's Vault configuration to use that token. To avoid the Vault token from prematurely expiring again, follow the steps outlined here to set up automatic renewal for your Vault token.

Repository Management

Repository must be added correctly in order to install Anyware Manager or Anyware Connector from online. See **Add Anyware Manager Repository** section in the Installing Anyware Manager - Default Configuration topic to manage Anyware Manager repositories and see Adding the Connector Repository to manage Anyware Connector repositories.

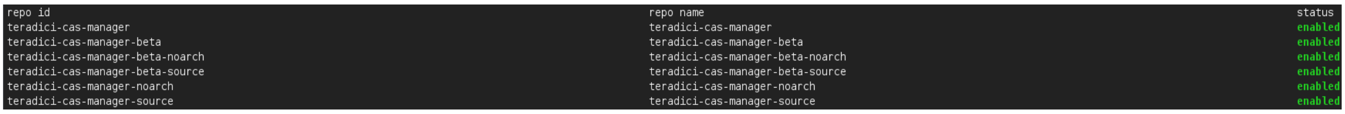
Cases that repository is not setup properly and is causing installation fails:

- Case 1: Multiple `cas-manager*` or `anyware-manager` repositories are added:

  If the server has multiple repositories beta or GA repos for `cas-manager` or `anyware-manager`, there could be a conflict of repositories. This can cause the installation to fail. To check the existing repository status, run the following command:

  ```
  dnf repolist teradici-*-manager*
  ```

  For Example: If you have beta or GA `cas-manager` repositories installed, the installer will display:

  ```
  repo id                                                        repo name                                                        status
  teradici-cas-manager                                           teradici-cas-manager                                             enabled
  teradici-cas-manager-beta                                      teradici-cas-manager-beta                                        enabled
  teradici-cas-manager-beta-noarch                               teradici-cas-manager-beta-noarch                                 enabled
  teradici-cas-manager-beta-source                               teradici-cas-manager-beta-source                                 enabled
  teradici-cas-manager-noarch                                    teradici-cas-manager-noarch                                      enabled
  teradici-cas-manager-source                                    teradici-cas-manager-source                                      enabled
  ```

  To solve the issue, make sure you only keep one of the repos that you want to install from. Run the following commands to remove unwanted repositories:

  Run the following commands to remove unwanted repositories:

  - To remove the stable `cas-manager` repo, run `sudo rm -rf /etc/yum.repos.d/teradici-cas-manager` command.
  - To remove the beta `cas-manager` repo, run `sudo rm -rf /etc/yum.repos.d/teradici-cas-manager-beta.repo` command.
  - To remove all the existing repos, run `sudo rm -rf /etc/yum.repos.d/teradici*` command.

- Case 2: An incorrect or no repository is added. If the repository list command above returns no repo or wrong repo name, you must run the add repo command to add correct repo before install.

Logging

Adding a Sumo Logic Log Collector

The following section details how to add a Sumo Logic log collector to Anyware Manager. For information on Sumo Logic, see here. In order to add the log collector you must have a Anyware Managers instance, and a Sumo Logic account that has the permissions levels required to create log collectors.

1. SSH to the Anyware Manager host and create the Sumo Logic configuration file:

   ```
   cd ~
   vim sources.json
   ```

2. Paste in the following information:

```
{
"api.version": "v1",
"sources": [
    {
        "name":  "test", # <<< Replace this with your own or leave it as is
        "category":  "manager/test", # <<< Replace this with your own
category or leave it as is
        "automaticDateParsing":  true,
        "multilineProcessingEnabled":  false,
        "useAutolineMatching":  false,
        "forceTimeZone":  false,
        "timeZone":  "Etc/UTC",
        "filters":  [
                    ],
        "cutoffTimestamp":  0,
        "encoding":  "UTF-8",
        "pathExpression":  "/var/log/containers/*.log", # <<< this tells
sumologic which file paterns to ingest. We only care about the logs. Leave
this as is.
        "blacklist":  [
                      ],
        "sourceType":  "LocalFile",
        "alive":  false
    }
]
}
```

3. Download the Sumo Logic Collector:

```
curl "https://collectors.sumologic.com/rest/download/linux/64" -o
SumoCollector.sh
sudo chmod +x SumoCollector.sh
```

4. Install the Sumo Logic Collector. For more information on installing the Sumo Collector, see here.

Once you have access to the Anyware Manager host, you need to perform one of the following:

- **Installation using an installation token**

Installation tokens can be created by going to **Administration>Security>Installation Tokens** in the Sumo Logic web app and adding a token. Once you have completed this, run the following command:

```
sudo ./SumoCollector.sh -q -Vsumo.token_and_url=<Your-Installation-Token> -
VsyncSources=/path/to/sources.json
```

- **Installation using an access key**

Access keys can be created by going to the **Preferences** page in the Sumo Logic web app and adding an Access key. You will then be able to copy the accessID and accessKey. Once you have completed this, run the following command:

```
sudo ./SumoCollector.sh -q -Vsumo.accessid=<accessid> -
Vsumo.accesskey=<accesskey> -VsyncSources=/path/to/sources.json
```

Once you have the Sumo Logic collector installed, you can log into Sumo Logic and access the logs for this collector.

Getting Support

If you are having trouble, help is available. This section contains information about contacting HP support and connecting with the HP user community.

Contacting Support

If you encounter problems installing or using HP technology, you can:

- Browse the HP Knowledge Base.
- Submit a Support Ticket.

The HP Community Forum

The PCoIP Community Forum allows users to have conversations with other IT professionals to learn how they resolved issues, find answers to common questions, have peer group discussions on various topics, and access the HP PCoIP Technical Support Service team. Our staff is heavily involved in the forums.

To join the HP community, visit the HP Knowledge Center.

Release Notes

To view the latest release notes for Anyware Manager, see Anyware Manager Release Notes.