

# Anyware Manager as a Service Administrators Guide

**None**

# Table of contents

Overview	6
What is Anyware Manager as a Service?	6
Who Should Read This Guide?	11
Key Concepts	12
System Requirements	14
Supported Domain Controller Servers	14
Authentication Service	14
Anyware Software	14
Required External Connections	16
Admin Console	19
Overview	19
Connecting to the Admin Console	20
Connecting to Anyware Manager	20
Connecting to Anyware Manager as a Service	20
Admin Console Dashboard	22
Configuring the Admin Console	22
Managing Deployments	24
Provider Service Accounts	25
Editing an Existing Deployment	28
Editing a Anyware Connector	30
Workstation Pools	32
Use Cases for Floating Workstation Assignment Policy	32
Creating a Workstation Pool	33
Adding Remote Workstations to a Workstation Pool	34
Adding Users to a Workstation Pool	35
Features and Known Limitations	35

Auto Log-Off Service	36
SAML Configuration with Anyware Manager	39
What is SAML?	39
Anyware Manager Initiated SAML Authentication Flow	40
Configure Anyware Manager as a SAML Service Provider to Enable Multi-Admin	41
Service Account and API Access	44
Remote Workstations	47
Adding a Remote Workstation	47
Editing a Remote Workstation	49
Viewing Remote Workstation Users	51
Updating Cloud Provider Information	52
Federated Authentication	53
OAuth	53
Single Sign-on (SSO)	67
Federated Authentication Troubleshooting	97
Admin Console Configuration	116
Setting Time and Date	116
Activity Log	117
Beta Features	118
Overview	118
Azure Remote Workstation Provisioning	119
Anyware Manager Configures Connector	123
Anyware Connector New Installation Wizard	127
Anyware Monitor	131
Anyware Connector	155
Overview	155
Connector on Ubuntu	156
Prerequisites	156
Installing Connector on Ubuntu	163

Upgrading the Connector on Ubuntu	174
Reference	183
Connector on RHEL	184
Prerequisites	184
Installing the Connector on RHEL/Rocky Linux	194
Upgrading the Connector on RHEL/Rocky Linux	215
Reference	216
Reference	226
Scaling and PCoIP Session Limits	226
Firewall and Load Balancing Considerations	227
Configuring the Active Directory for Anyware Connector	230
Floating Workstation Assignments	232
Security	235
Multi-Factor Authentication (MFA)	235
Multi-Factor Authentication with Duo	235
Multi-Factor Authentication with Azure	236
Anyware Manager as a Service Security and Privacy	238
Reference	239
Microsoft Azure Active Directory Authentication	239
Anyware Connector Multi-Factor Authentication	240
Duo Authentication	240
Azure MFA Authentication	241
Specifying Domain Controllers	244
Installing and Configuring Anyware Manager as a Service Idle Shutdown	245
Installing on Windows	246
Configuring on Windows	248
Installing on Linux	250
Configuring on Linux	250
Anyware Manager as a Service Deployment Scripts	253



Licensing Options with Anyware Manager as a Service	254
Anyware Manager as a Service Maintenance	258
OS Updates	258
Connector Updates	258
Disk Space Updates	258
Anyware Manager as a Service Provider Service Accounts	259
Provider Service Account Requirements	259
Providing Service Account Credentials	265
Anyware Manager as a Service Active Directory	266
Assigning Permissions to Active Directory Service Accounts	266
Verifying Active Directory Account Lockout	268
Anyware Manager as a Service Accounts	269
Anyware Manager as a Service Account Ownership	269
Troubleshooting	272
Anyware Manager as a Service Status	272
Retrieving Anyware Connector Version Numbers	273
Connector Installer Version	273
Connector Version	274
Anyware Connector Installer Issues	276
Anyware Connector Connectivity Issues	279
Remote Workstation Connectivity Check	280
Active Directory Connectivity Check	280
Anyware Connector Log Collection	282
Support	284
Getting Support	284
Contacting Support	284
The HP Community Forum	284
Getting Your Registration Code	285

# Overview

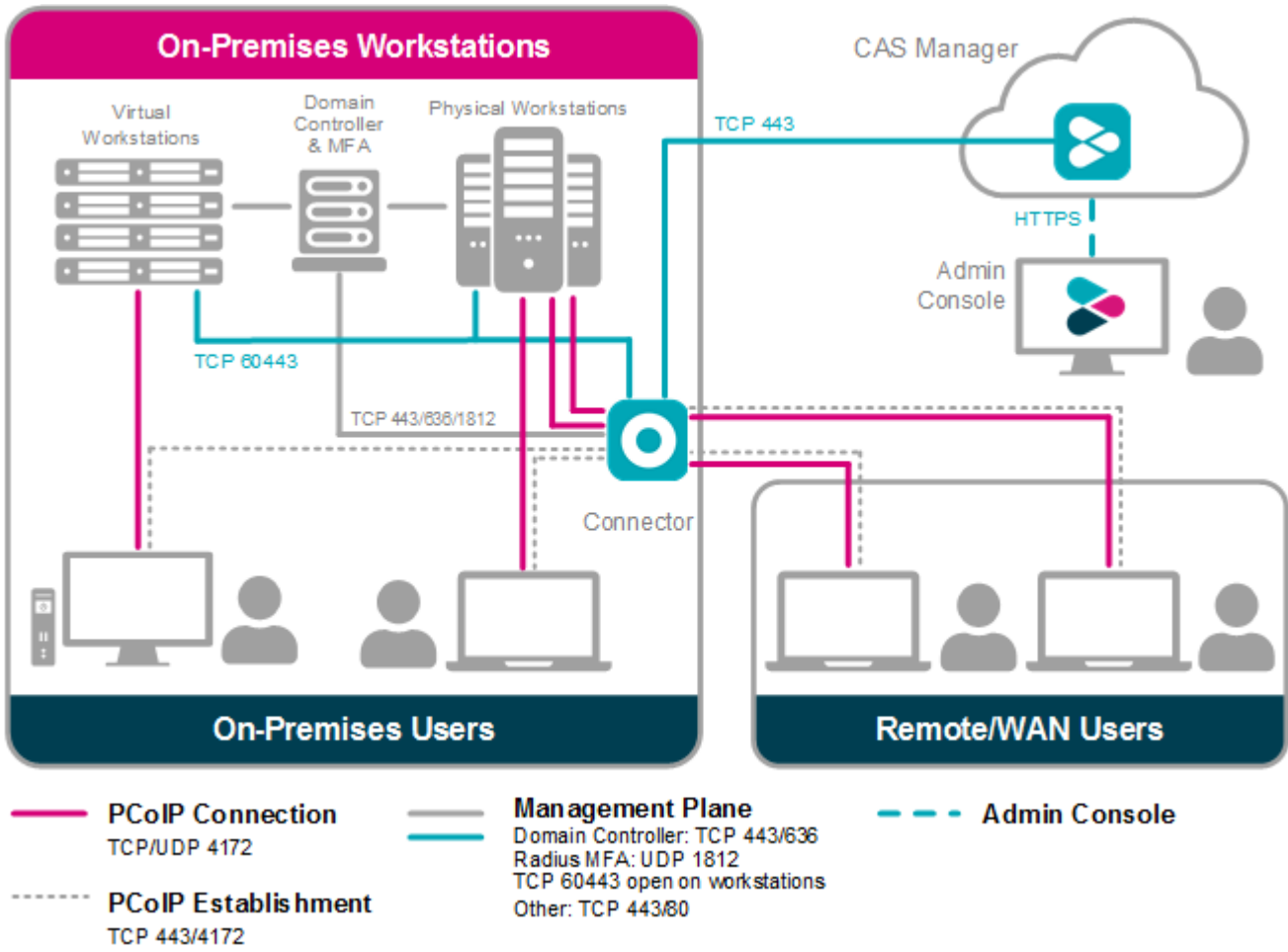
## What is Anyware Manager as a Service?

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 Windows or Linux workstations.

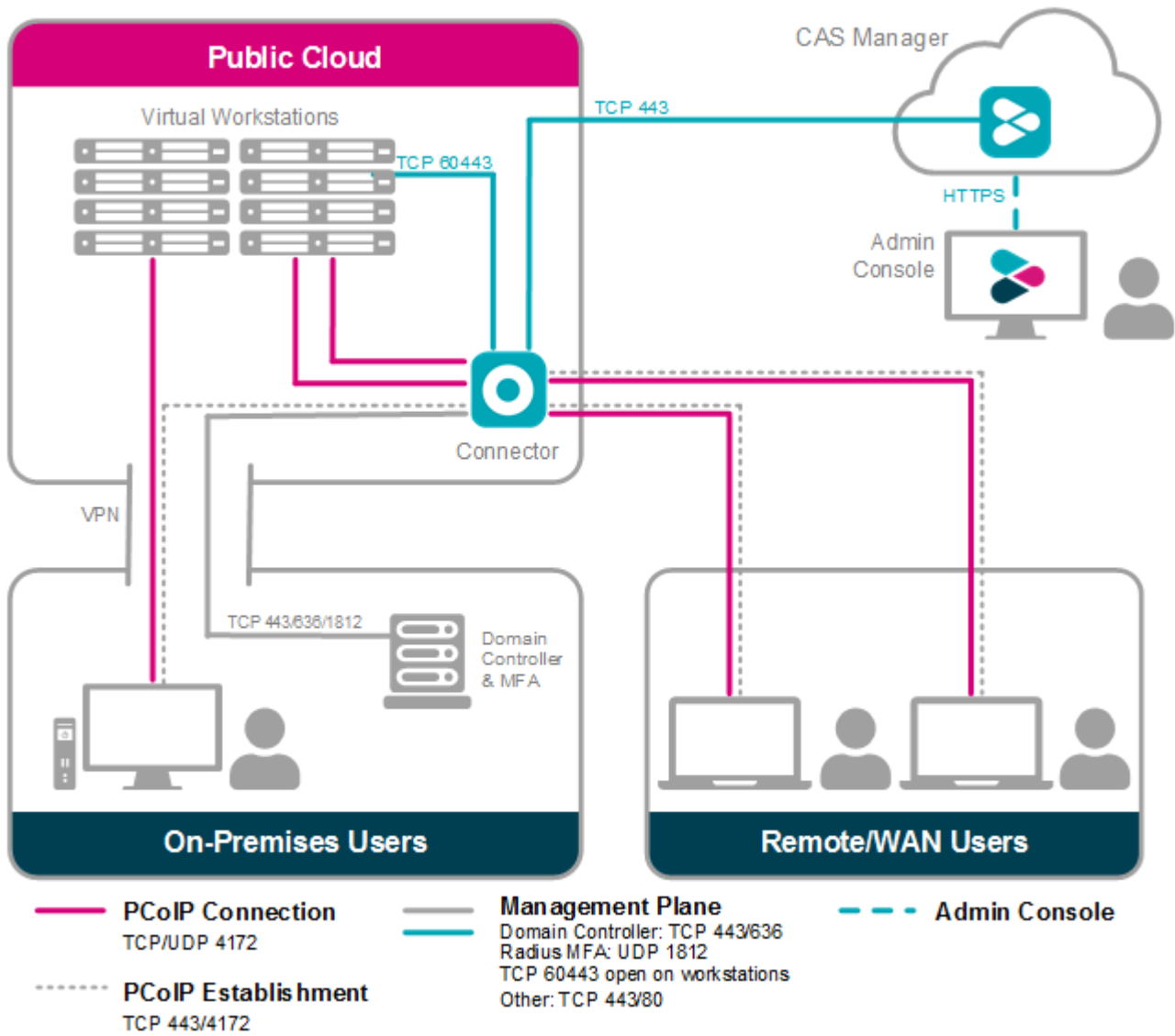
Anyware Manager as a Service is a service that is managed by HP that enables Anyware users to securely access the cloud-based version of Anyware Manager. Anyware Manager as a Service also requires an external component called Anyware Connector that resides in the users environment. Connector is a access hub that facilitates PCoIP connections to remote desktops and workstations by providing user authentication, entitlement and security gateway services. In all deployment environments, Anyware Manager as a Service interacts seamlessly with Connectors to access and manage your remote desktops and workstations.

Once Anyware Manager as a Service has been enabled, all configurations and deployment management will be carried out in the Admin Console.

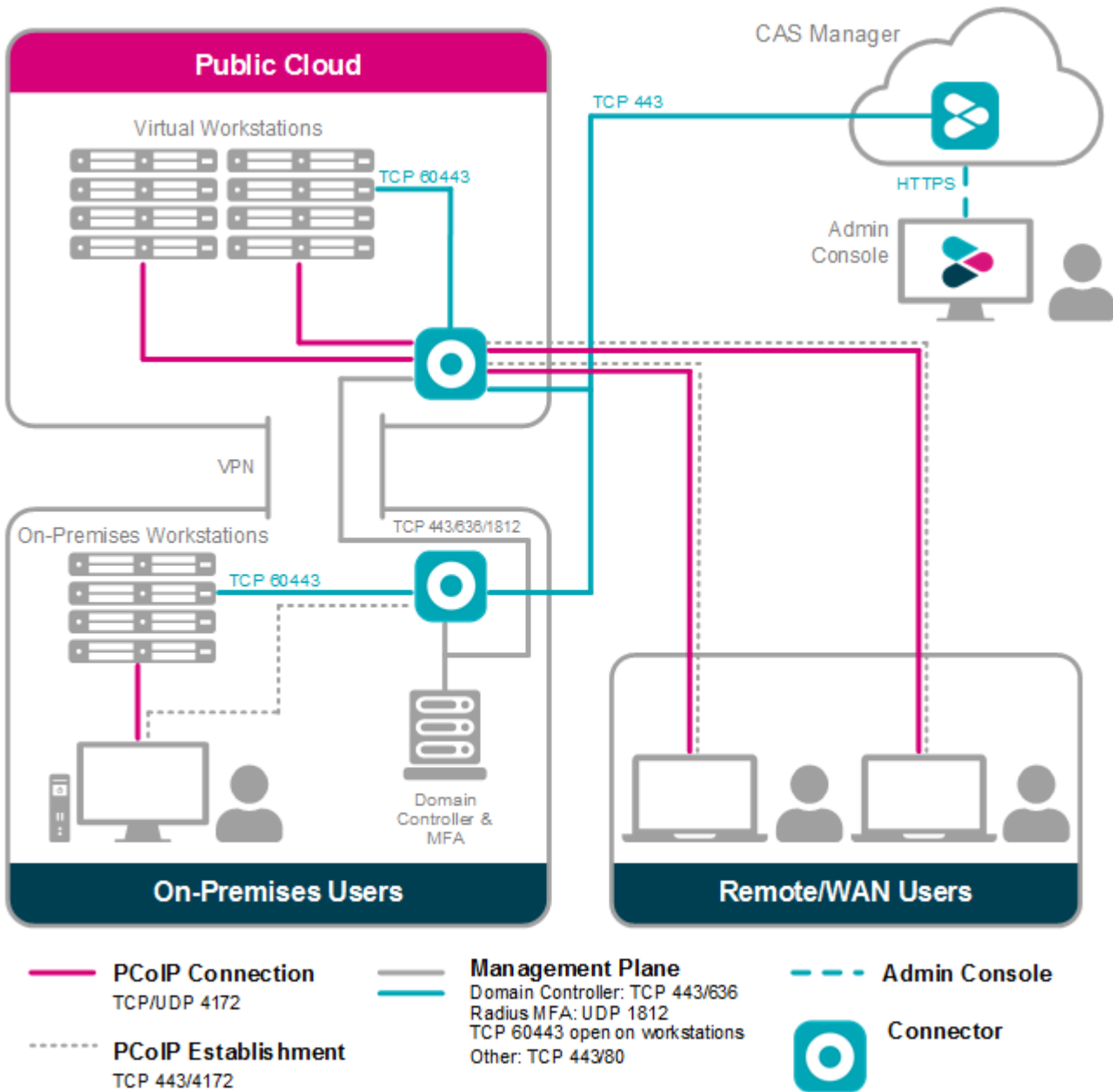
The following image outlines the Anyware Manager as a Service architecture for an on-premises scenario:



The following image outlines the Anyware Manager as a Service architecture for a public cloud scenario:



The following image outlines the Anyware Manager as a Service architecture for a multicloud scenario:



You must download, authenticate and then install the Connector. For more information on installing the Connector, see [Installing a Connector](#).

### **Anyware Manager as a Service and Connector Ports**

For a more detailed breakdown of the ports and connection descriptions, see [Firewall and Load Balancing Considerations](#).

 **Customer Costs**

Customers are responsible for the cloud computing costs associated with the Connector and the remote workstations that they create and run.

# Who Should Read This Guide?

This guide provides information for system administrators and IT professionals on using HP Anyware Manager as a Service. This guide provides instructions on how to enable and activate Anyware Manager as a Service's feature set.

## **HP Glossary**

For a glossary of terms and conditions associated with HP technology, see [HP Glossary](#).

# Key Concepts

The following concepts are terms used in the documentation and can be referred to when using Anyware Manager as a Service.

**Organization** – A user or group in possession of a valid HP Anyware license.

**Organization Administrators** – People who can manage HP Anyware deployments, Connectors, remote workstations within Anyware Manager.

**Deployment** – A way to organize the provisioning and power management of remote workstations as well as entitling users, from the Active Directory (AD), to these remote workstations. Each deployment may only have a single AD configuration. For more information on AD configuration with Anyware Manager as a Service, see [here](#).

- Use case: an IT admin would like to setup a production and a staging (or sandbox) environment. Two HP Anyware deployments would be setup, one called production and the other called staging.
- Use case: a service provider is managing the environment for three customers. Three HP Anyware deployments would be setup: Acme Association, Better Biz, and Cool Company.
- Use case: an IT admin would like to setup a production and a DR (disaster recovery) environment. Two HP Anyware deployments would be setup, one called production and the other called DR.
- Use case: an IT admin wants segregated groupings of remote workstations and access policies.

**Remote Workstation** – A remote desktop running Windows or Linux OS.

**Anyware Connector** – Software that is installed in a customer environment, for example Google Cloud Platform (GCP), Amazon Web Services (AWS), Azure or on-premises, that provides connectivity between the PCoIP clients and the remote workstations. The Connector provides a single point of entry into a deployment of remote workstations. It communicates with the CAM Service (SaaS operated by HP) and is part of a deployment. A deployment can have one or more Connectors. You cannot configure multiple Connector's in the same deployment to different ADs or with different AD configurations. It includes a NAT function for access through an IP address.

- Use case: an IT admin has a hybrid environment where some remote workstations are on-premises and others are in the cloud (i.e. GCP, AWS, Azure, on-premises). For a given deployment, a connector would be installed within the customer's cloud subscription as well as a connector would be installed within the customer's on-prem environment (i.e. a VM running on ESXi). The customer



should use the Connector that is geographically closest to their associated workstation to minimize egress costs and ensure the best performance.

- Use case: an IT admin has three offices (London, San Francisco, and New York) where remote workstations are deployed in the cloud (i.e. GCP, Azure, or AWS) which are closest to these three offices. For a given deployment, three Connectors would be installed within the customer's cloud subscription in London, WestUS and EastUS.

**Users** – People that are present in the AD. These people are assigned remote workstations to connect to.

**Admin Console** - A web application that can be used by an IT admin to manage and assess their HP Anyware deployments, Connectors and remote workstations. It can be accessed by opening a web browser and connecting to <https://cas.teradici.com/>.

**Private Cloud** - Computing services offered over the internet or a private internal network to select users instead of the general public. Private Cloud is used to define clouds or hypervisors that Anyware Manager is unable to directly interact with.

**On-Premises** - Also sometimes shortened to *On-Prem*, this is services and applications that run on a customer's hardware within their own data centre.

# System Requirements

For information on the system requirements for the Connector, see the [System Requirements](#) section in the Anyware Manager guide.

## Supported Domain Controller Servers

- Windows 2016 Server with Secure LDAP (LDAPS) enabled.
- Windows 2012 R2 Server with Secure LDAP (LDAPS) enabled.
- Windows 2019 Server with Secure LDAP (LDAPS) enabled.

## Authentication Service

### Admin Console

- Azure Active Directory organizational email address or a G-Suite or Google Cloud Identity enterprise account.

#### Cloud Identity Accounts

Personal Gmail accounts are not supported by default and need to be allowed by us before being used. For access to Anyware Manager as a Service with a personal Gmail account, contact [HP sales](#) or open a [support case](#).

### Remote Workstations and Workstation users

- Active Directory permissions set to **List contents** and **Read all properties**. If you do not set these permissions you will be unable to connect to specific remote workstations.

## Anyware Software

- License registration code emailed from us in the form of *ABCDEF1234@AB12-C345-D67E-89FG*.
- A [PCoIP Standard or Graphics agent](#) installed on the remote workstation.

- To connect to remote workstations you require a client. The following are the supported clients with HP:
  - HP PCoIP Software Clients for [Mac, Linux, Windows](#) or Chrome OS
  - HP PCoIP Mobile Clients for [iOS](#) and [Android](#) tablets
  - HP [PCoIP Zero Clients](#)
  - HP ThinPro Operating System

## Required External Connections

The Connector requires certain external connections and sites to be available to enable the Connector to function properly. The following table outlines the sites that need to be allowed and should be available to access:

Description	Destination	Protocol	Port
This is the Anyware Connector on Rocky Linux	- <a href="https://dl.rockylinux.org">dl.rockylinux.org</a> - <a href="https://mirrors.rockylinux.org">mirrors.rockylinux.org</a>	TCP	443
This is the Anyware Connector on RHEL Linux	<a href="https://cdn.redhat.com">cdn.redhat.com</a>	TCP	443
Default Apt Rep for Ubuntu 20.04.	<a href="https://security.ubuntu.com">security.ubuntu.com</a>	TCP	80
Source for first-party Ubuntu packages; required so that the OS on the Connector remote workstation can be kept up to date. This address is location dependent, so for example, if you are in the USA, it would be <a href="https://us.archive.ubuntu.com">us.archive.ubuntu.com</a> , or if you were in Canada it would be <a href="https://ca.archive.ubuntu.com">ca.archive.ubuntu.com</a> .	<a href="https://*.archive.ubuntu.com">*.archive.ubuntu.com</a>	TCP	80
This is Anyware Manager as a Service. It is required for both API usage, and to access the Admin Console. <a href="https://cas.teradici.com">https://cas.teradici.com</a> is fronted by Cloudflare, and all IP Address ranges are managed by Cloudflare. IP Ranges can be found here: <a href="https://www.cloudflare.com/ips/">https://www.cloudflare.com/ips/</a> . Please note that you are responsible to maintain the allowlist as per the published Cloudflare's list and request updates from Cloudflare if variances are identified. If you do not maintain the allowlist as expected, it may result in intermittent failures.	<a href="https://cas.teradici.com">https://cas.teradici.com</a>	TCP	443
Source for Connector components, configuration files and the Cloud Access Connector installer. It is required in order for the Connector to be installed, configured and updated over time.	- <a href="https://dl.anyware.hp.com">dl.anyware.hp.com</a> - <a href="https://dl.teradici.com">dl.teradici.com</a>	TCP	443
This is used by the installer to download docker containers used by the Connector that are developed and maintained by us.	<a href="https://docker.cloudsmith.io">docker.cloudsmith.io</a>	TCP	443
This domain is used by the installer for licensing and validating the registration code. It is the operations website for Flexera.	<a href="https://teradici.compliance.flexnetoperations.com">teradici.compliance.flexnetoperations.com</a>	TCP	443

Description	Destination	Protocol	Port
Source for Docker. It is required so that Docker can be installed to run the Connector.	<a href="https://download.docker.com">download.docker.com</a>	TCP	443
This site is used to download the public docker containers. These are not maintained by us.	hub.docker.com	TCP	443
This is a public docker repo.	registry-1.docker.io	TCP	443
This is a public docker repo.	production.cloudflare.docker.com	TCP	443
SumoLogic log collection. Logs from the Connector components are sent to SumoLogic. For sumologic, multiple FQDNs may need to be allowed, see <a href="https://help.sumologic.com/APIs/General-API-Information/Sumo-Logic-Endpoints-and-Firewall-Security">https://help.sumologic.com/APIs/General-API-Information/Sumo-Logic-Endpoints-and-Firewall-Security</a> for full list. For more details on the information we collect, and how we collect it, please see the <a href="#">Anyware Manager as a Service Privacy Policy</a> .	<a href="https://*.sumologic.com">*.sumologic.com</a>	TCP	443

\*These URLs are location dependent.

### Allowing IP Addresses

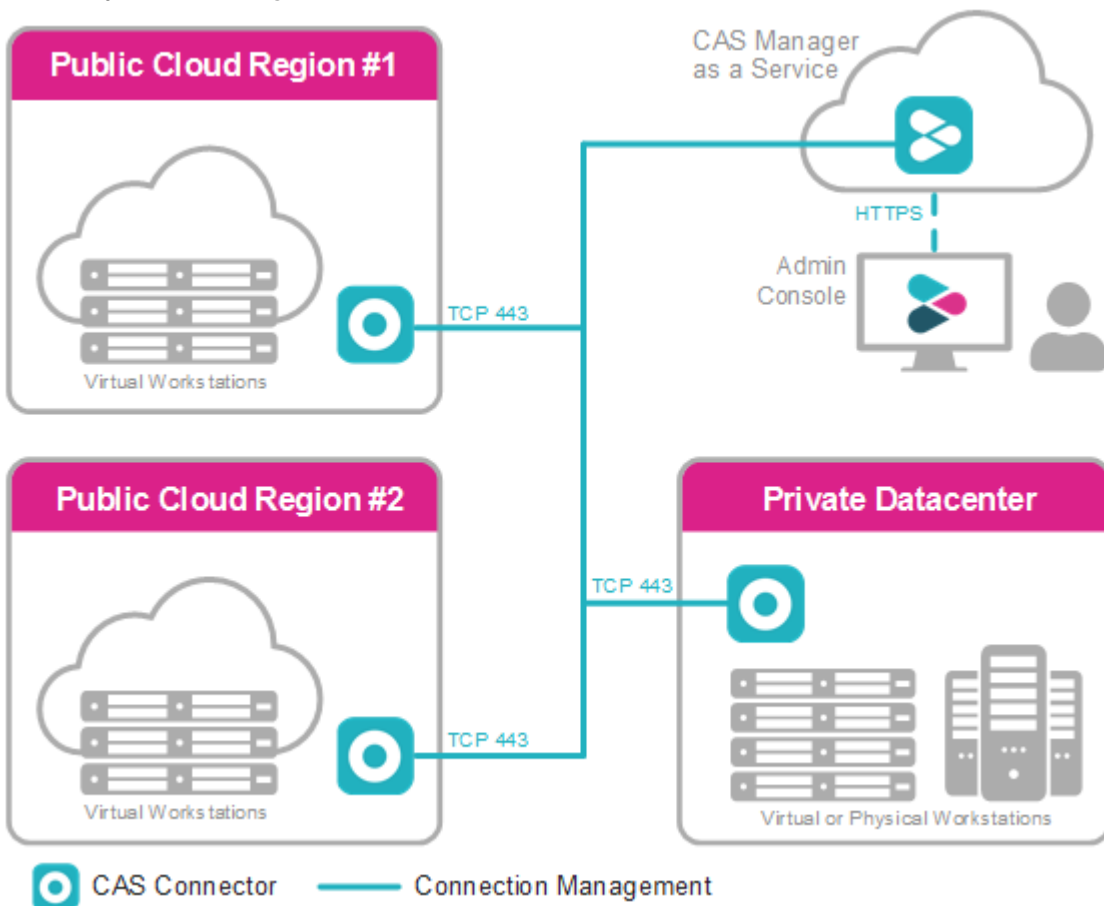
If you are still having issues with installation after allowing all the required sites and domains, try to resolve the failing sites by resolving the associated IP addresses and allowing these IPs in your firewall.

# 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. 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. If you want to log in using Microsoft Azure, you must have consent to access the HP Azure application. Depending on your restrictions, a user or a system administrator could grant this access. For information on how to grant admin consent, see [Grant tenant-wide admin consent to an application](#) on the Microsoft site.

### Email Account Support with Anyware Manager

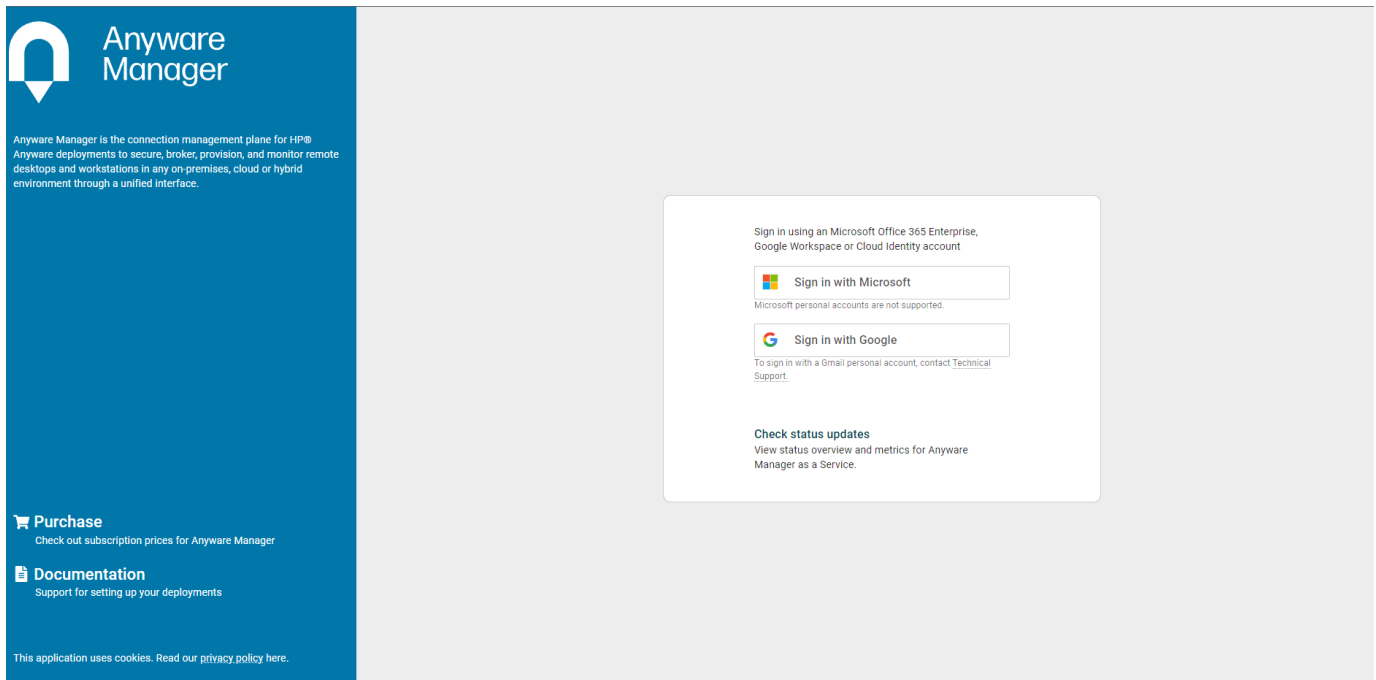
Anyware Manager supports two types of email accounts:

- 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 allowed 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.





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 allowed by HP.
- Cookies have been blocked on <https://cas.teradici.com/>.
- Pop-ups have been blocked on <https://cas.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 will 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.

The screenshot displays the Admin Console Dashboard. On the left, a light blue panel titled "Getting Started" contains a welcome message: "Welcome to the Admin Console! The Admin Console is a single interface for managing and deploying your PCoIP Remote Workstation environment." Below the text is an icon of a computer monitor displaying the Anyware logo. Underneath the icon, it says "Admin Console" and "Click on any of the cards to get started deploying your PCoIP environment." To the right of this panel is a vertical stack of five white cards, each with an icon and a title:

- Learn more**: Information on key concepts, installation and use of the Admin Console. (Icon: document)
- Add cloud credentials**: To enable interactions with public clouds for capabilities such as power management. (Icon: cloud)
- Create connector**: Connectors are required to connect users to their workstations. (Icon: network diagram)
- Add remote workstation**: A connector must be configured before workstations can be added. (Icon: monitor with lock)
- Set up PCoIP connection**: Learn how to connect to a remote workstation using a PCoIP client. (Icon: wrench)

## Configuring the Admin Console

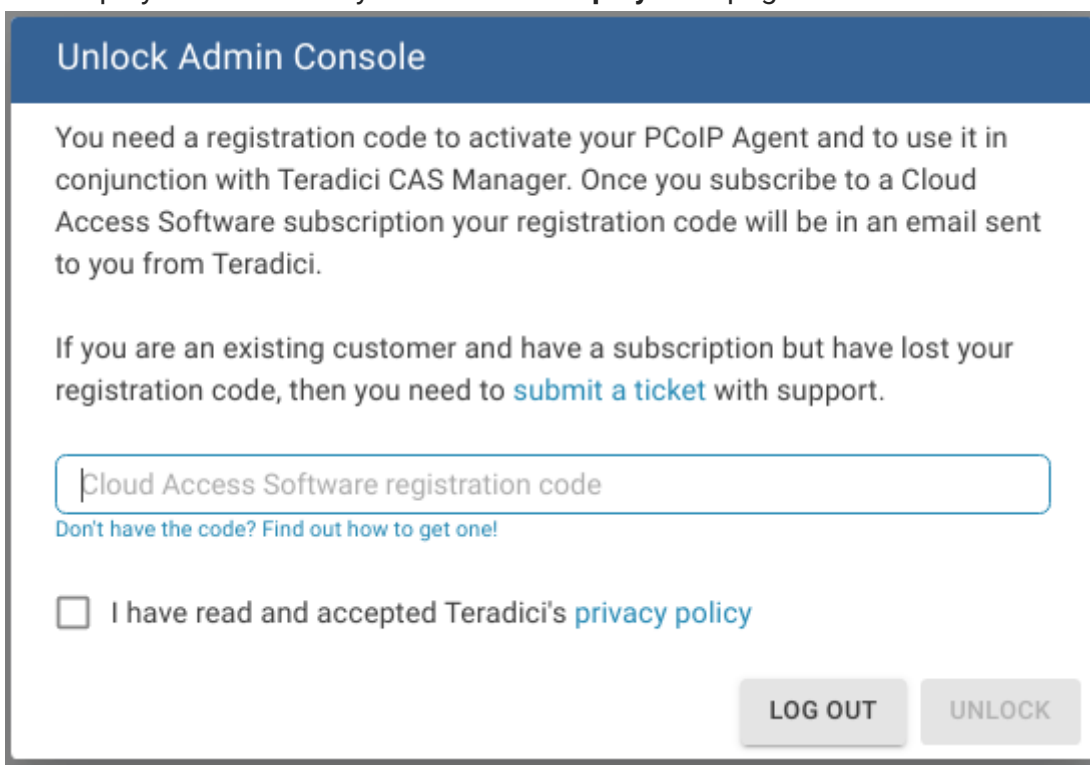
On the **Deployments**, **Connectors** and **Remote Workstations** pages you can control which columns are visible and in which order they appear for the listed resources. To change your column options,

select **COLUMNS** from the page heading and select which columns you wish to make visible. The format you select will be preserved when you log back into the Admin Console.

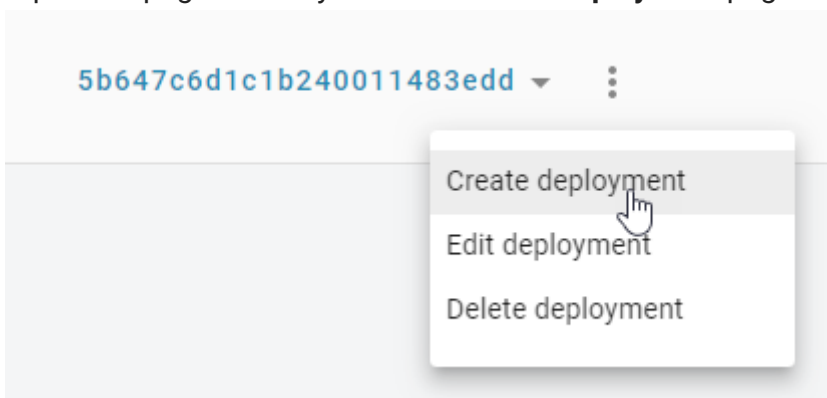
# Managing Deployments

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 will be prompted to enter your Anyware Software registration code. Once you enter the code it will automatically generate your first deployment and take you to the **Edit Deployment** page.



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.
- Click **CREATE**.

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

## Provider Service Accounts

You can now enter Provider 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.

### **Provider 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 workstation provider of your choice.

### **Domain Controllers in a Single Deployment**

You cannot deploy multiple Connectors against different Domain Controllers within the same deployment. This will cause 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 of the Anyware Manager Admin guide.

### 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 **Provider 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 will 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 will still add the role but will 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 straight away as it will not be 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 Provider 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 Provider 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 will now be 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	Created date
test-cn	Jul 4, 2019 16:51:08 UTC
	Last modified date
	Jul 15, 2019 21:35:14 UTC
	Internal IP
	10.0.1.2
	<input type="button" value="CANCEL"/> <input type="button" value="SAVE"/>

## Domain Controller Certificates

If all DC certificates have expired, the Anyware Connector will stop working. An error indicator will display on the **Connectors** page when a Anyware Connector has a DC with expired certificates.

A warning indicator that details the current state of the DC certs will display on the same page when a Anyware Connector has a certificate that less than a week away from expiring.

## Anyware Connector - Troubleshooting

If there is an issue installing the Anyware Connector or an existing Connector is failing, please see the troubleshooting section on [Anyware Connector Connectivity](#). Within this section there are steps to check the following:

- Remote Workstation connections
- Active Directory connections
- Anyware Connector component information

For information on installer errors related to a change in the distribution system, see [here](#).

# 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 will still be 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 20 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 will list 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 will be automatically unassigned from the user, and the remote workstation will become available for other users to connect to.

## Floating Workstation Assignment Policy

When assigning floating workstation to the users, you can assign a workstation holding time for a particular user and the corresponding workstation. To enable the workstation holding time:

1. Navigate to the **Workstation Pool** tab from the left pane, and click **+** to create a new workstation pool.
2. In the **Workstation Holding Time** section, select the desired time from the dropdown menu.

### Create a new workstation pool

**WORKSTATION ASSIGNMENT POLICY**

One time selection which determines how workstations are assigned to users. **This option cannot be changed once the pool is created.**

Persistent  
 Floating

You need to enable session tracking for this deployment to use the floating assignment policy

Session Tracking ?

**WORKSTATION HOLDING TIME**

Assignment holding time ?      Unit of time

Minutes ▾

**Workstation Holding Time limit**

The holding time can be set in the form of minutes, hours, or days. The minimum holding time for a workstation pool is 20 minutes and maximum holding time is 1096 days.

## 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 will only be able to 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 will be automatically assigned to the user. The following steps outline how to add users to a workstation pool:

1. Select the **Workstation Pool** tab from the left pane, 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 will become 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 will see the following error during session establishment "Resource does not exist on CAM Service".
- Remote workstations will 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 will work 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, the user will

see a 6604 error message. 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 will see the Windows Switch Users screen. They will then be prompted to enter their credentials again before accessing the desktop.

## 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 will result 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 table outlines the options you can use to manage the auto log-off service:

Option	Description
<code>--enable</code>	Enable the service.
<code>--disable</code>	Disable the service.
<code>--change-params</code>	Modify CPU utilization limit ( <code>CPUUtilizationLimit</code> ) and Idle time before logging off ( <code>MinutesIdleBeforeLogOff</code> ).
<code>--change-timer</code>	Modify polling interval ( <code>OnUnitActiveSec</code> ). This value sets how often the service runs.
<code>--show-logs</code>	Shows last 100 log messages.
<code>--follow-logs</code>	Shows live log messages.
<code>--help</code>	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
<code>MinutesIdleBeforeLogOff</code>	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.
<code>CPUUtilizationLimit</code>	20%	Value between 0 and 100 representing CPU utilization percentage. If average CPU utilization is below this value, the machine is considered idle, and will log-off if maintained for <code>MinutesIdleBeforeLogOff</code> .
<code>OnUnitActiveSec</code>	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
```

# 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:

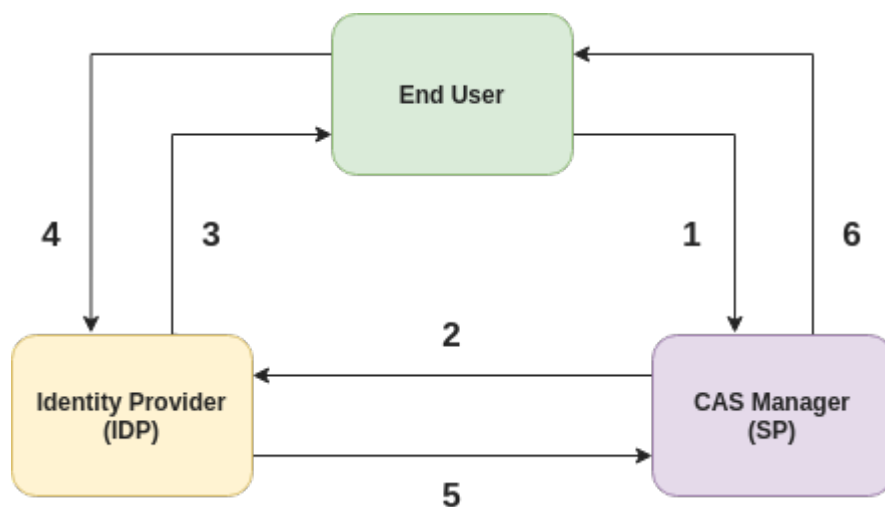
- **End User:** A user who is trying to access a service using federated login credentials
- **Identity Provider (IDP):** An identity provider performs the authentication about the end users identity and sends the necessary data to the service provider along with any other access control data in the 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 will allow 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 will 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. APIs 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 (HAPP) or have been pre-approved by HP. Contact us [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 <https://cas.teradici.com/api/docs>.

## Creating a 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 CAM 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 will return service account information. This information should be saved as a JSON file in a secure location, as it can only be retrieved once. It will return 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 will be 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 will 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 (HAPP) or have been pre-approved by HP. Contact HP [here](#) for more information.

# 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

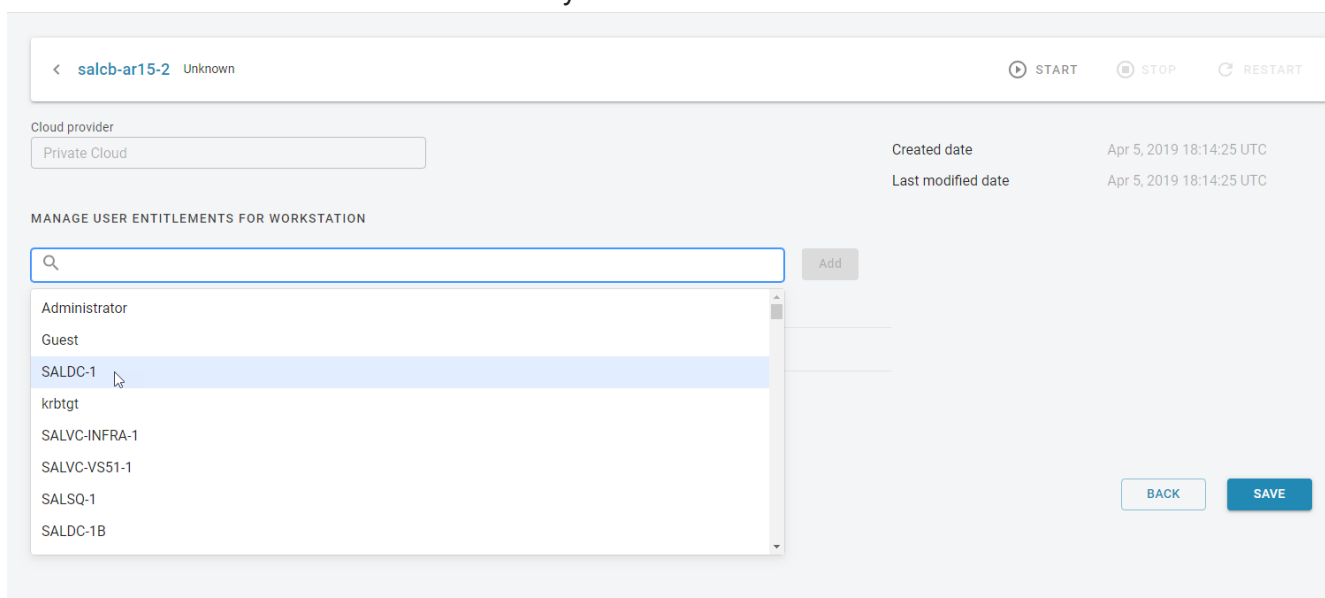
Once you have created a remote workstation within the Admin Console you can manage and reconfigure it directly from the **Remote Workstations** page.

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:



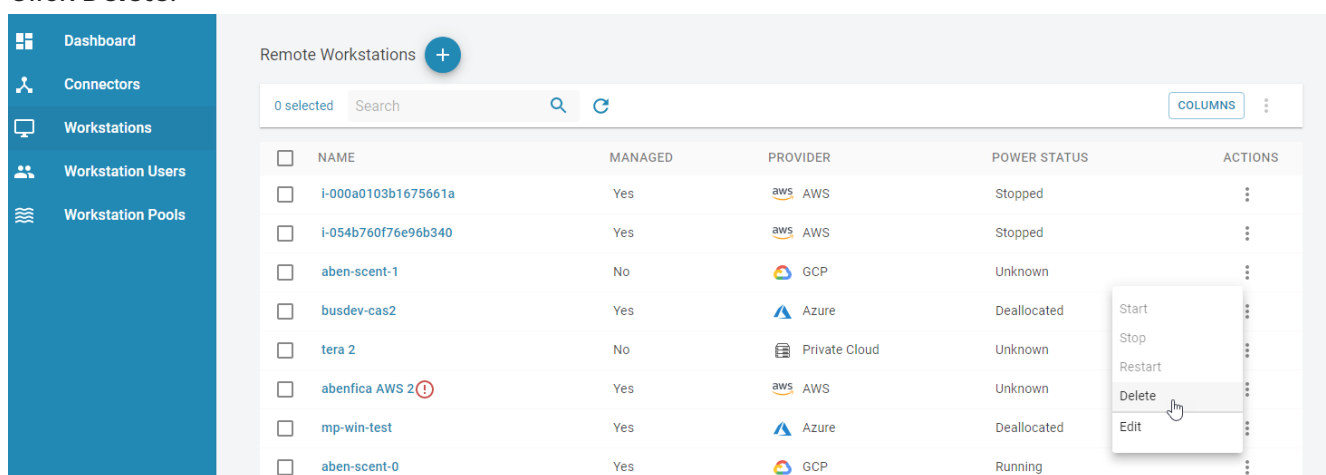
4. Click **Add** and then **SAVE**.

The user you entitled will appear 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 the Admin Console. Only remote workstations that exist in AWS, Azure, and GCP and are part of deployments that have valid provider 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**.



The screenshot shows the 'Remote Workstations' page in the Admin Console. The sidebar on the left contains navigation options: Dashboard, Connectors, Workstations, Workstation Users, and Workstation Pools. The main content area displays a table of remote workstations with columns for NAME, MANAGED, PROVIDER, POWER STATUS, and ACTIONS. A kebab menu is open for the 'abenfica AWS 2' workstation, showing options: Start, Stop, Restart, Delete, and Edit. The 'Delete' option is highlighted by the mouse cursor.

NAME	MANAGED	PROVIDER	POWER STATUS	ACTIONS
i-000a0103b1675661a	Yes	aws AWS	Stopped	⋮
i-054b760f76e96b340	Yes	aws AWS	Stopped	⋮
aben-scent-1	No	GCP	Unknown	⋮
busdev-cas2	Yes	Azure	Deallocated	⋮
tera 2	No	Private Cloud	Unknown	⋮
abenfica AWS 2	Yes	aws 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 will disappear 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 workstation provider to ensure a successful completion. You will be notified in the Admin Console on the whether the deletion was successful or not.

## 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 will be shown all 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
<a href="#">workstation1</a>	Running	Aug 24, 2019 05:06 PM PDT
<a href="#">workstation2</a>	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 public cloud provider. This enables Anyware Manager to use the credentials for that public cloud provider to access the remote workstation and enable power management. The 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 public cloud provider.

Editing the public cloud provider and zone information will 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 provider credentials for a public cloud provider you will not be able to change the remote workstation public 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 public cloud provider the remote workstation belongs to.
5. Select the region, resource group and zone, depending on the public cloud provider, the remote workstation resides in.
6. Select the remote workstation and update the provider.

If you enter the correct public cloud provider and zone for the remote workstation you will receive a notification that it has been updated. The new zone, public cloud provider and information will be listed on this page also.

If you enter an incorrect zone then you will receive an error message stating that the remote workstation does not exist in the entered zone.



# 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.

#### Federated Authentication with Single Sign-On (SSO)

Single Sign-On is a feature that permits using the IDP to authenticate to the point of selecting your desktop from the list of workstations, and you need not to authenticate again to log in. If you are interested in this functionality, please discuss with your HP account representative.

### PREREQUISITES

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

- Access to Anyware Manager as a Service
- 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 (Currently not supported in Anyware Connector-RHEL/Rocky Linux)
- Anyware Connector-RHEL/Rocky Linux 23.06 or later

### POST CONFIGURATION USER WORKFLOW

After completing the Federated Authentication configuration, the user workflow will be 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 will be 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 are 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**.

The screenshot displays the Okta Applications management page. On the left, a navigation sidebar lists: Dashboard, Directory, Applications (highlighted), Security, Reports, and Settings. The main area is titled 'Applications' and features two primary buttons: 'Create App Integration' and 'Browse App Catalog'. Below these is a search bar. A table shows the status of applications:

STATUS	Count	Action
ACTIVE	4	⚙️
INACTIVE	1	⚙️

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.

## Applications

Create App Integration
Browse App Catalog
Assign Users to App
More ▾

### 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)

Cancel
Next

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**

**Logo (Optional)**



**Grant type** Client acting on behalf of a user  
[Learn More](#)  Authorization Code  
 Interaction Code  
 Refresh Token  
 Resource Owner Password  
 SAML 2.0 Assertion  
 Device Authorization  
 Token Exchange  
 Implicit (hybrid)

---

**Sign-in redirect URIs**  Allow wildcard \* in sign-in URI redirect.

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

[Learn More](#)

---

**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](#)

---

**Assignments**

**Controlled access** 
 Allow everyone in your organization to access  
 Limit access to selected groups  
 Skip group assignment for now

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

6. Check the **Authorization Code** option as Grant type.

7. Enter `pcoip://oauth/` as the **Sign-in redirect URIs**.

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.

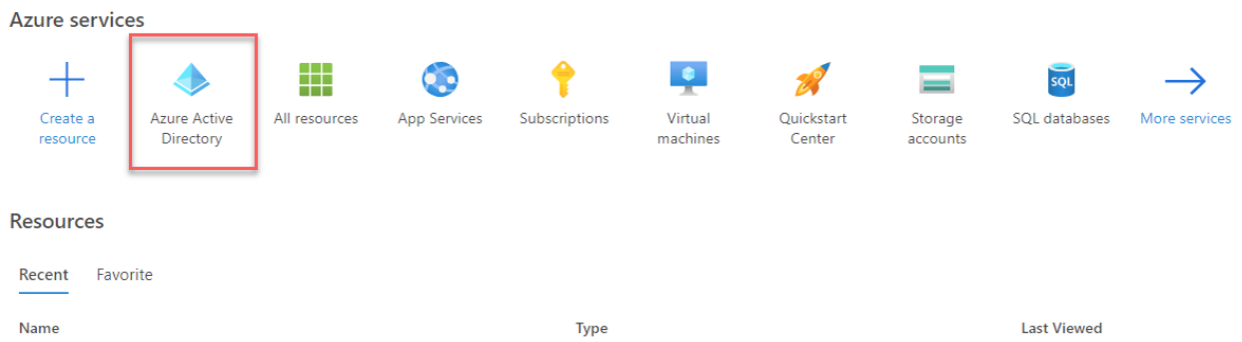
## Configuring Azure Active Directory

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

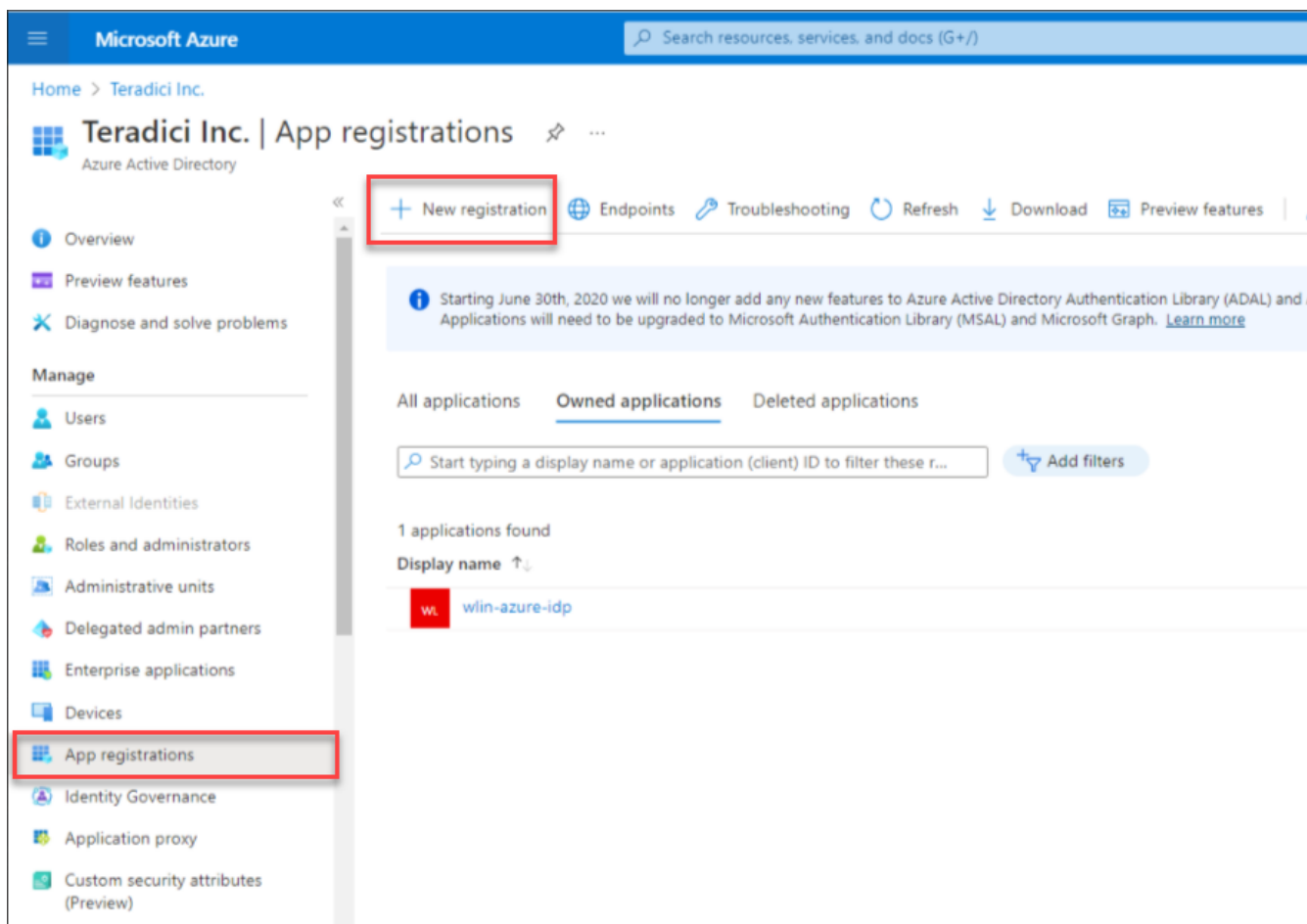
To configure:

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



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





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](#)

**Register**

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

Search resources, services, and docs (G+)

Delete | Endpoints | Preview features

**Essentials**

Display name : [redacted]

Application (client) ID : [redacted] 3307

Object ID : [redacted] 3f8c...

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 Authentication updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Micro...

### 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/[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/[redacted]/oauth2/token
- OpenID Connect metadata document  
https://login.microsoftonline.com/715c7...2cf18/v2.0/.well-known/openid-configuration

## Enable Federated Authentication for Anyware Manager

To use the Federated Authentication feature seamlessly you must have the latest 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. Navigate to <https://cas.teradici.com> and open the web 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:

- Dashboard ▼
- Directory ▼
- Applications ▲
- Applications ▲
- Security ▼
- Reports ▼
- Settings ▼

## Applications

Create App Integration
Browse App Catalog
Assign Users to App
More ▼

STATUS			
ACTIVE	5		
INACTIVE	0		

⚙️

[FedAuthWeb](#)

Client ID: Ooa520zsqvCiqjvN25d7

⚙️

[FuaVelTest](#)

Client ID: Ooa5rbzdevJDKEgSr5d7

⚙️

[My Web App](#)

Client ID: Ooa53acrd6phLLKfe5d7

⚙️

[PCoIP Client](#)

Client ID: Ooa52ocg3nulb2VSW5d7

⚙️

[VelAgentTest](#)

Client ID: Ooa56xofiol5xfidw5d7

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, run the following flags during installing/updating the Connector:

- For Anyware Connector: `anyware-connector configure <other configuration> --id-provider-url <authorization_url> --enable-oauth <true or false> --oauth-client-id <client id>`.
- For Ubuntu 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. - For RHEL/Rocky Linux Connector: - To configure a new connector after installation or update configuration for an existing Connector: - Log into the Connector using SSH. - Run the command:

```
sudo /usr/local/bin/anyware-connector configure <any other configuration flags you use> --pull-config-from-manager.
```

- For Ubuntu Connector:
  - To update:
    - 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.

### For RHEL/Rocky Linux Connector:

If you are configuring a new Connector after installation or updating the configuration for an existing Connector:

- Run this command: `sudo /usr/local/bin/anyware-connector configure [...other settings...] --enable-oauth true --id-provider-url https://id.provider.com --oauth-client-id XXXXXXXXXX`

### For Ubuntu Connector:

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 XXXXXXXXXX`

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 XXXXXXXXXX`

### Configuration Flags

Flag	Type	Description
<code>--enable-oauth</code>	Boolean	Enables OAuth authentication. (Default=False)
<code>--id-provider-url</code>	String	Sets the identity provider URL. Example: <code>--id-provider-url https://provider-1234567890.okta.com</code> . This flag is required if <code>--enable-oauth</code> is true.
<code>--oauth-client-id</code>	String	Gets the Client ID from the Identity Provider. This flag is required if <code>--enable-oauth</code> is true.
<code>--fa-url</code>	String	The Federated Auth Broker URL. for example <a href="https://cac-vm-fqdn:port">https://cac-vm-fqdn:port</a>
<code>--oauth-flow-code</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
<code>--enable-entitlements-by-upn</code>	Boolean	Enables/Disables searching entitlements by UPN. Note: This flag is not required for the Anyware Connector. It is supported for the Connector on Ubuntu for versions 164 or below.

# Single Sign-on (SSO)

## 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:

- Access to Anyware Manager as a Service
- 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
- Anyware Connector-RHEL/Rocky Linux 23.06 or later

### POST CONFIGURATION USER WORKFLOW

After completing the Federated Authentication configuration, the user workflow will be 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 identify 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:

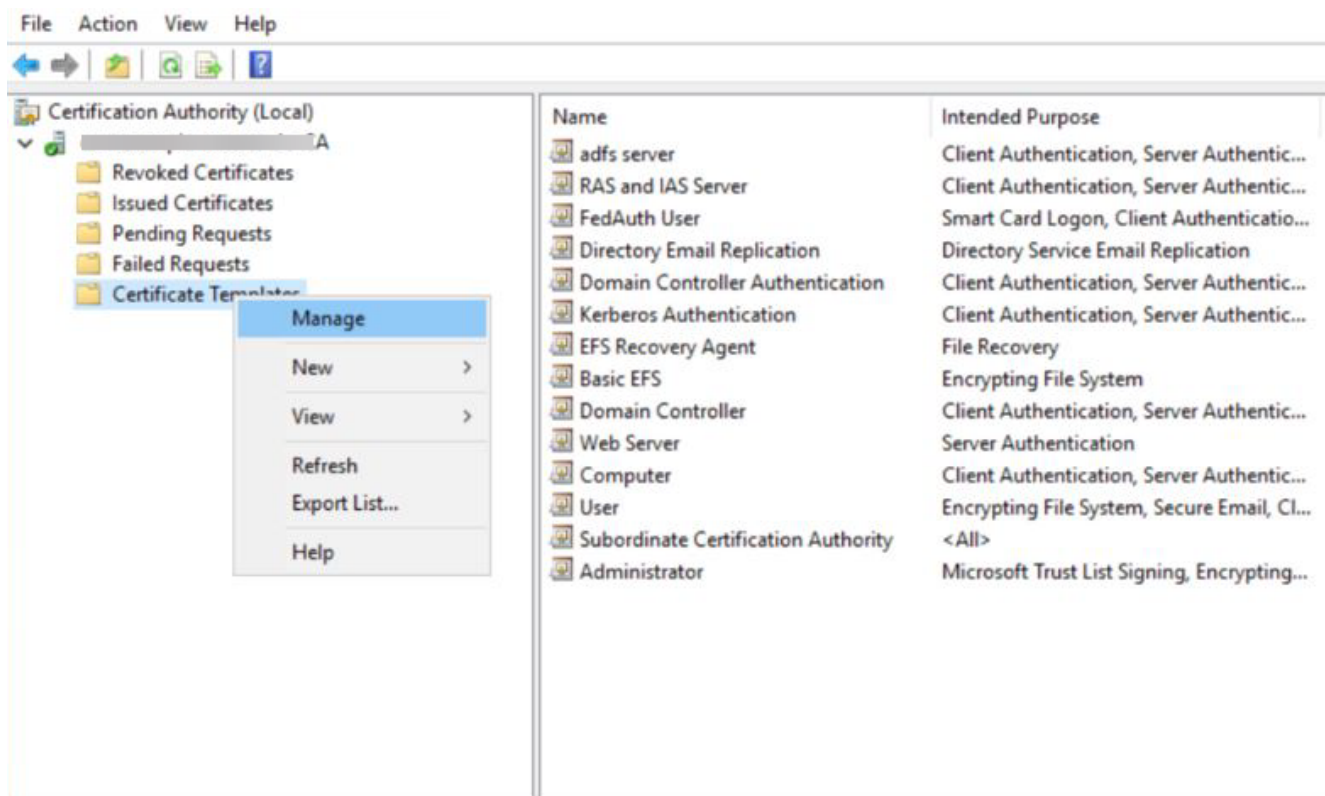
- [By Active Directory Certification Authority Web Enrollment](#)
- [By private key and certificate of the Certification Authority](#)

### By Active Directory Certification Authority Web Enrollment

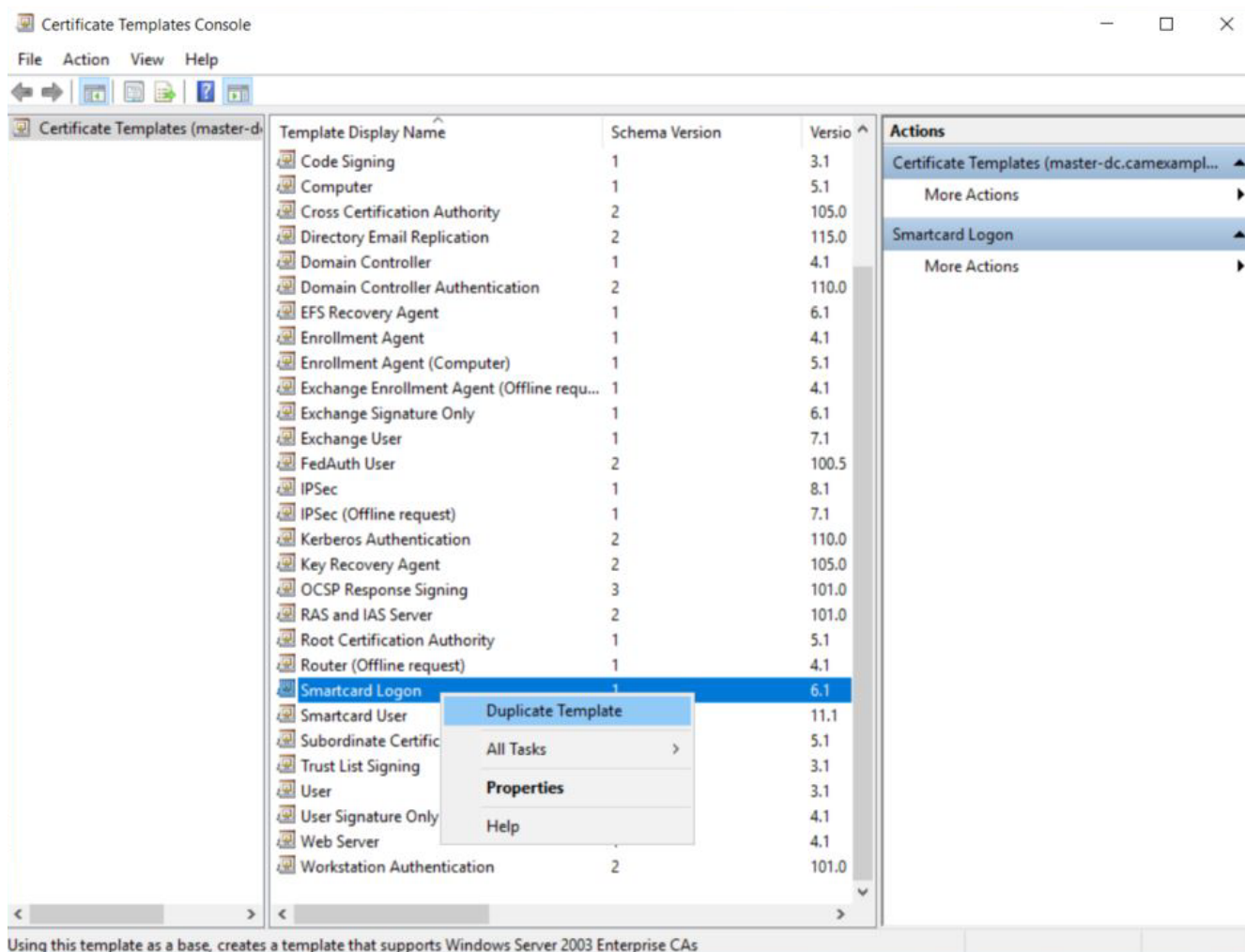
 **Note: The CA certificate and key could be used by malicious actors to impersonate valid devices on your network, impacting confidentiality, and integrity. We recommend following the [Active Directory Certification Authority Web Enrollment](#) method if your connector has an external IP address. If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

### Create Certificate Authority Template

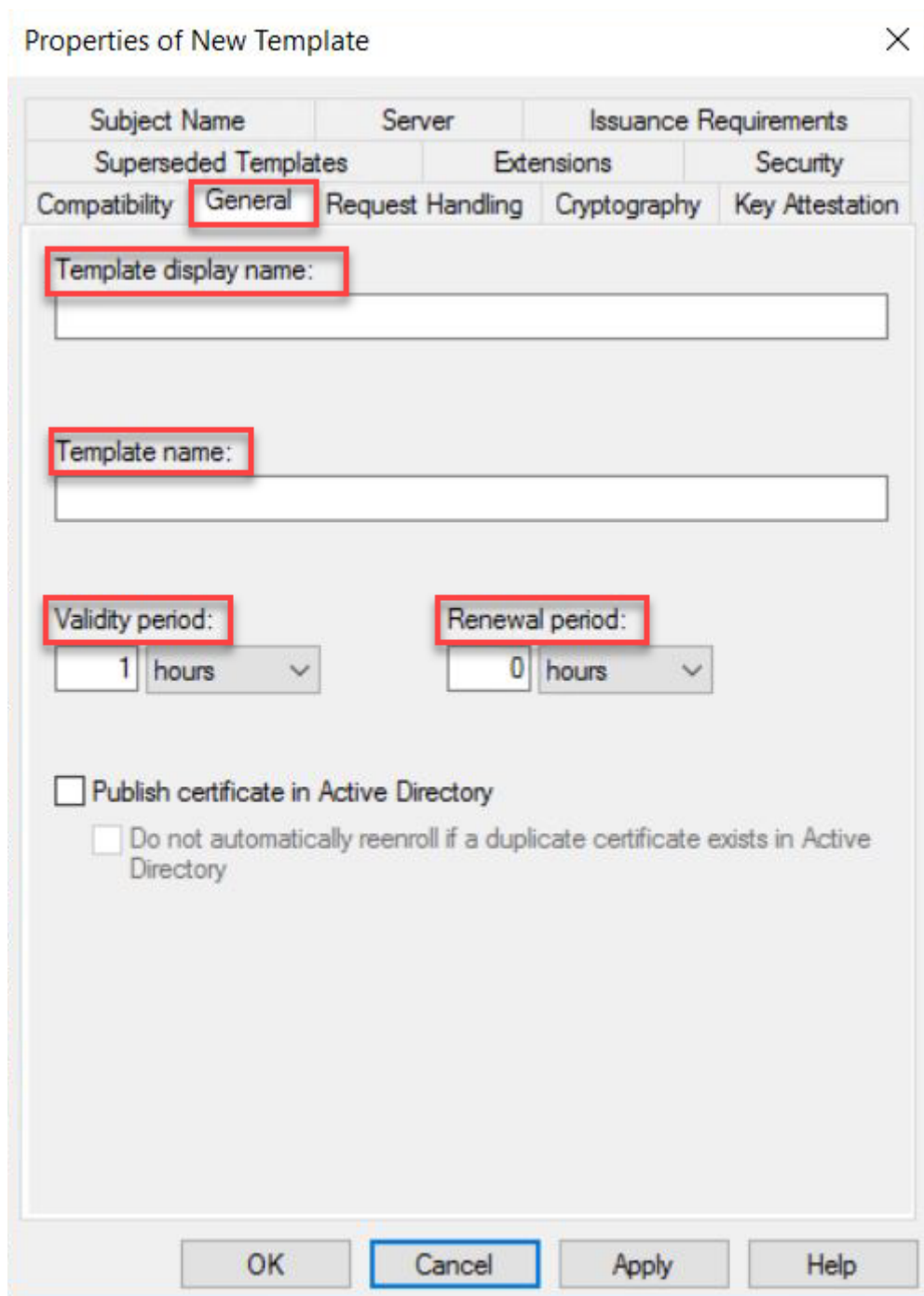
1. Log on to the Certificate Authority resource.
2. Open Certificate Authority MMC (`certsrv.msc`).
3. Right click the **Certificate Templates** and select **Manage**.



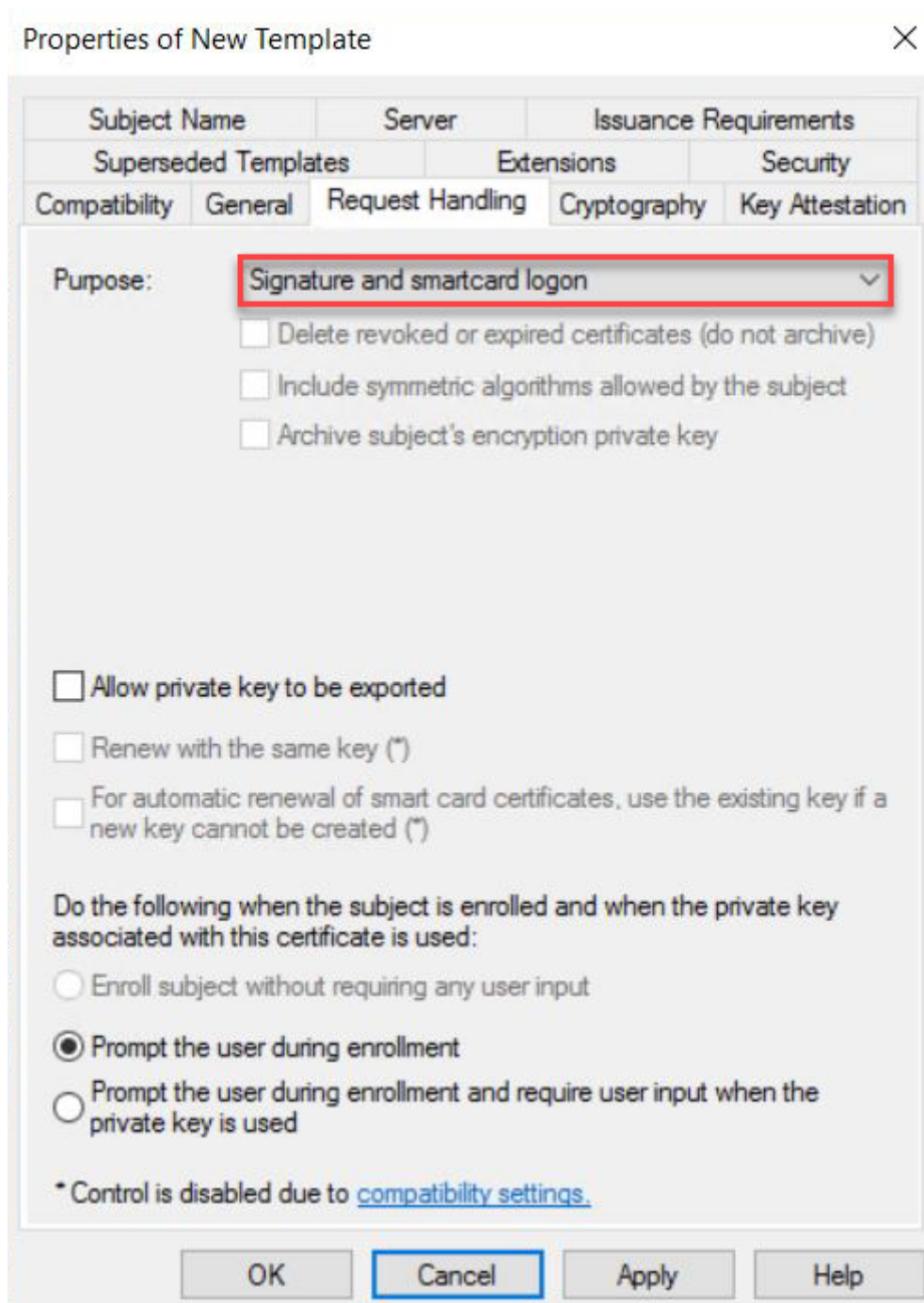
4. **Certificates Templates Console** window is now open. Right click **Smartcard User** and select **Duplicate Template**.



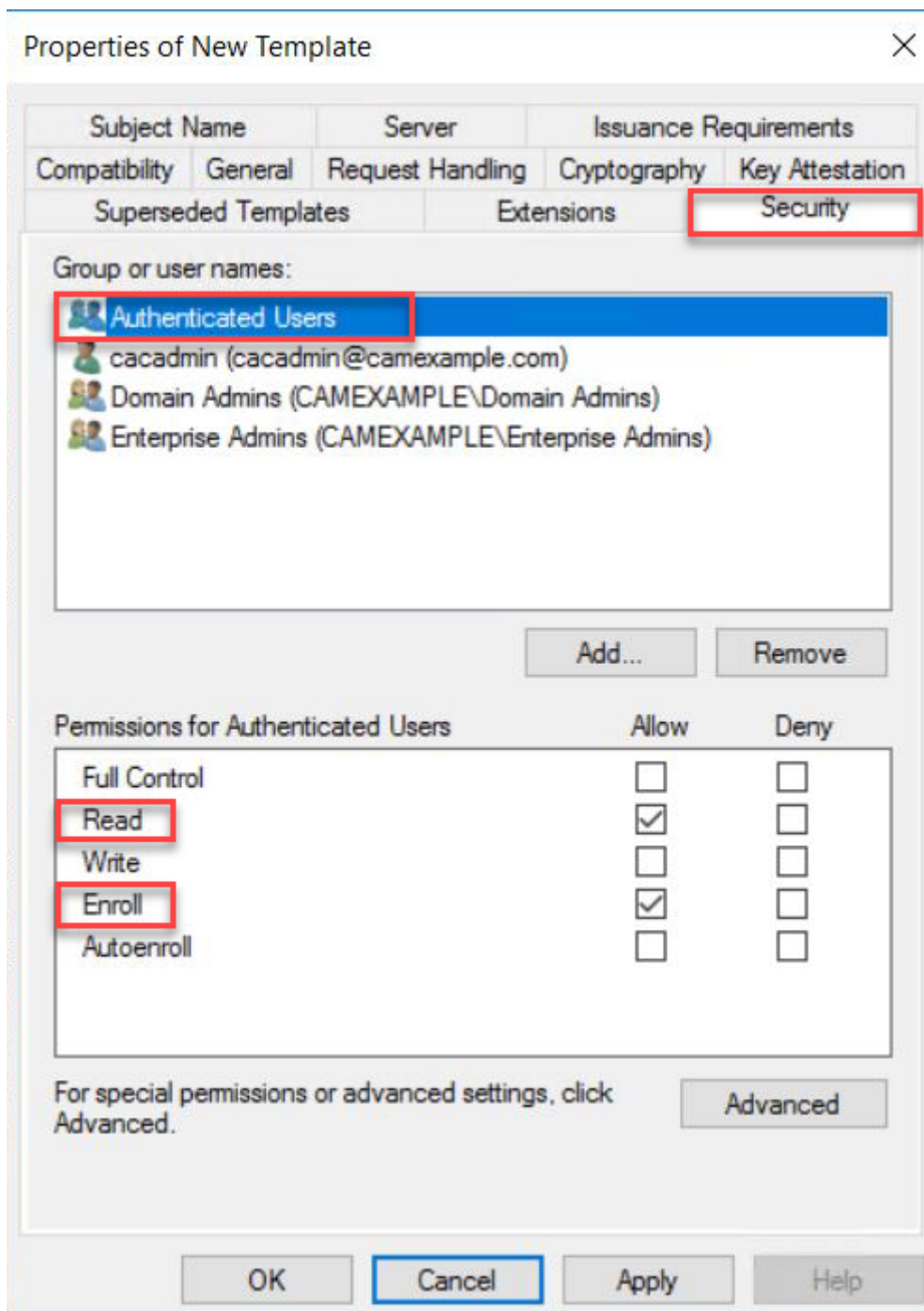
5. Navigate to the **General** tab and rename the template to a desired name and take note of the name as it is required during Connector installation. Change the **Validity Period** and **Renewal Period** to minimum such as 1 hours and 0 hours respectively.



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.

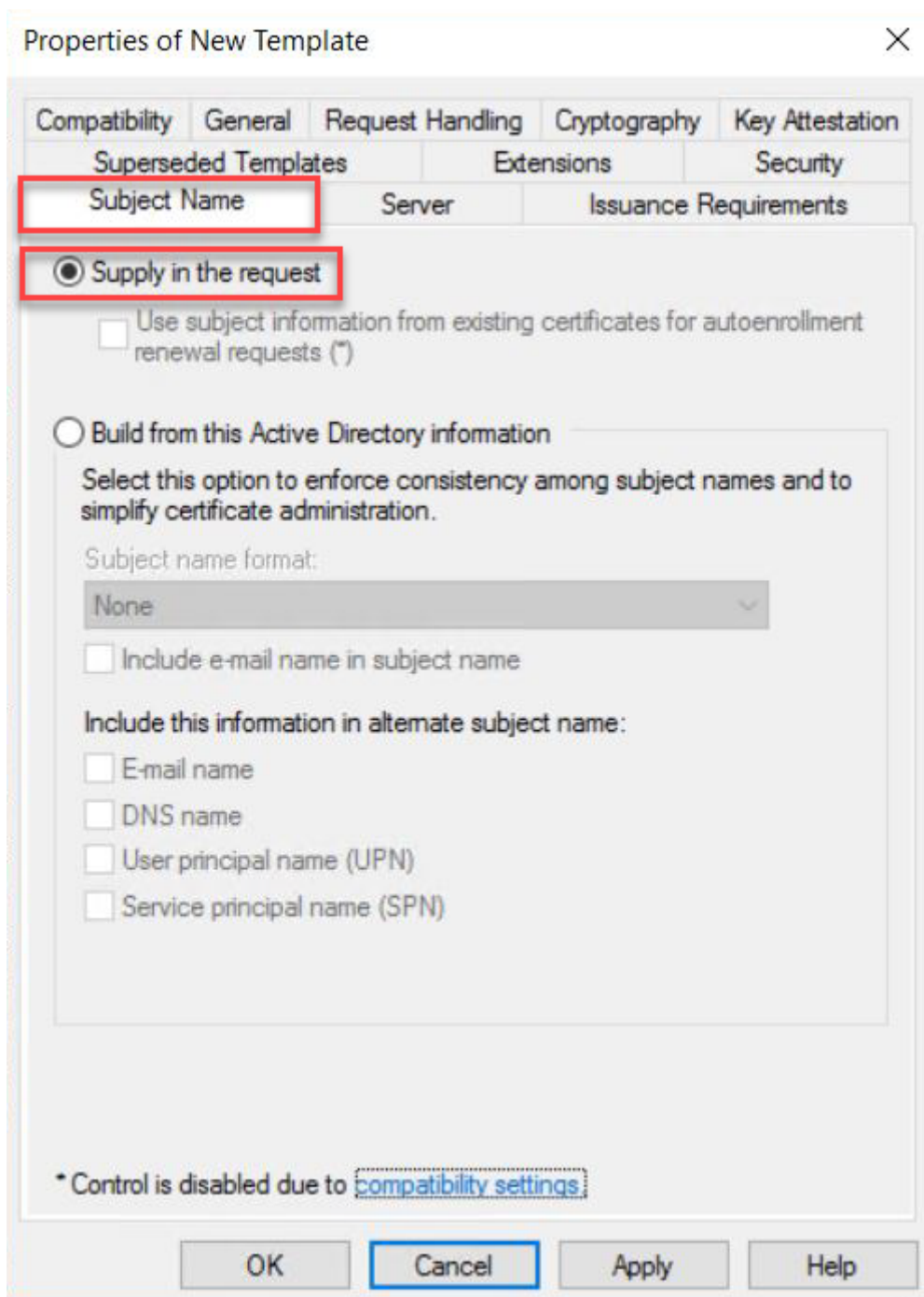


7. Navigate to **Security** tab and select **Read** and **Enroll** as **Allow** for **Authenticated Users**.



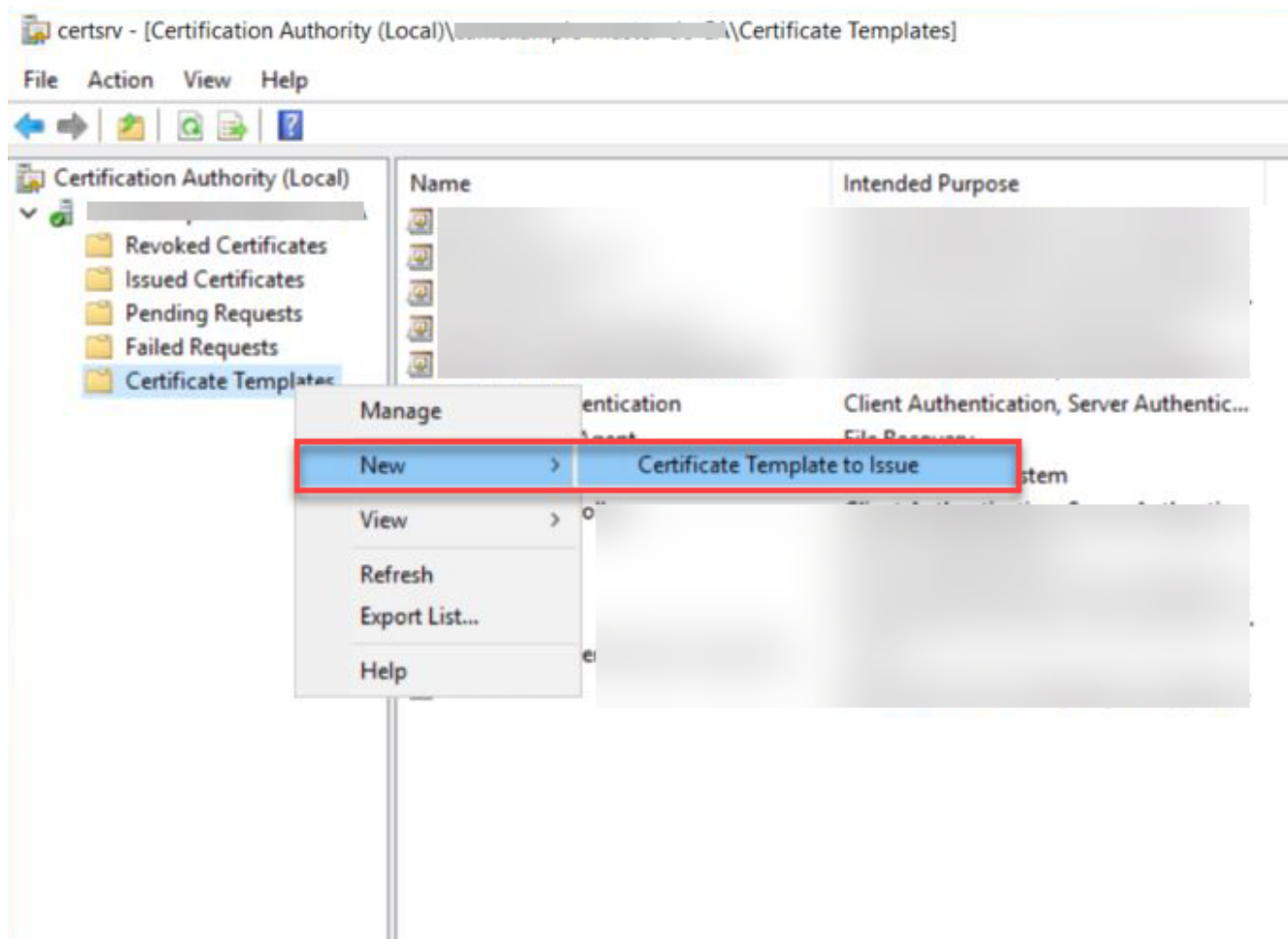
8. Navigage to **Subject Name** tab and select **Supply in the request**. A warning text box appears and click **OK** to close the warning text box.





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**.

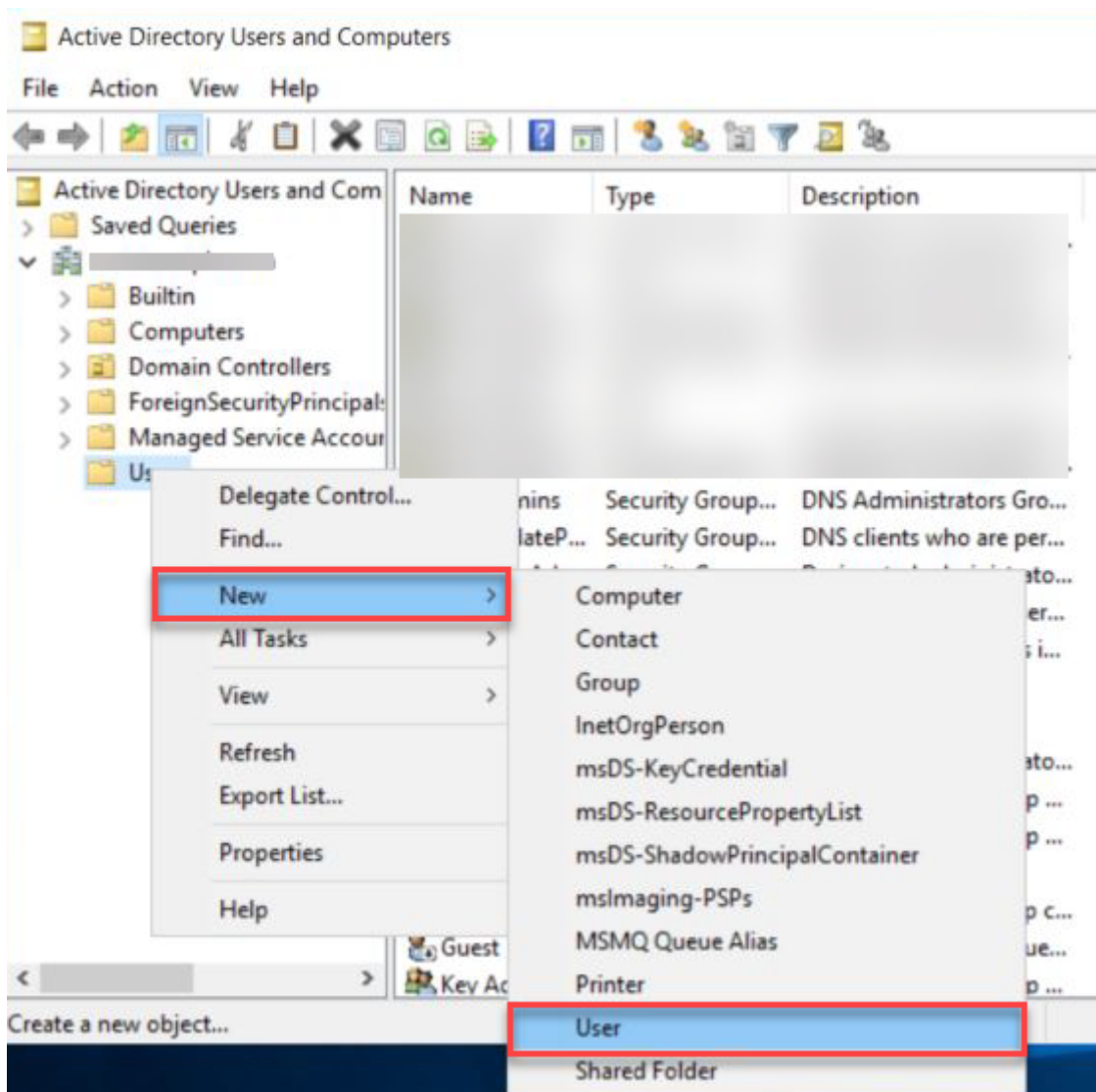


11. Select the template created above and click **OK** to add the template to CA.

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**.

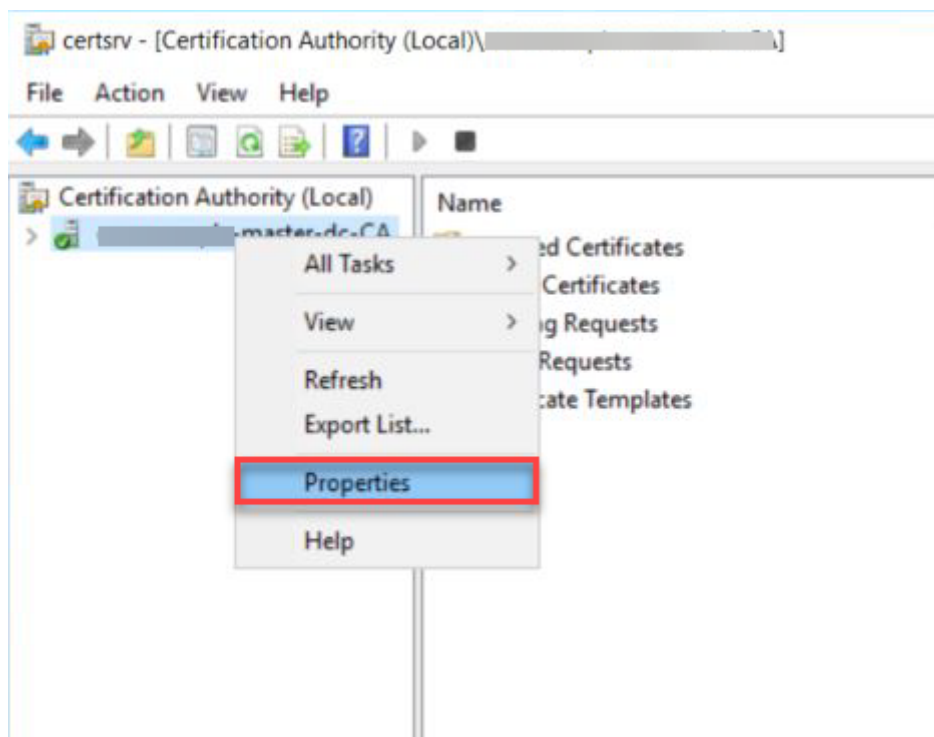




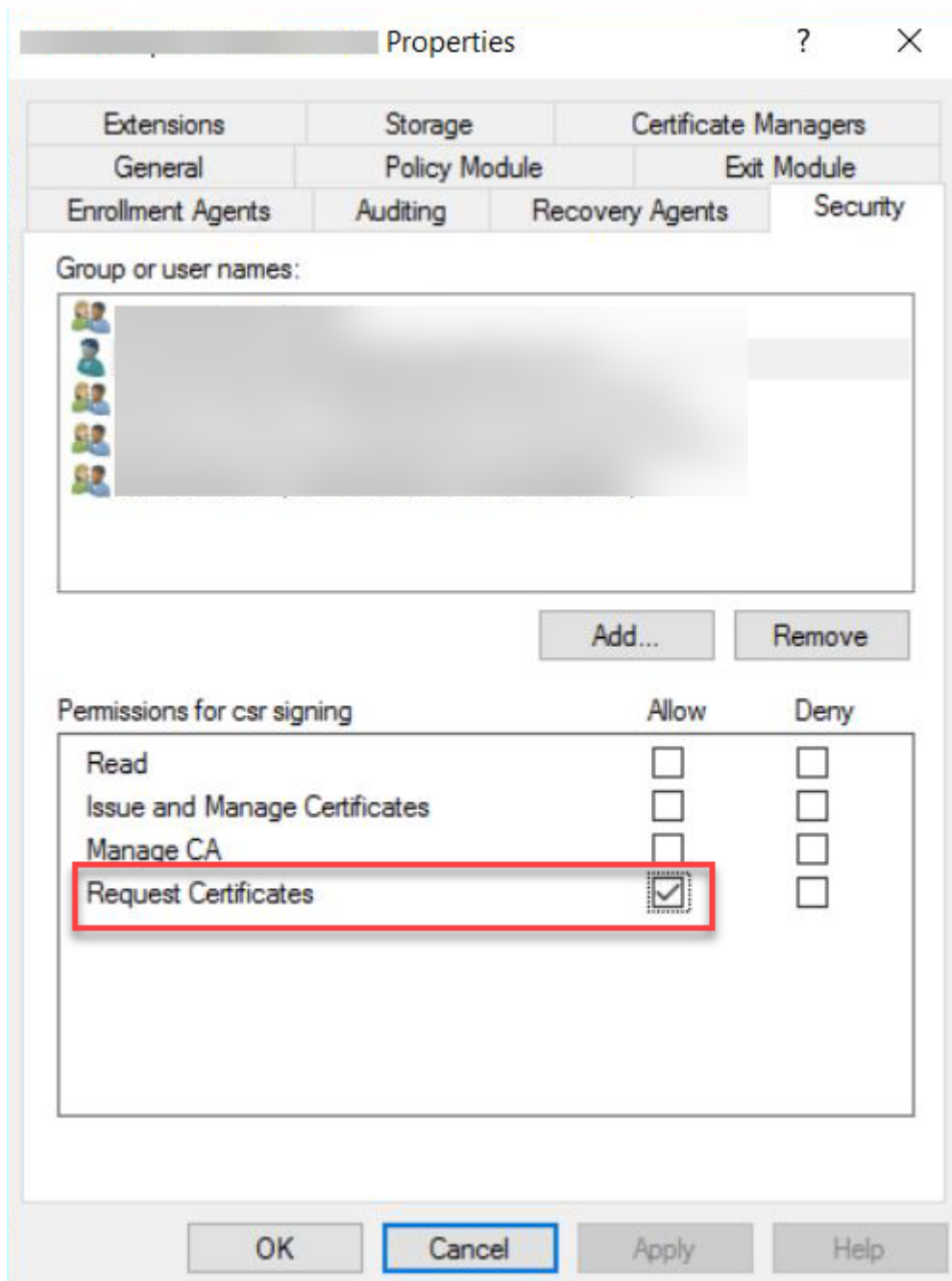
4. Enter the required information such as First name, Last name, User Logon name ...etc and click on **Next**.
5. Enter the Password for the user and click **Next**.
6. Note the username and password as it is required during Connector installation.
7. Click on **Finish** to create the user.

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**.

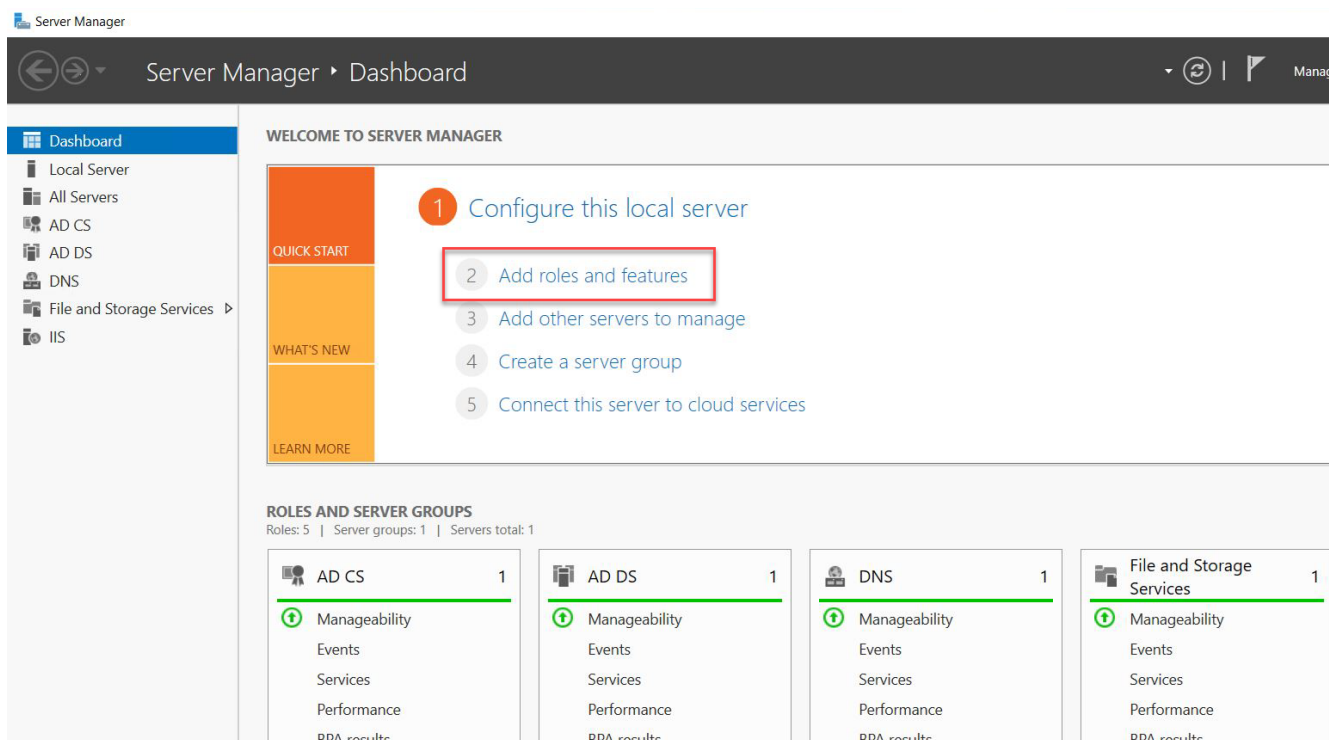


4. Navigate to **Security** tab and click **Add...** and add the user created above.
5. Ensure the user added is allowed to **Request Certificates**.



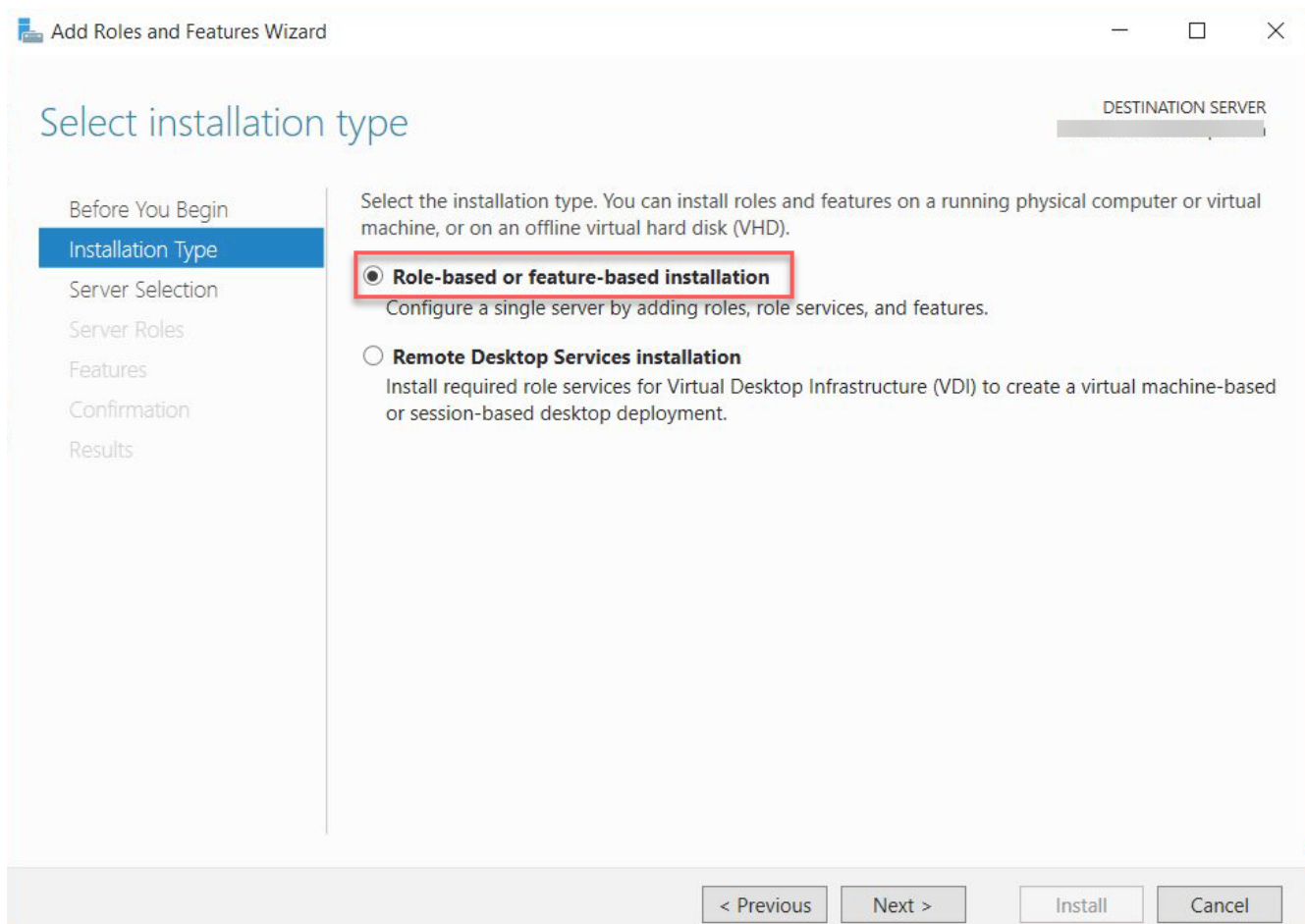
Set up Active Directory Certification Authority Web Enrollment

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

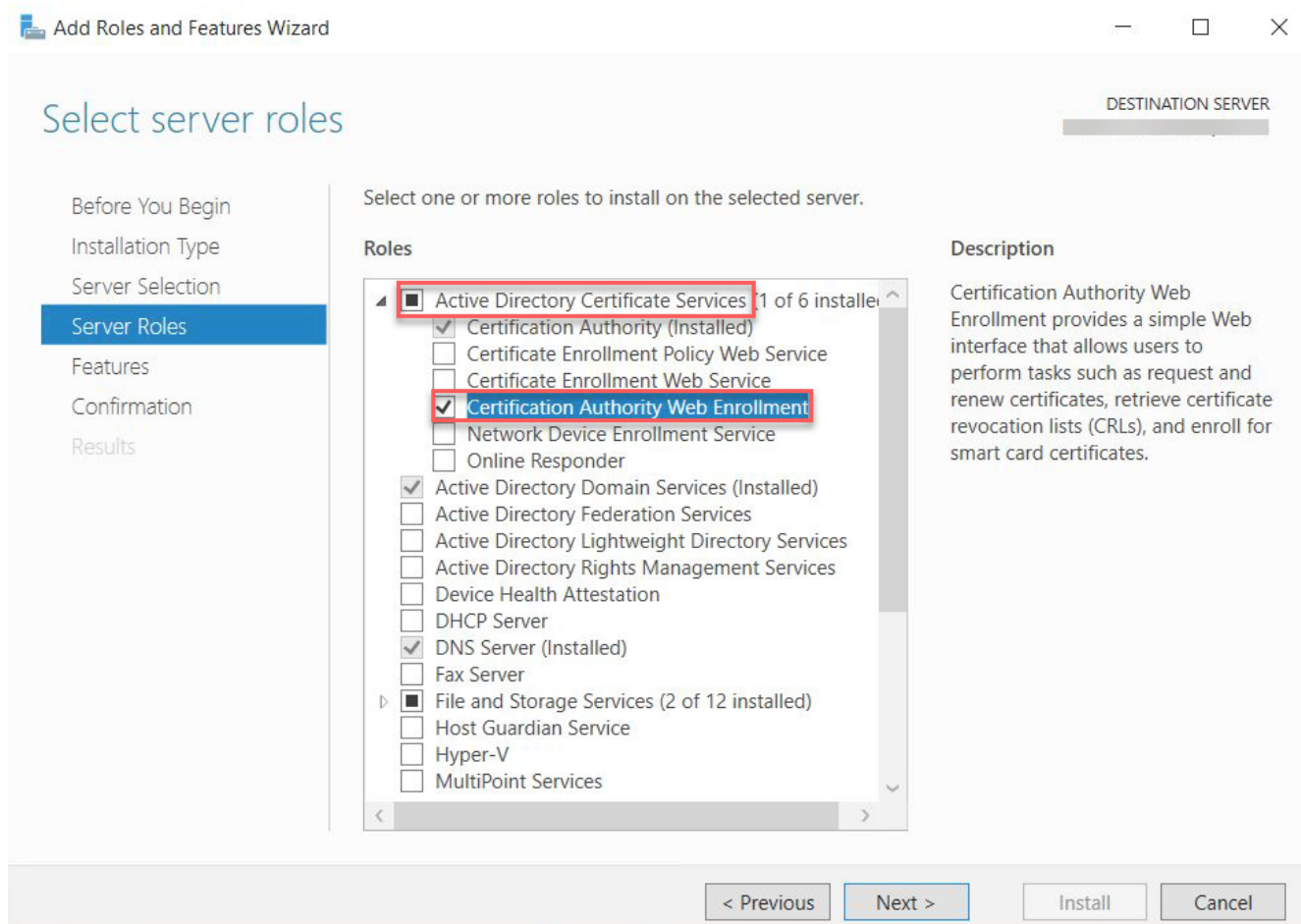


2. Click **Next** on the **Before you begin** window.

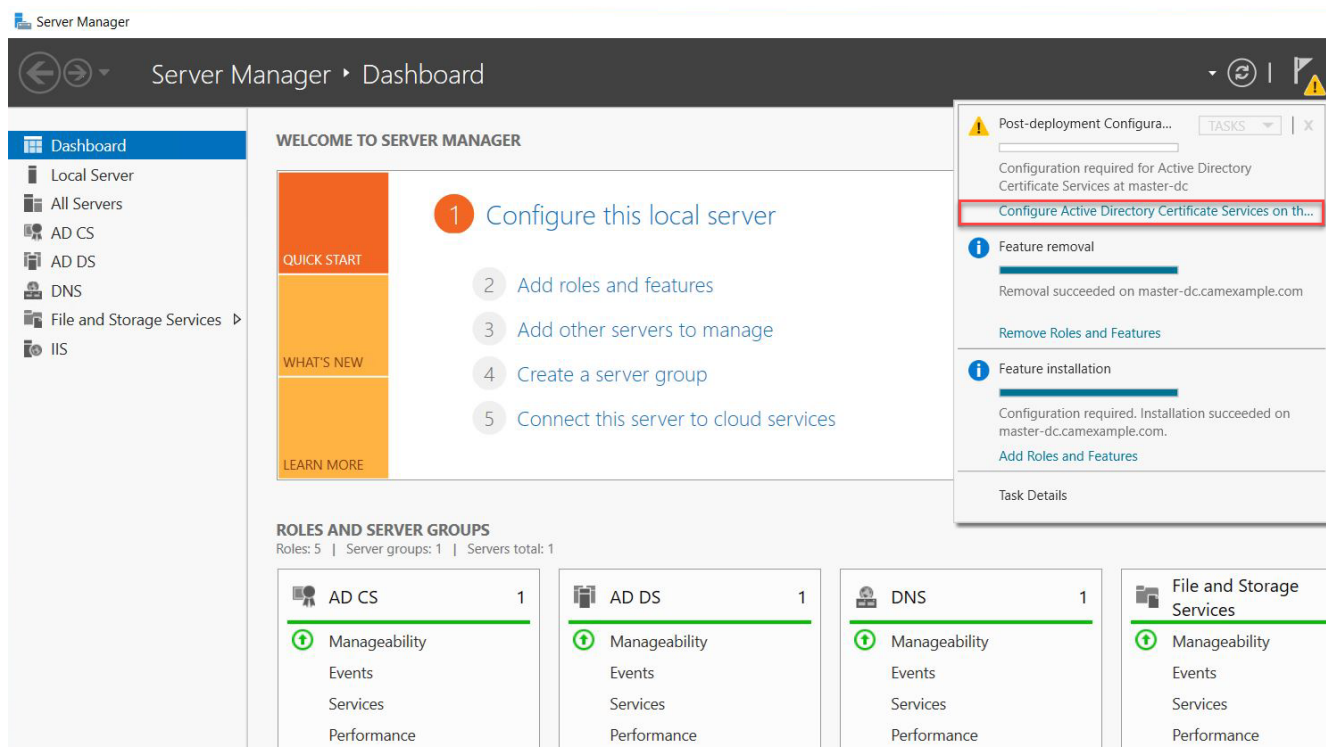
3. Select **Role-based or feature-based installation** on the **Installation Type** page.



4. Select a server from the server pool and press **Next**.
5. On the **Server Roles** page, expand **Active Directory Certificate Services** section, and select **Certificate Authority Web Enrollment**. Click **Next**.

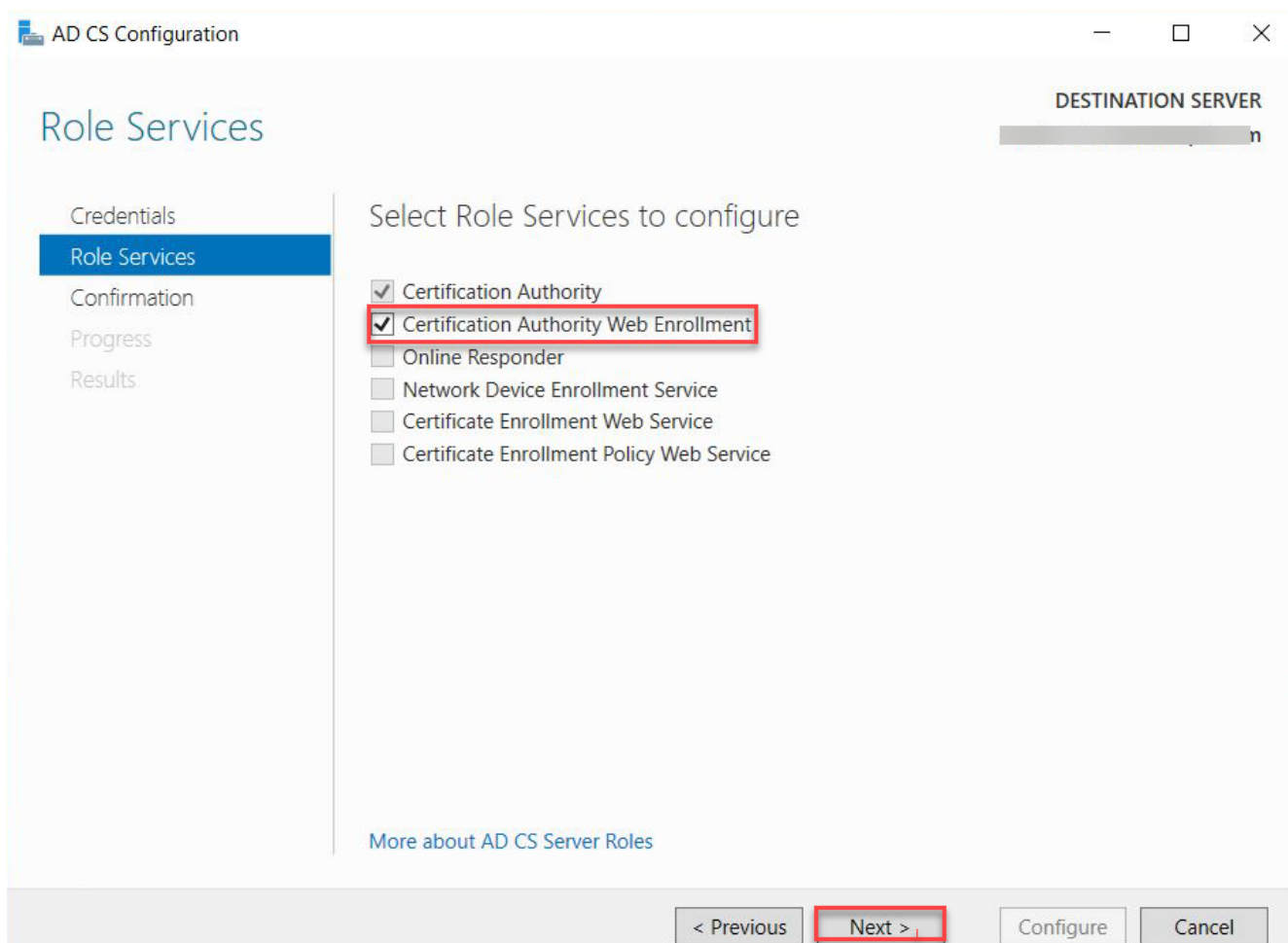


6. On the **Features** page, Click **Next**.
7. On the **Confirmation** page, select **Restart the destination server automatically if required** and press **Install**.
8. After installation, go to the **notification** tab and click **Configure Active Directory Certificate Services**.



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**.



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**

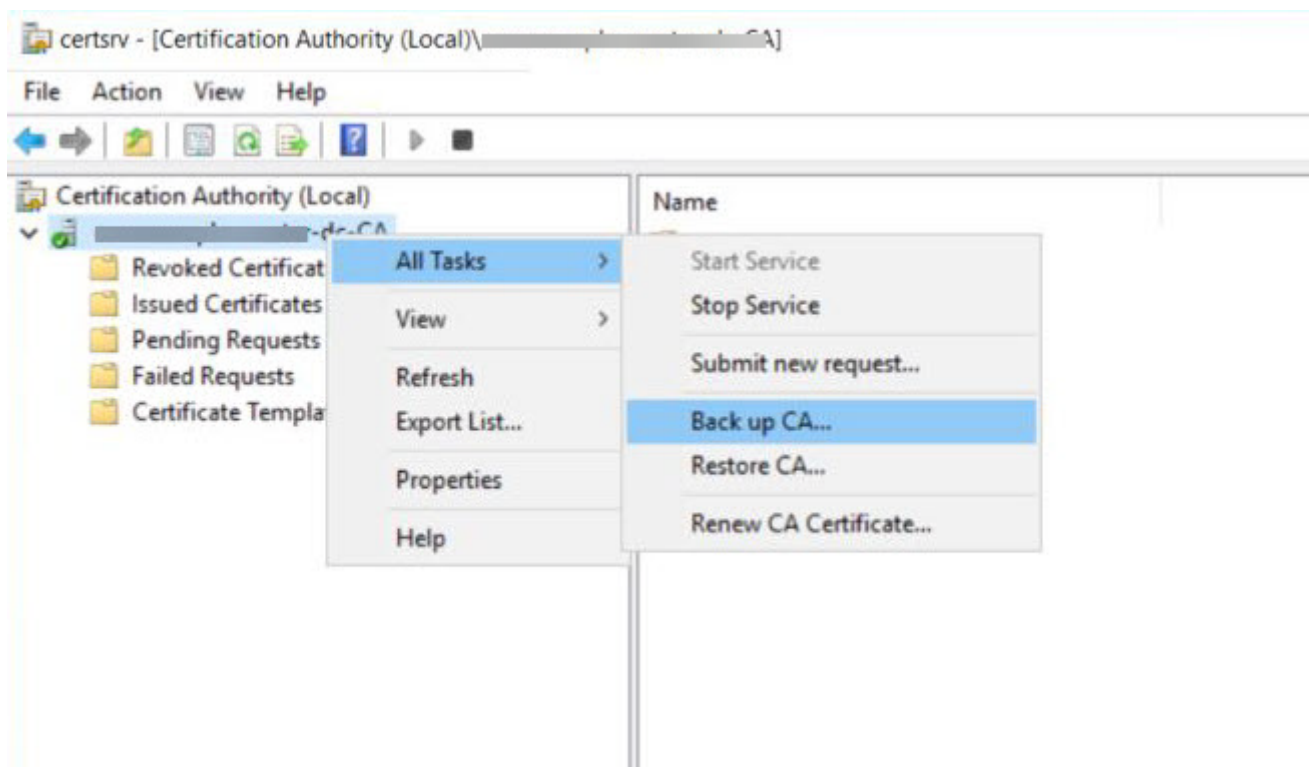
Working with your Certification Authority (CA) you will need to obtain:

- 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)

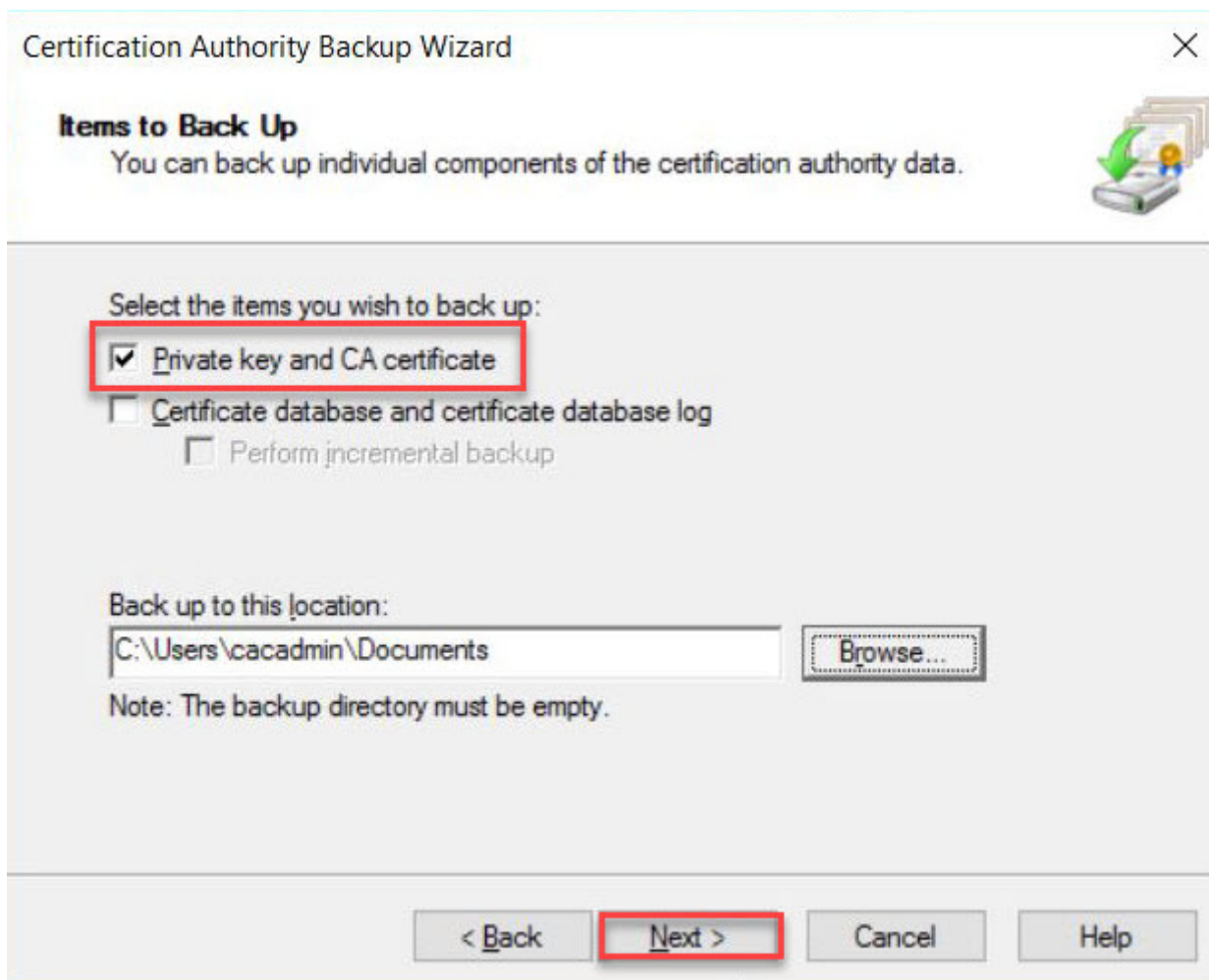
1. Log on to the Certificate Authority resource.
2. Open Certificate Authority MMC (`certsrv.msc`).
3. Right-click the CA in the tree, select **All Tasks** and click **Back up CA....**





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.





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
```

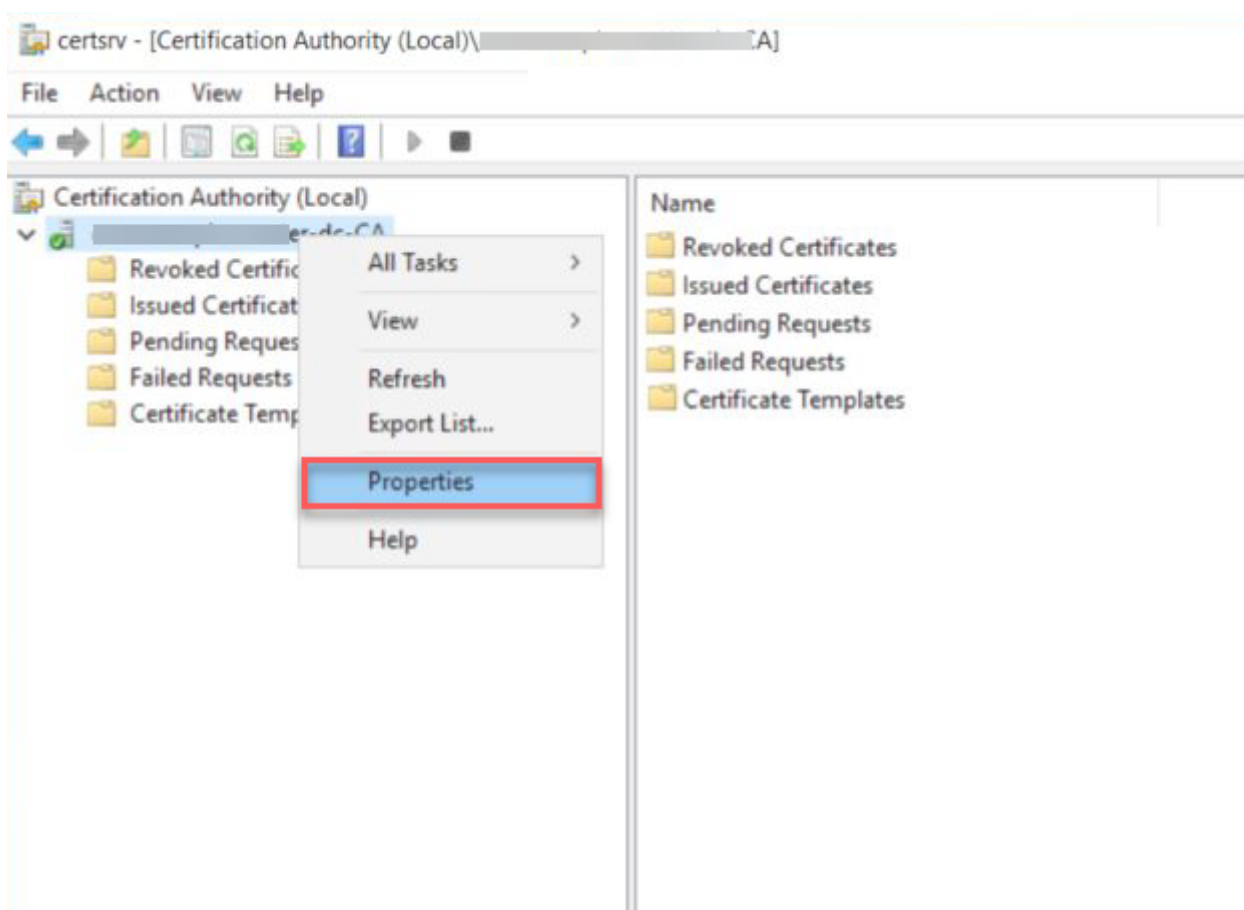
- Extract certificate with `openssl`. Run the following command and enter password when prompted:

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

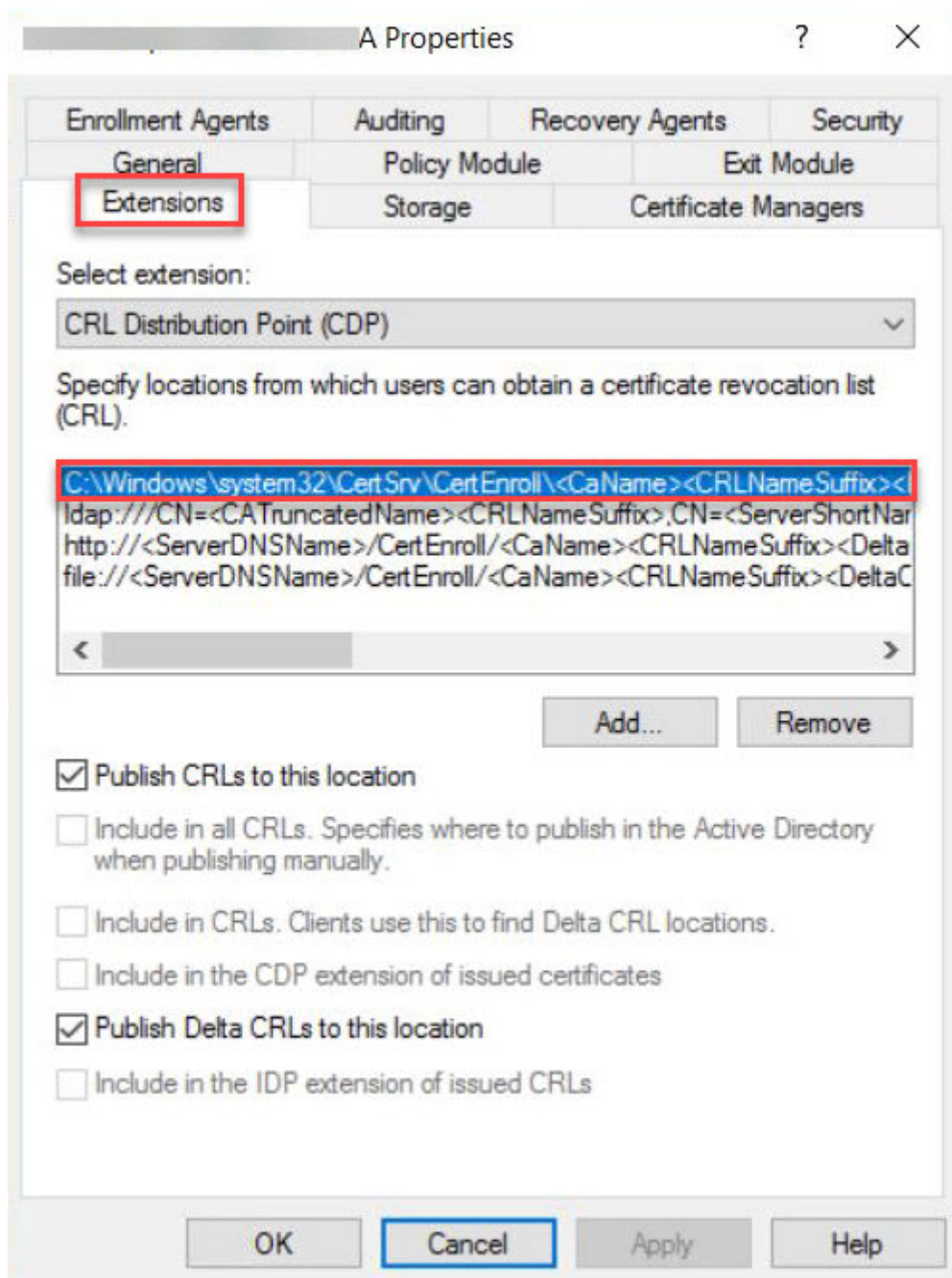
Locate Certificate Revocation List (CRL) file of the Intermediate Windows CA (Microsoft Windows Server 2019 Datacenter)

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`.



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 latest 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. 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:

Dashboard	▼
Directory	▼
Applications	▲
Applications	
Security	▼
Reports	▼
Settings	▼

## Applications

- [Create App Integration](#)
[Browse App Catalog](#)
[Assign Users to App](#)
[More ▼](#)

STATUS			
ACTIVE	5		<a href="#">FedAuthWeb</a> Client ID: Ooa520zsquCiqivN25d7
INACTIVE	0		<a href="#">FuaVelTest</a> Client ID: Ooa5rbzdevJDKEgSr5d7
			<a href="#">My Web App</a> Client ID: Ooa53acrd6phLLKfe5d7
			<a href="#">PCoIP Client</a> Client ID: Ooa52ocg3nulb2VSW5d7
			<a href="#">VelAgentTest</a> Client ID: Ooa56xofiol5xfidw5d7

5. 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):

- For RHEL/Rocky Linux Connector:
  - To configure a new connector after installation or update configuration for an existing Connector:
    - Log into the Connector using SSH.
    - Run the command: `sudo /usr/local/bin/anyware-connector configure --pull-config-from-manager <any other configuration flags you use> --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 ""`.

- For Ubuntu Connector:

- To update:

- 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):

- For RHEL/Rocky Linux Connector:

- To configure a new connector after installation or update configuration for an existing Connector:

- Log into the Connector using SSH.

- Run the command: `sudo /usr/local/bin/anyware-connector configure --pull-config-from-manager <any other configuration flags you use> --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 ""`.

- For Ubuntu Connector:

- To update:

- 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.

**For RHEL/Rocky Linux Connector:**



If you are configuring a new Connector after installation or updating the configuration for an existing Connector:

- **Run this command:** `sudo /usr/local/bin/anyware-connector configure [...other settings...] --enable-oauth true --id-provider-url https://id.provider.com --oauth-client-id XXXXXXXXXX --enable-sso true --sso-signing-csr-ca <path to pem> --sso-signing-csr-key <path to pem> --sso-signing-crl <path to crl>.`

### For Ubuntu Connector:

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 XXXXXXXXXX --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 XXXXXXXXXX --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):

### For RHEL/Rocky Linux Connector:

If you are configuring a new Connector after installation or updating the configuration for an existing Connector:

- **Run this command:** `sudo /usr/local/bin/anyware-connector configure [...other settings...] --enable-oauth true --id-provider-url https://id.provider.com --oauth-client-id XXXXXXXXXX --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".`

### For Ubuntu Connector:

## If you are installing a new Connector:

- Run this command:

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

## 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 XXXXXXXXXX --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 "".
```

## Configuration Flags

Flag	Type	Description
<code>--enable-oauth</code>	Boolean	Enables Oauth authentication. (Default=False)
<code>--id-provider-url</code>	String	Sets the identity provider URL. Example: <code>--id-provider-url https://provider-1234567890.okta.com</code> . This flag is required if <code>--enable-oauth</code> is true.
<code>--oauth-client-id</code>	String	Gets the Client ID from the Identity Provider. This flag is required if <code>--enable-oauth</code> is true.
<code>--fa-url</code>	String	The Federated Auth Broker URL. for example <a href="https://cac-vm-fqdn:port">https://cac-vm-fqdn:port</a>
<code>--oauth-flow-code</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
<code>--enable-entitlements-by-upn</code>	Boolean	Enables/Disables searching entitlements by UPN. This flag is not required for the Anyware Connector. It is supported for the Connector on Ubuntu for versions 164 or below.
<code>--sso-signing-csr-ca</code>	String	Path to copy intermediate CA Certificate.
<code>--sso-signing-csr-key</code>	String	Path to the intermediate key.
<code>--sso-signing-crl</code>	String	Path to a certificate revocation list.
<code>--sso-enrollment-url</code>	String	Gets the URL to the Active Directory Certification Authority Web Enrollment Service.
<code>--sso-enrollment-domain</code>	String	Domain of the user to access Active Directory Certification Authority Web Enrollment Service.
<code>--sso-enrollment-username</code>	String	Username for accessing Active Directory Certification Authority Web Enrollment Service.
<code>--sso-enrollment-password</code>	String	Password for the username to access Active Directory Certification Authority Web Enrollment Service.
<code>--sso-enrollment-certificate-template-name</code>	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 out, or testing it. We recommend you revoke the Intermediate Signed Certificate and Private Key you generated to enable SSO.

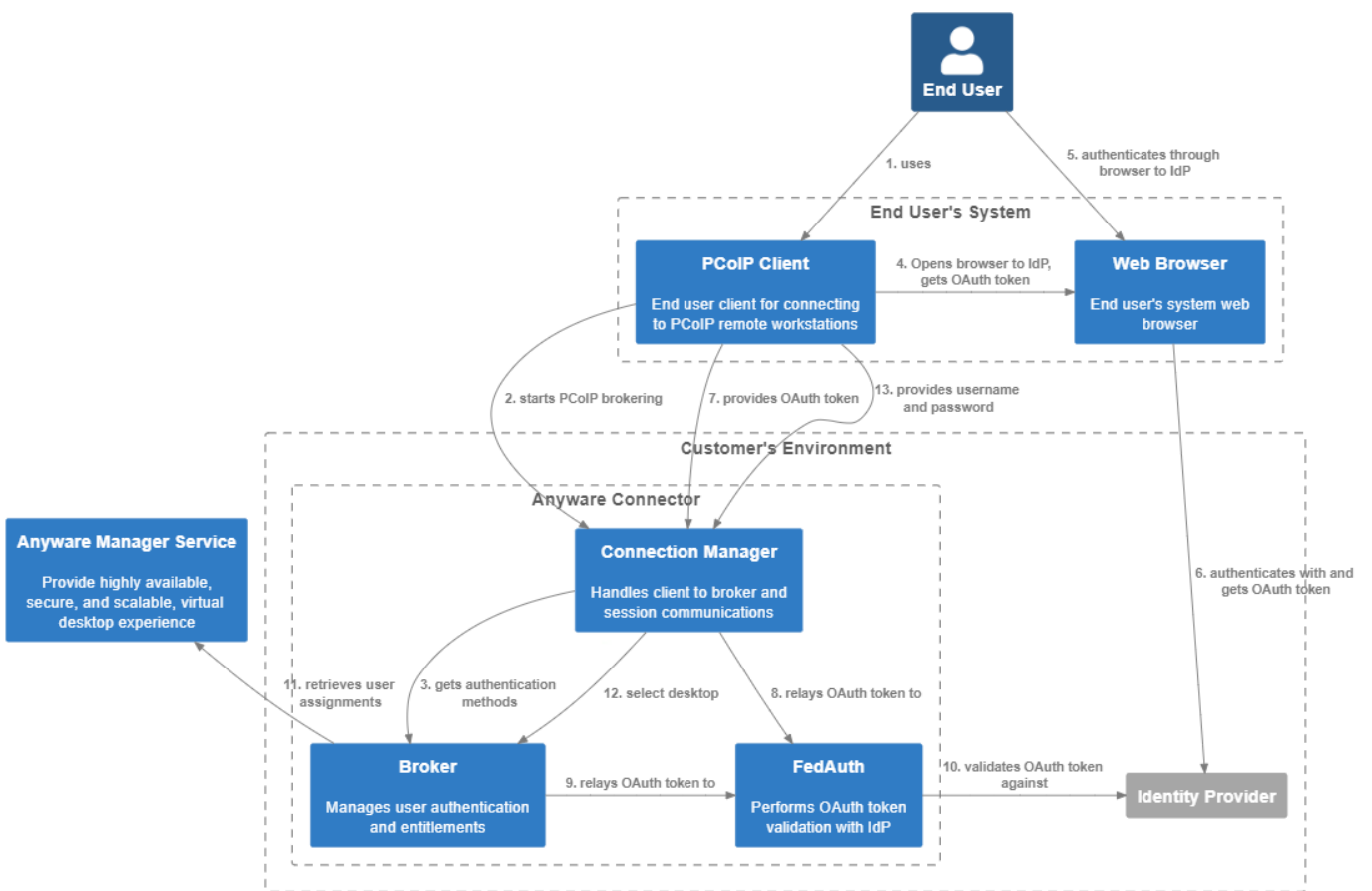
If you had configured this in production Connectors you need to turn off SSO. This can be done using the instructions above from the Admin Console and switching Enable Single Sign-On (SSO) so that it is disabled, or from the command line for each connector using the following command:

- **For Anyware Connector:** `sudo /usr/local/bin/anyware-connector configure [...other settings...] --enable-ss0 false.`
- **For Ubuntu Connector:** `sudo cloud-access-connector update [...other settings...] --enable-ss0 false.`

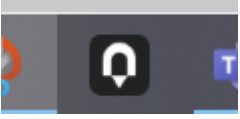
# Federated Authentication Troubleshooting

## Federated Authentication Process Overview

The diagram describes the steps to authenticate to an Anyware Manager Connector and select a desired remote workstation desktop using Federated User Authentication. 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 in the event of a failure.



## AUTHENTICATION PROCESS

Step	Visual
1	
2	

**Step****Visual**

# Saved connections

To begin, select a connection.

3



**Step****Visual**

# Saved connections

To begin, select a connection.





Step	Visual
4	

Step	Visual

dev- ██████████ okta.com

## Connecting to

Sign in with your ██████████996 account to access PColP Client



### Sign In

Username

Password


Keep me signed in

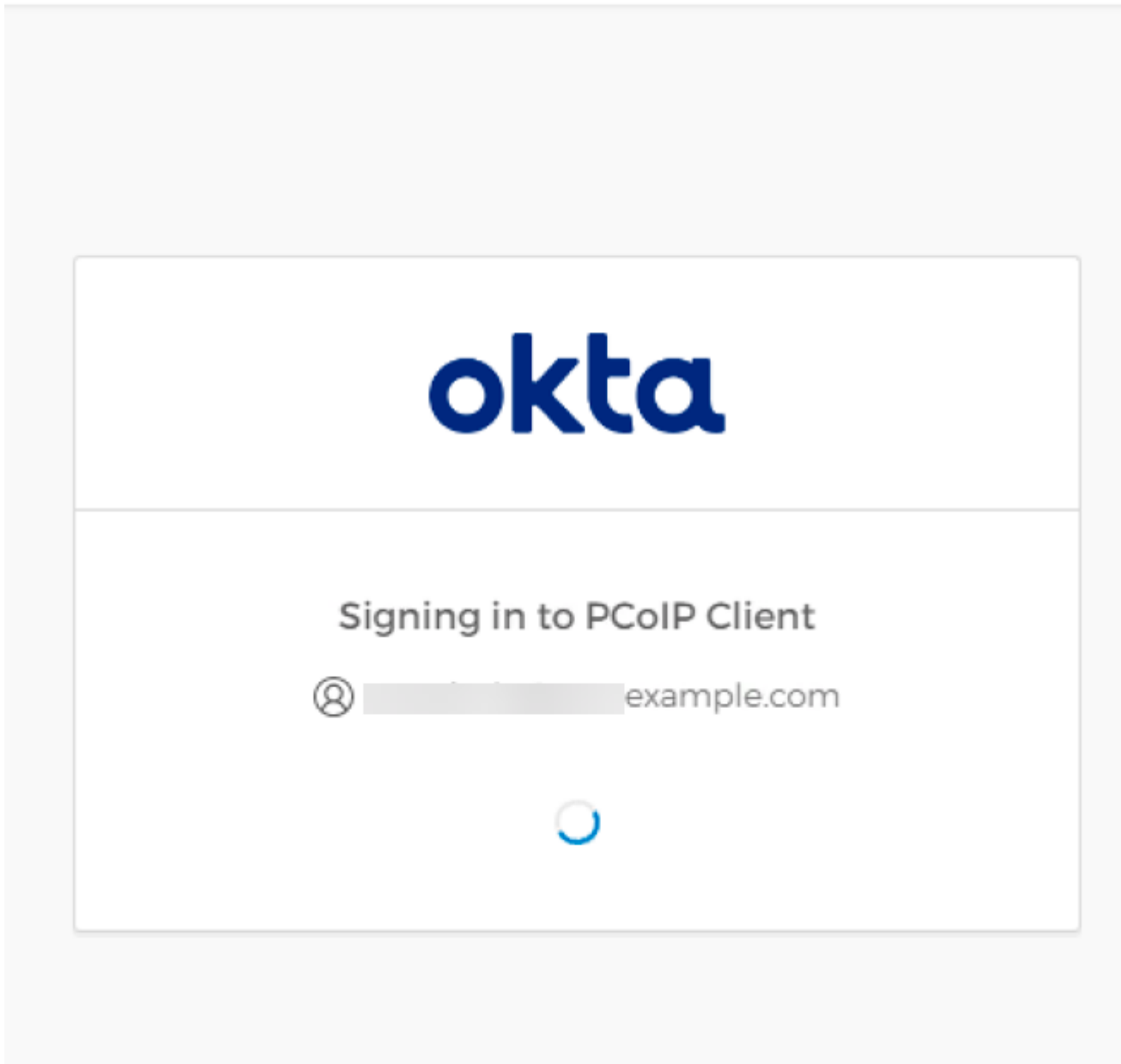
Sign In

[Forgot password?](#)

[Help](#)

Step	Visual
------	--------

Connecting to   
Sign in with your okta- account to access PCoIP Client



5	NA
---	----

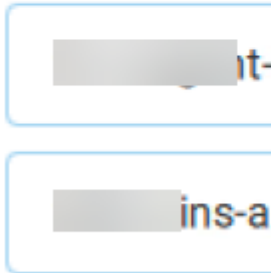
Step	Visual
6	



Step	Visual
------	--------

# Desktop selection

Federated Auth with Okta



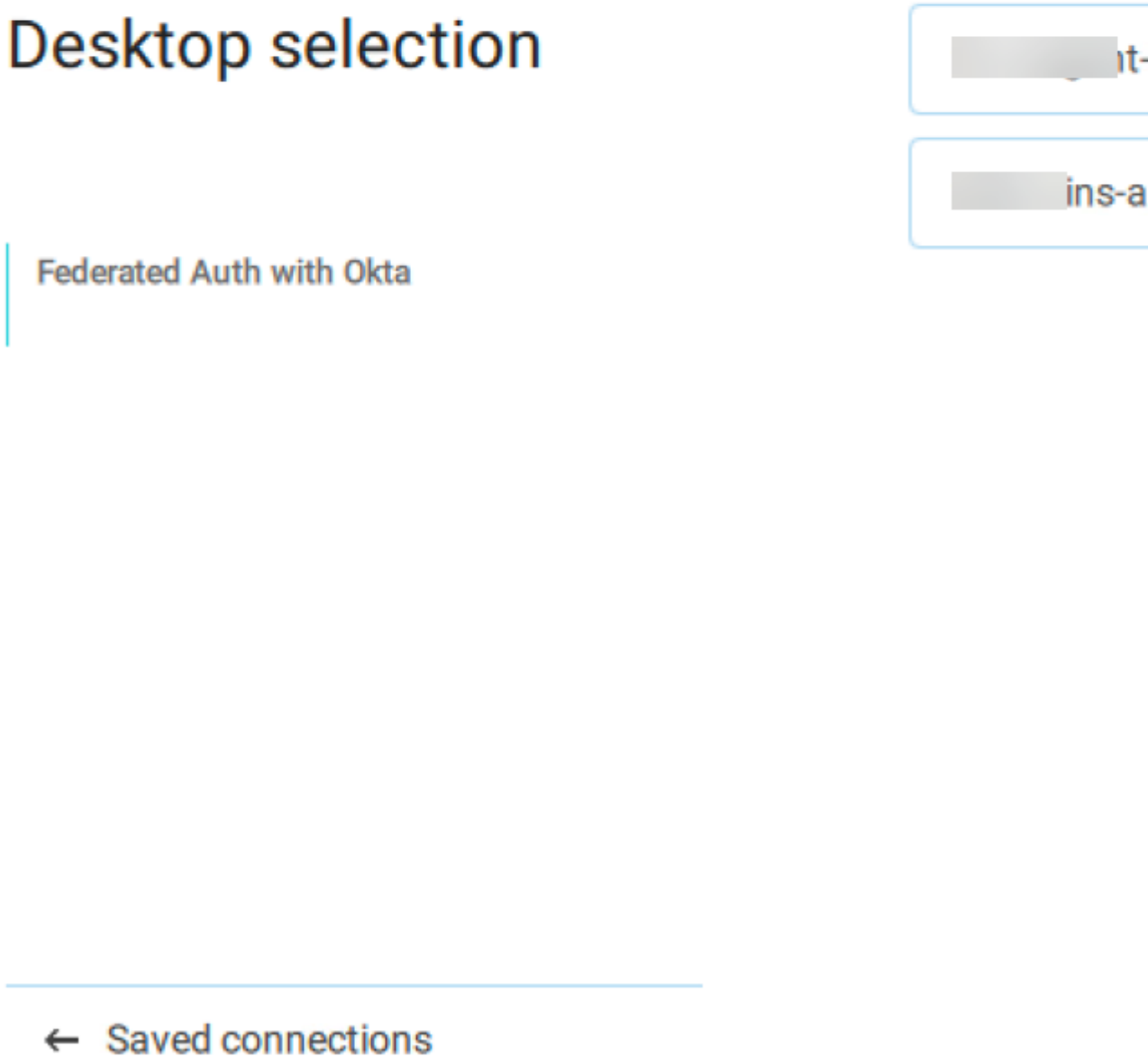
---

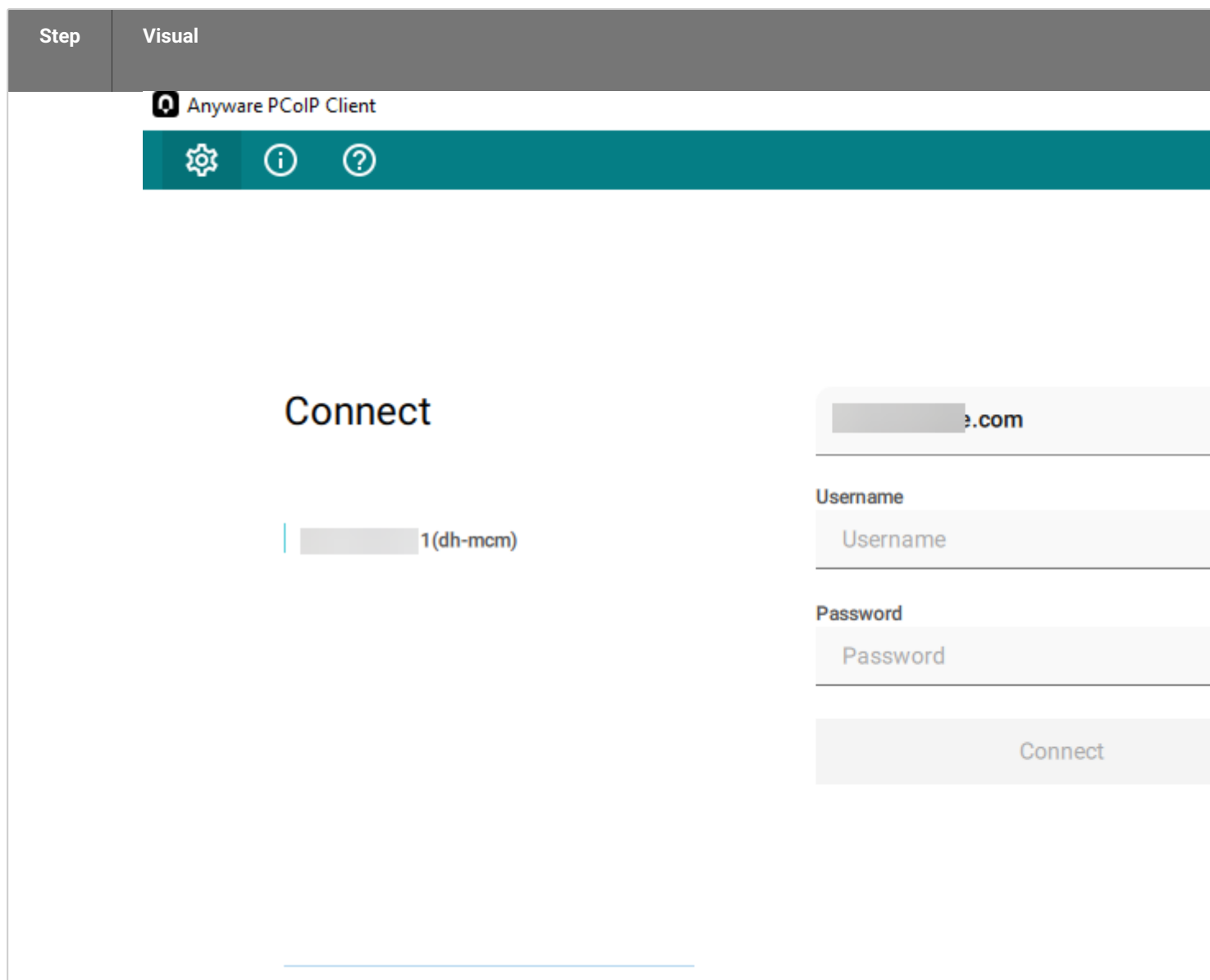
← Saved connections

Step	Visual





Step	Visual
7	 <p>Desktop selection</p> <p>Federated Auth with Okta</p> <p>it-</p> <p>ins-a</p> <p>← Saved connections</p>
8	



## 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/](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/](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/](https://www.teradici.com/web-help/pcoip_client/mac/current/support/logs/)

**• Connector**

- Anyware Connector Log Collection - [Anyware Manager as a Service](#)

**• 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 Authentication Broker:**

- client inside the corporate network: `sudo docker service logs connector_brokerinternal`
- client outside the corporate network: `sudo docker service logs connector_brokerexternal`

**• Federated Authentication Service:**

- `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/](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/](https://www.teradici.com/web-help/pcoip_agent/graphics_agent/windows/current/admin-guide/diagnostics/locating-log-files/)

# 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 will be 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 will now be 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 will show the date, user account, source and activity details.

You can search for logs based on specific operations that occurred. 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 HP 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://cas.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.

# Beta Features

## Overview

This section outlines beta features and enhancements that have not yet been pushed to the production version of the Anyware Manager Admin Console. As a result, these features may change as they are developed, and they are not supported by HP Global Support Services. Features in the beta version are considered not yet ready for full production and you use them at your own risk.

The following beta features for the Anyware Manager Admin Console are currently documented:

- [Azure Remote Workstation Provisioning](#)
- [Anyware Manager Configures Connector](#)
- [Anyware Connector New Installation Wizard](#)
- [Anyware Monitor](#)

Once these features have been fully developed and moved to the production version of the Anyware Manager Admin Console, they are removed from this section and added to the main Administrators' guide.

## Azure Remote Workstation Provisioning

### ⚠ Beta Feature

Please be aware that the feature outlined below is only currently available in the beta version of the Anyware Manager Admin Console. As such, this feature may change as it is developed, and it will not be supported by HP Global Support Services. Features in the beta version are considered not yet ready for full production and you use them at your own risk.

### ✎ Pre-Defined Images and Templates

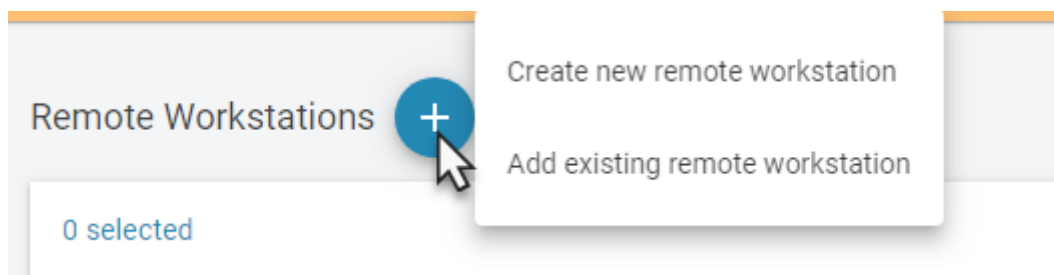
If you wish to use your own custom images or templates, you must create and manage those outside of Anyware Manager and create your remote workstation outside of Anyware Manager also. Once you have created a remote workstation you can add it to your deployment in Anyware Manager for brokering and management.

Users are now able to create and provision remote workstations in Azure in the beta version of the Admin Console. This beta feature is currently only supported with Anyware Manager as a Service. This feature is currently at parity with GCP in terms of creating a remote workstation, add a remote workstation to a pool, entitling users to a pool, etc.

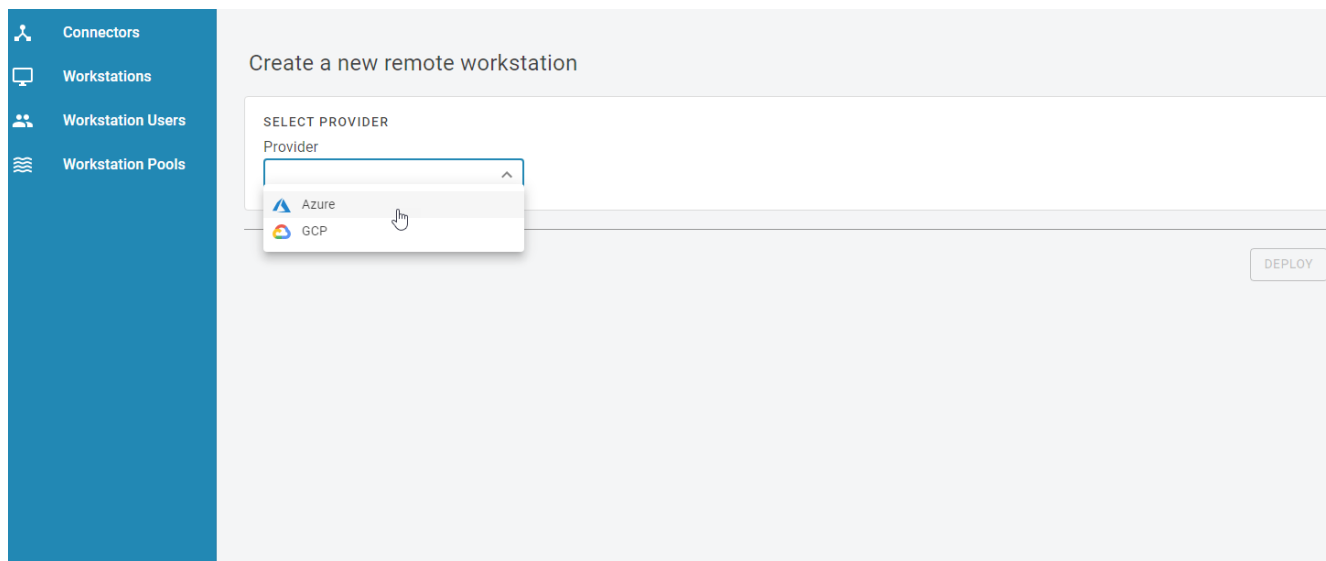
For information on which Provider Service accounts can perform certain features, please consult the [Service Account Requirements](#) section.

You must have a valid Provider 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.



### 3. Select **Azure** from the Provider menu.



4. Select an existing Connector from the Connector Information menu.
5. Select a remote workstation template from the Workstation Template menu.
6. Enter the provider properties for the Azure resource group, remote workstation location, Azure virtual network and Machine subnet.

#### **⚠ Remote Workstation Location**

The location of the remote workstation must match the location of the Azure resource group.

7. Enter the remote workstation properties from the Workstation Properties menu. Enter the machine name, Azure VM size, remote workstation username and remote workstation admin password, as

outlined below.

### Create a new remote workstation

**SELECT PROVIDER**  
Provider  
Azure

**CONNECTOR INFORMATION**  
Select a connector  
test connector

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

**PROVIDER PROPERTIES**  
Select the location of the remote workstation  
(US) West US

Azure resource group  
cloud-shell-storage-westus (westus)

Azure Virtual Network  
Select Virtual Network

Machine Subnet  
Virtual network required

**WORKSTATION PROPERTIES**  
Machine name  
TEST1

Select the size of the machine  
Basic\_A1 [How to avoid building a weak machine?](#)

Remote Workstation username  
testytest

Remote workstation admin password  
.....

#### Remote Workstation machine and user names

Due to a Windows limitation, remote workstation machine names are limited to only characters, letters, hyphens and must be 15 characters or less. Remote workstation user names are limited to 20 characters or less and cannot end in a period. The password entered for a remote workstation must be between 6-72 characters long and satisfy at least 3 of the following password requirements:

- Contains an uppercase character.
- Contains a lowercase character.
- Contains a numeric digit.
- Contains a special character.
- Control characters are not allowed.

For information on the remote workstation name and password requirements for Azure, see the following FAQs:

- [Windows Requirements](#)
- [Linux Requirements](#)

### Machine Type GPU


If you select a Graphics Agent from the remote workstation template, you must ensure that your machine type has an NVIDIA GPU. If the remote workstation does not have the correct GPU driver it will fail during the GPU driver installation phase and you will be unable to connect to your remote workstation.

8. Enter the active directory information for the remote workstation. The service account must have permission to join computers to the domain.

### Active Directory Information

Active Directory information is used only during provisioning to join the remote workstation to the domain. This information will not be saved by the Anyware Manager.

#### ACTIVE DIRECTORY INFORMATION

Domain service account 

The service account must have permission to join computers to the domain.

Service account password

**Active Directory information** is used only during provisioning to join the remote workstation to the domain. **It will not be saved by the CAS Manager.**

9. Click **Deploy**.

## Anyware Manager Configures Connector

When installing the Connector you are required to provide several command line parameters. This is a requirement for every Connector you want to install in a deployment. To avoid this redundant activity and enhance user experience, Anyware Manager allows you to save the Connector configuration and use them as-is for configuring another Connector. This functionality is termed as **Anyware Manager Configures Connector**. After configuring the first Connector in your deployment, the configuration details are saved and re-used if necessary for future Connector installations.

### Feature Compatibility

The Anyware Manager Configures Connector is a critical feature in the HP Anyware Manager software and the minimum supported versions for this feature are Anyware Manager 22.09 and the Connector v136. If a version of the Anyware Manager is not able to support this feature functionality, it throws a warning message during installation as an indication that pulling the Connector settings and pushing them into a new Connector is not supported. This feature is currently supported in the Beta mode of the Admin Console. Features in this mode are still being worked on and refined by HP.

### How to use Anyware Manager Configures Connector?

When the first Connector is configured, you need to save and push these settings for future use in the Anyware Manager. These saved settings are pulled later when configuring another instance of the Connector.

To save or push the Connector settings into the Anyware Manager use the following flag along with the install or update command:

```
--push-connector-config
```

To retrieve or pull the Connector settings from the Anyware Manager use the following flag along with the install or update command:

```
--pull-connector-config
```

## What Information is Stored in the Anyware Manager?

Anyware Manager stores the Connector configuration information on two levels. Deployment level and Connector level.

### Information Stored in the Anyware Manager on Deployment Level

Settings	Description
Computer's Domain Name	The base Domain Name to search for computers within the Active Directory. Specify multiple Domain Names with multiple options.
Computers Filter	The filter to search for computers within the Active Directory. Specify multiple filters with multiple options. Default computer filter (&(primaryGroupID=515)(objectCategory=computer))
User's Domain Name	The base Domain Name to search for users within the Active Directory. Specify multiple Domain Names with multiple options.
Users Filter	The filter to search for users within the Active Directory. Specify multiple filters with multiple options. Default user filter (&(objectCategory=person)(objectClass=user))
Domain Name	The Active Directory domain that remote workstations should be joined to.
IDAP CA Certificates	PEM formatted file containing any custom Certificate Authority's public certificate to be used for verifying LDAPs connections to Active Directory. An empty string will clear the setting.
Pools Group	The Domain Name for the Active Directory domain group that manages users and remote workstations in the Management interface.
Sync Interval	The interval (in minutes) for how often to sync the Active Directory users and computers with Anyware Manager Service.

When this information is saved for the first Connector in the deployment it can be re-used by any new connector in the same deployment.



## Information Stored in the Anyware Manager on Connector Level

Settings	Description
Accept Policies	Automatically accept the EULA and Privacy Policy
Connector Network CIDR	The CIDR to use for the Connector's docker network.
Domain Controllers	Domain controller FQDN to use. May be specified multiple times for more than one DC.
External Client CIDR	The CIDR for PCoIP Clients that connect to workstations through the Security Gateway.
Internal Client CIDR	The CIDR for PCoIP Clients that connect to workstations directly.
Https Proxy	URL for an HTTPS proxy (overrides related proxy settings in environment variables).
IP	Sets the IPv4 address for the Connector for external connections.
License Server URL	URL for HP PCoIP License Server to be used for PCoIP Sessions. If this is not provided, ensure that the Cloud License Server is registered on the PCoIP Agent.
MFA Enable	Enable MFA/2FA.
MFA Server	The FQDN or IP address of the RADIUS server to use for MFA.
Preferred Name	A Setting used to determine if a hostname or machine name should be displayed to identify the workstations.
Retrieve Agent State	Enable/disable retrieving PCoIP agent state.
Show Agent State	Show/hide PCoIP agent state (showing requires retrieve-agent-state to be true).
Service Account Username	The username for the AD account with permission to join machines to the domain.
Ingress TLS Certificate	Ingress TLS Certificate.
Self Signed	Automatically generate self-signed SSL cert and key for testing purposes.

These settings can be used only by the Connector.

## Creating a New Connector Using the Saved Configuration from another Connector

When setting up a new Connector, the user can use the clone feature to copy the setting from one Connector to another connector.

The procedure is as follows:

1. Log in to the **Admin Console**, and enable the Beta UI toggle.
2. Navigate to the **Connectors** tab and click "+" icon to create a new Connector.
3. Provide the new Connector name and select the Connector you wish to copy settings from in the **Copy connector configuration from** dropdown list.
4. Click **Generate** to generate a Connector token.
5. Install the Connector with the token and include the `--pull-connector-config` flag in the install command.

The new Connector is configured with the settings from the another Connector.

# Anyware Connector New Installation Wizard

You can install, deploy, and configure Anyware Connector using the new Installation Wizard.

## Beta Feature

Please be aware that the feature outlined below is only currently available in the beta version of the Anyware Manager Admin Console. As such, this feature may change as it is developed, and it is not supported by HP Global Support Services. Features in the beta version are considered not yet ready for full production and you use them at your own risk.

## PREREQUISITES

To use the new installation wizard functionality, you must meet the following criteria:

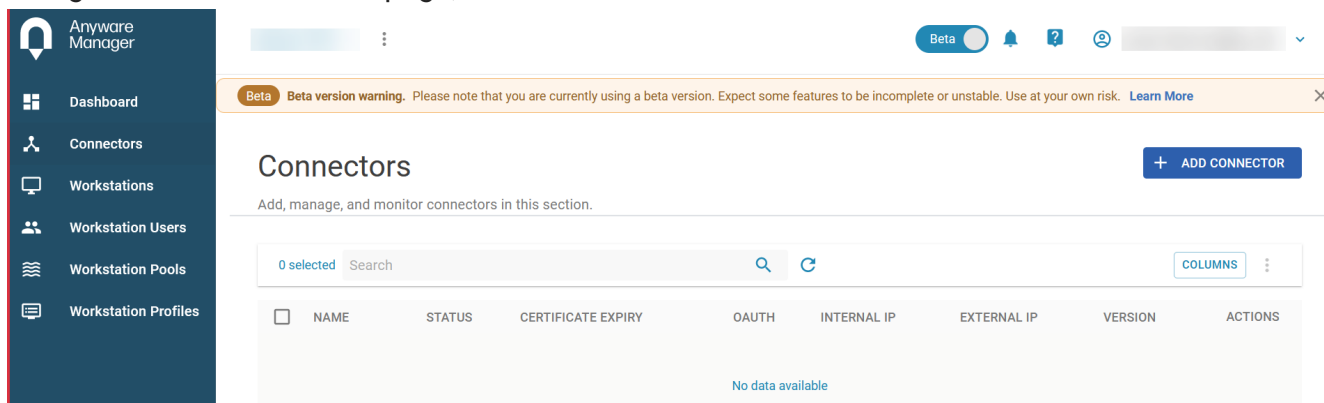
- A Linux based machine (physical or virtual) to install the Anyware Connector on - Rocky or RHEL distributions are supported. For more information, see [Prerequisites for Anyware Connector](#).
  - The machine should be able to communicate with both your domain and Anyware Manager. For more information, see [DNS Name Resolution Configuration on RHEL/Rocky Linux](#).
  - You must be able to access the machine's terminal (e.g: SSH).

## CREATING A NEW CONNECTOR

To begin using the Installation Wizard:

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. Navigate to the **Connectors** page, and click **Create Connector**.



The screenshot shows the Anyware Manager interface. On the left is a dark blue sidebar with the Anyware Manager logo and navigation links: Dashboard, Connectors, Workstations, Workstation Users, Workstation Pools, and Workstation Profiles. The main area is titled 'Connectors' and features a '+ ADD CONNECTOR' button. Below this is a table with columns: NAME, STATUS, CERTIFICATE EXPIRY, OAUTH, INTERNAL IP, EXTERNAL IP, VERSION, and ACTIONS. The table is currently empty, showing '0 selected' and 'No data available'.

### 4. Follow the instructions in the Pre-Installation Checklist in order to prepare your Linux machine for the Connector. For your convenience, you can press **Copy ALL Commands**, and paste the copied command into the Connector terminal in order to prepare your machine.

#### Pre-installation Checklist

##### Linux machine requirements

Before adding a new Connector to your Anyware Manager deployment, ensure you have the following prerequisites:

- A Linux based machine (physical or virtual) - Rocky or RHEL distributions are supported. [Learn more about supported distributions.](#)
- The machine must be able to communicate with both your domain and Anyware Manager. [Learn more about DNS requirements.](#)
- Administrator can access the machine (eg, SSH or terminal).

##### Note

You will need this machine to run the generated installation command at a later stage.

##### Commands to run

After preparing your Linux machine, execute these commands on the machine to install the necessary components and set up the required configurations. You can copy all commands at once or can select each command.

**COPY ALL COMMANDS**

### 5. Click **Generate Installation Command**.

### 6. Enter all the required information for the new Connector.

### 7. An installation command is generated. Click **Copy** to copy the installation command and paste it into your workstation.

A new Connector is installed and configured.

## CONFIGURING AN EXISTING CONNECTOR

To configure an existing connector using the Installation Wizard:

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. Navigate to the **Connectors** page, and select an existing Connector.
4. Using the tabs in this page, select the configuration section you want to change.
5. Enter the configuration details in the fields, and then copy the configuration command to the clipboard.
6. Paste the command on your workstation to execute the configuration.

The Connector is now configured.

### Example Configuration for Anyware Connector

An example configuration of a Connector used for a proof of concept could be as follows:

```
Connector name: <Enter a name>
Domain name: <Enter a name>
Active Directory settings:
  Integration Method: LDAP
  Active Directory Sync: Disabled
MFA: Disabled
```

### Example Anyware Connector Configuration for Production

An example configuration of a Connector used for a production environment could be as follows:

```
Connector name: <Enter a name>
Domain name: <Enter a name>
Active Directory settings:
  Integration Method: LDAPS
  Active Directory Sync: Enabled
  Active Directory Service Account Credentials: <Enter account
credentials>
  Active Directory Filters: Blank (defaults).
MFA: Enabled
```

## ASSIGN USER TO WORKSTATIONS BY UPN

You can assign a user to a workstation to start a PCoIP session without having to use the Active Directory Sync by using a UPN (User Principal Name).

A UPN is usually their email address in their domain (e.g. [abc@hp.com](mailto:abc@hp.com))

To map user to a workstation:

1. Navigate to <https://cas.teradici.com> and open the web console.
2. Navigate to the **Workstations** page and select the workstation you want to assign a user.
3. Go to the **User Management** tab, enter the UPN of the user in the search bar and select **Entitle UPN** in the search results.
4. Select **Add** to add a user assignment.

A user is assigned to the workstation.

# Anyware Monitor

## Using Anyware Monitor

### Beta Feature

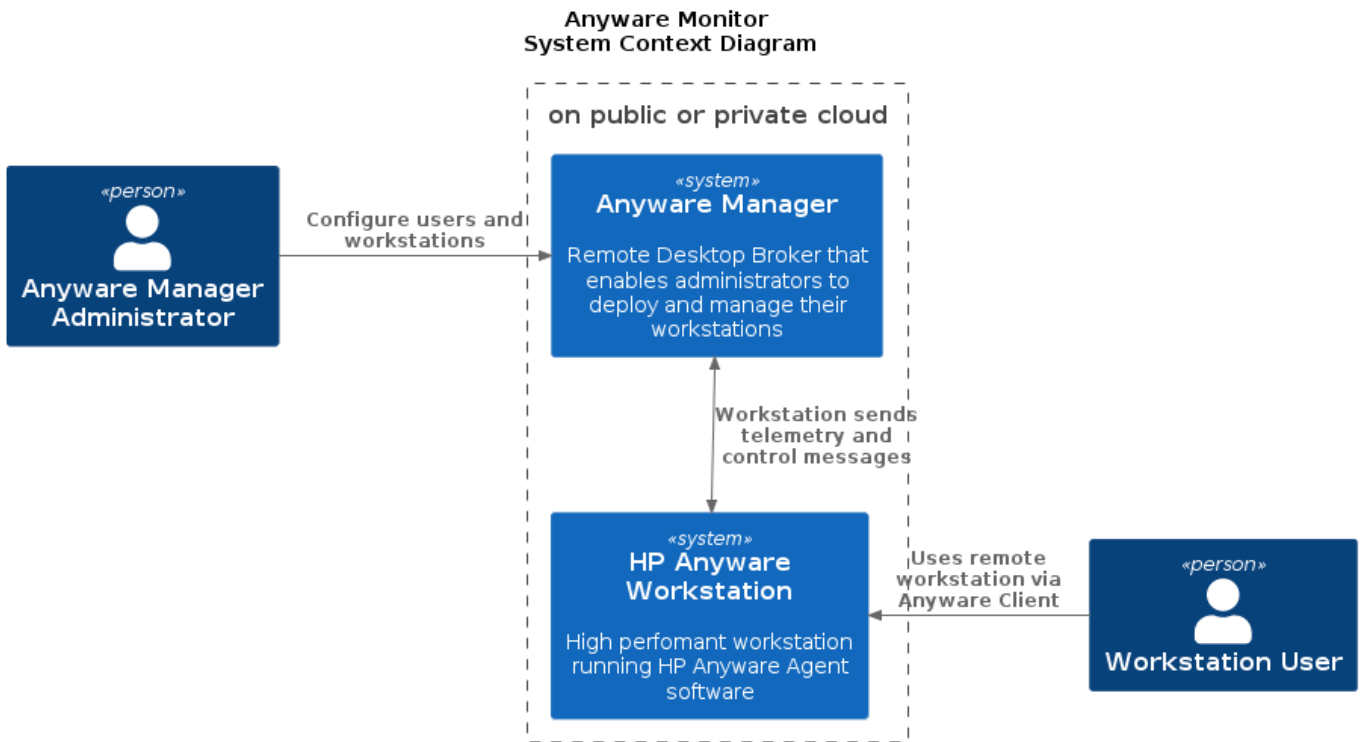
Please be aware that the feature outlined below is only currently available in the beta version of the Anyware Manager Admin Console. As such, this feature may change as it is developed, and it is not be supported by HP Global Support Services. Features in the beta version are considered not yet ready for full production and you use them at your own risk.

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.

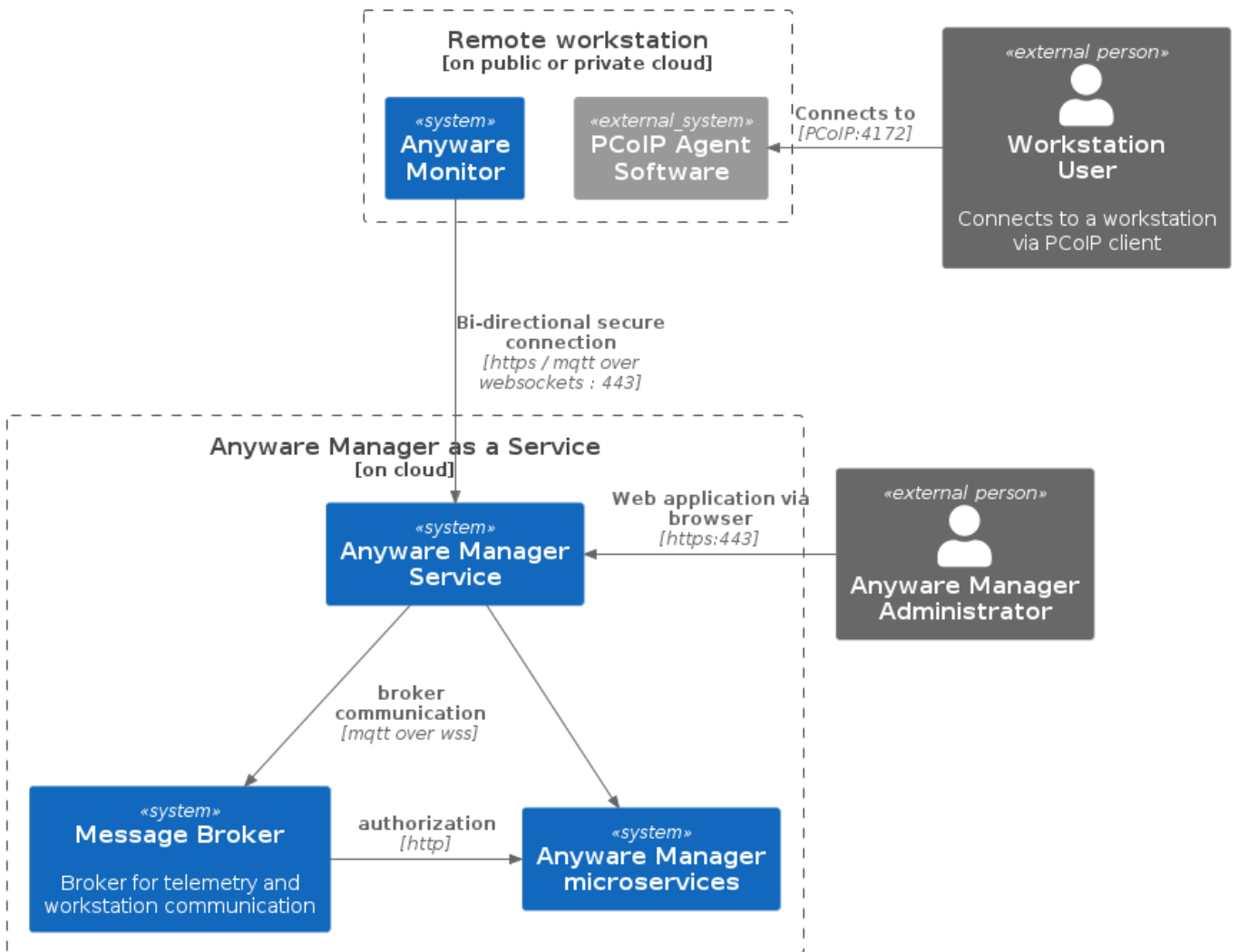


### Anyware Monitor Container Diagram

The following diagram depicts the various components and the role of Anyware Monitor in the HP Anyware architecture.



**Anyware Monitor Container Diagram**



**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.

OVERVIEW	USER MANAGEMENT	ANYWARE MONITOR	SESSION INFORMATION
<b>WORKSTATION INFORMATION</b>			
Workstation ID 64b9458803cf64ed1c893285	Created On Jul 20, 2023 11:32 AM -03	Last modified on Jul 20, 2023 11:32 AM -03	
Anyware Monitor Version 23.08.0	Anyware Monitor Connection <b>Healthy</b>		

OVERVIEW


USER MANAGEMENT

ANYWARE MONITOR

SESSION INFORMATION

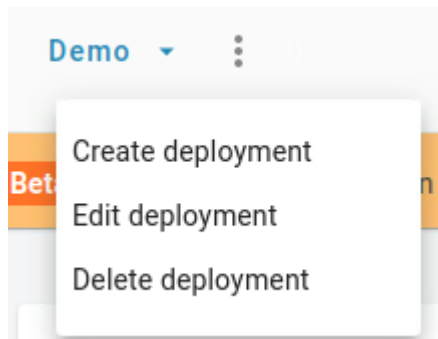
**ANYWARE MANAGER MONITOR CONFIGURATION**Version  
23.08.0Connection  
HealthyLast Connection  
Jul 31, 2023 10:15:58 AM -03

Enabling this feature allows Anyware Manager 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 **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.

OVERVIEW

USER MANAGEMENT

ANYWARE MONITOR

SESSION INFORMATION

**ANYWARE MANAGER MONITOR CONFIGURATION**Version  
23.08.0Connection  
HealthyLast Connection  
Jul 31, 2023 10:15:58 AM -03

Enabling this feature allows Anyware Manager 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.

!!! Note "The session state in the Session column in the Remote Workstations table can be viewed by hovering over the username".

**Log Users 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 the 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 Off**

This action only logs out users that are logged into a desktop session and 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.

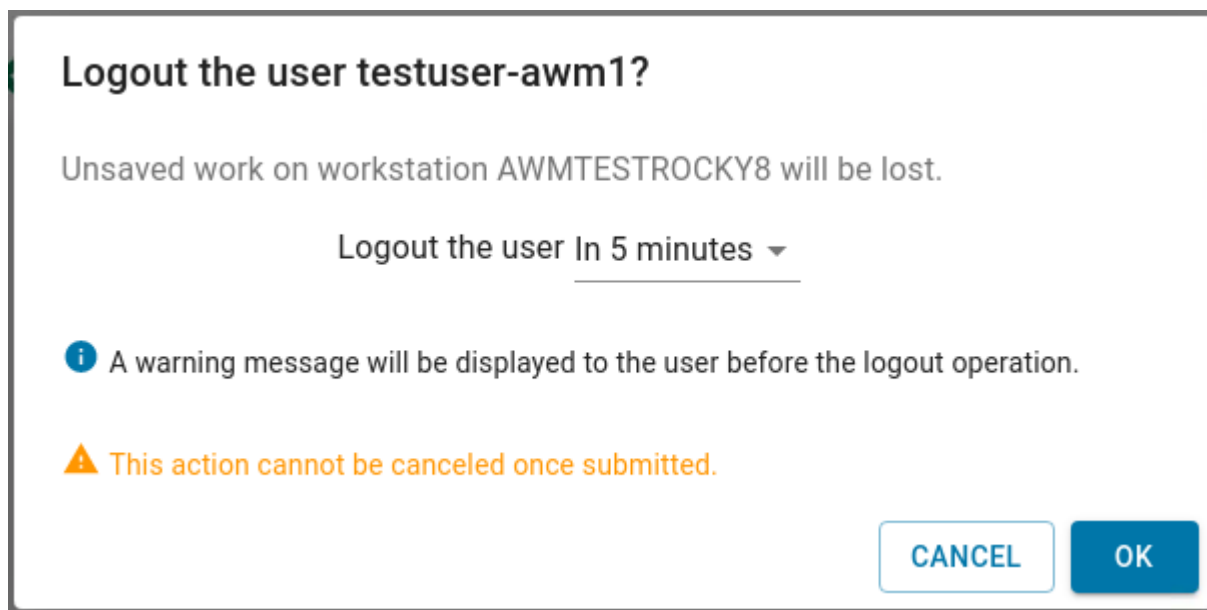
Admin manually log out user in a session

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 in session of the selected workstation.

Select a timespan in which to log out the user and confirm the action.



**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

OVERVIEW	USER MANAGEMENT	ANYWARE MONITOR	SESSION INFORMATION
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			

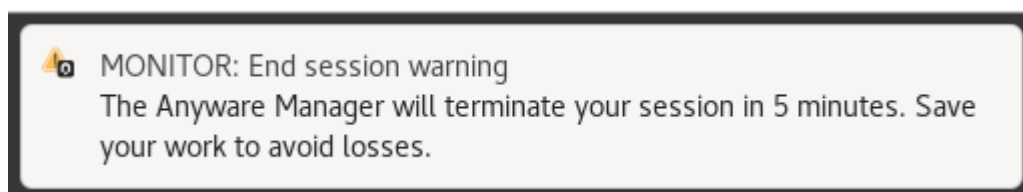
- **Session** column of the **Remote Workstations** table shows the logout time upon hovering over the username

SESSION		ACTIONS
 testuser-awm1	 Ending Session scheduled for 11:00 AM	

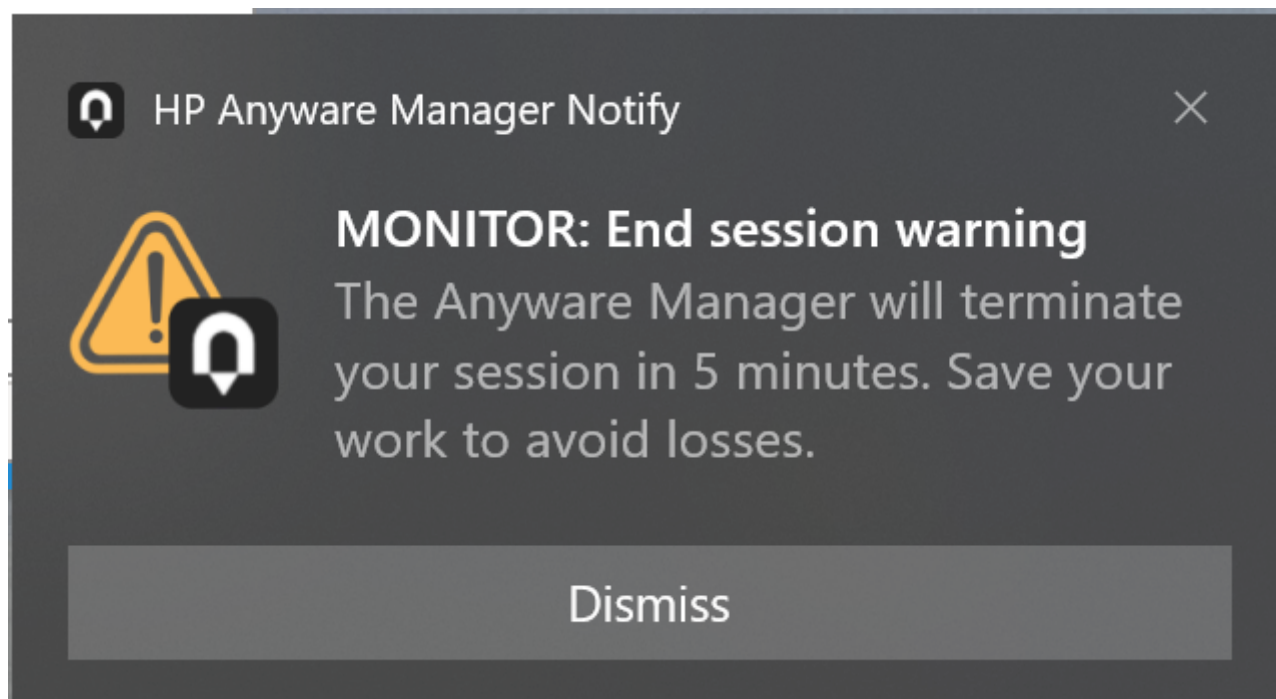
Rows per page: 15 ▾ 1-1 of 1 < >

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

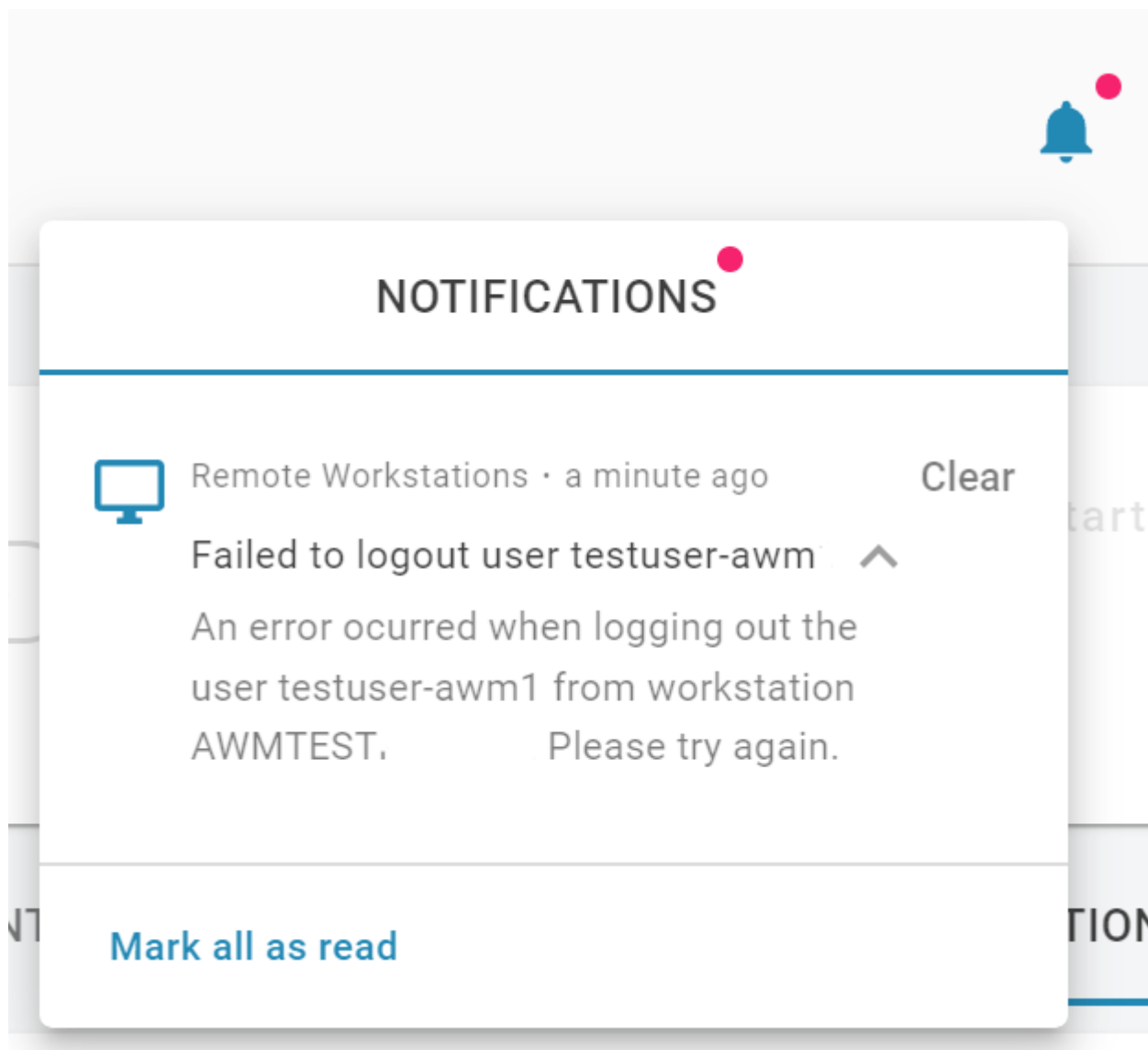


- Example of logout warning notification on Windows



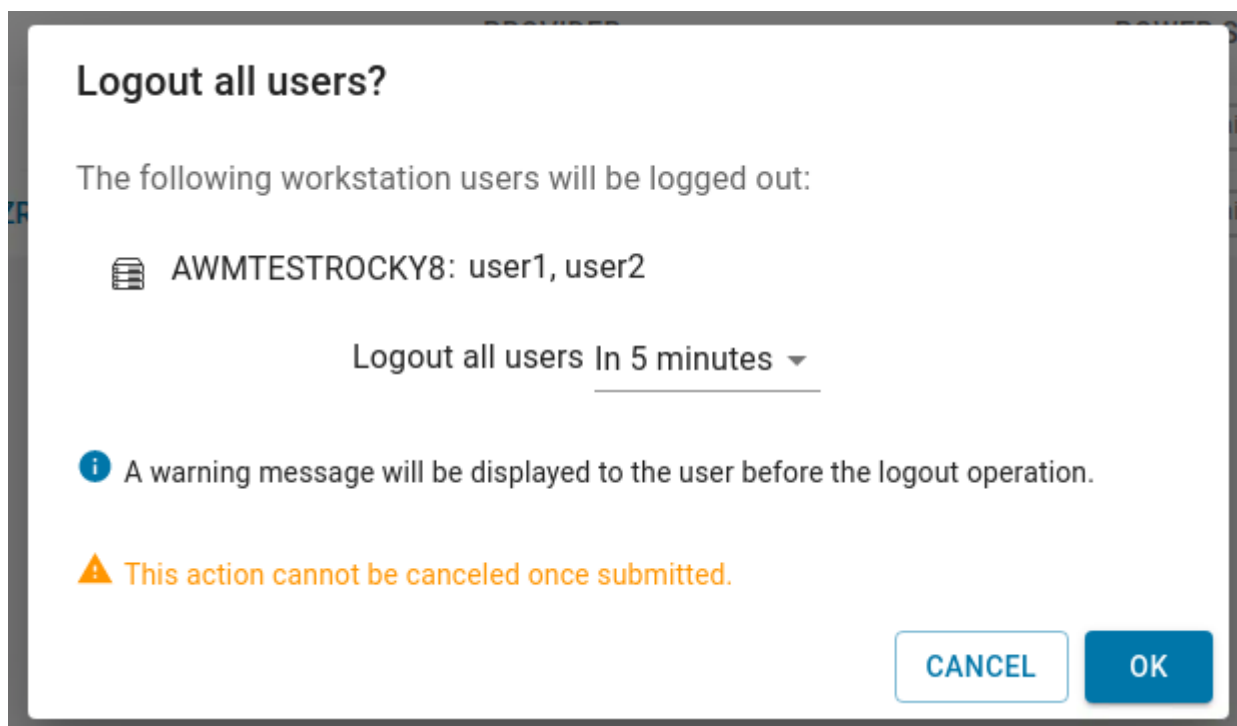
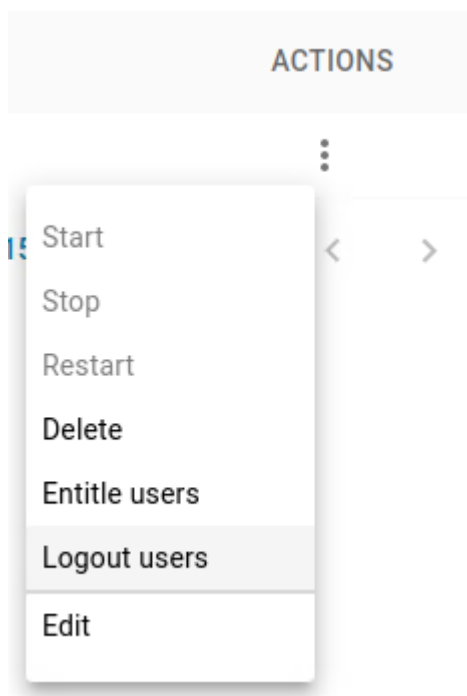
### Log out Attempt

If the user is not logged out due to network errors, the notification center warns the admin that the log out attempt was unsuccessful.



### Multiple users logout

If you have more than one user logged in a remote workstation, you can log them out by clicking in the logout action button.

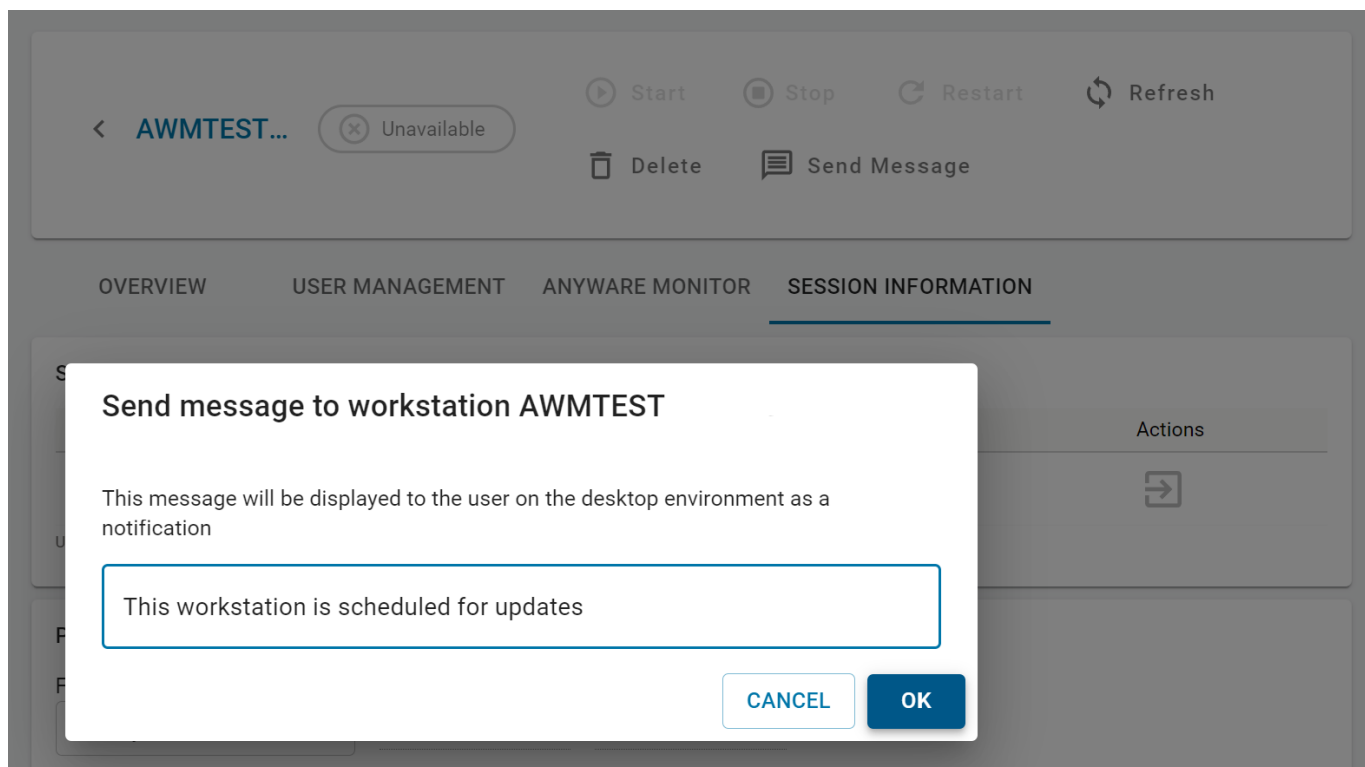


Manual Notifications

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**.





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.
2. Ubuntu- `/etc/gdm3/custom.conf`
3. CentOS/RHEL- `/etc/gdm/custom.conf`
4. Open the file with `sudo/root privileges` command.

5. Uncomment `WaylandEnable=false` by deleting the `#` at the beginning of the line.
6. Restart the VNC Server.

## 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 21H1, 21H2
- Windows 11 21H2, 22H2
- Windows Server 2019, 2022
- Ubuntu 18.04 LTS
- Ubuntu 22.04 LTS
- RHEL 7.8, 7.9, 8
- CentOS 7.8, 7.9
- 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. 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 Manager Monitor  
Copy and run the generated command in a terminal with administrator privileges. This will install and register the Anyware Manager Monitor. When the process is complete, we will attempt to establish a connection.

LINUX® WINDOWS

```
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.)

COPY

Running this command on Workstations downloads the Anyware Monitor and its dependencies, installs the Monitor, and registers the Workstation with the Anyware Manager.

#### ⚠ Warning

For each Workstation, you need to generate a token using a new command by following steps 1 to 5. The command carries a 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](#).

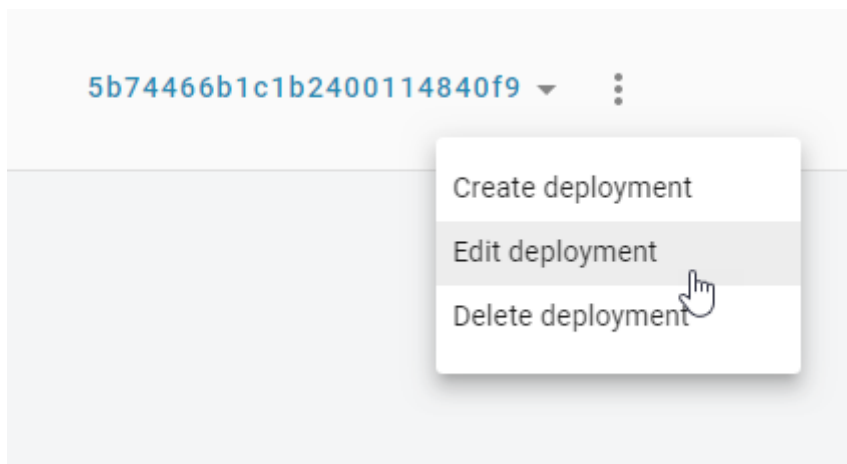
6. Run the command inside a terminal from your chosen workstation with administrative privileges.
7. Once the installation and registration has succeeded, you can see your Workstation with a connection status of Healthy. The Anyware Monitor feature is ready to use.
8. Repeat steps 1 to 7 for installing Anyware Monitor on each subsequent workstation added in Anyware Manager.

## ANYWARE MONITOR BULK INSTALLATION

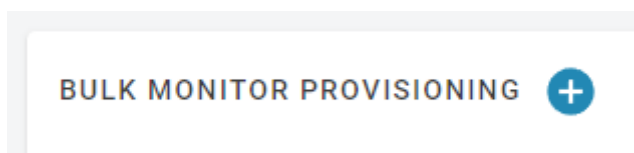
To expedite the deployment of several monitor installations, a bulk enrollment option is available. This option uses a single command that can be passed to any number of machines to start an automated process of installation and registration. It should be noted that machines do not need to be added to 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.

To facilitate Anyware Monitor Bulk installation:

1. Open the Admin Console and click the kebab option in the dashboard and select **Edit Deployment**.



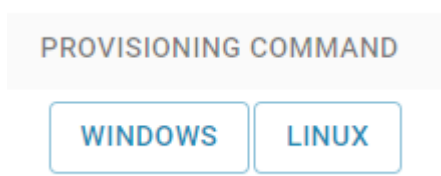
2. Navigate to the **Anyware Monitor** section in the **Workstations** tab, click "+" next to **Bulk Monitor Provisioning** and enter a Command Name.



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. Select an Operating System to generate a command that is copied to your clipboard.



5. 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**

6. 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.**

7. 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.

[SEE HOSTNAMES](#)

8. 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.

## 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 are 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** 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 -sLfS https://dl.anyware.hp.com/token/anyware-manager/raw/names/anyware-monitor-sh/versions/latest/anyware-monitor_latest.sh | sudo -E manager_uri=https://cam.teradici.com 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://dl.anyware.hp.com/token/anyware-manager-dev/raw/names/anyware-monitor-ps1/versions/latest/anyware-monitor_latest.ps1 } | Invoke-Expression; install -manager_uri https://cam.teradici.com -proxy_uri https://myproxyserver:port -token enrollment_token -mode enroll -channel stable -download_token token;exit"
```

### 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 `anyware-monitor` package. You can run the following commands:

Example for Ubuntu:

**With apt:**

```
sudo apt remove anyware-monitor
```

**Example for RHEL:****With yum:**

```
sudo yum remove anyware-monitor
```

**With dnf:**

```
sudo dnf remove anyware-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.**

OVERVIEW    USER MANAGEMENT    **AWM MONITOR**    SESSION INFORMATION

#### ANYWARE MANAGER MONITOR CONFIGURATION

Version 23.01.386-dev	Connection Healthy	Last Connection Aug 16, 2022 04:40:03 PM MDT
--------------------------	-----------------------	---

Enabling this feature allows Anyware Manager 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 AWM Monitor 

#### 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.

[SHOW INSTALL INSTRUCTIONS](#)

### Proxy Settings

If your workstation is behind a proxy, you might need to configure proxy settings in [Proxy Configuration](#).

### 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



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

#### 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 attempts 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.
```

# Anyware Connector

## Overview

The Connector is an access hub installed in the customer environment which facilitates PCoIP Client connections to remote workstations. It operates in conjunction with HP Anyware Manager to provide user authentication and entitlement for remote workstation access, including MFA. It enables secure connectivity between users and the remote workstations by eliminating the need for a dedicated VPN by providing NAT services for external users.

The Connector currently runs on an Ubuntu server, we are adding the support to run on Rocky Linux 8 or RHEL 8 starting from Connector version 23.04.0. At HP, we are in a constant endeavour to simplify and unify our OS support strategy. To that effect, Anyware Manager and Connector will only support RHEL / Rocky Linux (8.0 & Above) starting H2 of 2023, and we will be EOLing Ubuntu CAC (actual Date TBD). You will be notified six months before a migration path from Ubuntu to RHEL / Rocky Linux for new Anyware Connectors.

The Connector enables Anyware Manager to broker desktops or workstations located in AWS, Google Cloud, Microsoft Azure and on-premises environments. Based on customers' infrastructure, they may need more than one Connector. The Connector communicates with the Anyware Manager which orchestrates and manages Anyware deployments.

You are required to have a valid registration code for HP Anyware Software to be able to successfully deploy Anyware Manager. This code is sent to you via email from HP and looks like ABCDEF1234@AB12-C345-D67E-89FG. For more information on Anyware Software, see [HP Anyware](#).

# Connector on Ubuntu

## Prerequisites

### System Requirements

Connector is software that runs within an Ubuntu server and enables secure connectivity between users and the remote workstations. Connector runs in the customer environment such as on-premises, AWS and Google Cloud. The Connector communicates with the Anyware Manager which orchestrates and manages HP Anyware deployments.

#### CREATING THE CONNECTOR SERVER

The Connector runs on an Ubuntu server (called the Connector server).

YOu need to create a dedicated Ubuntu server with the following specifications:

- Ubuntu Server 18.04.
- At least 4GB RAM.
- 30GB available storage or more.
- 2 vCPUs or more.

Once you have setup a dedicated virtual machine for the Connector, please ensure the following environment conditions are met:

- You must have access to the internet.
- You must have an Active Directory (AD) user account located in the designated Connector domain admins group, in order to log into the Admin Console.
- The server must be able to resolve the AD domain.
- You must be able to access the server using SSH.
- You must have superuser (sudo) privileges on the server.
- The networking information of the server (including the IP address) must not change while the Connector is operational.



- The server must have a single network interface and IP address. If the server has multiple network interfaces, the Connector will fail to install.
- If you are deploying Ubuntu on ESXi, you must install open-vm-tools to enable the ESXi host to communicate with the Connector server.
- The Connector runs on the following supported domain controller servers:
  - Windows 2016 Server with secure LDAP (LDAPS) enabled.
  - Windows 2012 R2 Server with secure LDAP (LDAPS) enabled.
  - Windows 2019 Server with secure LDAP (LDAPS) enabled.

For information on the session establishment and session bandwidth limits when working with external connections, see [System and Scaling Limits](#).

#### **Creating a DNS record**

If you want to create a DNS record for the Connector, you need to obtain an SSL certificate with its FQDN and provide it (along with the key) when installing the Connector. This will avoid SSL certificate verification warnings.

## VERIFYING THE CONNECTOR SERVER

To verify your Connector server network configuration, SSH into the machine and ping the domain and a remote workstation in the domain. You should get a positive response from both attempts:

```
ping <domain FQDN>
ping <remote workstation FQDN>
```

If any of your attempts to verify these components fails, the DNS settings on the Connector server might be misconfigured. For more information on DNS configuration, see [Configuring Network Settings in Ubuntu 18.04](#).

## Enabling Connections over WAN

If the Connector server will be accessed outside the domain, it must be configured for external access (this step is only required if you want to enable remote access to the workstations without requiring a VPN):

- The server must have a public IP address. This can be done via bi-directional NAT mapping.
- The `--external-client-cidr` flag takes priority over the `--internal-client-cidr`. The default for the `--internal-client-cidr` is `10.0.0.0/8,172.16.0.0/12,192.168.0.0/16`. Any source that does not match to a `--internal-client-cidr` will default to an external connection.

For example `--external-client-cidr 0.0.0.0/0` will treat everything as an external connection, to reset to the default behaviour you would need to enter the following command and flag parameters:

```
./cloud-access-connector update --internal-client-cidr 10.0.0.0/8 --internal-client-cidr 172.16.0.0/12 --internal-client-cidr 192.168.0.0/16
```

When setting connections from a firewall or security gateway to be external, the internal CIDR will treat connections under a certain range as internal. For example the following example will treat connections originating from under the `10.11.12.0/24` CIDR except `10.11.12.1` as internal:

```
./cloud-access-connector update --internal-client-cidr 10.11.12.0/24 --external-client-cidr 10.11.12.1/32
```

Port 443 TCP and 4172 UDP/TCP need to be open. Session set-up is done through port 443 and in-session traffic runs through port 4172. The `--external-pcoip-ip` flag sets the IPv4 address for the Connector for external connections. If this value is not set, the external IPv4 address will be determined automatically. This is an optional setting that can be used when installing the Connector. For information on the session establishment and session bandwidth limits when working with external connections, see here.

### Reboot the server after NAT changes

If the NAT is configured after the Connector has been installed, reboot the Connector server.

## Multi-Factor Authentication

When you install the Connector you can specify whether the PCoIP session uses Multi-Factor Authentication (MFA) during authentication or not. The Connector can be integrated with your RADIUS server. To do this you will need to provide the following information during the Connector installation:

- The FQDN or IP address of the RADIUS server.
- The RADIUS server port. If this port is not specified the default port (1812) will be used.
- The shared secret used for configuring RADIUS authentication.

If you do not enable MFA when installing the Connector, you can enable it later when performing an update, see [Updating the Connector](#). For more information on Connector MFA, see [Multi-Factor Authentication](#).

## Active Directory Service Accounts

The following sections outline the Active Directory (AD) Service Account permissions required for installing the Connector. It also outlines the steps required to set these permissions.

### PERMISSIONS REQUIRED TO INSTALL THE CONNECTOR

There are no mandatory permissions required for the AD Service Account to install the Connector. You can optionally delegate the **Reset user passwords and force password change at next logon** task in the Delegation of Control Wizard panel. For steps on how to delegate the password reset task to the AD Service Account, see Permissions to Change and Reset Passwords.

Delegating this task will enable users to change and reset their passwords while connecting to the remote workstations. If this is not set, the user will receive an error.

#### Higher AD Service Account Permissions

If the user has a higher level of permissions than the AD Service Account, then you will experience password change errors even if the delegation is configured as outlined above.

#### Domain Controller Certificates

If all DC certificates have expired, the Connector will stop working. An error indicator will display on the Connectors page when a Connector has a DC with expired certificates. A warning indicator that details the current state of the DC certs will display on the same page when a Connector has a certificate that less than a week away from expiring. For information on how to create and install a self-signed certificate on a Windows 2016 AD server to test LDAP connections, see [KB 1707](#).

### Permissions to Change and Reset Passwords

The following steps outline how to delegate the **Reset user passwords and force password change at next logon** task in the Delegation of Control Wizard:

1. Open the **Active Directory Users and Computers** application.
2. Select the user or group you want to delegate, and click **Delegate Control**.
3. Click **Next**.
4. Click **Add** and enter the username or group name that will be granted reset permission.

5. Click **OK**.
6. Click **Next**.
7. Select **Delegate the following common tasks** and select the **Reset user passwords and force password change at next logon** task.
8. Click **Finish**.

#### During Installation

When the Connector is installed, you will be prompted for the following information:

- The AD Service Account username.
- The AD Service Account password.

#### Permissions Required to Provision Remote Workstations

Before provisioning a remote workstation you need to ensure that the AD Service Account 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 specific permissions, for information on these permissions and how to configure them, see [Provisioning Remote Workstations](#).

## Assigning an SSL Certificate

You can assign an SSL certificate to the Connector during installation. This will prevent certificate verification errors when connecting to the Anyware Manager or Anyware Manager as a Service Interface through your browser. It will also prevent the PCoIP client from reporting an insecure connection when establishing a PCoIP session.

The certificate you provide must be signed and validated by a root certificate that the client trusts. The certificate must be combined or bundled with the intermediate certificates in PEM format and copied, along with the key, to the Connector server prior to installation.

For an example of how to create a self-signed certificate, see [Creating a self-signed certificate on a Windows 2016 Active Directory Server](#). For an example of a method to install a certificate on your Active Directory, see [Installing a certificate on your Active Directory server to enable LDAPS](#).

The DNS needs to be setup so that 'casm.test.com' for example, is registered to the public IP address of the application gateway.

When the Connector is installed, you will be prompted for the following information:

- The full path and filename of the SSL key
- The full path and filename of the SSL certificate

If you do not wish to specify a certificate when installing the Connector, you can bypass this by entering the command line option `--self-signed` (which is recommended strictly for testing purposes). If you decide to use a certificate later, HP recommends creating a new Connector and deleting the old one. For information on updating SSL certificates, see [Updating Connector](#).

# Installing Connector on Ubuntu

The following section outlines how to download and install the Connector. There are three steps involved in this process:

- Downloading the Connector installer files.
- Obtaining an authorization token.
- Installing the Connector.

## PREREQUISITE STEPS

For instructions and documentation on the Connector prerequisite steps, see [Connector System Requirements](#).

It is important to read and address all the prerequisites outlined.

## 1. DOWNLOADING THE CONNECTOR

The following section outlines how to download the installer files for the Connector. First, connect to the machine and download the Connector files. The commands below will download the Connector archive, and extract it.

You need to ensure that you have a customer account created on our website to access the download information.

### Downloading the Installer from our website

The following steps outline the current process that enables you to download the installer directly from our website as a `tar.gz` file or else run the shell script:

1. SSH into the machine:

```
ssh <username>@<server-ip-address>
```

2. Download the installer from HP:

- Open a web browser and navigate to the [Downloads and Scripts](#) tab on the HP support site.
- Download the installer and upload it to the machine or run the shell script provided to download the installer to the machine.

### 3. Unpackage the installer:

- Previously the installer was extracted into the ~/v2connector directory. This location has now changed. Run the following command to extract the installer to /usr/sbin/:

```
sudo tar xzvf <PATH TO FILE>/cloud-access-connector_<version>_Linux.tar.gz -C /
```

## 2. OBTAINING THE CONNECTOR TOKEN

You are required to have a Connector token when installing the Connector. You need to create or have created a deployment prior to obtaining a token. For information on how to log into the Admin Console, see Admin Console Connection. The following section outlines how to obtain a Connector token using the Admin Console:

1. Click **Connectors** from the console sidebar.
2. Click the add connector button (+ sign located beside the **Connectors** heading) to display the connector creation panel.
3. Enter the following information:
  - Select the deployment you want to add the Connector to. If you do not have an existing deployment you need to create one.
  - Enter the name of the Connector.
  - Follow the step by step instructions outlined in the **private cloud install instructions** panel.
4. Click **GENERATE**.
5. Copy the Connector token by clicking the copy icon.
6. Click **CLOSE** to exit the panel.

You can now use this Connector token when prompted during installation.

## 3. INSTALLING THE CONNECTOR

Once the files are downloaded and the access token is set, you can install the Connector. If you are not already connected, connect to the machine via SSH and navigate to the /usr/sbin directory.



### Latest Installer Version

Ensure that you are using the latest installer prior to installing or upgrading the Connector. If you are not using the latest installer, you may see one of the following errors or warnings:

- The installer is out of date. Please obtain the latest version and try again. See [Downloading the Connector](#) for instructions.
- The installer is out of date. Please download the latest version from [teradici.bintray.com/cloud-access-connector/cloud-access-connector-0.1.1.tar.gz](https://teradici.bintray.com/cloud-access-connector/cloud-access-connector-0.1.1.tar.gz) and try again.
- A newer version is available. Please go to [Downloading the Connector](#) to obtain the latest.

For information on troubleshooting Connector installer issues related to this distribution change, see [Installer Issues](#).

### Limiting Active Directory Data Used

The `--users-dn` and `--computers-dn` flags are highly recommended to be used during installation to limit the scope of your Active Directory used by Anyware Manager to locate remote workstations and users. Limiting this scope can improve Anyware Manager performance when searching and syncing data, or searching for users and remote workstations. Additionally, it ensures only the minimum amount of data is synced.

## 3.1 Installing the Connector for Anyware Manager as a Service

Install the Connector for Anyware Manager as a Service by running the following command:

```
cd /usr/sbin
sudo ./cloud-access-connector install
```

Ensure that you use the options and flags that best suit your system architecture and requirements. If required values are not provided on the command line, you will be prompted for them. For additional flags and options, see [Installation Flags and Options](#).

## MULTI-FACTOR AUTHENTICATION

When installing the Connector you can enable multi-factor authentication (MFA) by running the `--enable-mfa` flag. MFA will be disabled by default. If you want MFA to only apply to external connections, you should have separate Connectors. One Connector should be for external

connections, where MFA is enabled, and one for internal or direct connections, where MFA is disabled. For steps on how to install the Connector with MFA bypassed for internal connections, see [Installing the Connector for Internal Connections](#).

For external facing Connectors you should apply firewall and network settings, such as placing it in a DMZ for example. For external facing Connectors, ensure that you set `--external-client-cidr` to `0.0.0.0/0` so that everything through this Connector is treated as an external connection. It is not recommended to rely on the IP range to manage authentication levels, and for better security you should use separate Connectors.

Ensure that you use the options and flags that best suit your system architecture and requirements. If required values are not provided on the command line, you will be prompted for them. For additional flags and options, see [Installation Flags and Options](#).

### Installing the Connector for Internal Connections

The following steps outline how to install the Connector for internal connections to bypass MFA:

1. Prepare a virtual machine in your private network that meets the system requirements with the following sub-steps:
  - Skip the step for preparing the system for external access.
  - Skip the step for setting up MFA.
2. Install the Connector with the following sub-steps:
  - Do not set the Public IP using the `--external-pcoip-ip` flag. The Connector will instead return the virtual machines IP address.
  - No MFA flag is required as MFA is disabled by default.
3. Once you have installed the Connector connect to a remote workstation with a PCoIP Software Client with the following sub-step:
  - In the *Host Address or Code* field enter the private IP of the internal Connector you just installed and log-in.

If you want to use the same url for an external Connector as an internal Connector, for example `connector.domain.com`, you must set-up an internal/private DNS. In this DNS create an entry called `connector.domain.com` and map it to the private IP of the internal Connector. User's will then be able to connect to this entry by entering `connector.domain.com` in the *Host Address or Code* field in the PCoIP Client. The internal connection will connect to the internal Connector, and the external connection will connect to the external Connector.

## Installation Flags and Options

The following flags can be used to provide values at the command line. If they are omitted from the command and are required, you will be prompted for them:

Flag	Type	Description
<b>Anyware Manager</b>		
<code>--manager-url</code>	String	Required for Anyware Manager, Specifies the Anyware Manager URL that the Connector connects to. If this is not specified it will point to <a href="https://cas.teradici.com">https://cas.teradici.com</a> by default, which is the URL for Anyware Manager as a Service.
<code>--manager-ca-cert</code>	String	Enables users to supply a CA certificate for Anyware Manager to enable the Connector to connect to a Anyware Manager instance using self-signed certificates.
<code>--manager-insecure</code>	String	Is required when the Connector is connecting to a Anyware Manager instance that is using self-signed certificates. If Anyware Manager is using trusted TLS certificates signed by a public CA, then users will not need to use the this command.
<code>--ldaps-ca-cert</code>	String	Enables users to supply a CA certificate for the connection to Active Directory over LDAPS.
<code>--self-signed</code>	String	Installs the Connector with self-signed certificates. This mode is not secure and is intended for testing. The <code>--insecure</code> flag is still supported.
<code>--pull-connector-config</code>	Boolean	This flag gets the Connector configuration from the Anyware Manager.
<code>--push-connector-config</code>	Boolean	This flag saves the Connector configuration into the Anyware Manager.
<b>Connector</b>		
<code>--token (-t)</code>	String	Required. The token generated for Anyware Manager.
<code>--accept-policies</code>	–	Automatically accept the <a href="#">EULA</a> and <a href="#">Privacy Policy</a> .
<code>--force-install</code>	String	Replaces any existing Connector installation.
<code>--debug</code>	String	This flag can be run if you initial install of the Connector fails. It provides a detailed output of the Connector installation. This is useful for self-troubleshooting or to provide to the HP support team when logging a support ticket.
<code>--local-license-server-url</code>	String	Sets the URL for PCoIP License Server to be used for PCoIP Sessions. If this is not provided, ensure that the Cloud License Server is registered on the PCoIP Agent. Example: <code>--local-license-server-url <a href="http://10.10.10.10:7070/">http://10.10.10.10:7070/</a></code>

Flag	Type	Description
		<a href="#">request</a> . For more information on the PCoIP License Server, see <a href="#">PCoIP License Server</a> .
<code>--add-pool-group</code>	String	Specifies one or more Active Directory groups, by entering the distinguished name (DN), to be assigned to pools for remote workstation management (eg, <code>--pool-group 'CN=GroupPool1,CN=Users,DC=sample,DC=com'</code> <code>--pool-group 'CN=GroupPool2,CN=Users,DC=sample,DC=com'</code> ). By providing all the existing pools groups in the Connector settings would get replaced by the user specified ones. When running this command you need to run it with <b>adconfig</b> . Example: <code>sudo ./cloud-access-connector adconfig --add-pool-group</code> .
<code>--setup-docker-image</code>	String	Specifies the docker image to be used from the setup container. This is intended to be used for debugging purposes and is not recommended to be used without guidance from HP support. Usage without guidance could result in failed installations.
<code>--docker-registry</code>	String	This is an optional flag that enables users to specify the docker image registry that they want to use when installing or updating a Connector. If an option is not specified, the default registry <code>docker.cloudsmith.io/teradici/cloud-access-connector</code> is used. This is intended to be used for debugging purposes and is not recommended to be used without guidance from HP support. Usage without guidance from us could result in failed installations.
<code>--prune-image</code>	Boolean	Removes all unused docker images on this machine to reclaim more disk space. <b>Warning:</b> This command will remove all unused images under Connector and other services, if any. This is equivalent to the <code>docker image prune</code> command.
<b>Firewall</b>		
<code>--https-proxy</code>	String	Specify the URL for a HTTPS proxy (overrides related proxy settings in environment variables)
<code>--connector-network-cidr</code>	String	This is the CIDR to use for the Connector's docker network. The default docker network subnet is 10.101.0.0/16.
<code>--internal-client-cidr</code>	String	The CIDR for PCoIP Clients that connect to remote workstations directly. It is possible to specify multiple <code>--internal-client-cidr</code> networks.

Flag	Type	Description
<code>--external-client-cidr</code>	String	The CIDR for PCoIP Clients that connect to remote workstations through the Security Gateway. If external CIDRs settings are set, internal settings must be explicitly set. It is possible to specify multiple <code>--external-client-cidr</code> networks.
<b>PCoIP Software Client</b>		
<code>--retrieve-agent-state</code>	Boolean	Enables the broker to retrieve the agent state for unmanaged and managed remote workstations. The default value for this flag is false. The available states are <i>In Session</i> , <i>Ready</i> , <i>Starting</i> , <i>Stopping</i> , <i>Stopped</i> and <i>Unknown</i> . The value of this flag can either be true or false.
<code>--show-agent-state</code>	Boolean	Controls if the agent state is displayed as part of the remote workstation name in the PCoIP Client. The default value for this flag is true. Setting the value of this flag to true and the <code>--retrieve-agent-state</code> flag to false will result in no agent state displaying.
<code>--external-pcoip-ip</code>	String	Sets the public IP for PCoIP Client to PCoIP Agent connection. This is the public IP that the Connector is listening to on port 4172. The installer will reach out to cas.teradici.com and first try to automatically resolve the external IP; if this fails, or is not able to resolve the correct IP, this flag is required. In the case that the Connector machine doesn't have an internet connection, for example in a dark site environment, or the ingress and egress internet traffic are running through different public IPs, this flag is required. For more information on external network access, see <a href="#">Enabling External Network Access</a> .
<b>Domain</b>		
<code>--domain</code>	String	The AD domain that remote workstations will join.
<code>--sa-user</code>	String	The Active Directory service account username.
<code>--sa-password</code>	String	The Active Directory service account password.
<code>--domain-controller</code>	String	Specifies one or more domain controllers to use with the Connector.
<code>--users-filter</code>	String	The filter to search for users within Active Directory. Specify multiple filters with multiple options. Default user filter: (&(objectCategory=person)(objectClass=user)).

Flag	Type	Description
<code>--computers-filter</code>	String	The filter to search for computers within Active Directory. Specify multiple filters with multiple options. Default computer filter: (&(primaryGroupID=515)(objectCategory=computer)).
<code>--users-dn</code>	StringArray	The base DN to search for users within AD. Specify multiple DNs with multiple options. Newly provided base DN(s) will automatically replace previous base DN(s). This field is looking for user's within the user-defined DN and SGs.
<code>--computers-dn</code>	StringArray	The base DN to search for computers within AD. Specify multiple DNs with multiple options. Newly provided base DN(s) will automatically replace previous base DN(s).
<code>--sync-interval</code>	uint8	The interval (in minutes) for how often to sync AD users and computers with the AWM Service.
<b>MFA</b>		
<code>--enable-mfa</code>	String	Installs with multi-factor authentication enabled.
<code>--radius-server</code>	String	The FQDN or IP address of the RADIUS server to use for MFA. This flag is optional.
<code>--radius-port</code>	String	The RADIUS server port. If not specified, the default port (1812) is used. If <code>--radius-server</code> is specified then this flag is optional.
<code>--radius-secret</code>	String	The shared secret used for configuring RADIUS authentication. If <code>--radius-server</code> is specified then this flag is required.
<b>Oauth</b>		
<code>--id-provider-url</code>	String	Sets the Identity Provider URL. Example: <code>--id-provider-url https://id.provider.com</code>
<code>--enable-oauth</code>	Boolean	Enables/Disables oauth authentication (if enabled <code>--id-provider-url</code> and <code>--oauth-client-id</code> must be provided)
<code>--oauth-client-id</code>	String	Sets the Oauth Application Client id
<code>--oauth-flow-code</code>	String	Specify the oauth flow / grant type
	String	The full path and filename of Oauth Server CA certificate

Flag	Type	Description
<code>--oauth-server-ca</code>		
<code>--fa-url</code>	String	The Federated Auth Broker URL. for example <a href="https://cac-vm-fqdn:port">https://cac-vm-fqdn:port</a>
<b>Single Sign-On (SSO)</b>		
<code>--sso-signing-csr-ca</code>	String	Path to copy intermediate CA Certificate.
<code>--sso-signing-csr-key</code>	String	Path to the intermediate key.
<code>--sso-signing-crl</code>	String	Path to a certificate revocation list.
<code>--sso-enrollment-url</code>	String	Gets the URL to the Active Directory Certification Authority Web Enrollment Service.
<code>--sso-enrollment-domain</code>	String	Domain of the user to access Active Directory Certification Authority Web Enrollment Service.
<code>--sso-enrollment-username</code>	String	Username for accessing Active Directory Certification Authority Web Enrollment Service.
<code>--sso-enrollment-password</code>	String	Password for the username to access Active Directory Certification Authority Web Enrollment Service.
<code>--sso-enrollment-certificate-template-name</code>	String	Name of the certificate template that Active Directory Certificate Services (AD CS) uses to sig CSR.
<code>--sso-enrollment-certificate-template-name</code>	String	Name of the certificate template that Active Directory Certificate Services (AD CS) uses to sig CSR.
<b>Certificates</b>		
<code>--ssl-key</code>	String	The full path and filename of the SSL key to use. The <code>--self-signed</code> flag overrides this flag.
<code>--ssl-cert</code>	String	The full path and filename of the SSL certificate (in PEM format) to use. The <code>--self-signed</code> flag overrides this flag.



## Troubleshooting the Connector

If you encounter issues when attempting to install the Connector, please see the Troubleshooting section for information on how to potentially diagnose the specific issue. You can also view the following KB article [here](#) which provides a list of troubleshooting steps for common issues related to installing the Connector. For information on installer errors related to a change in the distribution system, see [Installer Issues](#).

## 4. CONNECTING TO A REMOTE WORKSTATION WITH A PCOIP CLIENT

After successfully installing a Connector, you can initiate a session to connect to a remote workstation with a PCoIP Software Client. HP enables customers to use multi-factor authentication for these PCoIP Client sessions. The following steps outline how to connect to a remote workstation using the PCoIP Software Client:

1. Double-click the PCoIP Client desktop icon or program file `PCoIPClient` to launch the application.
2. In the *Host Address or Code* field, enter one of the following:
  - For direct connections, provide the address of the host machine.
  - For managed connections, provide the address of the connection manager.
3. Click **NEXT**.
4. Select your domain and enter the credentials for the remote workstation. If you have enabled MFA then you will be prompted for the 2<sup>nd</sup> factor passcode. The method of how this passcode is communicated depends on the provider you used. It is usually either a One Time Password or push notification.
5. Click **LOGIN**.
6. If your login is successful you should be able to select the remote workstation and connect to it. Please note that if you have a single remote workstation, that remote workstation is automatically selected and the connection is initiated immediately. In this case you will not be presented with a remote workstation selection screen.

For more information about the PCoIP Software Client, please see the following PCoIP Software Client guides:

- [PCoIP Software Client for Windows](#)
- [PCoIP Software Client for macOS](#)
- [PCoIP Software Client for Linux](#)

## Upgrading the Connector on Ubuntu

When updating an installed Connector you must download the latest version of the Connector installer. For information on how to download the Connector installer, see [Installing the Connector](#). All parameters persist from installation using pre-defined configurations and do not need to be updated unless new configurations are required. For more information on this please see the [Persistent Parameters](#) section below.

Once you have downloaded the latest installer, run the update command:

```
cd /usr/sbin
sudo cloud-access-connector update
```

### Internal IP Address

As part of the update command the Connector will send its internal IP address to Anyware Manager. Previously, this only occurred during installation.

### Latest Installer Version

Ensure that you are using the latest installer prior to installing or upgrading the Connector. If you are not using the latest installer, you may see one of the following errors or warnings:

- The installer is out of date. Please obtain the latest version and try again. See [Downloading the Connector](#) for instructions.
- The installer is out of date. Please download the latest version from [teradici.bintray.com/cloud-access-connector/cloud-access-connector-0.1.1.tar.gz](https://teradici.bintray.com/cloud-access-connector/cloud-access-connector-0.1.1.tar.gz) and try again.
- A newer version is available. Please go to [Downloading the Connector](#) to obtain the latest.

For information on troubleshooting Connector installer issues related to this distribution change, see [Installer Issues](#).

## Persistent Parameters

Parameters can persist from installation through an update using the pre-defined configurations. As part of the update command, the Connector will search and read from the existing configuration and use the pre-existing information as part of the update.

If you wish to update any parameters with new information as part of the update, you can add these parameters when you are running the update command, for example, if you wanted to update the domain controller you would run the following command:

```
cd /usr/sbin
sudo cloud-access-connector update --domain-controller mydomain.com
```

If you do not add domain controllers during the update, any domain controllers that have been previously saved in the configuration will be used. If there are no domain controllers saved, the system will do an auto-discovery to find which domain controllers could be used.

### Expired User Credentials

Be aware that you have a `--sa-user` or `--sa-password` that are expired and you do not add the new credentials to the update, then the update will fail. Please ensure these credentials are valid when performing an update of the Connector.

## Installation Flags and Options

The following flags can be used to provide values at the command line. If they are omitted from the command and are required, you will be prompted for them:

Flag	Type	Description
<b>Anyware Manager</b>		
<code>--manager-url</code>	String	Required for Anyware Manager, Specifies the Anyware Manager URL that the Connector connects to. If this is not specified it will point to <a href="https://cas.teradici.com">https://cas.teradici.com</a> by default, which is the URL for Anyware Manager as a Service.
<code>--manager-ca-cert</code>	String	Enables users to supply a CA certificate for Anyware Manager to enable the Connector to connect to a Anyware Manager instance using self-signed certificates.
<code>--manager-insecure</code>	String	Is required when the Connector is connecting to a Anyware Manager instance that is using self-signed certificates. If Anyware Manager is using trusted TLS certificates signed by a public CA, then users will not need to use the this command.
<code>--ldaps-ca-cert</code>	String	Enables users to supply a CA certificate for the connection to Active Directory over LDAPS.
<code>--self-signed</code>	String	Installs the Connector with self-signed certificates. This mode is not secure and is intended for testing. The <code>--insecure</code> flag is still supported.
<b>Connector</b>		
<code>--token (-t)</code>	String	Required. The token generated for Anyware Manager.
<code>--accept-policies</code>	—	Automatically accept the <a href="#">EULA</a> and <a href="#">Privacy Policy</a> .
<code>--force-install</code>	String	Replaces any existing Connector installation.
<code>--debug</code>	String	This flag can be run if you initial install of the Connector fails. It provides a detailed output of the Connector installation. This is useful for self-troubleshooting or to provide to the HP support team when logging a support ticket.
<code>--local-license-server-url</code>	String	Sets the URL for PCoIP License Server to be used for PCoIP Sessions. If this is not provided, ensure that the Cloud License Server is registered on the PCoIP Agent. Example: <code>--local-license-server-url <a href="http://10.10.10.10:7070/request">http://10.10.10.10:7070/request</a></code> . For more information on the PCoIP License Server, see <a href="#">PCoIP License Server</a> .
<code>--add-pool-group</code>	String	Specifies one or more Active Directory groups, by entering the distinguished name (DN), to be assigned to pools for remote workstation management (eg, <code>--pool-group 'CN=GroupPool1,CN=Users,DC=sample,DC=com'</code> <code>--pool-group 'CN=GroupPool2,CN=Users,DC=sample,DC=com'</code> ).

Flag	Type	Description
		By providing all the existing pools groups in the Connector settings would get replaced by the user specified ones. When running this command you need to run it with <b>adconfig</b> . Example: <code>sudo ./cloud-access-connector adconfig --add-pool-group</code> .
<code>--setup-docker-image</code>	String	Specifies the docker image to be used from the setup container. This is intended to be used for debugging purposes and is not recommended to be used without guidance from HP support. Usage without guidance could result in failed installations.
<code>--docker-registry</code>	String	This is an optional flag that enables users to specify the docker image registry that they want to use when installing or updating a Connector. If an option is not specified, the default registry <code>docker.cloudsmith.io/teradici/cloud-access-connector</code> will be used. This is intended to be used for debugging purposes and is not recommended to be used without guidance from HP support. Usage without guidance from us could result in failed installations.
<code>--prune-image</code>	Boolean	Removes all unused docker images on this machine to reclaim more disk space. <b>Warning:</b> This command will remove all unused images under Connector and other services, if any. This is equivalent to the <code>docker image prune</code> command.
<b>Firewall</b>		
<code>--https-proxy</code>	String	Specify the URL for a HTTPS proxy (overrides related proxy settings in environment variables)
<code>--connector-network-cidr</code>	String	This is the CIDR to use for the Connector's docker network. The default docker network subnet is 10.101.0.0/16.
<code>--internal-client-cidr</code>	String	The CIDR for PCoIP Clients that connect to remote workstations directly. It is possible to specify multiple <code>--internal-client-cidr</code> networks.
<code>--external-client-cidr</code>	String	The CIDR for PCoIP Clients that connect to remote workstations through the Security Gateway. If external CIDRs settings are set, internal settings must be explicitly set. It is possible to specify multiple <code>--external-client-cidr</code> networks.
<b>PCoIP Software Client</b>		

Flag	Type	Description
<code>--retrieve-agent-state</code>	Boolean	Enables the broker to retrieve the agent state for unmanaged and managed remote workstations. The default value for this flag is false. The available states are <i>In Session</i> , <i>Ready</i> , <i>Starting</i> , <i>Stopping</i> , <i>Stopped</i> and <i>Unknown</i> . The value of this flag can either be true or false.
<code>--show-agent-state</code>	Boolean	Controls if the agent state is displayed as part of the remote workstation name in the PCoIP Client. The default value for this flag is true. Setting the value of this flag to true and the <code>--retrieve-agent-state</code> flag to false will result in no agent state displaying.
<code>--external-pcoip-ip</code>	String	Sets the public IP for PCoIP Client to PCoIP Agent connection. This is the public IP that the Connector is listening to on port 4172. The installer will reach out to cas.teradici.com and first try to automatically resolve the external IP; if this fails, or is not able to resolve the correct IP, this flag is required. In the case that the Connector machine doesn't have an internet connection, for example in a dark site environment, or the ingress and egress internet traffic are running through different public IPs, this flag is required. For more information on external network access, see <a href="#">Enabling External Network Access</a> .
<b>Domain</b>		
<code>--domain</code>	String	The AD domain that remote workstations will join.
<code>--sa-user</code>	String	The Active Directory service account username.
<code>--sa-password</code>	String	The Active Directory service account password.
<code>--domain-controller</code>	String	Specifies one or more domain controllers to use with the Connector.
<code>--users-filter</code>	String	The filter to search for users within Active Directory. Specify multiple filters with multiple options. Default user filter: (&(objectCategory=person)(objectClass=user)).
<code>--computers-filter</code>	String	The filter to search for computers within Active Directory. Specify multiple filters with multiple options. Default computer filter: (&(primaryGroupID=515)(objectCategory=computer)).
<code>--users-dn</code>	StringArray	The base DN to search for users within AD. Specify multiple DNs with multiple options. Newly provided base DN(s) will automatically replace previous base DN(s). This

Flag	Type	Description
		field is looking for user's within the user-defined DN and SGs.
<code>--computers-dn</code>	StringArray	The base DN to search for computers within AD. Specify multiple DNs with multiple options. Newly provided base DN(s) will automatically replace previous base DN(s).
<code>--sync-interval</code>	uint8	The interval (in minutes) for how often to sync AD users and computers with the AWM Service.
<b>MFA</b>		
<code>--enable-mfa</code>	String	Installs with multi-factor authentication enabled.
<code>--radius-server</code>	String	The FQDN or IP address of the RADIUS server to use for MFA. This flag is optional.
<code>--radius-port</code>	String	The RADIUS server port. If not specified, the default port (1812) is used. If <code>--radius-server</code> is specified then this flag is optional.
<code>--radius-secret</code>	String	The shared secret used for configuring RADIUS authentication. If <code>--radius-server</code> is specified then this flag is required.
<b>Certificates</b>		
<code>--ssl-key</code>	String	The full path and filename of the SSL key to use. The <code>--self-signed</code> flag overrides this flag.
<code>--ssl-cert</code>	String	The full path and filename of the SSL certificate (in PEM format) to use. The <code>--self-signed</code> flag overrides this flag.
<b>Federated Authentication</b>		
<code>--enable-oauth</code>	Boolean	Enables Oauth authentication. (Default=False)
<code>--id-provider-url</code>	String	Sets the identity provider URL. Example: <code>--id-provider-url https://provider-1234567890.okta.com</code> . This flag is required if <code>--enable-oauth</code> is true.
<code>--oauth-client-id</code>	String	Gets the Client ID from the Identity Provider. This flag is required if <code>--enable-oauth</code> is true.
<code>--fa-url</code>	String	



Flag	Type	Description
		The Federated Auth Broker URL. for example <a href="https://cac-vm-fqdn:port">https://cac-vm-fqdn:port</a>
<code>--oauth-flow-code</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
<code>--enable-entitlements-by-upn</code>	Boolean	Enables/Disables searching entitlements by UPN. This flag is not required for the Anyware Connector. It is supported for the Connector on Ubuntu for versions 164 or below.

### Connector Upgrade and Diagnose Issues

Several previous versions of Connector installers are no longer compatible with our latest infrastructure upgrades. When you run the update or diagnose commands with these older versions you may receive errors such as "Error response from daemon: GET <https://docker.cloudsmith.io/.....: unauthorized>" for example. If this occurs you need to download the latest version of the Connector installer from [here](#).

## ENABLING MFA WHILE UPDATING

You can enable MFA to the Connector with the `--enable-mfa` flag when performing an update:

```
sudo ./cloud-access-connector update --enable-mfa
```

You need to have the following information:

- RADIUS server IP address or FQDN.
- RADIUS shared secret for configuring RADIUS authentication.

If you do not provide the locations of your RADIUS server and RADIUS shared secret, you will be prompted to do so.

## REMOVING MFA WHILE UPDATING

You can disable MFA from the Connector with the `--disable-mfa` flag when performing an update:

```
sudo ./cloud-access-connector update --disable-mfa
```

## UPDATING SSL CERTIFICATES

Before updating SSL certificates, ensure that you are aware of the requirements for creating and updating certificates, see [Assigning a Certificate to the Connector](#). You can update your Connectors SSL certificate and key by running the following command and specifying your SSL certificate and SSL key information:

```
sudo ./cloud-access-connector update --ssl-cert path/to/cert --ssl-key path/to/key
```

### Certificate format

The SSL certificate must be a PEM file. A CRT formatted file will not work with the update command above.

This command will enable you to update your SSL certificate information without having to re-install the Connector. This command also enables you to change your self-signed certificate to a signed certificate.

### Domain Controller Certificates

If all DC certificates have expired, the Anyware Connector will stop working. An error indicator will display on the **Connectors** page when a Anyware Connector has a DC with expired certificates. A warning indicator that details the current state of the DC certs will display on the same page when a Anyware Connector has a certificate that less than a week away from expiring.

# Reference

## Configuring the Broker Response Timeout

The following section outlines how to increase and set the *BROKER\_MAX\_WAIT\_SECONDS* parameter for the Connector.

1. Make a copy of the *docker-compose.yaml* file by running the following command:

```
cp /opt/connector_data/docker-compose.yaml /opt/connector_data/docker-  
compose-new.yaml
```

2. Edit */opt/connector\_data/docker-compose.yaml* to add an environmental variable.

- If you have an active Security Gateway, find the *cm* service section and add the following parameter and enter a value in seconds:

```
BROKER_MAX_RESP_WAIT_SECONDS=<required_value>
```

- If you don't have an active Security Gateway, find the *cm* service section and add the following parameter and enter a value in seconds:

```
BROKER_MAX_RESP_WAIT_SECONDS=<required_value>
```

3. Update the Connector by running the following command:

```
cloud-access-connector update --compose-file /opt/connector_data/docker-  
compose-new.yaml
```

# Connector on RHEL

## Prerequisites

### Creating the Connector Server

This sections outline how to create the Connector servers on RHEL/Rocky Linux and other system requirements that are required to install and run the Connector.

#### Minimum Requirements

The following section outlines the minimum requirements for installing the Connector on Rocky Linux and RHEL. You need an operating system with the following specifications:

- Operating System: RHEL/Rocky Linux 8.x.
- Minimum 4GB RAM.
- 4 CPU
- Minimum 30 GB Storage
  - If you are using LVM and `/var` is mounted on a separate volume, that volume must have 30 GB or more. This is to ensure that the installation process succeeds and Anyware Connector can function at an optimum level.

#### Network Requirements

Once you have setup a dedicated Virtual Machine(VM) for the Connector, please ensure the following environment conditions are met:

- You must have access to the internet for an online installation. For Darksite installation see, [Installing the Connector on RHEL/Rocky Linux- Darksite Installation](#)
- The virtual machine must have ports TCP 443, and ports TCP/UDP 4172 enabled, Please check [Firewall Load Balancing Considerations](#) for additional port and firewall information.
- You must have console access to the virtual machine using SSH.
- The server must be able to resolve the AD domain.
- You must have superuser (sudo) privileges on the virtual machine.

- The networking configuration of the server (including the IP address) must not change while the Connector is operational.

### Firewall Configuration

Before you configure firewall, please ensure the following conditions are met:

- The Virtual Machine must have port TCP 443 and TCP/UDP 4172 enabled in its firewall rules
- Within virtual network in the VM, the Firewalld is configured properly for Anyware Connector to run within the Virtual Machine.
- You can confirm it by running the following command:

```
sudo systemctl status firewalld
```

If the firewalld status is 'active', make sure you execute the following commands to configure firewall correctly. If the firewalld status is 'inactive' and your organization does not require firewall on the Anyware Connector VM, then please skip the step below.

Commands to configure firewall:

```
sudo firewall-cmd --permanent --add-port=6443/tcp # virtual network flannel
sudo firewall-cmd --permanent --add-port=4172/tcp # PCoIP SG port
sudo firewall-cmd --permanent --add-port=4172/udp # PCoIP SG port
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
```

### Disable Swap

Connector is built on K3s, and it's strongly recommended to disable swap on a Linux system to avoid memory issue in a production environment. It is recommended to disable swap on a Linux system to avoid memory issue.

You can do the following to disable swap:

- If this is a new install and you want to disable swap permanently on the Connector server:
  - Edit the `/etc/fstab` file and add '#' in front of any line that contains the word 'swap'.

- If you have an existing Connector and is running into memory issue, run the following command to disable swap immediately. (This is not retained after a system reboot):

- `sudo swapoff -a`

If Swap is required for any reason, it should be greater or equal to the size of the RAM. There is no guarantee that it works, so it is strongly recommended to disable it.

### Enabling Connections over WAN

When the Connector server is accessed outside the domain, it should be configured for external access (this step is only required if you want to enable remote access to the workstations without requiring a VPN):

To enable external PCoIP connections:

- The remote server should have a public IP address. This can be done via bi-directional NAT mapping. During the installation, you should use the `--external-pcoip-ip` flag to set the IPv4 address for the Connector for external connections.
- By default `--enable-security-gateway` is set to true forcing all sessions to go through security gateway to allow external users to connect to their workstations, if your environment consists of internal users, the Security Gateway can be disabled by passing `--enable-security-gateway=false`.

### Verifying the Connector Server

To verify your Connector server network configuration, SSH into the machine and ping the domain and a remote workstation in the domain. You should get a successful response from both attempts:

```
ping <domain FQDN>
ping <remote workstation FQDN>
```

#### 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](#).

## Confirming the CIDR for Connector Cluster

Once the Connector server is verified, you need to confirm the CIDR for the Connector Cluster.

### Confirm the CIDR for Connector Cluster

- The default CIDR used for the Connector's k3s network are: 10.42.0.0/16, 10.43.0.0/16,10.43.0.10.
- The CIDR must not be in conflict with customer's enterprise network CIDRs, where the Connector Virtual Machine is accessible.
- If any of the default Connector Cluster's CIDR is in conflict, confirm the desired CIDRs to be used by Connector that are Not in conflict:
  - `--cluster-cidr` : this is to set cluster CIDR, default is 10.42.0.0/16.
  - `--service-cidr`: this is to set service CIDR, default is 10.43.0.0/16.
  - `--cluster-dns`: this is to set cluster dns ip address, default is 10.43.0.10, it has to be part of of the `--service-cidr`.
- Record the new CIDRs if the default is in conflict, they are required for Connector configuration during installation, For example, to change the cluster CIDR to 192.168.10.0 and service to 172.16.0.0. The configure command example: `sudo anyware-connector configure --cluster-cidr 192.168.10.0/24 --service-cidr 172.16.0.0/16 --cluster-dns 172.16.0.10.`

## DNS Name Resolution Configuration on RHEL/Rocky Linux

To install and configure Anyware Connector on the RHEL or Rocky Linux machine, its important to have a connection between the machine and the Active Directory Domain Controller.

Check that the DNS Name Resolution works as expected

1. Check the `/etc/resolv.conf` file to ensure that the desired DNS servers and search suffixes are present.

```
cat /etc/resolv.conf
# Generated by NetworkManager
search example-domain.com
nameserver 10.162.0.42
```

2. Test the DNS by pinging the Domain, in this example example-domain.com:

```
ping example-domain.com
```

3. If the response is successful, you should receive a message similar to the example below:

```
PING example-domain.com (10.162.0.42): 56 data bytes
64 bytes from 10.162.0.42: icmp_seq=0 ttl=118 time=16.622 ms
64 bytes from 10.162.0.42: icmp_seq=1 ttl=118 time=50.675 ms
64 bytes from 10.162.0.42: icmp_seq=2 ttl=118 time=27.682 ms
64 bytes from 10.162.0.42: icmp_seq=3 ttl=118 time=19.886 ms
^C
--- example-domain.com ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
```

4. Restart the Virtual Machine(VM) and check if the DNS settings in `/etc/resolv.conf` persist and that you can still ping the domain as shown in steps 2-3 above. If it does not work, please follow the steps in [Configure DNS Settings](#) below.



## Applying Host VM's DNS settings to K3S

The host Virtual Machine's DNS settings are copied from `/etc/resolv.conf` and applied to the Anyware Manager and/or Connector whichever is installed when the K3S service starts. Hence, it is important that settings are correct after a restart. You will either need to reboot the VM or restart the K3S service to apply the DNS settings to the Anyware Manager or Connector whichever is installed, if changes are made post installation or configuration.

### Configure DNS settings

If the DNS Name resolution work as expected, please skip the steps below.

To ensure DNS settings are configured properly on the machine for Anyware Manager or Connector to operate, please perform the following steps(the sample IP of the Domain Controller is 10.162.0.42 for `example-domain.com.`):

1. Disable auto-configuration of DNS settings bto prevent overwriting on reboot. In this example the device name is `eth0`.

```
nmcli device modify eth0 ipv4.ignore-auto-dns yes
```

You also need to disable this on the connection level in some cases. In this example the connection name is `eth0`.

```
nmcli connection modify eth0 ipv4.ignore-auto-dns yes
```

2. Add the DNS1 for the IP address for Active Directory's DNS server (typically the Domain Controller itself) and optionally DNS2 for fallback DNS server and optionally DOMAIN for a DNS suffix (typically the Domain name) in the network configuration scripts.

```
sudo vi /etc/sysconfig/network-scripts/ifcfg-eth0
TYPE=Ethernet
PROXY_METHOD=none
BROWSER_ONLY=no
BOOTPROTO=dhcp
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=yes
IPV6_AUTOCONF=yes
IPV6_DEFROUTE=yes
IPV6_FAILURE_FATAL=no
NAME=ens192
UUID=dfe16427-21f1-429c-99cb-a1e9b42be181
DEVICE=ens192
ONBOOT=yes
DNS1=10.162.0.42
DOMAIN=example-domain.com
PEERDNS=no
```

3. Restart the Network Manager.

```
sudo systemctl restart NetworkManager
```

4. Follow steps in the [Check that the DNS Name Resolution works properly](#) section to confirm the DNS name resolution works properly.

## Preparing Security Certificates

To ensure the communications between Anyware Connector and external entities are trusted and secured, the following certificates are required:

- Certificate for establishing LDAPs connection from Connector to AD , typically it is the DC certificate
- Certificate for the Connector to establish HTTPs connection from PCoIP client to Connector for Login
- Certificate for Anyware Manager to establish HTTPs connection from Connector to Anyware Manager installed locally

For testing purposes, there is option to bypass some of them, however it is recommended to have them for production use.

### DOMAIN CONTROLLER CERTIFICATES

#### Configuring *ldaps-ca-cert* Flag

Domain Controller Certificate is required for secure and trusted communication to the Active Directory using LDAPs. By default the certificate is signed by a private Certificate Authority(CA). However for the Connector to validate the certificate and communicate securely with the Active Directory the certificate should be signed by a Public Certificate Authority(CA). If verifying Active Directory certificate is required use `--ldaps-ca-cert` to pass Active Directory root certificate, in the case where validating the certificate is not required use `--ldaps-insecure flag` to skip verification.

Anyware Connector runs with the following supported Domain Controller servers:

- Windows 2016 Server with secure LDAP (LDAPS) enabled.
- Windows 2012 R2 Server with secure LDAP (LDAPS) enabled.
- Windows 2019 Server with secure LDAP (LDAPS) enabled.

It is recommended to provide Domain Controller or Domain's root certificate. Alternatively you can provide the public certificate for the leaf certificate for the Domain Controllers instead, leaf certificate is valid for a shorter time such as 1 year than the CA cert, which usually is valid for 5 years. For more information, see [How to create and install a self-signed certificate on a Windows 2016 Active Directory server to enable LDAPS](#).

If you don't have the CA cert, you can get the leaf certificate by running the following command:

```
openssl s_client -connect domain-controller.domain.com:636
```

Here the `domain-controller.domain.com` is the Domain Controller's Fully qualified domain name and 636 is the LDAPs port.

#### Configuring *ldaps-insecure* Flag

LDAPs with a root Certificate is the recommended way to use Anyware Connector. This way, communication from the Connector to the Active Directory is done using a secure TLS connection. If you do not wish to install the CA cert or want to skip certification verification for testing purposes, you can use `--ldaps-insecure` flag. This flag helps you establish a encrypted connection between the Connector and Active Directory however, that connection is not validated.

#### Configuring *enable-plaintext-ldap* Flag

For non production environment, LDAP could be used instead of LDAPs to avoid setting up certificates. LDAP is non secure protocol and message between the Connector and Active Directory are sent in plain text.

To enable the LDAP mode, use the following flag:

```
--enable-plaintext-ldap
```

#### Domain Controller certificates expiry

When all the LDAPs certificates expire, the Connector stops working and displays an error message on the Connectors page. Also, a warning message that details the current state of the certificates is displayed on the same page when a Connector has a certificate that is less than a week away from expiring.

## CONNECTOR TLS CERTIFICATE

Connector TLS certificate is required for secure and trusted connection between PCoIP client and Anyware Connector, you can bypass this using `--self-signed` (or `--insecure`) flag which will generate a self-signed certificate and key for the Connector. However, the PCoIP clients gets insecure warning when establishing a connection, which is recommended strictly only for testing purposes. For production use, you should assign a TLS certificate to the Connector during installation. This

prevents insecure connection errors when connecting to Anyware Connector, Anyware manager is not affected by this certificate.

## ANYWARE MANAGER CERTIFICATE

Anyware Manager Certificate could be required and obtained using `--manager-ca-cert` flag for secure and trusted connection from Connector to the Manager. You don't need to provide Anyware Manager certificate if:

- You are using Anyware Manager as it uses a certificate signed by a public CA
- You are using a trusted TLS certificates signed by a public CA when connecting to Anyware Manager.

If Anyware Manager is installed with self-signed certificate or a certificate signed by a public CA that is not trusted by the Connector, you need to provide Anyware Manager Certificate unless `--manager-insecure` flag is used to skip certificate validation for testing purpose.

For more information on supported certificate file format, see

## EXPECTED CERTIFICATE FILE

The certificate supported by the Connector has certain requirements. They are as follows:

The Anyware Connector supports the certificate file in the following form:

- A certificate in the **PEM** format as shown below:

```
-----BEGIN CERTIFICATE-----  
base64encodedcertdata  
-----END CERTIFICATE-----
```

- A certificate file including only a single certificate. For example: - A single self-signed certificate - A root CA certificate - A single leaf certificate that is signed by an existing root CA

The Anyware Connector doesn't support the certificate file in following form:

- A bundle certificate that includes multiple certificates such as root, intermediate, or leaf certificate.
- Leaf certificate that is signed by a different or an untrusted root CA by the Connector.

# Installing the Connector on RHEL/Rocky Linux

You can configure the firewall, setup the system, download and install the Anyware connector on RHEL/Rocky Linux. If you are currently using Connector on Ubuntu, it is important to read and understand the differences Connector on RHEL/Rocky Linux introduced, To find out the side by side comparison, see [Difference between Anyware Connector on Ubuntu and RHEL/Rocky Linux](#).

The following sections outlines how to download and install the Connector on **Rocky Linux and RHEL**. There are five main steps involved in this process:

1. [Adding the Connector repository](#)
2. [Configuring the SELinux components](#)
3. [Installing the RPM](#)
4. [Generating the Connector Token](#)
5. [Configuring the Connector](#)

## Anyware Connector Installation Wizard Beta section

You can install the Anyware Connector from the Admin Console using the new installation wizard. The new Connector installation wizard is currently a part of the Beta section. For more information, see [Anyware Connector New Installation Wizard](#).

## 1. Adding the Connector Repository

The virtual machine you are adding the repo to must have access to the internet. If it doesn't, you cannot download and install the required files.

### CHECKING EXISTING REPOSITORIES FOR ANYWARE CONNECTOR

If the Anyware Connector was installed previously on your virtual machine, there could be existing repos related to it on your system. Run the command below to check all existing repos related to Anyware Connector (Skip this step if Anyware Connector was never installed on your virtual machine).

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

Check the current Anyware Connector repo to make sure it is the desired repo that you want to use for installation. If there are unwanted repositories on your VM, see [Repository Management](#) to remove them.

## ADDING A REPOSITORY

To access the scripts and configure the RHEL and Rocky Linux repository, select the Downloads and scripts option [here](#) and select the **Anyware Connector (RHEL/Rocky Linux)** option. Click **Downloads and scripts** and copy the script to add the Connector repo.

Once you have copied the curl command you need to run it to download the repository.

## 2. Configuring SELinux Policies

The following SELinux policies enable persistent storage and container logging on the Connector. If SELinux policies are not found, data stored in the Connector will be lost when the virtual machine is shut down.

Once configured, and the installation has verified SELinux, all Connector related data persists when the target machine hosting the Connector 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 `selinux` is already running on your system. If it is not, then you need to run the following commands to install the SELinux policies:

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

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

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

```
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
```

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

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

### 3. Installing the Connector RPM

Once you have installed and configured the SELinux policies you must install the Connector RPM and configuration files.

Run the following command to install the Connector RPM, the sample configuration files will be generated once the install is done:

```
sudo dnf install -y anyware-connector
```

### 4. Generating a Connector Token

You must generate a Connector token using the Admin Console. The steps outlined below must be performed on the target virtual machine.

You need to create or have created a deployment prior to obtaining a token. For information on how to log into the Admin Console, see [Admin Console Connection](#). The following section outlines how to obtain a Connector token using the Admin Console:

1. Click **Connectors** from the console sidebar.



2. Click the add connector button (+ sign located beside **Connectors** heading) to display the connector creation panel.
3. Enter the following information:
  - Select the deployment you want to add the Connector to. If you do not have an existing deployment you need to create one.
  - Enter the name of the Connector.

- Follow the step by step instructions outlined below.

### SELECT A DEPLOYMENT

Deployment name

Test\_Teradici\_1

### DEFINE THE CONNECTOR

Connector name

Test\_Connector\_01

The length is 2 to 32 and character: ~!@#\$%^&\*()|+=~?;:~",.<>{}[]/ is not allowed.

#### Private cloud install instructions

- 1. Create the Cloud Access Connector server**

Create a dedicated Ubuntu server for GCP, AWS, and Private Cloud with the necessary specifications.
- 2. Verify the Cloud Access Connector server**

You need to SSH into the machine and ping the domain and a remote workstation in the domain to verify.
- 3. Enable external access**


Only required if you want to enable remote access to the workstations without requiring a VPN.
- 4. Download the Cloud Access Connector server**

Follow 2 simple steps to connect to the machine and download the Connector installer.
- 5. Get connector token**
- 6. Install the Cloud Access Connector**

When the installer completes, the IP address of the Cloud Access Connector will be displayed.

(token is only valid for 2 hours.)

eyJhbGciOiJIUzUxMiIsInR5cCI6IkpXVCJ9.eyJjb25uZWN0b3JOYW1



4. Click **GENERATE**.
5. Copy the Connector token by click the copy icon.
6. Click **CLOSE** the exit the panel.

You can now use this Connector token when prompted during installation.

## 5. Configuring the Connector-Example Commands

The following section provides example configuration commands for configuring the Connector with Anyware Manager as a Service. These example commands use flags, but the same parameters can be configured using the configuration files also.

### CONFIGURING THE CONNECTOR FOR ANYWARE MANAGER AS A SERVICE


Once you have installed the Connector RPM, and have generated a Connector token from the Anyware Manager as a Service, run the following commands to configure the Connector to work with the Anyware Manager as a Service. The first line for these commands maps the Connector token to a variable in the shell, the ' ' for the string values are not required if there are no special chars in the string.

#### Minimum Configuration Sample Command for Quick Start

The following command with dummy values configures a Connector with minimum flags to work with the Anyware Manager in your enterprise network. Communications with external integrations such as PCoIP clients, Active Directory server, etc are not secure without certificate validation, this should only be used for testing purpose.

```
export token=<token from Anyware Manager Admin Console>
/usr/local/bin/anyware-connector configure \
--token $token \
--domain 'testlab.internal' \
--accept-policies \
--enable-ad-sync=false \
--ldaps-insecure
```

You can use the minimum command for testing or base installation excluding additional configurations. When editing a workstation, you should manually add workstations from the Admin Console and add a user assignment by the user's UPN as the domain users or computers are synced.

 **The ability to manually add a user assignment by the user's UPN is supported only in Anyware Manager as a Service combined with Anyware Connector RHEL/Rocky Linux 23.06 or later or Ubuntu Connector version 164 or later.**

## Typical Configuration Sample Command

```
export token=<token from Anyware Manager Admin console>
/usr/local/bin/anyware-connector configure \
--token $token \
--domain 'testlab.internal' \
--sa-user 'sampleuser' \
--sa-password 'Passwordstring' \
--ldaps-ca-cert '/home/rocky/DC-Cert.pem' \
--computers-dn 'CN=Computers,DC=testlab,DC=internal' \
--users-dn 'CN=Users,DC=testlab,DC=internal' \
--self-signed \
--accept-policies \
--debug
```

- If this is the first Connector installed in the deployment, use `--computers-dn` and/or `--users-dn` flags to sync AD objects to Anyware Manager. The additional Connector in the same deployment can pull the DN(s) configuration from Anyware Manager without needing to provide these flags. If these flags are not provided the Active Directory sync will sync all objects from the Active Directory to the Anyware Manager.
- If `--self-signed` flag is not used, you must use `--tls-key` and `--tls-cert` flags to provide the full path and filename of the TLS key and PEM formatted TLS certificate to use.
- If `--ldaps-ca-cert` flag is not used, you should use either `--ldaps-insecure` to skip certificate validation, or `--enable-ldap-plaintext` to use LDAP instead of LDAPS for test purposes.

Ensure that you use the options and flags that best suit your system architecture and requirements. If required values are not provided on the command line, you will be prompted for them. For additional flags and options, see [Installation Flags and Options](#).

### Anyware Connector - Troubleshooting

If there is an issue installing the Anyware Connector or an existing Connector is failing, please see the troubleshooting section on [Anyware Connector Connectivity](#). Within this section there are steps to check the following:

- Remote Workstation connections
- Active Directory connections
- Anyware Connector component information

For information on installer errors related to a change in the distribution system, see [here](#).

## ADDITIONAL CONFIGURATIONS FOR THE ANYWARE CONNECTOR

### Multi-Factor Authentication

When you enable MFA for the Connector for RHEL/Rocky Linux, all PCoIP Clients authenticated through the Connector are prompted to enter MFA credentials. Previously, only the external PCoIP Clients were prompted for MFA information.

#### Multi-Factor Authentication for the Connector

When installing the Connector you can enable multi-factor authentication (MFA) by running the `--enable-mfa` flag. MFA is disabled by default. If you want MFA to only apply to external connections, you should have separate Connectors. One Connector should be for external connections, where MFA is enabled, and one for internal or direct connections, where MFA is disabled. For steps on how to install the Connector with MFA bypassed for internal connections, see [Installing the Connector for Internal Connections](#). For steps on how to install the external Connector, see [Installing the Connector for External Connections](#).

Ensure that you use the options and flags that best suit your system architecture and requirements. If required values are not provided on the command line, you will be prompted for them. For additional flags and options, see [Installation Flags and Options](#).

### Installing the Connector for Internal Connections

The following steps outline how to install the Connector for internal connections to bypass MFA:

1. Prepare a virtual machine in your private network that meets the [system requirements](#) with the following sub-steps:
  - Skip the step for preparing the system for external access.
  - Skip the step for setting up MFA.
2. Install the Connector with the following sub-steps:
  - If you don't have external users, then you could disable security gateway by passing `--enable-security-gateway=false`, otherwise it's set to true enabled by default.
  - Do not set the Public IP using the `--external-pcoip-ip` flag. The Connector will instead return the virtual machines IP address.
  - No MFA flag is required as MFA is disabled by default.

3. Once you have installed the Connector connect to a remote workstation with a [PCoIP Software Client](#) with the following sub-step:

- In the *Host Address or Code* field enter the private IP of the internal Connector you just installed and log-in.

#### Installing the Connector for External Connections

The following steps outline how to install the Connector for external connections:

1. Prepare a virtual machine in your private network that meets the [system requirements](#) with the following sub-steps:

- Skip the step for preparing the system for internal access.

2. Install the Connector with the following sub-steps:

- Set the Public IP using the `--external-pcoip-ip` flag.

3. Once you have installed the Connector, connect to a remote workstation with a [PCoIP Software Client](#) with the following sub-step:

- In the *Host Address or Code* field enter the IP address or DNS name of the external Connector you just installed and log-in.

#### Updating CIDR for Connector Cluster

The default CIDR for Connector Cluster are as follows:

- 10.42.0.0/16 cluster CIDR
- 10.43.0.0/16 Service CIDR
- 10.43.0.10 Cluster DNS

If the default CIDRs conflict with your internal network, use the following flags to update the cluster with different CIDR.

To update, run the following command:

```
sudo anyware-connector configure --cluster-cidr <IP Address> --service-cidr <IP Address> --cluster-dns <IP Address>
```

Example Command with dummy values:

```
sudo anyware-connector configure --cluster-cidr 192.168.10.0/24 --service-cidr 172.16.0.0/16 --cluster-dns 172.16.0.10
```

-->

## 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:

### Groups of flags

The flags are here categorized by their configuration groups:

### States for Boolean Flags

The state of all the Boolean Flags is interpreted as follows: "--boolean-flag" means "true". "--boolean-flag=true" means "true". "--boolean-flag=false" means "false". "--boolean-flag anytext" uses default as "true".

## Anyware Manager

Configuration File Parameter	Flag	Description
<i>caCertPath</i>	<code>--manager-ca-cert</code>	Enables users to supply a CA certificate for Anyware Manager to enable the Connector to trust the certificate in order to connect to the Anyware Manager instance.
<i>insecure</i>	<code>--manager-insecure</code>	This flag is required when the Connector is connecting to a Anyware Manager instance that is using self-signed certificates, and you want to turn off the verification of the certificate.
<i>url</i>	<code>--manager-url</code>	This flag is required for Anyware Manager, Specifies the Anyware Manager URL that the Connector connects to. If this is not specified it points to <a href="https://cas.teradici.com">https://cas.teradici.com</a> by default, which is the URL for Anyware Manager as a Service.
<code>--pull-connector-config</code>	Boolean	This flag gets the Connector configuration from the Anyware Manager.
<code>--push-connector-config</code>	Boolean	This flag saves the Connector configuration into the Anyware Manager.



## PCoIP Software Client Flags

Configuration File Parameter	Flag	Description
<code>showAgentState</code>	<code>--show-agent-state</code>	<p>This flag controls if the agent state is displayed as part of the remote workstation name in the PCoIP Client.</p> <p>The default value for this flag is true. Setting the value of this flag to true and the <code>--retrieve-agent-state</code> flag to false results in no agent state displaying. A boolean parameter.</p>
<code>retrieveAgentState</code>	<code>--retrieve-agent-state</code>	<p>Enables the broker to retrieve the agent state for unmanaged and managed remote workstations.</p> <p>The default value for this flag is false. The available states are <b>In Session, Ready, Starting, Stopping, Stopped</b> and <b>Unknown</b>. The value of this flag can either be true or false. A boolean parameter.</p>
<code>ip</code>	<code>--external-pcoip-ip</code>	<p>Sets the public IP for PCoIP Client to PCoIP Agent connection. This is the public IP that the Connector is listening to on port 4172. The installer reaches out to <code>cas.teradici.com</code> and try to automatically resolve the external IP;</p> <p>if this fails, the <code>--external-pcoip-ip</code> flag is required. In the case that the Connector machine doesn't have an internet connection, for example in a dark site environment, or the ingress and egress internet traffic are running through different public IPs, this flag is required. For more information on external network access, see <a href="#">Enabling External Network Access</a>. A string parameter.</p>

## Connector

Configuration File Parameter	Flag	Description
<i>acceptPolicies</i>	<code>--accept-policies</code>	Automatically accept the <a href="#">EULA</a> and <a href="#">Privacy Policy</a> .
<i>token</i>	<code>--token (-t)</code>	Required. The token generated from Anyware Manager for Connector to create a service account to connect to Anyware Manager.
<i>licenseServerUrl</i>	<code>--local-license-server-url</code>	Lets the URL for PCoIP License Server to be used for PCoIP Sessions. If this is not provided, ensure that the Cloud License Server is registered on the PCoIP Agent. Example: <code>--local-license-server-url http://10.10.10.10:7070/request</code> . For more information on the PCoIP License Server, see <a href="#">PCoIP License Server</a> . A string parameter.
<i>enableSecurityGateway</i>	<code>--enable-security-gateway</code>	By default the security gateway for external traffic is set to true. For internal traffic disable this feature using the <code>--enable-security-gateway=false</code> flag.
<i>clear</i>	<code>--clear</code>	Forces new configuration of Anyware Connector.

## Connector/Diagnosis

Configuration File Parameter	Flag	Description
<i>anywareConnectorDiagnose</i>	<code>--diagnose</code>	This flag executes the diagnostic checks for Anyware Connector.
<i>anywareConnectorHealth</i>	<code>--health</code>	This flag generates reports for Anyware Connector's health status.
<i>maintenanceModeOn</i>	<code>--diagnose --maintenance-mode on</code>	This mode sets the Connector in maintenance mode and no new sessions are accepted.
<i>maintenanceModeOff</i>	<code>--diagnose --maintenance-mode off</code>	This flag turns off the Connector maintenance mode and new sessions are accepted.

## Connector/certificates

Configuration File Parameter	Flag	Description
<i>selfSigned</i>	<code>--self-signed</code>	This mode is not secure and intended for testing only. PColP client will receive a untrusted warning when connecting to the Connector. The previous <code>--insure</code> flag is still supported
<i>keyPath</i>	<code>--tls-key</code>	The full path and filename of the TLS key to use. The <code>--self-signed</code> flag overrides this flag. A string parameter.
<i>certPath</i>	<code>--tls-cert</code>	The full path and filename of the TLS certificate (in PEM format) to use. The <code>--self-signed</code> flag overrides this flag. A string parameter.
<i>trustCustomerLicenseCert</i>	<code>--trust-customer-license-cert</code>	Trusted customer license certificate path.
<i>trustCustomerLicenseKey</i>	<code>--trust-customer-license-key</code>	Trusted customer license key path.

## Connector/multifactorAuthentication

Configuration File Parameter	Flag	Description
<i>enable</i>	<code>--enable-mfa</code>	This flag can be used if you wish to enable multi-factor authentication. Multi-factor authentication will be enabled for all connections, both internal and external. Internal users will be required to enter the multi-factor authentication code for the Connector when connecting to the PCoIP Client. It is recommended to install separate Connectors for internal vs external connections. A boolean parameter.
<i>port</i>	<code>--radius-port</code>	This is the RADIUS server port. If not specified, the default port (1812) is used. If <code>--radius-server</code> is specified, then this flag is optional. A string parameter.
<i>server</i>	<code>--radius-server</code>	The FQDN or IP address of the RADIUS server to use for MFA. This flag is optional. A string parameter.
<i>sharedSecret</i>	<code>--radius-secret</code>	The shared secret used for configuring RADIUS authentication. If <code>--radius-server</code> is specified then this flag is required. A string parameter.

## deployment/domain/DomainName

Configuration File Parameter	Flag	Description
<i>name</i>	<code>--domain</code>	The AD domain that the remote workstations will join. A string parameter.

## deployment/domain/domainControllers

Configuration File Parameter	Flag	Description
<i>domainControllers</i>	<code>--domain-controller</code>	This flag specifies one or more domain controllers to use with the Connector. To specify multiple domain controllers use the following format: <code>--domain-controller dc1.domain.com, --domain-controller dc2.domain.com, --domain-controller dc3.domain.com</code> . A string parameter.

## deployment/domain/serviceAccount

Configuration File Parameter	Flag	Description
<i>userName</i>	<code>--sa-user</code>	The AD service account username. A string parameter.
<i>password</i>	<code>--sa-password</code>	The AD service account password. A string parameter.

## deployment/domain/adSynch

Configuration File Parameter	Flag	Description
<i>computerDns</i>	<code>-- computers- dn</code>	The base DN to search for computers within AD for AD sync. Can specify multiple DNs with multiple options. See the differences between the Connectors at the top of this page for details. Newly provided base DN(s) will automatically replace previous base DN(s).
<i>computerFilters</i>	<code>-- computers- filter</code>	The filter to search for computers within Active Directory. Specify multiple filters with multiple options. Default computer filter: (&(primaryGroupID=515)(objectCategory=computer)). A string parameter.
<i>usersDns</i>	<code>--users-dn</code>	The base DN to search for users within AD. Specify multiple DNs with multiple options. Newly provided base DN(s) will automatically replace previous base DN(s). The base DN to search for computers within the AD for AD sync. You can specify multiple DNs with multiple options. See the table above on the differences between the Connectors for more information. Newly provided base DN(s) will automatically replace previous base DN(s). A string array parameter.
<i>usersDns</i>	<code>--users-dn</code>	The base DN to search for users within AD. Specify multiple DNs with multiple options. Newly provided base DN(s) will automatically replace previous base DN(s). The base DN to search for computers within the AD for AD sync. You can specify multiple DNs with multiple options. See the table above on the differences between the Connectors for more information. Newly provided base DN(s) automatically replaces previous base DN(s). A string array parameter.
<i>usersFilters</i>	<code>--users- filter</code>	The filter to search for users within Active Directory. Specify multiple filters with multiple options. Default user filter: (&(objectCategory=person)(objectClass=user)). A string parameter.
<i>interval</i>	<code>--sync- interval</code>	The interval (in minutes) for how often to sync AD users and computers with the CASM Service. A uint8 parameter.
<i>adSync</i>	<code>--enable- ad-sync</code>	Enable Active Directory synchronisation. A boolean value (Default=True).

## deployment/domain

Configuration File Parameter	Flag	Description
<i>caCertPath</i>	<code>--ldaps-ca-cert</code>	To supply a CA certificate for the connection to AD over LDAPS. A string parameter.
<i>insecure</i>	<code>--ldaps-insecure</code>	Skip certificate validation when connecting to the Active Directory using LDAPS. This option should only be used when connecting to the Active Directory deployed with self signed certificates. This will be ignore if a CA cert is provided.
<i>enableLdapMode</i>	<code>--enable-plaintext-ldap</code>	Connections to Active Directory will be made using plaintext LDAP instead of encrypted LDAPS. This is meant only for testing, do NOT use it in production.
<i>poolGroups</i>	<code>--pool-group</code>	Specifies one or more Active Directory groups, by entering the distinguished name (DN), to be assigned to pools for remote workstation management (eg, <code>--pool-group 'CN=GroupPool1,CN=Users,DC=sample,DC=com'</code> <code>--pool-group 'CN=GroupPool2,CN=Users,DC=sample,DC=com'</code> ). A string parameter.
N/A	<code>--preferred-name</code>	This is an optional flag to determine if the hostname or machine name should be displayed to identify the remote workstations, the default is set to display machine name.

## Federated Authentication

Configuration File Parameter	Flag	Description
<code>--enable-oauth</code>	Boolean	Enables Oauth authentication. (Default=False)
<code>--id-provider-url</code>	String	Sets the identity provider URL. Example: <code>--id-provider-url https://provider-1234567890.okta.com</code> . This flag is required if <code>--enable-oauth</code> is true.
<code>--oauth-client-id</code>	String	Gets the Client ID from the Identity Provider. This flag is required if <code>--enable-oauth</code> is true.
<code>--fa-url</code>	String	The Federated Auth Broker URL. for example <a href="https://cac-vm-fqdn:port">https://cac-vm-fqdn:port</a>
<code>--oauth-flow-code</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
<code>--enable-entitlements-by-upn</code>	Boolean	Enables/Disables searching entitlements by UPN. This flag is not required for the Anyware Connector. It is supported for the Connector on Ubuntu for versions 164 or below.

## Federated Authentication With Single Sign-On

Configuration File Parameter	Flag	Description
<code>--sso-signing-csr-ca</code>	String	Path to copy intermediate CA Certificate.
<code>--sso-signing-csr-key</code>	String	Path to the intermediate key.
<code>--sso-signing-crl</code>	String	Path to a certificate revocation list.
<code>--sso-enrollment-url</code>	String	Gets the URL to the Active Directory Certification Authority Web Enrollment Service.
<code>--sso-enrollment-domain</code>	String	Domain of the user to access Active Directory Certification Authority Web Enrollment Service.
<code>--sso-enrollment-username</code>	String	Username for accessing Active Directory Certification Authority Web Enrollment Service.
<code>--sso-enrollment-password</code>	String	Password for the username to access Active Directory Certification Authority Web Enrollment Service.
<code>--sso-enrollment-certificate-template-name</code>	String	Name of the certificate template that Active Directory Certificate Services (AD CS) uses to sig CSR.



These configuration parameters are only applicable for the Connector on RHEL/Rocky Linux.

### Troubleshooting the Connector

If you encounter issues when attempting to install the Connector, please see the Troubleshooting section for information on how to potentially diagnose the specific issue. You can also view the following KB article [here](#) which provides a list of troubleshooting steps for common issues related to installing the Connector. For information on installer errors related to a change in the distribution system, see [Installer Issues](#).

## 6. Connecting to a Remote Workstation with a PCoIP Client

After successfully installing a Connector, you can initiate a session to connect to a remote workstation with a PCoIP Software Client. We enable customers to use multi-factor authentication for these PCoIP Client sessions. The following steps outline how to connect to a remote workstation using the PCoIP Software Client:

1. Double-click the PCoIP Client desktop icon or program file `PCoIPClient` to launch the application.
2. In the *Host Address or Code* field, enter one of the following:
  - For direct connections, provide the address of the host machine.
  - For managed connections, provide the address of the connection manager.
3. Click **NEXT**.
4. Select your domain and enter the credentials for the remote workstation. If you have enabled MFA then you will be prompted for the 2<sup>nd</sup> factor passcode. The method of how this passcode is communicated depends on the provider you used. It is usually either a One Time Password or push notification.
5. Click **LOGIN**.
6. If your login is successful you should be able to select the remote workstation and connect to it. Please note that if you have a single remote workstation, that remote workstation is automatically selected and the connection is initiated immediately. In this case you will not be presented with a remote workstation selection screen.

For more information about the PCoIP Software Client, please see the following PCoIP Software Client guides:

- [PCoIP Software Client for Windows](#)

- [PCoIP Software Client for macOS](#)
- [PCoIP Software Client for Linux](#)

## Upgrading the Connector on RHEL/Rocky Linux

The Anyware connector on RHEL/Rocky Linux can be upgraded in a 2-step process outlined as follows:

### Upgrading a Connector

It is not possible to upgrade a Connector installed on Ubuntu to a Connector installed on RHEL or Rocky Linux. To replace a Connector installed on Ubuntu, you must install the RHEL/Rocky Linux Anyware Connector on a new virtual machine and configure it exactly the same as the existing Connector on Ubuntu.

1. You must install the new version of the Connector RPM:

```
sudo dnf upgrade -y anyware-connector
```

2. Run the following command to upgrade the Connector with the current configuration:

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

Once you have successfully upgraded the Connector you should see a response similar to the example output outlined below.

```
sudo /usr/local/bin/cas-connector upgrade
INFO Starting cas-connector version=22.04.0-rc0-18-g5825b44 built on 2022-01-26
INFO Upgrading
INFO Extracting Manifest
WARN namespaces "connector" already exists
WARN namespaces "ingress-nginx" already exists
WARN namespaces "logging" already exists
INFO Beginning Upgrade
INFO Deploying CAS Connector service
INFO Deploying Cloud Access Software Connector. This process usually takes 5 to 10 minutes to complete
INFO Performing Cloud Access Software Connector health probe. This process usually takes 1 to 5 minutes to complete
INFO ***** Connector installation complete *****
INFO The IP address of your connector ip=
INFO Please visit CAS Manager to further manage your connector Cloud Access Software Connector Url=https://10.0.0.2
```

# Reference

# Anyware Connector Features

Items	Connector on RHEL/Rocky Linux
<b>Operating System</b>	RHEL/Rocky Linux 8.x
<b>Packaging</b>	RPM Package
<b>Deployment</b>	Kubernetes
<b>Connector Configuration</b>	Configuration files and/or command line flags and parameters.
<b>Required Configuration Flags</b>	<pre>--token --domain --sa-user --sa-password --accept-policies --self-signed (or --tls-key and --tls-cert must be provided) --ldaps-ca-cert (or --ldaps-insecure or --enable-ldap-plaintext)</pre>
<b>MFA Configuration</b>	All connection requests both internal and external will require MFA credentials to be entered.
<b>Active Directory Synchronization</b>	If computer ( <code>--computers-dn</code> ) and/or users DNs ( <code>--users-dn</code> ) parameters are not provided during installation, and no AD configuration is returned from Anyware Manager, Active Directory sync will sync all objects from the Active Directory to the Anyware Manager.
<b>Active Directory LDAPS Certificate</b>	<p>The Active Directory CA certificate must be provided to the installer by entering the information with the <code>--ldaps-ca-cert</code> parameter or by setting it in the configuration file.</p> <p>Skip the certificate validation when connecting to the Active Directory using the following flag <code>--ldaps-insecure</code>.</p> <p>For testing purposes the AD connection can use ldap in the plaintext form with the <code>--enable-ldap-plaintext</code> flag.</p>
<b>Diagnose Commands</b>	Diagnose commands has two flags <code>--health</code> to check the overall status of Anyware Connector and <code>--support-bundle</code> to generate support bundle.
<b>Key path and Certificate path flag</b>	<code>--tls-key</code> and <code>--tls-cert</code>
<b>Installation Commands</b>	<p>Add the repository and install the Connector RPM with the following command: <code>sudo dnf install -y anyware-connector</code>.</p> <p>Configure the Connector with flags or configuration files using the following command: <code>sudo /usr/local/bin/anyware-connector configure {flags or path to config file}</code>.</p> <p>The <code>configure</code> command fails with a missing parameter error if the mandatory flags or</p>

Items	Connector on RHEL/Rocky Linux
	<p>parameters are missing, the mandatory flags are <code>--token</code>, <code>--domain</code>, <code>-sa-user</code>, <code>--sa-password</code>, <code>--ldaps-ca-cert</code> (or must provide <code>ldaps-insecure</code> or <code>--enable-ldap-plaintext</code>), <code>--self-signed</code> (or must provide <code>--tls-key</code> and <code>--tls-cert</code>).</p>
<p><b>Update Configuration</b></p>	<p>Update the configuration using: <code>sudo /usr/local/bin/anyware-connector configure {flags or path to config file}</code> command.</p>
<p><b>Upgrade Commands</b></p>	<p><code>sudo dnf update anyware-connector</code> and <code>sudo /usr/local/bin/anyware-connector upgrade</code></p>
<p><b>Internal/External Session Detection</b></p>	<p>In most cases the Connector on RHEL/Rocky Linux works without any special configuration, but if you know the Connector on RHEL/Rocky Linux is only for LAN connections, it is recommended to set the <code>--enable-security-gateway</code> flag to false by using <code>--enable-security-gateway=false</code>.</p>

## **Difference between Anyware Connector on Ubuntu and RHEL/Rocky Linux**

Anyware Connector on RHEL/Rocky Linux stands out from the Connector on Ubuntu. Here is a feature comparison between two Connectors.



Items	Connector on Ubuntu	Connector on RHEL/Rocky Linux
<b>Operating System</b>	Ubuntu 18.04	RHEL/Rocky Linux 8.x
<b>Packaging</b>	tar file	RPM Package
<b>Deployment</b>	Docker Swarm	Kubernetes
<b>Connector Configuration</b>	Configuration files and/or command line flags and parameters.	Configuration files and/or command line flags and parameters.
<b>Required Configuration Flags</b>	<pre>--token --domain --sa-user sa-password --accept-policies --self-signed (or --ssl-key and --ssl-cert)</pre>	<pre>--token --domain --accept-policies --enable-ad-sync=false --ldaps-insecure (or --ldaps-ca-cert or --enable-ldap-plaintext) --external-pcoip-ip 'public.ipv4.sg.ip'</pre>
<b>MFA Configuration</b>	When MFA is enabled all connection requests from internal PCoIP Clients have MFA bypassed.	All connection requests both internal and external will require MFA credentials to be entered.
<b>MFA Configuration</b>	When MFA is enabled all connection requests from internal PCoIP Clients will have MFA bypassed.	All connection requests both internal and external will require MFA credentials to be entered.
<b>Active Directory Synchronization</b>	If computer ( <code>--computers-dn</code> ) and/or users DNs ( <code>--users-dn</code> ) parameters are not provided during installation, and no Active Directory configuration is returned from Anyware Manager, Active Directory sync will sync all objects from the Active Directory to the Anyware Manager.	If computer ( <code>--computers-dn</code> ) and/or users DNs ( <code>--users-dn</code> ) parameters are not provided during installation, and no Active Directory configuration is returned from Anyware Manager, Active Directory sync will sync all objects from the Active Directory to the Anyware Manager.
<b>Active Directory LDAPS Certificate</b>	If <code>--ldaps-ca-cert</code> is not provided during installation, the Active Directory CA certificate is automatically collected by the Connector by	The Active Directory CA certificate must be provided to the installer by entering the information with the <code>--ldaps-ca-cert</code> parameter or by editing the configuration file. Skip the certificate validation when connecting to the

Items	Connector on Ubuntu	Connector on RHEL/Rocky Linux
	connecting to each DC on the LDAPS port, and the certificate is saved to the Connectors CA certificate store.	Active Directory using the following flag <code>--ldaps-insecure</code> . For testing purposes the Active Directory connection can use ldap in the plaintext form with the <code>--enable-ldap-plaintext</code> flag.
<b>Active Directory Service Accounts</b>	The Active Directory service account username and password is required.	The Active Directory service account is optional.
<b>Diagnose Commands</b>	You can diagnose remote workstation connectivity, and Active Directory connectivity by running the <code>diagnose</code> command.	Diagnose commands has two flags <code>--health</code> to check the overall status of Anyware Connector and <code>--support-bundle</code> to generate support bundle.
<b>Key path and Certificate path flag</b>	<code>--ssl-key</code> and <code>--ssl-cert</code>	<code>--tls-key</code> and <code>--tls-cert</code>
<b>Installation Commands</b>	Download the installer from teradici.com and extract the package, then run the install command with the required flags: <code>sudo /usr/sbin/cloud-access-connector install {flags}</code> . The installer will then prompt for mandatory flags if you do not provide them in the command.	Add the repository and install the Connector RPM with the following command: <code>sudo dnf install -y anyware-connector</code> . Configure the Connector with flags or configuration files using the following command: <code>sudo /usr/local/bin/anyware-connector configure {flags or path to config file}</code> . The <code>configure</code> command will fail with a missing parameter error if the mandatory flags or parameters are missing, the mandatory flags are <code>--token</code> , <code>--domain</code> , <code>--sa-user</code> , <code>--sa-password</code> , <code>--self-signed</code> (or must provide <code>--tls-key</code> and <code>--tls-cert</code> ), <code>--ldaps-ca-cert</code> (or <code>--ldaps-insecure</code> or <code>--enable-ldap-plaintext</code> ).
<b>Update Configuration</b>	<code>cd /usr/sbin sudo cloud-access-connector update {flags to be updated}</code>	Update the configuration using: <code>sudo /usr/local/bin/anyware-connector configure {flags or path to config file} command</code> .
<b>Upgrade Commands</b>	<code>cd /usr/sbin sudo cloud-access-connector update {flags to be updated}</code>	<code>sudo dnf update anyware-connector</code> and <code>sudo /usr/local/bin/anyware-connector upgrade</code>

Items	Connector on Ubuntu	Connector on RHEL/Rocky Linux
<p><b>Internal/External Session Detection</b></p>	<p>Typically the Connector on Ubuntu works without any special configuration, but in some cases you may need to explicitly set the <code>--internal-client-cidr</code> and <code>--external-client-cidr</code> so that sessions get treated correctly (eg, NATing external connections from a Firewall).</p>	<p>In most cases the Connector on RHEL/Rocky Linux works without any special configuration, but if you know the Connector on RHEL/Rocky Linux is only for LAN connections, it is recommended to set the <code>--enable-security-gateway</code> flag to false by using <code>--enable-security-gateway=false</code></p>
<p><b>Connector Cluster Network</b></p>	<p><code>--connector-network-cidr</code> is the CIDR flag to use for the Connector's docker network. The default docker network subnet is 10.101.0.0/16.</p>	<p>There are three flags to use for the Connector's network. They are; <code>--cluster-cidr</code> to set cluster CIDR,default is 10.42.0.0/16, <code>--service-cidr</code> to set service CIDR, default is 10.43.0.0/16. and <code>--cluster-dns</code> to set cluster dns ip address, default is 10.43.0.10, it has to be part of of the service-cidr.</p>

## Transitioning Anyware Connectors

It is not possible to migrate directly from the Anyware Connector on Ubuntu to the Anyware Connector on RHEL/Rocky Linux as they run on different operating systems. The best method to transition to the Connector on RHEL/Rocky Linux is to create this new Connector using the same Anyware Manager deployment you used for the Connector on Ubuntu.

### Minimize Transition Downtime

The Connector on RHEL/Rocky Linux can co-exist with the Connector on Ubuntu in the same Anyware Manager deployment. To minimize downtime, it is recommended that you run the newly created RHEL/Rocky Linux Connector for a period of time to ensure it is working properly before decommissioning the Connector on Ubuntu.

## MFA CONFIGURATION

When you enable MFA for the Connector for RHEL/Rocky Linux, all PCoIP Clients authenticated through the Connector will be prompted to enter MFA credentials. Previously with the Connector on Ubuntu, internal and external clients had different MFA configurations. If you want to have the same MFA configuration for the Connector on RHEL/Rocky Linux as the Connector on Ubuntu, you must install multiple Connectors on RHEL/Rocky Linux.

## TRANSITIONING THE CONNECTOR

The following steps outline how to transition to the Connector on RHEL/Rocky Linux:

1. Before you install the Connector, ensure you have met all the required prerequisite steps. For instructions and documentation on the Connector prerequisite steps when install on RHEL/Rocky Linux, see [Connector System Requirements](#). It is important to read and address all the prerequisites outlined.
2. Review the differences between the Connector on RHEL/Rocky Linux and Ubuntu, as outlined [here](#).
3. Prepare your Connector configuration files. For information on configuring your Connector, see [Configuring the Connector](#).
4. When generating the Anyware Connector token for the new Connector, ensure you use the same Anyware Manager deployment as the existing Connector on Ubuntu. For information on generating the Connector token, see [Generating a Connector Token](#).

5. Install and configure the Connector on RHEL/Rocky Linux. For information on installing and configuring the Connector, see [Installing the Connector](#).

## TESTING THE CONNECTOR

Once you have installed the Connector on RHEL/Rocky Linux you should test it and ensure it has been correctly installed and configured. The following steps outline how to test the Connector:

1. Run the following command to check that all installed services are running:

```
sudo /usr/local/bin/kubectl get pods -c connector
```

2. Access the virtual machine where you have the PCoIP Client installed and establish a connection using the Connector IP or FQDN. If this connection is successful then it confirms the Connector has been installed correctly. If it is not, you should re-check the virtual machine configuration and Connector configuration.

## ADDING THE CONNECTOR TO A LOAD BALANCER

If the original Connector on Ubuntu was configured with a load balancer, you need to add the new Connector on RHEL/Rocky Linux to the load balancer. Once you have tested the Connector on RHEL/Rocky Linux install, and are happy that it was successful, you can remove the Connector on Ubuntu.

# Reference

## Scaling and PCoIP Session Limits

When using Anyware Manager as a Service there are certain session establishment and session bandwidth limits when dealing with external connections.

The following table outlines the RAM, vCPU and correlated estimated bandwidth support:

vCPUs	RAM	Estimated Bandwidth
2vCPU	7.5 GB RAM	~ 365 Mbit/s
4vCPU	15 GB RAM	~ 830 Mbit/s
8vCPU	30 GB RAM	~ 1100 Mbit/s

### Estimated Bandwidth

These are estimated bandwidth levels. The bandwidth can vary based on the host, OS, CSP, etc.

1100 Mbit/s is approximately the maximum bandwidth that can be achieved. Additional gains may be possible with larger sizing.

## Firewall and Load Balancing Considerations

Anyware Manager and the Connector require certain ports to be open to enable connections between the Anyware Manager, Connector, Remote Workstations, as well as other components.

## Ports and Component Connections

Component	Allow	Port/Protocol	Source/ Destination Component	Descriptions
Connector	Inbound	80 TCP	From administrative web browsers.	For accessing the Management Interface, redirects to port 443.
Connector	Inbound	443 TCP	From PCoIP Clients and administrative web browsers.	For users to negotiate connections to their remote workstations. For accessing the Management Interface for (legacy) management of Anyware Manager.
Connector	Outbound	443 TCP	To CAM Service, <a href="#">PCoIP Cloud License Server</a> and to <a href="#">SumoLogic</a> .	To sync AD information to the CAM service and call Anyware Manager APIs related to negotiating PCoIP sessions. To verify license activation code during the Connector installation. For log aggregation for support purposes.
Connector	Outbound	60443 TCP	To remote workstations.	Prepares PCoIP Agents for a new user session.
Connector	Inbound	4172 TCP/UDP	From PCoIP Clients.	For PCoIP Sessions with users that are outside of the corporate network.
Connector	Outbound	4172 TCP/UDP	To remote workstations.	For PCoIP Sessions with users that are outside of the corporate network.
Connector	Outbound	636 TCP	To Domain Controllers.	To authenticate users, and query user and computer information.
Connector	Outbound	1812 UDP (This port is configurable)	To RADIUS Server.	For authentication against RADIUS Server.
Connector	Outbound	53 UDP	To DNS.	Domain name resolution.
PCoIP License Server	Inbound	7070 TCP (This port is configurable)	From remote workstations.	For license activation and verification from PCoIP Agent if the PCoIP License Server is used instead of the Cloud License Server.



**Port and Component Notes:**

- Port **80 TCP** can be blocked and is not required to be open if users all use port 443 instead.
- Port **443 TCP** is not required if the PCoIP License Server is used in place of the Cloud License Server.
- The RADIUS Server is optionally configured.
- See the PCoIP License Server guide for [changing port](#) and [configuring TLS encryption](#).

## Configuring the Active Directory for Anyware Connector

We recommend having a single Active Directory configuration for a single deployment, which means all Anyware Connectors within that deployment should be configured to the same AD. If you want to have multiple Anyware Connectors with different Active Directory settings then you need to ensure that each Anyware Connector belongs to a separate deployment. If you create two Anyware Connectors that are associated with the same deployment then both will use the same Active Directory sync settings, and the configuration of the last Anyware Connector created will take precedence.

### Configuring User and Computer Active Directory Distinguished Names

The Anyware Connector can optionally be configured to use specific Distinguished Names (DNs) when querying Active Directory for users and computers. This has been extended to be available when running the `update` command in addition to the `install` command.

The following is an example of the DN string format: `CN=CASM`

`Admins,CN=Users,DC=example,DC=com`. You can also configure the frequency at which the Anyware Connector syncs this data with the AWM service, as outlined in the following table:

Flag	Type	Description
<code>--users-dn</code>	String	The base DN to search for users within Active Directory. This option may be specified multiple times to provide multiple DNs.
<code>--computers-dn</code>	String	The base DN to search for computers within Active Directory. This option may be specified multiple times to provide multiple DNs.
<code>--sync-interval</code>	String	The interval time in minutes for how often to sync Active Directory users and computers with the AWM service. It must be at least five minutes.
<code>--users-filter</code>	String	The filter to search for users within Active Directory. Specify multiple filters with multiple options. Default user filter: <code>(&amp;(objectCategory=person)(objectClass=user))</code> . An example for a user group filter: <code>(&amp;(objectCategory=person)(objectClass=user)(memberOf:1.2.840.113556.1.4.1941:=CN=PCoIP Users Group,CN=Users,DC=example,DC=com))</code> .
<code>--computers-filter</code>	String	The filter to search for computers within Active Directory. Specify multiple filters with multiple options. Default computer filter: <code>(&amp;(primaryGroupID=515)(objectCategory=computer))</code> .

These flags outlined are optional and may be provided with the `install` or `update` commands. If you are updating a Anyware Connector you only need to provide these flags if you want to changing the DN settings associated with that Anyware Connector. If you do not add these flags when performing an update then the Anyware Connector will retain the same settings.

You can reset user or computer DNs to their default values by providing an explicit DN with a wider scope than the original DN used.

## Configuring Active Directory Pool Groups

A set of command line flags enables users to update Active Directory pool groups. These flags apply changes to the Active Directory settings of the Anyware Connector.

By providing the following flags the appropriate update gets applied to the Anyware Connector settings. If no command-line option is provided, the Anyware Connector will display all available options for this operation.

Flag	Type	Description
<code>--cam-insecure</code>	String	Skips certificate validation when connecting to Anyware Manager as a Service. This option should only be used when connecting to Anyware Manager as a Service deployed with self-signed certificates.
<code>--add-pool-group</code>	String	Adds specified Active Directory group to the existing pool group settings. By providing all the existing pools groups in the Anyware Connector, settings would get replaced by the user specified ones.
<code>--remove-pool-group</code>	String	Removes specified pool Active Directory group by its DN.
<code>--clear-pools-groups</code>	String	Clears all pools Active Directory groups. This operation is exclusive and cannot be combined with <code>--remove-pool-group</code> or <code>--add-pool-group</code> .
<code>--get-cam-settings</code>	String	Prints all Anyware Manager as a Service settings to Admin console.

## 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 will be automatically unassigned, and will be 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 utilise 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 organisations to enforce logical separation of remote workstations.

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

```
This feature is currently supported in the Beta mode of the Admin Console.
Features in this mode are still being worked on and refined by us, as a result
there may be certain issues that arise.
```

### Enable Session Tracking

In order to enable this feature, you must first enable session tracking from the Admin Console.

1. Log in to the Admin Console.
2. Click on the Beta UI toggle from the top menu. This feature currently only works in the Beta version of the Admin Console.
3. Navigate to the deployment you want to enable floating workstation assignments on. In the top menu bar beside the deployment click on the kebab menu item and click **Edit deployment**.

4. Select the **CONNECTOR SETTINGS** tab from the deployment and click on the **Session Tracking** toggle.

The screenshot shows the 'CONNECTOR SETTINGS' tab for a deployment named 'default-1702'. At the top, there is a 'Beta' warning banner: 'This is not the production interface. It may contain features and changes that are not yet considered ready for production.' Below this, the breadcrumb is '< default-1702'. The navigation tabs are 'OVERVIEW', 'DEPLOYMENT SERVICE ACCOUNTS', 'CLOUD SERVICE ACCOUNTS', and 'CONNECTOR SETTINGS', with 'CONNECTOR SETTINGS' being the active tab. The main content area is titled 'SESSION STATISTICS' and contains the following text: 'Enabling this feature allows Cloud Access Connectors to send information about PCoIP sessions going through a Security Gateway to CAS Manager. This can workstation.' Below this text is a toggle switch for 'Session Tracking' with a help icon (?), which is currently turned off. Below the 'SESSION STATISTICS' section is the 'MANAGE AD GROUPS' section, which contains the text: 'Active Directory groups can be added to CAS Manager to entitle a group of users to a remote workstation pool. Learn more about [AD Groups Configurations](#)'. Below this text is a table with two columns: 'DISTINGUISHED NAME' and 'GROUP GUID'. The table is currently empty, and a message below it states: 'No groups were found in the connector settings for this deployment'.

## 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 will work 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 will remain assigned to a user for **approximately 20 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, the user gets a 6604 Error. If you observe this error, reboot the remote workstation.

# Security

## Multi-Factor Authentication (MFA)

Anyware Manager as a Service supports Multi-Factor Authentication (MFA) for PCoIP client sessions. The Anyware Manager as a Service MFA implementation is based on the RADIUS protocol. Customers can leverage their existing RADIUS server installation to enable MFA for Anyware Manager as a Service deployments. The following MFA scenarios have been tested with specific versions of the MFA software in question. Different versions may not yield the same results and may lead to different behavior.

### Multi-Factor Authentication with Duo

#### Duo Authentication Version

The Connector was tested with Duo version **2.4.21**.

In regards Duo authentication, the following information is configured in the `authproxy.cfg` file. When installing the Connector it will require the following information to configure the Duo Radius server:

- Radius Client IP (Connector IP)
- Radius Server Port
- Radius Shared Secret
- Duo authentication settings (ikey, skey and api host)

#### Multi-Factor Authentication PCoIP Client Support

Android PCoIP clients do not presently support RADIUS MFA.

For information on enabling Duo authentication with Anyware Manager as a Service, see [Anyware Manager as a Service Duo MFA](#).

## Multi-Factor Authentication with Azure

### Microsoft Azure MFA Component Versions

We tested the Connector with Microsoft Azure MFA on **November 15<sup>th</sup> 2019** with the following components.

HP component versions:

- PCoIP Software Client for Windows 19.11.
- Connector with MFA flag enabled.
- PCoIP Standard/Graphics Agent 19.11.

3<sup>rd</sup> party component versions:

- Azure Active Directory Premium or Microsoft 365 Business offering to use Azure MFA.
- Network Policy Server (NPS) acting as the RADIUS server.
- NPS extension **1.0.1.32**.
- Microsoft Authenticator App **1911.7724** (Android/iOS).

Using different versions may result in different behavior and has not been tested by us.

Azure MFA can successfully be used as a 2<sup>nd</sup> factor tool for authenticating into the Connector. The following components are required to enable this MFA set-up:

- Azure Active Directory Premium or Microsoft 365 Business offering to use Azure MFA.
- Network Policy Server (NPS) acting as the RADIUS server.
- NPS extension **1.0.1.32** for Azure MFA sending requests from NPS to Azure MFA cloud service.
- Microsoft Authenticator App **1911.7724** (Android/iOS) to receive Push or to generate a Passcode.

### Generated Passcode is not usable with Connector and Azure MFA

Only Microsoft Authenticator App Push Notification is supported due to Azure MFA using [Modern Authentication](#). Selecting **Send Me a Push** or **Submit Passcode** triggers a push notification on your Microsoft Authenticator App. You will successfully connect to your PCoIP Session once you approve the push on your Android/iOS device.



For further information on configuring the required 3<sup>rd</sup> party components to enable Azure MFA with Connector, see [Anyware Manager as a Service Azure MFA](#).

# Anyware Manager as a Service Security and Privacy

The [Anyware Manager as a Service Privacy Statement](#) details information around the collection, use, processing and disclosure of personal information and other information in connection with the Anyware Manager as a Service. The statement outlines the information we collect, how and when it is used, as well as other privacy and security information. For privacy information on HP's other services and activities, see [HP Privacy Policy](#).

# Reference

## Microsoft Azure Active Directory Authentication

The Admin Console supports Microsoft Azure Active Directory for authentication. All users with a work or school account from Microsoft can sign in to the Admin Console using Azure Active Directory. A work or school account is an account created by an organization's administrator to enable a member of the organization to access Microsoft cloud services, such as Microsoft Azure or Office 365. This account can take the form of a user's organizational email address, such as [username@orgname.com](#) for example.

Please check with your organization's administrator to see if you can set up a work or school account. For more information about configuring your organization to use Microsoft's cloud services, view the documentation here: <https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/sign-up-organization>.

# Anyware Connector Multi-Factor Authentication

## Duo Authentication

If you wish to use Duo authentication with Anyware Connector you will be required to setup an authentication server provided by Duo. For more information on this, see [Duo Authentication Proxy - Reference](#).

### Duo Authentication Version

The Connector was tested with Duo version **2.4.21**.

The following are key items in the *authproxy.cfg* file that are relevant for the Anyware Manager as a Service configuration:

```
[duo_only_client]
[radius_server_duo_only]
ikey=<integration key for duo>
skey=<secret key for duo>
api_host=<host used for duo>
radius_ip_1=<cac connection server ip>
radius_secret_1=<shared secret for above>
radius_ip_2=<cac connection server ip2>
radius_secret_2=<shared secret for above>
port=1812
```

For further information on the above integration, see [RADIUS Duo Only](#).

## Azure MFA Authentication

### Microsoft Azure MFA Component Versions

HP tested the Connector with Microsoft Azure MFA on **November 15<sup>th</sup> 2019** with the following components.

HP component versions:

- PCoIP Software Client for Windows 19.11.
- Connector with MFA flag enabled.
- PCoIP Standard/Graphics Agent 19.11.

3<sup>rd</sup> party component versions:

- Azure Active Directory Premium or Microsoft 365 Business offering to use Azure MFA.
- Network Policy Server (NPS) acting as the RADIUS server.
- NPS extension **1.0.1.32**.
- Microsoft Authenticator App **1911.7724** (Android/iOS).

Using different versions may result in different behavior and has not been tested by HP.

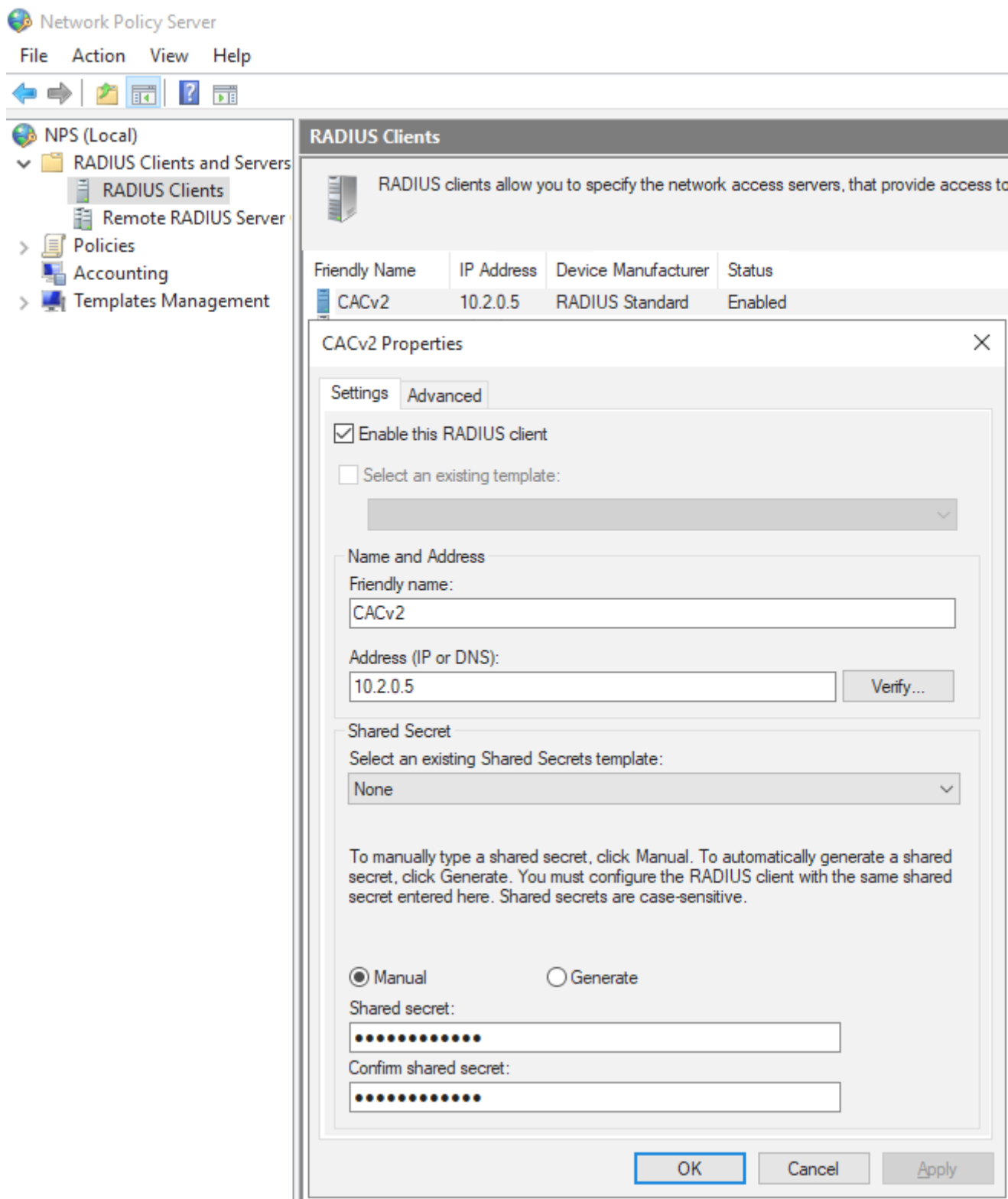
## Azure MFA Configuration

If you wish to use Azure MFA with the Connector you need to configure a number of 3<sup>rd</sup> party components. The following steps outline this process:

1. From within the Azure portal click **Azure AD**.
2. Click **Enable MFA for target users**.
3. Install the [Microsoft Authenticator App](#) on an Android or iOS mobile device.
4. Ensure that if the users requiring MFA are not yet populated in Azure AD, that you setup Azure AD Connect to sync On-Premises users to Azure.
5. Install Network Policy and Access role on Windows Server 2016 or 2019.
6. Install Network Policy Server (NPS) extension for Azure MFA.
7. Register NPS to Active Directory to enable it to query the list of users.

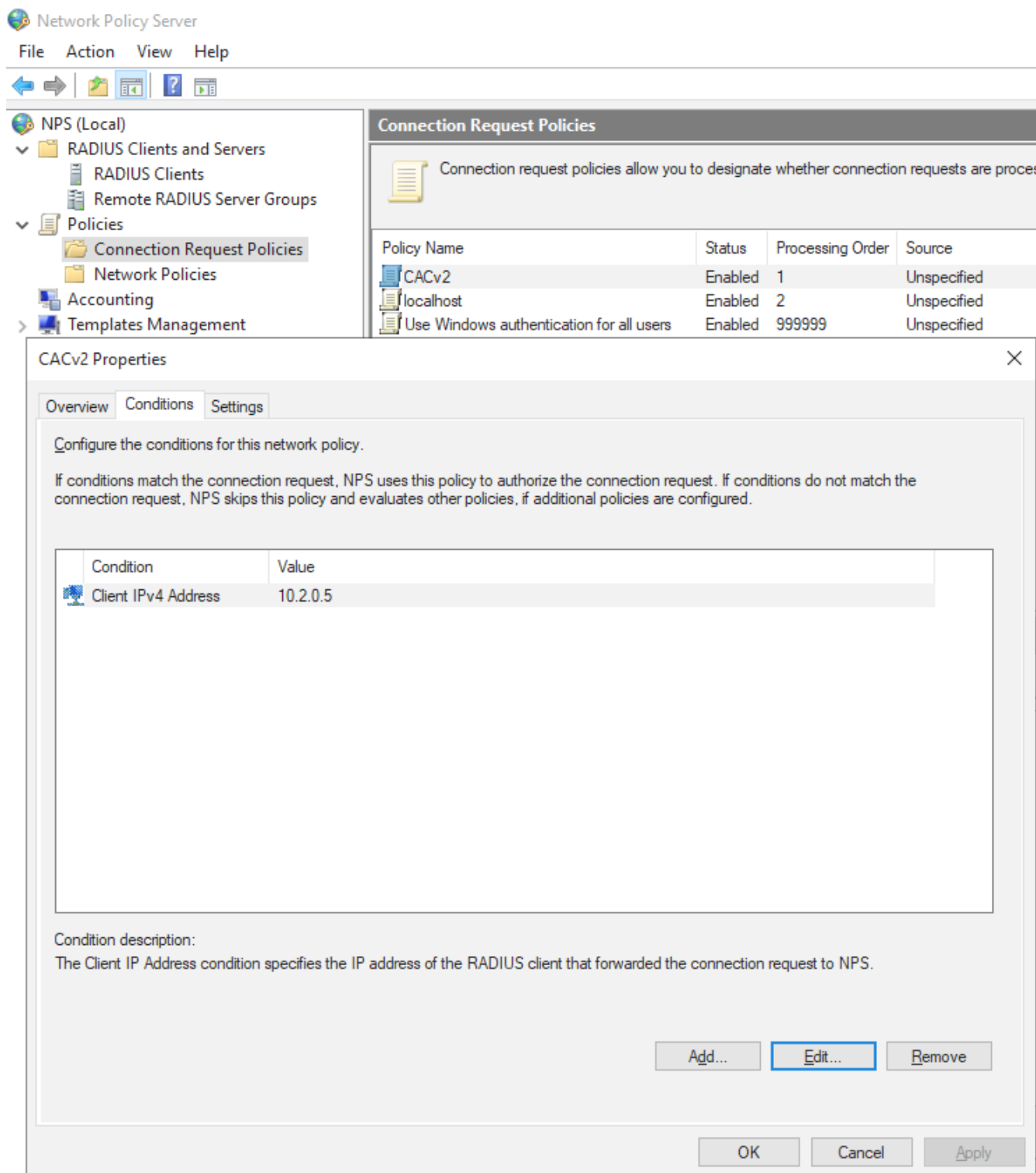
Once you have registered the NPS you need to configure the server. The following steps outline the NPS configuration:

1. From within the NPS console click **RADIUS Clients**.
2. Add the Connector IP address and Shared Secret and click **OK**.



3. Click **Policies > Connection Request Policies** and add a new policy name and click **OK**.

4. From the **Conditions** tab add the Client IPv4 Address of the Connector and click **OK**.



5. From the **Settings** tab under **Authentication** click *Accept users without validating credentials*.

6. Restart NPS services to enable these changes to take effect.

# Specifying Domain Controllers

You can optionally specify one or more domain controllers to use with the Connector by providing the `--domain-controller` option with the `install` or `update` commands. The following is an example of how this command might look (other required options excluded):

```
sudo ./cloud-access-connector install --domain-controller dc1.domain.com [--  
domain-controller dc2.domain.com]
```

Multiple domain controllers can be specified by providing multiple `--domain-controller` options. If you explicitly provide domain controllers the Connector will only use these domain controllers when authenticating or syncing users and computer information to the CAM service, regardless of whether other domain controllers are available.

## FQDN Specification

The domain controller you provide must be specified as an FQDN, and not an IP address.



# Installing and Configuring Anyware Manager as a Service Idle Shutdown

The following section outlines how to install and configure idle shutdown on remote workstations not provisioned by Anyware Manager as a Service on Windows and Linux.

Any remote workstations provisioned by Anyware Manager as a Service will have this feature installed and configured by default. If idle shutdown has been installed and configured on remote workstations that were not provisioned by Anyware Manager as a Service and are not managed by Anyware Manager as a Service, then the administrator may be required to log into their cloud environment to reboot these remote workstations whenever the idle shutdown powers them off.

This setting may not suit all customers' needs and can be customized to suit.

## **Service Account and Access Prerequisites**

Powering the remote workstation on or off from the Anyware Manager as a Service at session start, or from the web interface, requires that the remote workstation exists in a cloud environment with appropriate service account credentials that supports power management with Anyware Manager as a Service.

## Installing on Windows

After installing the PCoIP Agent, run the following commands in PowerShell:

```
$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."
}
}
```

## Configuring on Windows

For the PCoIP Agent for Windows the settings must be retrieved from the registry. The following steps outline how to configure these settings for Windows:

- For PCoIP Agent versions 2.15 and earlier, the settings are stored in:

```
HKLM\SOFTWARE\WOW6432Node\Teradici\CAMShutdownIdleMachineAgent
```

PCoIP Agent version 19.05 and later, the settings are stored in:

```
HKLM\SOFTWARE\Teradici\CAMShutdownIdleMachineAgent
```

### PCoIP Agent Versions

PCoIP Agent versions 2.15 and earlier are 32-bit, and versions 19.05 and later are 64-bit.

The table below outlines the settings and defaults:

Type	Name	Default	Description
DWORD	<i>PollingIntervalMinutes</i>	15 minutes	Polling interval in minutes for checking the CPU utilization. Must be between 1 and 60.
DWORD	<i>MinutesIdleBeforeShutdown</i>	240 minutes	Number of minutes the machine must be considered idle before it can be shutdown. The timer starts only when all active users have disconnected (or logged off), and is reset if any user connects. Must be between 5 and 10000.
DWORD	<i>CPUUtilizationLimit</i>	20%	Value between 0 and 100 representing CPU utilization percentage. If CPU utilization is below this value the machine is considered idle and will shutdown if maintained for <i>MinutesIdleBeforeShutdown</i> .
DWORD	<i>EnableCAMDebug</i>	0	Additional debugging messages to the event log when this value is non-zero.

1. After installation the service will be enabled by default. To enable or disable the service explicitly, run:

```
Set-Service CAMIdleShutdown -StartupType "Automatic"
```

or

```
Set-Service CAMIdleShutdown -StartupType "Disabled"
```

2. *MinutesIdleBeforeShutdown* can be configured through the Microsoft Azure ARM provisioning template as the *autoShutdownIdleTime* setting in the parameters file. Once the *autoShutdownIdleTime* setting is installed on a remote workstation, you can configure the setting by pushing the desired registry key settings directly to the specific remote workstation.

## Installing on Linux

After installing the PCoIP Agent, run the following commands in the command line:

```
AUTO_SHUTDOWN_IDLE_TIMER=<Desired-Idle-Time>
ENABLE_AUTO_SHUTDOWN=<true-or-false>
mkdir /tmp/idleShutdown
wget "https://raw.githubusercontent.com/HPInc/Anyware-Idle-Shutdown/master/
remote-workstations/new-agent-vm/Install-Idle-Shutdown.sh
awk
'{ sub("\r$", ""); print }' /tmp/idleShutdown/Install-Idle-Shutdown-raw.sh > /
tmp/idleShutdown/Install-Idle-Shutdown.sh && sudo chmod +x /tmp/idleShutdown/
Install-Idle-Shutdown.sh
INSTALL_OPTS="--idle-timer ${AUTO_SHUTDOWN_IDLE_TIMER}"
if [[ "${ENABLE_AUTO_SHUTDOWN}" = "false" ]]; then
    INSTALL_OPTS="${INSTALL_OPTS} --disabled"
fi
sudo /tmp/idleShutdown/Install-Idle-Shutdown.sh "${INSTALL_OPTS}"
```

## Configuring on Linux

For the PCoIP Agent for Linux, the idle shutdown is configured through a system service and can be configured through the accompanying service and timer .conf and files.

The table below outlines the settings and defaults:

Location	Setting	Default	Description
/etc/systemd/system/ CAMIdleShutdown.service.d/ CAMIdleShutdown.conf	<i>MinutesIdleBeforeShutdown</i>	240 minutes	Number of minutes the machine must be considered idle before it can be shutdown. The timer starts only when all active users have disconnected (or logged off), and is reset if any user connects. NOTE: This includes SSH sessions.
/etc/systemd/system/ CAMIdleShutdown.service.d/ CAMIdleShutdown.conf	<i>CPUUtilizationLimit</i>	20%	Value between 0 and 100 representing CPU utilization percentage. If average CPU utilization is below this value the machine is considered idle and will shutdown if maintained for <i>MinutesIdleBeforeShutdown</i> .
/etc/systemd/system/ CAMIdleShutdown.timer.d/ CAMIdleShutdown.conf	<i>OnUnitActiveSec</i>	15 minutes	Polling interval in minutes for checking the CPU utilization.

1. To apply any changes, you need to run the following command:

```
systemctl daemon-reload
```

2. After installation the service will be enabled by default. To enable or disable the service explicitly, run:

```
systemctl enable CAMIdleShutdown.timer
systemctl start CAMIdleShutdown.service
systemctl start CAMIdleShutdown.timer
```

or

```
systemctl stop CAMIdleShutdown.service
systemctl stop CAMIdleShutdown.timer
systemctl disable CAMIdleShutdown.timer
```

3. *MinutesIdleBeforeShutdown* can be configured through the Microsoft Azure ARM provisioning template as the *autoShutdownIdleTime* setting in the parameters file. Once the

*autoShutdownIdleTime* setting is installed on a remote workstation, you can configure the setting by pushing the desired registry key settings directly to the specific remote workstation.



# Anyware Manager as a Service Deployment Scripts

HP has an open github repository that contains a collection of scripts that simplify the setup, installation and usage of Anyware Manager as a Service. This repository enables users to set-up the necessary cloud resources (networking, firewalls, NAT gateway, storage buckets, etc.), as well as Domain Controllers, Connectors and remote workstations from scratch to produce a working environment.

## Infrastructure Limitations

The scripts in this repository are suitable for creating reference deployment for demonstration, evaluation or development purposes. The infrastructure created may not meet the reliability, availability or security requirements of your organization.

The tools in this repository are provided as-is, with no expectation of support. Users are encouraged to clone, modify and to submit bug reports in github.

The repository which contains scripts for deploying Connectors is available at [https://github.com/teradici/cloud\\_deployment\\_scripts](https://github.com/teradici/cloud_deployment_scripts).

# Licensing Options with Anyware Manager as a Service

With Anyware Manager as a Service, you can choose to put all your licenses into a single "cloud based" licensing pool or you can setup your own local PCoIP License Server if you require more advanced options.

## How to Choose?

Use a Cloud License Server if you not need the advanced features of the local PCoIP License Server and do not want the overhead of deploying and managing the PCoIP License Server.

Use the PCoIP License Server if your use case includes one or more of the following advanced features or scenarios:

- Your remote workstations do not have access to the internet.
- You want to use an offline (dark site) activation process.
- You want to divide your license pool into multiple pools for multiple users.
- You want to actively track license usage.

## Cloud License Server

This is a license server managed by us that exists in the cloud. Users must obtain a license key for it and enter it into the Connector during the [installation process](#). You must enter this key in the Admin Console when creating a deployment.

## PCoIP License Server

The PCoIP License Server is a standalone software application that runs on a Linux (RHEL or CentOS) machine, and handles both PCoIP session license registrations and PCoIP session request authorization. If you want to use the PCoIP License Server with Anyware Manager as a Service you need to have a PCoIP License Server activation code.

When a PCoIP Agent attempts to establish a new PCoIP session, it will request authorization from the assigned PCoIP License Server. The PCoIP License Server checks to see if an activated PCoIP

session license is available in its trusted storage, and authorizes the session. Each PCoIP session activation consumes one PCoIP session license. For more information on the PCoIP License Server, see [here](#).

### **⚠ PCoIP License Server Activation Code**

In order to use Anyware Manager as a Service with the PCoIP License Server, you will require both a Cloud License Server registration code and a PCoIP License Server activation code. Contact support [here](#) to ensure you have both codes available.

You can enter in the FQDN or IP address into the Connector during the [installation process](#) using the `--local-license-server-url` flag.

## Licensing Features

The following table outlines the features supported for both licensing types

### Licensing Features Comparison

Features	Cloud License Server	PCoIP License Server
Online activation supported?	Yes	Yes
Offline (Dark site) activation supported?	No	Yes
Internet proxy supported?	Yes	Yes
High Availability options available?	No	Yes
Ability to track license usage?	No	Yes

For more information on Licensing with HP, see [here](#).

## Using Cloud Licensing with Anyware Manager as a Service

If you are using Anyware Manager as a Service you will need a PCoIP registration code (format: XXXXX@YYYY-YYYY-YYYY-YYYY)

A PCoIP Agent configured for a cloud license server will continue to use the cloud license server even if the PCoIP License Server has been configured in the Connector.

## INSTALLATION STEPS

- When installing the Connector, use your registration code to register with the HP licensing system. For more information on installing the Connector, see [here](#).

All PCoIP connections will check the Cloud Licensing service prior to enabling a connection. You will be limited to the amount of sessions you have configured, for example if you are configured to have 5 concurrent sessions, the licensing system will limit you to 5 sessions. If you require more connections, you can scale up or down the cloud-based licensing pool by purchasing additional cloud-based licenses.

## Using a PCoIP License Server with Anyware Manager as a Service

If you have chosen to use a PCoIP License Server, you will need:

- PCoIP registration code
- Activation code(s)

### Activation and PCoIP Registration Code

In order to use Anyware Manager as a Service with the PCoIP License Server, you will require both a Cloud License Server registration code and a PCoIP License Server activation code. Contact support [here](#) to ensure you have both codes available.

## INSTALLATION STEPS

1. Install a local PCoIP License Server in your environment. For more information on this, see [here](#).
2. Activate the licenses using your activation codes.
3. Once the PCoIP License Server has been installed, record your FQDN or IP address of the PCoIP License Server.
4. Install the Connector(s), use your registration code to register with the HP licensing system. In addition, you will need to enter the FQDN or IP address obtain in the previous step by entering the `--local-license-server-url` flag at installation. This is an optional flag, so if you do not provide it then the installer will not ask for it.

For more information on installing the Anyware Connector, see [here](#).

All PCoIP connections will check your PCoIP License server prior to enabling a connection. You will be limited to the amount of sessions you have configured, for example if you are configured to have 5 concurrent sessions, the licensing system will limit you to 5 sessions. If you require more connections, you can scale up or down by purchasing additional PCoIP License Server licenses. For each license you purchase you will receive an activation code. You will be required to manually install these on your PCoIP License Server. It is possible to have licenses both in the cloud and on your local PCoIP License Server. The system will always check the cloud license system first and if there are no available licenses, it will then check with the PCoIP License Server.

## Licensing Requirements with Anyware Manager as a Service

- Anyware Manager as a Service requires a Cloud License Server registration code to be entered in the Admin Console when creating a deployment.
- The user can install the PCoIP License Server URL directly into the Connector during installation.
- Any remote workstations provisioned by Anyware Manager as a Service will need to use the Cloud License Server for licensing purposes.
- Any remote workstation without a Cloud License Server license already installed, will need to use the PCoIP License Server URL from the Connector to obtain a license.

### Licensing Priority Levels

Licenses will be acquired based on the following priority levels:

- PCoIP License Server address setting from GPO.
- Cloud License Server.
- PCoIP License Server address from the PCoIP Connection Manager.

These priority levels come from the PCoIP Agent, Please check the PCoIP Agent documentation for changes or updates:

- [PCoIP Standard Agent for Windows](#)
- [PCoIP Standard Agent for Linux](#)
- [PCoIP Graphics Agent for Windows](#)
- [PCoIP Graphics Agent for Linux](#)

# Anyware Manager as a Service Maintenance

The following page outlines how to perform updates to the OS, Connector(s) and how to clean up unnecessary disk space.

## OS Updates

The Connector can run on Ubuntu 18.04. Updates for the OS are pushed for installed packages frequently. In order to ensure the OS is as secure and up to-date as possible, it is important to run OS updates regularly by running the following command:

```
apt update
apt upgrade -y
```

## Connector Updates

The Connector needs to be updated as new features are added and/or security updates are required. In order to ensure you are running the latest version of the Connector, it is important to run updates regularly. For more information on how to update the Connector, see [here](#). Teradici recommends updating once a month. Updates can be carried out in place or by deploying a new Connector machine as part of a red-black deployment update.

## Disk Space Updates

The Connector uses Docker to run and as a result you may encounter issues with disk space usage after some of the Docker containers have been updated with newer images. If this becomes an issue you can run the following Docker commands to clean up unused docker images that may have been previously downloaded for older versions of the Connector:

```
docker system prune
```

For more information on this, see <https://docs.docker.com/config/pruning/>.

# Anyware Manager as a Service Provider Service Accounts

## Provider Service Account Requirements

Anyware Manager as a Service's capabilities are enhanced if you provide service account or role credentials for your specific cloud environment. This section describes which capabilities are enabled by providing service account access, and what levels of access are required to restrict accounts.

## Roles and Permission Policies - AWS

You can use the AWS Management Console to create a role which Anyware Manager as a Service is able to assume. For more information on creating roles in AWS, see [Creating a role to delegate permissions to an IAM user](#). You must use the Account ID and External ID that can be generated from the Admin Console, for information on how to generate these credentials, see the section outlined [below](#).

### AWS PROVIDER CREDENTIALS FOR ANYWARE MANAGER AS A SERVICE

The following section outlines how to generate the Account ID and External ID from the Anyware Manager Admin Console. The following steps outline how to generate a Anyware Manager Account ID and External ID:

1. In the Anyware Manager Admin Console select the deployment you wish to use.
2. Click **Edit Deployment**.
3. Click **Provider 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 will need to create a permissions policy for Anyware Manager as a Service that contains the permissions outlined in the section below.

#### **AWS PERMISSIONS POLICIES**

Once you have created the role in the AWS Management Console you can create and assign a permissions policy 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: *SimulatePrincipalPolicy*



The following example can be copied and pasted into the JSON field when creating the policy instead of manually selecting each role:

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

If the user tries to add an AWS role that doesn't have these permissions, Anyware Manager as a Service will still add the role but will not validate that it has the required permissions.

You can now associate a permissions policy to this role.

## Service Account Permission Requirements - Azure

You need a service account that has adequate permissions and can manage compute instances to power manage a remote workstation in Microsoft Azure with Anyware Manager as a Service. The following roles are required:

- Reader
- Virtual Machine Contributor

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 straight away as it will not be 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.

## Service Account Permission Requirements - GCP

You need a service account that has adequate permissions and can manage compute instances to provision a remote workstation in Google Cloud Platform (GCP) with Anyware Manager as a Service.

The table below outlines the default roles that are required for the service account on GCP, and which features they are required for.

Default Roles and Feature Requirements - GCP

Default Roles	Workstation Provisioning	Power Management
Deployment Manager Editor	Required	—
Compute Admin	Required	Required
Cloud KMS Admin	Required	—
Cloud KMS CryptoKey Encrypter/Decrypter	Required	—

For GCP the service account requires access to the following APIs:

- Service Usage API
- Cloud Resource Manager API
- Cloud Deployment Manager V2 API
- Cloud Key Management Service (KMS)
- Compute Engine API

**🔑 Key File Storage**

Anyware Manager as a Service does not store the key file provided and only extracts the fields that are entered into the dialog.

The following links have more information on GCP service accounts:

- [GCP - Getting Started](#)
- [GCP - Access Information](#)
- [Managing Service Account Keys](#)
- [Enabling GCP API for Projects](#)

## Creating a Cloud IAM Custom Role

Users can create a single custom IAM role by using the following permissions for Anyware Manager as a Service:

- cloudkms.cryptoKeyVersions.useToDecrypt
- cloudkms.cryptoKeyVersions.useToEncrypt
- cloudkms.cryptoKeys.create
- cloudkms.cryptoKeys.get
- cloudkms.keyRings.create
- cloudkms.keyRings.get
- compute.acceleratorTypes.list
- compute.addresses.create
- compute.addresses.delete
- compute.diskTypes.list
- compute.disks.list
- compute.images.list
- compute.instances.create
- compute.instances.delete
- compute.instances.get
- compute.instances.getGuestAttributes
- compute.instances.osLogin
- compute.instances.reset
- compute.instances.setMetadata
- compute.instances.setServiceAccount

- compute.instances.setTags
- compute.instances.start
- compute.instances.stop
- compute.instances.suspend
- compute.instances.update
- compute.instances.updateNetworkInterface
- compute.instances.use
- compute.machineTypes.list
- compute.networks.create
- compute.networks.list
- compute.regions.list
- compute.subnetworks.list
- compute.zones.get
- compute.zones.list
- deploymentmanager.deployments.create
- deploymentmanager.deployments.delete
- deploymentmanager.deployments.get
- deploymentmanager.resources.list
- resourcemanager.projects.get

Using these permissions you can create a custom IAM role. If you use this single custom role you do not need to use other default roles discussed above. For information how to do this, see [Creating and managing custom roles](#).

## Providing Service Account Credentials

Service account credentials can be provided as part of the Anyware Manager as a Service deployment. These credentials can be manually entered, or for GCP deployments a key file can be provided that can be used to populate the fields. For more information on creating a deployment, see [Creating a Deployment](#).

The table below outlines the features supported by the different Connector versions, and the public cloud providers that work with the Anyware Manager as a Service.

### Anyware Manager Features enabled by Provider Service Accounts

Feature	Azure	GCP	AWS	ESX
<b>Deallocation*</b>	<b>Supported</b>	Not Applicable	Not Applicable	Not Applicable
<b>Power Management</b>	<b>Supported</b>	<b>Supported</b>	<b>Supported</b>	Not Supported
<b>Workstation Provisioning</b>	Not Supported	<b>Supported</b>	Not Supported	Not Supported

\*Deallocation is a power state within Microsoft Azure. When a remote workstation is powered off by a user, it will be shutdown and the account will still be billed. Anyware Manager as a Service can deallocate remote workstations that have been shutdown in order to stop them being billed.

# Anyware Manager as a Service Active Directory

## Assigning Permissions to Active Directory Service Accounts

The following section outlines the steps to enable permissions to create and delete computer objects, permissions on these objects, and permissions to change and reset user credentials. These permissions are the minimum level of permissions required for a service account when installing the Connector.

### Organisational Unit [OU] Permissions Dialog

Permissions are being assigned to the service account through the OU permissions dialog.

#### 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:

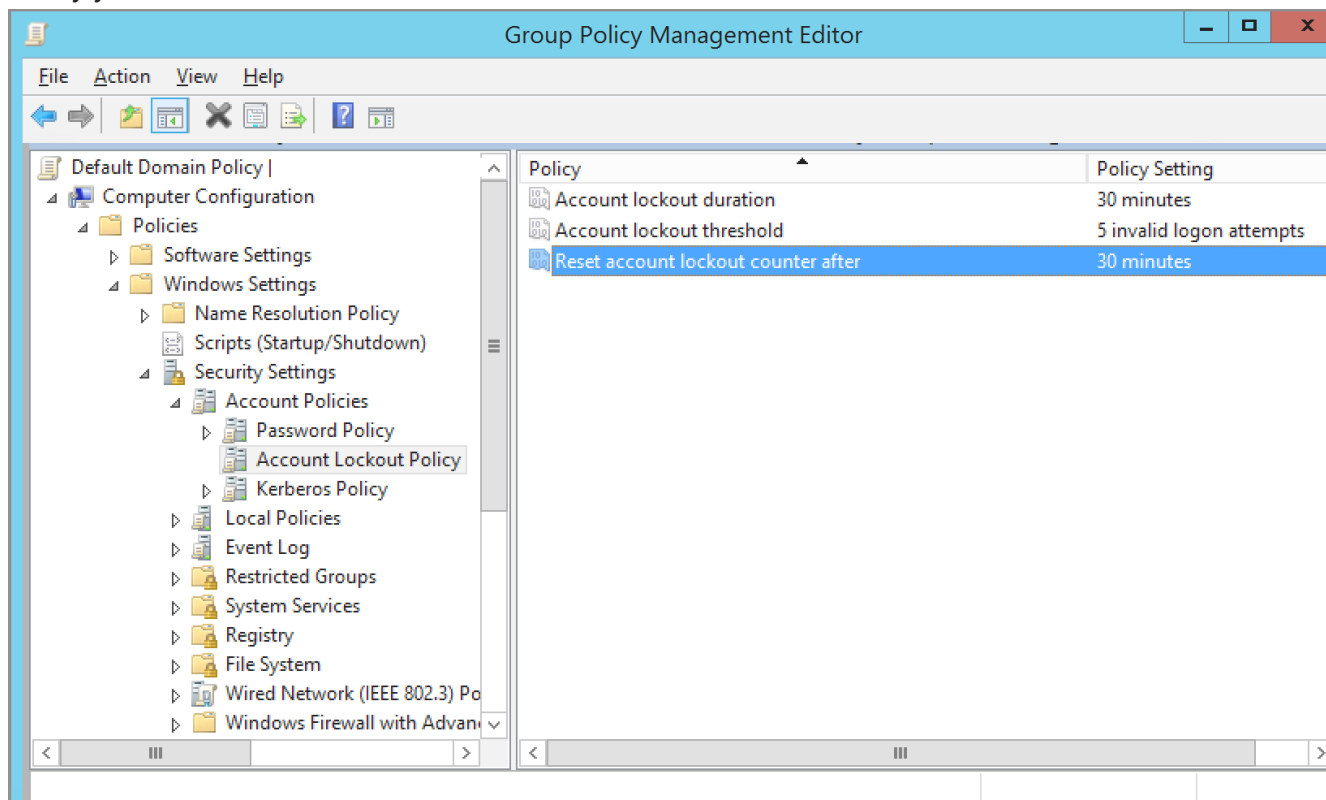
1. Go to the security tab of the OU you want to give permissions to.

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**.

## Verifying Active Directory Account Lockout

The following section outlines how to verify your on-premises AD DS account lockout policy. The steps below need to be carried out on a domain-joined system with administrator privileges:

1. Open the **Group Policy Management Editor** by clicking the start menu and searching for **Edit group policy**.
2. Edit the group policy that includes your organization's account lockout policy, such as the Default Domain Policy.
3. Navigate to **Computer Configuration>Policies>Windows Settings>Security Settings>Account Policies>Account Lockout Policy**.
4. Verify your Account lockout threshold and Reset account lockout counter after values.





# Anyware Manager as a Service Accounts

## Anyware Manager as a Service Account Ownership

Anyware Manager as a Service accounts have a single account owner, and one or more administrators who have the ability to authenticate to the Admin Console and manage Anyware Manager as a Service deployments and services. The account owner is any user who is able to sign in with a supported identity provider and provide a PCoIP registration code. The following are some important points around the Anyware Manager as a Service account owner:

- Account ownership changes will change all account data, including all deployment, remote workstation and user data to another account owner and cannot be reversed without the new account owner providing authorization.
- If the account owner password is lost it can only be recovered through the [identity provider](#). We do not store any of the passwords. It is the customer's responsibility to maintain access to their account owner's password and if necessary securely store the account information.
- As the account owner's account is provided by an identity provider such as Google or Microsoft, We do not have the ability to recover account owner's account and is unable to transfer data to a new account if there is no access to the old account.
- We can transfer a Anyware Manager as a Service account to another account owner provided the old and new owner accounts are accessible by the system administrator. In order to perform an account transfer see [below](#).

## Identity Providers

Both Microsoft and Google support transferring accounts from one organization to another. The process for doing this differs between the providers and in order to initiate this account transfer the user must work with the identity provider in question. Once the account has been transferred through the identity provider, the user will be able access Anyware Manager as a Service but they will not see any of their old data as Anyware Manager as a Service recognizes this as a different account. Anyware Manager as a Service uses a unique object identifier returned by the identity providers to associate specific data to specific user's. This identifier is immutable and cannot be changed.

## Account Ownership Transfers

If a Anyware Manager as a Service account needs to be transferred to a different account, the owner will need to open a support case and upon request from us, provide the following information:

- **Anyware Manager as a Service Authorization token from the old account:** This needs to be provided by the user.
- **Anyware Manager as a Service Authorization token from the new account:** This needs to be provided by the user.

For information on how to obtain a Anyware Manager as a Service authorization token from the Admin Console, see the [API Access Token](#) section of the Anyware Manager Administrator's Guide.

All the tokens are acquired by authenticating the identity provider and as a result must have specific permissions in order to succeed.

### Account Data Transfers

Transferring an account means that all data from one account is moved to another. This might not be suitable for Managed Service Providers that may be managing multiple deployments.

The two general use-cases for requiring an account ownership transfer are:

#### **Owner account is disabled and access to the old account is possible**

In the scenario where the account owner leaves the organization and their account is permanently disabled but it is possible to access the old account, an account transfer can be undertaken. The following steps need to be followed:

1. The user's IT organization needs to reactivate the account and sign into Admin Console.
2. Create a support ticket. See [here](#) for information on creating a support ticket with us.
3. Provide an authorization token from the old account.
4. Provide an authorization token from the new account. Anyware Manager as a Service operations uses the above information to migrate the accounts.
5. Disable the old account once more.

#### **Owner account is disabled and access to the old account is not possible**

In the scenario where the account is permanently disabled and access to old account is not possible then there is no way to validate the authenticity of the request and requester. An account transfer cannot be completed.

## Performing an Account Ownership Transfer

The following steps outline how to transfer a Anyware Manager as a Service user account:

1. Sign into the [Admin Console](#) with the old account.
2. Click the user account icon and click on the **Get API token**.
3. Copy the token and sign out of the Admin Console.
4. Do the same process with the new account and copy the token again.
5. Send the old account and new account tokens to HP and the transfer needs to be processed within 48 hours of receiving the tokens.

### Login Credentials

You need to login to <https://cas.teradici.com/> with your Google or Microsoft account only.

# Troubleshooting

## Anyware Manager as a Service Status

We provide service status at the following site: [Anyware Manager as a Service Status](#). From this site it is possible to view the current status of the Anyware Manager as a Service API's, as well as all recent and upcoming updates.

From this site you can subscribe to be notified via email about upcoming updates. These updates may affect the performance and functionality of the Service API's which will affect your use of the Anyware Manager as a Service. To subscribe click on the **Subscribe to Updates** button at the top right of the screen and enter the email address you wish to be notified on.

An email will be sent to you shortly afterwards indicating that you have successfully subscribed to these updates.

# Retrieving Anyware Connector Version Numbers

Understanding the version number of a Connector can be useful when troubleshooting issues and to ensure you are running the latest version of the Connector. The Connector, from version 67 on, has a single version number. Previously, the installer and connector version numbers were different. These have now been combined to display a single version number going forward.

## Connector Installer Version

The installer is used for installing, updating and diagnosing issues related to the Connector installation process. It can be updated at the same time as the Connector, and also updated independent of the Connector as updates are made to improve installation specific areas. A change in the version of the installer does not require an upgrade to the Connector itself.

If you have downloaded the Connector installer you can obtain the version number by running one of the following commands (depending on where it has been copied to):

```
./cloud-access-connector --version
```

or

```
/usr/sbin/cloud-access-connector --version
```

A successful response is outlined below:

```
cloud-access-connector v66.0.63_9606001760
```

The first command should be used if you are currently in the same directory as the installer. This is more common for older versions of the installer. The second command is the location where newer versions of the installer have been copied to.

The Connector installer version also appears at the top of the output when you run an installation:

```
user@vm:~$ sudo /usr/sbin/cloud-access-connector install
[2021-02-03T17:16:01Z] INFO Set docker registry as: docker.cloudsmith.io/
teradici/cloud-access-connector
[2021-02-03T17:16:01Z] INFO Starting cloud-access-connector
version=v66.0.63_9606001760
...
```

It will also be logged by the installer:

```
user@vm:/var/log$ sudo more /var/log/cloud-access-connector/
install_2021-02-03T17-16-01.log
time="2021-02-03T17:16:01Z" level=info msg="Starting cloud-access-connector"
version=v66.0.63_9606001760
time="2021-02-03T17:17:14Z" level=error msg="You must accept the EULA and
Privacy Policy to continue."
...
```

You can also view the Connector installer version number from the [HP download](#) site when viewing the download filename.

## Connector Version

The Connector version, sometimes referred to as the YAML or compose file, denotes the combination of containers that make up a particular release of the Connector. The primary location to view the version of your running Connector is from the [Connectors page](#) in the Admin Console.

This version number represents a combination of specific versions of services that run on the Connector. For example, version 42 of the Connector includes the PCoIP Connection Manager 21.01.0. When troubleshooting issues, this version is used by HP's support team to inform them as to which version of each service is running on your Connector.

### Legacy Connector Versions

You should ensure that you keep this version as up to date as possible. We are continuously enhancing, adding features, fixing bugs and improving the overall security of the Connector. If you have a version that is v38 or lower, you should update your Connector as previous versions were integrated with an installer that predates our current Connector download location, and further installs or updates from that legacy installer may not work correctly.

If you are unable to access the Admin Console, you can obtain the version of the Connector from the configuration file itself, as outlined in the below example:

```
user@vm:/var/log$ cat /var/local/teradici/docker-compose.yaml | grep  
CACV2_VERSION  
  CACV2_VERSION: 42
```

# Anyware Connector Installer Issues

We have moved to a new distribution system and on December 31, 2020 the legacy system was shut down. As a result of this change some errors may occur for users with Connectors that were installed from older installer versions.

In almost all cases downloading the latest installer version and running the `cloud-access-connector install`, `cloud-access-connector update` or `cloud-access-connector diagnose` commands with the new install should work.

For information on this, see [here](#).

## Error Messages

The following are a list of potential error messages that a user may encounter as a result of the change of distribution system:

### Attempting to download the installer

#### Error 1

```
user@vm:~$ mkdir ~/v2connector && cd ~/v2connector
user@vm:~/v2connector$ curl -LO https://teradici.bintray.com/cloud-access-connector/cloud-access-connector-0.1.1.tar.gz
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 41 0 41 0 0 141 0 --:--:-- --:--:-- --:--:-- 141
user@vm:~/v2connector$ tar xzvf cloud-access-connector-0.1.1.tar.gz

gzip: stdin: not in gzip format
tar: Child returned status 1
tar: Error is not recoverable: exiting now
```



## Error 2

```

user@vm:~$ mkdir ~/v2connector && cd ~/v2connector
user@vm:~/v2connector$ curl -LO https://teradici.bintray.com/cloud-access-
connector/cloud-access-connector-0.1.1.tar.gz
  % Total    % Received % Xferd  Average Speed   Time    Time     Time
Current
                                 Dload  Upload  Total  Spent    Left  Speed
  0   0   0    0    0    0     0     0  --:--:--  --:--:--  --:--:--
0curl: (6) Could not resolve host: teradici.bintray.com

```

## Running older installer versions

If the Connector installer was installed before December 11, it may generate some of the following errors:

### Error 3

```

[2020-12-22T20:36:57Z] INFO Verifying installer version
[2020-12-22T20:36:57Z] ERROR yaml: unmarshal errors:
  line 1: cannot unmarshal !!str `The req...` into docker.ComposeConfig

```

### Error 4

```

[2020-12-22T20:07:09Z] INFO Downloading compose file
[2020-12-22T20:07:09Z] INFO curl: (60) SSL certificate problem: self signed
certificate
[2020-12-22T20:07:09Z] INFO More details here: https://curl.haxx.se/docs/
sslcerts.html
[2020-12-22T20:07:09Z] INFO
[2020-12-22T20:07:09Z] INFO curl failed to verify the legitimacy of the
server and therefore could not
[2020-12-22T20:07:09Z] INFO establish a secure connection to it. To learn
more about this situation and
[2020-12-22T20:07:09Z] INFO how to fix it, please visit the web page
mentioned above.
[2020-12-22T20:07:09Z] ERROR exit status 60

```

## Error 5

```
[2020-12-22T20:24:06Z] INFO Configuring Docker Daemon
[2020-12-22T20:24:06Z] INFO populateTrustAndKeyStore: Pulling setup container
and populating Java trust and key store
[2020-12-22T20:24:07Z] INFO Error response from daemon: error parsing HTTP
404 response body: invalid character '<' looking for beginning of value: "<!
doctype html><html lang=\"en\"><head><title>HTTP Status 404 - Not Found</
title><style type=\"text/css\">body {font-family:Tahoma,Arial,sans-serif;} h1,
h2, h3, b {color:white;background-color:#525D76;} h1 {font-size:22px;} h2
{font-size:16px;} h3 {font-size:14px;} p {font-size:12px;} a
{color:black;} .line {height:1px;background-color:#525D76;border:none;}</
style></head><body><h1>HTTP Status 404 - Not Found</h1><hr class=\"line\" /
><p><b>Type</b> Status Report</p><p><b>Description</b> The origin server did
not find a current representation for the target resource or is not willing to
disclose that one exists.</p><hr class=\"line\" /><h3>Apache Tomcat/8.5.59</
h3></body></html>"
[2020-12-22T20:24:07Z] ERROR exit status 1
```

## Error 6

```
[2021-02-11T01:02:42Z] INFO Error response from daemon: Head https://teradici-
docker-registry.bintray.io/v2/diagnostics/manifests/stable: unauthorized:
Unauthorized
[2021-02-11T01:02:42Z] ERROR exit status 1
```

# Anyware Connector Connectivity Issues

Anyware Manager as a Service provides some diagnostic checks that can be used to troubleshoot the cause of issues you may be experiencing with your Connector. Run the following command:

```
cd /usr/sbin
sudo ./cloud-access-connector diagnose
```

Please note that older installs and updates may still be in the legacy directory at `~/v2connector`.

This command can also be used to verify that your Connector has been correctly configured. The diagnostic checks cover Remote Workstation connectivity and Active Directory connectivity.

The following table lists the flags associated with this command:

Flag	Description
<code>--rw</code>	The Remote Workstation FQDN
<code>--ad</code>	Verify connectivity to currently configured Active Directory server
<code>-h --</code> <code>help</code>	help for diagnose
<code>--</code> <code>debug</code>	This flag can be run if you initial install of the Connector fails. It provides a detailed output of the Connector installation. This is useful for self-troubleshooting or to provide to the HP support team when logging a support ticket.

## Common Installation Issues with the Connector

For information on issues relating to failed Connector installations, We have a KB article that details troubleshooting steps for common issues related to installing the Connector, see [here](#).

### ⚠ Connector Upgrade and Diagnose Issues

Several previous versions of Connector installers are no longer compatible with our latest infrastructure upgrades. When you run the update or diagnose commands with these older versions you may receive errors such as "Error response from daemon: GET <https://docker.cloudsmith.io/.....: unauthorized>" for example. If this occurs you need to download the latest version of the Connector installer from [here](#).

## Remote Workstation Connectivity Check

This command will attempt to connect to the specified remote workstation on the ports required for establishing a PCoIP session. It checks to ensure that the PCoIP agent is running on the remote workstation.

Example command to diagnose remote workstation connectivity issues:

```
sudo ./cloud-access-connector diagnose --rw fqdn.of.my.rw
```

### Check Passes

- Your Connector is able to resolve the FQDN of the remote workstation and connect to it.
- The PCoIP agent is running and responding on the remote workstation.

### Check Fails

If the check fails it may be as a result of one or more of the following issues:

- Firewall or network routing rules or restrictions may be in place.
- A failure has occurred and the FQDN of the remote workstation cannot be resolved.
- The PCoIP agent on the remote workstation is not running or is unresponsive.

## Active Directory Connectivity Check

This command will attempt to connect to the Active Directory domain controller that was provided during installation using those same credentials.

Example command to diagnose Active Directory connectivity issues:

```
sudo ./cloud-access-connector diagnose --ad
```

### Check Passes

- The Connector is able to resolve the FQDN of the domain controller and authenticate to it.

### Check Fails

If the check fails it may be as a result of one or more of the following issues:

- Firewall or network routing rules or restrictions may be in place.
- A failure has occurred and the FQDN of the domain controller cannot be resolved.
- The Active Directory server may be unresponsive.
- The check was unable to authenticate to the Active Directory server.

# Anyware Connector Log Collection

The following section outlines how to view the logs and view the status of the Connector services and installer. This information can help troubleshoot issues relating to the Connector.

To view the status of all services in the Connector run the following command:

```
sudo docker service ls
```

To get logs from services run the following command:

```
sudo docker service logs [service]
```

The installer and update logs are saved in the `/var/log/cloud-access-connector/` directory. The runtime logs from the Connector services are saved in the `/var/lib/docker/containers/` directory. If you want to setup a log aggregator for the Connector you should point it to this directory. To disable log aggregation from the Connector you must ssh to the Connector and run the following command:

```
sudo docker service rm connector_sumologic
```

The following list details some of the important Connector services that will be included in the logs:

- `connector_activedirectorysync`: This service contains information or errors related to domain controllers. It contains information on what is transmitted to Anyware Manager and highlights any failures the AD might be having communicating to Anyware Manager.
- `connector_brokerexternal`: This service is only used for users connecting from outside the corporate network. It includes incorrect password and MFA errors, as well as errors with from the AD when authenticating a user. This service works with the Connection Manager and Security Gateway got session establishment.
- `connector_brokerinternal`: This service is only for users connecting from inside the corporate networks.
- `connector_cm`: This service contains information related to users connecting to their remote workstations. It includes usernames, source IP, PCoIP Client type and version information. It details any failures that may occur during authentication or brokering.

- `connector_cmsg`: This service is only used for users connecting from outside the corporate network.
- `connector_sg` This service is used for external communication to connect to the `connector_cmsg` component. It includes statistics on connections from PCoIP Clients to PCoIP Agents.
- `connector_connectorgateway`: This service includes basic network connection information, such as Client IP, response codes and records of which service or route the Client was trying to access.
- `connector_healthcheck`: This service provides the status of the Connector components that are passed to the Anyware Manager. It will highlight any errors with communication between the Connector and Anyware Manager. This information is also available in the Admin Console or via the Anyware Manager API's for the Connector.
- `connector_sumologic`: This service contains information or errors that occur when using sumologic to aggregate logs from the Connector.
- `connector_rwtelemetry` This service is responsible for reporting PCoIP session states for remote workstations in floating pools to Anyware Manager.

The runtime logs from the these services are saved in the `/var/lib/docker/containers/` directory.

# Support

## 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. HP staff are heavily involved in the forums.

To join the HP community, visit the [HP Knowledge Center](#).



# Getting Your Registration Code

You need a registration code to activate your PCoIP agent and to use it in conjunction with HP Anyware Manager as a Service. Once you subscribe to a Anyware Software subscription your registration code will be in an email sent to you from HP. 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](#).

If you do not have a subscription with us then you need to [contact sales](#) to find out about our subscriptions, components and solutions.