

PCoIP Management Console

24.03

Table of contents

PCoIP Management Console Overview	7
About PCoIP Management Console Releases	8
PCoIP Management Console Modes	9
PCoIP Management Console Free	11
PCoIP Management Console Enterprise	11
Quick Links	13
What's New in this Release	14
System Requirements	15
Management Console Formats	15
Online and Dark Site Packages	15
System Configuration and Requirements	16
Licensing for PCoIP Management Console	17
Port Numbers	17
Network	17
Browser Compatibility	18
PCoIP Endpoint Firmware	18
Where to Find Information about Other Components	19
Installation Guide	20
Installing the PCoIP Management Console and Configuring Your System	20
Installation Overview	20
Using IPv6 with Management Console	21
Management Console Host Requirements	21
Limitations	21
Installing PCoIP Management Console using vSphere	23
Installing PCoIP Management Console into AWS EC2	25
Deployment Considerations	25

Deployment	26
Management Console as an RPM	28
Management Console RPM Installation and Removal	29
Remove Management Console	32
Moving to a New Version of Management Console	34
Running Different PCoIP Management Console Versions in Parallel	35
Administrators' Guide	37
PCoIP Management Console Administrators' Guide	37
Getting Started	38
Log In to the PCoIP Management Console Web User Interface	38
Understanding the PCoIP Management Console Dashboard	43
Managing Licenses Online	48
Managing Licenses Offline	53
Uploading Endpoint Firmware to the PCoIP Management Console	59
Setting up Security	60
Active Directory Authentication	64
Identity Provider (IDP) Integration with Management Console (Enterprise)	70
Securing User Passwords	76
Securing PCoIP Management Console User Passwords	76
Accessing the PCoIP Management Console Virtual Machine Console	77
Changing the PCoIP Management Console Web Interface Default Password	82
Changing the PCoIP Management Console Virtual Machine Default 'Root' Password	85
Moving to a Newer Version	86
Migrating PCoIP Management Console to a Newer Release Using OVA	86
Upgrading using RPM	92
Moving Between IPv4 and IPv6	97
Migrating from PCoIP Management Console 1	105
Managing Firmware	111
Managing PCoIP Zero Client and Remote Workstation Card Firmware	111

Upgrading Endpoints to Firmware 5.0 or Later	112
Downgrading Endpoints to an Older Firmware	115
Discovering Endpoints	119
Discovery Process Overview	119
Configuring DHCP for Endpoints that use Auto Discovery	125
Configuring DNS for Endpoints that use Autodiscovery	130
Discovering Endpoints Manually from PCoIP Management Console	138
Managing Endpoints	141
Managing Endpoints	141
Managing Profiles	142
Organizing Endpoints into Groups	150
Auto Configuring Endpoints (Enterprise)	155
Auto Naming Endpoints	159
Requesting Endpoint Certificates Using SCEP (Enterprise)	161
Managing Schedules (Enterprise)	169
Hidden Endpoint Settings	176
Remote Endpoint Management (Enterprise)	194
Using the Endpoints Page	205
Endpoints Page Overview	205
Displaying Endpoint Properties	209
Using the ENDPOINT DETAILS Page	223
Performing Power Management	230
Powering Down PCoIP Zero Clients	230
Renaming Endpoints	233
Deleting Endpoints	234
Searching an Endpoint Table	235
Filtering the Endpoint List	236
Exporting an Endpoint List	239

Managing the Console	240
Creating and Managing User Roles	240
Managing Users	247
Managing PCoIP Management Console Logs	253
Creating and Managing PCoIP Management Console Certificates	256
Updating PCoIP Management Console Certificates after Endpoint Discovery	270
Uploading the PCoIP Management Console Certificate to an Endpoint	276
Configuring the Console Settings	279
Configuring PCoIP Management Console Session Timeout (Enterprise)	279
Configuring PCoIP Management Console web UI Time Zone	280
Default CentOS Configuration for PCoIP Management Console	281
Changing the Default Network Configuration	285
Configuring an Endpoint Manager Manually from an Endpoint	291
Managing PCoIP Management Console Databases	295
References	300
PCoIP Management Console 1 Profile Properties Renamed or Not Migrated	300
Time Zone Definitions for PCoIP Management Console 1 or later releases	316
Expanding the PCoIP Management Console Disk Size	322
Using your Virtual Machine Console to Administer Licenses when Connected to the Internet	324
Activating Licenses	324
Viewing Installed Licenses	325
View installed licenses via the command prompt:	326
Deactivating Licenses	326
Deactivating Your PCoIP Management Console License	327
HTTP Strict Transport Security	329
Chrony NTP Configuration	332
Disabling the Chrony	336
SSH Security Considerations	337
Disable Root Login	337

Limit User Logins	337
Disable SSH Protocol 1	338
Use Public/Private Keys for authentication and disable Password Authentication	338
Identity Provider(IDP) Integrations	340
Create Self-Signed Certificate	340
Okta Reference	343
Smartcard Authentication with SSO	357
PingFederate Installation Reference	380
PingFederate Configuration for Management Console	381
Firewall References	418
Configuring firewalld for New Installs of Management Console 20.04 or newer	418
Configuring firewalld after a Management Console Upgrade	428
Migrating PCoIP Management Console to a Newer Release Using firewalld	447
Removing Management Console iptables Configuration	452
Deleted Data When Migrating between IP Protocols	455
Troubleshooting	468
Troubleshooting	468
Troubleshooting Endpoints in Recovery Mode	469
Locating Endpoints in Recovery Mode	469
Recovery Mode Causes and Solutions	470
Recovery Mode Examples	471
Troubleshooting DNS	472
Viewing License Information via Command Line	475
Deactivating and Activating Licenses via Command Line	475
FAQ	476
FAQs	476
Support	477
Contacting Support	477
Finding the PCoIP Management Console Release Number	478

PCoIP Management Console Overview

Welcome to the PCoIP® Management Console Administrators' Guide. This documentation explains how to install and use your PCoIP Management Console to discover, configure, and manage your PCoIP Zero Client and Remote Workstation Card endpoints.

PCoIP® Management Console manages PCoIP Zero Clients and Remote Workstation Cards using the Tera2 chipset. For more information about these PCoIP endpoints, see the PCoIP Zero Client Firmware Administrators' Guide and Remote Workstation Card Firmware Administrators' Guide.

Support for PCoIP Zero Client and Remote Workstation Card firmware 4.x and earlier

If you are using PCoIP firmware 4.x or earlier, the corresponding PCoIP Management Console is version 1.x. See [PCoIP Management Console 1.x User Manual](#) for details.

PCoIP Management Console provides IT administrators with a browser-based console for managing PCoIP endpoints. You can quickly provision new endpoints, configure settings, and update firmware.

Based on Teradici's Management Protocol, the PCoIP Management Console delivers a secure and reliable way to configure and manage the endpoints in your PCoIP deployment.

PCoIP Management Console enables you to organize and manage PCoIP endpoints and their configurations in groups. Using PCoIP Management Console, you can:

- Display the status, health, and activity of your PCoIP deployment at a glance
- Discover endpoints in a variety of ways and automatically name and configure them
- Organize endpoints into multi-level groups
- Schedule firmware and configuration updates to endpoints based on their groups
- Reset endpoints to factory defaults and control their power settings
- Use custom certificates to secure your PCoIP system

PCoIP Management Console is packaged in a variety of formats for easy deployment. These formats are:

- **OVA:** An Open Virtual Appliance (OVA) format for quick and easy deployment on a VMware Horizon ESXi host
- **AMI:** An Amazon Machine Image (AMI) format for services delivered using Amazon Elastic Compute Cloud (EC2)
- **RPM:** Red Hat Package Manager (RPM) format to allow for efficient updates using any one of a variety of Linux operating system.

About PCoIP Management Console Releases

PCoIP Management Console underwent an architecture change since release 2.0 which is not compatible with all releases of endpoint firmware.

The following information identifies which firmware versions to use with your PCoIP Management Console deployment.

- PCoIP Management Console 3.x and higher manages PCoIP Zero Clients and Remote Workstation Cards using firmware 20.01 or higher.
- PCoIP Management Console 1.10 manages PCoIP Zero Clients and Remote Workstation Cards using firmware up to and including 4.9.
- We recommend using the latest firmware versions available at the time of the Management Console release.

PCoIP Management Console Release	Recommended PCoIP Zero Client Firmware	Recommended Remote Workstation Card Firmware
20.01+	20.01+	20.01+
2.0 - 19.11	5.x - 19.11	5.x - 19.11
1.10 (end of life)	Up to 4.8.2	Up to 4.9

In this guide, references to PCoIP Management Console will refer to the current release unless other releases are specifically identified.

PCoIP Management Console Modes

PCoIP Management Console is one product that operates in two modes—Enterprise and Free. PCoIP Management Console Enterprise requires activating a valid license to operate in Enterprise mode. The banner on the PCoIP Management Console's web interface identifies which mode you are running.

This document discusses both modes of operation and indicates differences in the features as they are introduced.

For information about PCoIP Management Console Free, license offers, term lengths, trial licenses, and the Support and Maintenance program see [PCoIP Management Console](#) on our web site. For more information about the differences between the two modes of operation. See [Comparison of PCoIP Management Console Enterprise and PCoIP Management Console Free](#).

The Web User Interface provides the user with some useful information that new users to Management Console will find helpful.

teradici®

PCoIP MANAGEMENT CONSOLE - FREE ¹
Release - 19.05.0 ²

You are using PCoIP Management Console Free. To learn more about PCoIP Management Console Enterprise features and subscribe to Teradici at sales@teradici.com or +1 604 628 1200. ³

USERNAME

PASSWORD

REMEMBER ME

Help | License Agreement | Support | teradici.com ⁴
Release - 19.05.0@10292 ²
© Copyright 2019 Teradici Corporation

1. Banner indicating if the version of Management Console is Free or Enterprise.

2. Installed release number in use.

3. Information on how to obtain Enterprise information

4. Links to documentation

PCoIP Management Console Free

PCoIP Management Console Free enables a single administrative user to manage a basic deployment of up to 100 endpoints, as well as to upgrade firmware, manage configuration profiles, and discover endpoints.

PCoIP Management Console Enterprise

PCoIP Management Console Enterprise enables large enterprise deployments to manage up to 20,000 endpoints from a single console as well as to upgrade firmware, manage configuration profiles, discover endpoints, schedule actions and configure remote endpoints. PCoIP Management Console Enterprise supports multiple administration users and includes the assurance of support and maintenance for Tera2 endpoint firmware. PCoIP Management Console Enterprise is available through HP Anyware subscriptions. PCoIP Management Console Enterprise reverts to Free mode when all licenses expire.

Comparison of PCoIP Management Console Enterprise and PCoIP Management Console Free

Feature Comparison	Enterprise	Free
Price	See All Access Plans	\$0
Multi-device support	Up to 20,000 PCoIP Zero Clients & PCoIP Remote Workstation Cards	Up to 100 PCoIP Zero Clients & PCoIP Remote Workstation Cards
Apply firmware updates		
Device profile, filtering/delete		
Power down/reset		
Deployment dashboard		
Multi-level group organization		
Device factory reset		
One-time & recurring schedules		
Auto discovery & configuration		
SCEP Support		
Multiple administrator accounts		
Role-based access with granular permissions		
Active Directory support		
Concurrent user access		
Inventory reporting		
Remote device management		
Zero Client / Workstation Card peering		
Export / Import endpoint group profiles		
Offline license activation		
Support & Maintenance: Software, Zero Client Firmware and Remote Workstation Card Firmware		

Quick Links

The following links contain information you will need when you first download and install the PCoIP Management Console:


- For information about deployment platforms, system specifications, browser compatibility, and PCoIP endpoint firmware specifications, see [System Requirements](#).
- For instructions on how to activate your license, see [Managing Licenses Online](#).
- For instructions on how to get up and running quickly, see [Installing the PCoIP Management Console and Configuring Your System](#).
- For instructions on how to migrate your PCoIP Management Console 1 to PCoIP Management Console release 2.x or later, see [Migrating from PCoIP Management Console 1](#).

What's New in this Release

PCoIP Management Console version **24.03** is a release with security updates over release **23.12.2**.

System Requirements

The PCoIP Management Console is intended for deployment within a secured corporate network for the management of PCoIP endpoints that are internal or external (Enterprise) to the network.

 **Note: PCoIP Management Console must not be accessible from unsecured networks**

The PCoIP Management Console must only be accessible by endpoints from the open Internet as described within this guide. Any other exposure to the open Internet is an unsupported use of the product and will void any warranty.

Management Console Formats

PCoIP Management Console is released in three formats that feature CentOS 7.9 64 bit as the PCoIP Management Console installation OS. The first called Open Virtual Appliance (OVA) format with supported hypervisor platforms of VMware ESXi 6.5, 6.7 and 7.0. The second format is the Amazon Machine Image (AMI) format for services delivered using Amazon Elastic Compute Cloud (EC2). The third format is RPM which is one standard for Linux Administrators to manage software installations.

Online and Dark Site Packages

RPM formatted versions of PCoIP Management Console may require additional steps for installation, upgrades or licensing. Installations and upgrades occasionally require dependency updates to your Management Console host operating system before using the Management Console RPM.

If you are a Dark Site customer, you must have all the available MC RPM dependencies installed in the Management Console host operating system along with the Dark Site package for RPM prior to the RPM update.

The following RPM packages have been provided for download and are included in installation and upgrade instructions when needed to get you up and running quickly.

- **Online dependency package:** This package contains PostgreSQL 14.8, Python 3, installation and upgrade scripts.
- **Dark Site package for RPM:** This package contains Management Console RPM, PostgreSQL 14.8, Python 3 upgrade installation and upgrade scripts, and Java 8 upgrade package.
 - For installations that require licensing when there is no internet access see [Managing Licenses Offline](#).

System Configuration and Requirements

Update your software to the current release

From time to time, updates may be made available from support, or the developers of CentOS. While we recommend staying current on releases, it is also recommended that you test updates on a test system prior to upgrading your production system or back up a snapshot of the PCoIP Management Console before running the update.

PCoIP Management Console requires the following minimum system configuration and requirements:

OVA format	AMI format	RPM format
<ul style="list-style-type: none"> • 4 CPUs • 12 GB RAM • 62 GB hard drive space 	<ul style="list-style-type: none"> • 4 vCPUs • 12 GB RAM • 62 GB hard drive space • Recommended instance type: m5.xlarge 	<ul style="list-style-type: none"> • 4 CPUs or vCPUs • 12 GB RAM • 20 GB free hard drive space ¹ • dependency package (offline and online installations) • CentOS 7.9, RHEL 7.9, RHEL 8.6, RHEL 8.8

⚠ Caution: Lowering minimum system requirements

Changing minimum system requirements, such as lowering RAM to 4 GB may produce error messages such as **Waiting for the server to start. Please refresh the page to try again**

Minimum requirements help ensure you have the greatest chance for a successful deployment.

Licensing for PCoIP Management Console

PCoIP Management Console requires access to the activation server on the Internet, directly on port 443 or via a proxy, in order to activate a license. For more information, please see [Managing Licenses Online](#).

Port Numbers

The PCoIP Management Console uses the following ports with both formats:

- **Inbound port 443:** HTTPS for access to the web interface (administrative interface)
- **Inbound port 5172:** PCoIP Management Protocol (management interface)
- **Outbound port 5172:** PCoIP Management Protocol required for manual discovery only
- **Outbound port 443:** HTTPS (licensing interface)
- **Inbound port 8080:** Redirects port 80 to 8080
- **Inbound port 8443:** Redirects port 443 to 8443
- **Inbound port 22:** TCP (for SSH)

Network

• IP Address Configuration

The PCoIP Management Console supports both pure-IPv4 and pure-IPv6 networks, and can join any network that is using DHCP. The PCoIP Management Console also supports static IP addressing. HP recommends giving the PCoIP Management Console a fixed IP address, either through a DHCP

reservation or by assigning a static IP address. See [Assigning a Static IP Address](#) and [Using IPv6](#) for further details.

- **Network Latency**

PCoIP Management Console supports networks with latency under 100 ms.


Browser Compatibility

PCoIP Management Console supports the release of each browser available at the time of product release, with the exception of Internet Explorer:

- Firefox
- Chrome
- Microsoft Edge

PCoIP Endpoint Firmware

HP recommends using the latest version of firmware for PCoIP endpoints. For the latest information on current and supported versions, see the [HP Support Center](#) for your product page.

 **PCoIP Management Console requires PCoIP endpoints have a minimum firmware release installed**

Management Console 20.xx can manage PCoIP Zero Client firmware 5.x and newer. Check release notes for any special considerations when managing firmware with Management Console.

-
1. Minimum 20 GB of FREE disk space dedicated specifically to Management Console use. You can increase this recommended size by the space necessary for the CentOS operating system and any other files required on your Linux system. ←

Where to Find Information about Other Components

This guide describes the PCoIP Management Console.

For tips and suggestions to get the best experience from your PCoIP endpoint deployment:

- [PCoIP Session Planning Guide](#)

For more information about PCoIP endpoints managed by PCoIP Management Console, see either of the following:

- [PCoIP Zero Client Administrators' Guide](#)
- [Remote Workstation Card Administrators' Guide](#).

Installation Guide

Installing the PCoIP Management Console and Configuring Your System

The topics in this section contain information to help you get up and running quickly.

Topics that refer to specific versions of PCoIP Management Console will be identified by the release number.

Migrating, upgrading, or downgrading from other versions

If you are migrating to a new PCoIP Management Console version see [Migrating to a Newer Version](#). If you need to downgrade endpoints from firmware 20.01 or higher to an older version, see [Downgrading Endpoints to Older Firmware](#).

Installation Overview

PCoIP Management Console is released in three formats. The first called Open Virtual Appliance (OVA) format with supported hypervisor platforms of VMware ESXi 6.5, 6.7 and 7.0. The second format is the Amazon Machine Image (AMI) format for services delivered using Amazon Elastic Compute Cloud (EC2). The third format is RPM which is one standard for Linux Administrators to manage software installations.

OVA and AMI installations contain all dependencies required for Management Console and provide for an easy first time install.

RPM releases may require the installation of a dependency package for either online or offline (dark site) deployments. If required, these packages will be available from the support site download area and may change with each release. To obtain a supported download, go to the version of Management Console you require and download the available download required for your deployment.

Using IPv6 with Management Console

Management Console 20.07 and newer versions support pure IPv4 or pure IPv6 networks; hybrid or dual stacked networks are not supported. In a pure IP deployment, Management Console only stores and displays the PCoIP endpoint data that is relevant to the IP version of the Management Console NIC. This means that when migrating between networks, data that is not relevant to the new network is permanently deleted. Please see [Deleted Data When Migrating between IP Protocols](#) for details.

Management Console will automatically display the IP information such as ip addresses relative to it's configured NIC. For example, if the NIC is configured for IPv6, all endpoint properties will display their IPv6 information. Searching for PCoIP endpoints will only display properties for endpoints in IP-only networks.

Management Console supports DHCPv6 with and without SLAAC configurations. The Web UI can be accessed by either a manual, DHCPv6, or SLAAC IPv6 address depending on the network configuration and the Management Console NIC configuration.

Management Console Host Requirements

- Only one NIC can be configured with one IP version
- Must be able to **ping** and communicate with PCoIP endpoints
- Must have an internet connection
- Firewall must be configured before installing Management Console
- PCoIP endpoints must be using firmware 20.07 or higher

Limitations

In an environment with DHCPv6 without SLAAC, there is a limitation between the caching systems of the Management Console CentOS host operating system and administrators using Windows-based

clients to access the Web UI. This limitation prevents a connection on the initial connection to the Management Console Web UI. This limitation requires any of two work arounds to fix the issue.

1. Configure a static route from the Management Console CentOS host operating system to Windows host (MC Client). This can be done by issuing a command similar to:

```
sudo ip -6 route add via link local address of Windows host dev Ethernet name in CentOS
```

Example:

```
sudo ip -6 route add 3505:b900:9000:19::/64 via fe80::e887:4e5d:fab7:cc dev eth0
```

2. From the Management Console host operating system, ping the administrators Windows computer that is accessing the Management Console Web UI prior to the first connection.

Information on IPv6 is included in the Installation and Migration topics for all formats of Management Console.

Installing PCoIP Management Console using vSphere

Once you have downloaded PCoIP Management Console, deploy it as an Open Virtual Appliance (OVA) using vSphere Client. The following instructions apply to deployments in IPv4 networks. Installations into pure IPv6 networks require an additional firewall configuration. See [New Installation of Management Console OVA format in IPv6](#).

To install PCoIP Management Console using vSphere Client:

1. Download the latest PCoIP Management Console OVA file to a location accessible from your vSphere Client.
2. Log in to your vSphere Client.
3. If you have more than one ESXi host, select the desired ESXi node; otherwise, there is no need to select a node.
4. From the vSphere client's *File* menu, select **Deploy OVF Template**.
5. In the *Source* window, click **Browse**, select the PCoIP Management Console's OVA file, click **Open** and **Next**.
6. In the *OVF Template Details* window, view the information and click **Next**.
7. In the *End User License Agreement* window, read the EULA information, click **Accept** and then **Next**.
8. In the *Name and Location* window, enter the name for your PCoIP Management Console and click **Next**.
9. In the *Host/Cluster* window, select the ESXi host on which you want to deploy the PCoIP Management Console and click **Next**.
10. In the *Storage* window, select the local disk or SAN where you wish to deploy the PCoIP Management Console and click **Next**.
11. In the *Disk Format* window, select a thick or thin provision option and click **Next**.
12. In the *Network Mapping* window, select the network or VLAN where you wish to deploy the PCoIP Management Console and click **Next**.
13. In the *Ready to Complete* window, view your settings, enable Power on after deployment (if desired), and click **Finish**.

14. When you see the 'Completed Successfully' message, click **Close**.
15. Make a note of the IP address of your PCoIP Management Console's virtual machine (VM) to log in to your PCoIP Management Console from a browser.
16. To activate PCoIP Management Console Enterprise, see [Managing Licenses Online](#).

NEW INSTALLATION OF MANAGEMENT CONSOLE OVA FORMAT IN IPV6

See [Using IPv6](#) for an overview of IPv6 with Management Console.

TO DEPLOY MANAGEMENT CONSOLE OVA IN AN IPV6 ENVIRONMENT PERFORM THE FOLLOWING STEPS:

1. Deploy Management Console OVA in an IPv6 environment with the guidance from steps 1-16.
2. Configure the firewall for IPv6.
Installations into IPv6 networks require you make firewall configurations for IPv6. See [OVA New Installations: To configure firewalld in IPv6 environment](#).
3. Confirm your IP address.
DHCPv6 networks that are SLAAC enabled will display two addresses which can be used to access Management Console.

```
ip a
```
4. Access Management Console via an IPv6 address.

Installing PCoIP Management Console into AWS EC2

The PCoIP Management Console AMI is a conversion of the OVA file into the Amazon Machine Image (AMI) format with SSH enabled to permit secure administrative access.

The virtual machine is made available for users of the PCoIP Management Console that wish to move more of their deployment to the cloud—especially those deploying Amazon WorkSpaces with PCoIP Zero Clients.

Non-System Requirements

- Amazon Web Services account with access to deploying EC2 instances
- SSH client

Deployment Considerations

Ensure you have the [Port Numbers](#) opened and all inbound ports are restricted to your corporate network and you meet the [System Configuration](#) requirements for your PCoIP Management Console.

Important: PCoIP Management Console must not be accessible from unsecured networks

The PCoIP Management Console must only be accessible by endpoints from the open Internet as described within the PCoIP Management Console Administrators' Guide. Any other exposure to the open Internet is an unsupported use of the product and will void any warranty.

Info: Notable network behaviors

Network usage can be higher when firmware is being uploaded to endpoints. A permanent web socket connection is maintained to every online endpoint

Deployment

To deploy PCoIP Management Console AMI:

1. Log in to AWS Console.
2. Choose the region the AMI resides in.
3. Navigate to EC2.
4. Navigate to AMIs.
5. Search Public AMIs for the AMI ID in your region. A list of AMI ID's are presented when clicking on the AMI download button seen after accepting the EULA from the Management Console [download](#) section of the support site.
6. Select the **PCoIP Management Console AMI** and click **Launch**.
7. Choose an Elastic Network Adapter (ENA) supported instance type (m5.xlarge recommended - see [system requirements](#)).
8. Configure the AWS Launch steps 2-5 as appropriate for your organization.
9. Select or create a security group in step 6 that will provide access to the required ports, with the inbound ports restricted to only your corporate network. Ensure network access is appropriate such that administrators are able to access ports 22 and 443, and that endpoints can access port 5172.

Important: Connectivity issues

If you are unable to get this access working, you will need to review your VPC configurations (VPCs, Subnets, Route Tables), Security configurations (Network ACLs, Security Groups), and possibly VPN Connections or Direct Connect settings.

10. Complete the steps.
11. When Launching, select a keypair. To ssh into the instance you will use the user **admin** in conjunction with the keypair you used on launch.
12. After accessing Management Console via an SSH client such as PuTTY, follow the same migration steps [Moving between IPv4 and IPv6](#) for switching IPv4 to IPv6 and vice versa.
13. After the Management Console is deployed, it is important the system is appropriately secured.

Accessing Management Console Web UI

You cannot access Management Console Web UI using ports 8080 or 8443

Related Information

[Securing PCoIP Management Console User Passwords](#)

[Default CentOS Configuration for PCoIP Management Console](#)

[Setting up Security](#)

[Managing Licenses Online](#)

[PCoIP Management Console Remote Endpoint Management \(Enterprise\)](#)

Management Console as an RPM

The Management Console RPM allows administrators an opportunity to manage and control Linux packages in a way that complies to their individual corporate IT policies. The **teradicimc-
<version>.rpm** package, when connected to the internet, will automatically update any required dependencies not available on your Linux VM so you can be operational quickly. The RPM is provided as a file for download. A public RPM repository will be available for seamless installs in a future release.

By introducing this RPM package into your network, you accept that there are risks involved in deploying the system, and you acknowledge that you have reviewed the default PCoIP Management Console and CentOS configuration and have performed any other changes to make the security level appropriate for your deployment.

Update your software to the current release

From time to time, updates may be made available from support, or the developers of CentOS. While we recommend staying current on releases, it is also recommended that you test updates on a test system prior to upgrading your production system or back up a snapshot of the PCoIP Management Console before running the update.

Linux Proficiency

It is expected that administrators of Linux operating systems are proficient at using the Linux OS and have an account with **sudo** access. Different Linux distributions may require different procedures. We use the Linux CentOS distribution for instructional information.

Dedicated Host

It is recommended that the Management Console host be dedicated for Management Console use only.

Minimum Requirements Validation

The Management Console RPM package will check for the minimum hardware resource requirements (CPU, disk, ram) and fail if it is not met. To disable the minimum requirement check, enter the following command:

```
sudo MC_NO_CHECK=1 rpm -Uvh teradicimc-<mc_version>.rpm
```

Disabling the minimum requirements check is not recommended! Lowering minimums may reduce Management Console performance, particularly in large deployments.

Management Console RPM Installation and Removal

Management Console and [additional dark site and online downloads](#) are provided with everything needed in order to get Management Console to work except the firewall exceptions. After installation, make sure that you have configured your firewall and that it complies to your corporate security policies. If you don't have a security policy, you can review the [firewall reference](#) that will allow you to get an understanding of what firewall requirements Management Console needs to be operational. Once the firewall exceptions are made, you can upgrade or remove the Management Console as required.

Directions for upgrades are described in [Upgrading Management Console Using RPM](#).

There are two different scenarios that require slightly different steps when installing or upgrading Management Console using the RPM. One scenario has Management Console deployed on a site that has access to the Internet and the other scenario is having Management Console deployed on a dark site where there is no internet access.

Online Installation using RPM

These instructions apply to the **first time installation** of Management Console on a host Linux machine that contains the RPM and any required packages for this release. The administrator installing the RPM should have sudo privileges.

1. Download the [available RPM](#) and applicable online dependency file for this release from the [support site](#) and ensure they are located on the Management Console Linux VM.

You can use a third party tool such as WinSCP to copy and move files into the CentOS/RHEL host operating system.

2. Install the online dependency file from the directory where the online dependency file is located.

- CentOS 7.9 and RHEL 7.9

```
sudo sh ./teradicimc_<mc_version>-online-dependency-centos-rhel7.9.tar.gz
```

- RHEL 8.6, 8.8

```
sudo sh ./teradicimc_<mc_version>-online-dependency-rhel8.tar.gz
```

3. Verify PostgreSQL version is 14.8

```
psql -V
```

Example:

```
[root@localhost ~]# psql -V
psql (PostgreSQL) 14.8
[root@localhost ~]#
```

4. Install the RPM using the commands of your Linux distribution.

- CentOS 7.9

```
sudo yum install teradicimc-<mc_version>.rpm from the directory where the rpm file is located.
```

- RHEL 7.9

```
sudo subscription-manager repos --enable rhel-7-server-optional-rpms --enable rhel-7-server-extras-rpms
```

```
sudo yum install https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
```

```
sudo yum install teradicimc-<mc_version>.rpm from the directory where the rpm file is located.
```

- RHEL 8.6, 8.8

```
sudo subscription-manager repos --enable rhel-8-for-x86_64-baseos-rpms --enable rhel-8-for-x86_64-appstream-rpms
```

```
sudo yum install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

```
sudo yum install teradicimc-<mc_version>.rpm from the directory where the rpm file is located.
```

5. Verify the Java version is 1.8.0_372 or newer.

```
java -version
```

Example:

```
[root@localhost ~]# java -version
openjdk version "1.8.0_372"
OpenJDK Runtime Environment (build 1.8.0_372-b07)
OpenJDK 64-Bit Server VM (build 25.372-b07, mixed mode)
[root@localhost ~]# █
```

6. Configure your firewall.

- IPv4

See the firewall reference on how [to configure Management Console firewall for use in an IPv4 environment perform the following steps:](#)

- IPv6

See the firewall reference on how [to configure Management Console firewall for use in an IPv6 environment perform the following steps:](#)

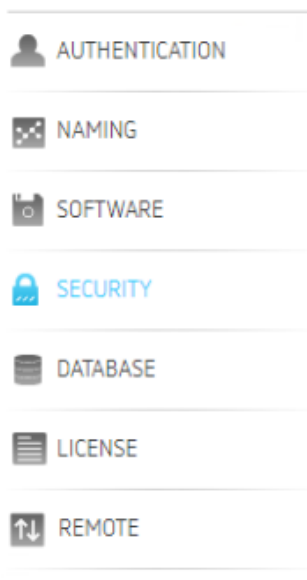
7. If applicable, enable your HSTS policy. See [HTTP Strict Transport Security](#).

8. If installing Management Console Enterprise, license your installation.

- See [Managing Licenses Online](#).
- If applicable see [Managing Licenses Offline](#).

New default self-signed certificate

Management Console began using a new default self-signed certificate as of 23.08. Certificate details can be verified in SETTINGS > SECURITY under CERTIFICATES.



SECURITY

SESSION

CERTIFICATES

ACTIVE DIRECTORY CERTIFICATES

UPDATE

REVERT SELF-SIGNED CERTIFICATE

Allows you to set up security requirements for the Management Console:

Management Console Security Certificate

Security Certificate: ?

Subject: localhost

Issued By: localhost

Expiration Date: 2032-01-01 10:09 PM UTC

Security Chain: ?

Subject:

Issued By:

Expiration Date:

Remove Management Console

To remove Management Console, you will have two choices, remove Management Console or remove Management Console with all its dependencies.

Ignore warning message

Please ignore the following warning message as it does not have any impact on the Management Console removal process.

warning: file remove failed: No such file or directory.

REMOVE ONLY MANAGEMENT CONSOLE

To remove Management Console only run the following command:

```
sudo yum remove teradicimc
```

REMOVE MANAGEMENT CONSOLE WITH ALL DEPENDENCIES

To remove Management Console and any package that was required by Management Console, run the following command:

```
sudo yum autoremove teradicihc
```

REMOVE POSTGRESQL

To remove PostgreSQL, run the following command:

```
psql -U <username>  
drop database <mc_database_name>;  
\q  
sudo yum remove postgresql\*
```

Moving to a New Version of Management Console

If you are upgrading from an older version of PCoIP Management Console, you may have additional steps or considerations to review. Review the relevant topics particular to your upgrade path.

- [Upgrading using OVA](#)
- [Upgrading using RPM](#)
- [Migrating from Management Console 1](#)
- [Moving Between IPv4 and IPv6](#)
- [Migrating to firewalld](#)

Running Different PCoIP Management Console Versions in Parallel

During the migration process to a new PCoIP Management Console, you will need to run both PCoIP Management Console 1 (which has reached End of Support as of April, 2020) and the new PCoIP Management Console in parallel. You may also need to operate two versions of the PCoIP Management Console if you have endpoints that cannot be updated to firmware version 20.01 or higher.

 **Note: Test a small number of endpoints first before upgrading all the endpoints**

Test a small number of endpoints before upgrading all the endpoints in your system. Place them in a test group in a segregated network. If you are using automatic discovery, this may require modifications to your DHCP options or DNS SRV records.

An endpoint can only be managed by one PCoIP Management Console at a time. If you are using DHCP options discovery and you plan to keep some of your endpoints managed by PCoIP Management Console 1, you can configure your DHCP server with the PCoIP Endpoint MC Address option on a scope-by-scope basis. See [Configuring Endpoints using Auto Discovery](#) for details.

 **Note: Ensure different versions of PCoIP Management Console have different IP addresses**

If you are running PCoIP Management Console 1 in parallel with a newer PCoIP Management Console, ensure the two versions of the PCoIP Management Console have different IP addresses.

The table shown next lists interoperability issues when running a newer release of PCoIP Management Console in parallel with PCoIP Management Console 1 which has reached End of Support as of April, 2020.

Current versions of PCoIP Management Console and PCoIP Management Console 1 Interoperability

Category	PCoIP Management Console (2.x to Current Version)	PCoIP Management Console 1 (1.10.8) End of Support
Endpoint firmware	PCoIP endpoints must run firmware 20.01 or higher. PCoIP Management Console cannot discover and manage endpoints running previous versions of the firmware.	PCoIP Endpoints must run a 4.x firmware version. PCoIP Management Console 1 cannot discover and manage devices running firmware 20.01 or higher.
DHCP/DNS discovery	Current versions of PCoIP Management Console use a different format for DHCP options and DNS SRV records from PCoIP Management Console 1.	For information on DHCP and DNS discovery for PCoIP Management Console 1, see the PCoIP Management Console 1.x User Manual .
Management	PCoIP endpoints are managed by at most one PCoIP Management Console.	PCoIP Zero Clients can be managed by more than one PCoIP Management Console 1 simultaneously.
Database	Cannot import PCoIP Management Console 1 database.	Importing a database from a current version of PCoIP Management Console is not supported
Profiles	You can import PCoIP Management Console 1.10.x profiles.	Importing profiles from a current version of PCoIP Management Console is not supported
Communication	Does not communicate with PCoIP Management Console 1.	Does not communicate with current versions of PCoIP Management Console.

Administrators' Guide

PCoIP Management Console Administrators' Guide

RPM upgrades may require new certificates uploaded to your endpoints

If you are upgrading to Management Console 24.03 from version 23.06 or earlier, and if you are not using custom certificates, you must upload the [new Management Console certificate](#) to your endpoints. For the new Management Console certificate SHA-256 & SHA-512 values, see the [release notes](#).

For instructions on how to upload your certificate see [Updating PCoIP Management Console Certificates after Endpoint Discovery](#)

Prior to upgrading Management Console you can:

- Clear the management state on all your endpoints **before** the upgrade and rediscover them after the upgrade.
- Ensure that the new certificate is uploaded to your endpoints **before** you upgrade to Management Console 24.03.

Welcome to the PCoIP Management Console Administrators' Guide.

The PCoIP Management Console is an Enterprise level management software appliance that allows ease of management of PCoIP endpoints through a single interface. With Management Console Enterprise, administrators can quickly and easily provision new devices, peer PCoIP Zero Clients with Remote Workstation Cards, report on inventory, review metrics, configure settings, and update firmware from a single console.

Getting Started

Log In to the PCoIP Management Console Web User Interface

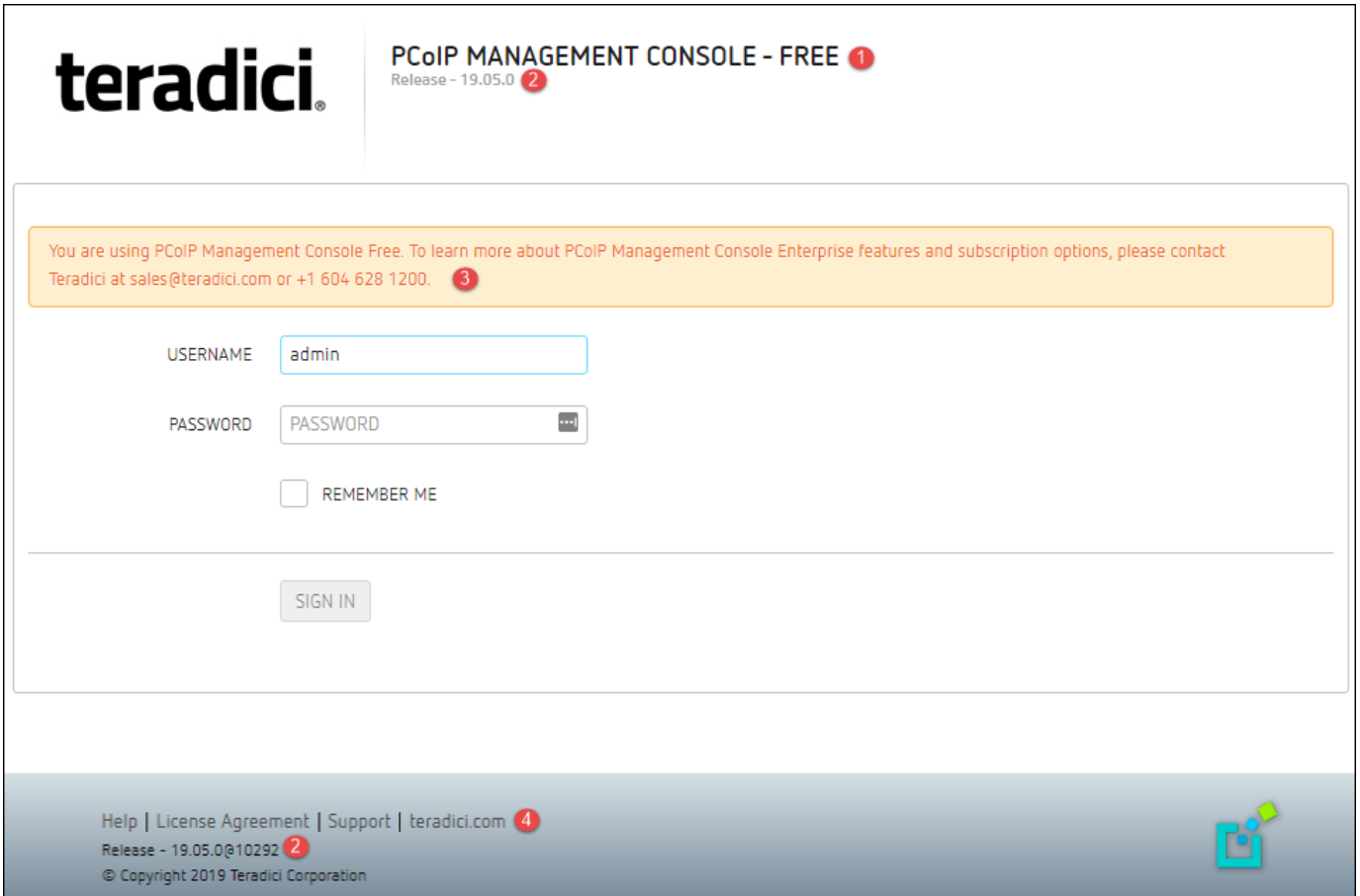
This section assumes that the PCoIP Management Console is configured to connect to your network. If you used DHCP to assign the IP address, then you will be able to continue in this section. If you require static IP addresses, see [Changing the Default Network Configuration](#) for instructions prior to continuing.

Before accessing the PCoIP Management Console web user interface (UI) from your browser for the first time, ensure that the following are in place:

- Your license has been activated for PCoIP Management Console Enterprise. See [Activating Licenses](#).
- You know the IP address of your PCoIP Management Console virtual machine. To locate the address:
 - Using vSphere Client, log in to your vCenter server.
 - In the *Inventory* list, select **VMs and Templates**.
 - Select your PCoIP Management Console virtual machine and then click the **Summary** tab.
 - Note the IP address in the *General* pane.

Using the Web Interface for the First Time

The Management Console's Web User Interface (Web UI) contains information that can be useful when troubleshooting issues. These references are identified in the following web user interface login screen example.



WebUI Area	Description
1	Identifies if you are using FREE or licensed ENTERPRISE mode of PCoIP Management Console
2	Identifies the release number of your Management Console
3	Informational message advising on how to upgrade to ENTERPRISE if new features are required
4	Links to find further information. <ul style="list-style-type: none"> • Help: redirects you to the current product page of Management Console • License Agreement: Displays the license agreement for your installed Management Console • Support: Redirects you to the support site • teradici.com: Links to our web page where you can quickly find further information such as white papers and the latest information on new products

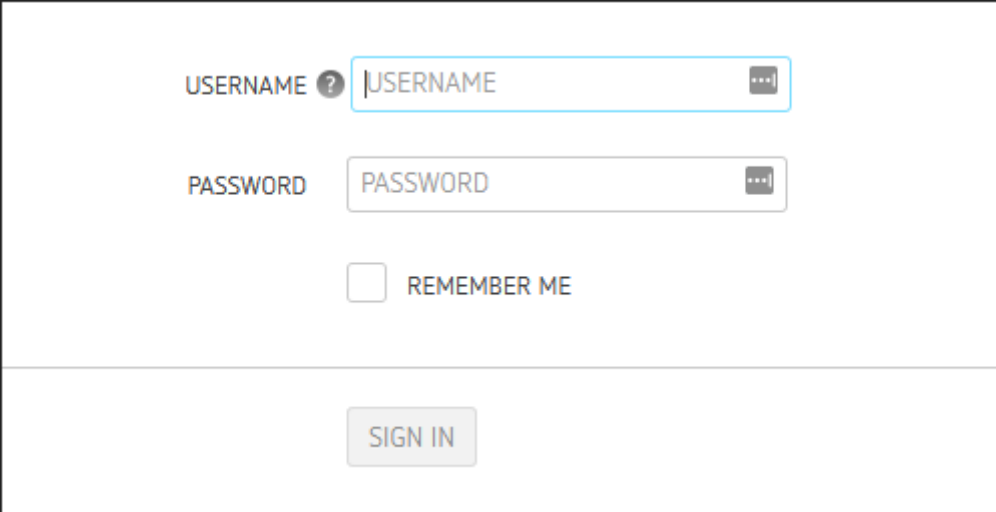
Note: The Web UI admin account for PCoIP Management Console is different "from the virtual machine admin account"

The default **admin** account that you use when first logging in to the PCoIP Management Console web UI is *not* the same **admin** account you use for logging in to the PCoIP Management Console virtual machine console.

To log in to the PCoIP Management Console web interface:

1. In your browser's address bar, enter the IP address of the PCoIP Management Console virtual machine. See [Installing PCoIP Management Console using vSphere](#).
2. At the PCoIP Management Console login screen, enter the web interface credentials.

- USERNAME **admin**
- PASSWORD **password**



USERNAME ? USERNAME

PASSWORD PASSWORD

REMEMBER ME

SIGN IN

Login Screen

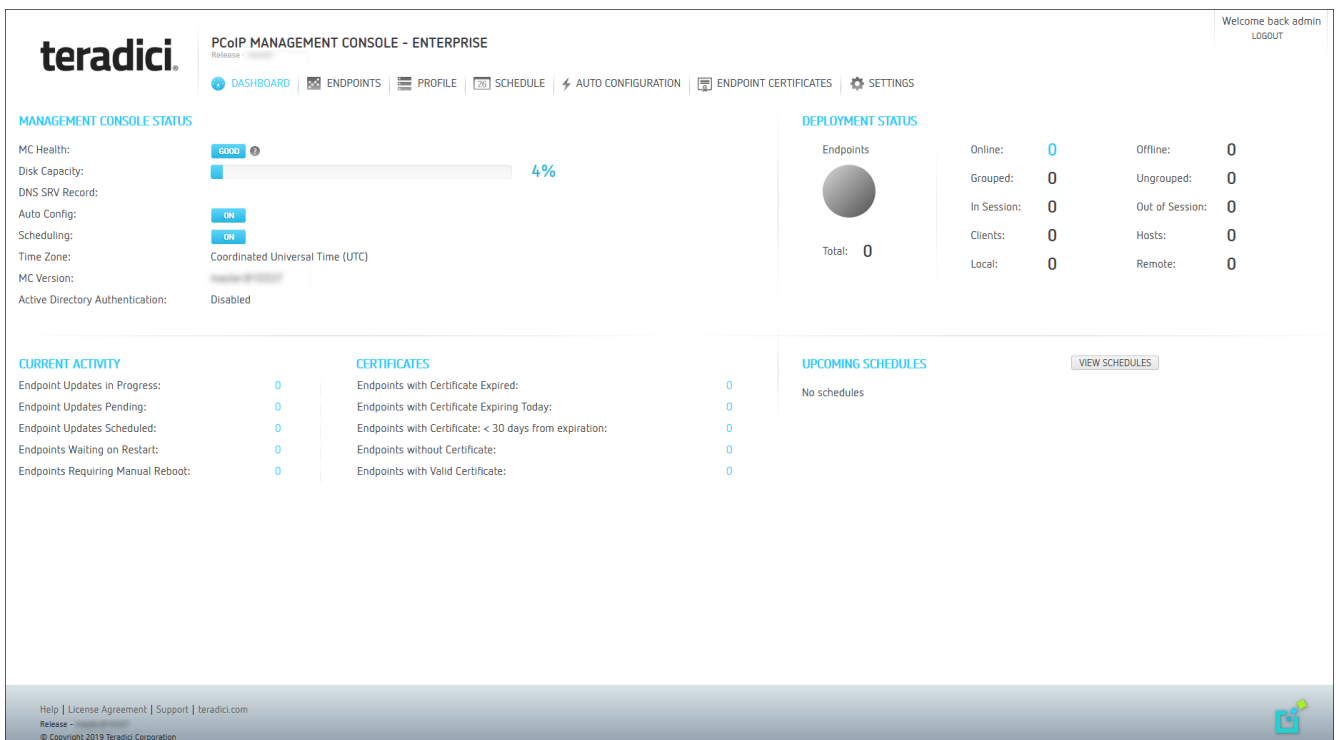
Note: Changing default settings

In order to change the PCoIP Management Console's default settings and run various scripts, you must connect to the PCoIP Management Console's virtual machine console and log in. See [Accessing the PCoIP Management Console Virtual Machine Console](#)

1. Click **SIGN IN**. If login is successful, the PCoIP Management Console dashboard displays in your browser window.

PCoIP Management Console Enterprise

The next example shows the PCoIP Management Console Enterprise dashboard. The banner will indicate PCoIP Management Console Free if you are running in free mode.



teradici PCoIP MANAGEMENT CONSOLE - ENTERPRISE

Welcome back admin
LOGOUT

DASHBOARD | ENDPOINTS | PROFILE | SCHEDULE | AUTO CONFIGURATION | ENDPOINT CERTIFICATES | SETTINGS

MANAGEMENT CONSOLE STATUS

MC Health: GOOD

Disk Capacity: 4%

DNS SRV Record:

Auto Config: ON

Scheduling: ON

Time Zone: Coordinated Universal Time (UTC)

MC Version:

Active Directory Authentication: Disabled

DEPLOYMENT STATUS

Endpoints

Total: 0

Online:	0	Offline:	0
Grouped:	0	Ungrouped:	0
In Session:	0	Out of Session:	0
Clients:	0	Hosts:	0
Local:	0	Remote:	0

CURRENT ACTIVITY

Endpoint Updates In Progress:	0
Endpoint Updates Pending:	0
Endpoint Updates Scheduled:	0
Endpoints Waiting on Restart:	0
Endpoints Requiring Manual Reboot:	0

CERTIFICATES

Endpoints with Certificate Expired:	0
Endpoints with Certificate Expiring Today:	0
Endpoints with Certificate: < 30 days from expiration:	0
Endpoints without Certificate:	0
Endpoints with Valid Certificate:	0

UPCOMING SCHEDULES

No schedules

[VIEW SCHEDULES](#)

Help | License Agreement | Support | teradici.com
Release -
© Copyright 2019 Teradici Corporation

PCoIP Management Console Web UI User Account Lockout

The PCoIP Management Console inhibits automated system attacks on its web UI. If a user login fails 6 times within a 30-minute period, that user account will be locked out for 30 minutes. If this occurs, the login screen will display the message shown next.

Sorry, your account is locked.

USERNAME

PASSWORD

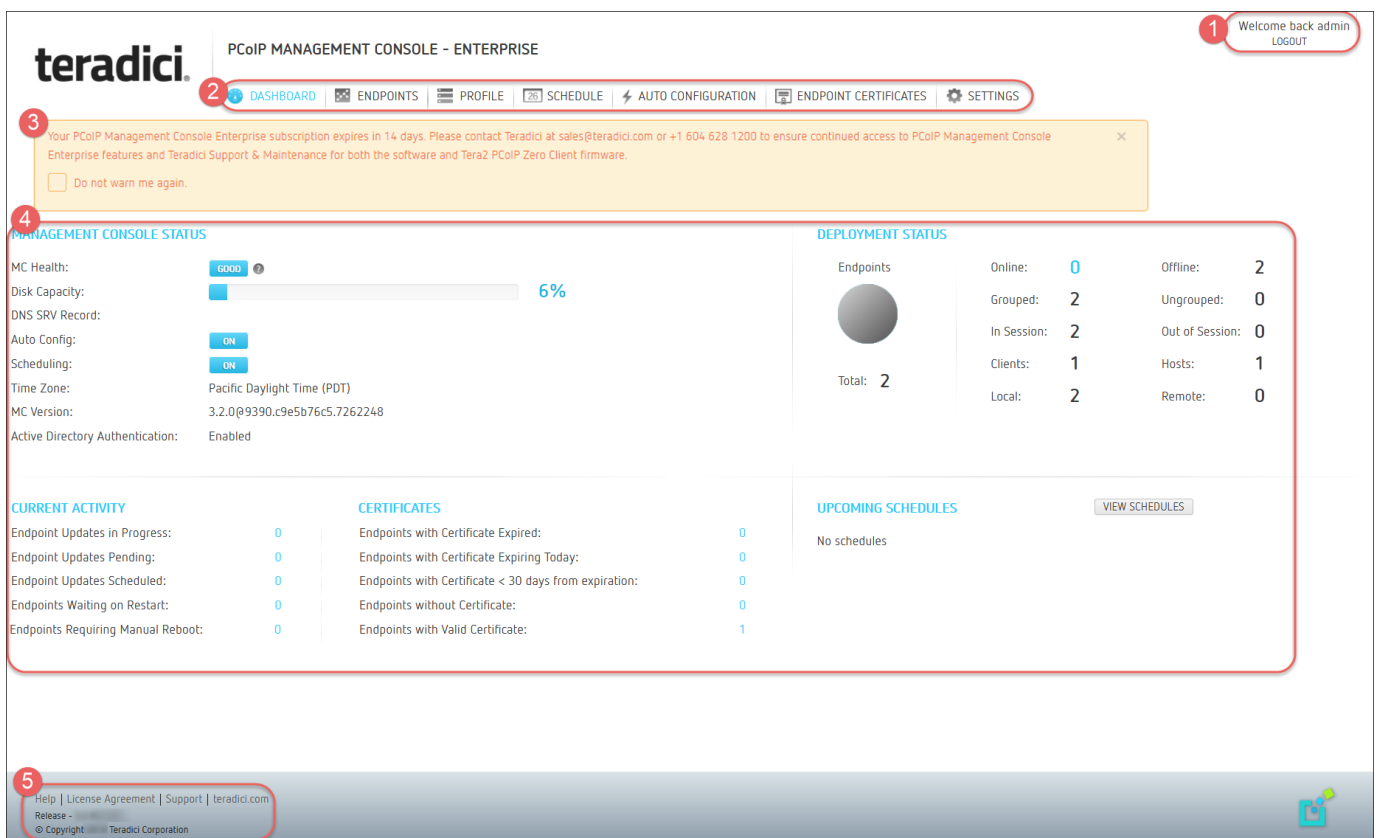
REMEMBER ME

User Account Lockout Screen

Understanding the PCoIP Management Console Dashboard

The **DASHBOARD** page gives you an overview of the PCoIP Management Console’s current configuration and health, as well as the status and activity of your PCoIP deployment. You can also use the dashboard to keep track of upcoming schedules and to view their details.

An example of the PCoIP Management Console Enterprise dashboard is shown. The table that follows describes the various sections in the dashboard layout and contains links to more information about the dashboard components.



PCoIP Management Console Dashboard

PCoIP Management Console Dashboard Description

Area	Dashboard	Description
1	Welcome message LOGOUT	Displays the PCoIP Management Console user account for the logged in user. Lets you log out from your PCoIP Management Console session.
2	DASHBOARD	Navigates to the DASHBOARD page. The DASHBOARD link occurs at the top of all PCoIP Management Console pages.
	ENDPOINTS	Navigates to the ENDPOINTS page. From this page you can structure endpoints into groups, apply profiles, discover endpoints manually, view endpoint details, search, and filter endpoints in the endpoint tables. The ENDPOINTS link occurs at the top of all PCoIP Management Console
	PROFILE	
	SCHEDULE (Enterprise)	Navigates to the SCHEDULE page which includes the schedule HISTORY tab. From the SCHEDULE page you can create, view, edit, delete, enable and disable schedules to update groups of endpoints in the future and access the PCoIP Management Console's schedule history tab. The SCHEDULE link occurs at the top of all PCoIP Management Console pages.
	AUTO CONFIGURATION (Enterprise)	Navigates to the AUTO CONFIGURATION page. From this page you can configure, edit, and delete rules to automatically assign endpoints to a specific group when they are first discovered or whenever they move to or from a group. The AUTO CONFIGURATION link occurs on at the top of all PCoIP Management Console pages.
	ENDPOINT CERTIFICATES (Enterprise)	Allows administrators to configure rules that request certificates for endpoints.
	SETTINGS	Navigates to the SETTINGS page. From this page you can manage PCoIP Management Console users, change the time zone for your PCoIP Management Console web interface, configure a persistent naming convention for automatically naming endpoints, upload firmware and certificates to the PCoIP Management Console , manage PCoIP Management Console databases, view license information, view PCoIP Management Console version information, and configure the PCoIP Management Console log level. The SETTINGS link occurs at the top of all PCoIP Management Console pages.
3	License expiry notification banner	Displays the number of days remaining until the PCoIP Management Console Enterprise's license expires. If you disable this message, it will not appear again for 30 days when viewing the PCoIP Management Console Enterprise using that browser. You will see it again if you access the PCoIP Management Console Enterprise using a different browser that does not have the notification disabled.
4	MANAGEMENT CONSOLE STATUS	Shows the PCoIP Management Console's status and contains information about how the PCoIP Management Console is configured:

Area	Dashboard	Description
		<ul style="list-style-type: none"> • Health: The PCoIP Management Console health displays as 'good' unless the disk is more than 80% full and/or the PCoIP Management Console daemon is halted. • Disk Capacity: Shows the percentage of disk space used. • DNS SRV Record: Displays the PCoIP Management Console's FQDN that is configured in the DNS SRV record. If no record exists, this field is left blank. • Auto Config: Indicates whether auto configuration is enabled or disabled. • Scheduling: Indicates whether schedules are enabled or disabled. • Time Zone: Indicates the time zone setting for the user's PCoIP Management Console web interface. By default, the time zone is set to the PCoIP Management Console virtual machine's time zone, which is always in Coordinated Universal Time (UTC). If desired, you can set your web interface time to reflect your local time zone. • MC Version: Displays the current PCoIP Management Console release version.
	DEPLOYMENT CONSOLE STATUS	Displays status information about the managed endpoints in your system, such as the number that are online and offline, and the number that are grouped and ungrouped. This section also indicates important information about profiles that failed to apply.
	CURRENT ACTIVITY	Displays the number of endpoint updates in progress, pending, scheduled, and the number of endpoints waiting to restart or requiring a manual reboot.
	UPCOMING SCHEDULES	Displays information about upcoming schedules, including the date and time they will apply.
	CERTIFICATES (This dashboard feature is limited to SCEP generated certificates)	Identifies the number of endpoints with SCEP generated certificates: <ul style="list-style-type: none"> • Expired certificates • Certificates expiring today • Certificates that are less than 30 days from expiring • No certificates • Valid certificates
	VIEW SCHEDULES	Lets you open the SCHEDULE page to view details for a schedule.
5	Footnote Information	The following links occur at the bottom of every PCoIP Management Console page:


Area	Dashboard	Description
		<ul style="list-style-type: none">• Help: Opens the PCoIP Management Console support page where you can find information about the PCoIP Management Console.• License Agreement: Opens the End User License Agreement (EULA) in your browser window.• Support: Opens the Teradici Support page in your browser window.• teradici.com: Opens the Teradici web page in your browser window.• Release: Identifies the PCoIP Management Console release version.

Managing Licenses Online

PCoIP Management Console Enterprise is enabled through subscription licensing provided on a per managed device basis for terms of one and three years. Licenses can be added together to achieve the total number of necessary managed devices.

Licenses come by email after you order them and contain one activation code for each license SKU ordered. Activation codes (also known as entitlement IDs) have an alphanumeric format of *0123-4567-89AB-CDEF*.

The following is an example of the email content for 3x100 license SKUs:

 **Note: License keys shown next are examples**

The license keys shown next do not contain real activation codes.

Description: Teradici PCoIP® Management Console Enterprise – 1 year. Includes support and maintenance.

No. of Devices: 10 Devices

Quantity: 3

Valid Until: 12/31/2016

Activation Code: 0123-456Z-89AB-CDEF

Contact your reseller to obtain your license key for PCoIP Management Console Enterprise or go to <https://connect.teradici.com/mc-trial> to request a free PCoIP Management Console Enterprise trial license. For more information on license options and packaging, see <https://www.teradici.com/products-and-solutions/pcoip-products/management-console> or one of Teradici's resellers.

License Requirements and Restrictions

The following requirements and restrictions apply for PCoIP Management Console:

Caution: Return all licenses before migrating

If your PCoIP Management Console appliance will be moved to another server or replaced with an upgrade, you must return all the PCoIP Management Console licenses before the migration and then re-activate the licenses after the migration.

- When a license expires, PCoIP Management Console will operate in Free mode. Enterprise mode features will stop working Licenses are installed per PCoIP Management Console appliance.
- If no licenses are installed, the PCoIP Management Console will operate in Free mode.
- Internet access to **<https://teradici.flexnetoperations.com/>** on port **443** is required for the PCoIP Management Console to activate the license against the license server. The PCoIP Management Console may also require the ability to contact this server from time to time to keep the license activated.
- Licenses can be returned multiple times. If the system prevents activation after returning a license, contact support at [Support Center](#).
- You can have multiple licenses active on PCoIP Management Console, however each license can only be active on one PCoIP Management Console.
- Licenses are activated one license at a time.

Expiry Notifications

The Management Console interface displays a notification when licenses are about to expire, when they have expired, when you are approaching your licensed device count limit, and when you have reached the limit.

Support and Maintenance

Use the activation code you received to request Support and Maintenance.

For more information on support and maintenance, see the [Support Programs](#).

Info: License Scripts

If managing licenses through the command line, please see License Scripts

Activating Licenses

Before you can activate your license, you will need your activation key. If you are activating from behind a proxy, you will also need the IP address, port number, username, and password to authenticate to your proxy server. If you wish to use the virtual machine console to manage your licenses, see [Using your Virtual Machine Console to Administer Licenses when Connected to the Internet](#)

Using the UI to activate your PCoIP Management Console Enterprise license:

1. Navigate to *SETTINGS > LICENSE* page.
2. Select the **NEW LICENSE** button.
3. Enter your License Key and select the **ACTIVATE LICENSE** button.

Using the UI to activate your PCoIP Management Console Enterprise license from behind a proxy server:

Activating your license from behind a proxy server requires you configure the additional parameters that appear after activating the **Connect through a proxy** option. The additional parameters are Proxy Address, Port, Username, and Password of the proxy server.

ACTIVATE NEW LICENSE

Please type in the license key you wish to activate:

License Key:

Connect through a proxy

Proxy Address:

Port:

Username:

Password:

Activate New License Dialog

Viewing Installed Licenses

Once your license is activated, its information is stored on the PCoIP Management Console virtual machine.

To view installed licenses via the PCoIP Management Console user interface:

- Navigate to *SETTINGS > LICENSE*.

The following information will be displayed:


- **Fulfillment ID: XXXXXXXX**: An ID assigned to a license after it is activated. This ID is required if you deactivate the license. The fulfillment ID will be different each time you reactivate a license after it has been deactivated.
- **Entitlement ID: XXXX-XXXX-XXXX-XXXX**: The license key you received via email that you use to activate your license.
- **Expiration date: DD-MMM-YYYY**: The day, month, and year your license expires.

LICENSE

LICENSE Page

Deactivating Licenses

It is important to deactivate a license when you no longer need it, for example, when you decommission a virtual machine. This frees up the license and makes it available for a different PCoIP Management Console Enterprise deployment.

 **Note: Deactivating license reverts PCoIP Management Console to PCoIP Management Console Free**

PCoIP Management Console will run in Free mode when all its licenses are deactivated.

 **Warning: Internet Access Required**

When deactivating a license, an internet connection to the licensing server is required unless the offline license activation steps are used.

Deactivating Your PCoIP Management Console License

Using your UI to deactivate PCoIP Management Console Enterprise license:

1. Navigate to *SETTINGS > LICENSE* page.
2. Highlight the licenses you want deactivated and select the **DEACTIVATE** button.

Deactivating your PCoIP Management Console Enterprise license from behind a proxy server:

Deactivating your license from behind a proxy server requires you configure the additional proxy server parameters that appear after activating the Connect through a proxy option. The additional parameters are Proxy Address, Port, Username, and Password.

Using your UI to deactivate PCoIP Management Console Enterprise license behind a proxy server:

1. Navigate to *SETTINGS > LICENSE* page.
2. Highlight the licenses you want deactivated and select the **DEACTIVATE** button.
3. Select the **Connect through a proxy** radio button and fill out the proxy fields.
4. Select the **DEACTIVATE** button in the *DEACTIVATE LICENSE* dialog.

Managing Licenses Offline

License Scripts

HP provides shell scripts that let you activate, view information about, and deactivate PCoIP Management Console Enterprise licenses. All scripts are located in the PCoIP Management Console virtual machine console's `/opt/teradici/licensing` directory and require you to connect to your PCoIP Management Console virtual machine console. See [Logging in to the PCoIP Management Console OVA Virtual Machine Console](#).

Activating Your PCoIP Management Console License from a Location Without Internet Access

To activate your PCoIP Management Console Enterprise license when the PCoIP Management Console is located on a site without Internet access (sometimes referred to as a dark site), you will need to create a ticket for Offline License Activation. A [support site account](#) will be required to create this ticket. The ticket must include your license activation code that was provided by email when you requested a trial license or when your Enterprise license was purchased. Once the ticket is created, you will be provided with an offline activation `.asr` file allowing you to produce an offline activation short code to return to support. Support will in turn provide you with a response text file which you will use to activate PCoIP Management Console Enterprise. Activating and deactivating licenses from a site without Internet access must be done using the virtual machine console.

REQUESTING OFFLINE ACTIVATION

Go to the [support site](#), sign in and create a ticket for Offline License Activation. Include your PCoIP Management Console Enterprise license activation code that was provided by email when your trial license was requested or when your Enterprise license was purchased.

PRODUCING AN OFFLINE ACTIVATION SHORT CODE

The ticket will first be updated by support with an ASR file which you have to upload to your PCoIP Management Console. Once you have the ASR file, perform the following steps from your PCoIP Management Console virtual machine console.

1. Enable SSH if using PCoIP Management Console in OVA format. See: [Temporarily Enabling SSH Access](#)

2. Connect a Secure Copy Protocol (SCP) client such as Putty or WinSCP to the PCoIP Management Console virtual machine using the PCoIP Management Console virtual machine administrative credentials.
3. Upload the ASR file provided in your ticket to the administrative home directory (/home/admin/).
4. Connect a Secure Shell (SSH) client to to the PCoIP Management Console virtual machine using the PCoIP Management Console virtual machine administrative credentials.

5. Change directories to the licensing directory.

```
[admin@localhost ~]$ cd /opt/teradici/licensing/
```

6. Set the **LD_LIBRARY_PATH** variable.

```
[admin@localhost licensing]$ export LD_LIBRARY_PATH=.
```

7. Process offline_activation.asr with appactutil.

```
[admin@localhost licensing]$ ./appactutil -shortcode ~/offline_activation.asr
```

Activation short code output example:

Activation short code: 216360-082292-891921-316997-475492-227533-740186-228152

8. Copy your Activation short code into a text file and enter it into your ticket. Wait for the response code text file to be returned from support.

COMPLETING THE OFFLINE ACTIVATION

Once the support ticket has been updated with a response code text file, you can then follow these steps to activate your PCoIP Management Console Enterprise with the response code file.

1. From the PCoIP Management Console virtual machine console enable SSH. See: Temporarily Enabling SSH Access

Info: PCoIP Management Console AMI format

Enabling SSH is not required for the AMI

2. Connect a Secure Copy Protocol (SCP) client such as Putty or WinSCP to the PCoIP Management Console virtual machine using the PCoIP Management Console virtual machine administrative credentials.
3. Upload the response text file provided in your ticket to the administrative home directory (/home/admin/).
4. Change directories to the licensing directory.

```
[admin@localhost ~]$ cd /opt/teradici/licensing/
```

5. Set the *LD_LIBRARY_PATH* variable.

```
[admin@localhost licensing]$ export LD_LIBRARY_PATH=/opt/teradici/licensing
```

6. Process response.txt with appactutil.

```
[admin@localhost licensing]$ ./appactutil -process ~/response.txt
```

```
Reading response from /home/admin/response.txt  
SUCCESSFULLY PROCESSED RESPONSE  
ProductID MC, FulfillmentID FID-CUSTNAME-2016-1
```

Viewing Installed Licenses

To view your installed licenses:

1. Enable SSH. See: [Temporarily Enabling SSH Access](#)
2. Connect a Secure Shell (SSH) client to the PCoIP Management Console virtual machine using the PCoIP Management Console virtual machine administrative credentials.

3. Change directories to the licensing directory.

```
[admin@localhost ~]$ cd /opt/teradici/licensing/
```

4. Set the `LD_LIBRARY_PATH` variable

```
[admin@localhost licensing]$ export LD_LIBRARY_PATH=/opt/teradici/licensing
```

5. View the installed licenses and note the Fulfillment ID of the license to return.

```
[admin@localhost licensing]$ ./appactutil -view
```

```
-----  
Trust Flags: FULLY TRUSTED  
Fulfillment Type: SHORTCODE  
Status: ENABLED  
Fulfillment ID: FID-OFFLINE-12345678-1  
Entitlement ID: ENTL-OFFLINE-12345678-2-1  
Product ID: MC  
Suite ID: NONE  
Expiration date: 30-may-2017  
Feature line(s):  
INCREMENT MC_nDevices TERADICI 2.00000 30-may-2017 1 \  
VENDOR_STRING="nDev=500, FNO=90, SN=19137747" ISSUER=Teradici \  
ISSUED=13-mar-2017 NOTICE="Teradici - Dev Ops" TS_OK \  
SIGN="00D0 A25F 78FB A9C4 7093 EB1A 2744 8500 DF9B 8201 9CFE \  
F024 08A5 67DE CD45"  
-----
```

Deactivating Your PCoIP Management Console Enterprise License from a Location Without Internet Access

To deactivate your PCoIP Management Console Enterprise license when the PCoIP Management Console is located in a site without Internet access:

1. Enable SSH. See: [Temporarily Enabling SSH Access](#)

2. Connect a Secure Copy Protocol (SCP) client such as Putty or WinSCP to the PCoIP Management Console virtual machine using the PCoIP Management Console virtual machine administrative credentials.
3. Upload the ASR file provided in your ticket to the administrative home directory.
4. Connect a Secure Shell (SSH) client to the PCoIP Management Console virtual machine using the PCoIP Management Console virtual machine administrative credentials.

5. Change directories to the licensing directory.

```
[admin@localhost ~]$ cd /opt/teradici/licensing/
```

6. Set the `LD_LIBRARY_PATH` variable

```
[admin@localhost licensing]$ export LD_LIBRARY_PATH=/opt/teradici/licensing
```

7. View the installed licenses and note the Fulfillment ID of the license to return.

```
[admin@localhost licensing]$ ./appactutil -view
```

```
-----  
Trust Flags: FULLY TRUSTED  
Fulfillment Type: SHORTCODE  
Status: ENABLED  
Fulfillment ID: FID-OFFLINE-12345678-1  
Entitlement ID: ENTL-OFFLINE-12345678-2-1  
Product ID: MC  
Suite ID: NONE  
Expiration date: 30-may-2017  
Feature line(s):  
INCREMENT MC_nDevices TERADICI 2.00000 30-may-2017 1 \  
VENDOR_STRING="nDev=500, FNO=90, SN=19137747" ISSUER=Teradici \  
ISSUED=13-mar-2017 NOTICE="Teradici - Dev Ops" TS_OK \  
SIGN="00D0 A25F 78FB A9C4 7093 EB1A 2744 8500 DF9B 8201 9CFE \  
F024 08A5 67DE CD45"  
-----
```

8. Generate the return request code by using `appactutil`. The ASR file referenced must be the one used to activate the license. The `-return` parameter is the Fulfillment ID noted in the previous step.

```
[admin@localhost licensing]$ ./appactutil -shortcode ~/offline_activation.asr -  
return FID-OFFLINE-12345678-1
```

```
Return short code: 163698-563854-292262-189561-853089-634323-881517-668156
```

9. Send the return short code returned in step 8 as a text file to HP.
10. Support will return a response file where you must finish the deactivation by following the [Completing the Offline Activation](#)

Note: Finding fulfillment ID

To find your fulfillment ID, see [Viewing Installed Licenses](#).

Uploading Endpoint Firmware to the PCoIP Management Console

Endpoint firmware files must first be uploaded to the PCoIP Management Console before you can create profiles or perform firmware updates.

Note: Prior to importing a PCoIP Management Console 1 profile

For PCoIP Zero Clients and Remote Workstation Cards, PCoIP Management Console must have at least one firmware image uploaded to it before you can import a PCoIP Management Console 1 profile. Migrated profiles will be assigned the latest firmware version that is present on PCoIP Management Console.

To upload endpoint firmware files to PCoIP Management Console:

1. From the PCoIP Management Console's top menu, click **SETTINGS**.
2. Click **SOFTWARE** in the left pane.
3. Click **Add Software/Firmware**.
4. Click **Select file**.
5. Select the desired combined firmware file (*.pcoip*), and then click ****Open*** and **Upload** to upload the file to the PCoIP Management Console.

Setting up Security

⚠ Caution: Ensure system operates at a security level that matches your organization's requirements

As an administrative user, you must ensure your system operates at a security level that matches the requirements of your organization.

⚠ Update your software to the current release

From time to time, updates may be made available from support, or the developers of CentOS. While we recommend staying current on releases, it is also recommended that you test updates on a test system prior to upgrading your production system or back up a snapshot of the PCoIP Management Console before running the update.

The OS admin user must use the sudo command when performing actions that require elevated privileges.

✎ Note: Non-root Linux passwords must be at least ten characters long

Non-root Linux passwords must be at least ten characters long and contain one each of upper case, lower case, decimal, and special characters. When changing a non-root Linux password, the new password must be at least four characters different from the previous password.

The following table contains some further recommendations for securing your PCoIP Management Console over and above the default CentOS security configuration undertaken by Teradici.

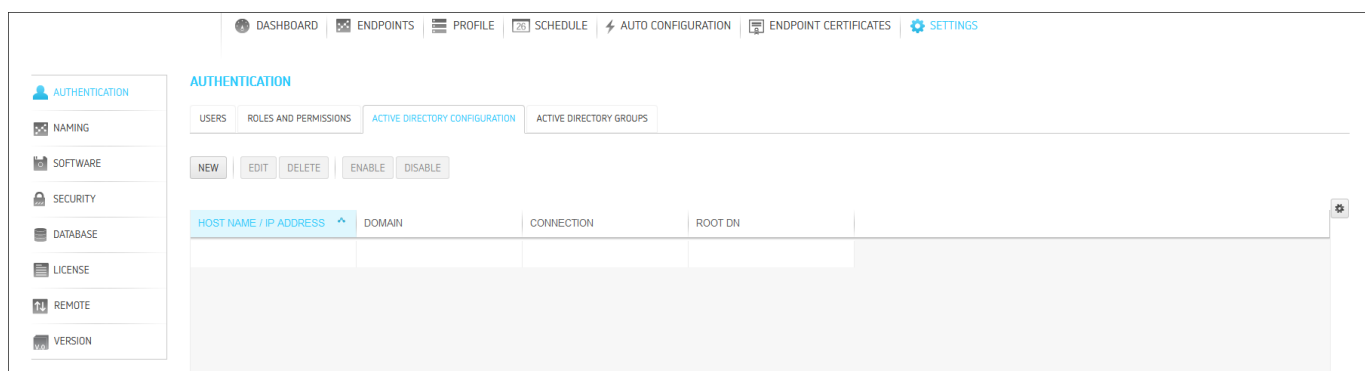
PCoIP Management Console Security Recommendations

Recommendations	Description
Network security	<p>Configure your corporate firewall as follows:</p> <ul style="list-style-type: none"> • Block inbound traffic from unsecured networks to the PCoIP Management Console on all ports (for example, block traffic from the Internet). • Block outbound traffic from the PCoIP Management Console to unsecured networks on all ports except for ports 80 and 443. Port 80 must be open for system updates and port 443 for system updates and licensing.
Operating system security	<ul style="list-style-type: none"> • Change the default passwords for the virtual machine admin user, root user, and web UI admin user immediately after installing the PCoIP Management Console. See Accessing the PCoIP Management Console Virtual Machine Console. • Ensure the CentOS firewall only allows port access to the ports that are required for the PCoIP Management Console to run. See Default firewall port settings are as follows. • Update CentOS third-party packages on a regular basis using the sudo yum update "package" command. <ul style="list-style-type: none"> Note: Prior to updating your production system To ensure that a library update does not cause problems, HP recommends that you perform updates on a test system (or that you take a snapshot of the PCoIP Management Console) before updating your production system. See Backing Up PCoIP Management Console Database. • Remove external NTP server references. See NTP Configuration Considerations
PCoIP Management Console web UI security	<ul style="list-style-type: none"> • Create a new PCoIP Management Console web UI administrative user and disable the default admin account and provide the desired role. (PCoIP Management Console Enterprise only). <ul style="list-style-type: none"> Note: Re-enabling admin account If you have disabled the admin account and plan to revert the PCoIP Management Console Enterprise to PCoIP Management Console Free, this account must be re-enabled before you can log in again to the PCoIP Management Console web UI. Alternatively, you can run a script from the PCoIP Management Console virtual machine console to re-enable the default admin account. • Replace the PCoIP Management Console certificate with your own custom certificate and upload it to all endpoints. See Managing PCoIP Management Console Certificates.

Recommendations	Description
	<ul style="list-style-type: none">• Check the HP support site for the latest PCoIP Management Console release.
Enable HTTP Strict Transport Security (HSTS)	<p>HTTP Strict Transport Security (HSTS) is a policy that helps protect web server appliances against particular types of attacks against the communication between the web browser and the web server.</p> <p>See HTTP Strict Transport Security for details on how to enable HSTS.</p> <p>Important: Requirements</p> <p>HTTP Strict Transport Security (HSTS) requires:</p> <ul style="list-style-type: none">• PCoIP Management Console have a proper trusted certificate installed• The chain or root certificate installed in the browser used to connect to the PCoIP Management Console

Active Directory Authentication

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



⚠ Caution: LDAP or LDAPS

LDAPS is the secure version of LDAP and is recommended for production environments and requires installation of the Active Directory Certificate.

⚠ Active Directory Users

All Active Directory users have a default time zone of UTC which can be modified by a Management Console System Administrator after the user has logged in the first time.

Important Notes

This release of AD in PCoIP Management Console has important limitations which need to be considered before using this feature in your deployment.

- The MC's AD authentication only works for the same domain as the Domain Controller you have configured in the Management Console's **SETTINGS > AUTHENTICATION > ACTIVE DIRECTORY CONFIGURATION** tab
- Only supports on-premises Active Directory

- Only supports one active domain at a time
- Only supports UPN/AD and local user login
- Only supports uploading one AD certificate to the certificate store

Upload the Root Certificate

Upload the Root Certificate from the CA that issued the Domain Controller's certificate

- Configurations for parent groups do not transfer to child groups. Ensure the child group is configured as required.
- Does not support domain trust relationships
- A user must be member of at least one group created in the Active Directory Server that exists in the Management Console Active Directory Groups configuration.
- The Management Console **Root DN** field must include the users Active Directory Servers parent or child container's distinguished name (i.e. OU=Users,OU=Accounting,DC=domain,DC=local)

AUTHENTICATION				
USERS	ROLES AND PERMISSIONS	ACTIVE DIRECTORY CONFIGURATION	ACTIVE DIRECTORY GROUPS	
NEW	EDIT	DELETE	ENABLE	DISABLE
HOST NAME / IP ADDRESS	DOMAIN	CONNECTION	ROOT DN	
ldap://10.0.8.18	domain.local	ENABLED	OU=Users,OU=Accounting,DC=domain,DC=local	

Installing an Active Directory Certificate

LDAPS requires a Base64 encoded certificate in .pem or .cer format to be uploaded to the certificate store. The LDAPS certificate should be downloaded from the same Active Directory that will be used for authentication. This can be done before or after enabling Active Directory.

To install your Active Directory Certificate:

1. Browse to **SETTINGS > SECURITY** and select the *ADD CERTIFICATES* tab.
2. Select the **UPLOAD CERTIFICATE** button.
3. Use the **SELECT CERTIFICATE** button and browse to where your Active Directory Certificate is located, highlight it and select the **Open** button.

4. Select the **UPLOAD** button and then **OK** in the Active Directory Certificate Details dialog.
5. Access the PCoIP Management Console virtual machine console, (see [Accessing the PCoIP Management Console Virtual Machine Console](#)) and run the import script located in **/opt/teradici/scripts** directory.

To run the script ensure you include the full path to the script and that you type the name of the correct AD uploaded certificate.

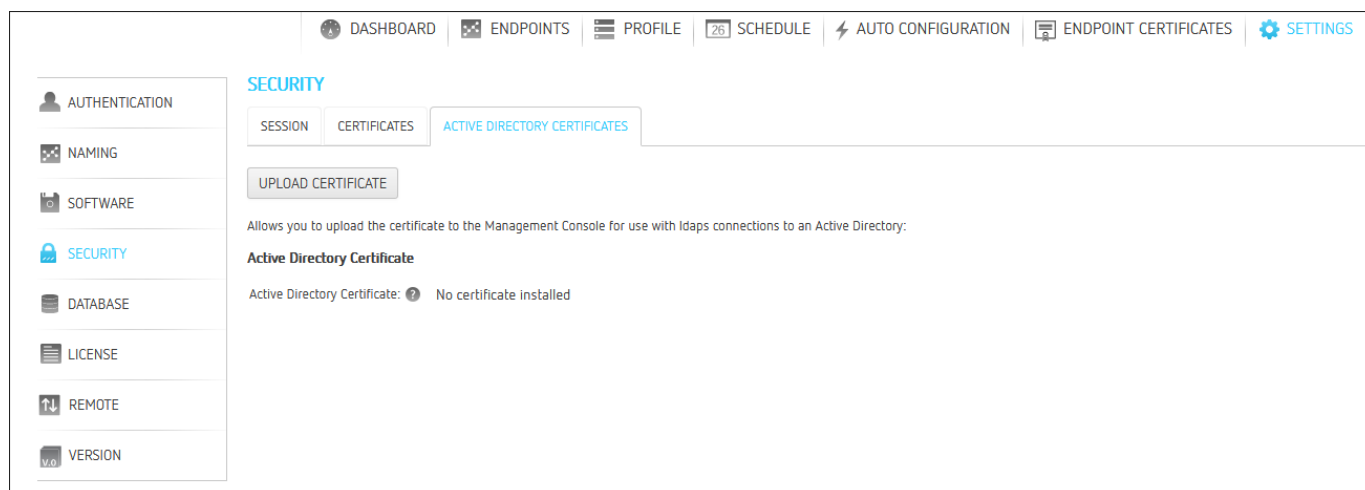
```
sudo /opt/teradici/scripts/import_ldaps_certificate.sh /opt/teradici/console/certs/  
adcerts/< certificate_name >
```

Tip: Dialog Information

After selecting the certificate the dialog contains additional information that is useful for managing your certificate from the virtual machine console.

Viewing your Active Directory Certificate

You can view the Active Directory Certificate by viewing the *ACTIVE DIRECTORY CERTIFICATES* tab located on the *SECURITY* settings page.



The screenshot shows the PCoIP Management Console interface. At the top, there is a navigation bar with tabs: DASHBOARD, ENDPOINTS, PROFILE, SCHEDULE (with a '26' notification), AUTO CONFIGURATION, ENDPOINT CERTIFICATES, and SETTINGS. On the left, a sidebar menu lists various settings categories: AUTHENTICATION, NAMING, SOFTWARE, SECURITY (highlighted in blue), DATABASE, LICENSE, REMOTE, and VERSION. The main content area is titled 'SECURITY' and has three sub-tabs: SESSION, CERTIFICATES, and ACTIVE DIRECTORY CERTIFICATES (which is selected). Below the sub-tabs, there is an 'UPLOAD CERTIFICATE' button. A text block explains that this allows uploading certificates for use with Idaps connections to an Active Directory. Under the heading 'Active Directory Certificate', it shows 'Active Directory Certificate: No certificate installed' with a help icon.

Active Directory Certificates tab

Removing your Active Directory Certificate

Removing your Active Directory Certificate requires you to login to the PCoIP Management Console virtual machine console, see [Accessing the PCoIP Management Console Virtual Machine Console](#) to run the removal script located in the `/opt/teradici/scripts` directory.

Once logged in to the virtual machine console, browse to the `opt/teradici/scripts` directory and enter `./remove_ldaps_certificate.sh`.


Creating and Enabling Active Directory Configuration

The optional **Root DN** field, allows you to limit where the Management Console search begins in Active Directory. The entries must be in the correct format and order. For example the format would be **OU=Users,OU=Accounting,DC=domain,DC=local** or **DC=domain,DC=local** or similar.

To create and enable an Active Directory configuration:

1. Log in to PCoIP Management Console
2. Browse to **SETTINGS > AUTHENTICATION** and select the *ACTIVE DIRECTORY CONFIGURATION* tab.
3. Select the **NEW** button.
4. Select your preferred protocol **LDAP** or **LDAPS**.
5. Enter the **Host Name / IP Address** of your Active Directory Server and any specific port that you want to use.
6. Enter the **Domain Name** that the Active Directory Server manages.
7. Enter the **Root DN** (optional).

The Root DN or root distinguished name will tell Management Console which container in AD to start searching for approved Management Console users instead of searching the full list of domain users. Perform a group query (e.g. **OU=Users,OU=Accounting,DC=domain,DC=local**). Error messages for incorrect query strings will be presented that help guide the user using this method. Valid attributes are **DC, CN, OU, O, STREET, L, ST, C, UID**.
8. Save your configuration.
9. Return to the *ACTIVE DIRECTORY CONFIGURATION* tab and click **Enable** to enable the connection. The PCoIP Management Console will reboot.
10. Login to Management Console with your Active Directory UPN and domain password.

 Tip: If PCoIP Management Console does not restart

If your PCoIP Management Console does not restart using the PCoIP Management Console GUI, you can issue the following command from the PCoIP Management Console virtual machine console:

```
sudo service mcconsole restart
```


Adding Active Directory Groups

Adding Active Directory groups require that you have already enabled and configured Active Directory on the PCoIP Management Console. When adding Active Directory groups to PCoIP Management Console, ensure the added group has the identical name as the group in Active Directory and the [Managing Users](#) have been assigned to the group for PCoIP Management Console use. You can use just the group name or the group UPN name in this field.

To add or edit an active directory group:

1. Browse to **SETTINGS > AUTHENTICATION** and select the *ACTIVE DIRECTORY GROUPS* tab.
2. Select the **ADD** button.
3. Enter the required information.

- **Group:** Enter the group name.

 **Multiple Groups**

- The Active Directory Group cannot be nested under any other group.
- If the name of the user is in multiple groups, the user in the first matching group is used.
- If a user is removed from that Active Directory group, then the next listed group will be used.

- **Domain:** Select the domain from the drop down where the Active Directory group resides.
- **Role:** This will be the PCoIP Management Console role given to the user for use when logging into the PCoIP Management Console. User roles can be changed at any time from the *Authentication* page. See [Managing Users](#) for further information on Users and User Roles.

4. Select the **SAVE** button.

AUTHENTICATION			
USERS	ROLES AND PERMISSIONS	ACTIVE DIRECTORY CONFIGURATION	ACTIVE DIRECTORY GROUPS
ADD EDIT REMOVE			
GROUP	DOMAIN	ROLE	HOST NAME / IP ADDRESS
mc_group	domain.local	System_Administrator	ldap://10.0.8.18

Added AD Group

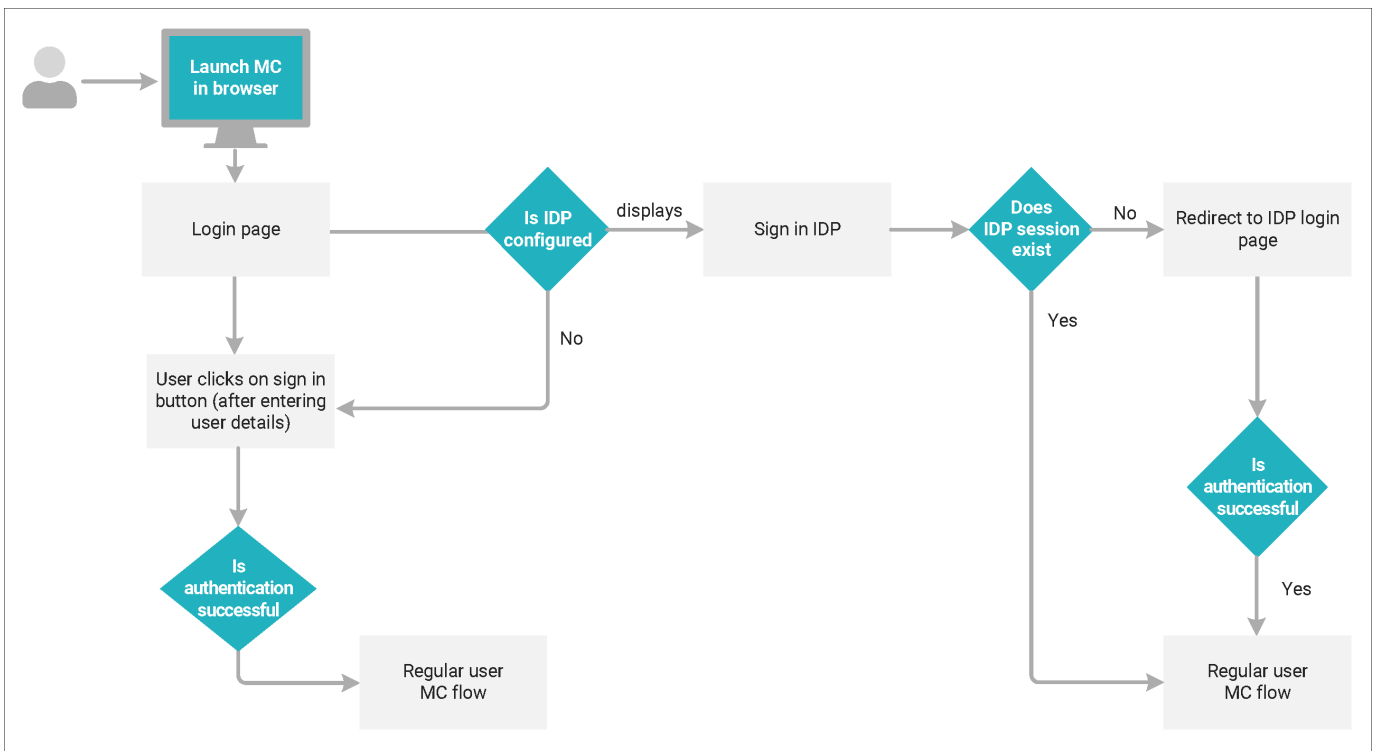
Identity Provider (IDP) Integration with Management Console (Enterprise)

Management Console allows for secure network Single Sign-on (SSO) with Multi-factor Authentication (MFA). It also allows for integration with your Active Directory servers and your Identity Providers (IDP) using the Security Assertion Markup Language 2.0 (SAML). With the benefit of SSO, users will be able to securely sign into Management Console without having to remember a separate Management Console password. These instructions are to help with configuration of single sign-on with a third party Identity Provider (IDP) which will allow for the authentication of management console users.

The Service Provider (SP) referenced in this instruction topic is the Management Console while the Identity Provider (IDP) used for reference is Okta and PingFederate. When you configure the IDP, you are using SAML2.0 to allow the IDP to pass the authorization credentials to Management Console or any other service provider.

You can enable IDP configuration via the IDP CONFIGURATION tab on the AUTHENTICATION page.

The basic IDP flow for Management Console is shown in this flow image.



Requirements

- Management Console Enterprise License
- IPv4 network (IDP, SSO and MFA for IPv6 currently not supported)
- Account with an IDP Service Provider (Okta and PingFederate IDPs will be used for reference)
 - IDP Metadata XML file
- Matching time configuration

The date and time configurations on Management Console and your IDP must match for the successful authentication of the Management Console using an IDP user. This includes the same date, time, and time zone.

- IDP must be enabled on Management Console. (SETTINGS > AUTHENTICATION > IDP CONFIGURATION > ON)

AUTHENTICATION

USERS ROLES AND PERMISSIONS ACTIVE DIRECTORY CONFIGURATION ACTIVE DIRECTORY GROUPS IDP CONFIGURATION

Configure IDP: ? ON

Upload IDP Metadata: ? Metadata file already exists. To override the existing file, click SELECT FILE to upload the new file and click Save Configuration

Encryption Certificate: ?

Encryption Certificate: ? Subject: MC SAML SECURITY
Issued By: MC SAML SECURITY
Expiration Date: Tue Jan 07 16:40:10 UTC 2031

Encryption Certificate Chain: ? Subject:
Issued By:
Expiration Date:

SSO Behaviors

Single Sign-on configurations for web based applications are browser specific, and do not support cross browser authentication. When you maintain an active browser session to an application that has been authenticated by an IDP, you will auto-login to applications authenticated by that IDP as long as the session is active.

IDP configured with SSO for Management Console and other applications (e.g. Office 365, Atlassian, ServiceNow)

When you are logged into another application and access the Management Console with the same browser, you will auto-login to Management Console without being prompted for IDP login credentials. Similarly, when you are logged into Management Console and access another application with the same browser, you will auto-login to the application without being prompted for IDP login credentials.

- Browser session time-outs do not affect Management Console user time-out settings. You have to sign out of Management Console to close your Management Console session. This applies to both IDP and direct Management Console sign ins.
- If your browser times out, re-launching your browser and accessing the Management Console will not prompt you for login credentials.

IDP Behaviors

- A continuous session for an IDP user is independent of the Management Console session time out.
- For all IDP users, the session will end by explicitly logging out of Management Console.
- If an IDP user session expires, the IDP user's session in Management Console will not close until they log out of the existing session from Management Console. This is due to the IDP not sending a closed session notification.
- If an IDP user session expires and the user then logs out of Management Console, than if the user logs in again with the **SIGNIN WITH IDP** button, the user will be redirected to the IDP login page.
- First time sign in to Management Console using an IDP user will automatically create a Management Console user with the default Administrator role.

Administrator default role

An IDP created user in Management Console will not have access to the SETTINGS page nor will they be able to change the default Management Console settings.

Administrators should consider changing the default IDP user role to System Administrator to provide access to SETTINGS and have the session timeout disabled.

Logging Out

- Logging out of a Management Console session only terminates the local Management Console session and does not affect the IDP session, nor sessions at other SPs where the IDP user may have been logged in using SSO.
- Logging out of a Management Console session using the dashboard LOGOUT link will close the user session and redirect the user to the Management Console login page.
- Using the **Sign In With IDP** button after logging out from the same browser will redirect the user to the Management Console dashboard page without redirecting to the IDP login page, as the IDP session is still active.
- All Management Console sessions in all browsers will close when a user logs out from any Management Console IDP connected session.
- Logging out of an IDP session will redirect the user to the IDP login page when using the **Sign In With IDP** button.

Roles and Permissions

- The default IDP role is Administrator and can be changed by any user with the System Administrator role.
- Management Console created/edited user roles do not affect the IDP.
- IDP created/edited user roles do not affect Management Console

Management Console IDP Configuration

Prior to configuring the IDP for Management Console, you will need an IDP service that you can manage. Complete the referenced Okta or PingFederate configuration prior to performing the next steps. [Okta Reference](#) | [PingFederate Install Reference](#) & [PingFederate Configuration Reference](#)

1. Download the IDP metadata XML file from your IDP and upload this to Management Console. (See Okta reference [here](#))

XML metadata file validation

To confirm the IDP metadata.xml file is valid, ensure the following:

- The Metadata XML file, Attributes, and Tags are not empty
- The file contains starting and ending tags
- The contained signing certificate is valid
- The file does not contain a <RoleDescriptor> tag

2. Enter the **Assertion Consumer Service URL**.

The Assertion Consumer Service URL should be the same as the single sign-on URL in the IDP configuration and it must be entered in following format **https://<MC_FQDN/MC_IP_ADDRESS>/saml/SSO**.

3. Enter the **SP Entity ID**.

This ID will be any unique string specified in the IDP configuration to identify the Management Console application as a service provider connection.

4. Update the **Encryption Certificate** on Management Console.

By default, a self-signed certificate is available in Management Console which you can update at any time. You can use any of the following certificates when updating your Management Console certificate:

- **The default Management Console Certificate:**** Select the **Revert Self-Signed Certificate** button to have all the proper configurations using the default Management Console certificate applied. The Management Console will reset and be offline for a short period of time.
- **CA Signed Certificate:** Select the **Update Certificate** button and then individually upload the Encryption Certificate, Encryption Private Key, and the Encryption Chain.
- **Self-Signed Certificate:** Select the **Update Certificate** button and then individually upload the Encryption Certificate, Encryption Private Key, and the Encryption Chain.

AUTHENTICATION

- USERS
- ROLES AND PERMISSIONS
- ACTIVE DIRECTORY CONFIGURATION
- ACTIVE DIRECTORY GROUPS
- IDP CONFIGURATION**

Configure IDP: **ON** To save IDP configuration, ensure IDP metadata and below all fields are updated

Upload IDP Metadata:

Assertion Consumer Service URL:

SP Entity Id:

Encryption Certificate: Default MC certificate will be used for encryption on click of Revert Self-Signed Certificate

Upload Encryption Certificate:

Upload Encryption Private Key:

Upload Encryption Chain:

Download SP metadata option will be available once configuration is saved

- Download the Encryption Certificate used in step 4 which will be required in your IDP configuration.
- Use the **Save Configuration** button to save the IDP SAML configuration.
This will cause the Management Console to restart and present the additional **SIGN IN WITH IDP** option on the Management Console sign in page.
- Download the Service Provider(SP)/Management Console metadata XML file by using the **Download SP Metadata** button. This button becomes active once the SAML configuration is enabled after performing step 6. See [OKta - Obtaining IDP Metadata File](#)
- Sign in to the Management Console using the **SIGN IN WITH IDP** button.

Securing User Passwords

Securing PCoIP Management Console User Passwords

This section provides an overview of how to change your PCoIP Management Console default passwords.

Accessing the PCoIP Management Console Virtual Machine Console

In order to change the PCoIP Management Console's default settings and run various scripts, you must connect to the PCoIP Management Console's virtual machine console and log in. The AMI release of PCoIP Management Console has SSH enabled by default to provide access to its virtual machine console. The SSH server on the CentOS operating system virtual machine is disabled on the OVA release of PCoIP Management Console since access to the virtual machine console can be made using VMware vSphere Client. However, if your security requirements permit SSH access, you can temporarily or permanently enable SSH for the PCoIP Management Console virtual machine **admin** user. This section provides instructions for both methods.

Info: PCoIP Management Console AMI virtual machine console

When using PCoIP Management Console AMI format, SSH on the CentOS operating system virtual machine is enabled by default to provide console access via an SSH Client.

Caution: SSH access on PCoIP Management Console AMI

Disabling SSH access on PCoIP Management Console AMI releases is not recommended as it will prevent you from gaining vm console access which may be required to make changes such as security updates and password changes.

PCoIP Management Console AMI users should start at [Logging in from an SSH Client](#)

Logging in to the PCoIP Management Console OVA Virtual Machine Console

To log in to virtual machine console from vSphere Client:

1. Launch VMware vSphere Client.
2. Enter the IP address or FQDN for your vCenter Server along with your user name (**DOMAIN\user name**) and password.
3. Select **Inventory > VMs and Templates**.
4. Expand the inventory tree and locate your PCoIP Management Console virtual machine.

5. Right-click on the virtual machine and select **Open Console**.
6. Log in to the console:
user name: **admin**
password: **ManagementConsole2015** (default) or the password you have assigned to the **admin** user.

 **Note: Releasing the cursor once connected**

Once you are connected to the console through the VMware vSphere client, you can release the cursor at any time by pressing `Ctrl` + `Alt` (Windows) or `Fn` + `Control` + `Option` (Mac).

7. When you have finished using the console, type `logout` to log out.

Enabling/Disabling SSH Access

By default, SSH access is disabled when the PCoIP Management Console OVA release is first installed. If your security requirements permit SSH access and you wish to log in to the PCoIP Management Console virtual machine console this way, you can run commands to enable SSH temporarily or permanently.

 **Note: Only admin user can access SSH on AMI and OVA distributions**

The PCoIP Management Console is configured to only enable SSH access for the admin user when the SSH server is enabled. The PCoIP Management Console (OVA or AMI) always restricts SSH access for the root user.

TEMPORARILY ENABLING SSH ACCESS

To run the SSH server and enable SSH access for the admin user until the next reboot:

1. Log in as admin to the PCoIP Management Console OVA virtual machine console from your vSphere Client. See [Logging in to the PCoIP Management Console OVA Virtual Machine Console](#).
2. Run the following command at the command line:

```
sudo /sbin/service sshd start
```

TEMPORARILY DISABLING SSH ACCESS

To stop the SSH server and disable SSH access for the admin user until the next reboot:

1. Log in as **admin** to the PCoIP Management Console virtual machine console from your vSphere Client. See [Logging in to the PCoIP Management Console OVA Virtual Machine Console](#).
2. Run the following command at the command line:

```
sudo /sbin/service sshd stop
```

Note: Permanent SSH configuration

A permanent SSH configuration will automatically start the SSH service on reboot.

PERMANENTLY ENABLING SSH ACCESS

To permanently enable SSH on next reboot:

1. Log in as **admin** to the PCoIP Management Console OVA virtual machine console from your vSphere Client. See [Logging in to the PCoIP Management Console OVA Virtual Machine Console](#).
2. Run the following command at the command line:

```
sudo chkconfig sshd on
```

3. If SSH is disabled, Run the following command at the command line to start SSH immediately:

```
sudo service sshd start
```

PERMANENTLY DISABLING SSH ACCESS

Caution: Disabling SSH access on PCoIP Management Console AMI release not recommended

Disabling SSH access on PCoIP Management Console AMI releases is not recommended as it will prevent you from gaining vm console access which may be required to make changes such as security updates and password changes.

To permanently disable SSH for the admin user after the next reboot:

1. Log in as **admin** to the PCoIP Management Console OVA virtual machine console from your vSphere Client. See [Logging in to the PCoIP Management Console OVA Virtual Machine Console](#).

2. Run the following command at the command line:

```
sudo chkconfig sshd off
```

3. Disable the service by running the following command at the command line:

```
sudo service sshd stop
```

LOGGING IN FROM AN SSH CLIENT

To log in to virtual machine console from SSH Client once SSH is enabled:

1. Launch your preferred SSH client.
2. Enter the following information:
 - **Host name:** Enter the FQDN or IP address for your PCoIP Management Console virtual machine.
 - **Port:** 22
 - **Connection type:** SSH
3. Click **Open**.
4. Log in to the PCoIP Management Console virtual machine console:
5. **user name:** admin
6. **password:** ManagementConsole2015 (default) or the password you have assigned to the admin user. See [Changing the PCoIP Management Console Virtual Machine Default User Password](#).
7. When you are finished using the console, type exit to log out and exit the application.
8. If desired, disable SSH. See [Enabling/Disabling SSH Access](#).

CHANGING THE PCOIP MANAGEMENT CONSOLE VIRTUAL MACHINE DEFAULT USER PASSWORD

The PCoIP Management Console's default password when it is first installed is ManagementConsole2015. To secure the PCoIP Management Console, it is critical to change this password immediately after installation.

To change the virtual machine default user password:

1. Log in to your PCoIP Management Console virtual machine console as admin using the default password, ManagementConsole2015.
2. Type passwd at the command prompt.

3. When prompted, enter the default password and then your new password twice:

```
passwd  
Changing password for admin user.  
New password:  
Retype new password:<br>passwd:<br>password updated successfully.
```

4. Follow your company's policy for storing and sharing passwords.

Changing the PCoIP Management Console Web Interface Default Password

Disable default admin user

For security reasons, you must disable the default admin user and create a different administrative user with a new name and password (Management Console Enterprise only). See [Managing Users](#).

Important: Set time zone

You should select your time zone at this point. If you do not set the desired time zone, you may run schedules at an undesirable time.

The PCoIP Management Console web user account has the following default user name and password when it is first deployed which must be changed immediately after first login:

- User name: **admin**
- Default password: **password**
- Default Role: **System Administrator**

If further changes to the admin account password are required, perform the following steps:**To change the admin account password:**

1. Click **SETTINGS** and then **AUTHENTICATION** to display the *MANAGEMENT CONSOLE USERS* window.
2. In the *USERNAME* column, select **admin** and then click **EDIT**.
3. In the *Current Password* field enter the current password.
4. In the *New Password* field, enter the new password.
5. In the *Confirm Password* field, enter the password again.
6. Click **SAVE**.

Re-enabling the PCoIP Management Console's Web UI Admin User Account

The PCoIP Management Console virtual machine contains a script that lets you re-enable the PCoIP Management Console web UI **admin** account from the PCoIP Management Console virtual machine console command line. This is useful if you disable the **admin** account from PCoIP Management Console Enterprise and subsequently transition to PCoIP Management Console Free before re-enabling the account from the PCoIP Management Console web UI. In this case, you can run this script to re-enable the **admin** user and enable administrative access to the PCoIP Management Console Free web UI.

To re-enable the admin account:

1. Select one of the following choices depending on whether you are using the OVA or AMI version of PCoIP Management Console.
 - Open the PCoIP Management Console console from vSphere Client. See [Logging in to the PCoIP Management Console OVA Virtual Machine Console](#).
 - SSH into the PCoIP Management Console AMI console.
2. Log in using the PCoIP Management Console console admin user name and password.
3. Change to the scripts directory:

```
cd /opt/teradici/scripts
```

4. Type the following command to run the script:

```
./enable_admin.sh
```

Reverting the PCoIP Management Console's Web UI Admin User Password

The PCoIP Management Console virtual machine contains a script that lets you revert the password for the PCoIP Management Console's web interface **admin** user to **password** (the default) from the PCoIP Management Console console command line. This is useful if administrators lose their PCoIP Management Console web interface passwords and need a way to get logged in again.

To revert the admin account password to its default value:

1. Open the PCoIP Management Console console from vSphere Client. See Logging in to the PCoIP Management Console OVA Virtual Machine Console .
2. Log in using the PCoIP Management Console console admin user name and password.
3. Change to the scripts directory:

```
cd /opt/teradici/scripts
```

4. Type the following command to run the script:

```
./reset_admin_password.sh BCRYPT New_Password
```

Password Hashes

There are two hash arguments when resetting the admin password. BCRYPT is the recommended hash argument to use for passwords over SHA512

Changing the PCoIP Management Console Virtual Machine Default 'Root' Password

For security reasons, the **root** user is not used for PCoIP Management Console administration. This user account has a large, randomly-generated password that is not published. To secure the PCoIP Management Console, it is critical to change this password immediately after installation.

Virtual Machine Password

On first boot, the PCoIP Management Console generates a random password. Though the password is randomly generated, it is still recommended that you change this password. Consult with your security team to ensure your new password conforms with your local security policy.

To change the virtual machine default root password:

1. Log in to your PCoIP Management Console virtual machine console as **admin**.
2. Type the following command at the prompt:
`sudo passwd root`
3. When prompted, enter the new password twice:

```
Changing password for root user.  
New password:  
Retype new password:  
passwd: all authentication tokens updated successfully.
```

Moving to a Newer Version

Migrating PCoIP Management Console to a Newer Release Using OVA

Note: DNS Records

Ensure your PCoIP Management Console has a correctly configured A record and PTR record on your DNS server. It is important to maintain the IP address and DNS hostname of your currently deployed PCoIP Management Console when migrating to a newer release. This enables a seamless transition to the new PCoIP Management Console and eliminates unnecessary PCoIP endpoint configuration as each endpoint is configured to report to the previous PCoIP Management Console IP address.

Tip: Disable Auto-Config and Scheduling

Consider turning off Auto-Config and Scheduling prior to doing a database backup. Performing this step ensures both features will be off when you restore the database preventing unexpected schedules from running and preventing new devices from suddenly appearing in the PCoIP Management Console during the migration process. After confirming a successful database restore consider re-enabling Auto-Config and Scheduling.

These instructions explain how to migrate PCoIP Management Console 2.x or later to a more current PCoIP Management Console release.

At the end of this section you will find instructions that will allow the new Management Console OVA format to work in an IPv6 environment.

To migrate PCoIP Management Console to a newer release:

1. Connect to your PCoIP Management Console virtual machine console that you wish to migrate from and log in using the admin account and password. See [Accessing the PCoIP Management Console Virtual Machine Console](#).
 - If migrating from PCoIP Management Console 2.x go to step 2.
 - If migrating from PCoIP Management Console 3.x, 19.x or higher go to step 3.
2. PCoIP Management Console 2 users. Perform the following steps to record the IP address, netmask, and default gateway:
 - a. Type `sudo system-config-network` to launch the network configuration tool.
 - b. From the main menu, select **Device configuration**.
 - c. In the next screen, select **eth0 (eth0) - vmxnet3**.
 - d. Make a note of PCoIP Management Console 2's static IP address, netmask, default gateway, and DNS server. If no IP information is displayed, it is because the PCoIP Management Console 2 is configured to use DHCP which is not recommended. See [Assigning a Static IP Address](#).
 - e. Select **Ok**.
 - f. In the next screen, select **Cancel**.
 - g. In the next screen, select **Quit**.

Recommendation

Support does not recommend changing the PCoIP Management Console DNS configuration.

3. PCoIP Management Console 3 and higher users. Perform the following steps to record the IP address, netmask, and default gateway:
 - a. Type `sudo nmtui` to launch NetworkManager TUI.
 - b. From the main menu, select **Edit a connection**.
 - c. In the next screen, select **eth0**, and press .
 - d. Make a note of PCoIP Management Console 3's static IP address, netmask, default gateway DNS servers, and domains (if configured). If no IP information is displayed, it is because the

PCoIP Management Console is configured to use DHCP which is not recommended. See [Assigning a Static IP Address](#).

e. Select **< OK >** or **< Cancel >** and press .

f. Select **< Back >** to return to the main screen.

Recommendation

Support does not recommend changing the PCoIP Management Console hostname using this tool.

g. In the next screen, select **Quit**.

4. Manage your PCoIP Management Console certificate:

Management Console default certificate expiry date

The default Management Console certificate used in versions 23.06 or older expired on October 15, 2023.

If you are managing endpoints using the default Management Console certificate from Management Console 23.06 or older, you will no longer be able to manage new endpoints. Existing endpoints will be lost if they lose communication to Management Console (i.e. network or power loss). You will need to upload a valid certificate to your existing endpoints and Management Console.

Management Console 23.08 and newer has an [updated default certificate](#).

- To use the **updated 23.08+ default Management Console certificate**, first you will need to update your endpoint profiles to include the new default Management Console certificate and push the profile out to every endpoint, including any ungrouped endpoints, before deploying the new console. If necessary, use each individual endpoint's AWI to upload the new default Management Console certificate to the endpoint. See [Managing Profiles](#).


Important: Update endpoint profile's new certificate before deploying the upgrade

Ensure that you roll out the new certificate to the endpoints prior to deploying the new PCoIP Management Console; that is, update your profile certificates using the original console. Otherwise, you will lose the management of the endpoint.

- If you plan to use your **custom PCoIP Management Console certificate** after upgrading, our support team recommends that you copy it to a safe location where you can retrieve it to use with the new PCoIP Management Console. See [Managing PCoIP Management Console Certificates](#).
- If you plan to use a **new custom PCoIP Management Console certificate** after upgrading, first you will need to update your endpoint profiles to include the new PCoIP Management Console certificate (or its issuer) and push the profile out to every endpoint, including any ungrouped endpoints, before deploying the new console. If necessary, use each individual endpoint's AWI to upload the new PCoIP Management Console certificate (or its issuer) to the endpoint. See [Managing PCoIP Management Console Certificates](#).

5. Back up and download the current PCoIP Management Console database archive file to an external location before beginning the upgrade:

- a. Log in to the PCoIP Management Console web interface.
- b. From **SETTINGS > DATABASE**, select **BACK UP**.
- c. Enter a description for the backup and click **BACK UP**.
- d. When the backup completes, select the file in the database table, click **DOWNLOAD**, and then save the archive file. You will need to retrieve this file later.

 **Important: Database upgrades when migrating from PCoIP Management Console 2.4 or older**

Upgrades when migrating from PCoIP Management Console 2.4 or older can generate large databases that can cause issues during upgrades. See [knowledge base article 1029](#) for workarounds.

6. If you are using PCoIP Management Console Enterprise, record the following licensing information by [viewing installed licenses for online](#) installations or [viewing installed licenses for offline](#) installations.

- Fulfillment ID
- Entitlement ID (activation code)

7. If you are using PCoIP Management Console Enterprise, deactivate the PCoIP Management Console Enterprise license from the **SETTINGS > LICENSE** page.

8. Shut down the PCoIP Management Console virtual appliance.


9. Follow [Installing PCoIP Management Console using vSphere](#) to deploy the new PCoIP Management Console release.
10. Connect to your PCoIP Management Console virtual machine console. See [Logging in to the PCoIP Management Console OVA Virtual Machine Console](#).
11. Log in as admin using the default password (ManagementConsole2015) and change the admin user password. See [Accessing the PCoIP Management Console Virtual Machine Console](#).
12. Use the same network settings as the previous PCoIP Management Console release.

 **Note: Reserve IP address against the new virtual machine if using DHCP reservation**

If you are using DHCP reservation, reserve the IP address against the new PCoIP Management Console virtual machine. Otherwise, see [Assigning a Static IP Address](#) for instructions.

- **Migration between IPv4 and IPv6:** If your migration includes changing IPv4 and IPv6 networks, review [using IPv6](#) and [moving between IPv4 and IPv6](#)

13. Restart the PCoIP Management Console and ensure it has the correct addressing information.
14. If you are using PCoIP Management Console Enterprise, activate its license from the **SETTINGS > LICENSE** page.
15. Log in to the PCoIP Management Console web interface using the following default user account:
 - User name: **admin**
 - Password: **password**
16. If you are using a custom PCoIP Management Console certificate (either the custom certificate from the previous PCoIP Management Console release or a new custom certificate), upload the certificate to the new PCoIP Management Console. For more information creating and uploading your own certificate, see [Managing PCoIP Management Console Certificates](#).

 **Note: Skip this step if using the default signed certificate**

If you are using the default self-signed PCoIP Management Console certificate, *skip this step*.

17. Upload the database archive file you saved in step 5, and then restore the database. See [Managing PCoIP Management Console Databases](#).

This step reverts user accounts and passwords to previous PCoIP Management Console release

This step replaces all users on the system with the user accounts and passwords that existed on the previous PCoIP Management Console. If you changed the default web UI password for the admin account, it will not be the standard default password. If necessary, you can revert the admin account password to its default value and then reset the password. To revert the password, see [Reverting the PCoIP Management Console Web Interface Default Password](#).

18. Log in again using your standard user account.
19. Check the Management Console Health field on the **DASHBOARD** page to ensure the PCoIP Management Console status is **GOOD**. See [Understanding the PCoIP Management Console Dashboard](#).
20. From the ENDPOINTS page, click **REFRESH** to see endpoints begin contacting the new PCoIP Management Console. You can also verify groups, profiles, schedules, and auto configuration rules at this time. See [Managing Endpoints](#).

Migrating Management Console OVA format to IPv6

To migrate Management Console OVA format to IPv6, you must configure your network interface to IPv6 and then configure your firewall rules to remove IPv4 rules and allow IPv6 rules for Management Console communication. The firewall rules referenced below refer to firewallD.

1. Perform the steps above. After performing the steps above, change the Management Console network configuration to IPv6 by performing the steps in [Moving between IPv4 and IPv6](#)
2. Access Management Console Web UI via IPv6 address.

Time Settings

Ensure your Management Console time settings are correct by using the `sudo hwclock --debug` command. If there are issues, check your host computer time and date settings, BIOS and VM hardware settings.

Upgrading using RPM

Upgrading Management Console Using RPM

Update your software to the current release

From time to time, updates may be made available from support, or the developers of CentOS. While we recommend staying current on releases, it is also recommended that you test updates on a test system prior to upgrading your production system or back up a snapshot of the PCoIP Management Console before running the update.

Backup Your Database

Always ensure you have a working backup of your Management Console data when performing a Management Console removal, upgrade, or installation. Considerations should include:

- * having a current snapshot of your virtual machine
- * having a complete backup or clone of your Linux PC
- * having a current backup of your Management Console database.

There are two different scenarios that require slightly different steps when installing or upgrading Management Console using the RPM. One scenario has Management Console deployed on a site that has access to the Internet and the other scenario is having Management Console deployed on a dark site where there is no internet access.

Prior to performing a RPM upgrade, the default certificate should be uploaded to all endpoints either through a profile or directly from an endpoint AWI.

UPGRADING MANAGEMENT CONSOLE WITH INTERNET ACCESS

Upgrade from Management Console 23.08 or older to Management Console 24.03

RPM upgrades may require new certificates uploaded to your endpoints

If you are upgrading to Management Console 24.03 from version 23.06 or earlier, and if you are not using custom certificates, you must upload the [new Management Console certificate](#) to your endpoints. For the new Management Console certificate SHA-256 & SHA-512 values, see the [release notes](#).

For instructions on how to upload your certificate see [Updating PCoIP Management Console Certificates after Endpoint Discovery](#)

Prior to upgrading Management Console you can:

- Clear the management state on all your endpoints **before** the upgrade and rediscover them after the upgrade.
- Ensure that the new certificate is uploaded to your endpoints **before** you upgrade to Management Console 24.03.

Important: Upgrading on RHEL 8.8 in an IPV6 environment

If you are upgrading the Management Console and are using both RHEL 8.8 and IPV6, you must disable the local repository before starting the upgrade and then re-enable it after the upgrade is complete. Run the following commands:

- **Before upgrading**, disable local repos:

```
subscription-manager config --rhsm.manage_repos=0
```

- **After upgrading is complete**, re-enable local repos:

```
subscription-manager config --rhsm.manage_repos=1
```

If you are using a different RHEL version or are using IPV4, you do not need to take these steps.

1. Upload the Management Console default self-signed certificate to all endpoints either through a profile or directly from an endpoint AWI if you are using the Management Console default certificate.
 - a. Login to your existing Management Console, create a profile with the provided default certificate ([cert.pem](#)) file uploaded in the Certificate Store.
 - b. Apply the profile to all the endpoints discovered in Management Console. Once the profile is applied successfully, the endpoint will have the new default certificate uploaded.
2. Download the [available RPM](#) and applicable online dependency file for this release from the [support site](#) and ensure they are located on the Management Console Linux VM.

You can use a third party tool such as WinSCP to copy and move files into the CentOS/RHEL host operating system.
3. Upgrade Management Console dependencies using the online dependency package for your Linux deployment.
 - CentOS 7.9 and RHEL 7.9

```
sudo sh ./teradicimc_<mc_version>-online-dependency-centos-rhel7.9.tar.gz
```
 - RHEL 8.6, 8.8

```
sudo sh ./teradicimc_<mc_version>-online-dependency-rhel8.tar.gz
```
4. Verify the PostgreSQL version is 14.8.

```
psql -V
```

5. Upgrade the Management Console from the directory where the RPM file is located.

```
sudo yum install teradicimc-<mc_version>.rpm
```

6. Verify Java 8 version

```
java -version
```

Example:

```
[root@localhost ~]# java -version
openjdk version "1.8.0_372"
OpenJDK Runtime Environment (build 1.8.0_372-b07)
OpenJDK 64-Bit Server VM (build 25.372-b07, mixed mode)
[root@localhost ~]# █
```

Upgrade from Management Console 23.12 and Newer to Management Console 24.03

1. Download the [available RPM](#) file for this release from the [support site](#) and ensure it is located in the on the Management Console Linux VM.

You can use a third party tool such as WinSCP to copy and move files into the CentOS/RHEL host operating system.

2. Upgrade the Management Console from the directory where the RPM file is located.

```
sudo yum install teradicimc-<mc_version>.rpm
```

Note: Applying Profiles

If a profile was created in Management Console 23.12.1 or earlier with the **Enable Audio** property set to Disabled and FW 23.12.x version, and you intend to apply this profile in Management Console 23.12.2 or later, ensure that **Enable Analog Audio Input** is disabled before applying this profile.

UPGRADING MANAGEMENT CONSOLE WITHOUT INTERNET ACCESS (DARK SITE)

1. Upload the Management Console default self-signed certificate to all endpoints either through a profile or directly from an endpoint AWI if you are using the Management Console default certificate.
 - a. Login to your existing Management Console, create a profile with the provided default certificate ([cert.pem](#)) file uploaded in the Certificate Store.

b. Apply the profile to all the endpoints discovered in Management Console. Once the profile is applied successfully, the endpoint will have the new default certificate uploaded.

2. Download the dark site package, which includes PostgreSQL, Python 3 dependencies, Java 8 upgrade package, and the Management Console RPM, from the [support site](#) and ensure it is located in the <logged in user directory> on the Management Console Linux VM.

You can use a third party tool such as WinSCP to copy and move files into the CentOS/RHEL host operating system.

3. Use the dark site package to install or upgrade Management Console and all dependencies in your offline environment. Execute the commands where the dark site package file is located for your Linux environment.

- CentOS 7.9

```
sudo sh ./teradicimc_<mc_version>-offline-centos7.9.tar.gz
```

- RHEL 7.9

```
sudo sh ./teradicimc_<mc_version>-offline-rhel7.9.tar.gz
```

- RHEL 8.6, 8.8

```
sudo sh ./teradicimc_<mc_version>-offline-rhel8.tar.gz --disablerepo=*
```

4. Verify the PostgreSQL version is 14.8.

```
psql -V
```

5. Verify the Java version is 1.8.0_372 or newer.

```
java -version
```

Moving Between IPv4 and IPv6

Management Console supports only pure IPv4 or IPv6 networks and not hybrid or stacked networks.

Upgrading and migrating at the same time

If a user wants to upgrade and migrate (IPv6 to IPv4 and vice versa) at the same time e.g. user want to upgrade from 20.04 IPv4 to 20.07 IPv6, we suggest they first complete upgrade (20.04 IPv4 to 20.07 IPv4 upgrade) and then following the IPv4 to IPv6 migration guideline

These steps must be performed in order for Management Console to operate successfully in a pure IPv4 or pure IPv6 environment.

Deleted Data

Be sure to backup your database in case you have to revert your change. When changing networks, Management Console will permanently delete unrelated data. See [deleted data](#) for more information on what is deleted.

To configure firewalld for an existing Management Console deployment that has been changed from IPv4 to IPv6 or vice versa

1. Login to the Management Console host operating system console.
2. Stop the mcconsole service.

```
sudo systemctl stop mcconsole
```

3. Stop the mcdaemon service.

```
sudo systemctl stop mcdaemon
```

4. To Enable or Disable IPv6 environment, you must modify the **teradici.ipv6.conf** file by executing either of the following commands.

- To disable IPv6 configuration in an IPv4 environment

```
sudo su
echo -e
"net.ipv6.conf.all.disable_ipv6=1\nnet.ipv6.conf.default.disable_ipv6=1"
> /usr/lib/sysctl.d/teradici_ipv6.conf
exit
```

- To enable IPv6 configuration in an IPv6 environment

```
sudo su
echo -e
"net.ipv6.conf.all.disable_ipv6=0\nnet.ipv6.conf.default.disable_ipv6=0"
> /usr/lib/sysctl.d/teradici_ipv6.conf
exit
```

5. Change the NIC IP address to IPv4 or IPv6.

6. Reboot your computer.

```
sudo init 6
```

7. Configure your Management Console firewall for the appropriate network.

- Configuration rules from 20.04 or later to 20.07.1
 - **Moving from IPv4 to IPv6:** Follow the same steps as shown at [Firewall changes required after an RPM Upgrade from Management Console 20.04 to Management Console 20.07 in IPv6 Environment](#)
 - **Moving from IPv6 to IPv4:** Follow the same steps as shown at [Firewall changes required after an RPM Upgrade from Management Console 20.04 to Management Console 20.07 in IPv6 Environment](#)
- Configuration rules from 20.01 or older to 20.07.1
 - **Moving from IPv4 to IPv6:** Follow the same steps as shown at [Updating firewall configuration after upgrading from Management Console 19.05 through to 20.01 to Management Console 20.07 with IPv6](#)
 - **Moving from IPv4 to IPv4:** Follow the same steps as shown at [Firewall changes after a RPM Upgrade from Management Console 20.01 or older using IPv4](#)

8. Run the scripts to delete unrelated data to maintain a pure IPv4 or IPv6 network.

```
cd /opt/teradici/database
sudo python mc_env_db.py
```

9. Start the mcconsole service.

```
sudo systemctl start mcconsole
```

10. Start the mcdaemon service.

```
sudo systemctl start mcdaemon
```

Existing IPv6 rule removal

If your Management Console happens to have previous Management Console IPv6 rules configured, remove them now by performing the following steps.

Note : If rule is not enabled it shows a warning NOT_ENABLED

1. Close port 443:

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --remove-rich-rule='rule family=ipv6 port port=443 protocol=tcp accept'
```

2. Close port 22:

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --remove-rich-rule='rule family=ipv6 port port=22 protocol=tcp accept'
```

3. Close port 5172:

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --remove-rich-rule='rule family=ipv6 port port=5172 protocol=tcp accept'
```

4. Close port 80:

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --remove-rich-rule='rule family=ipv6 port port=80 protocol=tcp accept'
```

5. Remove port forwarding of 8443 to 443:

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --remove-rich-rule='rule family=ipv6 forward-port to-port=8443 protocol=tcp port=443'
```

6. Remove port forwarding of 8080 to 80:

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --remove-rich-rule='rule family=ipv6 forward-port to-port=8080 protocol=tcp port=80'
```

To configure firewalld rules for an existing Management Console moving from an IPv6 to an IPv4 network perform the following steps:

1. Login to the Management Console host operating system console.

2. Enable required IPv4 ports.

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --add-port={22,443,80,5172}/tcp
```

3. Redirect IPv4 port 443 to port 8443.


```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --add-forward-port=port=443:proto=tcp:toport=8443
```

4. Redirect IPv4 Port 80 to 8080.

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --add-forward-port=port=80:proto=tcp:toport=8080
```

5. Remove IPv6 rules.

- Remove port forwarding to 8443 and 8080

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --add-forward-port=port=443:proto=tcp:toport=8443
```

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --add-forward-port=port=80:proto=tcp:toport=8080
```

- Close port 443

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --remove-rich-rule='rule family=ipv6 port port=443 protocol=tcp accept'
```

- Close port 22

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --remove-rich-rule='rule family=ipv6 port port=22 protocol=tcp accept'
```

- Close port 5172

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --remove-rich-rule='rule family=ipv6 port port=5172 protocol=tcp accept'
```

- Close port 80

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --remove-rich-rule='rule family=ipv6 port port=80 protocol=tcp accept'
```

6. Remove redirect of IPv4 port 443 to 8443.

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --remove-rich-rule='rule family=ipv6 forward-port to-port=8443 protocol=tcp port=443'
```

7. Remove redirect IPv6 Port 80 to 8080.

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --remove-rich-rule='rule family=ipv6 forward-port to-port=8080 protocol=tcp port=80'
```

8. Reload the firewall.

```
sudo firewall-cmd --reload
```

9. Confirm the rules are applied.

a. Check the firewalld status is active.

```
sudo systemctl status firewalld
```

```
[autorunner@gcp892b829c82864a9aa9b870e795e74383 ~]$ sudo systemctl status firewalld
● firewalld.service - firewalld - dynamic firewall daemon
  Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor preset: enabled)
  Active: active (running) since Fri 2020-02-14 10:24:12 UTC; 34min ago
  Docs: man:firewalld(1)
  Main PID: 730 (firewalld)
  CGroup: /system.slice/firewalld.service
          └─730 /usr/bin/python2 -Es /usr/sbin/firewalld --nofork --nopid
```

b. Verify all rules are added in firewalld or not, all rules should be applied.

```
sudo firewall-cmd --list-all
```

```
[admin@localhost ~]$ sudo firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: eth0
  sources:
  services: dhcpv6-client ssh
  ports: 80/tcp 22/tcp 443/tcp 5172/tcp
  protocols:
  masquerade: no
  forward-ports: port=443:proto=tcp:toport=8443:toaddr=
                port=80:proto=tcp:toport=8080:toaddr=
  source-ports:
  icmp-blocks:
  rich rules:
```

To configure firewalld rules for an existing Management Console moving from an IPv4 to an IPv6 network perform the following steps:

1. Login to the Management Console host operating system console.
2. Remove IPv4 rules.

- Close IPv4 ports

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --remove-port={22,443,80,5172}/tcp
```

- Remove IPv4 port forwarding to 8443 and 8080

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --remove-forward-port=port=443:proto=tcp:toport=8443
```

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --remove-forward-port=port=80:proto=tcp:toport=8080
```

3. Enable required IPv6 ports.

- Open port 443

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --add-rich-rule='rule family=ipv6 port port=443 protocol=tcp accept'
```

- Open port 22

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --add-rich-rule='rule family=ipv6 port port=22 protocol=tcp accept'
```

- Open port 5172

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --add-rich-rule='rule family=ipv6 port port=5172 protocol=tcp accept'
```

- Open port 80

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --add-rich-rule='rule family=ipv6 port port=80 protocol=tcp accept'
```

4. Redirect IPv6 port 443 to 8443.

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --add-rich-rule='rule family=ipv6 forward-port to-port=8443 protocol=tcp port=443'
```

5. Redirect IPv6 Port 80 to 8080.

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --add-rich-rule='rule family=ipv6 forward-port to-port=8080 protocol=tcp port=80'
```

6. Reload the firewall.

```
sudo firewall-cmd --reload
```

7. Confirm the rules are applied.

- a. Check the firewalld status is active.

```
sudo systemctl status firewalld
```

```
[autorunner@gcp892b829c82864a9aa9b870e795e74383 ~]$ sudo systemctl status firewalld
● firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2020-02-14 10:24:12 UTC; 34min ago
     Docs: man:firewalld(1)
   Main PID: 730 (firewalld)
   CGroup: /system.slice/firewalld.service
           └─730 /usr/bin/python2 -Es /usr/sbin/firewalld --nofork --nopid
```

b. Verify all rules are added in firewalld or not, all rules should be applied.

```
sudo firewall-cmd --list-all
```

```
[primeuser@localhost ~]$ sudo firewall-cmd --list-all
public (active)
target: default
icmp-block-inversion: no
interfaces: enp0s25 wlp2s0
sources:
services: dhcpv6-client ssh
ports:
protocols:
masquerade: no
forward-ports:
source-ports:
icmp-blocks:
rich rules:
rule family="ipv6" port port="443" protocol="tcp" accept
rule family="ipv6" port port="22" protocol="tcp" accept
rule family="ipv6" port port="3172" protocol="tcp" accept
rule family="ipv6" port port="80" protocol="tcp" accept
rule family="ipv6" forward-port port="443" protocol="tcp" to-port="8443"
rule family="ipv6" forward-port port="80" protocol="tcp" to-port="8080"
[primeuser@localhost ~]$
```

Migrating from PCoIP Management Console 1

Follow the steps outlined here to migrate your PCoIP Management Console 1 to PCoIP Management Console version 2 or later.

PCoIP Management Console properties

Not all properties from PCoIP Management Console 1 have been migrated to the current release of PCoIP Management Console. For further details, see [PCoIP Management Console 1 Profile Properties Renamed or Not Migrated](#)

Step 1: Install and configure this version of PCoIP Management Console

Management Console formats

These instructions are for configurations using the OVA format of this release of Management Console. Different formats (AMI, RPM) will require similar steps.

To install and configure the current OVA version of PCoIP Management Console:

1. [To install PCoIP Management Console using vSphere Client](#)
2. [To log in to virtual machine console from vSphere Client](#)
3. [Changing the PCoIP Management Console Virtual Machine Default User Password](#)
4. [Changing the Default Network Configuration](#)
5. [Managing Licenses Online](#) (optional).
6. If you are using an autodiscovery method, update your DHCP or DNS server with the new PCoIP Management Console information:
 - [Configuring DHCP Options](#) (for DHCP discovery)
 - [Adding the DNS SRV Record](#) (for DNS discovery)
 - [Adding a DNS TXT Record](#) (for DNS discovery)
7. [Using the Web Interface for the First Time.](#)

8. [Changing the PCoIP Management Console Web Interface Default Password.](#)

HP recommends that you disable the web UI **admin** user and create a new PCoIP Management Console administrative user.

9. From the PCoIP Management Console web UI, upload the desired 20.01 or later firmware file for your endpoints.

At least one 20.01 or later firmware image must be uploaded before a profile can be created.

Step 2: Import profiles, create groups, and assign profiles to the groups

PCoIP Management Console provides a profile import script that enables you to import your PCoIP Management Console 1 profiles into newer releases of PCoIP Management Console.

Importing process creates tab for endpoints

The profile import process will create a tab for Tera2 Dual and Quad PCoIP Zero Clients and Remote Workstation Cards. If you are only migrating one type of endpoint (quad or dual), it is recommended that you delete the tab for the other type to avoid accidentally configuring the wrong profile type. For example, if you are only migrating dual PCoIP Zero Clients and you set properties in the **QUAD** tab, the profile will not be applied.

Migrated Profile Naming Rules

Migrated profiles are named according to the following rules:

- If there is no profile in the new PCoIP Management Console with the PCoIP Management Console 1 profile name, then the migrated profile is called the same name as was used in PCoIP Management Console 1.
- If there is a profile in the new PCoIP Management Console with the PCoIP Management Console 1 profile, then the migrated profile is called the PCoIP Management Console 1 name with **imported** appended to it. If that name is already taken, then the script appends #, where # is an integer that starts counting up from one until it finds a name that is not taken.

Example

If the new PCoIP Management Console does not have a 'My Profile' profile, importing this profile four times from PCoIP Management Console 1 would result in the following PCoIP Management Console profile names.

Migrated Profile Naming Example

# of Times Migrated	PCoIP Management Console 1 Profile Name	PCoIP Management Console Profile Name
1	My Profile	My Profile
2	My Profile	My Profile_imported
3	My Profile	My Profile_imported 1
4	My Profile	My Profile_imported 2

Sort the DESCRIPTION column to show the last created profile

If you are unsure what name the migrated profile is called, sort the profile table's DESCRIPTION column by the last created description. The most recently created profile will be at the top. See [Displaying Profile Information](#).

Before You Import Your Profiles

Before beginning, ensure the following prerequisites are in place:

- For PCoIP Zero Clients and Remote Workstation Cards, ensure you have uploaded the firmware version used in your profiles, otherwise migrated profiles will be assigned the latest firmware version that exists in PCoIP Management Console.
- The import script requires the following firmware conditions be met, or the migration script will abort and provide an error message.

Firmware applied in PCoIP Management Console 1 profile being migrated	Firmware required to be preloaded to PCoIP Management Console 3 or later for migration script to run successfully
No firmware applied to MC1 profile	Client and Remote Workstation Card
Client only	Client
Remote Workstation Card only	Remote Workstation Card
Client and Remote Workstation Card	Client and Remote Workstation Card

- You know your PCoIP Management Console 1 user password (that is, the password for the *teradici* administrative user) if it was changed. The default password is **4400Dominion**.
- You know the PCoIP Management Console 1 profile name(s).

PCoIP Management Console 1

Profile names are case and white space sensitive.

- Both PCoIP Management Console 1 virtual appliance and the new PCoIP Management Console virtual appliance reside on the same network.
- PCoIP Management Console virtual appliance is able to open an SSH tunnel to the PCoIP Management Console 1 virtual appliance over port 22.

To test if the virtual appliance is able to open an SSH tunnel:

- a. From your PCoIP Management Console VM console, type **ssh teradici@< PCoIP Management Console 1 IP address or domain name >**.
 - b. Enter your PCoIP Management Console 1 VM password.
 - c. Type **exit** to close the session and return to your PCoIP Management Console.
- On PCoIP Management Console 1.x, you perform the following steps:
 - a. With root privileges, modify `/etc/postgresql/9.1/main/postgresql.conf` by replacing the line
`listen_addresses = 'localhost'` with `listen_addresses = '*'`.

Commented lines

Note that any code preceded by the # symbol is a comment. The functioning line of code in this step is located at the bottom of the file.

- b. With root privileges, modify `/etc/postgresql/9.1/main/pg_hba.conf` by appending a new line `host all all 0.0.0.0/0 md5` and saving the file.
 - c. Reboot MC1 and make sure the changes were saved.
- On PCoIP Management Console 3.x or newer releases, you perform the following step:
 1. Run the command `sudo iptables -I INPUT 1 -p tcp -m state --state NEW --dport 5432 -j ACCEPT`

Import Individual Profiles

To import profiles to PCoIP Management Console release 2 or later, run the migration script shown next for each profile that you want to import:

1. Log in to your new PCoIP Management Console VM console. See [Logging in to the VM Console on page 1](#).

2. Change to the **migration_script** directory:

```
cd /opt/teradici/database/legacy/migration_script
```

3. Run the script (one or more times) to migrate one profile at a time using one of the following commands:

- If you have not changed the PCoIP Management Console 1 user password:

```
./migrate_mc1_profile.sh -a <MC 1 address> -p <"profile name">
```

- If you have changed the PCoIP Management Console 1 user password:

```
./migrate_mc1_profile.sh -a <MC 1 address> -p <"profile name"> -l <MC 1 user password>
```

where <"profile name"> is the exact PCoIP Management Console 1 profile name enclosed in double quotes (for example, "My Profile").

Profile Names in PCoIP Management Console 1

Profile names are case and white space sensitive.

4. Load (or reload) the new PCoIP Management Console *PROFILE* page to see the migrated profiles. See [Managing Profiles](#).

5. Select each profile and click **EDIT** to check that the profile settings are correct. For example, if your PCoIP Management Console 1 profile contained a certificate file, this file should also be present in your new PCoIP Management Console profile.

Note: OSD logo is never imported

The OSD logo is never imported. While you are in edit mode, you can manually add this logo to your PCoIP Management Console profile or modify the profile as desired. For details about other profile properties that are not migrated or that have been renamed by the profile import process, see [PCoIP Management Console 1 Profile Properties Renamed or Not Migrated](#).

6. From the PCoIP Management Console 1 web UI, make a note of the groups that contain the endpoints you want to migrate and then create the groups from the new **ENDPOINTS** page on the new PCoIP Management Console using the same group names.
7. Associate the correct profile with each group in turn.

Troubleshooting the Profile Import Script

The profile import script is case and white space sensitive because PCoIP Management Console 1 profile names are case and white space sensitive. If the script is unable to find your 1.10.x profile, try copying the exact profile name from PCoIP Management Console 1.

To copy the exact profile name from PCoIP Management Console 1:

1. In the PCoIP Management Console 1 *PROFILES* page, click the profile's Edit link.
2. In the *Edit Profile* dialog, select the entire content of the Name field and copy it.
3. When you run the script, paste this name enclosed in double quotes as the *< profile name >* in the migration script instructions.

Step 3: Migrate each group of PCoIP Management Console 1 endpoints to this version of PCoIP Management Console

If you have a large deployment, support recommends that you migrate your endpoints on a group-by-group basis, checking that the endpoints in each group have successfully migrated to the new PCoIP Management Console, before proceeding with the next group.

To migrate each group of endpoints:

1. Create and enable an auto configuration rule.
2. From PCoIP Management Console 1, upgrade PCoIP endpoints to firmware 20.01 or higher.
3. If you are not using DHCP options or DNS service record discovery, perform a manual discovery from the new PCoIP Management Console to discover the endpoints.
4. Refresh the new PCoIP Management Console **ENDPOINTS** page and check that the endpoints have been discovered and placed in the correct group with the correct associated profile.

Managing Firmware

Managing PCoIP Zero Client and Remote Workstation Card Firmware

[Upgrading Endpoints to Firmware 5.0 or Later](#) and [Downgrading to Older Firmware](#) provide an overview of how to upgrade or downgrade your version of the PCoIP Zero Client or Remote Workstation Card firmware.

Deployments containing endpoint groups with different versions of firmware should consider upgrading all endpoints to the (same) latest version of firmware for ease of management and upgradeability.

Firmware in migrated profiles

Migrating from Management Console 1

When using profiles from PCoIP Management Console 1 that were migrated to newer versions of PCoIP Management Console, ensure [firmware requirements are met](#). You must upload at least one image of the firmware you wish to upgrade to. Migrated profiles will be assigned the latest firmware version that is present on PCoIP Management Console.

Recommendations for firmware use in Management Console

- First upgrade to Management Console 20.01 or newer and secondly deploy firmware 20.01 or newer.
- After upgrading your Management Console you will be able to manage any endpoints with older firmware.
- If you have a large deployment with multiple endpoint groups, we recommend scheduling firmware upgrades one group at a time.

Upgrading Endpoints to Firmware 5.0 or Later

PCoIP Management Console cannot upgrade endpoints running firmware versions prior to 5.0. Instead, you can perform this step remotely for a group of endpoints using PCoIP Management Console 1 or you can update the firmware for individual endpoints locally using each endpoint's AWI.

Firmware 20.01

If you use PCoIP Management Console to deploy firmware 20.01 or newer, it is strongly recommended that you first upgrade to Management Console 20.01 or newer and secondly deploy firmware 20.01 or newer.

Important: Test the upgrade with a small group of test endpoints

Before upgrading all your endpoints, first test the procedure with a small group of test endpoints to ensure that they can be discovered and managed by PCoIP Management Console.

Caution: Remote Workstation Cards

Remote Workstation Cards cannot be **powered down**, **power reset**, or **reset to default** by the PCoIP Management Console as the Remote Workstation Card requires the host computer to be restarted due to the Remote Workstation Card obtaining its power from the host computer motherboard. An alternate method of restarting the host computer is required to restart the host computer.

Upgrading Firmware Using PCoIP Management Console 1

To update the firmware for a group of endpoints using PCoIP Management Console 1:

1. Ensure that the endpoints you wish to update are placed in their own group. Depending on your site configuration, this may require modifications to your DHCP options or DNS SRV records, or it may require disabling persistent auto-configuration or placing the endpoints into a segregated network with a new PCoIP Management Console 1.
2. From the PCoIP Management Console 1 or later home page, click **Update Firmware**.

3. Click the **Import Firmware** link to transfer the firmware 20.01 or higher release file from your host machine to the PCoIP Management Console 1 virtual machine.
4. Click **Browse**, locate the combined firmware file, and then click **Open**. This file will have a `.pcoip` extension.
5. Click **Import Now** to transfer the firmware 20.01 or higher release file from your host machine to the PCoIP Management Console 1 virtual machine.
6. Click the **Update Devices** link.
7. In the Select Devices to Update section, you can further define the endpoints you wish to upgrade by 3 different groupings.
 - **Device Family:** lists the processor family used by the endpoint **Tera2**.
 - **Version Number:** represents the currently applied firmware on the endpoints you want to update (for example, **20.07**).
 - **Group:** lists any groups you have previously configured for endpoint management.

 **Tip: Upgrade firmware one group at a time**

HP recommends upgrading firmware one group at a time. Groups that are not migrated and will have to be recreated manually in the new PCoIP Management Console.

8. Click **View Devices to Update**.
9. Select the endpoints you wish to update, choose the desired endpoint restart and schedule options, and then click **Schedule Update**.
10. If desired, click **View Status** to watch the update status of the endpoints.

 **Note: Update endpoint firmware by applying a profile**

You can also update endpoint firmware by applying a profile that contains an associated firmware file. For information about managing endpoints with PCoIP Management Console 1, see the [PCoIP Management Console 1.x User Manual](#).

After the endpoints reboot, they are no longer online in PCoIP Management Console 1. If you configure the endpoints to include the address for the newer PCoIP Management Console, or update

your DHCP options appropriately, then the endpoints are present in the new PCoIP Management Console in a few minutes.

Upgrading Firmware Using the Endpoint's AWI

To update the firmware for an individual endpoint using the AWI:

1. Enter the endpoint's IP address in your browser's address bar and then log in to its AWI.
2. Select the **Upload > Firmware** menu.
3. From the *Firmware Upload* page, browse to the folder containing the firmware file. This file will have an `.all` extension.
4. Double-click the *.all* firmware file and then click ****Upload***.
5. Click **OK** to confirm that you want to proceed with the upload. The operation may take a few minutes. When completed, the AWI page displays two buttons—**Reset** and **Continue**.
6. Click **Reset**.
7. Click **OK**.

Downgrading Endpoints to an Older Firmware

From PCoIP Management Console, you can apply a profile to a group of endpoints running firmware 20.01 or higher to remotely downgrade firmware to an older version. Alternatively, you can downgrade the firmware on an individual endpoint using the endpoint's AWI.

Important: Perform a firmware upload twice when downgrading firmware to 4.8.x on a Tera2 PCoIP Zero Client

For PCoIP Zero Clients, you will need to perform a firmware upload twice. This is because the current firmware installed in the endpoint also contains a recovery image that exists in a different location in flash memory from the firmware image. When you upload a new firmware file to the endpoint, the recovery image is left untouched to guarantee that if the firmware upload fails, a bootable image to boot from still exists. It is therefore necessary to perform another full upload to ensure that the recovery image is completely removed. When using PCoIP Management Console to perform a downgrade to an older firmware, the second firmware upload will need to be completed using PCoIP Management Console 1. Alternatively, you can upload the firmware twice from the PCoIP Zero Client AWI. For more details about recovery mode, please see [PCoIP Zero Client Firmware Administrators' Guide](#). This does not apply to Remote Workstation Cards.

Downgrading Endpoint Firmware Using a PCoIP Management Console Profile

Before you begin, be sure you assign the firmware for the endpoints you wish to downgrade to a group. See [Organizing Endpoints into Groups](#) to find out more.

DOWNLOADING THE FIRMWARE

All access subscribers can obtain the latest firmware by navigating to the [Uploading the Firmware to the PCoIP Management Console](#)

[To upload the firmware to the PCoIP Management Console:](#)

- [1. Download the older firmware file for PCoIP Zero Clients, and if required the older firmware file for Remote Workstation Cards, and extract the package contents.](#)

2. From PCoIP Management Console, click **SETTINGS > SOFTWARE** to display the *SOFTWARE MANAGEMENT* window.
3. Click **Add Software/Firmware**.
4. Click **Select file**, select the combined firmware `.pcoip` file that you extracted previously, and then click **Open** and **Upload** to upload the file to the PCoIP Management Console.

ASSOCIATING A PROFILE WITH A GROUP

To associate a profile with a group:

1. In the PCoIP Management Console top menu, click **PROFILE** and then **NEW PROFILE**.
2. Enter a name and description for the older firmware profile.
3. Click the + tab, select the appropriate profile option and click **ADD**.

Options are:

- TERA2: CLIENT [DUAL] - (latest firmware)
- TERA2: CLIENT [QUAD] - (latest firmware)
- TERA2: HOST [DUAL] - (latest firmware)
- TERA2: HOST [QUAD] - (latest firmware)

4. In the *SOFTWARE* section, select the firmware file from the Firmware Version drop-down list, and then click **SAVE**.
5. From the *ENDPOINTS* page, select the group containing the endpoint(s) you want to downgrade.
6. Click **PROFILE** and then select **CHANGE**.
7. In the drop-down list, select the profile you just created, and then click **OK**.
8. Select the **I understand** message and click **OK** again.

APPLYING THE PROFILE IMMEDIATELY

You can apply the profile immediately to either a group of endpoints or an individual endpoint.

To apply the group or individual profile immediately:

1. In the PCoIP Management Console top menu, click **ENDPOINTS** and select the desired group or endpoint.
2. Click **PROFILE** and then select **APPLY**.
3. Enable the **I understand** message and then click **APPLY**.
4. From the *DASHBOARD*, check **Endpoint Updates in Progress** in the *CURRENT ACTIVITY* section for information about the update.

 **Note: Synchronize firmware image after applying profile**

After the profile applies, the selected PCoIP Zero Clients will automatically restart and upload the latest firmware image. The Remote Workstation Cards will need to be restarted manually before it uploads the latest firmware image. After the restart, the endpoints will either no longer appear in the **ENDPOINTS** table or they may appear as offline. The PCoIP Management Console will not be able to manage them. To synchronize the recovery image (applicable to PCoIP Zero Clients only) in flash memory, perform the update again from PCoIP Management Console 1 using the **UPDATE > Update Devices > Update Firmware** feature. For details, see the PCoIP Management Console 1.x User Manual.

Creating a Schedule to Apply the Profile (Enterprise)

You can also create a schedule to apply the profile at a specific date and time.

To create a schedule to apply the profile:

1. In the PCoIP Management Console top menu, click **SCHEDULE**.
2. Ensure that the *All Schedules* setting is toggled to **ON**.
3. Select **NEW SCHEDULE**.
4. Configure the parameters as follows:
 - **Type:** Select **Apply Profile**.
 - **Name:** Enter a name for the schedule.
 - **Description:** Enter a description for the schedule.
 - **Enabled:** Toggle to **ON**.

- **Groups:** Click **ADD**, select the group containing the endpoints you want to downgrade, and then click **ADD**.
- **Start Time:** Click the time zone widget and select the desired date, then click the clock widget below the calendar and select the desired time.

 **Note: Change the default time zone**

By default, the PCoIP Management Console time zone is Coordinated Universal Time (UTC). If you are in a different time zone, you can display the PCoIP Management Console web interface in your own time zone to facilitate creating schedules. See [Config_local_time.md](#).

- Ensure that **Run Once** is selected.
5. Click **SAVE** at the top of the page.
 6. From the *DASHBOARD*, check **UPCOMING SCHEDULES** to see schedule information. When the schedule runs, you can view its progress by checking **Endpoint Updates in Progress** in the *CURRENT ACTIVITY* section.


Discovering Endpoints

Discovery Process Overview

Before endpoints can be managed by the PCoIP Management Console, they must first be discovered. Once discovered, the PCoIP Management Console will label the device as either a local or remote endpoint.

During the discovery process, the PCoIP Management Console determines whether a device is local or remote by comparing the IP address of the communicating endpoint with the IP address that the endpoint is configured with. If the two addresses are the same, the PCoIP Management Console labels the endpoint as a local endpoint. If the two IP addresses are different, such as in networks utilizing NAT devices, the PCoIP Management Console labels the endpoint as a remote endpoint. The PCoIP Management Console also labels an endpoint as local if the endpoint reports its IP address in the configured Local IP Address Ranges field found on the **SETTINGS > REMOTE > REMOTE CONFIGURATION** page. Endpoints identified as remote endpoints require a reverse proxy and additional configurations which are further described in [Remote Endpoint Management \(Enterprise\)](#)

This topic provides an overview of the main steps of the PCoIP endpoint discovery process.

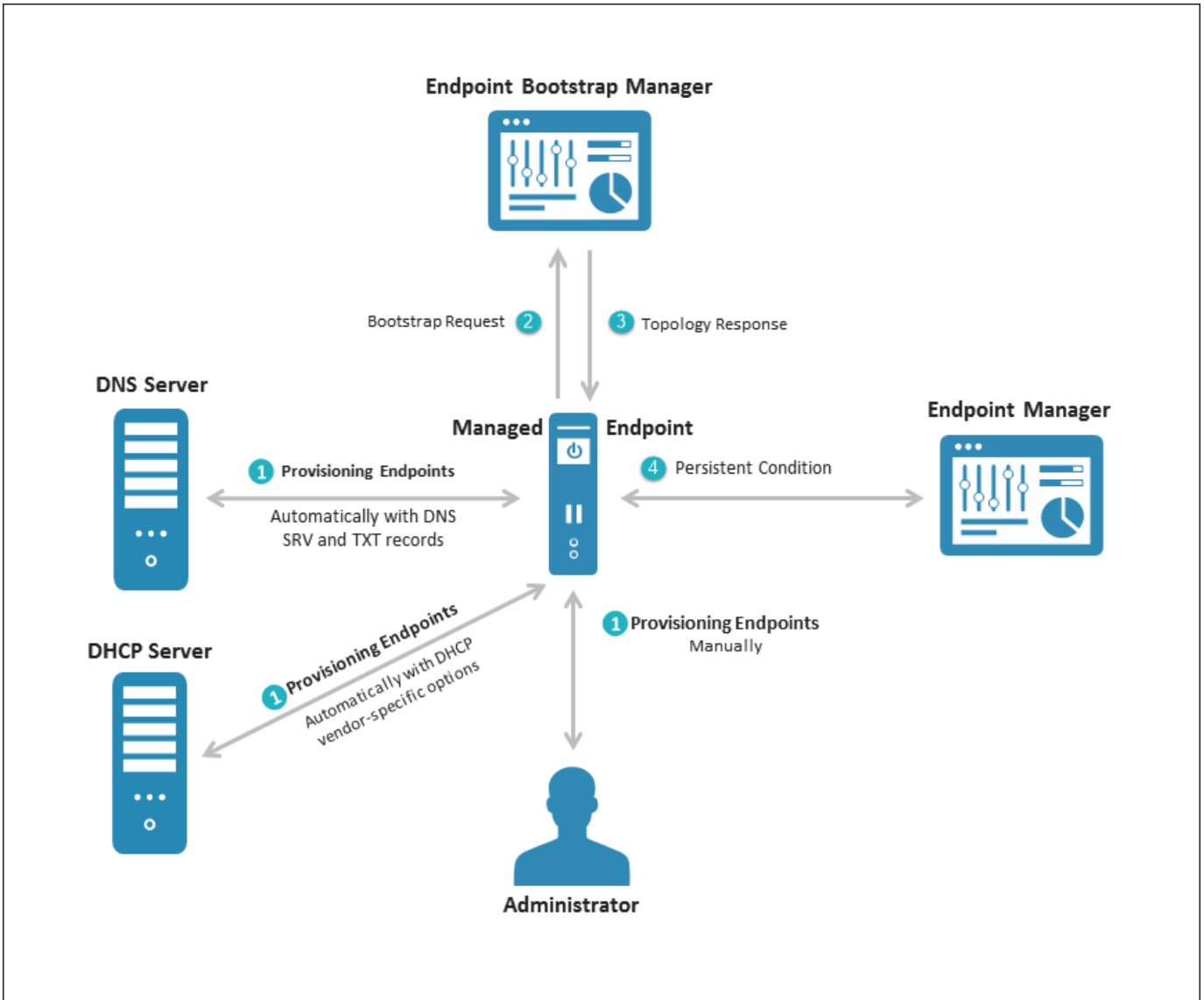
 **Important: Replace the default self-signed certificate with your own before configuring a discovery method and adding endpoints**

We strongly recommend that you replace the PCoIP Management Console self-signed certificate with your own PCoIP Management Console certificates before configuring a discovery method and before adding endpoints to the PCoIP Management Console. See [Managing PCoIP Management Console Certificates](#) for details.

The following diagram illustrates how endpoints discover a PCoIP Management Console.

Note: PCoIP Management Console serves as both Endpoint Bootstrap Manager and Endpoint Manager

The PCoIP Management Console serves as both the Endpoint Bootstrap Manager and the Endpoint Manager. It is possible that other endpoint managers of the PCoIP Management Console may separate these roles.



An illustration of PCoIP endpoint discovery process

Endpoint Discovery Process

The steps outlined in the preceding illustration are explained next.

Note: Endpoint Bootstrap Manager and Endpoint Manager information

The Endpoint Bootstrap Manager/Endpoint Manager information with which an endpoint must be provisioned before it can be discovered depends on the endpoint's discovery method and security level. You can configure both these options from the endpoint's AWI **Configuration > Management** page. Please see [PCoIP Zero Client Firmware Administrators' Guide](#) for details. See also [Configuring an Endpoint Manager Manually from an Endpoint](#) for instructions on how to manually configure an Endpoint Manager from its AWI Management page.

Stage 1: Provisioning Endpoints

There are three ways in which you can provision endpoints with endpoint bootstrap manager or endpoint manager information for automatic and manual discovery – DHCP vendor-specific options, DNS service and text records, Uniform Resource Identifier (URI).

The first stage provisions endpoints with the information they need either to connect to the Endpoint Bootstrap Manager for bootstrapping, or to connect directly to the Endpoint Manager. Depending on the endpoint's configured discovery method, you can manually enter the information or it can be provisioned automatically.

DISCOVERY METHODS

For automatic discovery, endpoints are populated with the IP address or FQDN of the PCoIP Management Console to which they should connect via DHCP vendor-specific options or DNS service and text records. Optionally, endpoints can also be configured with the PCoIP Management Console certificate's fingerprint (that is, its digital signature) by the DHCP or DNS server. If the PCoIP Management Console certificate fingerprint is provided in the DHCP or DNS record, the endpoint (in low security mode) will verify the PCoIP Management Console certificate by only matching the fingerprint. This is intended for use cases where the PCoIP Management Console trusted root CA certificate (the PCoIP Management Console chain certificate) is not uploaded to the endpoint, or if the PCoIP Management Console certificate does not meet the verification requirement. If a fingerprint is not provisioned, an endpoint without a trusted PCoIP Management Console certificate will fail to connect. Automatic discovery is used for low and medium security environments.

For manual discovery, you manually configure each endpoint with the uniform resource identifier (URI) of the Endpoint Bootstrap Manager (for low and medium security environments), or with the URI of the actual Endpoint Manager (for high security environments).

ENDPOINT CERTIFICATE REQUIREMENTS

Depending on an endpoint's configured security level, you may also need to provision endpoints with an PCoIP Management Console certificate.

Endpoints configured for medium or high security must have a trusted certificate in their certificate store before they can connect to an PCoIP Management Console. For some endpoints, certificates may be pre-loaded by the vendor as a factory default. Otherwise, you can manually upload certificates using an endpoint's AWI.

Endpoints that are configured for low security do not need a PCoIP Management Console certificate in their trusted certificate stores if either of the following is true:

- They are using DHCP discovery or DNS discovery and the DHCP or DNS server has provisioned them with the PCoIP Management Console certificate's fingerprint.
- They are discovered using the PCoIP Management Console's manual discovery method. See [Discovering Endpoints Manually from PCoIP Management Console](#).

The following table summarizes the certificate requirement for endpoints based on their discovery method and configured security level.

Certificate Requirements for Endpoints

Discovery Method	Low Security	Medium Security	High Security
DHCP/DNS discovery without Endpoint Bootstrap Manager fingerprint provisioned	Certificate required	Certificate required	N/A
DHCP/DNS discovery with Endpoint Bootstrap Manager fingerprint provisioned	Certificate *not*required	Certificate required	N/A
Discovery initiated by an endpoint configured for a high security environment	N/A	N/A	Certificate required
Manual discovery initiated by the PCoIP Management Console	Certificate not required	N/A	N/A

Information about endpoint security levels is summarized next.

Low Security

When low security is in use, endpoints can be discovered manually from the PCoIP Management Console. See [Discovering Endpoints Manually from PCoIP Management Console](#).

Endpoints can use DHCP or DNS autodiscovery. If the Endpoint Bootstrap Manager fingerprint is also provisioned by the DHCP or DNS server, endpoints do not require a certificate.

Medium Security

When medium security is in use, endpoints cannot be discovered manually from the PCoIP Management Console.

Endpoints will not use the certificate fingerprint retrieved from the DHCP or DNS server to trust the PCoIP Management Console. A PCoIP Management Console certificate or its issuer public key certificate must be pre-loaded in the endpoint.

High Security


When high security is in use, endpoints cannot be discovered manually from the PCoIP Management Console and cannot use DHCP or DNS autodiscovery.

The Endpoint Manager's address must be manually entered into the endpoint.

A PCoIP Management Console public key certificate or its issuer public key certificate must be pre-loaded in the endpoint.

Stage 2: Entering the Bootstrap Phase

Endpoints that have been provisioned with Endpoint Bootstrap Manager information enter a bootstrap phase where they evaluate the Endpoint Bootstrap Manager's certificate fingerprint to determine whether the Endpoint Bootstrap Manager can be trusted. If the certificate fingerprint match succeeds, the endpoints proceed to the next step.

 **Note: High security endpoints configured with Endpoint Manager information bypass the bootstrap process**

Endpoints in high security environments that are already configured with Endpoint Manager connection information bypass the Endpoint Bootstrap Manager bootstrap process and attempt to connect to the Endpoint Manager right away.

Stage 3: Receiving Endpoint Manager Information

Next, the Endpoint Bootstrap Manager provides the IP address and certificate fingerprint of the Endpoint Manager to which the endpoint should connect. The endpoint then disconnects from the Endpoint Bootstrap Manager and attempts to establish a connection with the Endpoint Manager.

Stage 4: Entering the Managed Phase

If Endpoint Manager certificate verification succeeds and the endpoint is able to establish a successful connection with the Endpoint Manager, the Endpoint Manager connection information is saved to the endpoint's permanent storage, and the endpoint enters the managed phase.

Configuring a Discovery Method

 **Note: Confirm your endpoint's discovery method**

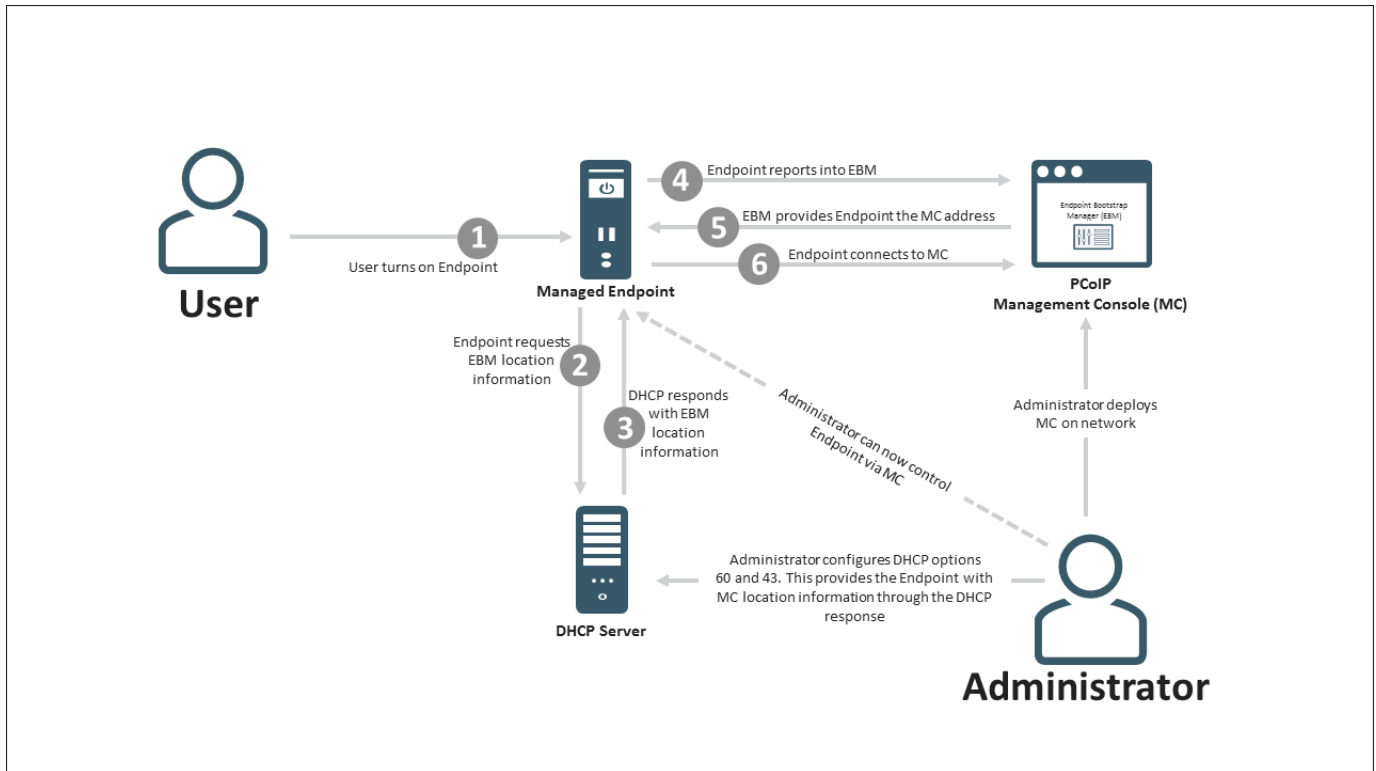
Review the administrators' guide for your endpoint to confirm the discovery method it supports.

The following topics contain information about how to configure an endpoint discovery method:

- [Configuring Endpoints using Auto Discovery](#): Explains how to configure your DHCP server to provision endpoints with Endpoint Bootstrap Manager information.
- [Configuring DNS SRV Record Discovery](#): Explains how to configure your DNS server to provision endpoints with Endpoint Bootstrap Manager information.
- [Configuring an Endpoint Manager Manually from an Endpoint](#): Explains how to manually configure an Endpoint Manager for an endpoint in a high security environment.
- [Discovering Endpoints Manually from PCoIP Management Console](#): Explains how to manually initiate discovery from the PCoIP Management Console. Endpoints must be configured for low security if you use this method.

Configuring DHCP for Endpoints that use Auto Discovery

This section explains how to configure your DHCP server to provision endpoints with Endpoint Bootstrap Manager information.



DHCP Discovery Process


When DHCP vendor class option discovery is used, endpoints receive a DHCP option value that contains information about the PCoIP Management Console (that is, the Endpoint Bootstrap Manager/Endpoint Manager) to which they should connect. If an endpoint has already obtained a DHCP lease before the server is configured with PCoIP Management Console DHCP options, it will be updated with this information when it renews the lease or acquires a new one. An endpoint will renew its lease after a reboot or when it detects that the network has returned after going down (for example, if someone reconnects the endpoint's network cable after unplugging one end of it).

Note: Endpoints also poll DHCP server for option values

Endpoints also poll the DHCP server for option values at an interval equal to half the DHCP lease time.

You can configure your DHCP server with vendor class options to provide the following information:

- The PCoIP Management Console's IP address or FQDN.
- The PCoIP Management Console's certificate fingerprint (digital signature). This fingerprint is required if you have not installed the PCoIP Management Console's trusted root CA certificate (the PCoIP Management Console chain certificate) in the endpoint's certificate store and you want to use automatic discovery. DHCP options discovery will not succeed if you do not provide a digital signature and do not configure endpoints with a certificate that enables them to trust the PCoIP Management Console. If provided, this fingerprint is only used when the endpoint's security level is set to **Low Security Environment** and certificate verification has failed. It is ignored when the security level is set to **Medium Security Environment** or **High Security Environment**.

 **Note: Provide PCoIP Management Console information using either DHCP options or DNS records**


The endpoint only picks up the fingerprint in a DHCP option if the PCoIP Management Console address is also specified in a DHCP option. For example, if the PCoIP Management Console address is specified as a DNS SRV record but the fingerprint is provided as a DHCP option, the endpoint will not retrieve the fingerprint information in the DHCP server. You should configure PCoIP Management Console information using either DHCP options or DNS records, but not both.

This discovery method requires you to have a DHCP server in your network that meets the following requirements:

- The DHCP server must support both DHCP option 60 (vendor class identifier) and option 43 (vendor-specific information). Option 60 is sent from the endpoint to the DHCP server. It contains a text string that uniquely identifies the endpoint type. Option 43 is created by the user. The steps provided in the sections that follow show how to create a DHCP option 43 called **PCoIP Endpoint** along with two sub-options under it— **EBM URI (sub-option 10)** and **EBM X.509 SHA-256 fingerprint** (sub-option 11).
- The PCoIP endpoints must have DHCP enabled so they can send a request to the DHCP server and receive the address of the PCoIP Management Console in response. This is their default setting.

Before You Begin

These instructions explain how to create a **PCoIP Endpoint** vendor class and how to create two DHCP options (sub-options 10 and 11) that provide PCoIP Management Console information to the PCoIP Endpoint.

 **Note: Skip adding vendor class if you have previously configured PCoIP Endpoint vendor class**

If you have used DHCP vendor class option discovery with a previous 1.x release of the PCoIP Management Console and have already configured your DHCP server with the PCoIP Endpoint vendor class, you can skip the following section entitled Adding the PCoIP Endpoint Vendor Class.

Before beginning, you should have the following information handy:

- The PCoIP Management Console's IP address or FQDN. In the following example, this address is configured in a DHCP sub-option called **EBM URI**.
- The PCoIP Management Console certificate SHA-256 fingerprint. In the following example, this hash value is configured in an optional DHCP sub-option called **EBM X.509 SHA-256 fingerprint**.

To locate the PCoIP Management Console's fingerprint:

1. Use Mozilla Firefox to log in to the PCoIP Management Console web interface.
2. Click the padlock icon in the browser's address bar.
3. Click **More Information**.
4. Click **View Certificate**.
5. In the **Fingerprints** section, copy and paste the SHA-256 fingerprint into a text editor.

 **Note: Examples shown use Windows Server 2012 R2**

The instructions provided may change slightly depending on your specific server version.

Adding the PCoIP Endpoint Vendor Class

To add the PCoIP DHCP vendor class to your DHCP server:

1. Log in to your Windows Server and select **DHCP**.
2. Right-click on your DHCP server in the **SERVERS** pane and select **DHCP Manager**.
3. Expand your server in the tree, right-click on **IPv4**, and then select **Define Vendor Classes**.
4. Click **Add** to add a new DHCP Vendor Class.
5. Enter **PCoIP Endpoint** in the *Display* name field.
6. Enter **PCoIP Endpoint** in the *ASCII* column as the Vendor ID.
7. Click **OK** to save and close the dialog.

Configuring DHCP Options

To add two PCoIP Management Console DHCP options and apply them to a scope:

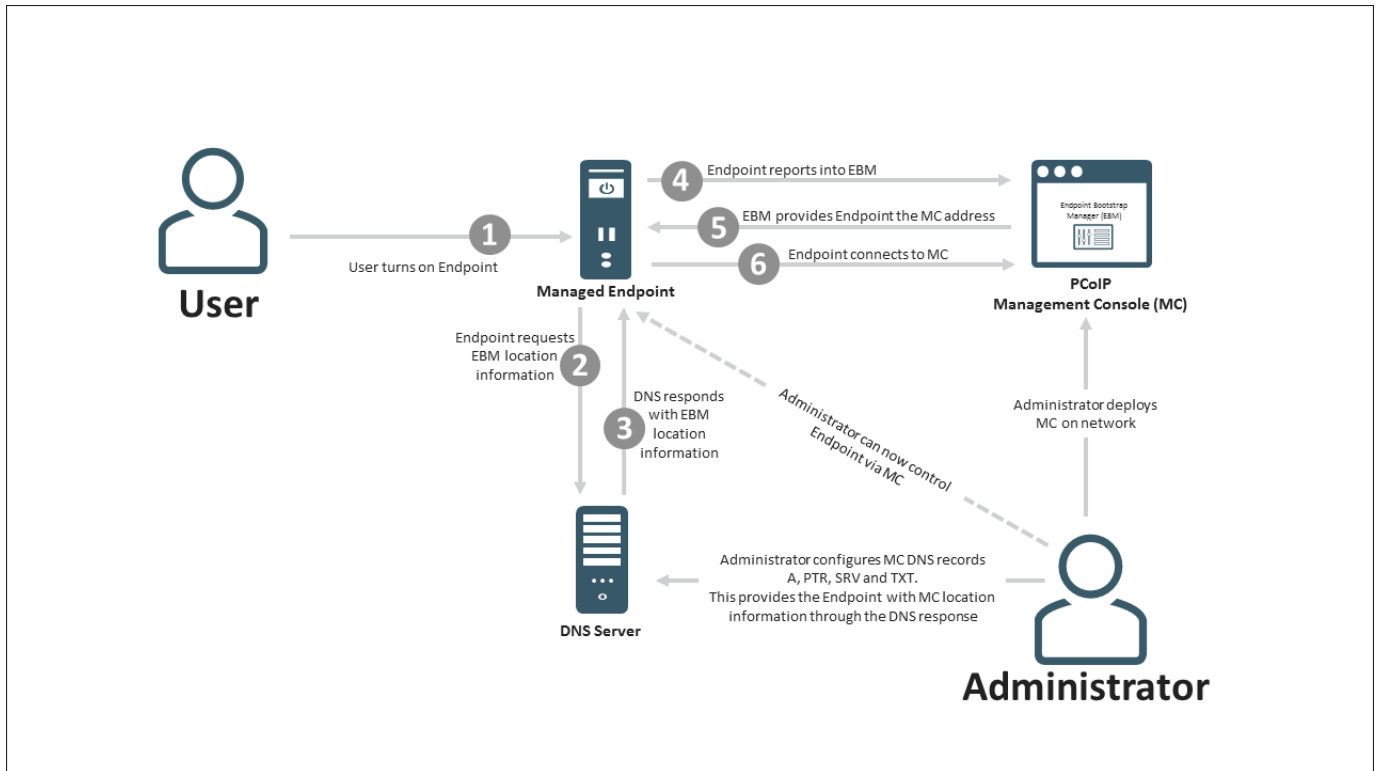
1. Right-click on **IPv4** in the tree and select **Set Predefined Options**.
2. Select **PCoIP Endpoint** as the **Option** class and click **Add**.
3. In the *Option Type* dialog, enter the name **EBM URI**, data type **String**, code **10**, and description **Endpoint Bootstrap Manager URI**, then click **OK**.
4. Click **OK** to save and close the dialog.
5. For the PCoIP Management Console's SHA-256 certificate fingerprint, repeat steps 1 and 2 to add another option.
6. In the *Option Type* dialog, enter the name **EBM X.509 SHA-256 fingerprint**, data type **String**, code **11**, and description **EBM X.509 SHA-256 fingerprint**, then click **OK**.
7. Expand the tree for the DHCP scope to which you want to apply the options.
8. Right-click **Scope Options** and select **Configure Options**.
9. Click the **Advanced** tab and select the **PCoIP Endpoint** vendor class.
10. Enable the check box for **010 EBM URI** and then enter a valid Management Console URI in the **Data entry** field, and click **Apply**.

This URI requires a secured WebSocket prefix (for example, `wss://:[port number]`). The PCoIP Management Console's listening port is 5172. Entering this port number is optional. If you do not include it, port 5172 will be used by default.

11. Choose the checkbox for **011 EBM X.509 SHA-256 fingerprint** and paste the PCoIP Management Console certificate SHA-256 fingerprint you obtained previously into the *String value* field.
12. Click **OK** to save and close the dialog.

Configuring DNS for Endpoints that use Autodiscovery

This section explains how to configure your DNS server to provision endpoints with Endpoint Bootstrap Manager information, as part of the endpoint autodiscovery process.



DNS Discovery Process

Endpoints poll the DNS server for information about the PCoIP Management Console (that is, the Endpoint Bootstrap Manager/Endpoint Manager) to which they should connect only if the DHCP server does not have a DHCP option containing the PCoIP Management Console’s IP address or FQDN.


If an endpoint has already retrieved a DNS record before the DNS server is configured with PCoIP Management Console information, it does not poll the DNS server again until the record’s Time-To-Live expires (or the endpoint is rebooted). If the DHCP server does provide an option for the PCoIP Management Console address but the endpoint fails to connect for any reason (for example, because of a certificate verification failure or the PCoIP Management Console address is not reachable), DNS record lookup will not occur.

 **Note: Do not configure DHCP options when you are using DNS record discovery**

Do not configure DHCP options if you want to use DNS record discovery. Endpoints always prefer the PCoIP Management Console address or fingerprint that is specified in the DHCP options over that specified in the DNS record. If you provide the PCoIP Management Console address both as DHCP option and also as the DNS record, the endpoint will only use the PCoIP Management Console address found in the DHCP option.

DNS service record discovery requires you to have a DNS server in your network that is configured with the following DNS records:

- **An address record (A record):** Specifies the FQDN and IP address of the PCoIP Management Console. This record may be automatically created by the DHCP server.
- **A service location record (SRV record):** Associates information such as the PCoIP Management Console's TCP/IP service and the port the PCoIP Management Console listens on with the PCoIP Management Console's domain and host name. The PCoIP Management Console's TCP/IP service is called **_pcoip-bootstrap**, as shown in [Adding the DNS SRV Record](#).
- **A DNS TXT record:** Contains the PCoIP Management Console certificate SHA-256 fingerprint is also required if you have not installed the PCoIP Management Console's trusted root CA certificate (the PCoIP Management Console chain certificate) in the endpoint's certificate store and you want to use automatic discovery. The record's name must be the host name of the PCoIP Management Console offering the service. In the following example, this record is called **pcoip-mc38719**. The domain is appended automatically.

 **Note: Endpoint only picks up DNS TXT fingerprint if the PCoIP Management Console address is specified in a DNS SRV record**

The endpoint only picks up the fingerprint from the DNS TXT record if the PCoIP Management Console address is specified in a DNS SRV record. For example, if the PCoIP Management Console address is specified as a DHCP option but the fingerprint is provided as a DNS TXT record, the endpoint will not retrieve the fingerprint information in the DNS server. Configure your PCoIP Management Console information using either DHCP options or DNS records, but not both.

Before You Begin

Before configuring your DNS SRV record discovery, you'll need the following information:

- The PCoIP Management Console's FQDN
- The PCoIP Management Console's certificate fingerprint (that is, the certificate's digital signature). If provided, this fingerprint is only used when the endpoint's security level is set to **Low Security Environment** and certificate verification has failed. It is ignored when the security level is set to **Medium Security Environment** or **High Security Environment**.

To locate the PCoIP Management Console's fingerprint:

1. Use Mozilla Firefox to log in to the PCoIP Management Console web interface.
2. Click the padlock icon in the browser's address bar.
3. Click **More Information**.
4. Click **View Certificate**.
5. In the **Fingerprints** section, copy and paste the SHA-256 fingerprint into a text editor.

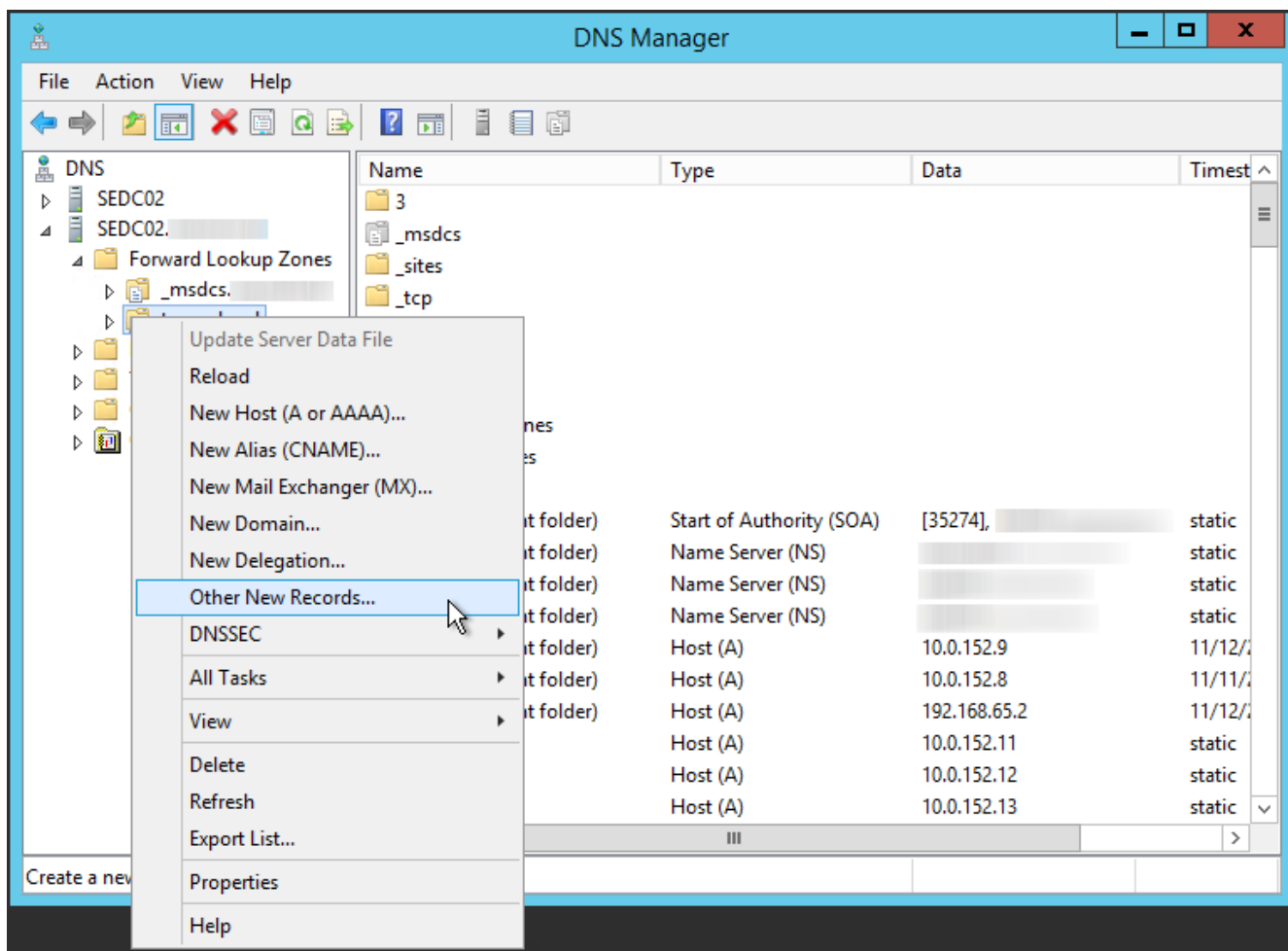
 **Note: Examples shown use Windows Server 2012 R2**

The instructions provided may change slightly depending on your specific server version.

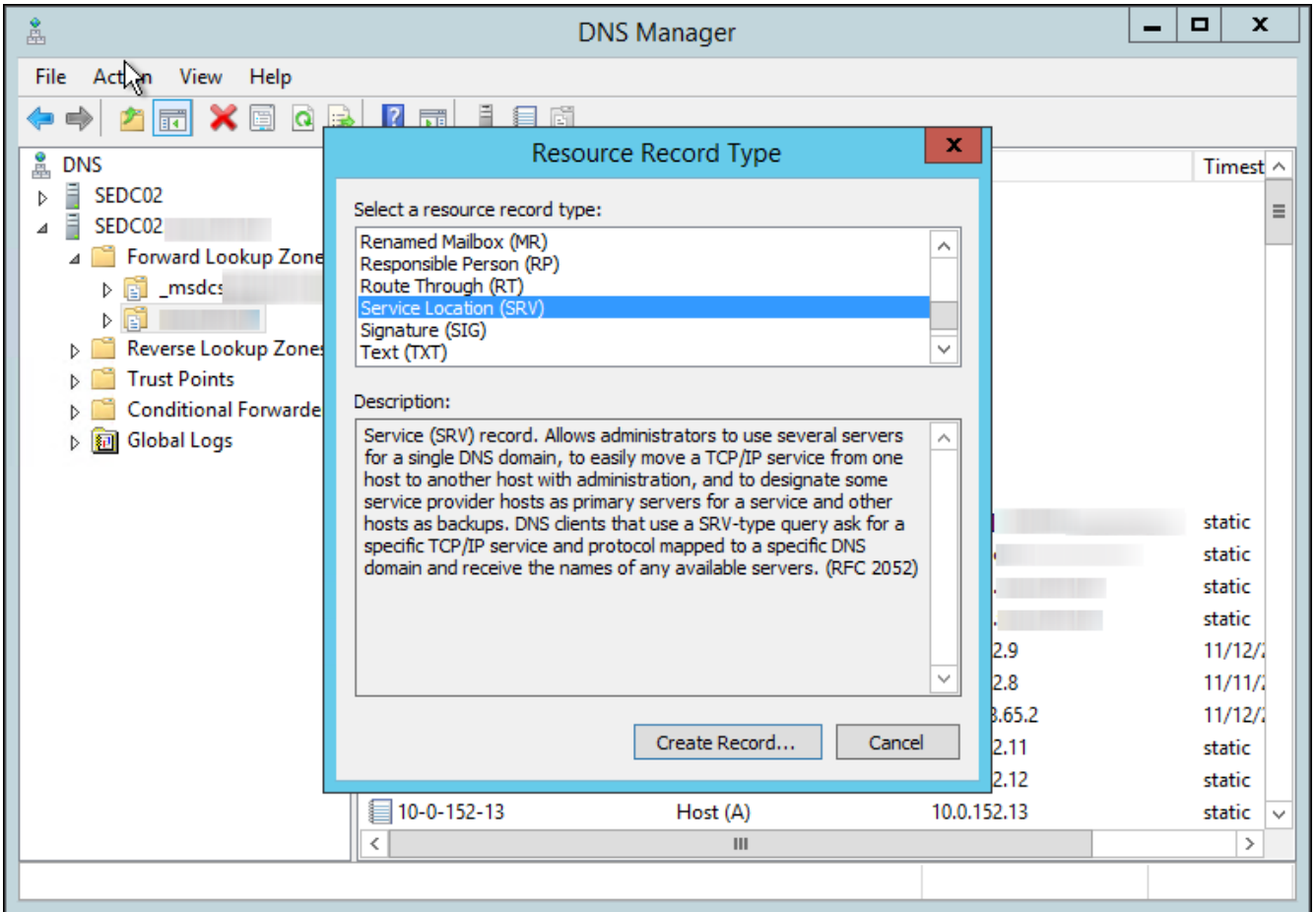
Adding the DNS SRV Record

To add the PCoIP Management Console DNS SRV record to DNS server:

1. Log in to your Windows Server and select **DNS**.
2. Right-click on your DNS server in the *SERVERS* pane and select **DNS Manager** from the context menu.
3. In *Forward Lookup Zones*, right-click on your domain and select **Other New Records** from the context menu.



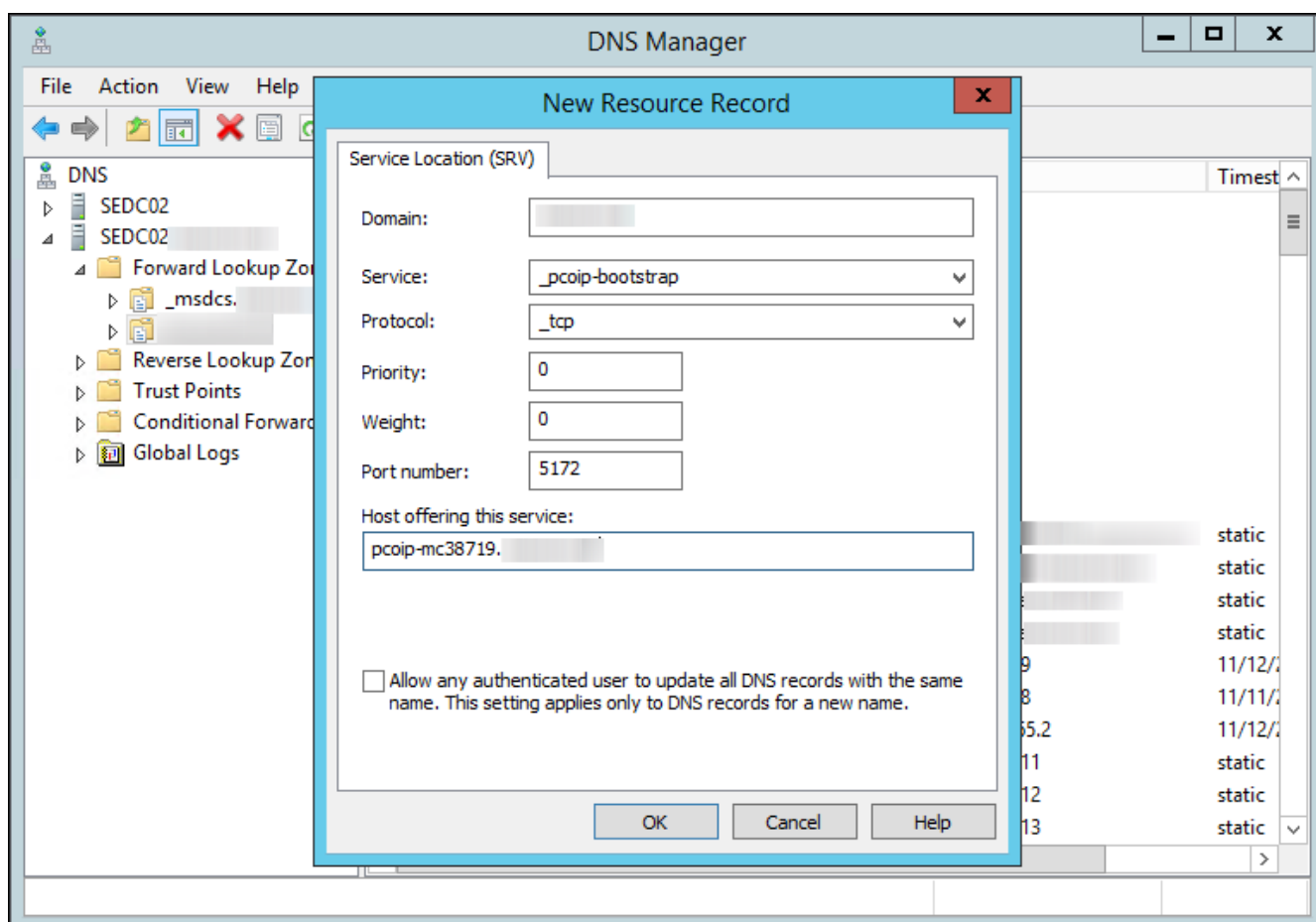
4. In the *Resource Record Type* dialog, select **Service Location (SRV)** from the list and click **Create Record**.



5. Fill in the entries as shown in the following example. Set Service to **_pcoip-bootstrap**, Protocol to **_tcp**, and *Port number* to **5172**, the PCoIP Management Console’s default listening port. For *Host offering this service*, enter the PCoIP Management Console’s FQDN.

Note: FQDN must be entered in place of IP address

The PCoIP Management Console’s FQDN must be entered because the DNS specification does not enable an IP address in SRV records.



6. Click **OK**.
7. If you are not adding an optional DNS TXT record (see next) and have finished configuring your DNS server, power cycle your endpoints or put them online to enable them to make the connection to the PCoIP Management Console. You must also upload the PCoIP Management Console's root CA certificate to the endpoint's certificate store.

Adding a DNS TXT Record

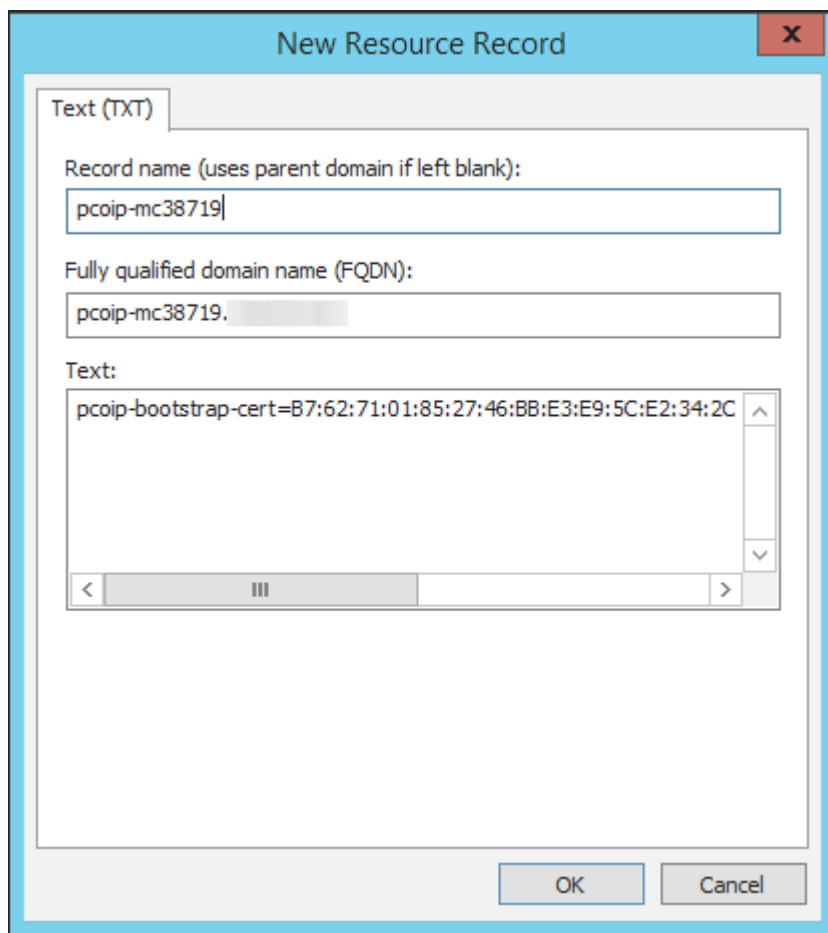
If your endpoints do not have the PCoIP Management Console's root CA certificate installed in their certificate store, you must configure your DNS server with a DNS TXT record containing the PCoIP Management Console certificate SHA-256 fingerprint.

To add a DNS TXT record:

1. In *Forward Lookup Zones*, right-click on your domain and select **Other New Records** from the context menu.
2. In the Resource Record Type dialog, select **Text (TXT)** from the list and click ****Create Record***.

3. Fill in the entries as follows:

- In the *Record name* field, enter the host name of the PCoIP Management Console offering the service (this example uses *pcoip-mc38719*). The FQDN field will be automatically populated for you, and matches the FQDN of the PCoIP Management Console.
- In the *Text* field, type `pcoip-bootstrap-cert=` and then paste the PCoIP Management Console certificate SHA-256 fingerprint you obtained previously immediately after this prefix, as shown in the following example.




The screenshot shows a 'New Resource Record' dialog box with the following fields and values:

- Record name (uses parent domain if left blank):** pcoip-mc38719
- Fully qualified domain name (FQDN):** pcoip-mc38719.
- Text:** pcoip-bootstrap-cert=B7:62:71:01:85:27:46:BB:E3:E9:5C:E2:34:2C

The dialog box has 'OK' and 'Cancel' buttons at the bottom.

4. Click **OK**.

5. When you have finished configuring your DNS server, power cycle your endpoints or put them online to enable them to make the connection to the PCoIP Management Console.

 **Note: Automatically name and group endpoints**

You can configure the PCoIP Management Console to automatically name endpoints and place them in a specific group when they are discovered. See [Auto Naming Endpoints](#) and [Auto Configuring Endpoints \(Enterprise\)](#) for details.

See [Troubleshooting DNS](#) to verify that your DNS server is configured correctly for the PCoIP Management Console.

Discovering Endpoints Manually from PCoIP Management Console

The **ENDPOINTS** page contains an **ENDPOINT DISCOVERY** feature that lets you discover endpoints that are not pre-configured with PCoIP Management Console information. Endpoints must be configured for low security before they can be discovered using this method.

Important: If your endpoints are behind a NAT or proxy

Manual discovery of an endpoint will not work if the endpoint is behind a NAT or proxy.

MANAGEMENT profile properties, **Security Level** and **Discovery Mode** have been added to allow the PCoIP Management Console the ability to apply specific management security level and management server discovery methods. This enables highly secured environments to pre-stage endpoints in a secured environment with their future management settings, prior to delivery to their final location.

Note: Endpoint discovery options

The PCoIP Management Console also supports the DHCP vendor-specific option method, DNS service record method, and manual endpoint configuration for endpoint discovery.

You can discover endpoints from the PCoIP Management Console by scanning for their IP addresses. This discovery method is used in low security environments for endpoints that are not pre-configured with PCoIP Management Console connection information or certificates. It enables an improved out-of-box experience by removing the need for administrators to manually configure an endpoint with a PCoIP Management Console address and upload a PCoIP Management Console certificate to the endpoint. With this method, the endpoint retrieves the required trust information from the PCoIP Management Console during the discovery process.

In order for discovery to succeed, the following conditions must apply:

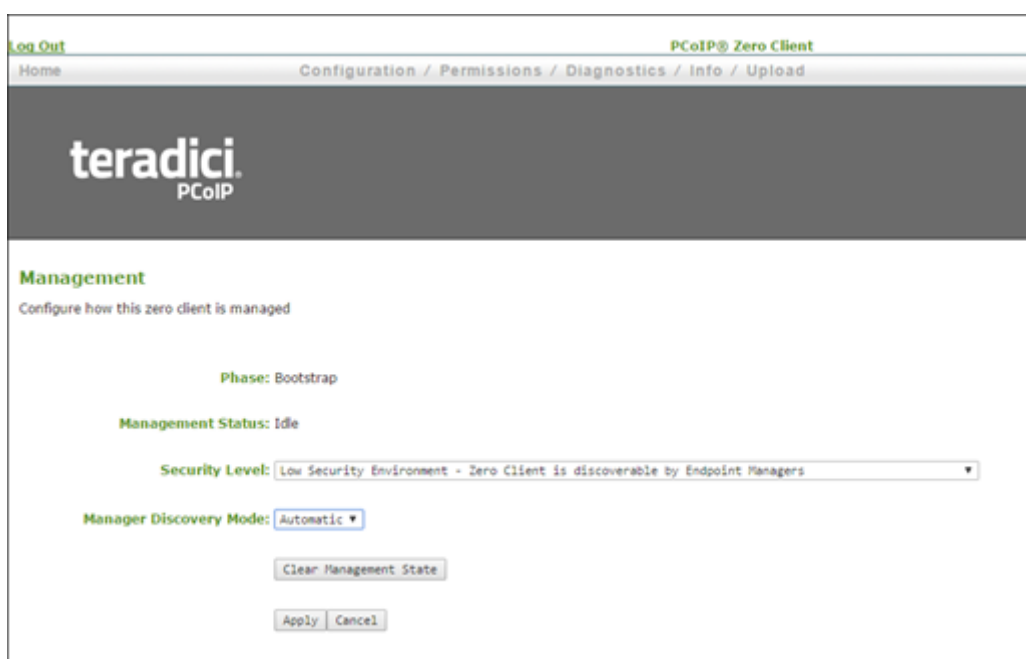
- The endpoint is powered on and connected to the network that is not behind a proxy or NAT.
- The endpoint is not connected to an Endpoint Manager and has an **Idle** management status (that is, is not engaged in any kind of PCoIP Management Console activity).
- The endpoint is configured for a Low Security Environment from its AWI Management page.

Configuring the Endpoint for Low Security Environment

Your endpoints may already be configured for low security by default. These steps are only necessary for endpoints with a different security configuration. It is important to complete them in the following order.

To configure the endpoint for Low Security Environment:

1. Enter the PCoIP Zero Client's IP address in your browser's address bar, then log in to its AWI.
2. From the Configuration menu, select **Management**.
3. Change the *Security Level* to **Low Security Environment**.



The screenshot shows the 'Management' configuration page for a PCoIP Zero Client. The page header includes 'Log Out' and 'PCoIP® Zero Client'. The breadcrumb trail is 'Home / Configuration / Permissions / Diagnostics / Info / Upload'. The Teradici PCoIP logo is displayed. The main content area is titled 'Management' and includes the instruction 'Configure how this zero client is managed'. The configuration details are as follows: Phase: Bootstrap; Management Status: Idle; Security Level: Low Security Environment - Zero Client is discoverable by Endpoint Managers (selected in a dropdown menu); Manager Discovery Mode: Automatic (selected in a dropdown menu). At the bottom, there are buttons for 'Clear Management State', 'Apply', and 'Cancel'.

4. If the endpoint is not in the Idle state, click **Clear Management State** and then **Continue**.
5. Click **Apply** and then **Continue**.

Discovering Endpoints from the PCoIP Management Console

To discover endpoints manually:

1. From the PCoIP Management Console's ENDPOINT page, click **ENDPOINT DISCOVERY**.
2. Enter the endpoint's IP address in the **FROM IP** boxes. If you want to discover a range of endpoints, enter the last IP address in the **TO IP** boxes; otherwise, leave these boxes empty.

Note: IP address range is limited to Class C ranges only

The IP address range is limited to Class C ranges or smaller (for example, 10.0.0.1 to 10.0.0.255). It cannot support a range larger than a class C such as 10.0.0.1 to 10.0.255.255.

3. Click outside a box, and then click **DISCOVER**.

4. Click **DONE** when it appears next to ENDPOINT DISCOVERY to end the discovery process.

5. To see the newly discovered endpoints, click **REFRESH** in the endpoint table (**GROUPED** or **UNGROUPED**, depending on your auto configuration settings).

NAME	MAC ADDRESS	FQDN	IPv4 ADDRESS	SOFTWARE VERSION	ENDPOINT DESCRIPTION	DEVICE STATUS	AUTO CONFIGURATION STATUS	INTERNAL IPv4	CONNECTED BY
00-30-04-12-66-3E	00:30:04:12:66:3e	pcoip-portal-0030040e4789.teradici.local	10.0.8.65	6.1.0	Tera2 Client Dual Display	Offline	Auto Configuration Disabled	10.0.8.65	Local

Note: Automatically name and group endpoints

You can configure the PCoIP Management Console to automatically name endpoints and place them in a specific group when they are discovered. See [Auto Naming Endpoints](#) and [Auto Configuring Endpoints \(Enterprise\)](#) for details.

Managing Endpoints

Managing Endpoints

This section contains the following topics:


- [Understanding the PCoIP Management Console Dashboard](#): Describes the information you can view from the PCoIP Management Console **DASHBOARD** page.
- [Changing the Web Interface Time Zone](#): Explains how to change the PCoIP Management Console web interface time zone. By default, the web interface uses the PCoIP Management Console's Coordinated Universal Time (UTC). For convenience when you create schedules, you can update your user account to display the web interface in your own local time zone.
- [The actions you can perform from the ENDPOINTS page are listed in the following table](#): Lists all the actions you can perform from the **ENDPOINTS** page and provides links to instructions for each one.
- [Displaying Endpoint Properties](#): Shows how to select the endpoint properties you wish to include in a *GROUPED* or *UNGROUPED* endpoint table.
- [Using the ENDPOINT DETAILS Page](#): Lists all the actions you can perform from the **ENDPOINT DETAILS** page and provides instructions for each one.
- [Performing Power Management](#): Explains how to power down and reset endpoints remotely.
- [Renaming Endpoints](#): Explains how to rename an endpoint from the **ENDPOINTS** page.
- [Deleting Endpoints](#): This topic explains how to delete endpoints.
- [Discovering Endpoints Manually](#): Provides information about how to use the PCoIP Management Console's manual endpoint discovery feature.
- [Searching an Endpoint Table](#): Explains how to use a text search to locate endpoints in a *GROUPED* or *UNGROUPED* endpoint table.
- [Filtering the Endpoint List](#): Explains how to use PCoIP Management Console filters to refine the endpoints that display in a *GROUPED* or *UNGROUPED* endpoint table.
- [Requesting Endpoint Certificates Using SCEP \(Enterprise\)](#): Available in PCoIP Management Console Enterprise. Explains how to simplify the retrieval and installation of digital certificates by enabling devices to obtain certificates automatically from a SCEP server.

Managing Profiles

The PCoIP Management Console lets you create profiles that contain a list of the settings you want to apply to one or more groups of endpoints. After creating a profile, you can apply it immediately to a group, or you can create a schedule to apply it to the group at a specific time in the future.

Displaying Profile Information

The **PROFILE** page contains a table showing all the profiles that are currently configured. You can create a new profile from this page, or you can select a profile from the table to edit, duplicate, or delete it.

Click the gear icon  to the right of the table to change the information you want to display in the table columns. Your customized settings are saved in your browser and will be used for any user who subsequently logs in from that browser.

NAME	DESCRIPTION	GROUP	ENDPOINT TYPES	CREATED	LAST UPDATED
Accounting	Vancouver accounting department	Accounting	TERA2	2016-01-11 03:55 PM PST	2016-01-11 04:49 PM PST
Engineering	Burnaby engineers	Engineering	TERA2	2016-01-11 03:55 PM PST	2016-01-11 04:49 PM PST
Marketing	Product marketing	Marketing	TERA2	2016-01-11 03:56 PM PST	2016-01-11 04:50 PM PST

PROFILE Page

Creating a Profile

When you configure a profile, you specify only the settings you want to configure in the endpoint. For example, you can create a profile that only updates endpoint firmware without changing any of the endpoint's other settings. Unless a particular setting is explicitly configured in a profile by enabling its **Set In Profile** check box, it will have no effect when the endpoints are updated.

Some settings will cause the endpoint to restart. These settings are identified by a white triangular



icon . If configured, a **Reset Notification Timeout** overlay will warn users of a pending restart. This warning can be configured to appear up to 5 minutes prior to the restart, and can be configured in the **POWER** section of the profile.

Firmware in profile is the same as on the endpoint

The Management Console will only apply the firmware in a profile to the endpoint, if the firmware version is different from the firmware identified from the last polling communication between the Management Console and endpoint.

The settings that are available are based on the endpoint type and the firmware version the target endpoints are currently using or will use when the profile is applied. For this reason, the relevant firmware file must already be uploaded to the PCoIP Management Console from the **SETTINGS > SOFTWARE** page before you can create a profile.

For the PCoIP Zero Client and Remote Workstation Card, you can configure profiles for dual and quad endpoint types. The dual PCoIP Zero Client supports two monitors. The quad PCoIP Zero Client supports four monitors. You need to create a separate profile for each endpoint type.

To create a profile:

1. From the PCoIP Management Console's top menu, click **PROFILE**.
2. Click **NEW PROFILE**.
3. Enter a unique profile name in the *Name* column and a description for the profile in the *Description* column.
4. Click the + tab and select one of the following profile types and then click **ADD**:
 - **TERA2: CLIENT [DUAL]**: For endpoints that support two monitors.
 - **TERA2: CLIENT [QUAD]**: For endpoints that support four monitors.
 - **TERA2: HOST [DUAL]**: For endpoints that support two monitors.
 - **TERA2: HOST [QUAD]**: For endpoints that support four monitors.
5. For each setting you want to configure:
 - a. Enable the **Set In Profile** check box.

b. Perform the required configuration.

Note: Navigating between profile settings

To navigate between profile settings, you can either use the scroll bar or select a setting category in the left pane. Any setting followed by the restart icon indicates that the endpoint requires a restart after being changed.

6. Click **SAVE**.

7. Click **PROFILE** in the navigation link at the top to return to the main page.

Associating a Profile with a Group

Before you can apply a profile, you must associate it with a group. Profiles can also be associated with multiple groups.

To associate a profile with a group:

1. From the **ENDPOINTS** page, select the desired group.
2. Click **PROFILE** and then **CHANGE**.

3. In the **Change Profile** dialog, select the profile from the drop-down list and click **OK**.
4. Enable the **I understand** message and click **OK**.

 **Note: Child groups will inherit their parent group's profile**

Child groups with no assigned profile inherit their parent group's profile. This rule is recursive. For example, if top-level group A has a profile and both its child B and B's child C do not, then B and C both use the profile assigned to A.

Changing a Profile Association

To change a profile that is assigned to a group:

1. From the **ENDPOINTS** page, select the desired group.
2. Click **PROFILE** and then **CHANGE**.
3. In the **Change Profile** dialog, select a different profile from the drop-down list and click **OK**.
4. Enable the **I understand** message and click **OK**.

Applying a Profile

You can apply profiles so they update endpoint settings right away (or after any currently running scheduled actions have completed), or you can create a schedule to apply the settings in the future.

You can apply a profile to one or more groups or endpoints from the **ENDPOINTS** page or you can apply a profile to an endpoint from its **ENDPOINT DETAILS** page.

Applying a Profile Immediately

To force the profile to apply right away or after any currently running scheduled actions have completed:

1. From the **ENDPOINTS** page, select one or more groups (or one or more endpoints).

 **Note:** Use **Shift**+Click and **Ctrl**+Click to click elements

Use **Shift**+Click to select contiguous elements and **Ctrl**+Click to select non-contiguous elements.

2. Click **PROFILE** and then **APPLY**.
3. Enable the **I understand** message and then click **APPLY**.

Applying a Profile in the Future (Enterprise)

You can also create a schedule to run at a later time in the future with PCoIP Management Console Enterprise. For details, see [Creating a Schedule](#).

Duplicating a Profile

The PCoIP Management Console provides an easy way to duplicate a profile when you want to copy all the profile's settings except for its group association.


To duplicate a profile:

1. Select the profile in the *PROFILE* list.
2. Click **DUPLICATE**.
3. Enter a unique name for the profile and click **DUPLICATE**.
4. Follow the instructions in Applying a Profile to associate the profile with the desired group and choose how to apply it.

Editing a Profile

To edit a profile:

1. Select the profile in the *PROFILE* list.
2. Click **EDIT**.
3. If desired, change the **Name** and/or **Description** entries.

4. To see the group(s) to which this profile is assigned, click the small group tab  that appears to the right.
5. To edit profile settings, choose one of the following:
 - To remove all of the settings click the on the profile tab and then click REMOVE. You can then click the + tab and [configure a new profile](#).
 - To change one or more settings, click the profile tab and make your changes, as explained in [Creating a Profile](#).
6. Click **SAVE**.
7. Click **PROFILE** in the navigation link at the top to return to the main **PROFILE** page.
8. Follow the instructions in [Applying a Profile](#) to choose how to apply the updated profile.

Importing or Exporting a Profile

Management Console allows the saving and reusing of profile configurations through the import and export feature accessed via the IMPORT and EXPORT buttons. This feature has the following characteristics:

- Only one profile can be imported or exported at a time.
- Profile files are saved with a **.profile** extension and have the date and time appended to the file name.

Example: <Profile name>-Date(YYYYMMDD)-Time(HHMMSS).milliseconds.profile

- The appended information is not displayed as part of the profile name on the PROFILE page

Profile files

Profile files are identified by the **.profile** extension. Support recommends not changing the file name of a profile file. Instead, when a profile name needs to be changed, perform this task by editing the profile name seen on the *PROFILE* page of the Management Console

- Displayed dialog windows provides messages to warn administrators of possible firmware issues prior to applying the profile
- Profiles must contain a configuration to be imported or exported

To ensure all configured settings are correctly applied to your endpoints, Management Console must be uploaded with the same version of host or client firmware . However, Management Console will compensate for missing firmware versions by including warning messages before applying the profile. Warnings include advising endpoints will move to a newer firmware, unsupported settings will be ignored when moving to an older firmware, duplicate profiles are present. These messages allow administrator's to take corrective actions prior to applying a profile if required.

To import a profile:

1. Click the **Import** button.
2. Click **SELECT FILE** and browse to the location of the profile file you wish to import
3. Click **Import**.

To export a profile:

1. Select the **EXPORT** button.
2. Save your profile to a location of your choice.

Deleting a Profile

To delete a profile:

1. If the profile is assigned to one or more groups, first remove the association for each group as follows:
 - a. From the *ENDPOINTS* page, select the group to which the profile is assigned.
 - b. Click **PROFILE** and then **CHANGE**.
 - c. In the *Change Profile* dialog, select **No Profile** from the drop-down list and click **OK**.
 - d. Enable the **I understand** message and click **OK**.
2. From the *PROFILE* page, select the profile you wish to delete.
3. Click **DELETE**.
4. Enable the **I confirm** message and click **DELETE**.

Viewing Profile Details

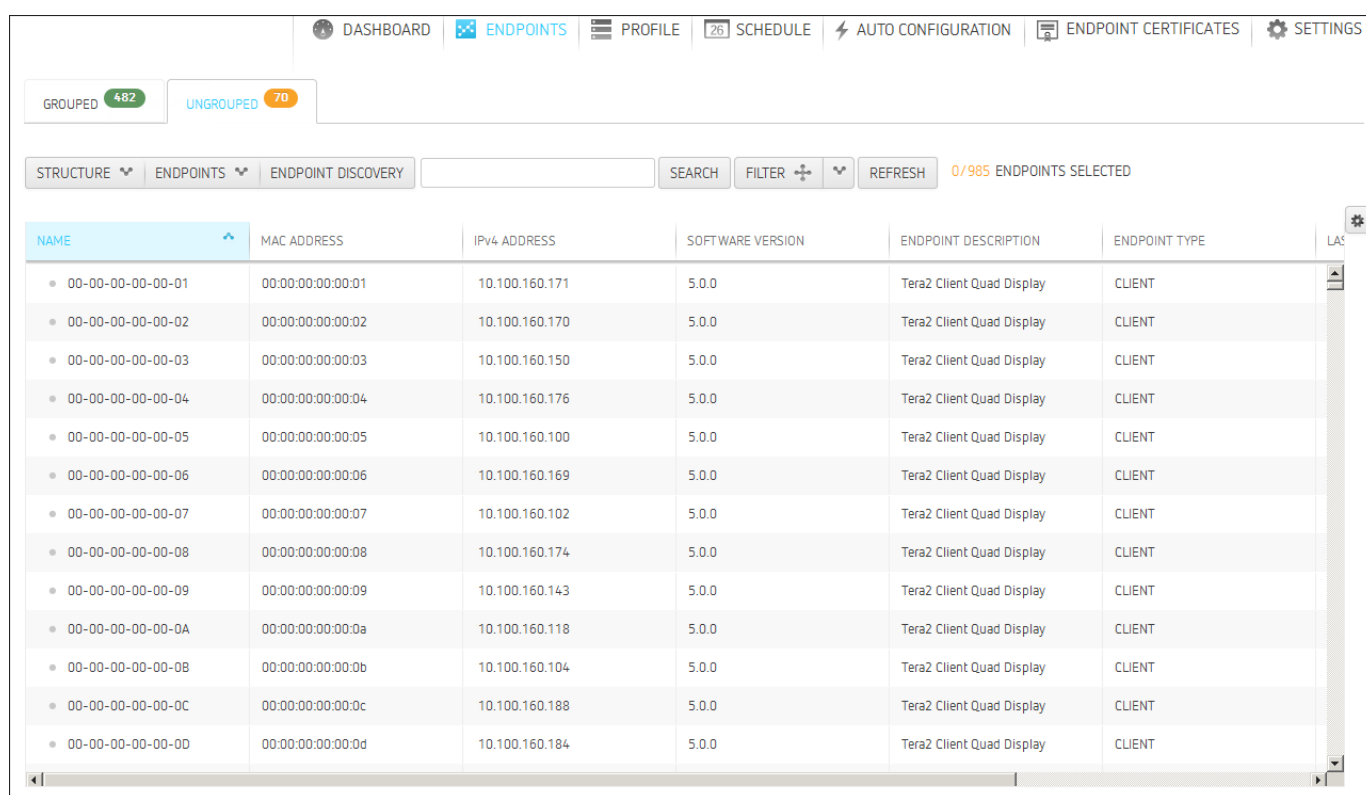
To view profile details:

1. From the *ENDPOINTS* page, select a group to which a profile is assigned.
2. Click **PROFILE** and then **DETAILS**.

Organizing Endpoints into Groups

The **ENDPOINTS** page enables you to organize managed endpoints into a hierarchy of parent groups and child groups. Each group can then be associated with a profile so that its endpoints can be updated with the same settings all at once.

When endpoints are first discovered, they appear in the **UNGROUPED** table if you have not created auto configuration rules to automatically group them as part of the discovery process. The following example shows a list of ungrouped endpoints.



The screenshot shows the PCoIP Management Console interface. At the top, there is a navigation bar with tabs for DASHBOARD, ENDPOINTS (selected), PROFILE, SCHEDULE (26), AUTO CONFIGURATION, ENDPOINT CERTIFICATES, and SETTINGS. Below the navigation bar, there are two tabs: GROUPED (482) and UNGROUPED (70). The UNGROUPED tab is active. Below the tabs, there is a search and filter section with buttons for STRUCTURE, ENDPOINTS, ENDPOINT DISCOVERY, SEARCH, FILTER, and REFRESH. A status bar indicates 0/985 ENDPOINTS SELECTED. The main content is a table with the following columns: NAME, MAC ADDRESS, IPV4 ADDRESS, SOFTWARE VERSION, ENDPOINT DESCRIPTION, and ENDPOINT TYPE. The table contains 11 rows of data, all of which are Tera2 Client Quad Display endpoints with CLIENT type.

NAME	MAC ADDRESS	IPV4 ADDRESS	SOFTWARE VERSION	ENDPOINT DESCRIPTION	ENDPOINT TYPE
00-00-00-00-01	00:00:00:00:01	10.100.160.171	5.0.0	Tera2 Client Quad Display	CLIENT
00-00-00-00-02	00:00:00:00:02	10.100.160.170	5.0.0	Tera2 Client Quad Display	CLIENT
00-00-00-00-03	00:00:00:00:03	10.100.160.150	5.0.0	Tera2 Client Quad Display	CLIENT
00-00-00-00-04	00:00:00:00:04	10.100.160.176	5.0.0	Tera2 Client Quad Display	CLIENT
00-00-00-00-05	00:00:00:00:05	10.100.160.100	5.0.0	Tera2 Client Quad Display	CLIENT
00-00-00-00-06	00:00:00:00:06	10.100.160.169	5.0.0	Tera2 Client Quad Display	CLIENT
00-00-00-00-07	00:00:00:00:07	10.100.160.102	5.0.0	Tera2 Client Quad Display	CLIENT
00-00-00-00-08	00:00:00:00:08	10.100.160.174	5.0.0	Tera2 Client Quad Display	CLIENT
00-00-00-00-09	00:00:00:00:09	10.100.160.143	5.0.0	Tera2 Client Quad Display	CLIENT
00-00-00-00-0A	00:00:00:00:0a	10.100.160.118	5.0.0	Tera2 Client Quad Display	CLIENT
00-00-00-00-0B	00:00:00:00:0b	10.100.160.104	5.0.0	Tera2 Client Quad Display	CLIENT
00-00-00-00-0C	00:00:00:00:0c	10.100.160.188	5.0.0	Tera2 Client Quad Display	CLIENT
00-00-00-00-0D	00:00:00:00:0d	10.100.160.184	5.0.0	Tera2 Client Quad Display	CLIENT

The ENDPOINTS page – UNGROUPED

After creating parent groups and child groups, you can create auto configuration rules to automatically move endpoints into a group when they are first discovered. Alternatively, you can manually move endpoints into groups.

After an endpoint is moved to a group, either manually or automatically, it then appears in the **GROUPED** table on the **ENDPOINTS** page. If you have created an auto naming rule to name endpoints when they are first discovered or when they are moved between ungrouped and grouped categories, this rule is also applied at this time.

The **GROUPED** and **UNGROUPED** tabs have a endpoint count indicator showing how many endpoints are in that state.

The following example shows a structure with endpoints in two different groups.

The screenshot shows the PCoIP Management Console interface. At the top, there are navigation tabs: DASHBOARD, ENDPOINTS (selected), PROFILE, SCHEDULE, AUTO CONFIGURATION, ENDPOINT CERTIFICATES, and SETTINGS. Below the navigation, there are two tabs: GROUPED (483) and UNGROUPED (70). The main area contains a table of endpoints with columns: NAME, IPV4 ADDRESS, ENDPOINT DESCRIPTION, SOFTWARE VERSION, PROFILE, MAC ADDRESS, and DEVICE STATUS. The table is filtered to show endpoints under two groups: Accounting and Engineering. Each group has a dropdown arrow to expand it. The Accounting group has 5 endpoints, and the Engineering group has 6 endpoints. All endpoints are listed as 'Out Of Session(online)'. The table also includes search, filter, and refresh buttons, and a selection indicator showing 0/1000 endpoints selected.

NAME	IPV4 ADDRESS	ENDPOINT DESCRIPTION	SOFTWARE VERSION	PROFILE	MAC ADDRESS	DEVICE STATUS
Accounting				Accounting		
• 00-00-00-00-01-9A	10.100.160.182	Tera2 Client Quad Display	5.0.0		00:00:00:00:01:9a	Out Of Session(online)
• 00-00-00-00-01-E5	10.100.160.109	Tera2 Client Quad Display	5.0.0		00:00:00:00:01:e5	Out Of Session(online)
• 00-00-00-00-02-80	10.100.160.178	Tera2 Client Quad Display	5.0.0		00:00:00:00:02:80	Out Of Session(online)
• 00-00-00-00-02-59	10.100.160.180	Tera2 Client Quad Display	5.0.0		00:00:00:00:02:59	Out Of Session(online)
• 00-00-00-00-03-AB	10.100.160.181	Tera2 Client Quad Display	5.0.0		00:00:00:00:03:ab	Out Of Session(online)
Engineering				Engineeri...		
• 00-00-00-00-02-7A	192.168.50.219	Tera2 Client Quad Display	5.0.0		00:00:00:00:02:7a	Out Of Session(online)
• 00-00-00-00-00-95	192.168.51.208	Tera2 Client Quad Display	5.0.0		00:00:00:00:00:95	Out Of Session(online)
• 00-00-00-00-02-EB	192.168.51.207	Tera2 Client Quad Display	5.0.0		00:00:00:00:02:eb	Out Of Session(online)
• 00-00-00-00-00-24	192.168.51.201	Tera2 Client Quad Display	5.0.0		00:00:00:00:00:24	Out Of Session(online)
• 00-00-00-00-02-91	192.168.51.205	Tera2 Client Quad Display	5.0.0		00:00:00:00:02:91	Out Of Session(online)
• 00-00-00-00-03-E7	192.168.51.204	Tera2 Client Quad Display	5.0.0		00:00:00:00:03:e7	Out Of Session(online)

The ENDPOINTS page – GROUPED

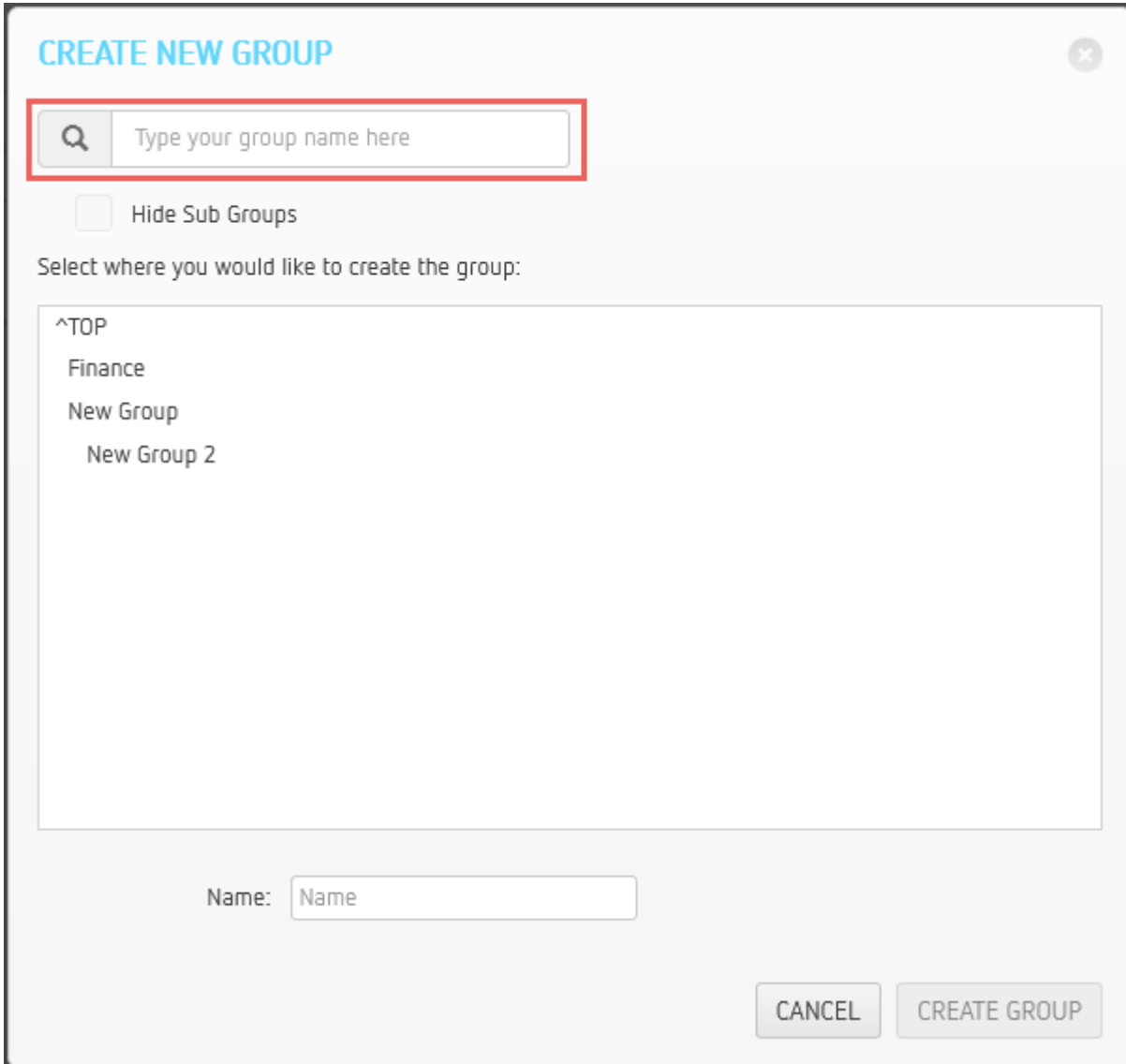
Creating Groups

To create groups:

1. From the PCoIP Management Console's top menu, click **ENDPOINTS**.
2. Click **STRUCTURE** and then **NEW GROUP**.
3. Select **^TOP** to create a group at the top level or select the parent group under which you want to create a child group.
4. Enter a unique name for the group (from within its group hierarchy) and click **CREATE GROUP**.

Cannot find an existing group

If you are unsure a group already exists in your environment, the search feature at the top of the CREATE NEW GROUP dialog will search for existing groups once text is entered in the search field.



CREATE NEW GROUP ✕

Hide Sub Groups

Select where you would like to create the group:

- ^TOP
- Finance
- New Group
- New Group 2

Name:

Moving Endpoints into Groups

You can move an endpoint either from its **ENDPOINT DETAILS** page or from the **ENDPOINTS** page.

To move endpoints into groups:

1. From the **ENDPOINTS** page, click either the **GROUPED** or **UNGROUPED** tab.

2. Select one or more endpoints in the table.

Use **Shift**+Click to select contiguous elements and **Ctrl**+Click to select non-contiguous elements.

3. Click **STRUCTURE** and then **MOVE**.

4. Select the desired parent group or child group, and then click **MOVE TO GROUP**.

If you have configured an endpoint naming convention that applies when you move endpoints to or from a group, the endpoints may also be renamed during this procedure.

Moving Groups

To move groups:

1. From the **ENDPOINTS** page, click the **GROUPED** tab.

2. Select a group in the table.

3. Click **STRUCTURE** and then **MOVE**.

4. Select the desired parent group or child group, and then click **MOVE TO GROUP**.

If you have configured an endpoint naming convention that applies when you move endpoints to or from a group, the endpoints may also be renamed during this procedure.

Renaming a Group

To rename a group:


1. From the **ENDPOINTS** page, click the **GROUPED** tab.

2. Select the group you want to rename.

3. Click **STRUCTURE** and then **RENAME**.

4. Enter a unique name (from within its group hierarchy) and click **RENAME GROUP**.

Removing a Group

 **Note: Child groups will be removed and any endpoint will become ungrouped**

If you remove a parent group that contains child groups or endpoints, the child groups will also be removed and any endpoints will become ungrouped.

To remove a group:


1. From the **ENDPOINTS** page, click the **GROUPED** tab.
2. Select the group you want to remove.
3. Click **STRUCTURE** and then **REMOVE GROUP**.
4. Enable the **I understand message** and click **REMOVE GROUP**.

Auto Configuring Endpoints (Enterprise)

The PCoIP Management Console Enterprise lets you create rules to apply profiles and automatically move endpoints into a specific group when they are first discovered. After discovery, you can find the endpoints in the [GROUPED table diagram](#) on the **ENDPOINTS** page. Profiles that are applied to a group used in auto configuration will be applied to all endpoints that are in the group, not just the newly discovered endpoints. If you are using PCoIP Management Console Free, you will be able to edit existing configurations.

Displaying Auto Configuration Rules

The **AUTO CONFIGURATION** page contains a table showing all the auto configuration rules that are currently configured. You can create a new rule from this page, or you can select a rule from the table to edit or delete it. The **ON/OFF** switch at the top of the page lets you globally enable or disable all rules at once.

Click the gear icon  to the right of the table to change the information you want to display in the table columns. Your customized settings are saved in your browser and will be used for any user who subsequently logs in from that browser.

Switching auto configuration rules on and off

The **AUTO CONFIGURATION** page has a global auto configuration **ON/OFF** switch that is located above the table. Auto configuration rules become active when this switch is set to **ON**. However, the rules are only applied to endpoints when the devices are first discovered. If the global auto configuration setting is switched on after discovery, your rules will have no effect. For this reason, it is important to set up your rules before enabling discovery of the endpoints to which the rules would apply.

teradici

PCoIP MANAGEMENT CONSOLE - ENTERPRISE

Welcome back admin
LOGOUT

DASHBOARD ENDPOINTS PROFILE SCHEDULE AUTO CONFIGURATION ENDPOINT CERTIFICATES SETTINGS

NEW RULE EDIT DELETE

AUTO CONFIGURATION

Endpoints can be automatically configured and assigned to groups once they are discovered based on the rules you specify below

ON

GROUP	RULE TYPE	IPV4 ADDRESS RANGES	GENERIC TAGS	REQUEST CERTIFICATE	MOVE TO GROUP ONLY	LAST UPDATED
-------	-----------	---------------------	--------------	---------------------	--------------------	--------------

AUTO CONFIGURATION page and switch button

Creating an Auto Configuration Rule

Help

Click the ? button beside each field for help with any of the settings.

The LAST UPDATED column displays the last time the Auto Configuration rule has been updated.

To create an auto configuration rule:

1. From the PCoIP Management Console's top menu, click **AUTO CONFIGURATION**.
2. Click **NEW RULE** and configure the rule as follows:

- **Rule Criteria:** Select the criteria your auto configuration rule is based on:

- **IP ADDRESS:** Click **ADD**, enter the IP address range of the endpoints you want to place in the group, and then click **OK**. The address range can encompass an entire class A network.

Example Name field displays endpoint name format

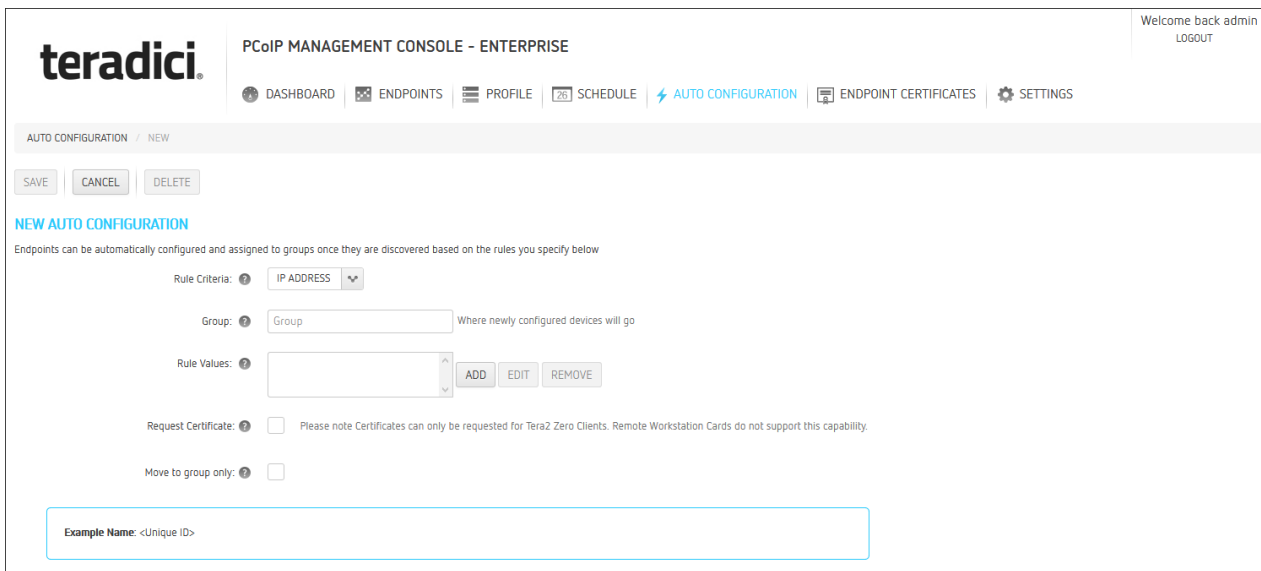
The Example Name field at the bottom of the page displays the endpoint name format based on your global naming convention. See [Creating a Global Endpoint Naming Convention](#).

- **PASSWORD:** Enter the endpoints password. Endpoints with matching passwords will be auto configured
- **GENERIC TAG:** Enter the endpoints Generic Tag. Endpoints with a matching Generic Tag label will be auto configured
- **Group:** Click in this field, select the desired pre-configured group, and then click **OK**.

Stop profile from being applied

Profiles are applied when auto configuration is on. Use this option to move endpoints into groups while not applying a profile to that group.

- **Rule Values:** Enter the specific values required by the *Rule Criteria*.
- **Request Certificate:** Select to automatically retrieve a Simple Certificate Enrollment Protocol (SCEP) digital certificate from a SCEP server.
- **Move to Group Only (Enterprise):** Groups the discovered endpoints and not apply a profile or firmware to them. This permits endpoints to be discovered at any time, and allows a profile application to be scheduled through the Management Console Schedule for a time that would be more convenient for a user.



The screenshot shows the Teradici PCoIP Management Console - Enterprise interface. The top navigation bar includes the Teradici logo, the title 'PCoIP MANAGEMENT CONSOLE - ENTERPRISE', and a 'Welcome back admin LOGOUT' message. The main navigation menu contains 'DASHBOARD', 'ENDPOINTS', 'PROFILE', 'SCHEDULE', 'AUTO CONFIGURATION' (highlighted), 'ENDPOINT CERTIFICATES', and 'SETTINGS'. The current page is 'AUTO CONFIGURATION / NEW'. Below the navigation are 'SAVE', 'CANCEL', and 'DELETE' buttons. The main content area is titled 'NEW AUTO CONFIGURATION' and contains the following fields and options:


- Rule Criteria:** A dropdown menu set to 'IP ADDRESS'.
- Group:** A text input field containing 'Group' with a note: 'Where newly configured devices will go'.
- Rule Values:** A text input field with 'ADD', 'EDIT', and 'REMOVE' buttons.
- Request Certificate:** A checkbox that is unchecked, with a note: 'Please note Certificates can only be requested for Tera2 Zero Clients. Remote Workstation Cards do not support this capability.'
- Move to group only:** A checkbox that is unchecked.

At the bottom, there is a text input field with the placeholder text 'Example Name: <Unique ID>'.

3. Click **SAVE**.

Creating overlapping or conflicting rules is not allowed

The PCoIP Management Console will prevent you from creating overlapping or conflicting rules. You will be required to resolve any problems before the rule can be created.

4. Click **AUTO CONFIGURATION** in the navigation link at the top to return to the main **AUTO CONFIGURATION** page.
5. If you want the rule to apply right away, make sure the global auto configuration setting is switched to **ON**. 

Viewing or Editing an Auto Configuration Rule

To view or edit an auto configuration rule:

1. Select the rule in the *AUTO CONFIGURATION* list.
2. Click **EDIT** to view or edit the rule.
3. Make desired changes.
4. Click **SAVE**.
5. Click **AUTO CONFIGURATION** in the navigation link at the top to return to the main page.

Deleting an Auto Configuration Rule

To delete an auto configuration rule:

1. Select the rule in the *AUTO CONFIGURATION* list.
2. Click **DELETE**.
3. Click **DELETE** again at the confirmation message.

Auto Naming Endpoints

The **ENDPOINT NAMING** page lets you construct a naming format for endpoints by selecting endpoint attributes to include in the name and entering a custom prefix and postfix to the name if desired. For example, you can create a name that begins with your prefix text, followed by the endpoint's PCoIP Management Console parent group or child group name, followed by the endpoint's MAC address or endpoint label, and ends with your postfix text.

The names created from these settings are visible from the **ENDPOINTS** and **ENDPOINT DETAILS** pages. They are only used with the PCoIP Management Console and are not available from the endpoint's AWI or OSD.

Each time you change a setting as you configure the naming convention, the **Example Name** field at the bottom of the page updates to show the format you have created. When you have finished constructing the name, you then choose when the name should be applied.

You can configure auto naming by clicking **SETTINGS** from the PCoIP Management Console's top menu and then clicking the **NAMING** menu in the left pane.

Creating a Global Endpoint Naming Convention

Note: Help with settings

Click the ? button beside each field for help with any of the settings.

To create a global endpoint naming convention:

1. From the PCoIP Management Console's top menu, click **SETTINGS**.
2. In the left pane, click **NAMING**.
3. Configure the endpoint name format as follows:
 - **Endpoint Name:** Select whether to incorporate the endpoint's current unique ID (that is, its MAC address) or its endpoint label (for example, pcoip-portal-) into the endpoint name.
 - **Prefix:** Enter any text you wish to prepend to the name.
 - **Group Naming:** Select whether to add the endpoint's group name and/or immediate child group name after the prefix.

- **Postfix:** Enter any text you wish to append to the name.

4. In the *Rename Endpoints when* field, select whether to apply the name when the endpoint is first discovered, or any time it is moved between groups or between a grouped and ungrouped category.

The screenshot shows the 'ENDPOINT NAMING' configuration page in the PCoIP Management Console. The page has a navigation bar at the top with links for DASHBOARD, ENDPOINTS, PROFILE, SCHEDULE, AUTO CONFIGURATION, ENDPOINT CERTIFICATES, and SETTINGS. A left sidebar contains menu items for AUTHENTICATION, NAMING (selected), SOFTWARE, SECURITY, DATABASE, LICENSE, REMOTE, and VERSION. The main content area is titled 'ENDPOINT NAMING' and includes a 'SAVE' button. Below the title, there is explanatory text: 'When new endpoints are added or updated they can be automatically renamed. These settings determine how automatic renaming is applied:'. The settings are as follows: 'Endpoint Name' is set to 'Use Endpoint Current Unique ID' (selected) with 'Use Device Label Name' as an alternative; 'Prefix' is set to 'Prefix' in a text input field; 'Group Naming' has 'Primary Group Name' and 'Deepest Sub-group Name' both unchecked; 'Postfix' is set to 'Postfix' in a text input field; and 'Rename Endpoints when' is set to 'first discovered' (selected) with 'moved between groups' as an alternative. At the bottom, an 'Example Name' field displays '<Unique ID>'.

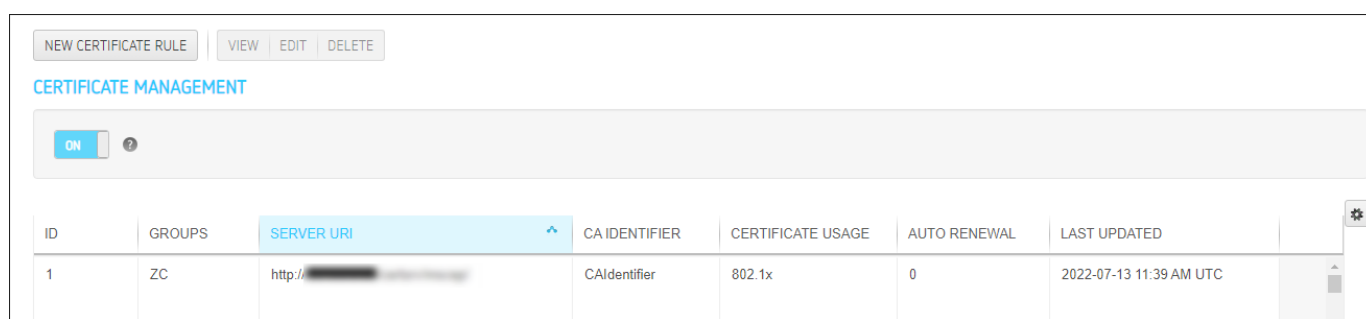
5. Click **SAVE**.

Requesting Endpoint Certificates Using SCEP (Enterprise)

Simple Certificate Enrollment Protocol (SCEP) lets you simplify the retrieval and installation of digital certificates by enabling devices to obtain certificates automatically from a SCEP server. Management Console supports SCEP requests for different certificates on client and host endpoints.

Administrators of Management Console Enterprise can reference SCEP issued certificate information from the dashboard and may now see certificate status of NOT APPLICABLE or NOT REQUESTED from the ENDPOINTS page when the certificate status column is displayed.

SCEP requested certificate information can be viewed from the Dashboard, ENDPOINTS, and ENDPOINT CERTIFICATES pages.



ID	GROUPS	SERVER URI	CA IDENTIFIER	CERTIFICATE USAGE	AUTO RENEWAL	LAST UPDATED
1	ZC	http://[redacted]	CAIdentifier	802.1x	0	2022-07-13 11:39 AM UTC

This topic covers creating, viewing, editing and deleting a certificate rule, and how to initiate a certificate request using SCEP.

⚠ Upgrading to firmware 21.07

For deployments using SCEP issued certificates, Management Console must be upgraded to version 21.07 or newer prior to upgrading firmware 21.07.

CONDITIONS FOR CERTIFICATE REQUESTS USING SCEP

The following conditions apply when performing a certificate request using SCEP:

- See [Obtaining Certificates Using SCEP](#) for complete information on SCEP behaviors.
- SCEP certificate renewal requests occur sequentially in 1 hour intervals when the renewal setting has been reached. The first request must successfully complete before renewal of the next certificate is initiated. If unsuccessful, the renewal request for the first certificate is attempted

again. Administrators should periodically review the validity period of the SCEP certificates to ensure that renewals were successful and the certificates do not expire.

- The PCoIP endpoint must have NTP properly configured.
- The renewal period must be less than the validity period of the certificate.
- A certificate usage can be used once in a rule per group
- A group can only be associated with one certificate rule
- Management Console will display information for one certificate on the **ENDPOINT DETAILS** page. You can review all certificates for an endpoint by reviewing the rules created on the **ENDPOINTS CERTIFICATE** page that apply to your endpoint's group.
- Remote Workstation Cards must be running firmware 21.07 or newer
- Zero Clients running firmware prior to 21.07:
 - Request 802.1x usage certificates only. Rules including Administrative Web Interface usage certificates will not initiate the AWI certificate request but will initiate an included 802.1X certificate request.
 - The Request Certificate button will not activate if the rule is only for AWI certificate usage and will display **NOT APPLICABLE** in the ENDPOINT page certificate status column.
- Endpoints running firmware 21.07 or newer:
 - Users can request all certificate usages available for that version of firmware
 - Initially the status will show **NOT REQUESTED** on the **ENDPOINTS** page
 - Users will have the information of only one certificate on the ENDPOINT DETAILS and ENDPOINTS pages after completion of the request even if multiple certificates are requested.

Certificate status for SCEP certificate request times

The certificate status will update after the SCEP requests complete which usually takes between 5 to 20 minutes.

SCEP Requested Certificate Usages

Certificate requests using SCEP are available for the following certificate uses:

- **802.1X**: Allows you to use SCEP to request a custom certificate to authenticate PCoIP endpoints in your 802.1x configuration.
- **Administrators Web Interface (AWI)**: Allows you to use SCEP to request a custom certificate to access the Administrative Web Interface (AWI).
- **Peer-to-peer Max Compatibility**: Allows you to use SCEP to automatically request a custom certificate that allows secure negotiation using any of the common cipher suites to offer flexibility for your network security requirements.
- **Peer-to-peer Suite B**: Used in environments requiring Suite B cryptography. Allows you to use SCEP to automatically request a custom certificate offering the greatest security for negotiating session connections with a PCoIP endpoint.
- **Syslog TCP/TLS**: Certificates used to ensure a secure connection to your Syslog server.

Select the **Syslog Connection Type** according to your security policies. If using Syslog TCP/TLS secure connections to your Syslog server, enable the **Syslog Enable Metadata** setting to tag every syslog entry with the PCoIP Device Name and Generic Tag. Add the client certificate for TCP with TLS syslog connections that require Mutual Authentication (Server and Client). See [Syslog TCP/TLS Authentication](#) in the Uploading Certificates topic of the Zero Client Administrators' Guide.

ENDPOINT CERTIFICATES / NEW

SAVE CANCEL DELETE

NEW CERTIFICATE RULE

Remote Workstation Cards SCEP requested certificates introduced in firmware 21.07.
Zero Clients using firmware prior to 21.07 only have BOZ.1x usage type and can request only one certificate

Groups:

Request-1

Usage Name:

Server URI:

Server Password:

CA Identifier:

Auto Renewal:

Tip: Organize endpoints into groups

Before you create an endpoint certificate, organize your endpoints into groups. See [Organizing Endpoints into Groups](#).

SCEP Feature Support Matrix

SCEP Issued Certificate Improvements	Management Console Version	Zero Client Firmware	Remote Workstation Card Firmware
802.1X certificate usage	All Versions	All Versions	21.07+
AWI Interface certificate usage	21.07+	21.07+	21.07+
Peer-to-peer Max Compatibility certificate usage	22.04+	22.01+	22.01+
Peer-to-peer Suite B certificate usage	22.04+	22.01+	22.01+
Automatic Renewal Period feature addition	22.04+	22.01+	22.01+
Syslog TCP/TLS certificate usage	22.07+	22.07+	22.07+

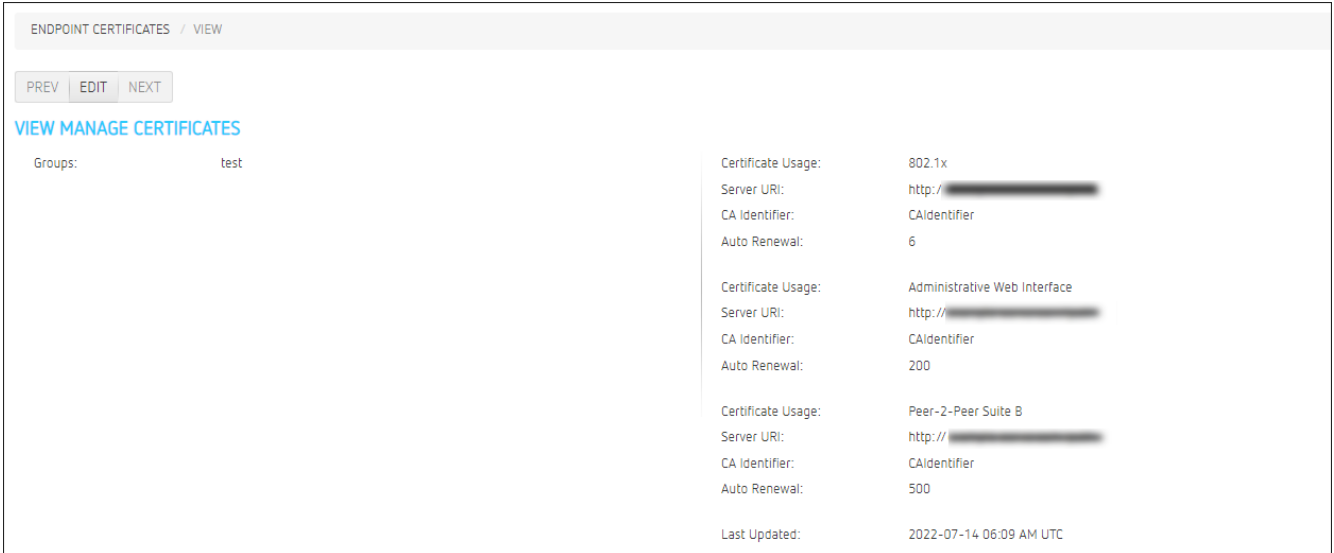
TO CREATE AN ENDPOINT CERTIFICATE RULE

1. Click **ENDPOINT CERTIFICATES** to display the *CERTIFICATE MANAGEMENT* window.
2. Click **NEW CERTIFICATE RULE**.
3. In the **Groups** field, click **ADD** to add a group that was set up on the **ENDPOINTS** page. If required, you can remove a group by highlighting it and clicking **REMOVE**.
4. From the **Request 1** tab, select the **Certificate Usage**.
5. In the **Server URI**, field, type the Uniform Resource Identifier (URI) of the SCEP server that is configured to issue certificates for the group.
6. In the **Server Password** field, type the password for the SCEP server.
7. In the **CA Identifier** field, type the certification authority issuer identifier if your SCEP server requires it (the CA Identifier is supported for devices running firmware 5.4 or later). A CA Identifier is any string that is understood by the SCEP server (for example, a domain name).
8. Enter the **Auto Renewal** period in days. The default value is 0 (disabled).
9. Click **+** icon beside the Request 1 tab to add a different certificate usage request per rule.
10. Click **SAVE**.

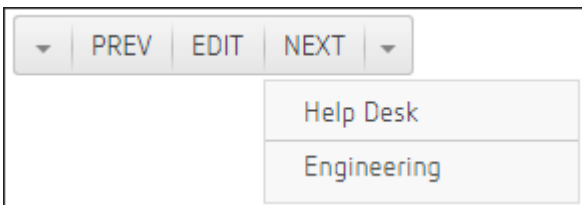
You can add an additional SCEP request by selecting the plus tab. When all the different certificate usages are configured, the plus tab no longer appears.

TO VIEW AN ENDPOINT CERTIFICATE RULE

1. Click **ENDPOINT CERTIFICATES** to display the **CERTIFICATE MANAGEMENT** window.
2. Highlight the certificate rule you would like to edit or review rule details and click the **View** button.



From the view rule window, you can use the **Next** or **Prev** (previous) buttons to browse your rules while looking at the details of each rule. In deployments with many rules, you can jump to a rule using one of the drop down menus that display the first group of the groups used in each rule.



TO EDIT AN ENDPOINT CERTIFICATE RULE

1. Click **ENDPOINT CERTIFICATES** to display the *CERTIFICATE MANAGEMENT* window.
2. Highlight the certificate rule you would like to edit.
3. Click **EDIT** to revise an endpoint certificate rule.
4. Click **Save** after you are finished making your edits.

TO DELETE AN ENDPOINT CERTIFICATE RULE

1. Click **ENDPOINT CERTIFICATES** to display the *CERTIFICATE MANAGEMENT* window.
2. Highlight a certificate rule that you want to delete.

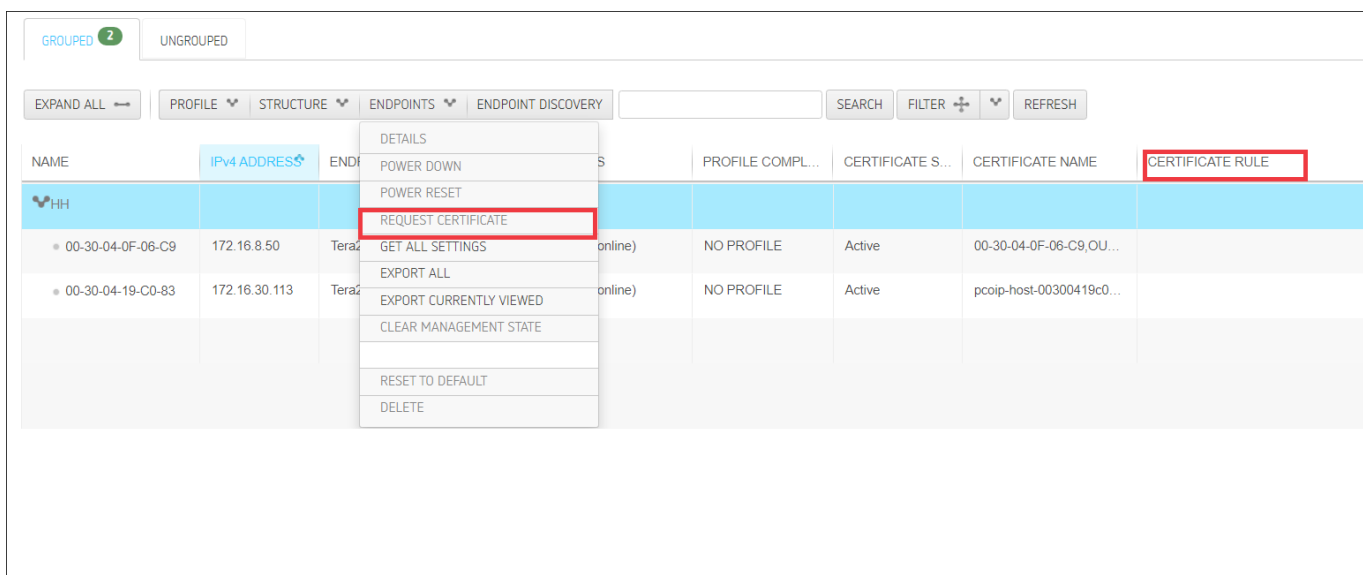
3. Click **DELETE**.
4. Confirm your deletion by clicking **DELETE** in the DELETE CERTIFICATE RULE dialog box.

Deleting SCEP certificate rules

You can also delete a SCEP certificate rule using the DELETE button while editing or creating a rule.

INITIATING A CERTIFICATE REQUEST

Prior to requesting a certificate, a certificate rule for your endpoint must exist. If your endpoint is not part of a group the rule is applied to, the request certificate button will be deactivated.



The screenshot displays the PCoIP Management Console interface. At the top, there are tabs for 'GROUPED' (with a '2' indicator) and 'UNGROUPED'. Below the tabs are navigation buttons: 'EXPAND ALL', 'PROFILE', 'STRUCTURE', 'ENDPOINTS', and 'ENDPOINT DISCOVERY'. A search bar and 'FILTER' and 'REFRESH' buttons are also present. The main area is a table with columns: 'NAME', 'IPv4 ADDRESS', 'ENDPOINT', 'PROFILE COMPL...', 'CERTIFICATE S...', 'CERTIFICATE NAME', and 'CERTIFICATE RULE'. A context menu is open over the first endpoint row, with options: 'DETAILS', 'POWER DOWN', 'POWER RESET', 'REQUEST CERTIFICATE' (highlighted in red), 'GET ALL SETTINGS', 'EXPORT ALL', 'EXPORT CURRENTLY VIEWED', 'CLEAR MANAGEMENT STATE', 'RESET TO DEFAULT', and 'DELETE'. The 'CERTIFICATE RULE' column header is also highlighted in red.

You can use Management Console to request certificates for endpoints in 4 ways.

• Using the **ENDPOINTS** page

- a. From the dashboard click **ENDPOINTS**.
- b. Highlight your endpoint or group of endpoints, and click **ENDPOINTS > REQUEST CERTIFICATES**.

• Using the **Endpoints details** page

- a. From the dashboard click **ENDPOINTS**.
- b. Highlight your endpoint and click **ENDPOINTS > DETAILS**.

c. Click **ENDPOINTS > REQUEST CERTIFICATES**.

- **Create a schedule**

a. From the dashboard click **SCHEDULE**.

b. Select **NEW SCHEDULE**.

c. Select the **Request Certificate** type and all other schedule requirements for your schedule.

d. Click **Save**. The request will initiate at the set scheduled time.

See [Managing Schedules](#) for further details creating schedules.

- **Create an auto configuration rule**

a. From the dashboard click **AUTO CONFIGURATION**.

b. Click **NEW RULE**.

c. Ensure the **Request Certificate** checkbox is selected and configure all other values required for your auto configuration.

d. Click **Save**.

See [Auto Configuring Endpoints](#) for further details creating auto configuration rules.

Managing Schedules (Enterprise)

The PCoIP Management Console Enterprise lets you create schedules that are configured to run either once, at a certain date and time, or repeatedly, over a specified time frame and at a specified frequency. You can create schedules to apply a profile to one or more groups of endpoints, to power down one or more groups of endpoints, or to perform a power reset on one or more groups of endpoints.

Displaying Schedule Information


All configured schedules are displayed on the PCoIP Management Console's **SCHEDULES** page. You can view information about schedules that have previously run by clicking the **HISTORY** tab. Any configured schedules that have yet to run are also displayed on the PCoIP Management Console dashboard in its **UPCOMING SCHEDULES** area.

SCHEDULES Page

The schedules page contains a table showing all the schedules that are currently configured for the PCoIP Management Console. You can create a new schedule from this page, or you can select a schedule from the table to view, edit, or delete.

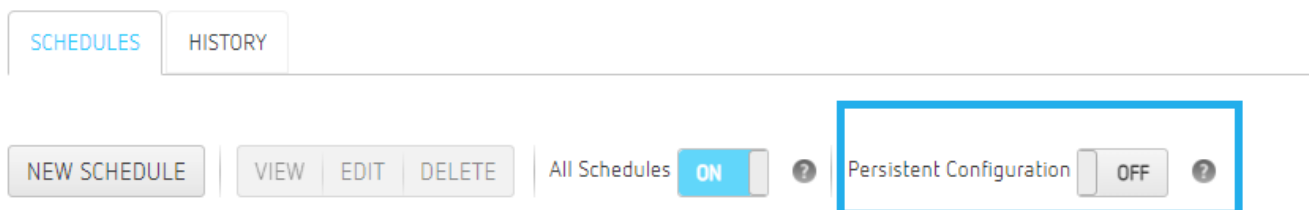
ENABLING AND DISABLING SCHEDULE TYPES

Schedule types can be enabled or disabled via the switches at the top of this page:

- The **All Schedules** switch  enables or disables *all* schedules at once, including persistent configuration schedules.


- **On:** All enabled schedules will run.
- **Off:** Disables and stops *all* schedules, including any Persistent Configuration schedules. Schedules that are currently running will be terminated.

- The **Persistent Configuration** switch enables or disables all *persistent configuration schedules*:



- **On:** All enabled *persistent configuration* schedules will run.
- **Off:** Disables and stops all *persistent configuration schedules*. Persistent Configuration schedules that are currently running will be terminated.

CUSTOMIZING THE SCHEDULES PAGE

Click the gear icon  to the right of the table to change the information you want to display in the table columns. Your customized settings are saved in your browser and will be used for any user who subsequently logs in from that browser.

 A screenshot of the 'SCHEDULES' page showing a table with the following columns: NAME, DESCRIPTION, ACTION TYPE, START, END, and FREQUENCY. The table contains one row of data:

NAME	DESCRIPTION	ACTION TYPE	START	END	FREQUENCY
Accounting - Apply	Updating profile for Accounting ...	Profile Application	2019-04-24 04:30 PM UTC		

SCHEDULES Page

PERSISTENT CONFIGURATION SCHEDULE TYPES

Persistent Configuration Schedules enforce a defined configuration profile on managed endpoints. Each time a persistent configuration schedule runs, its endpoints will be checked for compliance; if an endpoint's profile has been modified and does not match the expected configuration, the Management Console will re-apply the configured profile.



- Persistent schedule types can be switched on and off as a group; for more information, see [Enabling and Disabling Schedule Types](#). By default, persistent schedules are *disabled* and must be turned on to work.
- The ability to manage persistent schedules is controlled by a new permission setting; see [Available Role Permissions](#).


- To create a new Persistent Configuration schedule, open the schedule page and click **New**, then select the **Persistent Configuration** schedule type.


SCHEDULE / NEW


SAVE | CANCEL | DELETE

NEW SCHEDULE

Type:  Persistent Configuration 

Name: 


Description: 

Enabled:  OFF


- Apply Profile
- Power Down
- Power Reset
- Request Certificate
- Persistent Configuration**

HISTORY Page

The **HISTORY** page provides a list of schedules that have previously run, along with pertinent information about each one. All scheduled and manual activities will appear in the schedule history (for example, profile applications, power downs and resets).

 **Note: Unscheduled events do not appear in schedule history**

Events that are not scheduled, for example, profile updates driven by auto-configuration, do not appear in the schedule history.

Click the gear icon  to the right of the table to change the information you want to display in the table columns. Your customized settings are saved in your browser and will be used for any user who subsequently logs in from that browser.

SCHEDULES										
HISTORY										
NAME	GROUP	START	LAST UPDATED	RECURRING	ACTION	FREQUENCY	PENDING	IN PROGRESS	FAILED	COMPLETED
Philip-sched1	T2LC	2015-08-04 04:19 PM UTC					0	0	0	0
BJ Tera2 Apply	Tera2	2015-08-04 04:20 PM UTC	2015-08-04 04:20 P...	true	Profile Appli...	DAILY	0	0	0	1
Philip-sched1	T2LC, T2Quad	2015-08-04 04:25 PM UTC					0	0	0	0
Philip-sched1	T2LC, T2Quad	2015-08-04 04:29 PM UTC					0	0	0	0
Philip-sched1	T2LC, T2Quad	2015-08-04 04:33 PM UTC					0	0	0	0
Philip-sched1	T2LC, T2Quad	2015-08-04 04:35 PM UTC					0	0	0	0
Philip-sched1	T2LC, T2Quad	2015-08-04 04:38 PM UTC					0	0	0	0

HISTORY Page

Creating a Schedule

Note: Help with settings

Click the ? button beside each field for help with any of the settings.

To create a schedule:

1. From the PCoIP Management Console's top menu, click **SCHEDULE**.
2. Click **NEW SCHEDULE**.
3. Configure the settings as follows:
 - **Type:** Select the type of schedule.

⚠ Caution: Using the Skip reboot when applying profile on endpoints check box

This option allows you to push the profile but skip rebooting the endpoint. However, for new firmware to take affect, or for some settings to be applied, your endpoint must be rebooted.

- **Name:** Enter a unique name for the schedule.
- **Description:** Enter a description for the schedule.
- **Enabled:** Toggle the status to **ON**.
- **Groups:** Click **ADD**, select one or more groups, and then click **ADD** again. The schedule will operate on all the endpoints in any group you select. Use **Shift**+Click to select contiguous elements and **Ctrl**+Click to select non-contiguous elements.
- **Scheduled Time Zone:** Select the time zone for the start and end times when you want the schedule to run.
For ease of management, set the time zone to the same time zone where the endpoint(s) are located. The schedules table will show the schedule in the timezone that was selected and in the Management Console users timezone.
- **Start Time:** Click the time zone widget and select the desired date, then click the clock widget below the calendar and select the desired time.
- **Recurrence:** Select whether the schedule will run once or if it will recur over a period of time. If it is recurring, you must also select end date and time and frequency information.

SCHEDULE / NEW

SAVE CANCEL DELETE

NEW SCHEDULE

Type: Skip reboot when applying profile on endpoints

Name:

Description:

Enabled: OFF

Groups:

Schedule Time Zone:

Start Time:

Recurrence: Run Once
 Recurring

End Time:

Frequency: Daily
 Weekly

Recurring: Monday Tuesday Wednesday
 Thursday Friday Saturday
 Sunday

4. Click **SAVE**.

5. Click **SCHEDULE** in the navigation link at the top to return to the main page.

Viewing Schedule Details

To view schedule details:

1. From the table on the *SCHEDULES* page, select the schedule you wish to view.
2. Click **VIEW**.
3. If desired, you choose to view the previous or next schedule in the list, or you can click **EDIT** to edit the schedule.
4. Click **SCHEDULE** in the navigation link at the top to return to the main page.

Editing a Schedule

To edit a schedule:

1. From the table on the *SCHEDULES* page, select the schedule you wish to edit.
2. Click **EDIT**.
3. Change the schedule's settings as desired.
4. Click **SAVE**.
5. Click **SCHEDULE** in the navigation link at the top to return to the main page.

Deleting a Schedule

To delete a schedule:

1. From the table on the *SCHEDULES* page, select the schedule you wish to delete.
2. Click **DELETE**.
3. At the message prompt, click **DELETE**.

Hidden Endpoint Settings

Hidden OSD Menus and Settings

The PCoIP Zero Client can be further secured by hiding certain OSD menu options and by enabling certain options via the Management Console. These configurations can not be done from the PCoIP Zero Client OSD or AWI. An administrator can choose to hide OSD menu items, or activate features like Local Administrative Password.

The profile settings that hide menus are found under the profile SECURITY section. Select and enable one or all of the following options.

Hidden OSD Menu Entries

- Options/Configuration
- Options/Diagnostics
- Options/Information
- Options/User Settings
- Options/Password
- Hide the Options menu
- Options
- All Menus

Hidden PCoIP Zero Client OSD User Setting Tab Entries:

- Options > User Settings > Certificate
- Options > User Settings > Mouse
- Options > User Settings > Keyboard
- Options > User Settings > Image
- Options > User Settings > Display Topology
- Options > User Settings > Touch Screen
- Options > User Settings > Tablet
- Options > User Settings > Region
- Options > User Settings > User Interface

The screenshot displays two sections of hidden settings in the PCoIP Management Console. Each section has a radio button to its left, with the second one selected. The first section, 'Hidden OSD Menu Entries', lists seven options to hide from the OSD menu, all currently set to 'Enable'. The second section, 'Hidden OSD User Setting tab Entries', lists nine options to hide from the user settings tab, all also currently set to 'Enable'. Each option is followed by a dropdown menu showing 'Enable' and a downward arrow.

Setting Name	Current Value
Hide Options->Configuration:	Enable
Hide Options->Diagnostics:	Enable
Hide Options->Information:	Enable
Hide Options->User Settings:	Enable
Hide Options->Password:	Enable
Hide the Options menu:	Enable
Hide all Menus:	Enable
Hide User Settings-> Certificate:	Enable
Hide User Settings-> Mouse:	Enable
Hide User Settings-> Keyboard:	Enable
Hide User Settings-> Image:	Enable
Hide User Settings-> Display Topology:	Enable
Hide User Settings-> Touch Screen:	Enable
Hide User Settings-> Tablet:	Enable
Hide User Settings-> Region:	Enable
Hide User Settings-> User Interface(UI):	Enable

These are other profile settings that are not found on your PCoIP Zero Client or Remote Workstation Card and sometimes not available by default:

Enable Password Protection for OSD and AWI (occasionally not available as OEM default)

SECURITY

Set In Profile

<input type="checkbox"/>	Local Administrative Password: ?	Keep Device Setting
<input type="checkbox"/>	Force Password Change on Next Login: ?	Keep Device Setting
<input checked="" type="checkbox"/>	Enable Password Protection for OSD and AWI ?	Enable ▾
<input type="checkbox"/>	Password Protect User Settings for OSD ?	Keep Device Setting
<input type="checkbox"/>	Administrative Web Interface ?	Keep Device Setting
<input type="checkbox"/>	Hotkey Parameter Reset: ?	Keep Device Setting
<input type="checkbox"/>	Hide Parameter Reset Hotkey Sequence: ?	Keep Device Setting
<input type="checkbox"/>	802.1X Security: ?	Keep Device Setting
<input type="checkbox"/>	802.1X Authentication Identity: ?	Keep Device Setting
<input type="checkbox"/>	802.1X Legacy Support ?	Keep Device Setting
<input type="checkbox"/>	Management Console Interface ?	Keep Device Setting
<input type="checkbox"/>	Hidden OSD Menu Entries ?	Keep Device Setting
<input type="checkbox"/>	Hidden OSD User Setting tab Entries ?	Keep Device Setting

Session Disconnect Hotkey (CTRL + ALT + F12) (not available when Session Connection Type is Auto Detect in AWI/OSD)

SESSION Basic Advanced

Session Type

Set In Profile

Session Connection Type: ? Auto-Detect

Server URI: ? Not Set (eg. https://example.com or https://192.168.1.1:80)

Session Type (Advanced)

Set In Profile

Connection Server Cache Mode: ? Keep Device Setting

Session Lost Timeout: ? Keep Device Setting

Peer Loss Overlay: ? Keep Device Setting

Preparing Desktop Overlay: ? Keep Device Setting

Session Disconnect Hotkey: ? Enable (CTRL + ALT + F12)

Certificate Check Mode: ? Disable

PCoIP Utility Bar Mode: ? Keep Device Setting

Session Negotiation Cipher: ? Keep Device Setting

DSCP: ? Keep Device Setting

Transport Congestion Notification: ? Keep Device Setting

Disconnect Message Filter: ? Keep Device Setting

SNMP Trap Settings

These settings allow you to enable traps and enter the address of the network management system to send traps to. This setting will also require the authentication fields set on the endpoint. See the [PCoIP Zero Client Administrators' Guide SNMP Overview](#) for further information on SNMP authentication.

NETWORK Basic Advanced

Set In Profile

IPv4 ⓘ: ⓘ Keep Device Setting

IPv6 ⓘ: ⓘ Keep Device Setting

Maximum MTU Size ⓘ: ⓘ Keep Device Setting

SNMP ⓘ: ⓘ Enable ▼

Trap NMS Address: ⓘ Not Set

SNMP Cold Start Trap: ⓘ Enable ▼

SNMP V3 Traps: ⓘ Enable ▼

New SNMPv3 Auth Password ⓘ: ⓘ Not Set ⓘ ⓘ

New SNMPv3 Priv Password ⓘ: ⓘ Not Set ⓘ ⓘ

Keyboard Scan Code Filters

This setting allows you to create rules that prevent the PCoIP endpoint user from using certain keys or key combinations on their keyboard. Each filter consists of the following options.


- **Scan Codes:** Each key that is pressed produces a scan code that represents the key stroke in the form of hexadecimal value with a value range between 04 to FF.
- **Keyboard Layout:** You can select the keyboard layout associated with the supported languages available for keyboards connected to PCoIP Zero Clients
- **Lock State:** Represents the state of the NUM Lock, Caps Lock, Scroll Lock, and KANA Lock keys. States available are Any/All, Unlocked and Locked.
- **Modifier State:** Represents the state of the left and right CTRL, SHIFT, ALT, and GUI (i.e. Windows) keys. The available states are Any/All, Pressed and Depressed. Each key can be further identified by either the left, right or both. For example, LCTRL represents the left CTRL key, while RCTRL represents the right CTRL key and if your rule includes both left and right CTRL keys, you would use BCTRL.

Keyboard property values will be displayed in text on the profile page, and in hexadecimal on the endpoint details page.

Keyboard

Set In Profile



Keyboard Scan Code Filter: 

Scan Codes

(Hexadecimal range between 4 and FF)

Keyboard Layout

Lock State

- Any/All
- Lock options
 - NUM LOCK Any/All Locked Unlocked
 - CAP LOCK Any/All Locked Unlocked
 - SCROLL LOCK Any/All Locked Unlocked
 - KANA LOCK Any/All Locked Unlocked

Modifier State

- Any/All
- Modifier options
 - CTRL
 - Any/All
 - LCTRL
 - RCTRL
 - BCTRL
 - SHIFT
 - Any/All
 - LSHIFT
 - RSHIFT
 - BSHIFT
 - ALT
 - Any/All
 - LALT
 - RALT
 - BALT
 - GUI
 - Any/All
 - LGUI
 - RGUI
 - BGUI

Examples of using Keyboard Scan Code Filters with **PrtScn**

To block a screenshot of the whole screen using **PrtScn** while allowing a screenshot of the **Active Window** using **Alt + PrtScn**.

- Scan Code: 46
- Lock State: Any/ALL
- Modifier Option: ALT: BALT - Depressed

Keyboard

Set In Profile

Keyboard Scan Code Filter: ?

Scan Codes

(Hexadecimal range between 4 and FF)

Keyboard Layout



Lock State

- Any/All
- Lock options

Modifier State

- Any/All
- Modifier options

CTRL

- Any/All
- LCTRL
- RCTRL
- BCTRL

SHIFT

- Any/All
- LSHIFT
- RSHIFT
- BSHIFT

ALT

- Any/All
 - LALT
 - RALT
 - BALT
- Any/All Pressed Depressed

GUI

- Any/All
- LGUI
- RGUI
- BGUI

Keyboard

Set In Profile

Keyboard Scan Code Filter: ? Scan Code Value: 46
Keyboard Layout: Any Keyboard supported
Lock State: Any/All
Modifier State: ALT | BALT | Depressed

REMOVE

ADD NEW

Disable for all cases.

This means the filter will filter out any messages whenever is pressed, regardless if other keys are pressed.

- Scan Code: 46
- Lock State: Any/All
- Modifier Option: Any/All

Disable only when is in the off state.

This means the filter filters out any messages whenever is pressed and is depressed (not locked).

- Scan Code: 46
- Lock State: NUM LOCK - Depressed
- Modifier Option: Any/All

Disable + + only.

This means the filter filters out any messages whenever is pressed in conjunction with either the left or right and keys.

- Scan Code: 46
- Lock State: Any/All
- Modifier Option: BCTRL - Pressed and BALT - Pressed

Disable **ctrl + PrtScn** while allowing the use of **Ctrl + Alt + PrtScn** and **Ctrl + Gui + PrtScn**.

- Scan Code: 46
- Lock State: Any/All
- Modifier Option: BCTRL - Pressed and BALT - Depressed and BGUI - Depressed

Entering AWS Registration Codes via Broker Address Cache List

If you have an allotment of AWS WorkSpaces that are available for a Zero Client user to use, you can add up to 50 of them to a Zero Client running firmware 21.10.0 or newer via a Management Console profile. These added Workspaces will not be editable via the Zero Client OSD or AWI and will be displayed as a list from the OSD Connect drop-down menu when the Zero Client Connection Server Cache Mode is set to **Read Only**.

To apply a bulk additions of Amazon WorkSpaces from Management Console you must enter the Amazon WorkSpace Registration Codes via a profile's **Session > Broker Address Cache List** setting. This can be done individually or in bulk using a comma separated (CSV) file.

Broker Cache List

- Pushing a profile with Broker Address Cache entries will overwrite the current Zero Client Broker Address Cache list.
- Amazon Workspaces Connection type will allow you to bulk upload up to 50 Registration Codes to the Broker Server cache list from a CSV file.
- Autodetect, PCoIP Connection Manager and View Connection Server sessions have separate server caches that do not have a bulk loading option and have a upper limit of 25 entries.

The CSV file must meet the following requirements to upload successfully:

- must not be empty
- must be a CSV file format
- must not have a header row
- the first column must contain the WorkSpaces Registration Code
- must not have an empty first column entry
- must not have more than 50 entries
 - If there are existing cached entries, the number of csv entries plus the existing cached entries must not exceed 50
- must not contain duplicate entries
- must not contain commas

If the file only contains entries in the first column, then the column entries will be used as both **AWS WorkSpaces Registration Code** and **AWS WorkSpaces Registration Name**.

- SOFTWARE
- NETWORK
- DISCOVERY
- MANAGEMENT
- SECURITY
- SESSION**
- LOGGING
- POWER
- PERIPHERAL
- LANGUAGE
- OTHER

Session Type

Set In Profile

Session Connection Type: ? Amazon WorkSpaces ▼

AWS WorkSpaces Registration Code: ?

AWS WorkSpaces Registration Name: ?

Session Type (Advanced)

Set In Profile

Pool Name to Select: ? Keep Device Setting

Auto Connect: ? Keep Device Setting

Auto Launch If Only One Pool: ? Keep Device Setting

Session Lost Timeout: ? Keep Device Setting

Peer Loss Overlay: ? Keep Device Setting

Preparing Desktop Overlay: ? Keep Device Setting

Session Disconnect Hotkey: ? Keep Device Setting

Certificate Check Mode: ? Keep Device Setting

PCoIP Utility Bar Mode: ? Keep Device Setting

Session Negotiation Cipher: ? Keep Device Setting

DSCP: ? Keep Device Setting

Transport Congestion Notification: ? Keep Device Setting

Disconnect Message Filter: ? Keep Device Setting

Broker Address Cache

Set In Profile

Broker Address Cache List: ?

To add an Amazon WorkSpace for selection on a Zero Client perform the following steps.

1. Enter Amazon WorkSpaces Registration Codes to a CSV file with the Registration Code in the first column and the Registration Name in the second column.
2. Save the file to a location that can be access by the Management Console.
3. Navigate to an existing or new profile SESSION section and select the **Advanced** radio button.
4. Set the Session Connection Type to **Amazon WorkSpaces**.

Setting a dedicated Amazon WorkSpaces

An **AWS WorkSpaces Registration Code** and **AWS WorkSpaces Registration Name** can be entered if you have a dedicated Workspace.

5. Browse down to the *Broker Address Cache List* setting and click its **Set In Profile** button.
6. Use the appropriate button to add a new entry.
 - To bulk load up to 50 entries, use the **UPLOAD** button and add your saved CSV file.
 - To add entries individually, use the **ADD NEW** or **ADD** button for each entry.
7. Save the profile.
8. Apply the profile to the Zero Client group.


To remove Amazon WorkSpaces broker cache entries perform the following steps.

1. Edit an existing profile and browse to the **SESSION > Broker Address Cache List** section and use the **REMOVE** button to remove individual entries or use the **REMOVE ALL** button to remove all the profile entries.
2. Save the profile.
3. Apply the profile to the Zero Client group.

Broker Address Cache

Set In Profile



Broker Address Cache List: 

REMOVE

REMOVE

REMOVE

REMOVE

REMOVE

REMOVE

REMOVE

AWS Registration Code:

AWS Registration Name:

ADD

UPLOAD

CANCEL

REMOVE ALL

Enabling Analog Audio Input

Analog Audio can be enabled from the Management Console by configuring the **Enable Analog Audio Input** property in the **CLIENT DUAL** and **CLIENT QUAD** profiles. This property controls the analog audio input when connecting to a virtual machine.

Enable Analog Audio Input depends on the **Enable Audio** property. When **Enable Audio** is enabled, **Enable Analog Audio Input** can be set to "Enabled" or "Disabled".

To enable analog audio input:

1. Do one of the following:
 - Create a new profile by clicking **PROFILE > NEW PROFILE**.
 - Edit an existing profile by selecting a profile, and then clicking **EDIT**.
2. Click **Session**.
3. Ensure that **Enable Audio** is enabled. If **Enable Audio** is disabled or not set and attempts are made to enable or disable **Enable Analog Audio Input**, profile creation fails with the following message: *To enable or disable the Enable Analog Audio Input, ensure that the Enable Audio is enabled.*
4. In the **AUDIO INPUT** area, set **Enable Analog Audio Input** to "Enabled" or "Disabled".

Audio Input

Set In Profile

Enable Analog Audio Input: ? Enable Disable

Audio Device Type: ? Setting

Preferred USB Vendor ID: ? Keep Device Setting

If the **Enable Analog Audio Input** property is enabled or Not Set, and attempts are made to disable **Enable Audio**, profile creation fails with the following message: *To disable the Enable Audio, ensure that the Enable Analog Audio Input is disabled.*

5. Save your changes.

The **Enable Analog Audio Input** property can be viewed in the endpoint details page.

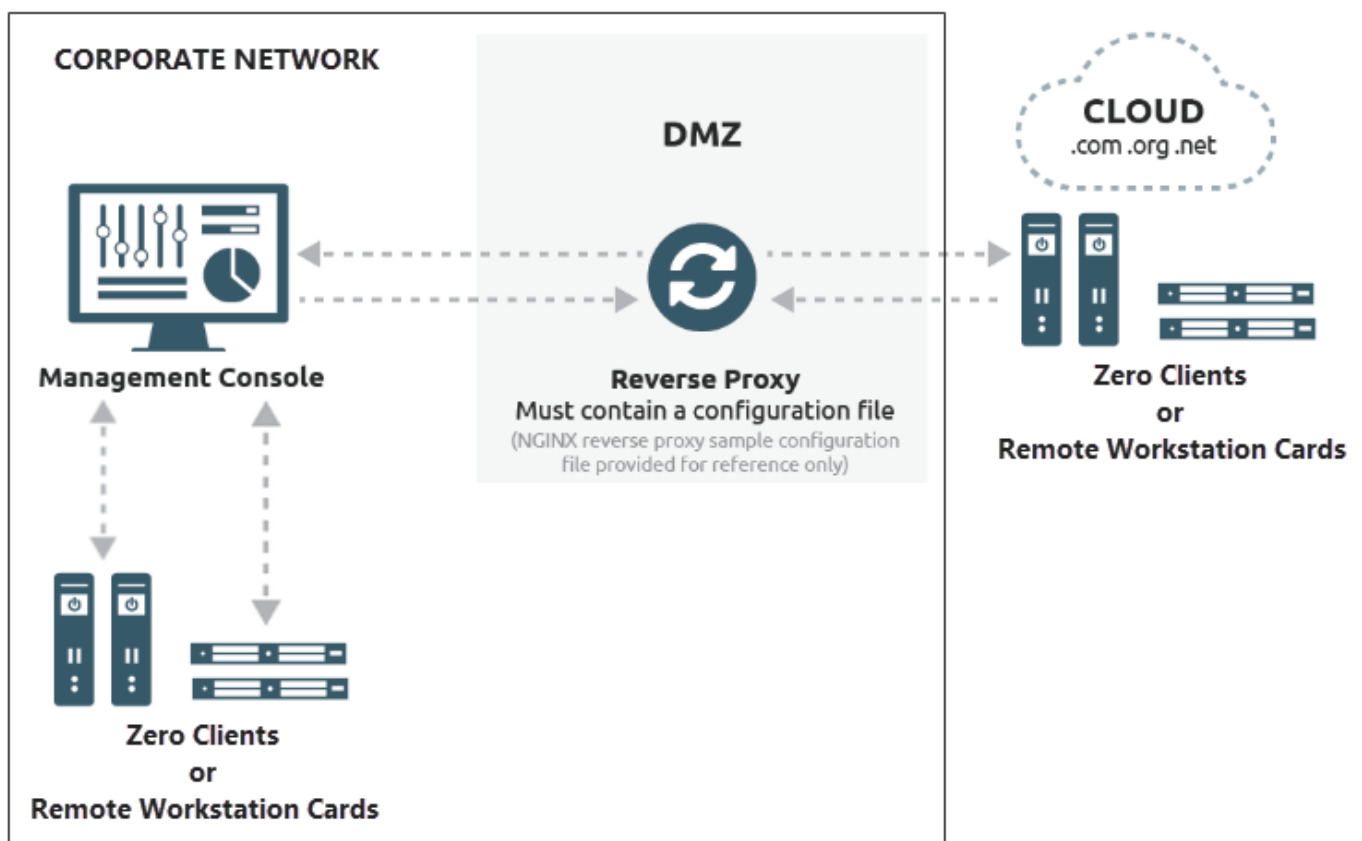
 **Note: Applying Profiles Created in Versions Earlier than 23.12.2**

If a profile is created in version earlier than 23.12.2 for Zero Clients running firmware 23.12.x and with **Enable Audio** disabled, while applying this profile in version 23.12.2, ensure that **Enable Analog Audio Input** is disabled.

Remote Endpoint Management (Enterprise)

Remote Endpoint Management (Enterprise) Overview

Remote endpoint management allows PCoIP administrators to maintain central management of endpoints when they are no longer on-premises. Remote management is available with the Enterprise version of Management Console therefore it must be licensed with a trial or enterprise license. See [Managing Licenses Online](#) for more information on licensing. Administrators will also need to deploy a reverse proxy and ensure the network connection between the PCoIP Management Console and the remote endpoint is using IPv4 and has a latency of approximately 100ms or less.



Reverse Proxy Overview

PCoIP Management Console determines if an endpoint is behind a reverse proxy by inspecting the websocket upgrade header for the presence of X-Forwarded-For, X-Real-IP or Forwarded information.

An endpoint is treated as a remote endpoint when it is:

- explicitly connecting to the external interface of the PCoIP Management Console

- determined to be behind a reverse proxy
- behind a NAT and has a different internal IP address from its external IP address.

To complete a remote management deployment, requires the configuration of the management console, remote proxy, endpoint and if desired an auto-provisioning DNS SRV record which is recommended.

Each configuration can be found in the following topics:

[Configuring PCoIP Management Console Remote Management](#)

[Reverse Proxy Configuration](#)

[Configuring DNS for Reverse Proxy](#)

[Connecting to a Remote Endpoint](#)

Reverse Proxy Configuration

For remote administration of PCoIP endpoints to work, the reverse proxy must be accessible by the remote devices and by the PCoIP Management Console. Typically a reverse proxy will be installed in the DMZ of the network.

For remote administration of PCoIP endpoints, the reverse proxy must meet the following requirements.

- It must be able to proxy the WebSocket protocol. The WebSocket protocol is used for communication between the endpoint and the Management Console. Encrypted websocket connections have a **wss://** preceding the FQDN.
- It must be configured with a publicly accessible address. This same address is entered in the PCoIP Management Console External Address field on the *REMOTE CONFIGURATION* page, in **SETTINGS > REMOTE**.
- It must have communication port TCP 5172 open in both directions.
- It must have a certificate with its private key added to its configuration. The reverse proxy must have a certificate with its private key added to its configuration. Use the SHA256 fingerprint from the reverse proxy certificate in the PCoIP Management Console **External Certificate Fingerprint** field on the *REMOTE CONFIGURATION* page, in **SETTINGS > REMOTE**.

HP has provided a [sample configuration using nginx for a reverse proxy](#), and is provided as-is, with no warranty. This sample configuration resides on a nginx proxy server.

Configuring PCoIP Management Console Remote Management

Remote Endpoint Management works by requiring a reverse proxy in the DMZ of the network and is configured by accessing the *REMOTE CONFIGURATION* page located by browsing PCoIP Management Console **SETTINGS > REMOTE**. Here you will find four configurable settings.

- **Internal Address:** Here you enter the internally published FQDN or IP address of the PCoIP Management Console. This is how "local" devices access the PCoIP Management Console.
- **External Address:** This address will lead to the reverse proxy. In this field you will enter the externally published FQDN or IP address of the reverse proxy. This is how "remote" devices will access the reverse proxy.
- **External Certificate Fingerprint:** Enter the Reverse Proxy Server's certificate SHA-256 fingerprint. Endpoints may require the fingerprint of the certificate used for external access.
- **Local IP Address Ranges:** Here you enter the IPv4 address ranges used within the corporate network. This will enable the PCoIP Management Console to identify local devices as opposed to remote devices.

Once your remote devices have checked in with the PCoIP Management Console, you can view the *ENDPOINTS* page, and see that the *IPv4 ADDRESS* column will show the IP address of the endpoint as seen by the PCoIP Management Console. In the case of a remote endpoint, this will be the public IP address.

The *INTERNAL IPv4* column will show the address assigned to the endpoint itself. In the case of a remote endpoint this will be the address assigned by the NAT or DHCP server of the remote endpoint.

The *CONNECTED BY* column will display either REMOTE or LOCAL based on where in the network the endpoint is in relation to the PCoIP Management Console.

Configuring DNS SRV Record Discovery for Reverse Proxy

This section explains how to configure a public facing DNS SRV and a DNS TXT record for your reverse proxy to provision endpoints with Endpoint Bootstrap Manager information, as part of the endpoint discovery process.

Endpoints polls the public facing DNS server for information about the reverse proxy (that is, the Endpoint Bootstrap Manager/Endpoint Manager) to which they should connect.

DNS service record discovery requires you to have a public facing DNS server in your network that is configured with the following DNS records:

- **An address record (A record):** Specifies the FQDN and IP address of the reverse proxy.
- **A service location record (SRV record):** Associates information such as the reverse proxy's TCP/IP service and the port the reverse proxy listens on with the reverse proxy's domain and host name. The reverse proxy's TCP/IP service is called **_pcoip-bootstrap**, as shown in [Adding the DNS SRV Record](#). The remote PCoIP Zero Client will look for this external facing DNS record.
- **A DNS TXT record:** Contains the reverse proxy certificate SHA-256 fingerprint. The record's name must be the host name of the reverse proxy offering the service. In the following example, this record is called **proxy**. The domain is appended automatically.

DNS Text fingerprint

Remote Endpoints only pick up the DNS TXT fingerprint if the reverse proxy address is specified in a DNS SRV record

BEFORE YOU BEGIN

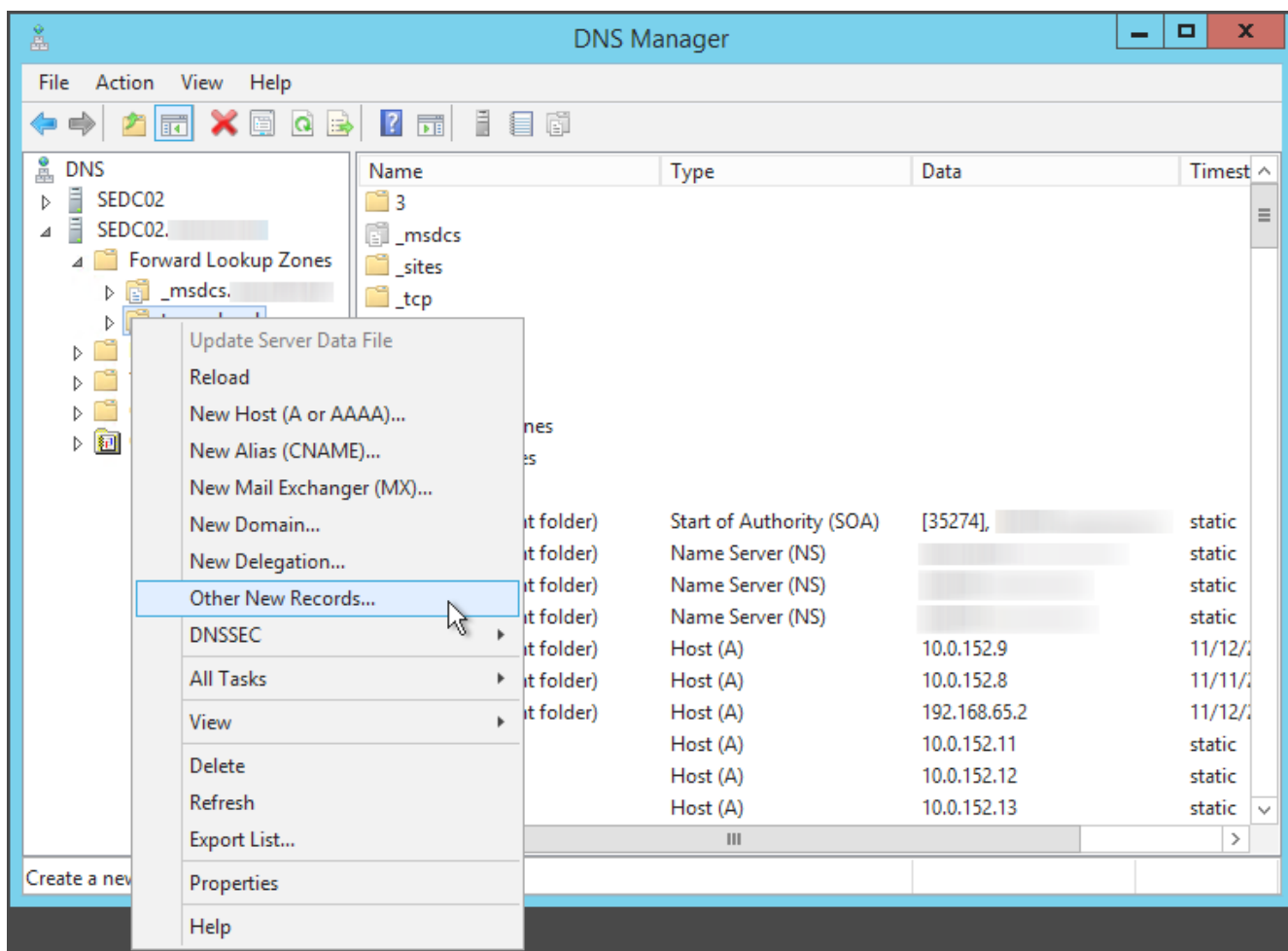
Before configuring your DNS SRV record discovery, you'll need the following information:

- The reverse proxy's FQDN
- The reverse proxy's certificate fingerprint (that is, the certificate's digital signature). If provided, this fingerprint is only used when the endpoint's security level is set to **Low Security Environment** and certificate verification has failed. It is ignored when the security level is set to **Medium Security Environment** or **High Security Environment**.

ADDING THE DNS SRV RECORD

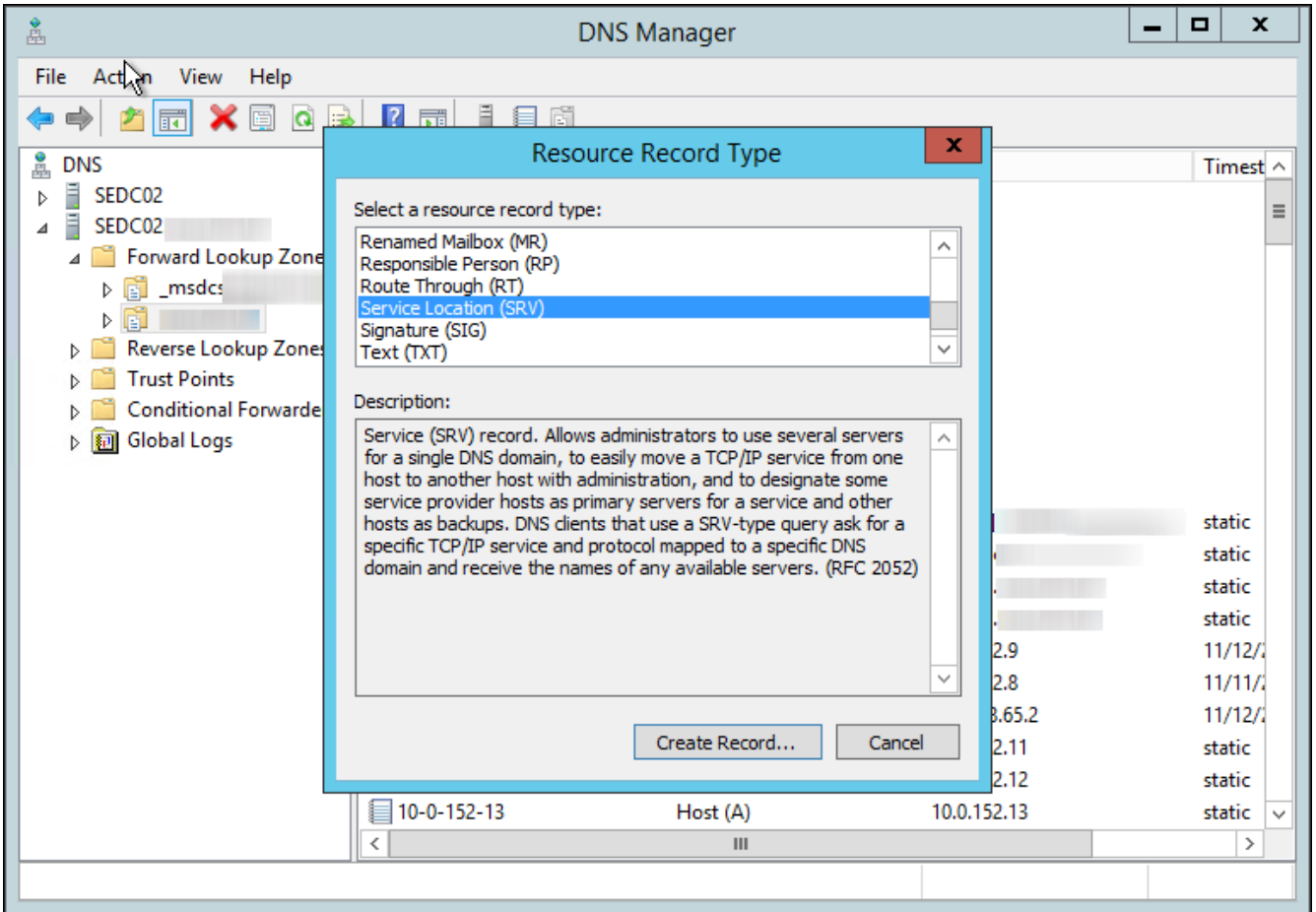
To add the public facing reverse proxy DNS SRV record to DNS server:

1. Log in to your Windows Server and select **DNS**.
2. Right-click on your DNS server in the *SERVERS* pane and select **DNS Manager** from the context menu.
3. In *Forward Lookup Zones*, right-click on your domain and select **Other New Records** from the context menu.




Public Facing Forward Lookup Zone

4. In the *Resource Record Type* dialog, select **Service Location (SRV)** from the list and click **Create Record**.



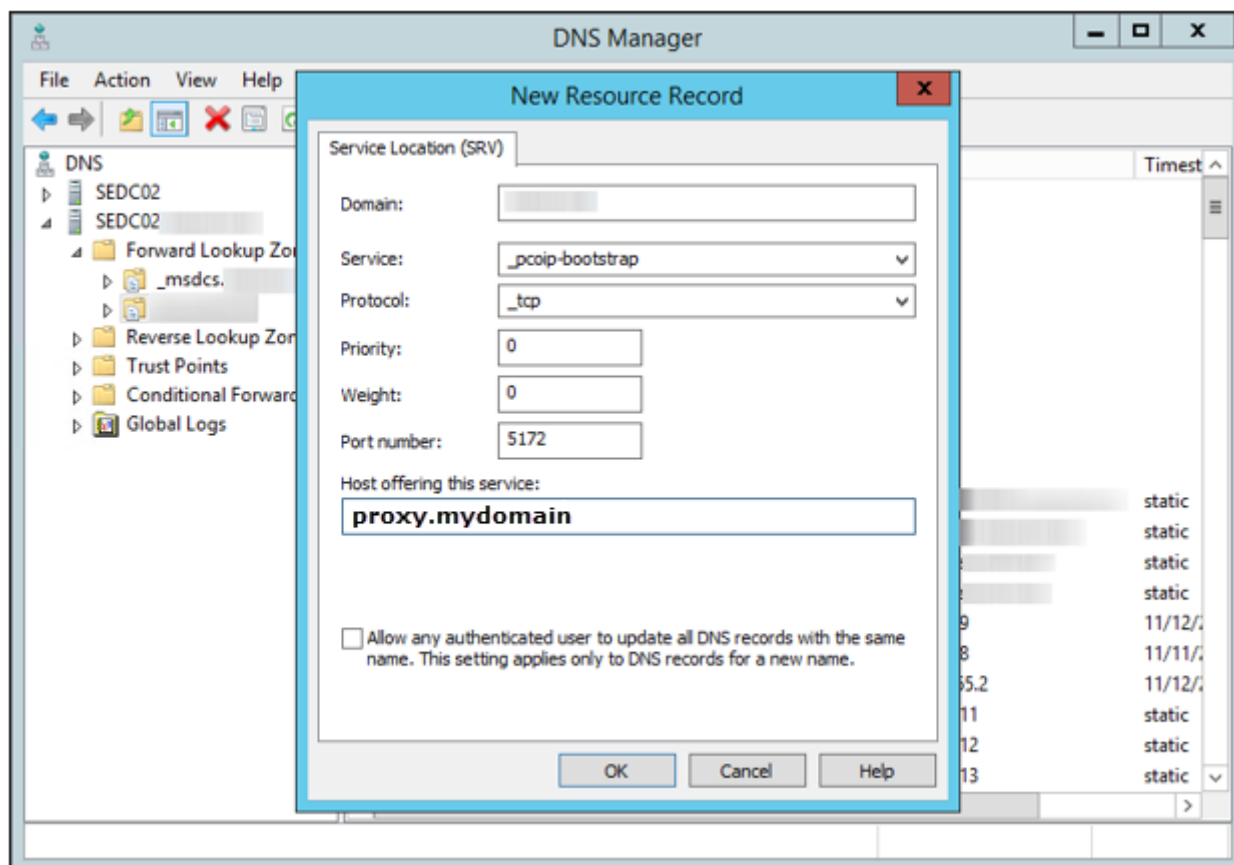
New Resource Record Type for SRV

- 5. Fill in the entries as shown in the following example. Set Service to **_pcoip-bootstrap**, Protocol to **_tcp**, and *Port number* to **5172**, the reverse proxy's listening port. For *Host offering this service*, enter the reverse proxy's FQDN.

 **FQDN entered**

FQDN must be entered in place of IP address

The reverse proxy's FQDN must be entered because the DNS specification does not enable an IP address in SRV records.



New Resource Record Dialog

6. Click **OK**.

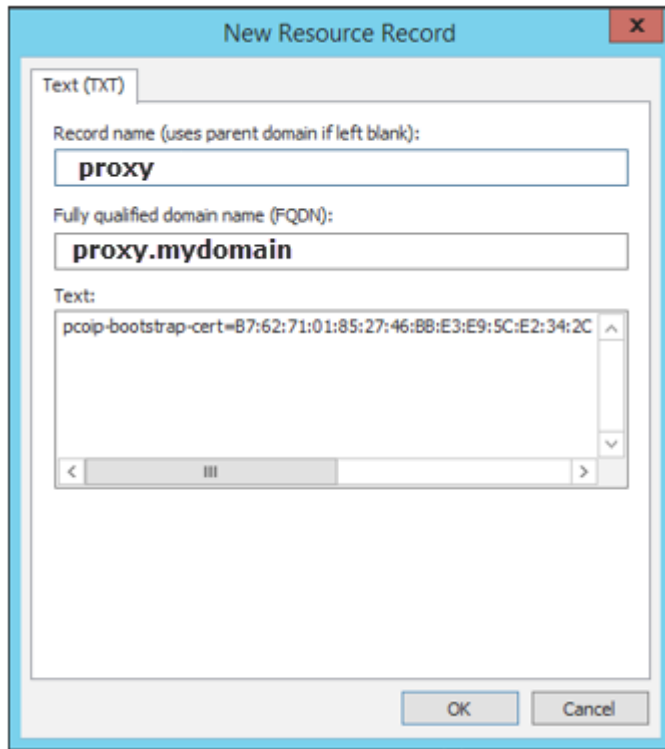
ADDING A DNS TXT RECORD

If your endpoints do not have the reverse proxy's root CA certificate installed in their certificate store, you must configure your DNS server with a DNS TXT record containing the reverse proxy certificate SHA-256 fingerprint.

To add a public facing DNS TXT record:

1. In *Forward Lookup Zones*, right-click on your domain and select **Other New Records** from the context menu.
2. In the Resource Record Type dialog, select **Text (TXT)** from the list and click **Create Record**.
3. Fill in the entries as follows:
 - In the *Record name* field, enter the host name of the reverse proxy offering the service (this example uses proxy). The FQDN field will be automatically populated for you and should match the FQDN of the reverse proxy.

- In the *Text* field, type `pcoip-bootstrap-cert=` and then paste the reverse proxy certificate SHA-256 fingerprint you obtained previously immediately after this prefix, as shown in the following example.



The screenshot shows a dialog box titled "New Resource Record" with a close button (X) in the top right corner. The dialog is divided into several sections:

- Text (TXT)**: A tabbed section containing the following fields:
 - Record name (uses parent domain if left blank):** A text input field containing the word "proxy".
 - Fully qualified domain name (FQDN):** A text input field containing "proxy.mydomain".
 - Text:** A large text area containing the string "pcoip-bootstrap-cert=B7:62:71:01:85:27:46:BB:E3:E9:5C:E2:34:2C".
- Buttons:** "OK" and "Cancel" buttons are located at the bottom right of the dialog.

New Text Record

4. Click **OK**.
5. When you have finished configuring your DNS server, power cycle your endpoints or put them online to enable them to make the connection to the reverse proxy.

See [Troubleshooting DNS](#) to verify that your DNS server is configured correctly for the reverse proxy.

Connecting to a Remote Endpoint

The remote endpoint must be configured with the external address of the reverse proxy. Depending on the configuration of the PCoIP Zero Client this can be done by either configuring and uploading the required certificates onto the PCoIP Zero Client via the AWI, or by creating an external DNS entry for the Reverse Proxy server via the PCoIP Zero Client OSD.

CONNECTING MANAGEMENT CONSOLE TO A REMOTE ENDPOINT FROM THE ENDPOINT OSD

This is the recommended method which requires the OSD be accessible and the end user knows the password, and that there is a properly configured corporate public facing DNS server that will provide the address and the SHA256 certificate fingerprint of the reverse proxy to the endpoint. ([Configuring DNS for Reverse Proxy](#))

1. From your PCoIP Zero Client OSD, navigate to **Options > Configuration > Network**.
2. Unlock your PCoIP Zero Client and un-check **Enable DHCP** (do not modify any other information)
3. In the **Domain Name** field enter the domain name of the domain you created the DNS entry in.
4. Select **OK**, you will be prompted to reset the PCoIP Zero Client, select **Reset** to restart your PCoIP Zero Client.

The PCoIP Zero Client will restart and it will reach out to the specified domain name based on your recently configured DNS SRV and DNS TXT records which will reach your configured reverse proxy server. The reverse proxy server will pass the connection to the PCoIP Management Console. The PCoIP Zero Client will now show up in your Ungrouped devices tab after a short period of time. This can be verified by viewing the management page from the OSD screen by navigating to **Options > Configuration > Management**.

CONNECTING MANAGEMENT CONSOLE TO A REMOTE ENDPOINT FROM THE ENDPOINT AWI

This method is done from the endpoint and requires the AWI be enabled, accessible, and the user knows the AWI password.

1. Install the certificate of the reverse proxy into the endpoint via the AWI *Certificate Upload* page by browsing to **Upload > Certificate**.

 **Reverse Proxy Certificate**

Typically this is the trusted root certificate for the reverse proxy.








2. Browse to **Configuration > Management** and set the **Manager Discovery Mode** to *Manual*.
3. Enter the address of the reverse proxy in the **Endpoint Bootstrap Manager URI** field. (i.e. wss://mc.company.local:5172)
4. Click **Apply** to save your changes and **Continue** to see the management connection status.

Using the Endpoints Page


Endpoints Page Overview

The actions you can perform from the **ENDPOINTS** page are listed in the following table.

ENDPOINTS Page Features

Menu	Action
<div data-bbox="161 264 400 322">EXPAND ALL </div> <div data-bbox="161 338 400 396">EXPAND ALL </div>	<p>Toggles to display the following:</p> <ul style="list-style-type: none"> • Expand top-level and parent groups to display all child level groups and endpoints. • Collapse the group hierarchy and display only top-level groups.
<div data-bbox="161 472 347 530">PROFILE </div>	<p>Displays on the GROUPED table and provides the following menus:</p> <ul style="list-style-type: none"> • DETAILS: View details about a profile assigned to a group. See Viewing Profile Details. • CHANGE: Change the profile assigned to a group. See Changing a Profile Association. • APPLY: Apply a profile to a group. See Applying a Profile.
<div data-bbox="161 777 384 835">STRUCTURE </div>	<p>Provides the following menus:</p> <ul style="list-style-type: none"> • MOVE: Move endpoints or groups to a group. See Moving Endpoints into Groups. • RENAME: Rename a group or endpoint. See Renaming a Group. • NEW GROUP: Create a new group. See Creating Groups. • REMOVE GROUP: Remove a group. See Removing a Group.
<div data-bbox="161 1081 379 1140">ENDPOINTS </div>	<p>Provides the following menus:</p> <ul style="list-style-type: none"> • DETAILS: View details about an endpoint. See Using the ENDPOINT DETAILS Page. • POWER DOWN: Power down one or more endpoints. See Powering Down PCoIP Zero Clients. • POWER RESET: Reset (reboot) one or more endpoints. See Resetting PCoIP Zero Clients. • RESET TO DEFAULT: Reset endpoint properties to their default values. See Resetting Endpoint Properties to Their Defaults. An endpoint reboot may be needed If the endpoint properties have not been reset to their default values, then an endpoint reboot will be required. • DELETE: Remove one or more endpoints from the PCoIP Management Console. See Deleting Endpoints.
<div data-bbox="161 1744 453 1803">ENDPOINT DISCOVERY</div>	<p>Lets you manually discover endpoints by their IP address. See Discovering Endpoints Manually from PCoIP Management Console.</p>
<div data-bbox="161 1848 298 1906">SEARCH</div>	<p>Lets you search for one or more endpoints in the endpoint table. See Searching an Endpoint Table.</p>
<div data-bbox="161 1951 387 2009">FILTER  </div>	<p>Lets you create and manage filters to display only specified endpoints. See Filtering the Endpoint List.</p>

Refreshes the endpoint table with the current configuration.

 **Click REFRESH after completing a manual discovery**

The endpoint table does not refresh automatically. Click REFRESH after completing a manual discovery and any time you do not see an endpoint that you expect to be there.


Displaying Endpoint Properties

The **ENDPOINTS** page, displayed next, contains GROUPED and UNGROUPED tables for displaying the endpoints in your system that are managed by the PCoIP Management Console.

NAME	IPv4 ADDRESS	ENDPOINT DESCRIPTION	SOFTWARE VERSION	PROFILE	MAC ADDRESS	DEVICE STATUS
Accounting				Accounting		
• 00-00-00-00-01-9A	10.100.160.182	Tera2 Client Quad Display	5.0.0		00:00:00:00:01:9a	Out Of Session(online)
• 00-00-00-00-01-E5	10.100.160.109	Tera2 Client Quad Display	5.0.0		00:00:00:00:01:e5	Out Of Session(online)
• 00-00-00-00-02-80	10.100.160.178	Tera2 Client Quad Display	5.0.0		00:00:00:00:02:80	Out Of Session(online)
• 00-00-00-00-02-59	10.100.160.180	Tera2 Client Quad Display	5.0.0		00:00:00:00:02:59	Out Of Session(online)
• 00-00-00-00-03-AB	10.100.160.181	Tera2 Client Quad Display	5.0.0		00:00:00:00:03:ab	Out Of Session(online)
Engineering				Engineeri...		
• 00-00-00-00-02-7A	192.168.50.219	Tera2 Client Quad Display	5.0.0		00:00:00:00:02:7a	Out Of Session(online)
• 00-00-00-00-00-95	192.168.51.208	Tera2 Client Quad Display	5.0.0		00:00:00:00:00:95	Out Of Session(online)
• 00-00-00-00-02-EB	192.168.51.207	Tera2 Client Quad Display	5.0.0		00:00:00:00:02:eb	Out Of Session(online)
• 00-00-00-00-00-24	192.168.51.201	Tera2 Client Quad Display	5.0.0		00:00:00:00:00:24	Out Of Session(online)
• 00-00-00-00-02-91	192.168.51.205	Tera2 Client Quad Display	5.0.0		00:00:00:00:02:91	Out Of Session(online)
• 00-00-00-00-03-E7	192.168.51.204	Tera2 Client Quad Display	5.0.0		00:00:00:00:03:e7	Out Of Session(online)

View of the ENDPOINTS page

Selecting Endpoint Properties to Display

Click the gear icon  to the right of the table to change the information you want to display in the table columns. Your customized settings are saved in your browser and will be used for any user who subsequently logs in from that browser.

Properties are ordered in the sequence you select them. You can rearrange a column by manually dragging the column heading to the desired position. You can also sort endpoints in ascending or descending order based on column contents by clicking on the column heading. Endpoints that occur in groups are sorted within their group.

You can choose to display the following properties:

Endpoint Properties

Property	Information	Grouped	Ungrouped	MC Enterprise Only
ATTACHED USB DEVICES	<p>Displays information from attached USB Devices.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • Model: Displays the model name of the USB device. • Vendor ID (VID): Displays the USB devices vendor identifying number provided to the vendor by the USB implementers forum. • Product ID (PID): Displays the product identifying number provided by the vendor or maker of the USB device. 			
AUTO CONFIGURATION STATUS	<p>Displays an endpoint's auto configuration status.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • NO PROFILE • NOT STARTED • AUTOCONFIG DISABLED • FAILED DHCP OPTION GROUP NOT FOUND • FAILED DHCP OPTION RULE NOT FOUND • FAILED DHCP OPTION BEHAVIOR NONE • FAILED DHCP OPTION MATCHING DISABLED • FAILED IP RANGE CHECK • FAILED UNKNOWN ERROR • ADDED TO DHCP OPTION GROUP • ADDED TO GROUP • PENDING PROFILE APPLICATION • FAILED PROFILE APPLICATION IN PROGRESS • FAILED PROFILE APPLICATION 			

Property	Information	Grouped	Ungrouped	MC Enterprise Only
	<ul style="list-style-type: none"> • COMPLETED 			
APPLY PROFILE	<p>Displays the status of endpoint's profile update.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • NO PROFILE • NOT STARTED • IN PROGRESS • COMPLETED • FAILED • PENDING REBOOT • FAILED OFFLINE • FAILED PENDING REBOOT TIMEOUT • SKIPPED NO REBOOT • SKIPPED <p>Some common reasons for the 'skipped' status is if the endpoint is already configured with the profile settings or if its group does not have an assigned profile.</p>			
CERTIFICATE EXPIRY DATE	<p>Displays the date the SCEP certificate will expire and become not valid.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • CERTIFICATE EXPIRY DATE 			
CERTIFICATE NAME	<p>Displays the SCEP certificate subject name.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • CERTIFICATE NAME 			

Property	Information	Grouped	Ungrouped	MC Enterprise Only
CERTIFICATE RULE	<p>Displays the SCEP certificate rule assigned to a group. This rule defines the SCEP SERVER address and password that an Endpoint can use to request a SCEP certificate. You can create a certificate rule from the ENDPOINT CERTIFICATE tab.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • RULE NAME 			
CERTIFICATE START DATE	<p>Displays the date the SCEP certificate becomes valid.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • DATE 			
CERTIFICATE STATUS (PCoIP Zero Client only)	<p>Displays the status of the SCEP certificate.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • Active • About To Expire • Expiring Today • Expired • Not Requested • Not Applicable 			
CLEAR MANAGEMENT STATE	<p>Indicates if devices now have all management settings cleared and set back to a default state.</p>			
CONNECTED BY	<p>Identifies where in the deployment the PCoIP endpoint is placed.</p> <p>Possible Values:</p> <ul style="list-style-type: none"> • NO PROFILE • Local • Remote 			

Property	Information	Grouped	Ungrouped	MC Enterprise Only
DENIED	<p>Indicates whether or not the PCoIP Management Console has enough licenses to manage all the discovered endpoints.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • NO PROFILE • True: The endpoint is denied (that is, it cannot be managed) because a license is not available for it. • False (displays as a blank in the column): The endpoint is not denied and can be managed. 			
DEVICE DESCRIPTION	<p>Displays the PCoIP Device Description text located on the endpoints AWI Label page.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • any text string 			
PCOIP DEVICE NAME	<p>The MAC Address value will be set to the PCoIP Device Name field after a profile with this setting configured is successfully applied. The Device Name has a maximum length of 63 characters.</p> <ul style="list-style-type: none"> • If the PCoIP device name in a profile is "true" and the PCoIP device name on the endpoint is the endpoint's MAC address, then the profile compliance will show as COMPLIANT • If the PCoIP device name in the profile is "true", and the PCoIP device name on the endpoint is not the endpoint's MAC address, then the profile compliance will show as NON COMPLIANT • If the PCoIP device name in the profile is "false", and the PCoIP device name on the endpoint is either the MAC address or non 			

Property	Information	Grouped	Ungrouped	MC Enterprise Only
	<p>MAC address, then the profile compliance will show as COMPLIANT</p> <p>Possible values:</p> <ul style="list-style-type: none"> • any text string 			
DEVICE STATUS	<p>Indicates whether or not an endpoint is connected to the PCoIP Management Console and if it is in a PCoIP session with another PCoIP software or hardware endpoint.</p> <p>DEVICE STATUS is a combination of the previous ONLINE and IN SESSION properties.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • NO PROFILE • Offline • Out of Session (online) • In Session (online) • In Recovery (online) 			
DISPLAY TYPE	<p>Displays the maximum number of monitors an endpoint supports.</p> <p>Possible values for a PCoIP Zero Client and Remote Workstation Card:</p> <ul style="list-style-type: none"> • NO PROFILE • Dual: The endpoint supports up to two monitors. • Quad: The endpoint supports up to four monitors. 			
ENDPOINT DESCRIPTION	<p>Displays information about the endpoint family and endpoint type.</p>			

Property	Information	Grouped	Ungrouped	MC Enterprise Only
ENDPOINT HEALTH	<p>Displays the status of an endpoint's health state.</p> <p>Possible Values:</p> <ul style="list-style-type: none"> • Unknown: The Management Console cannot determine, or is in the process of determining the status of endpoint. • Normal: The endpoint is operational and working as expected. • Recovery: This is a warning or notification to the user that the endpoint is in recovery mode and currently unable to connect to a session. 			
ENDPOINT PLATFORM	<p>Displays the endpoint's PCoIP family. In this release, only endpoints that support the Tera2 platform can be managed by the PCoIP Management Console.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • NO PROFILE • TERA2 			
ENDPOINT TYPE	<p>Displays the endpoint type.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • NO PROFILE • Client • Host 			
FIRMWARE BUILD ID	<p>Lists the firmware build number in use on the PCoIP endpoint.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • NO PROFILE • FIRMWARE BUILD ID 			

Property	Information	Grouped	Ungrouped	MC Enterprise Only
FIRMWARE POWER RESET	<p>Displays the status of an endpoint's power reset after updating its firmware.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • NO PROFILE • NOT STARTED • IN PROGRESS • COMPLETED • FAILED • SKIPPED • FAILED PENDING REBOOT TIMEOUT • SKIPPED NO REBOOT • PENDING REBOOT • SKIPPED <p>One common reason for the 'skipped' status is if a firmware update failed for the endpoint. In this case, the power reset would not occur either.</p>			
FIRMWARE UPLOAD	<p>Displays the status of an endpoint's firmware upload.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • NO PROFILE • NOT STARTED • IN PROGRESS • COMPLETED • FAILED • FAILED OFFLINE • PENDING REBOOT TIMEOUT • SKIPPED <p>One common reason for the 'skipped' status is if the endpoint is already running the specified firmware version.</p>			
FQDN				

Property	Information	Grouped	Ungrouped	MC Enterprise Only
	<p>Displays an endpoint's fully-qualified domain name.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • NO PROFILE • FQDN 			
GENERIC TAG	<p>Displays the Generic Tag text located on the endpoints AWI Label page.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • any text string 			
GET ALL SETTINGS	<p>Displays an endpoint's polling status.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • NO PROFILE • NOT STARTED • IN PROGRESS • COMPLETED • FAILED • FAILED OFFLINE 			
IPv4 or IPv6 ADDRESS	<p>Only the information of the network that Management Console is configured to operate in (IPv4 or IPv6) will be visible</p> <p>Possible values:</p> <ul style="list-style-type: none"> • NO PROFILE • IP Address <p>Displays an endpoint's IPv4/IPv6 address</p>			
INTERNAL IPv4 or IPv6	<p>Only the information of the network that Management Console is configured to operate in (IPv4 or IPv6) will be visible.</p> <p>Displays an endpoint's IPv4/IPv6 address for the network the endpoint is part of. For remote</p>			

Property	Information	Grouped	Ungrouped	MC Enterprise Only
	<p>endpoints, this will be their internal network addresses.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • NO PROFILE • IPv4 or IPv6 ADDRESS 			
LAST POLLED	<p>Displays the last date and time that the PCoIP Management Console polled an endpoint for its status and configuration information. The PCoIP Management Console's polling interval is 60 minutes.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • NO PROFILE 			
MAC ADDRESS	<p>Displays an endpoint's MAC address.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • NO PROFILE 			
OSD LOGO	<p>Displays the status of an endpoint's OSD logo bitmap file update to the endpoint's On Screen Display (OSD).</p> <p>Possible values:</p> <ul style="list-style-type: none"> • NO PROFILE • NOT STARTED • IN PROGRESS • COMPLETED • FAILED • SKIPPED <p>One common reason for the 'skipped' status is if the endpoint already has the OSD logo configured.</p>			
PEER	<p>If a peer is configured for an endpoint, it's IP address is shown in the column.</p>			

Property	Information	Grouped	Ungrouped	MC Enterprise Only
	<p>Possible values:</p> <ul style="list-style-type: none"> • NO PROFILE • PEER IP ADDRESS 			
PROFILE	<p>Appears next to a group to display the profile assigned to it.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • NO PROFILE • PROFILE NAME 			
PROFILE COMPLIANCE	<p>Indicates whether or not an endpoint's current known configuration differs from the PCoIP Management Console profile assigned to the endpoint's group.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • NO PROFILE • COMPLIANT: the endpoint matches the profile • NON-COMPLIANT: the endpoint does not match the profile • UNKNOWN: the MC cannot determine, or is in the process of determining if the endpoint matches the profile • NO PROFILE: there is no profile to compare the endpoint to 			
PROFILE POWER RESET	<p>Displays an endpoint's power reset status resulting from a profile property requiring a power reset and not a firmware change.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • NO PROFILE • NOT STARTED • IN PROGRESS • COMPLETED 			

Property	Information	Grouped	Ungrouped	MC Enterprise Only
	<ul style="list-style-type: none"> • FAILED • FAILED PENDING REBOOT TIMEOUT • SKIPPED NO REBOOT • PENDING REBOOT • SKIPPED <p>One common reason for the 'SKIPPED' status is if a profile update failed or skipped for the endpoint. In this case, the power reset would not occur.</p>			
RESET TO DEFAULT COLUMNS	<p>Resets the table to display the default columns.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • NO PROFILE 			
SERIAL NUMBER	<p>All endpoints provide their serial numbers to the PCoIP Management Console endpoints table. The serial number can also be exported into the Inventory Report.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • NO PROFILE • SERIAL NUMBER 			
SOFTWARE VERSION	<p>Firmware file name used in the PCoIP firmware build minus the build number.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • NO PROFILE 			
UNIQUE ID	<p>Displays an endpoint's MAC address delimited with hyphens instead of colons. This field can be incorporated into the automatic naming convention for endpoints.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • NO PROFILE 			

Property	Information	Grouped	Ungrouped	MC Enterprise Only
• ENDPOINT MAC ADDRESS				

Using the ENDPOINT DETAILS Page

The **ENDPOINT DETAILS** page displays complete configuration and status information for the selected endpoint.

It contains menu options that enable you to perform the following actions:

- [Open the endpoint's profile in edit mode](#)
- [Apply the profile to the endpoint right away](#)
- [Move the endpoint to a group](#)
- [Rename the endpoint](#)
- [Power down the endpoint](#)
- [Power reset \(reboot\) the endpoint](#)
- [Resetting Endpoint Properties to Factory Defaults](#)
- [Clear the management state of the endpoint](#)
- [Requesting an Endpoint Certificate](#)
- [Peering Endpoints \(ENTERPRISE\)](#)
- [Access the endpoint's web interface](#)
- [Refresh](#)

i Info: No data from the endpoint

In cases such as restoring a database, the PCoIP Management Console must first poll the online endpoint before it can display the endpoint details information.

The screenshot displays the 'ENDPOINT DETAILS' page in the PCoIP Management Console. At the top, there are navigation tabs: 'PROFILE', 'STRUCTURE', 'ENDPOINTS', 'WEB INTERFACE', and 'REFRESH'. The main content is divided into three columns:

- ENDPOINT:** Lists various identifiers and settings such as Full Name, IPv4 Address, MAC Address, FQDN, Unique ID, Internal IPv4 Address, Connected By, Certificate Status, Certificate Expiry Date, Certificate Rule, and Attached USB Devices (Model:USB Keyboard, PID:C31C, VID:046D; Model:USB Mouse, PID:C31C, VID:046D).
- STATUS:** Shows operational metrics including Last Attempted Update (2022-07-08 10:41 AM UTC), Last Polling Status, Last Restart (2022-07-08 06:51 AM UTC), Online Status (Offline), PCoIP Session Status (Out of Session), Denied (False), and Peer Address.
- PROFILE:** Displays the Profile Name, Last Applied Profile Time, Endpoint Type (Tera2 Client Dual Display), and Grouping (g1).

Displaying Endpoint Details

To display endpoint details:

1. From the PCoIP Management Console's top menu, click **ENDPOINTS**.
2. In either the *GROUPED* or *UNGROUPED* table, select the desired endpoint.
3. Click **ENDPOINTS** and then **DETAILS**.

Opening an Endpoint's Profile

To open an endpoint profile:

1. From the *ENDPOINT DETAILS* page, click **PROFILE**.
2. Click **DETAILS** to open the endpoint's profile in edit mode.

Applying a Profile to an Endpoint

You can update an endpoint by applying a profile from the **ENDPOINTS** page or the **ENDPOINT DETAILS** page. This applies the profile right away or after any currently running scheduled actions for this endpoint have completed.

To apply a profile to an endpoint:

1. From the *ENDPOINTS* page, select the endpoint.
2. Click **PROFILE > APPLY**.

Moving an Endpoint

You can move an endpoint to a group either from the *ENDPOINTS* page or the *ENDPOINT DETAILS* page.

To move an endpoint:


1. From the *ENDPOINT DETAILS* page, click **STRUCTURE** and then **MOVE**.
2. Select the desired parent group or child group, and then click **MOVE TO GROUP**.

Renaming an Endpoint

You can rename an endpoint either from the *ENDPOINTS* page or the *ENDPOINT DETAILS* page.

To rename an endpoint:

1. From the *ENDPOINT DETAILS* page, click **STRUCTURE** and then **RENAME**.
2. Enter a unique name for the endpoint (from within its group hierarchy) and click **RENAME ENDPOINT**.

 **Note: Auto naming endpoints**

If you have configured a global naming convention for endpoints that applies when they move to or from a group, this overrides any manually configured endpoint name. If you then move the endpoint into or out of a group, the automatic naming rule will apply. See [Auto Naming Endpoints](#).

Powering Down an Endpoint

Caution: Remote Workstation Cards

Remote Workstation Cards cannot be **powered down, power reset, or reset to default** by the PCoIP Management Console as the Remote Workstation Card requires the host computer to be restarted due to the Remote Workstation Card obtaining its power from the host computer motherboard. An alternate method of restarting the host computer is required to restart the host computer.

Powering Down a PCoIP Zero Client

The **POWER DOWN** option causes a PCoIP Zero Client to power down right away, or after any currently running scheduled actions for this endpoint have completed. You can power down a PCoIP Zero Client either from the *ENDPOINTS* page or the *ENDPOINT DETAILS* page.

To power down an endpoint:

1. From the *ENDPOINT DETAILS* page, click **ENDPOINTS** and then **POWER DOWN**.
2. Click **OK** at the message prompt.

Power Resetting an Endpoint

Caution: Remote Workstation Cards

Remote Workstation Cards cannot be **powered down, power reset, or reset to default** by the PCoIP Management Console as the Remote Workstation Card requires the host computer to be restarted due to the Remote Workstation Card obtaining its power from the host computer motherboard. An alternate method of restarting the host computer is required to restart the host computer.

The **POWER RESET** option causes a PCoIP Zero Client to reset (reboot) right away, or after any currently running scheduled actions have completed. You can reset a PCoIP Zero Client either from the *ENDPOINTS* page or the *ENDPOINT DETAILS* page.

To reset an endpoint:

1. From the *ENDPOINT DETAILS* page, click **ENDPOINTS** and then **POWER RESET**.
2. Click **OK** at the message prompt.

Resetting Endpoint Properties to Factory Defaults

The **RESET TO DEFAULT** option causes an endpoint to reset to its default factory configuration right away, or after any currently running scheduled actions have completed. You can reset an endpoint to its default factory configuration either from the *ENDPOINTS* page or the *ENDPOINT DETAILS* page.

Caution: Remote Workstation Cards

Remote Workstation Cards cannot be **powered down, power reset, or reset to default** by the PCoIP Management Console as the Remote Workstation Card requires the host computer to be restarted due to the Remote Workstation Card obtaining its power from the host computer motherboard. An alternate method of restarting the host computer is required to restart the host computer.

To reset endpoint properties to their defaults:

1. From the *ENDPOINT DETAILS* page, click **ENDPOINTS** and then **RESET TO DEFAULT**.
2. Click **OK** at the message prompt.
3. If the endpoint does not reboot after the reset to default command completes, reboot the endpoint either manually or from the PCoIP Management Console using the **POWER RESET** command.

Clearing the Management State of the Endpoint

The PCoIP Management Console allows you to place the endpoint in an unmanaged state allowing the endpoint to be managed by another PCoIP Management Console or a compatible management tool of your choice.

To clear the management state of an endpoint:

1. From the *ENDPOINT DETAILS* page, click **ENDPOINTS** and then **CLEAR MANAGEMENT STATE**.

Requesting an Endpoint Certificate

The REQUEST CERTIFICATE option is an active option when your endpoint is in a group defined in your SCEP rule. The rule can contain one or more certificate usage types or requests. When you request a certificate for an endpoint, the Management Console initiates a request for a certificate using the certificate rules that apply to the endpoint.

To request a SCEP certificate:

1. Ensure your SCEP rules are configured. See [Requesting Endpoint Certificates Using SCEP \(Enterprise\)](#).
2. From the *ENDPOINT DETAILS* page, highlight your endpoint or the group of endpoints for this request and click **ENDPOINTS** and then **REQUEST CERTIFICATE**.

Peering Endpoints (ENTERPRISE)

PCoIP Management Console allows the option of peering a specific PCoIP Zero Client with a predetermined Remote Workstation Card. This is done using the PEER and UNPEER options found on the Endpoint DETAILS page. UNPEER is enabled when a host endpoint is selected prior to reaching the DETAILS page.

To peer a client and a host endpoint:

1. From the *ENDPOINT* page, highlight the endpoint you want to peer with.
2. From the *ENDPOINT DETAILS* page, click **PEER**.
3. Click **OK** at the message prompt.

Caution: UNPEER behavior on endpoints

When unpeered, the host card will accept connections from any peer and the PCoIP Zero Client will continue to have the host IP configured until a session configuration change is made to that PCoIP Zero Client.

To unpeer a client and a host endpoint:

1. From the *ENDPOINT DETAILS* page of a Remote Workstation Card, click **ENDPOINTS** and then **UNPEER**.

2. Click **OK** at the message prompt.

i Info: Unpeer option

You can only unpeer a client from a Remote Workstation Card. The UNPEER option is disabled on the PCoIP Zero Client ENDPOINT DETAILS page.

Deleting an Endpoint

You cannot delete an endpoint from the ENDPOINTS DETAILS page but you can from the ENDPOINTS page. See [Deleting Endpoints](#).

Accessing an Endpoint's AWI

From the *ENDPOINT DETAILS* page click **WEB INTERFACE** to open the endpoint's AWI in a browser to configure the endpoint directly.

i Info: Network Access

If you do not have network access to the AWI, then the link won't work.

For information about the AWI, please see [PCoIP Zero Client Firmware Administrators' Guide](#) or the [Remote Workstation Card Firmware Administrators' Guide](#).

Refreshing an Endpoint

Click **Refresh** will display the correct information for anything listed on that page for that particular endpoint. This may take several minutes to complete.

Performing Power Management

The **ENDPOINTS** page provides menu options to let you power down and reset PCoIP Zero Clients from the PCoIP Management Console. These actions are performed on one or more individual PCoIP Zero Clients and occur as soon as you apply them from the **ENDPOINTS** menu, or after any currently running scheduled actions for this PCoIP Zero Client have completed. Alternatively, you can create a schedule to power down or reset one or more groups of PCoIP Zero Clients in the future. See [Creating a Schedule](#).

Caution: Remote Workstation Cards

Remote Workstation Cards cannot be **powered down, power reset, or reset to default** by the PCoIP Management Console as the Remote Workstation Card requires the host computer to be restarted due to the Remote Workstation Card obtaining its power from the host computer motherboard. An alternate method of restarting the host computer is required to restart the host computer.

Powering Down PCoIP Zero Clients

The **POWER DOWN** option causes an PCoIP Zero Client to power down right away, or after any currently running scheduled actions have completed. You can power down PCoIP Zero Clients either from its **ENDPOINT DETAILS** page or from the **ENDPOINTS** page.

To power down PCoIP Zero Clients:

1. From the PCoIP Management Console's top menu, click **ENDPOINTS**.
2. In either the *GROUPED* or *UNGROUPED* table, select one or more PCoIP Zero Clients that you wish to power down.
 - a. From the PCoIP Management Console's top menu, click **ENDPOINTS**.
 - b. In either the *GROUPED* or *UNGROUPED* table, select one or more PCoIP Zero Clients that you wish to reset.

 **Note: Use `shift` +Click and `ctrl` +Click to select elements**

Use `shift` +Click to select contiguous elements and `ctrl` +Click to select non-contiguous elements.

- c. Click **ENDPOINTS** and then **POWER RESET**.
 - d. Click **OK** at the message prompt.
3. Click **ENDPOINTS** and then **POWER RESET**.
 4. Click **OK** at the message prompt.

Resetting PCoIP Zero Clients

The **POWER RESET** option causes PCoIP Zero Clients to reboot right away, or after any currently running scheduled actions for this PCoIP Zero Clients have completed. You can reset an endpoint either from its **ENDPOINT DETAILS** page or from the **ENDPOINTS** page.

To reset endpoints:

1. From the PCoIP Management Console's top menu, click **ENDPOINTS**.
2. In either the *GROUPED* or *UNGROUPED* table, select one or more PCoIP Zero Clients that you wish to reset.

 **Note: Use `shift` +Click and `ctrl` +Click to select elements**

Use `Shift` +Click to select contiguous elements and `ctrl` +Click to select non-contiguous elements.

1. Click **ENDPOINTS** and then **POWER RESET**.
2. Click **OK** at the message prompt.

Resetting Endpoint Properties to Their Defaults

 **Note: Resetting an endpoint clears the management state and disables the AWI**

See [Configuring DNS for Endpoints that use Autodiscovery](#) or [Configuring DHCP for Endpoints that use Auto Discovery](#)

- **Management State:** Resetting an endpoint to factory defaults will clear the management state of the endpoint. The bootstrap and endpoint discovery will need to be done automatically or manually. If the endpoint has autodiscovery enabled, it will check back into the Management Console. If the endpoint has not been configured for autodiscovery, you will have to have physical access to the endpoint to use the OSD or configure management access.
- **AWI:** Resetting a Zero Client to factory defaults will disable the Administrative Web Interface. The Remote Workstation Card AWI is not disabled by default. You can gain access to the AWI again if you are on site and can access the OSD, or if autodiscovery is enabled where you can re-apply a profile that enables the AWI.

The **RESET TO DEFAULT** option causes an endpoint to reset to its default configuration right away, or after any currently running scheduled actions for this endpoint have completed. You can reset an endpoint to its default configuration either from its **ENDPOINT DETAILS** page or from the **ENDPOINTS** page. Performing a **RESET TO DEFAULT** on a Remote Workstation Card requires someone onsite to power cycle the host computer.

To reset endpoint properties to their defaults:

1. From the PCoIP Management Console's top menu, click the **ENDPOINTS** link.
2. In either the *GROUPED* or *UNGROUPED* table, select one or more endpoints that you wish to reset.

 Use +Click and +Click to select elements

Use +Click to select contiguous elements and +Click to select non-contiguous elements.

3. Click **RESET TO DEFAULT** then **OK**.

Renaming Endpoints

You can rename an endpoint either from its *ENDPOINT DETAILS* page or the *ENDPOINT* page.

To rename endpoints:

1. From the PCoIP Management Console's top menu, click **ENDPOINTS**.
2. In either the *GROUPED* or *UNGROUPED* table, select the endpoint that you wish to rename.
3. Click **STRUCTURE** and then **RENAME**.
4. Enter a unique name for the endpoint (from within its group hierarchy) and click **RENAME ENDPOINT**.

Note: Auto naming endpoints

If you have configured a global naming convention for endpoints that applies when they move to or from a group, this overrides any manually configured endpoint name. If you then move the endpoint into or out of a group, the automatic naming rule will apply. See [Auto Naming Endpoints](#).

Deleting Endpoints

You can delete an endpoint when you no longer wish it to be managed by the PCoIP Management Console. This also removes it from its *GROUPED* or *UNGROUPED* endpoints table.

If auto-discovery is used (DHCP option-based or DNS SRV records) and the endpoint is still connected to the network, it will attempt to initiate a new connection to the PCoIP Management Console and re-register with it.

Note: Deleting endpoint does not clear its management state

Once an endpoint is managed by a PCoIP Management Console, deleting an endpoint from the PCoIP Management Console does not clear the management state of the endpoint itself. If you wish to connect the endpoint to another PCoIP Management Console, then you must clear the management state of that endpoint from the endpoint's AWI. If you do not clear the management state of the endpoint, and it still has network connectivity to the PCoIP Management Console, then it will reconnect and re-register itself with the PCoIP Management Console.

To delete endpoints:

1. From the PCoIP Management Console's top menu, click **ENDPOINTS**.
2. In either the *GROUPED* or *UNGROUPED* table, select one or more endpoints that you wish to delete.

Tip: Press Shift+Click to select contiguous elements

Use Shift+Click to select contiguous elements and Ctrl+Click to select non-contiguous elements.

3. Click **ENDPOINTS** and then **CLEAR MANAGEMENT STATE**.
4. Click **ENDPOINTS** and then **DELETE**.
5. Click **I AM SURE** at the message prompt.

Searching an Endpoint Table

The **ENDPOINTS** page contains a search function that lets you locate endpoints in either the *GROUPED* or *UNGROUPED* endpoint table by searching on any text that appears in the displayed columns.

To perform a search:

1. Enter the desired search text in the search text box.
2. Press or click **SEARCH**.

To clear a search, click the **x** in the search text box.

Filtering the Endpoint List

The *ENDPOINTS* page contains a filter function that lets you select from a list of predefined filters to refine the endpoints that display in a *GROUPED* or *UNGROUPED* endpoints table. For example, you can display only endpoints with profile mismatches or endpoints that have failed to power down or reset. You can also create your own filter criteria and save your filters into the list. New filters may be added as improvements are developed.

The screenshot shows the PCoIP Management Console interface. At the top, there is a navigation bar with tabs: DASHBOARD, ENDPOINTS (selected), PROFILE, SCHEDULE (26), AUTO CONFIGURATION, and ENDPOINT CERTIFICATES. Below the navigation bar, there are two tabs: GROUPED (483) and UNGROUPED (70). The main area displays a table of endpoints with columns: NAME, IPV4 ADDRESS, ENDPOINT DESCRIPTION, SOFTWARE VERSION, PROFILE, MAC ADDRESS, and EN. A filter dropdown menu is open, showing a list of predefined filters. The table contains two groups of endpoints: Accounting and Engineering. The Accounting group has 5 endpoints, and the Engineering group has 7 endpoints. The filter dropdown menu includes options like CLEAR FILTER, MANAGE SAVED FILTERS, SAVE ACTIVE FILTER, and a list of predefined filters such as Profile Update Failures, Persistent Autoconfig Failures, Power Down Failures, Power Reset Failures, Profile Compliance, Endpoint Updates in Progress, Endpoint Updates Pending, Endpoints Waiting on Restart, Endpoints Scheduled, Endpoints With Expired Certificate, Endpoints With Certificate Expiring Today, Endpoints With About To Expire Certificate, Endpoints Without Certificates, Groups Without Certificate Rule, Endpoints With Active Certificate, Skipped Reboot On Profile Application, and Endpoints Requiring Manual Reboot.

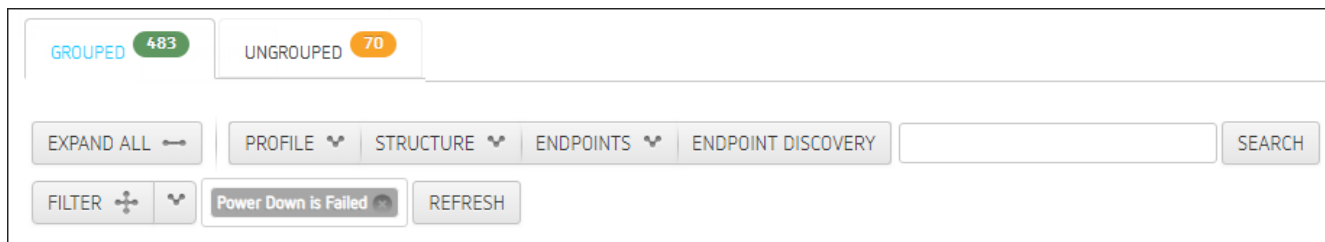
Endpoint predefined filters

Selecting a Predefined Filter

To select a predefined filter:

1. From the PCoIP Management Console's top menu, click **ENDPOINTS**.
2. Select either the *GROUPED* or *UNGROUPED* tab.
3. Click the arrow to the side of the **FILTER** button.

4. Select a predefined filter from the drop-down list. Your active filter will display as a new dark gray filter icon next to the **FILTER** button, as shown next.



5. To return to the unfiltered endpoint list, click the x on the filter icon, or select **CLEAR FILTER** from the *FILTER* drop-down list.

Adding a Filter

To add a filter:

1. From the PCoIP Management Console's top menu, click **ENDPOINTS**.
2. Select either the *GROUPED* or *UNGROUPED* tab.
3. Click the **FILTER** button.
4. In the **ADD FILTER** dialog, use the drop-down menus to select your filter criteria. When you are finished, click the filter icon to the right.
5. You can repeat this step to add additional criteria to the filter, for example, **Power DOWN is Failed** and **Online Status is Online**. Multiple criteria in a filter are logically ANDed, not ORed.
6. Click **OK**.
7. To save your filter, select **SAVE ACTIVE FILTER** from the *FILTER* drop-down list on the main *ENDPOINTS* page.
8. Enter a unique name for the filter in the **SAVE ACTIVE FILTER** dialog, and click **SAVE**. When you click the **FILTER** button, your filter will now appear in the **Predefined Filters** list.

Managing Saved Filters

To manage saved filters:

1. From the PCoIP Management Console's top menu, click **ENDPOINTS**.
2. Select either the *GROUPED* or *UNGROUPED* tab.
3. Click the arrow to the side of the **FILTER** button and select **MANAGE SAVED FILTERS**.

4. Select a saved filter in the drop-down list and choose one of the following:

- Click **NEW** to add a new filter.
- Click **EDIT** to change the filter criteria.
- Click **DELETE** to delete the saved filter.

Exporting an Endpoint List


You can generate a comma-delimited file listing all endpoints, or all endpoints and columns, visible in the *ENDPOINTS* table. PCoIP Management Console administrators can use this file to import inventory information on their deployment into third-party inventory management systems.

 **Note: Exporting endpoints available on PCoIP Management Console Enterprise**

This feature is available for the PCoIP Management Console Enterprise only.

To generate a list of endpoints visible in an endpoints table:

1. From the PCoIP Management Console's top menu, click **ENDPOINTS**.
2. Select either the *GROUPED* or *UNGROUPED* tab.
3. Click **ENDPOINTS** and then select **EXPORT ALL** or **EXPORT CURRENTLY VIEWED**.
4. Follow the prompts to open or save the file.

 **Note: Change the file type to .csv**

If the exported file has no file type, change the file type to .csv to open it in Microsoft Excel as a comma-delimited file.

Managing the Console

Creating and Managing User Roles

Management Console allows the creation and management of user roles. Roles are created with a set of permissions that allow the administrator to configure which Management Console pages are accessible as well as what options within each page that are enabled. Each role can be finely tuned to a set of permissions that limit the access users have to configurable options within Management Console.

Default roles for users are applied to users depending on where the user is created.

- Management Console created users obtain the System Administrator role.
- IDP created users obtain the Administrator role by default. Management Console System Administrators can subsequently change this users role.
- Active Directory users can have roles assigned to them from roles assigned to there AD Groups.

Unlicensed Management Console

The DELETE and EDIT buttons are deactivated on unlicensed versions of Management Console.

The **SET PERMISSIONS** allow each Management Console page to be made available for use by the role. Permissions of **Show** and **Hide** can be set for each page. Once the SET PERMISSION is selected, the **Detail Permissions** become viewable and represent the configurable options within each Management Console page. Detailed permissions can be set to **Enable, Disable** or **Hide**.

When managing a new role, take the time to plan your administrative structure for PCoIP endpoints. If your organization requires changes to existing roles, you can easily do this by using the **EDIT** button and changing the permissions of each role. If role permissions are changed while a user of the role is logged in, the permissions take affect right away and will be seen when the user refreshes the Management Console page.

Active Directory Groups

- You can identify Active Directory Groups associated with a user by viewing the AD GROUP column in the ROLES AND PERMISSIONS tab on the Management Console AUTHENTICATION page.
- When an Active Directory user belongs to multiple Active Directory groups, the USER ROLE will take from the first group listed by Active Directory Server.
- When a new role has been applied to an Active Directory group or user, the changes will be reflected in all relative fields only after logged in users log out and back in again.

Creating a User Role

To create a user role, perform the following steps:

1. From the SETTINGS > AUTHENTICATION page, click the **ROLES AND PERMISSIONS** tab.
2. Click **ADD**.
3. Enter the **Role Name** (no spaces allowed) and then select the set of permissions specific to that role.
4. Click **SAVE**.

The newly created role will now be available to assign to any Management Console user.

Deleting Roles

Roles cannot be deleted if a user is associated with that role. You can only delete multiple roles at once if all the selected roles for deletion do not have a user associated with it.

Resetting User Roles

Administrators can reset user roles using the provided script in the scripts folder located at **/opt/teradici/scripts**. This may be required when a role is limiting users to a Management Console feature. Running of the script will provide full Management Console access back to the specific user role. Allow a few minutes for Management Console to reboot.

To reset a user role to provide full access

1. [SSH to the Management Console](#).

2. Browse to **/opt/teradici/scripts** and type the command:

```
sh reset_user_role.sh &lt;userName&gt;
```

Available role permissions

SET PERMISSION (Show or Hide)	Detailed Permissions (Show, Hide, Enable, Disable or Hide)
ENDPOINTS	<p>Permissions with Show or Hide</p> <ul style="list-style-type: none">• Grouped• Ungrouped <p>Permissions with Enable, Disable or Hide</p> <ul style="list-style-type: none">• Profile (Group only)<ul style="list-style-type: none">• Details• Change• Apply• Structure<ul style="list-style-type: none">• Move• Rename• New Group (Grouped only)• Remove Group (Grouped only)

SET PERMISSION (Show or Hide)	Detailed Permissions (Show, Hide, Enable, Disable or Hide)
	<ul style="list-style-type: none"> • Endpoints <ul style="list-style-type: none"> • Details • Power Down • Power reset • Reset to default • Clear management state • Export all • Export currently viewed • Delete • Get all settings • Request Certificate (Grouped only) • Endpoints Discovery
PROFILE	Permissions with Enable, Disable or Hide <ul style="list-style-type: none"> • New profile • Edit profile • Duplicate profile • Delete profile • Import File • Export File
SCHEDULE	Permissions with Show or Hide <ul style="list-style-type: none"> • Schedule tab • History tab Permissions with Enable, Disable or Hide <ul style="list-style-type: none"> • New schedule • Edit schedule • View schedule • Delete schedule • Global turn on or off schedules • Global turn on or off persistent configuration

SET PERMISSION (Show or Hide)	Detailed Permissions (Show, Hide, Enable, Disable or Hide)
ENDPOINT CERTIFICATES	Permissions with Enable, Disable or Hide <ul style="list-style-type: none">• New certificate rule• View certificate rule• Edit certificate rule• Delete certificate rule• Global turn on or off certificate rule
AUTO CONFIGURATION	Permissions with Enable, Disable or Hide <ul style="list-style-type: none">• New autoconfig rule• Edit autoconfig rule• Delete autoconfig rule• Global turn on or off autoconfig
SETTINGS	N/A

Managing Users

PCoIP Management Console Enterprise supports multiple concurrent administrative users. There are two default user roles that have different administrative capabilities—System Administrator and Administrator. Additionally, Management Console allows you to create new user roles with your own set of permissions. Roles can be applied to individual users that are created locally on the PCoIP Management Console, created by an integrated Identity Provider, or by the Active Directory group that an AD authenticated user is part of. A user with the **System Administrator** role can perform any function on the Management Console, while a user with the **Administrator** role can access everything except the SETTINGS pages. Roles that have been specially created will have their own set of permissions depending on what the administrator has chosen when making the role. For more information on roles, see [Managing User Roles](#).

Management Console Free - Roles

PCoIP Management Console Free supports one administrative user with the System Administrator role.


Users with any role can edit their own profile by clicking on their username at the top right of the Management Console screen.

System Administrators can manage PCoIP Management Console Enterprise user accounts by clicking **SETTINGS** from the top menu and then clicking the **AUTHENTICATION > USERS** tab.

The following tasks are performed from a user account with the System Administrator role.

Displaying User Information

The PCoIP Management Console Enterprise *AUTHENTICATION* page contains a table showing all the users that are currently configured to use PCoIP Management Console. This page is viewable by any System Administrator. PCoIP Management Console Enterprise allows you to create, edit, enable or disable one or more user accounts, assign different user roles, and view user logs to see user activity. You can also refine the list of users in the table by clicking **ENABLED USERS** to display only users with enabled accounts, or **ALL USERS** to display all user accounts. With the introduction of IDP support, you can view which of your users are maintained by an IDP and which are local to Management Console. Local users are recognized as DB users and IDP users are recognized as IDP.

Click the gear icon  to the right of the table to change the information you want to display in the table columns. Your customized settings are saved in your browser and will be used for any user who subsequently logs in from that browser.

AUTHENTICATION

USERS | ROLES AND PERMISSIONS | ACTIVE DIRECTORY CONFIGURATION | ACTIVE DIRECTORY GROUPS

NEW USER | EDIT | ENABLE | DISABLE | ENABLED USERS | ALL USERS | VIEW LOG

USERNAME	LAST NAME	FIRST NAME	ROLES	IN SESSION	TIME ZONE	ENABLED	DOMAIN NAME
admin	User	Admin	System Administrator	Yes	UTC	Yes	
user1	One	User 1	Administrator	No	UTC	Yes	
user2	Two	User 2	Administrator	No	UTC	Yes	
user3	Three	User 3	System Administrator	No	UTC	Yes	
user4	Four	User 4	Dashboard User	No	UTC	Yes	

PCoIP Management Console Enterprise AUTHENTICATION Page

PCoIP Management Console Free supports only one administrative user. Enabling and disabling this user is not supported in PCoIP Management Console Free.

teradici | PCoIP MANAGEMENT CONSOLE - FREE | Welcome back admin | LOGOUT

DASHBOARD | ENDPOINTS | PROFILE | SCHEDULE UPGRADE | AUTO CONFIGURATION UPGRADE | ENDPOINT CERTIFICATES UPGRADE | SETTINGS

You are using PCoIP Management Console Free. You may be eligible for the Enterprise edition included with new PCoIP Zero Client and PCoIP Remote Workstation Card purchases. Please contact sales@teradici.com or +1 604 628 1200.

AUTHENTICATION

USERS | ROLES AND PERMISSIONS | ACTIVE DIRECTORY CONFIGURATION | ACTIVE DIRECTORY GROUPS

This feature is enabled by PCoIP Management Console Enterprise. Please contact Teradici at sales@teradici.com or +1 604 628 1200 to ensure continued access to PCoIP Management Console Enterprise.

NEW USER | EDIT | ENABLE | DISABLE | ENABLED USERS | ALL USERS | VIEW LOG

USERNAME	LAST NAME	FIRST NAME	ROLES	IN SESSION	TIME ZONE	ENABLED
admin	User	Admin	System_Administrator	Yes	UTC	Yes

PCoIP Management Console Free AUTHENTICATION Page

Naming Criteria

User and Role names cannot contain white spaces. Spaces given in starting and ending of role name will be trimmed automatically while whitespaces between words will not be accepted.

Creating a New User Account in PCoIP Management Console Enterprise

Before creating a new user, make sure you have planned your administrative environment first. This may require that you have created specific roles for your users. See [Managing User Roles](#) for information on role permissions.

To create a new user account in PCoIP Management Console Enterprise:

1. From the PCoIP Management Console's top menu, click **SETTINGS**.
2. Ensure the **USERS** tab is active.
3. Click **NEW USER**.
4. Configure the parameters as follows:
 - **Role:** Select **Administrator** (limited), **System Administrator** (full access), (access is limited to the configured options selected when creating the role)
 - **Username:** Enter a unique name for the user.
 - **First Name:** Enter the user's first name.
 - **Last Name:** Enter the user's last name.
 - **Password:** Enter a password for the user.
 - **Confirm Password:** Enter the password again.
 - **Time Zone:** Select the user's local time zone from the drop-down list. Time zones in this list are presented in IANA format.

Active Directory Users

All Active Directory users have a default timezone of UTC which can be modified by a Management Console System Administrator after the user has logged in the first time.

- **Account Enabled:** Select to enable the account.

AUTHENTICATION / USERS / NEW

AUTHENTICATION

NAMING

SOFTWARE

SECURITY

DATABASE

LICENSE

REMOTE

VERSION

SAVE CANCEL

NEW USER

Role:

Username:

First Name:

Last Name:

Password:

Confirm Password:

Time Zone:

Account Enabled:

5. Click **SAVE**.

Enabled vs. not enabled for new users

If a new user is not enabled and the *MANAGEMENT CONSOLE USERS* page is set to show enabled users only, this user will not be visible in the table until the page is changed to show all users.

Editing a User Account

To edit a user account:

1. From the table on the *MANAGEMENT CONSOLE USERS* page, select the user account you wish to edit.
2. Click **EDIT**.
3. Change the user's settings as desired.

4. Click **SAVE**.

Enabled vs. not enabled for existing users

If an edited user is not enabled and the *MANAGEMENT CONSOLE USERS* page is set to show enabled users only, this user will not be visible in the table until the page is changed to show all users.

Enabling or Disabling User Accounts in PCoIP Management Console Enterprise

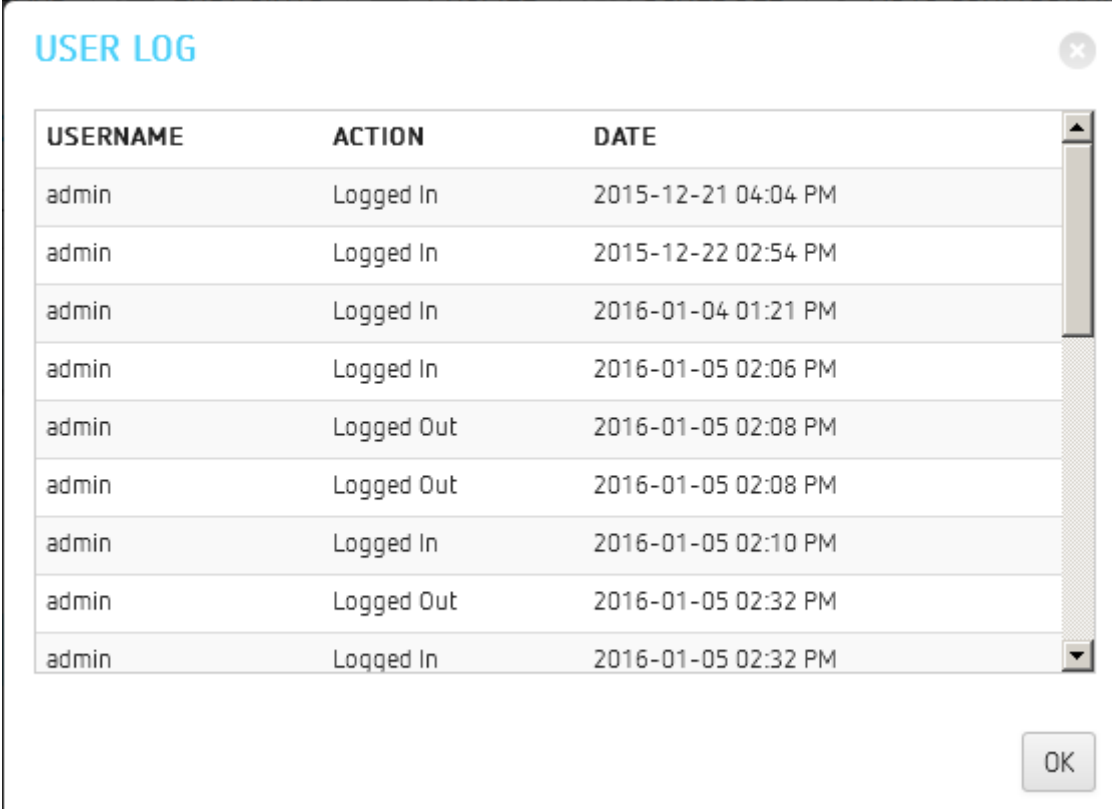
To enable or disable user accounts in PCoIP Management Console Enterprise:

1. From the table on the *MANAGEMENT CONSOLE USERS* page, select one or more users.
2. Use +Click to select contiguous elements and +Click to select non-contiguous elements.
3. Click **ENABLE** to enable the accounts or **DISABLE** to disable the accounts.

Viewing User Logs

To view user logs:

1. In the *MANAGEMENT CONSOLE USERS* page, click **VIEW LOG** to see the date and type of action for each user, as shown next:



USERNAME	ACTION	DATE
admin	Logged In	2015-12-21 04:04 PM
admin	Logged In	2015-12-22 02:54 PM
admin	Logged In	2016-01-04 01:21 PM
admin	Logged In	2016-01-05 02:06 PM
admin	Logged Out	2016-01-05 02:08 PM
admin	Logged Out	2016-01-05 02:08 PM
admin	Logged In	2016-01-05 02:10 PM
admin	Logged Out	2016-01-05 02:32 PM
admin	Logged In	2016-01-05 02:32 PM

OK

2. Scroll to the bottom of the list to see the most recent actions.
3. Click **OK** to close the user log.

Managing PCoIP Management Console Logs

The PCoIP Management Console **VERSION** page displays the version of the PCoIP Management Console that you are currently running, and also lets you select the level of diagnostic logging for the PCoIP Management Console. You can access this page by clicking **SETTINGS** from the PCoIP Management Console's top menu and then clicking the **VERSION** menu in the left pane.

Release version can be viewed on dashboard

The PCoIP Management Console release version is also displayed on the dashboard.

Locating the PCoIP Management Console's Log Files

All PCoIP Management Console logs are located in the PCoIP Management Console's virtual machine in its **/opt/teradici/log** directory. You can access these files by logging in to your PCoIP Management Console virtual machine console using vSphere Client. Log files are included in database archives.

The PCoIP Management Console's log directory contains the following files:

- **console.log**: Logs information about the PCoIP Management Console's front-end console. In this release, its level is set to Info and cannot be changed.
- **daemon.log**: Logs information about the PCoIP Management Console's back-end daemon. You can set a diagnostic log level for the PCoIP Management Console 2's daemon process.
- **daemon-startup.log**: Logs information about when the PCoIP Management Console's daemon starts up or stops.
- **daemon.log.< date >.gz**: Contains a gzip archive file for any daemon.log file that has reached 100 MB. These files are zipped to save space on the virtual machine.

Log File Size and Rotation

Both console and daemon logs are limited to 200 files—two uncompressed (up to 100 MB each) and 98 compressed (approximately 5 MB each). These files are rotated as needed.

Both console and daemon logs are limited to a set of 200 files. Out of this set, there are two uncompressed files that can grow to 100 MB each while the other 98 files are compressed and reach a size of approximately 5 MB each. These files are rotated as needed.

Linux system logs are rotated using default CentOS settings. The PCoIP Management Console does not configure Linux system logs.

Setting the PCoIP Management Console's Diagnostic Log Level

The PCoIP Management Console has five log levels that you can set. Troubleshooting an issue requires capturing all the details of an event in both the daemon and console logs. This is why setting the level for either daemon or the console adjusts both logs to the same level. By default the logging level is set to **INFO**.

The logging level can be set from the Management Console **SETTINGS > VERSION** page. Simply select the level of logging from the drop down field under MANAGEMENT CONSOLE DIAGNOSTIC LOGGING.

The five log levels are:

- **ERROR:** Only logs error messages. Error messages are logged events that occurred that were not supposed to have occurred.
- **WARN:** Only logs warning messages. Warning messages are logged events that may cause an issue in the future.
- **INFO:** Logs informational messages and events at a coarse-grained level.
- **DEBUG:** Logs deeper information that is useful for a debug application to troubleshoot.
- **TRACE:** Logs finer-grained informational messages and events. Trace should only be used under the direction of support for debugging issues.

Obtaining Management Console Logs

To obtain logs you first need to ensure SSH is enabled to allow access to the Management Console VM from applications like WinSCP or FileZilla. These applications can be downloaded from the Internet.

1. To enable SSH go to the VMware console screen for the Management Console VM, log in and type the following command:

```
sudo service sshd start
```

This will temporarily enable SSH access until the next reboot of the Management Console or you can stop the service by typing the following command:

```
sudo service sshd stop
```

Alternative method to access Management Console's VM console

See [Accessing the PCoIP Management Console Virtual Machine Console](#)

2. Next log into the Management Console VM using a utility such as WinSCP or FileZilla.
3. Change directories to /opt/teradici/log.
Normally you will be at the /home/admin folder.
4. Download both the **console.log** and the **daemon.log** files to be used for your investigation.

Management Console support

The **console.log** and the **daemon.log** files are required for Management Console investigations.

Creating and Managing PCoIP Management Console Certificates

This section contains information on how to manage your PCoIP Management Console certificates, including custom certificate requirements, creation, upload, update, and general management of certificates.

Important: Generate your own custom certificate and configuring endpoint discovery

The PCoIP Management Console is shipped with a default self-signed certificate. We strongly recommend that you generate your own certificates signed by a recognized certificate authority (CA), and then update both your PCoIP Management Console and your endpoints with the certificates **before configuring a discovery method or adding endpoints to your PCoIP Management Console.**

The following requirements and procedures will help guide you with creating a self-signed certificate for use with Management Console in a secure environment.

CUSTOM CERTIFICATE REQUIREMENTS

The certificate loaded onto the PCoIP Management Console for use as the PCoIP Management Console web interface certificate and for endpoint management must meet the following requirements:

- It must be a X.509 certificate in PEM format.
- Three PEM files are needed to install the certificate into the PCoIP Management Console:
 - The first file contains only the PCoIP Management Console public certificate. This is generally referred to as the leaf or server certificate.
 - The second file contains only the PCoIP Management Console certificate's private key. This is the private key that was generated when you made the certificate request.
 - The third file contains the PCoIP Management Console certificate's issuing chain, this chain will contain the first certificate and the root certificate and in some cases an intermediate certificate will be required (intermediate CAs, if applicable, and root CA).

Order of Issuing Chain

The certificate must have an entire verifiable chain. Any certificate used to sign the leaf certificate must be present in the chain.

Generally it will be the order of the certificates in the chain will be:

- a. Leaf/Server
- b. Intermediate
- c. Root Ca

- The certificate must be valid, meaning that the current time is after the 'not valid before' time and before the 'not valid after' time.
- Certificate RSA keys.
 - Management Console supports RSA keys or signing algorithm. (ECDSA is not currently supported)
 - Management Console also supports MD5 signatures.
 - The certificate's RSA key must be 1024 bit or greater. The recommended length is 2048 bits.
 - If the PCoIP Management Console certificate contains an Enhanced Key Usage extension, it must include the Server Authentication usage. It is also acceptable for the certificate to not include an Enhanced Key Usage extension.

Creating and Preparing Your Own Custom Certificate for PCoIP Management Console

This section demonstrates how to create your own certificate using OpenSSL and your own CA server. The following steps use the PCoIP Management Console VM and a Microsoft CA server but it can be done from any VM with OpenSSL and a CA server of your choice.

Examples use Teradici's PCoIP Management Console name

All the following examples use Teradici's PCoIP Management Console name. Replace any name with your own.

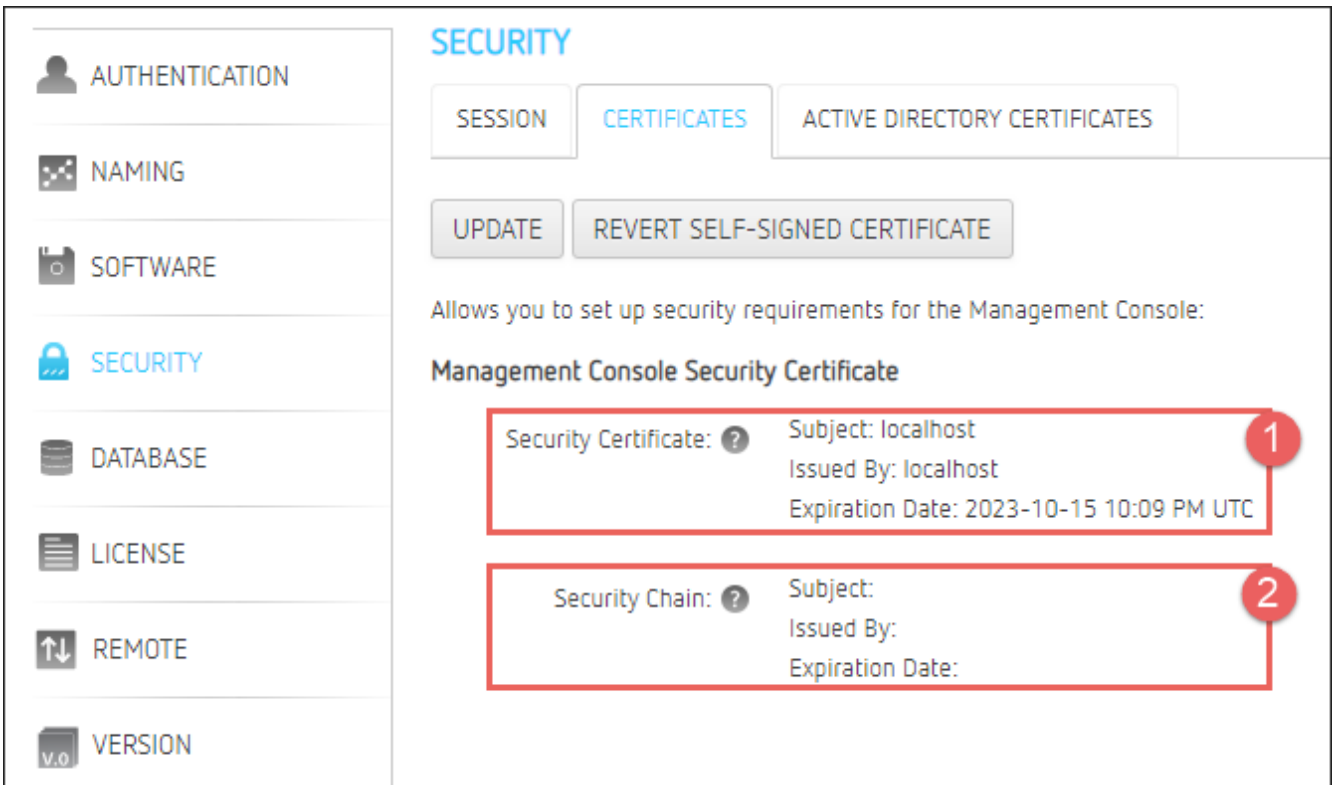
STEP 1 - ENSURE YOUR PCOIP MANAGEMENT CONSOLE DOES NOT HAVE ANY CUSTOM CERTIFICATES INSTALLED

To make sure you don't have custom certificates installed:

1. Log into the PCoIP Management Console web interface.
2. Go to **SETTINGS > SECURITY > CERTIFICATES** and ensure the default certificate is installed by confirming:
 - **Security Certificate** section *Subject* and *Issued By* are populated with **localhost**. (see #1)
 - **Security Chain** section is empty. (see #2)

i Custom Certificates

The Security Certificate and Security Chain fields of custom certificates will be populated by data that does not include localhost and will not have empty values.



STEP 2 - CONNECT AND ENABLE SSH TO CREATE YOUR CERTIFICATE SIGNING REQUEST VIA THE PCOIP MANAGEMENT CONSOLE VIRTUAL MACHINE

You will need to enable SSH prior to creating your certificate. See [Accessing the PCoIP Management Console Virtual Machine Console](#).

Run OpenSSL on a 'Trusted' computer

OpenSSL can be run on any 'Trusted' computer.

To create your Certificate Signing Request:

1. SSH into the PCoIP Management Console VM using your preferred SSH client. The example shown next uses PuTTY.
2. Run the OpenSSL command:

```
openssl req -out CSR.csr -new -newkey rsa:3072 -nodes -keyout mcertprivateKey.pem
```
3. You will get the following response and be asked a series of questions, as shown next:

```
[admin@semc230ga ~]$ openssl req -out mcert.csr -new -newkey rsa:3072 -nodes -keyout mcertprivateKey.pem
Generating a 3072 bit RSA private key
.....++
.....++
writing new private key to 'mcertprivateKey.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:US
State or Province Name (full name) []:CA
Locality Name (eg, city) [Default City]:LA
Organization Name (eg, company) [Default Company Ltd]:My Company
Organizational Unit Name (eg, section) []:IT
Common Name (eg, your name or your server's hostname) []:pcoipmc.my.domain
Email Address []:me@something.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:abc123
An optional company name []:What Ever
[admin@semc230ga ~]$
```

Modify each entry with your own detailed information. Descriptions are shown next:

- **Country Name:** Your country
- **State of Province Name:** Your state or province

- **Locality Name:** Your city
- **Organization Name:** Your company
- **Organizational Unit Name:** Your department
- **Common Name:** Your PCoIP Management Console Name (for example, hostname of PCoIP Management Console such as *se-pcoip-mc-200*)
- **Email Address:** you@yourcompany.com
- **A challenge password:** Your password
- **An optional company name:** Optional

4. Press .

5. Two files will be generated in the admin folder: **mccertprivateKey.pem** and **CSR.csr**.

6. Using a file management tool of your choice, copy the two files off of your PCoIP Management Console to a desktop of your choice.

STEP 3 - SUBMIT YOUR CERTIFICATE SIGNING REQUEST (CSR)

Caution: Certificates with Private Key

Do not send certificates containing your private key to the CA. A certificate with private key should not be sent outside your organization. The private key provides access to your secured resources and should remain under tight control.

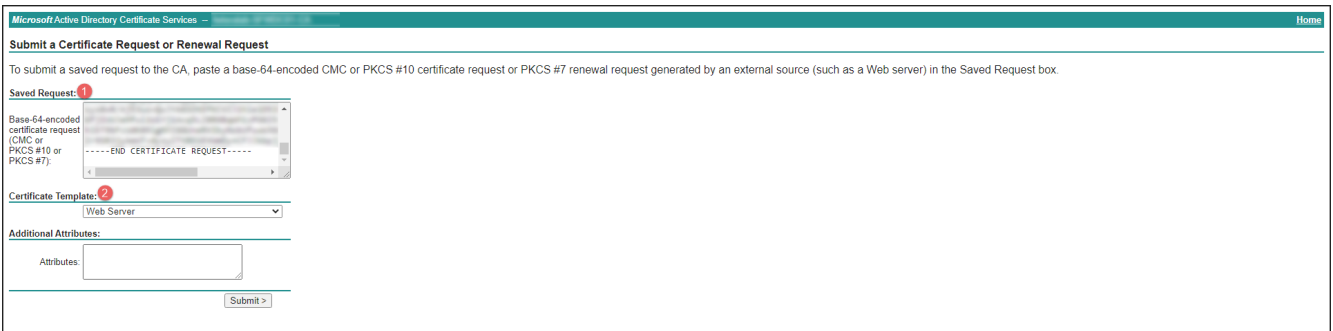
To submit your certificate signing request (CSR):

1. From your CA Server (this example is using a Microsoft CA server)
2. Select **Request a Certificate**.
3. Select **Advanced Certificate Request**.
4. From the VM/PC you saved your CSR.csr files, open the **CSR.csr** file in a text editor and copy the contents into the csr request field on your Certificate Authority (CA) server (<https://mycertserver.mydomain.local/certsrv>). The content will be Base 64 encoded.

Using text editor to copy the Certificate Signing Request

If CSR.csr does not open in your text editor, you can rename **CSR.csr** to **CSR.csr.txt** to open it in Notepad and copy the content.

5. For *Certificate Template*, select **Web Server**.
6. Do not add anything in the attributes box.
7. Click **Submit**.



Microsoft Active Directory Certificate Services – Home

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64 encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
-----END CERTIFICATE REQUEST-----
```

Certificate Template: Web Server

Additional Attributes:

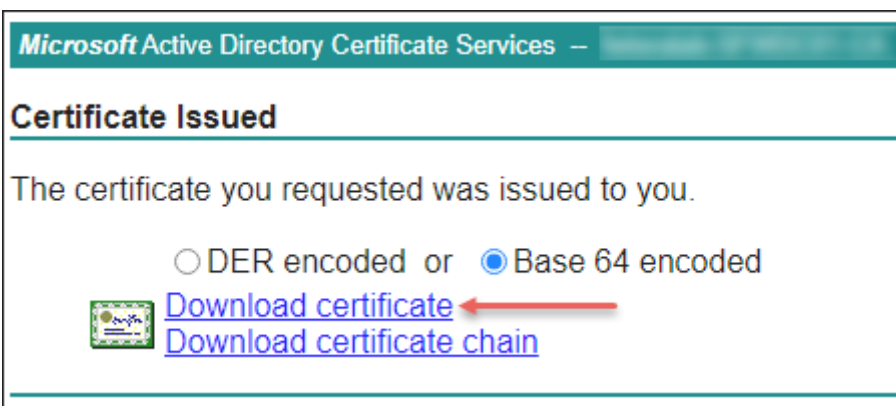
Attributes:

Submit >

STEP 4 - DOWNLOAD AND PREPARE THE CERTIFICATE

To download and prepare the certificate:

1. You can now download the created certificate from the CA server in Base 64 format. However, do not download the certificate chain as it is still in the wrong format. The certificate will show up as **certnew.cer**.




Microsoft Active Directory Certificate Services – Home

Certificate Issued

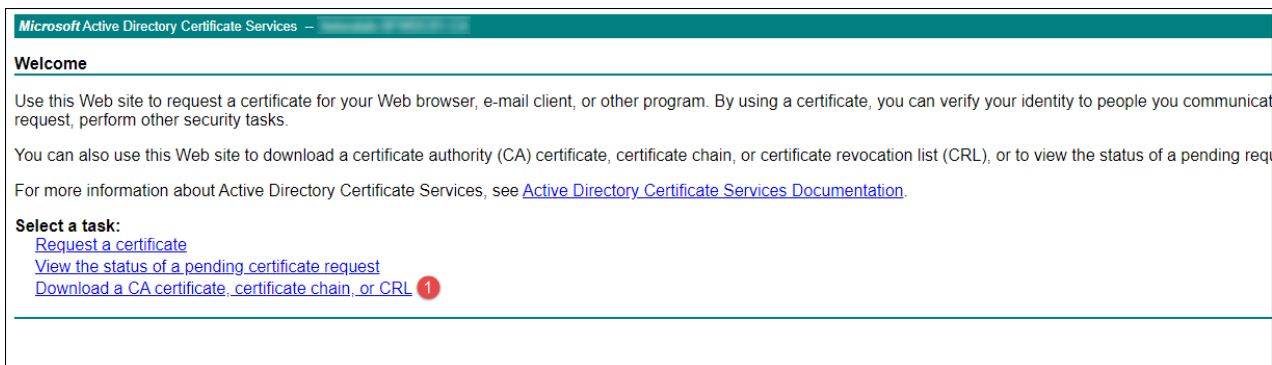
The certificate you requested was issued to you.

DER encoded or Base 64 encoded

 [Download certificate](#) ←

[Download certificate chain](#)

2. Rename **certnew.cer** to **certnew.pem**.
3. Get a copy of the CA certificate from the certificate server in Base64. The CA will return a certificate that will be used as part of the chain.
 - a. From the CA server home page click the **Download a CA certificate** link.



Microsoft Active Directory Certificate Services –

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with, request, perform other security tasks.

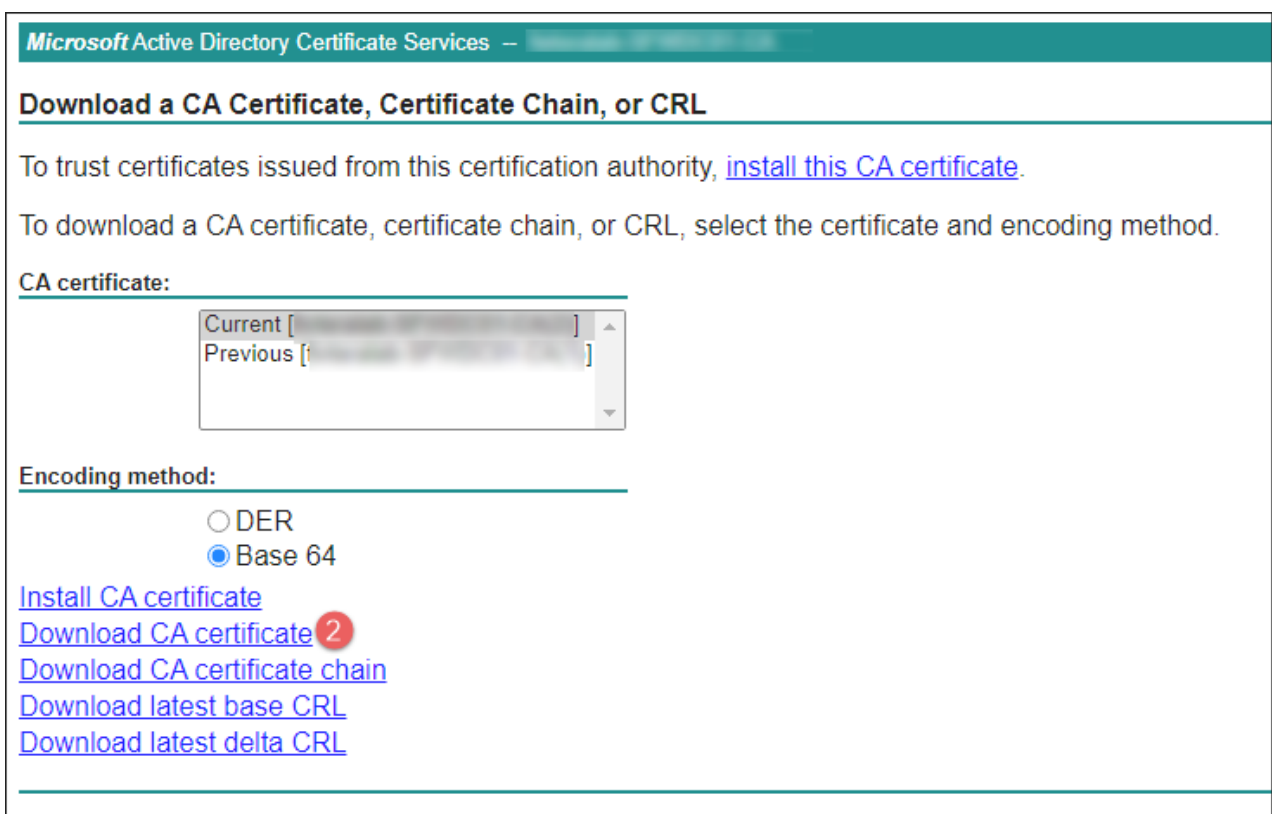
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

Select a task:

- [Request a certificate](#)
- [View the status of a pending certificate request](#)
- [Download a CA certificate, certificate chain, or CRL](#) 1

- b. Select Base64 and then click the **Download CA Certificate** link.



Microsoft Active Directory Certificate Services –

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, [install this CA certificate](#).

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.

CA certificate:

Current []
Previous []

Encoding method:

DER
 Base 64

[Install CA certificate](#)
[Download CA certificate](#) 2
[Download CA certificate chain](#)
[Download latest base CRL](#)
[Download latest delta CRL](#)

- c. Save the file as CA.cer.

- d. Rename the file to CA.pem.

4. Create a new certificate called **chain.pem** by combining the contents of **certnew.pem** with **CA.pem** using a text editor. (Occasionally the CA certificate may contain intermediate certificates which may need to be added to the chain)

To combine the certificates:

- Rename both certificate extensions to **.txt**.
- Using a text editor like Notepad, create a new file called **chain.txt** by combining the CA.txt content under the certnew.txt content.

c. Rename **chain.txt** to **chain.pem**.

 **Note: All certificates must be in PEM format**


All PCoIP Management Console certificates must be issued in PEM format.

5. Now, you will have three certificates:

- **certnew.pem**: The certificate returned from the CA
- **mccertprivateKey.pem**: The certificate from the OpenSSL command executed in Step 2 above.
- **chain.pem**: The combination of **certnew.pem** and **CA.pem**

Uploading Your Own PCoIP Management Console Certificates

This section explains how to upload your own certificates to the PCoIP Management Console and to endpoints that require a PCoIP Management Console certificate before discovery. If you wish to avoid browser certificate warnings when you access the PCoIP Management Console's web interface, you can also install the PCoIP Management Console certificate in your browser.

 **Important: Use the following sequence if you are installing certificates before adding endpoints**

If you are installing your own PCoIP Management Console certificates before you have added endpoints to the PCoIP Management Console, please follow the instructions in the order shown. If you need to update your PCoIP Management Console certificates for any reason after the PCoIP Management Console has already discovered your endpoints, the order of this procedure is slightly different. See [Updating PCoIP Management Console Certificates after Endpoint Discovery](#) for details.


The PCoIP Management Console requires the following certificates:

 **Note: All certificates must be in PEM format**

All PCoIP Management Console certificates must be issued in PEM format.

- **PCoIP Management Console server's certificate (*.pem):** Contains the public key. The PCoIP Management Console's public key certificate fingerprint is also used for DHCP/DNS endpoint discovery. (e.g. **certnew.pem** in this topic's example)
- **PCoIP Management Console server's private certificate (*.pem):** Contains the private key. (e.g. **mccertprivateKey.pem** in this topic's example)
- **PCoIP Management Console chain certificate (*.pem):** Contains the leaf/server certificate, any intermediate certificates, and the trusted root CA certificate used to issue PCoIP Management Console server certificates. (e.g. **chain.pem** in this topic's example)

STEP 1 - UPLOAD CUSTOM CERTIFICATE TO THE PCOIP MANAGEMENT CONSOLE VM

 **Note: Uploading Certificates causes the application to restart**

Uploading a certificate signs out all PCoIP Management Console users and causes the PCoIP Management Console application to restart. Users will not be able to access the PCoIP Management Console for one to two minutes.

To upload your certificates to the PCoIP Management Console VM:

1. From the PCoIP Management Console's top menu, click **SETTINGS**.
2. Click **SECURITY** in the left pane and select the **CERTIFICATES** tab in the **SECURITY** pane to the right.
3. Click **UPDATE**.
4. Click **SELECT CERTIFICATE**, select the PCoIP Management Console's public certificate file (eg. **certnew.pem**), and then click **NEXT**.

SECURITY CERTIFICATE UPLOAD

Update Certificate:

Security Certificate: Subject: hammer.fwteralab.local
Issued By: cms2-ca
Expiration Date: 2017-08-17 09:41 PM UTC

Security Key: ?

5. Click **SELECT KEY**, select the PCoIP Management Console's private certificate file (eg. **mccertprivateKey.pem**), and then click **NEXT**.

SECURITY CERTIFICATE UPLOAD

Update Certificate:

Security Certificate: Subject: hammer.fwteralab.local
Issued By: cms2-ca
Expiration Date: 2017-08-17 09:41 PM UTC

Security Chain: ?

6. Click **SELECT CHAIN**, select the PCoIP Management Console's chain certificate file (eg. **chain.pem**), and then click **NEXT**.

SECURITY CERTIFICATE UPLOAD

Update Certificate:

Security Certificate: Subject: hammer.fwteralab.local
Issued By: cms2-ca
Expiration Date: 2017-08-17 09:41 PM UTC

Security CA: Subject: fwteralab-SFWCA01-CA
Issued By: cms2-ca
Expiration Date: 2017-07-26 10:13 PM UTC

7. Click **Apply**.
8. Read the warning message and then click **APPLY**.
9. When the update process completes, click **LOGIN** to log in to the PCoIP Management Console again.

SECURITY CERTIFICATE UPLOAD

Applying Certificate Info:

Update process was completed with success

STEP 2 - UPDATE YOUR DHCP/DNS SERVER WITH THE PCOIP MANAGEMENT CONSOLE SERVER'S PUBLIC CERTIFICATE FINGERPRINT

If your DHCP or DNS server is configured to provision endpoints with the PCoIP Management Console's public certificate fingerprint, this information must be updated next. You can update your server with your PCoIP Management Console certificate fingerprint as follows:

- **DHCP server:** Edit the **EBM X.509 SHA-256 fingerprint** option for the PCoIP Endpoint option class. For details, see [Configuring DHCP Options](#).
- **DNS server:** Edit the **EBM-SHA-256-fingerprint** DNS text record. For details, see [Adding a DNS TXT Record](#).

STEP 3 - UPLOAD PCOIP MANAGEMENT CONSOLE CERTIFICATE TO YOUR ENDPOINTS

If your endpoints are configured with a discovery method and security level that require them to have a PCoIP Management Console certificate in their trusted certificate store before they can connect to the PCoIP Management Console, you can either upload the PCoIP Management Console certificate for a group of endpoints using a PCoIP Management Console profile, or you can upload the PCoIP Management Console certificate locally using each endpoint's AWI. Depending on your security requirements, you can upload either a PCoIP Management Console issuer certificate (that is, the root CA certificate (or intermediate certificate) that was used to issue a PCoIP Management Console server certificate) or you can upload the PCoIP Management Console server's public key certificate.

To upload the PCoIP Management Console certificate for a group of endpoints using PCoIP Management Console:

1. Ensure that all ungrouped endpoints are moved from the ungrouped category into a group.

Possible modifications due to your deployment

Depending on your site configuration, this may require modifications to your DHCP options or DNS SRV records, or it may require disabling persistent auto-configuration or placing the endpoints into a segregated network with a new PCoIP Management Console.

2. Ensure that every group (or at least one parent group) is associated with a profile.
3. Update all existing profiles to push the new certificate to endpoints. For each profile:
 - a. From the PCoIP Management Console's top menu click **PROFILE**.
 - b. Click the **NEW PROFILE** button.

- c. Enter a name and description for the profile in their respective fields.
- d. Click the **+** tab beside the **SETTINGS OVERVIEW** tab and then select the appropriate type of profile (e.g. TERA2: CLIENT [DUAL], TERA2 HOST [QUAD]) that applies to your endpoints and click **ADD**.
- e. In the *SOFTWARE* section, ensure the correct **Firmware Version** is selected for your endpoints.
- f. Click **SECURITY** in the left navigation pane, scroll down to **Certificate Store**, and select **Set in Profile**.
- g. Click **Add New**, browse to your PCoIP Management Console public key certificate, highlight it and click **Open**. (This certificate must have a .pem extension)
- h. Click **Upload**.
- i. Ensure the correct usage type is selected for any specialized certificates such as 802.1x and Syslog.

Certificate Usage type Limitation

Only one specialized usage type can be selected in one profile. Any subsequent certificate selected for the same usage type will cause the previous certificate to change usage type to **No Usage**.

802.1x and Syslog options are disabled when you upload certificates without a private key

- j. Click **SAVE** at the top of the page.
- k. [Apply the profile](#) immediately or [create a schedule](#) to update your group(s) with the profile.

Installing the PCoIP Management Console Certificate in Your Browser

If you wish to avoid browser certificate warnings when you access the PCoIP Management Console's web interface, you can install a PCoIP Management Console certificate in your browser. You can use either a PCoIP Management Console issuer certificate or the PCoIP Management Console server's public key certificate. For more information, see [How do I get the fix the unsecure browser warning when accessing the Management Console 2.x and 3.x web interface? \(1406\)](#)

Reverting to the Default Self-signed PCoIP Management Console Certificate

Note: Reverting the default certificate disables all users and causes application to restart

Reverting the PCoIP Management Console to its self-signed certificate disables all PCoIP Management Console users and causes the PCoIP Management Console application to restart. Users will not be able to access the PCoIP Management Console for one to two minutes.

To revert to the default PCoIP Management Console certificate:


1. From the PCoIP Management Console's top menu, click **SETTINGS**.
2. Click **SECURITY** in the left pane.
3. Click **REVERT SELF-SIGNED CERTIFICATE**.
4. Read the warning message and then click **APPLY**.



5. When the update process completes, click **LOGIN** to log in to the PCoIP Management Console again.

Updating PCoIP Management Console Certificates after Endpoint Discovery

The steps provided next are for updating your PCoIP Management Console certificates if your certificate expires, or if you need to update your PCoIP Management Console certificate for any other reason.

 **Note: Update endpoints with new certificate before updating the PCoIP Management Console certificates**

It is important to update endpoints with their new PCoIP Management Console certificate before you update the PCoIP Management Console's certificates. Otherwise, your endpoints will not be able to trust the PCoIP Management Console, and your profile update will fail when you attempt to apply it.

STEP 1 - UPDATE ENDPOINTS WITH THE NEW PCOIP MANAGEMENT CONSOLE CERTIFICATE

 **Note: All certificates must be in PEM format**

All PCoIP Management Console certificates must be issued in PEM format.

To upload the PCoIP Management Console certificate for a group of endpoints using PCoIP Management Console:

1. Ensure that all ungrouped endpoints are moved from the ungrouped category into a group.

 **Possible modifications due to your deployment**

Depending on your site configuration, this may require modifications to your DHCP options or DNS SRV records, or it may require disabling persistent auto-configuration or placing the endpoints into a segregated network with a new PCoIP Management Console.

2. Ensure that every group (or at least one parent group) is associated with a profile.

3. Update all existing profiles to push the new certificate to endpoints. For each profile:
 - a. From the PCoIP Management Console's top menu click **PROFILE**.
 - b. Click the **NEW PROFILE** button.
 - c. Enter a name and description for the profile in their respective fields.
 - d. Click the **+** tab beside the **SETTINGS OVERVIEW** tab and then select the appropriate type of profile (e.g. TERA2: CLIENT [DUAL], TERA2 HOST [QUAD]) that applies to your endpoints and click **ADD**.
 - e. In the *SOFTWARE* section, ensure the correct **Firmware Version** is selected for your endpoints.
 - f. Click **SECURITY** in the left navigation pane, scroll down to **Certificate Store**, and select **Set in Profile**.
 - g. Click **Add New**, browse to your PCoIP Management Console public key certificate, highlight it and click **Open**. (This certificate must have a *.pem* extension)
 - h. Click **Upload**.
 - i. Ensure the correct usage type is selected for any specialized certificates such as 802.1x and Syslog.

Certificate Usage type Limitation

Only one specialized usage type can be selected in one profile. Any subsequent certificate selected for the same usage type will cause the previous certificate to change usage type to **No Usage**.

802.1x and Syslog options are disabled when you upload certificates without a private key

- j. Click **SAVE** at the top of the page.
- k. [Apply the profile](#) immediately or [create a schedule](#) to update your group(s) with the profile.

Tip: Using the Tera2 Endpoint AWI

If a Tera2 endpoint's AWI is enabled, you can directly access it via the Management Console **ENDPOINT DETAILS** page and selecting the **WEB INTERFACE** button. This will allow you to directly manage a single Tera2 endpoint if required.

From the Management Console homepage:

1. Select **ENDPOINTS**.
2. Find your endpoint in the **GROUPED** or **UNGROUPED** tab and highlight it.
3. Select **ENDPOINTS > DETAILS**.
4. Select the **WEB INTERFACE** button.

For more information about using the endpoint AWI after selecting the WEB INTERFACE button see [Remote Workstation Card Firmware Administrators' Guide](#) or [PCoIP Zero Client Firmware Administrators' Guide](#).

STEP 2 - UPLOAD CUSTOM CERTIFICATE TO THE PCOIP MANAGEMENT CONSOLE VM

Note: Uploading Certificates causes the application to restart

Uploading a certificate signs out all PCoIP Management Console users and causes the PCoIP Management Console application to restart. Users will not be able to access the PCoIP Management Console for one to two minutes.

To upload your certificates to the PCoIP Management Console VM:

1. From the PCoIP Management Console's top menu, click **SETTINGS**.
2. Click **SECURITY** in the left pane and select the **CERTIFICATES** tab in the **SECURITY** pane to the right.
3. Click **UPDATE**.
4. Click **SELECT CERTIFICATE**, select the PCoIP Management Console's public certificate file (eg. **certnew.pem**), and then click **NEXT**.

SECURITY CERTIFICATE UPLOAD

Update Certificate:

Security Certificate: Subject: hammer.fwteralab.local
Issued By: cms2-ca
Expiration Date: 2017-08-17 09:41 PM UTC

Security Key: ?

5. Click **SELECT KEY**, select the PCoIP Management Console's private certificate file (eg. **mccertprivateKey.pem**), and then click **NEXT**.

SECURITY CERTIFICATE UPLOAD

Update Certificate:

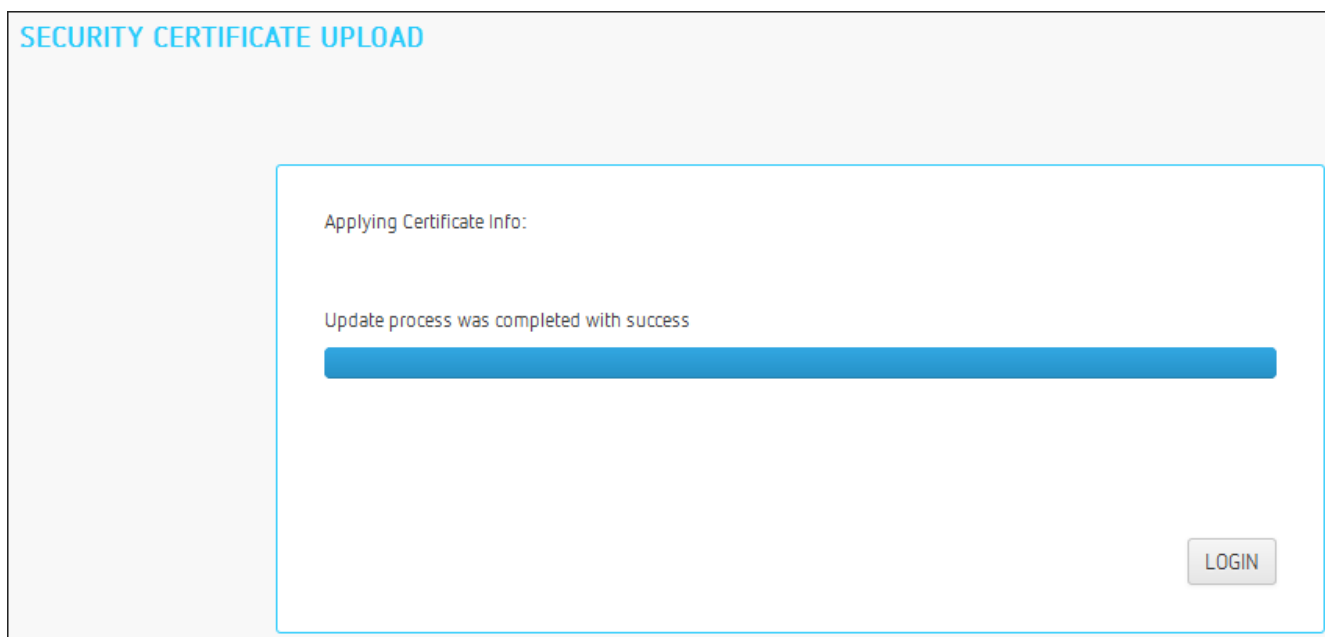
Security Certificate: Subject: hammer.fwteralab.local
Issued By: cms2-ca
Expiration Date: 2017-08-17 09:41 PM UTC

Security Chain: ?

6. Click **SELECT CHAIN**, select the PCoIP Management Console's chain certificate file (eg. **chain.pem**), and then click **NEXT**.



7. Click **Apply**.
8. Read the warning message and then click **APPLY**.
9. When the update process completes, click **LOGIN** to log in to the PCoIP Management Console again.



STEP 3 - UPDATE YOUR DHCP OR DNS SERVER

If your DHCP or DNS server is configured to provision endpoints with the PCoIP Management Console's public key certificate fingerprint, this information must be updated next. You can update your server with your PCoIP Management Console certificate fingerprint as follows:

- **DHCP server:** Edit the **EBM X.509 SHA-256 fingerprint** option for the PCoIP Endpoint option class. For details, see [Configuring DHCP Options](#).
- **DNS server:** Edit the **EBM-SHA-256-fingerprint** DNS text record. For details, see Adding a [DNS TXT Record](#).

Uploading the PCoIP Management Console Certificate to an Endpoint

If your endpoints are configured with a discovery method and security level that require them to have a PCoIP Management Console certificate in their trusted certificate store before they can connect to the PCoIP Management Console, you can either upload the PCoIP Management Console certificate to a group of endpoints using a PCoIP Management Console profile, or you can upload the PCoIP Management Console certificate locally using each endpoint's AWI. Depending on your security requirements, you can upload either a PCoIP Management Console issuer certificate (that is, the root CA certificate (or intermediate certificate) that was used to issue a PCoIP Management Console server certificate) or you can upload the PCoIP Management Console server's public key certificate.

For information on PCoIP Management Console certificates, see [Managing PCoIP Management Console Certificates](#).

Uploading PCoIP Management Console Certificates to Endpoints

 **Note: All certificates must be in PEM format**

All PCoIP Management Console certificates must be issued in PEM format.

To upload the PCoIP Management Console certificate for a group of endpoints using PCoIP Management Console:

1. Ensure that all ungrouped endpoints are moved from the ungrouped category into a group.

 **Possible modifications due to your deployment**

Depending on your site configuration, this may require modifications to your DHCP options or DNS SRV records, or it may require disabling persistent auto-configuration or placing the endpoints into a segregated network with a new PCoIP Management Console.

2. Ensure that every group (or at least one parent group) is associated with a profile.
3. Update all existing profiles to push the new certificate to endpoints. For each profile:
 - a. From the PCoIP Management Console's top menu click **PROFILE**.
 - b. Click the **NEW PROFILE** button.

- c. Enter a name and description for the profile in their respective fields.
- d. Click the **+** tab beside the **SETTINGS OVERVIEW** tab and then select the appropriate type of profile (e.g. TERA2: CLIENT [DUAL], TERA2 HOST [QUAD]) that applies to your endpoints and click **ADD**.
- e. In the *SOFTWARE* section, ensure the correct **Firmware Version** is selected for your endpoints.
- f. Click **SECURITY** in the left navigation pane, scroll down to **Certificate Store**, and select **Set in Profile**.
- g. Click **Add New**, browse to your PCoIP Management Console public key certificate, highlight it and click **Open**. (This certificate must have a *.pem* extension)
- h. Click **Upload**.
- i. Ensure the correct usage type is selected for any specialized certificates such as 802.1x and Syslog.

Certificate Usage type Limitation

Only one specialized usage type can be selected in one profile. Any subsequent certificate selected for the same usage type will cause the previous certificate to change usage type to **No Usage**.

802.1x and Syslog options are disabled when you upload certificates without a private key

- j. Click **SAVE** at the top of the page.
- k. [Apply the profile](#) immediately or [create a schedule](#) to update your group(s) with the profile.

Tip: Using the Tera2 Endpoint AWI

If a Tera2 endpoint's AWI is enabled, you can directly access it via the Management Console **ENDPOINT DETAILS** page and selecting the **WEB INTERFACE** button. This will allow you to directly manage a single Tera2 endpoint if required.

From the Management Console homepage:

1. Select **ENDPOINTS**.
2. Find your endpoint in the **GROUPED** or **UNGROUPED** tab and highlight it.
3. Select **ENDPOINTS > DETAILS**.
4. Select the **WEB INTERFACE** button.

For more information about using the endpoint AWI after selecting the WEB INTERFACE button see [Remote Workstation Card Firmware Administrators' Guide](#) or [PCoIP Zero Client Firmware Administrators' Guide](#).

Configuring the Console Settings

Configuring PCoIP Management Console Session Timeout (Enterprise)

PCoIP Management Console Enterprise allows administrators to set a session timeout for the Web UI of 10, 30, 60, or 120 minutes as well as disabling the session time out by using Never which is not recommended. This setting is located on the security page (**SETTINGS > SECURITY**). Once a period of inactivity reaches the set time, the administrator will be logged out of PCoIP Management Console Enterprise.

Configuring PCoIP Management Console web UI Time Zone

Important: PCoIP Management Console operates in Coordinated Universal Time (UTC)

The PCoIP Management Console virtual machine operates in Coordinated Universal Time (UTC) and *must not* be changed.

If you are in a different time zone, you can change the PCoIP Management Console's web interface to display your local time to make it more convenient to create schedules and view time-related information. The PCoIP Management Console will perform the conversion and run the schedule using your time.

To configure your local time zone:

1. Log in to the PCoIP Management Console web interface.
2. Click **SETTINGS** and then **AUTHENTICATION** to display the *MANAGEMENT CONSOLE USERS* window.
3. In the *USERNAME* column, select your user account and then click **EDIT**.
4. In the *Time Zone* field, select your local time zone from the drop-down list.
5. Click **SAVE**.

Default CentOS Configuration for PCoIP Management Console

After installation, the CentOS operating system on which your PCoIP Management Console virtual appliance runs has the following default configuration. For further recommendations on how to improve security for your PCoIP Management Console, see [Setting Up Security](#).

Default PCoIP Management Console CentOS Configuration

Configuration	Description
Installed packages	<p>The following applications have been installed on the CentOS operating system for PCoIP Management Console:</p> <ul style="list-style-type: none"> • Text editor (from the CentOS repo): vim • man • python-argparse • redhat-lsb-core • Python (from the Python project) • Java Platform: Openjdk-1.8 configured with weak ciphers and hashes disabled • PostgreSQL-server =14.8 (from the PostgreSQL project) • PostgreSQL-contrib =14.8 • openssl • epel-release <p>Important: Dependencies</p> <p>Installed packages may have included other additional dependencies.</p>
PCoIP Management Console users	<p>Note: Root user is not used for PCoIP Management Console administration</p> <p>For security reasons, the root user is not used for PCoIP Management Console administration. This user account has a large, randomly-generated password that is not published. It is critical to change this password immediately after installing your PCoIP Management Console.</p> <p>The following PCoIP Management Console virtual machine users are created by default:</p> <ul style="list-style-type: none"> • admin: Default administrative user; has sudo privileges; default password is ManagementConsole2015. Note: To secure your PCoIP Management Console, it is critical to change this password immediately after installing the PCoIP Management Console. • mconsole: No login shell; can use restricted sudo to manage PCoIP Management Console web UI components; has no password. • mcdemon: No login shell; has no password. • postgres: Has login shell due to PostgreSQL limitations; has no password.
Security	<p>Security-Enhanced Linux (SELinux) is enabled with a default configuration.</p>
	<p>The PCoIP Management Console SSH server is disabled by default. You can use vSphere Client to access the PCoIP Management Console's virtual machine console.</p> <p>Note: SSH access for the admin user</p> <p>Although the PCoIP Management Console permits you to re-enable the</p>

Configuration	Description
	<p>SSH server (temporarily or permanently), for security reasons it only allows SSH access for the admin user while the SSH server is enabled.</p>
	<p>Default firewall port settings are as follows:</p> <ul style="list-style-type: none"> • Port 22: Allow incoming SSH connections on TCP port 22. • Ports 80, 443, 8080 and 8443: Allow incoming web UI connection on TCP ports 80, 443, 8080, and 8443. The firewall redirects port 80 to port 8080 and port 443 to port 8443. The web UI server listens for HTTP connections on port 8080 and HTTPS connections on port 8443. • Port 5172: Allow incoming PCoIP Management Protocol connections on TCP port 5172. • Allow all outgoing traffic.
Open file limit	The maximum number of open files for all OS processes is 65,535.
IPv6	IPv6 is disabled.
NTP	By default, CentOS 7.x uses chrony as an NTP client. NTP traffic to outside sources can be found by entering the <code>chronyc sources -v</code> command to provide a verbose listing of NTP servers chrony is syncing too. Configuration changes can be made by editing the <code>/etc/chrony.conf</code> file. See Chrony Configuration for further information.
PCoIP Management Console directories and scripts	<p>The following scripts and files are included on the PCoIP Management Console virtual machine:</p> <p>/opt/teradici/scripts</p> <ul style="list-style-type: none"> • enable_admin.sh: Enables the PCoIP Management Console's web UI admin user. This is useful if you disable the admin Web UI account from PCoIP Management Console Enterprise and subsequently transition to PCoIP Management Console Free without re-enabling the account from the web UI. In this situation, you must run this script from the PCoIP Management Console's virtual machine console before the user can log in to the [PCoIP Management Console web UI]. • reset_admin_password.sh: Reverts the password for the PCoIP Management Console's web interface admin user to its default value (password). This is useful if the password to the admin user web UI account becomes lost and the user needs a way to get logged in again. • remove_ldaps_certificate.sh: Removes the uploaded Active Directory Certificate • import_ldaps_certificate.sh: Imports and activates the uploaded Active Directory Certificate <p>/opt/teradici/database/legacy/migration_script</p> <ul style="list-style-type: none"> • migrate_mc1_profile.sh: Imports individual PCoIP Management Console 1 profiles into your PCoIP Management Console release 2 or later. <p>/opt/teradici/log</p> <p>Contains PCoIP Management console log files.</p>

Changing the Default Network Configuration

The PCoIP Management Console virtual machine requires Linux command knowledge or a network configuration tool such as NetworkManager-tui (textual user interface) to [assign a static IP address](#) or change the PCoIP Management Console's default network configuration. The following example shows how to make this type of change using NetworkManager-tui. If your host Linux computer does not have this tool, you can install it using the following command `sudo yum install NetworkManager-tui`. Do NOT modify the *Hostname* configuration with this tool. The Management Console host name should be set correctly in DNS.

Resetting the network interface for changes to take affect immediately

The command line method to restart the network no longer applies IP configuration changes. Using nmtui to activate and deactivate the network interface is the recommended way for your IP configuration changes to take affect immediately. This is user friendly and works seamlessly for AMI, RPM and OVA implementations of Management Console.

Tip: Ensure you have correct DNS A and DNS PTR records set

Before you run the Network Configuration Tool, be sure to set the correct DNS A record and DNS PTR record in your DNS server for the PCoIP Management Console. If the records are already set, ensure you use the same IP address associated with the DNS records.

Note: Give PCoIP Management Console a fixed IP address

We recommend that you give the PCoIP Management Console a fixed "static" IP address, either through a DHCP reservation or by Assigning a Static IP Address using the PCoIP Management Console's network configuration tool. If a PCoIP Management Console is configured using DHCP and the IP address of the PCoIP Management Console changes, the endpoints it manages will be unable to connect to it.

Launching the PCoIP Management Console Network Configuration Tool

To launch the network configuration tool:

1. Log in to the PCoIP Management Console virtual machine console. For instructions, see [Accessing the PCoIP Management Console Virtual Machine Console](#).
2. Type the following command at the command line to launch the network configuration tool:

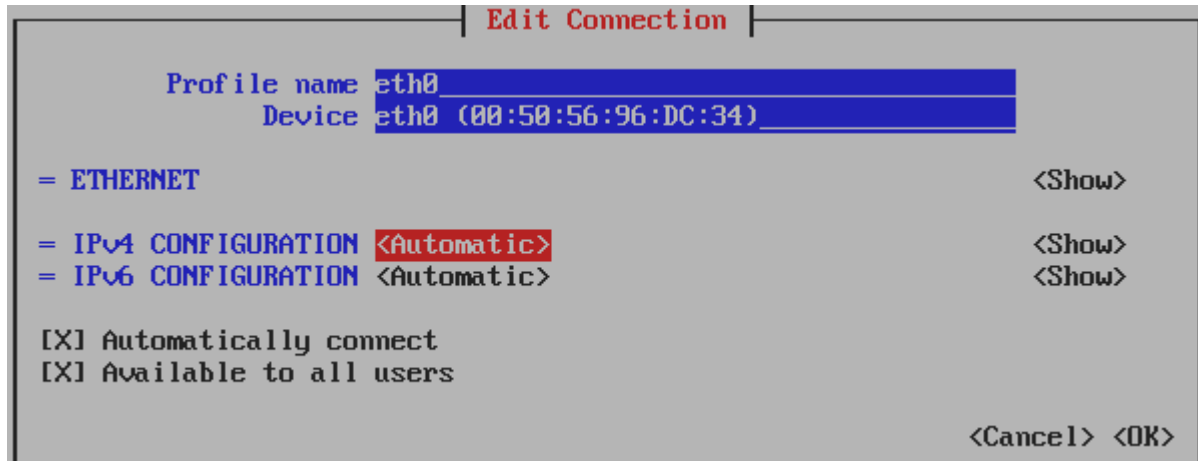
```
sudo nmtui
```



Network Manager Configuration Tool

Info: Default configuration

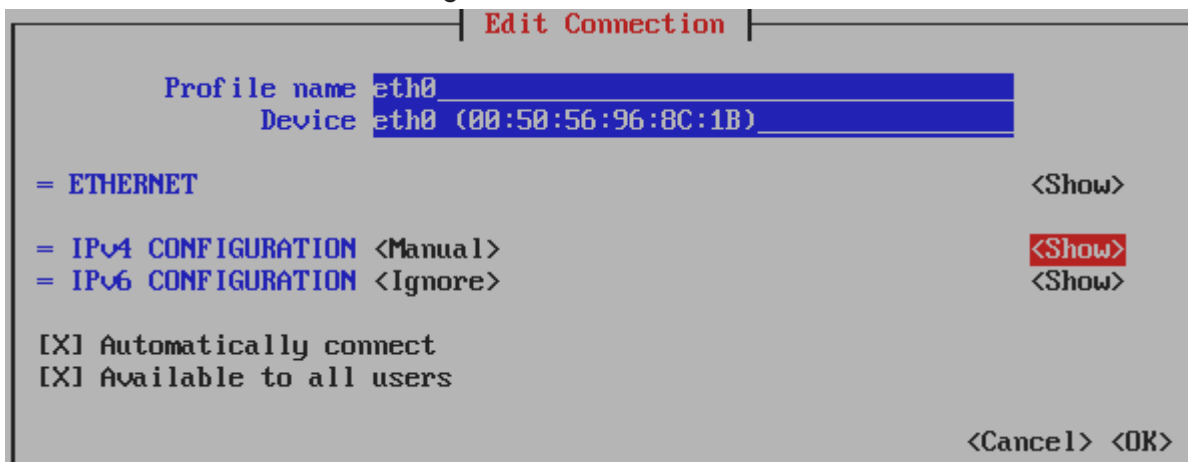
The default configuration for IPv4 is DHCP based, identified by **<Automatic>**.



Tip: Configurable Interactive Elements

Angle brackets contain interactive elements that can provide further selections, and OK or Cancel changes. Use the keyboard Tab or arrow keys to move between interactive elements.

Select to access additional configurable elements.



Assigning a Static IP Address

To assign a static IP address using the PCoIP Management Console's network configuration tool:

1. Launch the PCoIP Management Console's network configuration tool.

```
sudo nmtui
```

2. Select **Edit a connection**.
3. Select your correct connection such as **wired connection 1** (for RPM installs it may be referred to as **eth0**) and press the key.

Note: Shown next are example IP addresses

The IP addresses shown next are for example purposes only. Enter your own information.

Important: Correctly identifying subnets

Addresses and subnets must be correctly defined otherwise the PCoIP Management Console will not operate. Subnets are defined through the slash notation used in the Addresses field. The example of /24 represents 255.255.255.0. Your network may use different subnet sizes.

4. To access configurable parameters, tab to and configure your IPv4/IPv6 parameters:

- **IPv4/IPv6 CONFIGURATION:** Set to **Manual** for a static IP configuration. Be sure to enter your correct network details, see screen shot below.
- **Addresses:** Enter the IP address you selected for your Management Console, ensuring you use the appropriate slash notation to define your subnet mask.
- **Gateway:** Enter your default gateway IP address for the Management Console's network.
- **DNS servers:** Enter the IP address of your DNS servers.
- **Search domains:** Enter the domains used in your deployment in the format of mydomain.local.
- **Routing:** Enter your networks routing requirements.

Edit Connection

Profile name eth0
Device eth0 (00:50:56:9D:2C:17)

= ETHERNET <Show>

■ IPv4 CONFIGURATION <Manual> <Hide>

Addresses 192.168.100.10/24 <Remove>
<Add...>

Gateway 192.168.100.1

DNS servers 192.168.100.50 <Remove>
192.168.100.70 <Remove>
<Add...>

Search domains mydomain.local <Remove>
<Add...>

Routing (No custom routes) <Edit...>

Never use this network for default route
 Ignore automatically obtained routes

Require IPv4 addressing for this connection

= IPv6 CONFIGURATION <Ignore> <Show>

Automatically connect
 Available to all users

<Cancel> **<OK>**

5. Set manual address:

- Tab to **IPv4 CONFIGURATION** and change Automatic to Disabled if setting a static IPv6 address.
- Tab to **IPv6 CONFIGURATION** and change Automatic to Ignore if setting a static IPv4 address.

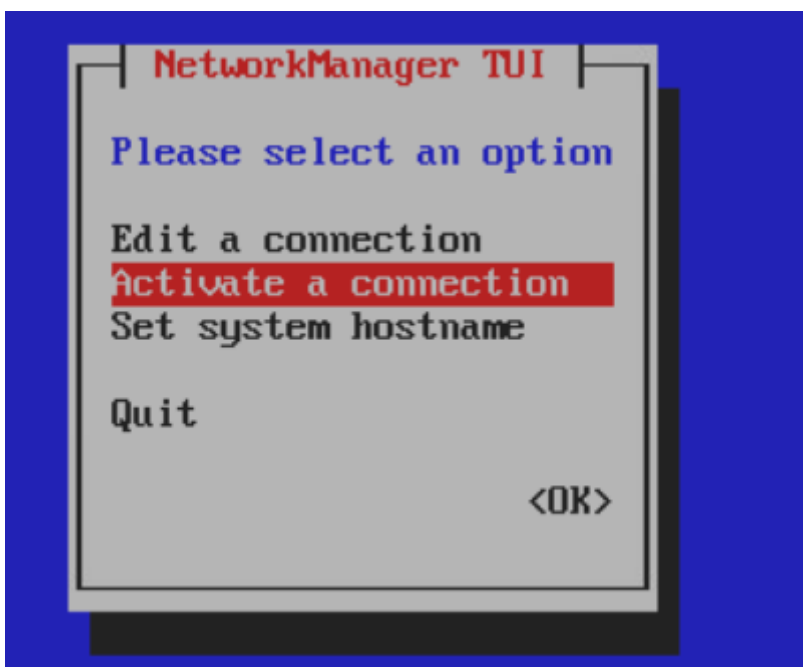
6. Tab to **<OK>** and press .

7. Tab to **<Back>** and press to get to the main screen of the network configuration tool.

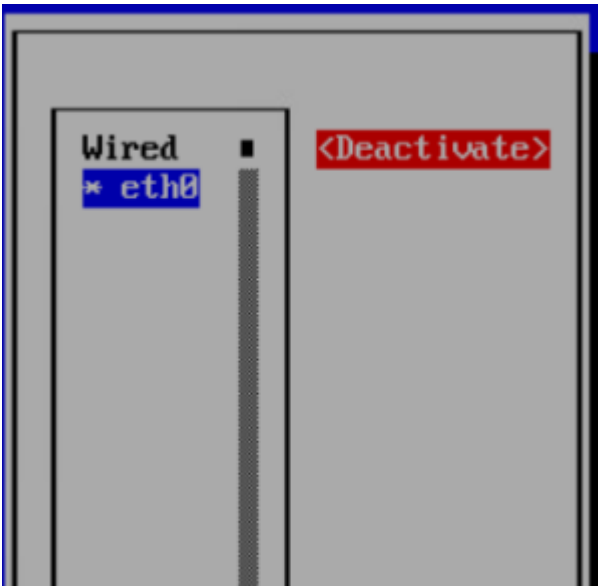
8. Reactivate your network so your changes take affect.

a. Tab and highlight **Activate a connection** and press .

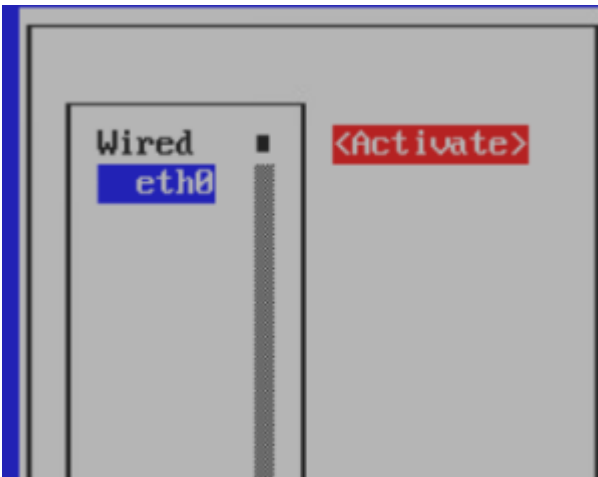
This brings you to the next screen which will allow you to highlight the connection you made your changes to.



a. With the connection you made your changes to highlighted in above steps such as **wired connection 1** or **eth0**, ensure **<Deactivate>** is highlighted and press to deactivate your connection.



- a. Ensure **<Activate>** is highlighted and press to activate your connection.




9. Tab to **<Back>** and press to get to the main screen of the network configuration tool.
10. Highlight **Quit** and tab to **OK** to exit nmtui.

Configuring an Endpoint Manager Manually from an Endpoint

For environments that do not use automatic DHCP or DNS discovery, you can manually configure each PCoIP Zero Client with the IP address or FQDN of the PCoIP Management Console to which it should connect. The endpoint must also have a trusted PCoIP Management Console certificate in its certificate store in order for discovery to succeed. Typically, this method is used in medium and high security environments. If your endpoint does not have a pre-loaded certificate, you can use the alternative method of manual endpoint discovery initiated by the PCoIP Management Console. See [Discovering Endpoints Manually from PCoIP Management Console](#).

This example shows how to configure a PCoIP Zero Client for discovery by a specific Endpoint Manager from the endpoint's AWI Management page. For information about configuring endpoints for automatic discovery from this page, please see the [PCoIP Zero Client Administrators' Guide](#).

 **Note: PCoIP Management Console servers as both Endpoint Bootstrap Manager and Endpoint Manager**

In the PCoIP Zero Client *Management* page, your PCoIP Management Console serves as both the Endpoint Bootstrap Manager and the Endpoint Manager. Use the PCoIP Management Console's IP address or FQDN when specifying either an Endpoint Bootstrap Manager or an Endpoint Manager URI.


To configure your endpoint with a specific Endpoint Manager:

 **Note: Complete the following steps in sequence**

It is necessary to complete these steps in the sequence shown next.

1. Enter the PCoIP Zero Client's IP address in your browser's address bar, then log in to its AWI.
2. From the **Configuration** menu, select **Management**.
3. Select the desired security level:
 - **Low Security Environment - PCoIP Zero Client is discoverable by Endpoint Managers:** This security level is intended for discovery that is initiated manually by a PCoIP Management

Console. It enables endpoints that are shipped with empty certificate stores to use trust information retrieved during the discovery process.

 **Note: Low Security Environment also works for endpoints configured for DHCP options or DNS SRV record discovery**

You can also use this security level for endpoints that are configured for DHCP options discovery or DNS SRV record discovery when the DHCP or DNS server also provisions the endpoint with the Endpoint Bootstrap Manager certificate's fingerprint.

- **Medium Security Environment - Endpoint Bootstrap Manager must be trusted by installed certificate:** When this security level is selected, the endpoint must have a trusted PCoIP Management Console certificate in its certificate store in order for discovery to succeed. The certificate can be provisioned either by the vendor when an endpoint is shipped or by uploading the PCoIP Management Console certificate to the endpoint. See [Uploading the PCoIP Management Console Certificate to an Endpoint](#).
- **High Security Environment - Bootstrap phase disabled:** With this security level, a user must manually enter an internal (and optionally an external) URI for the PCoIP Management Console from the endpoint's AWI Management page. The user must also upload a PCoIP Management Console certificate to the endpoint's trusted certificate store. Automatic provisioning and discovery methods cannot be used in a high security environment.

4. In the *Manager Discovery Mode* drop-down list, select Manual.
5. If the endpoint is not in the Idle state, click **Clear Management State** and then **Continue**.
6. Enter the URI for your PCoIP Management Console.

[Log Out](#) PCoIP® Zero Client

Home Configuration / Permissions / Diagnostics / Info / Upload

teradici

PCoIP

Management

Configure how this zero client is managed


Phase: Bootstrap

Management Status: Idle

Security Level:

Manager Discovery Mode:

Endpoint Bootstrap Manager URI:

 **Note: URIs require a secure WebSocket prefix**

URIs require a secured WebSocket prefix (for example, `wss://< internal EM IP address/FQDN >: [port number]`). The PCoIP Management Console's listening port is 5172. Entering this port number is optional. If you do not include it, port 5172 will be used by default.

7. Click **Apply** and then **Continue** once more.

If discovery succeeds, the endpoint's *Management* page will show the following information:

The screenshot displays the 'Management' page of the PCoIP Management Console. The page header includes 'Log Out', 'PCoIP@ Zero Client', and a breadcrumb trail: 'Home / Configuration / Permissions / Diagnostics / Info / Upload'. The Teradici PCoIP logo is prominently displayed. The main content area is titled 'Management' and includes the instruction 'Configure how this zero client is managed'. The configuration details are as follows:

- Phase:** Managed
- Management Status:** Connected to Endpoint Manager: 10.0.157.23:5172
- Security Level:** Medium Security Environment - Endpoint Bootstrap Manager must be trusted by installed certificate
- Manager Discovery Mode:** Manual
- Endpoint Bootstrap Manager URI:**
- EM Topology:**

URI Type	EM URI	Certificate Fingerprint
Internal EM URI:	wss://10.0.157.23:5172	B7:62:71:01:85:27:46:BB:E3:E9:5C:E2:34:2C:B5:76:7D:7A:F1:7F:6A:4D:5C:DB:AA:2B:99:BD:D5:A9:28:91
External EM URI:		

At the bottom of the configuration area, there are buttons for 'Clear Management State', 'Apply', and 'Cancel'.

Note: Automatically name and group endpoints

You can configure the PCoIP Management Console to automatically name endpoints and place them in a specific group when they are discovered. See [Auto Naming Endpoints](#) and [Auto Configuring Endpoints \(Enterprise\)](#) for details.

Managing PCoIP Management Console Databases

The PCoIP Management Console maintains a database containing its configuration data, information about the PCoIP endpoints it has discovered, console and daemon log files. You can archive multiple snapshots of these PCoIP Management Console database settings and store them on your PCoIP Management Console virtual machine. You can also download a stored archive to a location external to your PCoIP Management Console virtual machine, for instance, the host PC you use to access the PCoIP Management Console web browser.

Management Console requires at minimum, 1.5 times the size of the database to successfully perform a database restore, backup or upload. This calculation happens automatically and if the requirement is not met, a warning banner is displayed advising the Management Console VM is running out of disk space.

Database log file size

Database can become very large. If your backup is failing due limited disk space, you can try excluding the log files from the backup.


You can manage PCoIP Management Console database archives by clicking **SETTINGS** from the PCoIP Management Console's top menu, then clicking the **DATABASE** menu in the left pane.

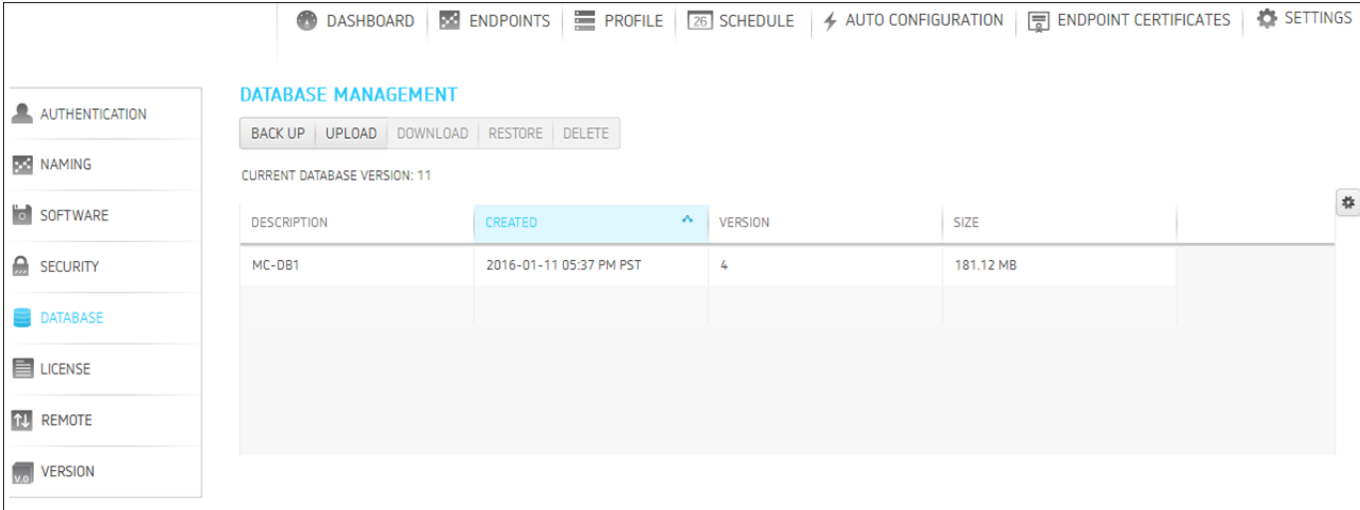
Note: Applying Profiles Created in Versions Earlier than 23.12.2

If a profile is created in version earlier than 23.12.2 for Zero Clients running firmware 23.12.x and with **Enable Audio** disabled, while applying this profile in version 23.12.2, ensure that **Enable Analog Audio Input** is disabled.

Displaying Database Information

The *DATABASE MANAGEMENT* page enables you to back up, upload, download, restore, and delete PCoIP Management Console database archives.

Click the gear icon  to the right of the table to change the information you want to display in the table columns. Your customized settings are saved in your browser and will be used for any user who subsequently logs in from that browser.



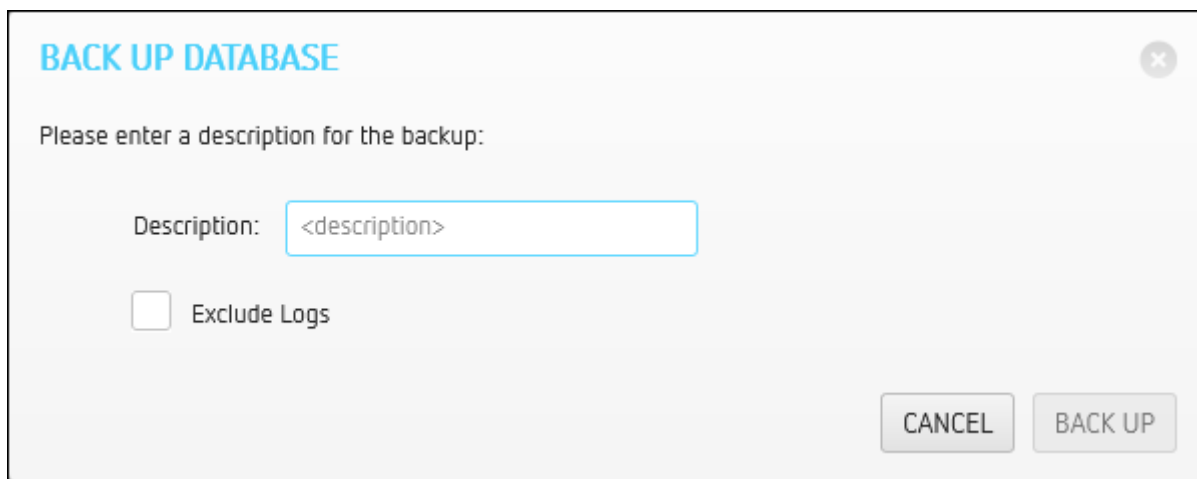
DESCRIPTION	CREATED	VERSION	SIZE
MC-DB1	2016-01-11 05:37 PM PST	4	181.12 MB

The **DATABASE MANAGEMENT** page

Backing Up PCoIP Management Console Database

To take a snapshot of your current PCoIP Management Console and store it in a database archive within the PCoIP Management Console virtual machine:

1. From the PCoIP Management Console's top menu, click **SETTINGS**.
2. Click **DATABASE** in the left pane.
3. Click **BACK UP**.
4. Enter a description, check the EXCLUDE LOGS option if you want to exclude the log files, and click **BACK UP**. Log files can become large and take up additional disk space, so you may wish to check this option if disk space is a concern.



BACK UP DATABASE

Please enter a description for the backup:

Description:

Exclude Logs

CANCEL BACK UP

Backup Dialog

The database log files can be found in the Management Console VM `/opt/teradici/backups/<database_folder>/logs` folder. For more information on database log files see [Managing Management Console Logs](#)

The archive will appear in the database table when the backup has completed.

Uploading a Database Archive from an External Location

To upload a database archive from an external location:

1. From the PCoIP Management Console's top menu, click **SETTINGS**.
2. Click **DATABASE** in the left pane.
3. Click **UPLOAD**.
4. Click **Select File**, locate the archive file (*.archive*) and then click **Open**.
5. Click **UPLOAD** to transfer the archive file to the PCoIP Management Console virtual machine. The archive file will appear in the database table when you are finished.

Downloading a Database Archive to an External Location

To download a database archive to an external location:

1. From the PCoIP Management Console's top menu, click **SETTINGS**.
2. Click **DATABASE** in the left pane.

3. From the database table, select the archive file you wish to transfer to a location external to your PCoIP Management Console virtual machine.
4. Click **DOWNLOAD**.
5. Save the file to the desired location.
Typically, this is a directory on the host PC that is running the PCoIP Management Console web browser.

Restoring PCoIP Management Console Database

⚠ Caution: Take a snapshot of your current virtual machine database before restoring a database archive

Restoring a database archive will permanently delete all current data from the database. Please ensure you have taken a snapshot of your current PCoIP Management Console virtual machine database before proceeding.

To restore a database archive from the PCoIP Management Console virtual machine:

1. From the PCoIP Management Console's top menu, click **SETTINGS**.
2. Click **DATABASE** in the left pane.
3. From the database table, select the archive file you wish to restore.
4. Click **RESTORE**.
5. Enable the message prompt and then click **RESTORE**.

Deleting PCoIP Management Console Database

To delete a database archive from the PCoIP Management Console virtual machine:

1. From the PCoIP Management Console's top menu, click **SETTINGS**.
2. Click **DATABASE** in the left pane.
3. From the database table, select the archive file you wish to delete.
4. Click **DELETE**.
5. Enable the message prompt and then click **DELETE**.

Expanding the PCoIP Management Console Virtual Machine Database and Disk Size

This section provides information on expanding your PCoIP Management Console Virtual Machine database size and the related disk sizing guidelines.

The basic PCoIP Management Console OVA will create a default configuration as follows:

- **Virtual Machine Hardware Version:** 10
- **CPU:** 4 vCPU
- **Memory:** 12 MB
- **Provisioned Storage:** 62 GB

⚠ Caution: Modifying virtual machine settings should only be considered by qualified individuals

Only qualified individuals should modify any virtual machine settings. Support strongly recommends you perform a database backup of the PCoIP Management Console and download the archive file to a safe location. You should also take a snapshot of the virtual machine prior to modifying any settings.

References

PCoIP Management Console 1 Profile Properties Renamed or Not Migrated

The following table lists PCoIP Management Console 1 profile properties that have been renamed PCoIP Management Console Enterprise or Free and are not migrated when you import a PCoIP Management Console 1 profile to a current release of PCoIP Management Console.

Reference to PCoIP Management Console refer to this release or later releases, unless otherwise specified.

Migrating and renaming notes

In the next table, when a PCoIP Management Console 1 property is not migrated, its Migration Notes column will have an explanation. If this column is blank, then the property only has a name change in the new PCoIP Management Console. Some properties that are currently not migrated may be included in future PCoIP Management Console releases.

PCoIP Management Console 1 Profile Information Renamed or Not Migrated

Release 1 Category	Release 1 Property Name	Current Release Category	Current Release Property Name	Migration Notes
Network Configuration	SNMP NMS Address	Network	Trap NMS Address	Not migrated when PCoIP Management Console 1 property Network Configuration > Enable SNMP is not Set in Profile or is set to False
Network Configuration	Enable SNMP Cold Start Trap	Network	SNMP Cold Start Trap	Not migrated when PCoIP Management Console 1 property Network Configuration > Enable SNMP is not Set in Profile or is set to False .
Network Configuration	Enable SNMP V1 Traps	Network	SNMP V1 Traps	Not migrated when PCoIP Management Console 1 property Network Configuration > Enable SNMP is not Set in Profile or is set to False .
Network Configuration	Enable SNMP V2c Traps	Network	SNMP V2 Traps	Not migrated when PCoIP Management Console 1 property Network Configuration > Enable SNMP is not Set in Profile or is set to False .
Network Configuration	SNMP Community Name	Network	SNMP Community Name	Not migrated when PCoIP Management Console 1 property Network Configuration > Enable SNMP is not Set in Profile or is set to False .
Network Configuration	Static Fallback IP Address	Network	Static Fallback IPv4 Address	Not migrated when PCoIP Management Console 1 property Network Configuration > Enable SNMP is not Set in Profile or is set to False .
Network Configuration	Static Fallback Subnet Mask	Network	Static Fallback IPv4 Subnet Mask	Not migrated when PCoIP Management Console 1 property Network Configuration > Enable

Release 1 Category	Release 1 Property Name	Current Release Category	Current Release Property Name	Migration Notes
				SNMP is not Set in Profile or is set to False.
Network Configuration	Static Fallback Gateway Address	Network	Static Fallback IPv4 Gateway	Not migrated when PCoIP Management Console 1 property Network Configuration > Enable SNMP is not Set in Profile or is set to False.
Network Configuration	Static Fallback Timeout	Network	Static Fallback IPv4 Timeout	Not migrated when PCoIP Management Console 1 property Network Configuration > Enable SNMP is not Set in Profile or is set to False.
Discovery Configuration	PCoIP Management Console DNS-Based Discovery Prefix			Never migrated. Not used in firmware 5.0.0 and later.
Session Configuration	PCoIP Connection Manager Server Address	Session > Session Type	Server URI	Not migrated when PCoIP Management Console 1 property Session Configuration > Session Connection Type is not Set in Profile or is not set to one of the following: <ul style="list-style-type: none"> • PCoIP Connection Manager • PCoIP Connection Manager + Auto-Logon
Session Configuration	Auto Detect Server URI	Session > Session Type	Server URI	Not migrated when PCoIP Management Console 1 property Session Configuration > Session Connection Type is not Set in Profile or is not set to Auto Detect .

Release 1 Category	Release 1 Property Name	Current Release Category	Current Release Property Name	Migration Notes
Session Configuration	Auto-Logon Username	Session > Session Type	Logon Username	Not migrated when PCoIP Management Console 1 property Session Configuration > Session Connection Type is not Set in Profile or is not set to one of the following: <ul style="list-style-type: none"> • View Connection Server + Auto-Logon • PCoIP Connection Manager + Auto-Logon
Session Configuration	Auto-Logon Password	Session > Session Type	Logon Password	Not migrated when PCoIP Management Console 1 property Session Configuration > Session Connection Type is not Set in Profile or is not set to one of the following: <ul style="list-style-type: none"> • View Connection Server + Auto-Logon • PCoIP Connection Manager + Auto-Logon
Session Configuration	Auto-Logon Domain	Session > Session Type	Logon Domain Name	Not migrated when PCoIP Management Console 1 property Session Configuration > Session Connection Type is not Set in Profile or is not set to one of the following: <ul style="list-style-type: none"> • View Connection Server + Auto-Logon • PCoIP Connection Manager + Auto-Logon

Release 1 Category	Release 1 Property Name	Current Release Category	Current Release Property Name	Migration Notes
Session Configuration	Enable View Connection Server SSL			Never migrated. Not used in firmware 4.x and later.
Session Configuration	Kiosk Mode Custom Username	Session > Session Type	Username	Not migrated when PCoIP Management Console 1 property Session Configuration > Session Connection Type is not Set in Profile or is not set to View Connection Server + Kiosk .
Session Configuration	Kiosk Mode Password	Session > Session Type	Password	Not migrated when PCoIP Management Console 1 property Session Configuration > Session Connection Type is not Set in Profile or is not set to View Connection Server + Kiosk .
Session Configuration	Organization ID			Never migrated. Currently not included in PCoIP Management Console.
Session Configuration	OneSign Direct to View Address			Never migrated. Currently not included in PCoIP Management Console.
Session Configuration	Disconnect Dialog Display Mode	Session > Session Type	Disconnect Message Filter	
Session Configuration	Enable Login Username Caching	Session > Session Type	Remember Username	
Session Configuration	Prefer GSC-IS Over PIV Endpoint	Session > Session Type	Prefer GSC-IS	
Session Configuration	Proximity Reader Beep Mode	Session > Session Type	Pre-Session Reader Beep	
Encryption Configuration	Enable Salsa20-256-			Never migrated. Applies to Tera1 endpoints only.

Release 1 Category	Release 1 Property Name	Current Release Category	Current Release Property Name	Migration Notes
	Round12 Encryption			
Encryption Configuration	Enable AES-128-GCM Encryption			Never migrated. Not configurable in FW 5.0.0 and later.
Encryption Configuration	Enable AES-256-GCM Encryption			Never migrated. Not configurable in FW 5.0.0 and later.
Encryption Configuration	Session Negotiation Security Level	Session > Session Type	Session Negotiation Cipher	
OSD Configuration	Hidden Menu Entries	Security	Hidden OSD Menu Entries	
Image Configuration	Low Bandwidth Text Codec Mode			Never migrated. Currently not included in PCoIP Management Console.
Image Configuration	Enable Client Image Settings			Never migrated. Remote Workstation Card property.
Display Configuration	Enable Monitor Emulation on Video Port 1-4			Never migrated. Remote Workstation Card property.
Display Configuration	Enable Host Hot-Plug Delay			Never migrated. Remote Workstation Card property.
Display Configuration	Enable Display Cloning	Session > Display Configuration	Clone Primary Display	
Display Configuration	Enable Accelerated Monitor Emulation			Never migrated. Remote Workstation Card property.
Time Configuration	Enable DST	Other > Time	Daylight Saving Time	
Time Configuration	Time Zone Offset	Other > Time	Time Zone	Converted to IANA zoneinfo time zone. See Time Zone Definitions for

Release 1 Category	Release 1 Property Name	Current Release Category	Current Release Property Name	Migration Notes
				PCoIP Management Console 1 or 2
Security Configuration	Password	Security	Local Administrative Password	
Security Configuration	Enable Password Protection	Security	Enable Password Protection for OSD and AWI	
Security Configuration	Enable 802.1X Support for Legacy Switches	Security	802.1X Legacy Support	
Audio Permissions	Enable Vista/Windows 7 64-bit Mode			Never migrated. Remote Workstation Card property
Audio Permissions	Enable Audio Line In			Never migrated. Remote Workstation Card property
Audio Permissions	Dual Audio Output Mode		Dual Audio Output	Migrated in PCoIP Management Console 19.11.
Audio Permissions	Audio In Device Type	Session > Audio Input	Audio Device Type	
Audio Permissions	Audio In Preferred USB Vendor ID	Session > Audio Input	Preferred USB Vendor ID	
Audio Permissions	Audio In Preferred USB Device Product ID	Session > Audio Input	Preferred USB Device Product ID	
Audio Permissions	Audio Out Device Type	Session > Audio Output	Audio Device Type	
Audio Permissions	Audio Out Preferred USB Vendor ID	Session > Audio Output	Preferred USB Vendor ID	
	Audio Out Preferred USB			

Release 1 Category	Release 1 Property Name	Current Release Category	Current Release Property Name	Migration Notes
Audio Permissions	Device Product ID	Session / Audio Output	Preferred USB Device Product ID	
Power Permissions	Client Power Button Function	Power	Remote Host Power Control	
Power Permissions	Wake-on-USB Mode	Power	Wake-on-USB	
Power Permissions	Wake-on-LAN Mode	Power	Wake-on-LAN	
Power Permissions	Power On After Power Loss ModeA	Power	Power On After Power Loss	
Power Permissions	Client Power Down Timeout Seconds	power	Auto Power-Off Timeout	
Power Permissions	Display Suspend Timeout Seconds	Power	Display Suspend Timeout	
Host Driver Configuration	Enable Host Driver			Never migrated. Remote Workstation Card property.
Event Log Control	Enable Diagnostic Log			Never migrated. Not used in firmware 5.0.0 and later.
Event Log Control	Event Log Filter Mode			Never migrated. Not used in firmware 5.0.0 and later.
Event Log Control	Syslog Facility Number	Logging	Syslog Facility	
Event Log Control	Enhanced Logging Mode Mask	Logging	Enhanced Logging Mode	Not migrated when PCoIP Management Console 1 is configured to Enhanced logging disabled .
		Peripheral	EHCI	

Release 1 Category	Release 1 Property Name	Current Release Category	Current Release Property Name	Migration Notes
Peripheral Configuration	Enable USB EHCI			
Peripheral Configuration	Force Local Cursor Visible	Peripheral	Force Local Cursor Visibility	Migrated in MC 3.2
		Peripheral	Devices Forced to USB 1.1	Migrated in MC 3.2. This feature is available in firmware 5.0+
IPv6 Configuration	IPv6 Domain Name	Network	IPv6 Domain Name	Not migrated when PCoIP Management Console 1 property IPv6 Configuration > Enable IPv6 is not Set in Profile or is set to False
IPv6 Configuration	Enable DHCPv6	Network	DHCPv6	Not migrated when PCoIP Management Console 1 property IPv6 Configuration > Enable IPv6 is not Set in Profile or is set to False
IPv6 Configuration	Enable SLAAC	Network	SLAAC	Not migrated when PCoIP Management Console 1 property IPv6 Configuration > Enable IPv6 is not Set in Profile or is set to False
IPv6 Configuration	IPv6 Gateway Address	IPv6 Gateway Address Prefix Length	Network	IPv6 Gateway
IPv6 Configuration	IPv6 Primary DNS Address	IPv6 Primary DNS Address Prefix Length	Network	Primary IPv6 DNS
IPv6 Configuration	IPv6 Secondary DNS Address	IPv6 Secondary DNS Address Prefix Length	Network	Secondary IPv6 DNS
SCEP Configuration	SCEP Server URI			Never migrated. Currently not included in PCoIP Management Console

Release 1 Category	Release 1 Property Name	Current Release Category	Current Release Property Name	Migration Notes
SCEP Configuration	Challenge Password			Never migrated. Currently not included in PCoIP Management Console
SCEP Configuration	Use Certificate for 802.1X			Never migrated. Currently not included in PCoIP Management Console
Display Configuration	Preferred Override Resolution on Port 1-4	Session > Display Configuration: Video Port 1-4	Preferred Resolution	Not migrated when PCoIP Management Console 1 property Preferred Resolution is set to Native
Display Topology Configuration (Dual and Quad)	Display Layout Alignment	Session > Display Configuration: Dual/Quad Display Topology	Display Layout Alignment	Not migrated when PCoIP Management Console 1 property Display Topology Configuration > Enable Configuration is not Set in Profile or is set to False
Display Topology Configuration (Dual and Quad)	Primary Port	Session > Display Configuration: Dual/Quad Display Topology	Primary Port	Not migrated when PCoIP Management Console 1 property Display Topology Configuration > Enable Configuration is not Set in Profile or is set to False
Display Topology Configuration (Dual and Quad)	Position	Session > Display Configuration: Dual/Quad Display Topology	Position	Not migrated when PCoIP Management Console 1 property Display Topology Configuration > Enable Configuration is not Set in Profile or is set to False
Display Topology Configuration (Dual and Quad)	Rotation	Session > Display Configuration: Dual/Quad Display Topology	Rotation	Not migrated when PCoIP Management Console 1 property Display Topology Configuration > Enable Configuration is not Set in Profile or is set to False
	Resolution		Resolution	

Release 1 Category	Release 1 Property Name	Current Release Category	Current Release Property Name	Migration Notes
Display Topology Configuration (Dual and Quad)		Session > Display Configuration: Dual/Quad Display Topology		Not migrated when PCoIP Management Console 1 property Display Topology Configuration > Enable Configuration is not Set in Profile or is set to False
Profile OSD Logo		Other > OSD	OSD Logo	Never migrated
Profile Firmware		Software		Firmware Version
Image Configuration	Low Bandwidth Text Codec Mode	Image	Enable Low Bandwidth Text Codec	Migrated value applicable only for DUAL Client device
Image Configuration	Enable Client Image Settings	Image	Use Client Image Settings	Migrated value applies to Host (DUAL and QUAD) device only
Display Configuration	Enable Monitor Emulation on Video Port 1-4	Session	Monitor Emulation: Video Port 1 Monitor Emulation: Video Port 2 Monitor Emulation: Video Port 3 Monitor Emulation: Video Port 4	Migrated values apply to Host device only. Values of port 3 and 4 are ignored for DUAL type
Display Configuration	Enable Host Hot-Plug Delay	Session Host Hot-Plug Delay		Migrated value applies to Host (DUAL and QUAD) device only
Display Configuration	Enable Display Cloning	Session > Monitor Emulation	Clone Primary Display	Applies to Client DUAL devices only
Display Configuration	Enable Accelerated	Session > Monitor Emulation	Accelerated Monitor Emulation	Migrated value applies to Host (DUAL and QUAD) device only

Release 1 Category	Release 1 Property Name	Current Release Category	Current Release Property Name	Migration Notes
	Monitor Emulation			
Audio Permissions	Enable Vista/Windows 7 64-bit Mode			Never migrated. Applied to Tera1 devices
Audio Permissions	Enable Audio Line In	Session > Audio		Audio Line In
Audio Permissions	Audio In Device Type	Session > Audio Input	Audio Device Type	Migrated value applies to Client (DUAL and QUAD) device only
Audio Permissions	Audio In Preferred USB Vendor ID	Session > Audio Input	Preferred USB Vendor ID	Migrated value applies to Client (DUAL and QUAD) device only
Audio Permissions	Audio In Preferred USB Device Product ID	Session > Audio Input	Preferred USB Device Product ID	Migrated value applies to Client (DUAL and QUAD) device only
Audio Permissions	Audio Out Device Type	Session > Audio Output	Audio Device Type	Migrated value applies to Client (DUAL and QUAD) device only
Audio Permissions	Audio Out Preferred USB Vendor ID	Session > Audio Output	Preferred USB Vendor ID	Migrated value applies to Client (DUAL and QUAD) device only
Audio Permissions	Audio Out Preferred USB Device Product ID	Session > Audio Output	Preferred USB Device Product ID	Migrated value applies to Client (DUAL and QUAD) device only
Power Permissions	Client Power Button Function	Power	Remote Host Power Control	<p>Migrated value applies to Client (DUAL and QUAD) device only</p> <p>Only the following values from MC1 are migrated, e rest are no longer supported in MC 3</p> <p>The user can only invoke a hard power off</p>

Release 1 Category	Release 1 Property Name	Current Release Category	Current Release Property Name	Migration Notes
				The user cannot invoke any power off
Power Permissions	Wake-on-LAN Mode	Power	Wake-on-LAN	Migrated value applies to Host (DUAL and QUAD) device only
Power Permissions	Power On After Power Loss Mode	Power	Power On After Power Loss	Migrated value applies to Client (DUAL and QUAD) device only
Power Permissions	Client Power Down Timeout Seconds	Power	Auto Power-Off Timeout	Migrated value applies to Client (DUAL and QUAD) device only
Power Permissions	Display Suspend Timeout Seconds	Power	Display Suspend Timeout	Migrated value applies to Client (DUAL and QUAD) device only
Host Driver Configuration	Enable Host Driver	Host Driver	Host Driver	Migrated value applies to Host (DUAL and QUAD) device only
Peripheral Configuration	Enable USB EHCI	Peripheral	EHCI	Migrated value applies to Client (DUAL and QUAD) device only
SCEP Configuration	SCEP Server URI			Never Migrated. Included under ENDPOINT CERTIFICATES IN mc 3.1
SCEP Configuration	Challenge Password			Never Migrated. Included under ENDPOINT CERTIFICATES IN mc 3.1
SCEP Configuration	Use Certificate for 802.1X			Never Migrated. Included under ENDPOINT CERTIFICATES IN mc 3.1
Display Topology Configuration (Dual and Quad)	Primary Port	"Session > Monitor emulation: Quad Display Session > Monitor Emulation Dual Display"	Position	"Not migrated when PCoIP Management Console 1 property Display Topology Configuration > Enable Configuration is not Set in Profile or is set to

Release 1 Category	Release 1 Property Name	Current Release Category	Current Release Property Name	Migration Notes
				False. Migrated value applies to Client (DUAL and QUAD) device only
Display Topology Configuration (Dual and Quad)	Rotation	"Session > Monitor emulation: Quad Display Session > Monitor Emulation Dual Display"	Rotation	"Not migrated when PCoIP Management Console 1 property "Display Topology Configuration > Enable Configuration is not Set in Profile or is set to False . Migrated value applies to Client device only. Values for Port 3 and 4 ignored for DUAL display"
Display Topology Configuration (Dual and Quad)	Resolution	"Session > Monitor emulation: Quad Display Session > Monitor Emulation Dual Display"	Resolution	"Not migrated when PCoIP Management Console 1 property Display Topology Configuration > Enable Configuration is not Set in Profile or is set to False. Migrated value applies to Client device only. Values for Port 3 and 4 ignored for DUAL display"
Profile Firmware	Software			Never migrated. All migrated profiles are assigned to appropriate PCoIP Zero Client or Hard Host firmware

In addition to the previous table, the following table lists properties that are also not migrated when you import a PCoIP Management Console 1 profile, because they are not managed by the PCoIP Management Console newer releases.


PCoIP Zero Client Properties not Managed by the PCoIP Management Console

Firmware Property	Firmware Version	Description
Prefer IPv6 FQDN Resolution	4.8.0	Not managed by PCoIP Management Console 1.x or later releases of PCoIP Management Console
IPv6 Address Resolution	4.8.0	Not managed by PCoIP Management Console 1.x or later releases of PCoIP Management Console
OSD Region Tab Lockout	5.0.0	Never managed by PCoIP Management Console 1.x

Time Zone Definitions for PCoIP Management Console 1 or later releases

Reference to PCoIP Management Console refer to releases 2.0 or later, unless otherwise specified.

The PCoIP Management Console web interface uses Internet Assigned Numbers Authority (IANA) time zone definitions to let users configure the PCoIP Management Console web interface in their local time. The following table shows how the profile import script converts the PCoIP Management Console 1 time zones to PCoIP Management Console IANA time zones.

 **Note: Time zone selection/setting in PCoIP Management Console display offset as standard time**

Time zone selection on Profile > Edit > OTHER and Settings > USERS > Edit pages show offsets with respect to 'Standard Time' only (not the 'Daylight Savings Time').

PCOIP MANAGEMENT CONSOLE 1 AND PCOIP MANAGEMENT CONSOLE TIME ZONE DEFINITIONS

PCoIP Management Console 1 Time Zone Definition	PCoIP Management Console Time Zone Definition
gmt_minus_1200_international_date_line_west	Asia/Anadyr
gmt_minus_1100_midway_island	Pacific/Midway
gmt_minus_1000_hawaii	Pacific/Honolulu
gmt_minus_0900_alaska	America/Anchorage
gmt_minus_0800_pacific_time	America/Vancouver
gmt_minus_0800_tijuana	America/Tijuana
gmt_minus_0700_arizona	America/Phoenix
gmt_minus_0700_chihuahua_new	America/Chihuahua
gmt_minus_0700_chihuahua_old	America/Chihuahua
gmt_minus_0700_mountain_time	America/Denver
gmt_minus_0600_central_america	America/Costa_Rica
gmt_minus_0600_central_time	America/Chicago
gmt_minus_0600_guadalajara_new	America/Mexico_City
gmt_minus_0600_guadalajara_old	America/Mexico_City
gmt_minus_0600_saskatchewan	America/Regina
gmt_minus_0500_bogota	America/Bogota
gmt_minus_0500_eastern_time	America/New_York
gmt_minus_0500_indiana	America/Indiana/Indianapolis
gmt_minus_0430_caracas	America/Caracas
gmt_minus_0400_atlantic_time	Atlantic/Bermuda
gmt_minus_0400_la_paz	America/La_Paz
gmt_minus_0400_manaus	America/Manaus
gmt_minus_0400_santiago	America/Santiago
gmt_minus_0330_newfoundland	America/St_Johns
gmt_minus_0300_brasilia	America/Sao_Paulo
gmt_minus_0300_buenos_aires	America/Argentina/Buenos_Aires
gmt_minus_0300_greenland	America/Godthab
gmt_minus_0300_montevideo	America/Montevideo

PCoIP Management Console 1 Time Zone Definition	PCoIP Management Console Time Zone Definition
gmt_minus_0200_mid_atlantic	Atlantic/South_Georgia
gmt_minus_0100_azores	Atlantic/Azores
gmt_minus_0100_cape_verde_is	Atlantic/Cape_Verde
gmt_plus_0000_casablanca	Africa/Casablanca
gmt_plus_0000_greenwich_mean_time	Europe/London
gmt_plus_0100_amsterdam	Europe/Amsterdam
gmt_plus_0100_belgrade	Europe/Belgrade
gmt_plus_0100_brussels	Europe/Brussels
gmt_plus_0100_sarajevo	Europe/Sarajevo
gmt_plus_0100_west_central_africa	Africa/Lagos
gmt_plus_0100_windhoek	Africa/Windhoek
gmt_plus_0200_amman	Asia/Amman
gmt_plus_0200_athens	Europe/Athens
gmt_plus_0200_beirut	Asia/Beirut
gmt_plus_0200_cairo	Africa/Cairo
gmt_plus_0200_harare	Africa/Harare
gmt_plus_0200_helsinki	Europe/Helsinki
gmt_plus_0200_jerusalem	Asia/Jerusalem
gmt_plus_0200_minsk	Europe/Minsk
gmt_plus_0300_baghdad	Asia/Baghdad
gmt_plus_0300_kuwait	Asia/Kuwait
gmt_plus_0300_moscow	Europe/Moscow
gmt_plus_0300_nairobi	Africa/Nairobi
gmt_plus_0330_tehran	Asia/Tehran
gmt_plus_0400_abu_dhabi	Asia/Dubai
gmt_plus_0400_baku	Asia/Baku
gmt_plus_0400_caucasus_standard_time	Asia/Yerevan
gmt_plus_0400_yerevan	Asia/Yerevan

PCoIP Management Console 1 Time Zone Definition	PCoIP Management Console Time Zone Definition
gmt_plus_0430_kabul	Asia/Kabul
gmt_plus_0500_ekaterinburg	Asia/Yekaterinburg
gmt_plus_0500_islamabad	Asia/Karachi
gmt_plus_0530_chennai	Asia/Kolkata
gmt_plus_0530_sri_jayawardenepura	Asia/Colombo
gmt_plus_0545_kathmandu	Asia/Kathmandu
gmt_plus_0600_almaty	Asia/Almaty
gmt_plus_0600_astana	Asia/Almaty
gmt_plus_0630_yangon	Asia/Rangoon
gmt_plus_0700_bangkok	Asia/Bangkok
gmt_plus_0700_krasnoyarsk	Asia/Krasnoyarsk
gmt_plus_0800_beijing	Asia/Hong_Kong
gmt_plus_0800_irkutsk	Asia/Chita
gmt_plus_0800_kuala_lumpur	Asia/Kuala_Lumpur
gmt_plus_0800_perth	Australia/Perth
gmt_plus_0800_taipei	Asia/Taipei
gmt_plus_0900_osaka	Asia/Tokyo
gmt_plus_0900_seoul	Asia/Seoul
gmt_plus_0900_yakutsk	Asia/Yakutsk
gmt_plus_0930_adelaide	Australia/Adelaide
gmt_plus_0930_darwin	Australia/Darwin
gmt_plus_1000_brisbane	Australia/Brisbane
gmt_plus_1000_canberra	Australia/Sydney
gmt_plus_1000_guam	Pacific/Guam
gmt_plus_1000_hobart	Australia/Hobart
gmt_plus_1000_vladivostok	Asia/Vladivostok
gmt_plus_1100_magadan	Asia/Magadan
gmt_plus_1200_auckland	Pacific/Auckland

PCoIP Management Console 1 Time Zone Definition	PCoIP Management Console Time Zone Definition
gmt_plus_1200_fiji	Pacific/Fiji
gmt_plus_1300_nukualofa	Pacific/Tongatapu

Expanding the PCoIP Management Console Disk Size

The following steps are required to expand the vdisk of the PCoIP Management Console.

⚠ Caution: Modifying virtual machine settings should only be done by qualified individuals

Modifying any virtual machine settings should only be done by qualified individuals. HP strongly recommends you do a database backup of the PCoIP Management Console and download the archive file to a safe location. You should also take a snapshot of the virtual machine prior to modifying any settings.

To expand your PCoIP Management Console disk size:

1. Check the current disk size from the command prompt:

```
df --total
```

This will display the space used by each volume in `/dev/mapper/vg_main-lv_root`.

2. Ensure you have allocated enough disk space.
3. From vSphere, select the virtual machine to be modified and power it down.
4. Determine the increased disk size.
5. Edit the virtual machine settings to increase the vDisk and the vRAM. To do this, run `sudo fdisk /dev/sda` and follow these steps in order:
 - a. You may get a Warning about DOS-compatible mode being deprecated. Type **C** to switch off DOS-compatible mode. Type **U** to change display units to sectors.
 - b. Press **P** to print the partition table to identify the number of partitions. By default, there are 2: sda1 and sda2.
 - c. Press **N** to create a new primary partition.
 - d. Press **P** for primary.
 - e. Press **3** for the partition number, depending on the output of the partition table print.
 - f. Press **Enter** two times.

- g. Press `T` to change the system's partition ID.
- h. Press `3` to select the newly creation partition.
- i. Type `8e` to change the Hex Code of the partition for Linux LVM.
- j. Press `W` to write the changes to the partition table.

6. Run `sudo init 6` to restart the virtual machine.

7. When the virtual machine restarts, run the following commands in order:

- a. `sudo pvcreate /dev/sda3` (This should create the physical volume /dev/sda3).
- b. `sudo vgextend vg_main /dev/sda3` (This will extend the Volume Group VG_Main).
- c. `sudo vgsdisplay` (This will display information about the Volume Group. Make note of the Free PE / Size. The first number is the number of free extents and will be used in the following command).
- d. `sudo lvextend -l 511 /dev/mapper/vg_main-lv_root` (You will get a message telling you the volume has been extended from 8.31GB to 15.97GB / 511 extents).
- e. `sudo resize2fs /dev/mapper/vg_main-lv_root` (This will resize the partition).
- f. `sudo init 6` (this will restart the virtual machine).

8. Power the virtual machine back on.

Note: Extending logical volume in Linux

For information on how to extend logical volume in a virtual machine running RedHat or CentOS, see https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1006371.

Using your Virtual Machine Console to Administer Licenses when Connected to the Internet

i Info: Virtual machine console

The use of the vm console is required for license management on PCoIP Management Console releases 2.0 to 3.0. From MC 3.1 onwards, a UI is present for managing licenses when connected to the internet.

Activating Licenses

Using your virtual machine console to activate your PCoIP Management Console Enterprise license:

1. Connect to your PCoIP Management Console virtual machine console and log in using the admin account and password. See [Logging in to the PCoIP Management Console OVA Virtual Machine Console](#).

2. Run the following command:

```
/opt/teradici/licensing/mc_activate_lic.sh -k <entitlementID>
```

where entitlementID is the activation key you received via email.

Example:

```
/opt/teradici/licensing/mc_activate_lic.sh -k 1234-5678-90AB-CDEF
```

Using your virtual machine console to activate your PCoIP Management Console Enterprise license from behind a proxy server:

i Info: Proxy parameter

Activating PCoIP Management Console Enterprise license when the PCoIP Management Console is located behind a proxy server requires appending the `-p` parameter that defines the proxy parameters.

1. Connect to your PCoIP Management Console virtual machine console and log in using the admin account and password.
2. Run the following command:

```
/opt/teradici/licensing/mc_activate_lic.sh -k <entitlementID> -p  
[<user:password>@] <proxyhost:port>
```

where:

`<entitlementID>` is the activation key you received via email.

`[<user:password>]` is optional. If `>user` is provided, `password` must also be provided.

`<proxyhost:port>` is the IP address and port number of your proxy server.

Examples:

- If the proxy requires a user name and password:

```
/opt/teradici/licensing/mc_activate_lic.sh -k 1234-5678-90AB-CDEF -p  
bob:bobpasswd@192.168.45.23:3128
```

- If the proxy does not require a user name and password:

```
/opt/teradici/licensing/mc_activate_lic.sh -k 1234-5678-90AB-CDEF -p  
192.168.45.23:3128
```

Viewing Installed Licenses

Once your license is activated, its information is stored on the PCoIP Management Console virtual machine.

You can view the installed licenses via the command prompt on the vm console.

View installed licenses via the command prompt:

1. Connect to your PCoIP Management Console virtual machine console and log in using the admin account and password. See [Logging in to the PCoIP Management Console OVA Virtual Machine Console](#).

2. Run the following command:


```
/opt/teradici/licensing/mc_view_lic.sh
```

The script will output the following information:

- **Fulfillment ID: XXXXXXXX:** An ID assigned to a license after it is activated. This ID is required if you deactivate the license. The fulfillment ID will be different each time you reactivate a license after it has been deactivated.
- **Entitlement ID: XXXX-XXXX-XXXX-XXXX:** The license key you received via email that you use to activate your license.
- **Expiration date: DD-MMM-YYYY:** The day, month, and year your license expires.

Deactivating Licenses

It is important to deactivate a license when you no longer need it, for example, when you decommission a virtual machine. This frees up the license and makes it available for a different PCoIP Management Console Enterprise deployment.

 **Note: Deactivating license reverts PCoIP Management Console to PCoIP Management Console Free**

PCoIP Management Console will run in Free mode when all its licenses are deactivated.

!!! warning "Warning: Internet Access Required" When deactivating a license, an internet connection to the licensing server is required unless the offline license activation steps are used.

Deactivating Your PCoIP Management Console License

Using your virtual machine console to deactivate PCoIP Management Console Enterprise license:

1. Connect to your PCoIP Management Console console and log in using the **admin** account and password.
2. Run the following command:

```
/opt/teradici/licensing/mc_return_lic.sh -f <fulfillment_ID>
```

where <fulfillment_ID> is the ID assigned to the license after it was activated.

Example:

```
/opt/teradici/licensing/mc_return_lic.sh -f 12345678
```

Note: Finding fulfillment ID

To find your fulfillment ID, see [Viewing Installed Licenses](#).

To deactivate your PCoIP Management Console Enterprise license when the PCoIP Management Console is located behind a proxy server:

1. Connect to your PCoIP Management Console Enterprise virtual machine console and log in using the admin account and password. See [Logging in to the PCoIP Management Console OVA Virtual Machine Console](#).
2. Run the following command:

```
/opt/teradici/licensing/mc_return_lic.sh -f <fulfillmentId> -p  
[<user:password>@] proxyhost:port>
```

where:

<fulfillmentID> is the ID assigned to the license after it was activated.

[<user:password>] is optional. If user is provided, password must also be provided.

<proxyhost:port> is the IP address and port number of your proxy server.

Example:

- If the proxy requires a user name and password:

```
/opt/teradici/licensing/mc_return_lic.sh -f 12345678 -p  
bob:bobpasswd@192.168.45.23:3128
```

- If the proxy does not require a user name and password:

```
/opt/teradici/licensing/mc_return_lic.sh -f 12345678 -p 192.168.45.23:3128
```

HTTP Strict Transport Security

HTTP Strict Transport Security (HSTS) is a policy that helps protect web server appliances against unwanted access. It allows only trusted connections with browsers using HTTPS. When HSTS is enabled, it informs a web browser that has previously visited a site to only use HTTPS connections. Web browsers that have never connected to the site may use HTTP for the initial connection. HSTS is an IETF standards track protocol and specified in RFC 6797.

⚠ Warning: Not all browsers will react the same way. Ensure you thoroughly test using all browsers you intend to use

Some web browsers may terminate the connection to the web server and prevent access to the PCoIP Management Console if the security of the connection cannot be verified. Therefore it is important to have a properly created and trusted certificate installed into the Management Console and the ability for the web browser to be able to verify the authenticity of that certificate.

HSTS can be enabled on the PCoIP Management Console by editing the **mc-external-config.yml** file. It also requires a proper certificate be loaded on the PCoIP Management Console. For more information on configuring HSTS and how it works please review [RFC 6797](#).

The certificate requirements are determined by the browser you are using. See browser documentation for requirements. Requirements include the following and can change at anytime:

- SHA 256 is the minimum signature algorithm
- CA signed (can not be a self-signed certificate)
- Subject Alternative Name (Chrome requirement)

To enable HSTS and configure the timeout setting:

1. [Accessing the PCoIP Management Console Virtual Machine Console](#)
2. SSH to the PCoIP Management Console virtual machine console.
3. Log in as administrator and enter the command `sudo su`.
4. Change to the following directory:
`/opt/teradici/console/config/`

5. Edit the **mc-external-config.yml** file to activate HSTS and set the time out by:

- a. Uncommenting (remove # symbol) from the **jetty, port, hsts, enableHSTS** and **stsMaxAge** from the following lines:

```
#jetty:
#   port: 8080
#   sendServerVersion: false
#   hsts:
#     enableHSTS: false
#     stsMaxAge: 31536000
#   traceEnabled: false
#   optionsEnabled: false
```

- b. Editing the **enableHSTS** value to true.

```
enableHSTS: true
```

- c. Editing the **stsMaxAge** value to the desired time out in seconds.

```
stsMaxAge: 31536000
```

stsMaxAge

is configurable from the default of -1 to one year (31536000 seconds) and defines how long the web browser should cache the HSTS policy against the server.


Your edited lines should look like the following:

```
jetty:
  port: 8080
#   sendServerVersion: false
  hsts:
    enableHSTS: true
    stsMaxAge: 31536000
#   traceEnabled: false
#   optionsEnabled: false
```

6. Save your edits to **mc-external-config.yml**.

7. Restart the Management Console console service.

```
sudo service mcconsole restart
```

 **Tip: Is HSTS enabled?**

To confirm if HSTS is enabled, run

```
curl -k -s -vv https://<PCoIP Management Console ip address>/login/auth | grep  
Strict
```

and look at any HTTP response from the server. If enabled, the header will display the max age.

Chrony NTP Configuration

By default, the Management Console RPM based on CentOS uses chrony as the NTP client in which there are default references to public NTP servers. To configure chrony to not communicate with external time servers and adhere to your companies security policy, consider the following actions:

1. Refer to your Security policy to ensure your NTP configuration complies to set standards.

Considerations should include:

- Confirming if your companies DNS server provides an NTP sever or server pool.
- Remove public server pools from **chrony.conf**
- Add your own public server pool to chrony.conf
- [Disabling chrony](#)

2. Review the current Management Console chrony configuration by entering the `chronyc sources -v` command from the [Management Console's console](#) to provide a verbose listing of NTP servers chrony is syncing too.

3. Consider using internal NTP servers authorized by your companies security policy by editing the `/etc/chrony.conf` file.

Example

We have provided the following example of viewing and editing an NTP configuration. In this example the default ntp servers are commented out and replaced by another NTP server.

1. Check the currently used NTP servers using `chronyc sources -v`.

```
[kono@localhost etc]$ chronyc sources -v
210 Number of sources = 6

.-- Source mode  '^' = server, '=' = peer, '#' = local clock.
/ .- Source state '*' = current synced, '+' = combined , '-' = not
combined,
| /  '?' = unreachable, 'x' = time may be in error, '~' = time too
variable.
||
||                                     .- xxxx [ yyyy ] +/-
zzzz
||      Reachability register (octal) -.      |  xxxx = adjusted
offset,
||      Log2(Polling interval) --.      |      |  yyyy = measured
offset,
||                                     \      |      |  zzzz = estimated
error.
||                                     |      |      \
MS Name/IP address             Stratum Poll Reach LastRx Last sample
=====
^* ip225.ip-54-39-173.net        2  10   377   652  +4224us[+4594us] +/-
35ms
^+ k8s-w02.tblflp.zone         2   9   373   147   -12ms[ -12ms] +/-
73ms
^- ntp2.torix.ca               2   9   377   113   +1082us[+1082us] +/-
538ms
^- dns2.switch.ca              3   9   377    95    +750us[ +750us] +/-
532ms
^- DC01.tera.local             3   6   377    48   -1332us[-1332us] +/-   98ms
^- DC02.tera.local             4   6   377    45   -1014us[-1014us] +/-  135ms
[kono@localhost etc]$
```

2. Edit the **chrony.conf** file to change the referenced NTP servers using the `sudo vi chrony.conf` command. In this example, the public tick.usask.ca and internal 192.168.1.50 NTP servers are

added. The `iburst` option speeds up the first synchronization and the `prefer` option advises chrony which NTP server you want to use if available.

```
[kono@localhost etc]$ sudo vi chrony.conf
# Use public servers from the pool.ntp.org project.
# Please consider joining the pool (https://www.pool.ntp.org/join.html).

server tick.usask.ca iburst prefer
server 192.168.1.50 iburst
# server 0.centos.pool.ntp.org iburst
# server 1.centos.pool.ntp.org iburst
# server 2.centos.pool.ntp.org iburst
# server 3.centos.pool.ntp.org iburst

# Record the rate at which the system clock gains/losses time.
driftfile /var/lib/chrony/drift

# Allow the system clock to be stepped in the first three updates
# if its offset is larger than 1 second.
makestep 1.0 3

# Enable kernel synchronization of the real-time clock (RTC).
rtcsync

# Enable hardware timestamping on all interfaces that support it.
#hwtimestamp *

# Increase the minimum number of selectable sources required to adjust
# the system clock.
#minsources 2

# Allow NTP client access from local network.
#allow 192.168.0.0/16

# Serve time even if not synchronized to a time source.
#local stratum 10

# Specify file containing keys for NTP authentication.
#keyfile /etc/chrony.keys

# Specify directory for log files.
logdir /var/log/chrony

# Select which information is logged.
#log measurements statistics tracking
```

3. Restart chrony for the changes to take effect using the command `sudo systemctl restart chronyd`.

```
[kono@localhost etc]$ sudo systemctl restart chronyd
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ====
Authentication is required to manage system services or units.
Authenticating as: kono
Password:
==== AUTHENTICATION COMPLETE ====
[kono@localhost etc]$
```

4. Confirm the new configuration of the **chrony.conf** file.

```
[kono@localhost etc]$ chronyc sources -v
210 Number of sources = 4

.-- Source mode  '^' = server, '=' = peer, '#' = local clock.
/ .- Source state '*' = current synced, '+' = combined , '-' = not
combined,
| /  '?' = unreachable, 'x' = time may be in error, '~' = time too
variable.
||
||                                     .- xxxx [ yyyy ] +/-
zzzz
||      Reachability register (octal) -.      |  xxxx = adjusted
offset,
||      Log2(Polling interval) --.      |      |  yyyy = measured
offset,
||                                     \      |      |  zzzz = estimated
error.
||                                     |      |      \
MS Name/IP address          Stratum Poll Reach LastRx Last sample
=====
^- stervandc01a.teradici.lo>    3   6   17    4  -1183us[-1219us] +/-
104ms
^* time.usask.ca              1   6   17    3   -12us[ -48us] +/-
15ms
^- GSSDC01.terase.local       3   6   17    3  -4130us[-4130us] +/-
132ms
^- GSSDC02.terase.local       4   6   17    3  -3260us[-3260us] +/-
166ms
[kono@localhost etc]$
```

5. View status in real time using the command `watch chronyc tracking`

```
[kono@localhost etc]$ watch chronyc tracking
Every 2.0s: chronyc tracking

Reference ID      : 80E99AF5 (time.usask.ca)
Stratum          : 2
Ref time (UTC)   : Fri Mar 22 15:50:33 2019
System time      : 0.000050575 seconds slow of NTP time
Last offset      : -0.000054492 seconds
RMS offset       : 0.000197914 seconds
Frequency        : 35.545 ppm slow
Residual freq    : -0.001 ppm
Skew             : 0.082 ppm
Root delay       : 0.029674415 seconds
Root dispersion  : 0.000992690 seconds
Update interval  : 2078.7 seconds
Leap status      : Normal
```

Disabling the Chrony

If required, disable chrony by issuing the following commands:

1. `sudo systemctl stop chronyd` to stop the chronyd service
2. `sudo systemctl disable chronyd` to disable the chrony service.

Issue the `systemctl status chronyd` command to confirm chrony is disabled.

SSH Security Considerations

The following SSH configuration considerations will help secure the Management Consoles underlying OS SSH package. Thorough knowlegde of using Linux commands is assumed.

These considerations are based on the CentOS wiki which contain additional configurations and can be found at <https://wiki.centos.org/HowTos/Network/SecuringSSH>.

The following configurations are separated individually but you can make all these changes at once if you decide that all these configurations conform to your IT departments security policy.

Disable Root Login

1. Edit `/etc/ssh/sshd_config`

```
# Prevent root logins:  
PermitRootLogin no
```

2. Restart SSH

```
$ sudo service sshd restart
```

Limit User Logins

1. Edit `/etc/ssh/sshd_config`

```
# Limit User Logins to the following  
AllowUsers admin
```

2. Restart SSH

```
$ sudo service sshd restart
```

Disable SSH Protocol 1

1. Edit `/etc/ssh/sshd_config`

```
# Protocol 2,1  
Protocol 2
```

2. Restart SSH

```
$ sudo service sshd restart
```

Use Public/Private Keys for authentication and disable Password Authentication

1. Generate public and private certificate.

```
$ ssh-keygen -t rsa
```

- Either specify a file name or accept the default.
- If you want to be asked for a password everytime you connect, supply a passphrase.
- A private (`id_rsa` by default) and a public key (`id_rsa.pub` by default) will be created in the `~/.ssh` directory.

2. In the Management Console, ssh as admin and copy the public key in the `~/.ssh` folder. You may need to create the `~/.ssh` folder.

3. Install the public key into the `authorized_keys` list:

```
$ cat id_rsa.pub >> ~/.ssh/authorized_keys
```

4. Set permissions on the `.ssh` directory and `authorized_keys` file

```
$ chmod 700 ~/.ssh  
$ chmod 600 ~/.ssh/authorized_keys
```

5. Enable SSH public key authentication

a. Edit `/etc/ssh/sshd_config`

```
#Enable Public Key authentication  
PubkeyAuthentication yes
```

b. Restart SSH

```
$ sudo service sshd restart
```

6. In the workstation where you will run the ssh client, copy the private key in the ~/.ssh folder. Set the permissions as follows:

```
$$$  
$ chmod 700 ~/.ssh  
$ chmod 600 ~/.ssh/id_rsa  
$$$
```

7. Test the SSH connection using public/private keys by using SSH to connect to your VM from a different VM where you have copied your generated SSH key

```
$ ssh admin@your_mc_ip_or_fqdn -i ~/.ssh/id_rsa
```

8. Disable password authentication.

a. Edit /etc/ssh/sshd_config

```
# Disable password authentication forcing use of keys:  
PasswordAuthentication no
```

b. Restart SSH

```
$ sudo service sshd restart
```

Identity Provider(IDP) Integrations

Create Self-Signed Certificate

Management Console by default contains a self-signed certificate that can be used for SAML encryption. However, some organizations prefer to use their own self-signed certificates. In order to complete these steps, you may need to install a version of OpenSSL if you don't have one installed already.

If you want to update Management Console with a new self-signed certificate, perform the following steps:

STEP 1: GENERATE RSA PRIVATE KEY

To generate a RSA private key, at the command prompt, run the following command:

```
openssl command: openssl genrsa -out <key_output_path> <modulus_bit_length>
```

Example:

```
openssl genrsa -out samlkey.key 2048
```

```
D:\development\KEYSTOREGUIDE>openssl genrsa -out samlkey.key 2048
Generating RSA private key, 2048 bit long modulus
.....+++
.....+++
unable to write 'random state'
e is 65537 (0x10001)

D:\development\KEYSTOREGUIDE>
```

STEP 2: GENERATE CERTIFICATE REQUEST

Once a private key has been generated, you can create a certificate request which is needed to generate a self-signed certificate. The openssl command `openssl req -new -key <key_path> -out <request_output_path>` will be used to generate the certificate request.

Example:


```
openssl req -new -key samlkey.key -out samlcertrequest.csr
```

You will be prompted to enter the attributes such as country name, province, email address, etc.

```
D:\development\KEYSTOREGUIDE>openssl req -new -key samlkey.key -out
samlcertrequest.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:IN
State or Province Name (full name) [Some-State]:AP
Locality Name (eg, city) []:HYD
Organization Name (eg, company) [Internet Widgits Pty Ltd]:PRIME
Organizational Unit Name (eg, section) []:SECA
Common Name (e.g. server FQDN or YOUR name) []:PRIME
Email Address []:abc@example.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:password
An optional company name []:PRIME

D:\development\KEYSTOREGUIDE>
```

STEP 3: GENERATE CERTIFICATE

Once you have a private key and certificate request, you are ready to create a self-signed certificate.

```
openssl x509 -req -days <expiry_in_days> -in <cert_request_path> -signkey
<private_key_path> -out <cert_output_path>
```

Example:

```
openssl x509 -req -days 3650 -in samlcertrequest.csr -signkey samlkey.key -out
samlcert.crt
```

Note: The above generated certificate(samlcert.crt) should be uploaded in IDP.

```
D:\development\KEYSTOREGUIDE>openssl x509 -req -days 3650 -in
samlcertrequest.csr -signkey samlkey.key -out samlcert.crt
Signature ok
subject=/C=IN/ST=AP/L=HYD/O=PRIME/OU=SECA/CN=PRIME/
emailAddress=abc@example.com
Getting Private key
unable to write 'random state'

D:\development\KEYSTOREGUIDE>
```

Okta Reference

This reference article describes an integration between Management Console and Okta's authentication software. The basic configuration principals should apply for most IDPs.

Okta Configuration

1. Register for an account at Okta.com.
2. Accept the multifactor authentication requirement.
3. Sign in to your account.
4. Create an application in Okta.
 - a. From the top left accordion button, select the Applications menu and click **Applications > Create App Integration**.
 - b. Select **SAML2.0** sign on method then **Next**.
 - c. Enter a name and optional logo (i.e. Management Console Vancouver) and select **Next**.
 - d. Enter your SAML settings:
 - **Single sign on URL:** <MC IP Address>/login/saml2/sso/idp
 - **Use this for Recipient URL and Destination URL:** selected
 - **Allow this app to request other SSO UIRLS:** deselected
 - **Audience URI:** <MC IP Address>/saml2/service-provider-metadata/idp
 - **Default Relay State:** leave default (empty)
 - **Name ID Format:** leave default value **Unspecified**
 - **Application username:** leave default value **Okta username**
 - **Response:** Signed (default)
 - **Update application username on:** leave default value **Create and update**

SAML Settings		Edit
GENERAL		
Single Sign On URL		https://10.12.56.139/login/saml2/sso/idp
Recipient URL		https://10.12.56.139/login/saml2/sso/idp
Destination URL		https://10.12.56.139/login/saml2/sso/idp
Audience Restriction		https://10.12.56.139/saml2/service-provider-metadata/idp
Default Relay State		
Name ID Format		Unspecified
Response		Signed
Assertion Signature		Signed

Show Advanced Settings

The defaults can be used unless you would like to use encrypted assertions. Encryption secures the assertion between the sender and receiver. See the caution note on **Using encrypted assertions** for configuration information on using Assertion Encryption. As of publication of this article, the advanced default settings are:


- **Assertion Signature:** Signed (default)
- **Signature Algorithm:** RSA-SHA256 (default)
- **Digest Algorithm:** SHA256 (default)
- **Assertion Encryption:** Unencrypted (default)

⚠ Using encrypted assertions

Encrypted assertions require you to upload the encryption certificate to Okta and is obtained by downloading it from the Management Console IDP Configuration tab. You cannot upload an encryption certificate that is expired, however if the expiry date is reached after it is being used, encryption assertions will continue to work as the expiry date is not monitored after implementation.

Selecting Encrypted for the Assertion Encryption type displays additional settings which the defaults can be used. The additional settings are:

- **Encryption Algorithm** set to AES256-CBC
- **Key Transport Algorithm** set to RSA-OAEP

Assertion Encryption ?	Encrypted
Encryption Algorithm ?	AES256-CBC
Key Transport Algorithm ?	RSA-OAEP
Encryption Certificate ?	<div> samcert.crt X Uploaded by SandhyaFirst SandhyaLast on Tue Feb 02 10:38:06 UTC 2021 CN=MC SAML SECURITY Valid from 2021-01-09T16:40:10.000Z to 2031-01-07T16:40:10.000Z Certificate expires in 3626 days</div>

- **Enable Single Logout:** deselected (default)
- **Assertion Inline Hook:** None(disabled) (default)
- **Authentication context class:** PasswordProtectedTransport (default)
- **Honor Force Authentication:** Yes (default)
- **SAML Issuer ID:** [http://www.Okta.com/\\${org.externalKey}](http://www.Okta.com/${org.externalKey}) (default)

Configuring FirstName and LastName

1. Enter the following two attribute statements in the Attribute Statements (optional) section:

- **Name:** firstName
Name format: Unspecified
Value: user.firstName

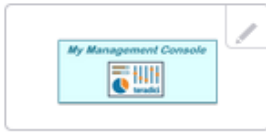
- **Name:** lastName
Name format: Unspecified
Value: user.lastName

2. Select **Next**.
3. Answer Okta's support question to be able to select **Finish** on the next screen. Continue with next step obtaining IDP metadata file.

Obtaining IDP Metadata File

1. From the Application settings Sign On tab, select the **Identity Provided metadata** link.

← Back to Applications



My Management Console

Active ▾



[View Logs](#) [Monitor Imports](#)

- General
- Sign On**
- Import
- Assignments

Settings

[Edit](#)

Sign on methods

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.

Application username is determined by the user profile mapping. [Configure profile mapping](#)

SAML 2.0

Default Relay State



SAML 2.0 is not configured until you complete the setup instructions.

[View Setup Instructions](#)

[Identity Provider metadata](#) is available if this application supports dynamic configuration.

Credentials Details

Application username format Okta username

Update application username on Create and update

[Update Now](#)

Password reveal Allow users to securely see their password (Recommended)

2. Right click on the newly opened page containing the XML metadata and save the page. This file is used in the Management Console IDP configuration.

Okta Multi-factor Authentication

In this reference article, we will change the default to Duo as the application authenticator performing MFA as an example for you to follow in the event you are already using a different authenticator. By default, Okta enables multi-factor authentication (MFA) using their authenticator application.

MFA can be achieved using a variety of different methods to improve security Management Console sign in security. This article provides Okta configurations for the following MFA authentication types:

- [Email Authentication](#)
- [DUO Authentication](#)
- [SMS Authentication](#)
- [Smart Card Authentication](#)

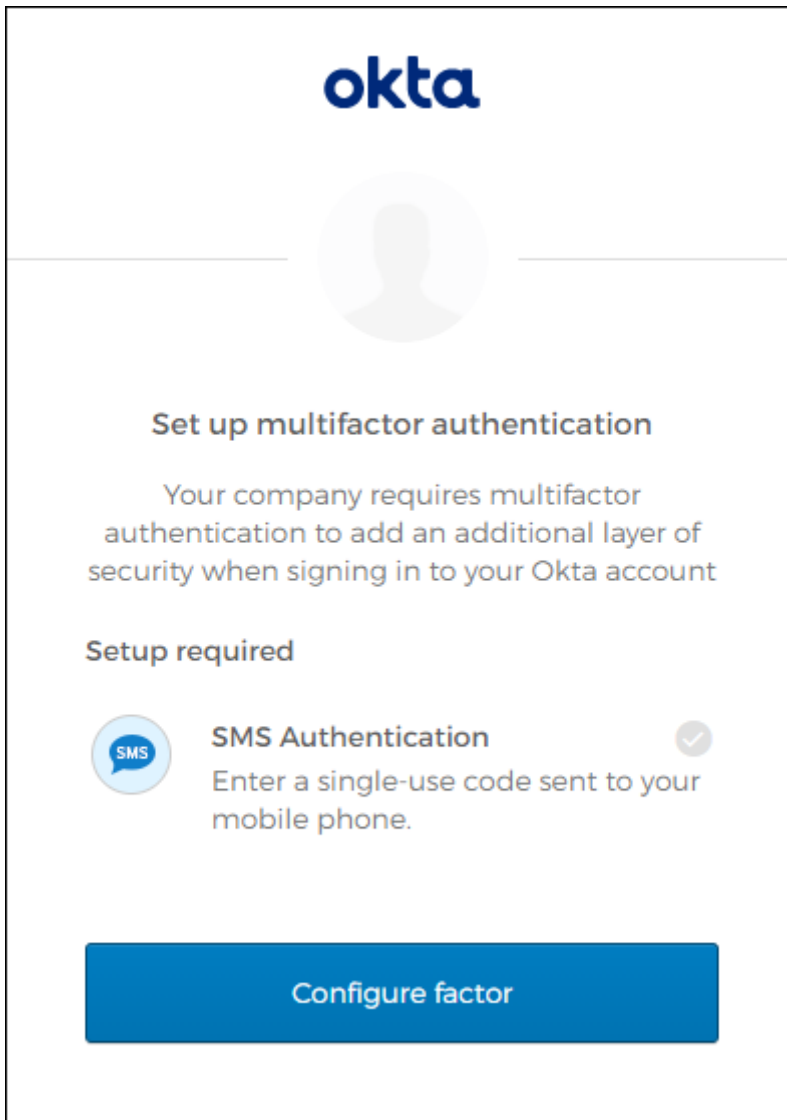
EMAIL AUTHENTICATION CONFIGURATION

1. From the **Security** tab, select **Multifactor**. You will be placed on the **Factor Types** setting tab.
2. Select **Email Authentication** and click the **Edit** link.
3. Select **Active** for Email Authentication and configure the *token lifetime* setting to comply with your corporate security policies.
4. Click **Save**.
5. Select the **Factor Enrollment** tab and select **Edit**.
6. Update **Assigned to groups** and select **Required** for Email Authentication and click **Update Policy**.
7. From the **Applications** window, select your appliance and then select the **Sign On** tab.
8. Select **Add Rule** under Sign On Policy.
9. Enter a rule name.
10. Under the actions section, check **Prompt for factor - Multifactor settings** and select **Every sign on** and save. (You can configure other options to your corporate security policies)

SMS AUTHENTICATION CONFIGURATION

1. Navigate to the **Security > Multifactor > SMS Authentication**.
2. Select **Activate** from the SMS Authentication drop down option.
3. Select the **Factor Enrollment** tab.
4. Select **Edit** and update Assigned to groups (use Everyone group for all users).
5. Change SMS Authentication to **Required** for Eligible Factors.
6. Add a sign on policy to Management Console.
 - a. Navigate to **Applications > Applications** and select your Management Console application.
 - b. Select the **Sign On** tab.
 - c. Click on **Add Rule** button in the Sign On Policy section.
 - d. Enter a **Rule Name**.
 - e. Under the *Actions* section, check **Prompt for factor - Multifactor settings** and select **Every sign on** (Configure other options according to your corporate security policies).
 - f. Ensure the drop down option for **When all the conditions above are met, sign on to this application is: Allowed**.
 - g. Select **Save**.

When an IDP user, attempts to sign into Management Console the user will be presented with a notice from the SSO provider (in this example Okta) that MFA is required.



The next screen will allow the IDP user to enter a cell number that will receive a code via SMS. Once the cell number is entered, another screen will allow the IDP user to verify the SMS code and if successful, they will be logged into Management Console.

Smart Card Authentication

The reference instructions for smart card authentication can be found [here](#).

DUO Authentication

For this example we are using DUO as the MFA application to approve the Single Sign on.

1. Sign up for a DUO account and log into your account.
2. Navigate to **Applications > Protect an Application**.
3. Locate *Okta* and select the **Protect** button.

4. Copy your **Integration key**, **Secret key**, and **API hostname** to use in your Okta configuration. Destroy your copied versions after you finish your configuration.

Okta Configuration

1. From the Okta dashboard navigate to **Security > Multifactor**.
2. Select **Duo Security** and click on the **Edit** link.
3. Enter the **Integration key**, **Secret key**, and **API hostname** appropriately and use the name format used to log in to Okta.
4. **Activate** Duo Security from the drop down option and select **Save**.
5. Navigate to **Security > Authentication** and select the **Sign On** tab.
6. Select **Default Policy**, and then select the **Add Rule** button.

You can either add a new rule for Duo Authentication to an existing Okta sign-on policy, or create a new policy for Duo and assign it to specific groups. In this example, we'll turn on Duo for all users in the **Default Policy**.

 - a. Enter a descriptive rule name.
 - b. Leave defaults and ensure **Prompt for Factor** is checked along with the **Every Time** option.
 - c. Select **Create Rule**.

User Management

To assign users to the Management Console application in Okta perform the following steps.

1. Login to Okta and navigate to **Directory > People** and click the **Add person** button, fill in the fields and click **Save**.

The screenshot shows the Okta Directory page. The navigation bar at the top includes 'Get Started', 'Dashboard', 'Directory', 'Applications', 'Security', 'Workflow', 'Reports', 'Settings', 'Upgrade', and 'My Apps'. A red circle with the number '1' is around 'Get Started', and an arrow labeled '1' points to the 'Directory' link. Below the navigation bar, the 'People' link is highlighted with a blue bar and a red circle with the number '2', with an arrow labeled '2' pointing to it. Below 'People' are buttons for 'Add Person', 'Reset Passwords', 'Reset Multifactor', and 'More Actions'. A search bar is present above a table with columns 'Person & Username', 'Primary Email', and 'Status'. The table lists users under categories like 'Everyone', 'ONBOARDING', 'ACTIVE', and 'INACTIVE'. The footer contains copyright information and links for 'Download Okta Plugin' and 'Feedback'.

	Person & Username	Primary Email	Status
Everyone 2	mcuser AD mcuser@abc.net	mcuser@abc.net	Active
ONBOARDING	Srinivas Dasari srao@teradici.com	srao@teradici.com	Active
Staged	0		
Pending user action	0		
ACTIVE			
Active	2		
Password Reset	0		
Locked out	0		
INACTIVE			
Suspended	0		
Deactivated	0		

The screenshot displays the Okta People management interface. At the top, a navigation bar includes the Okta logo, a 'Get Started' button, and links for Dashboard, Directory, Applications, Security, Workflow, Reports, Settings, and an Upgrade button. A 'My Apps' dropdown is also present. The main content area is titled 'People' and features a search bar and a list of user categories: Everyone, ONBOARDING (Staged, Pending user action), ACTIVE (Active, Password Reset, Locked out), and INACTIVE (Suspended, Deactivated). A modal window titled 'Add Person' is open, containing the following fields and options:

- User type:** A dropdown menu set to 'User'.
- First name:** A text input field.
- Last name:** A text input field.
- Username:** A text input field with a placeholder 'Must be an email'.
- Primary email:** A text input field.
- Groups (optional):** A section indicating 'You haven't added any groups'.
- Password:** A dropdown menu set to 'Set by user'.
- Send user activation email now**

At the bottom of the modal are three buttons: 'Save', 'Save and Add Another', and 'Cancel'. The footer of the page contains copyright information: © 2020 Okta, Inc. Privacy, Version 2020.12.1, OK12 Cell (US), Status site, Download Okta Plugin, and Feedback.

2. Navigate to **Applications**, click the **Assign** button and click the Assign link beside the people you want to assign Management Console too.

← Back to Applications



Management Console

Active ▾



View Logs

General Sign On Mobile Import **Assignments**



Assign ▾ **Convert Assignments** **People** ▾

FILTERS	Person	Type	
People	Srinivas Dasari srao@teradici.com	Individual	
Groups	mcuser AD mcuser@abc.net	Individual	

REPORTS

- Current Assignments
- Recent Unassignments

SELF SERVICE

You need to enable self service for org managed apps before you can use self service for this app.

[Go to self service settings](#)

Requests Disabled

← Back to Applications



Assign Management Console to People



General Sign On

Mcuser Test
mctest@gmail.com



Assign ▾ **Con**

FILTERS

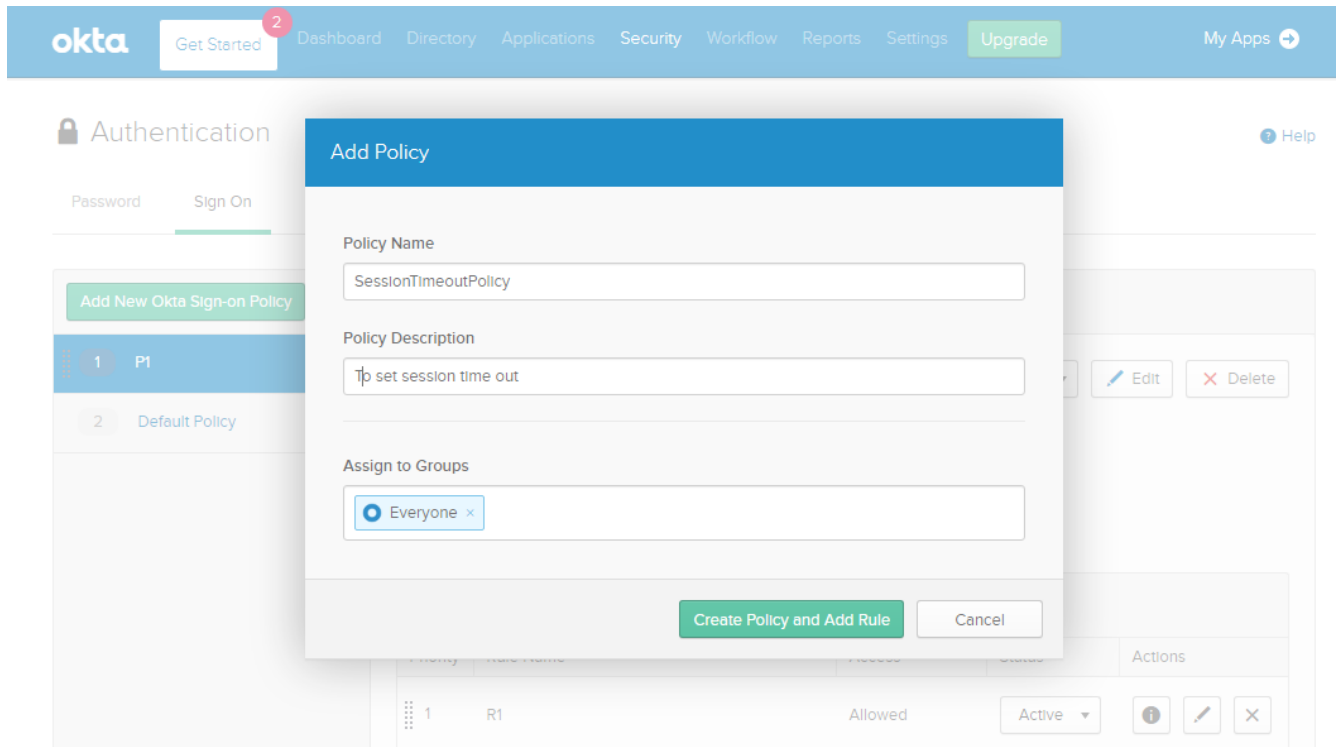
People

Groups

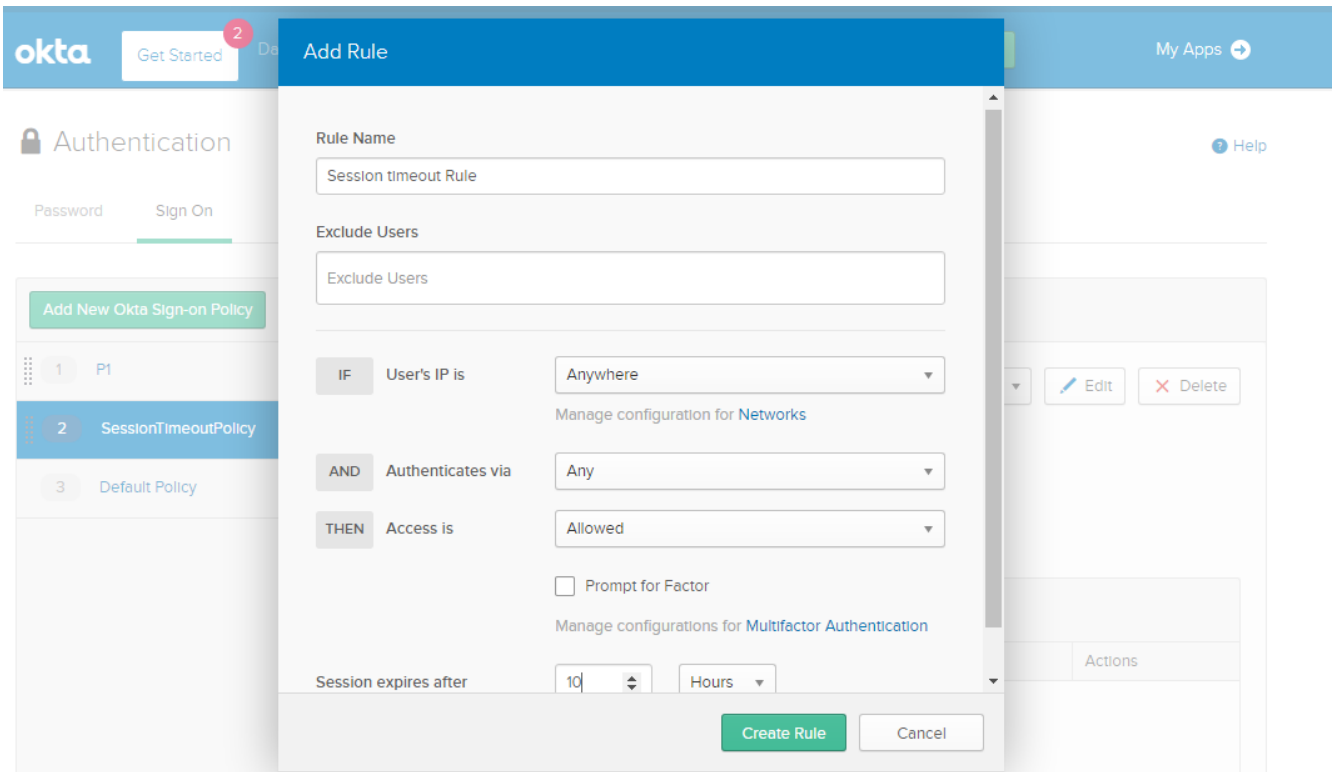
Session Time Out

Set session timeout rules to groups in Okta.

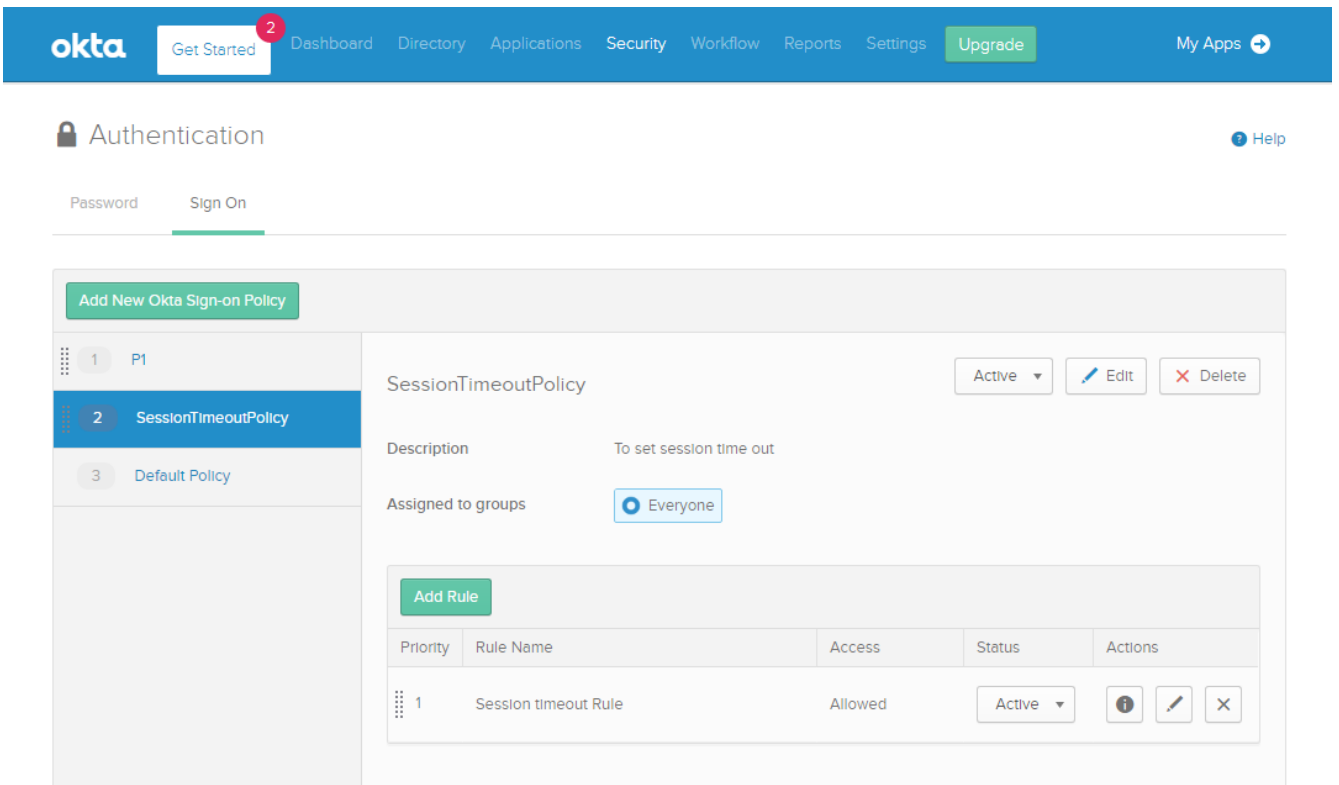
1. Navigate to **Security > Authentication** and select the **Sign On** tab.
2. Click the **Add New Okta Sign-on Policy** button, enter a policy name and click **Create Policy and Add Rule**.



3. Enter a rule name, set the session expiry and select **Create Rule**.



4. Verify the configuration is active.



Smartcard Authentication with SSO

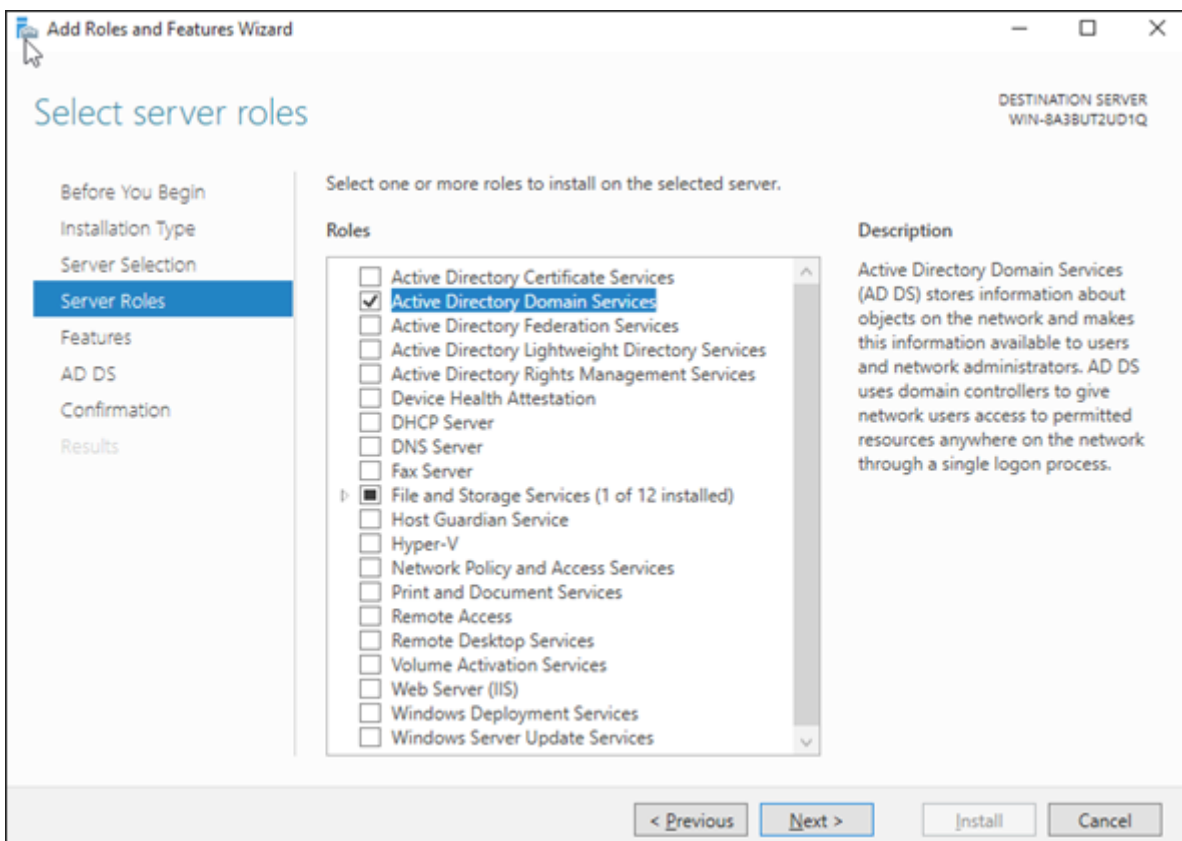
This article will provide you with basic details to configure a Domain Controller, add test users and integrate the users for smart card authentication using Okta as the IDP. This reference is based on using Windows Server 2019 Standard with Okta IDP for Single Sign-on.

After completing these steps you will be able to:

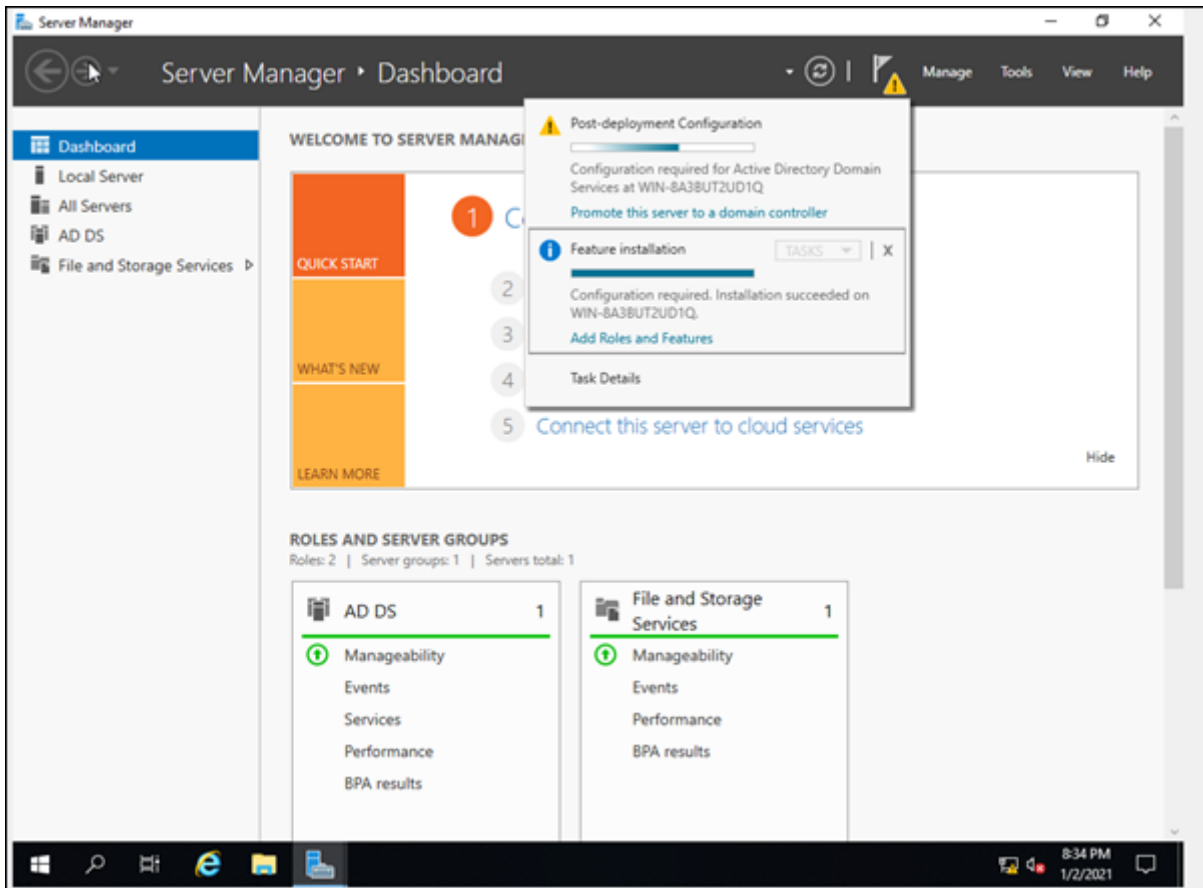
- Use Okta to login with Smart card authentication using an Active directory user certificate.
- Use Okta to login using the username and password of an Active directory user.

Windows Server Configuration

1. Open Server Manager from the Windows Server search field.
2. Select the **Active Directory Domains and Services** as a server role from the **Add Roles and Features Wizard** and click **Next** then **Install**.

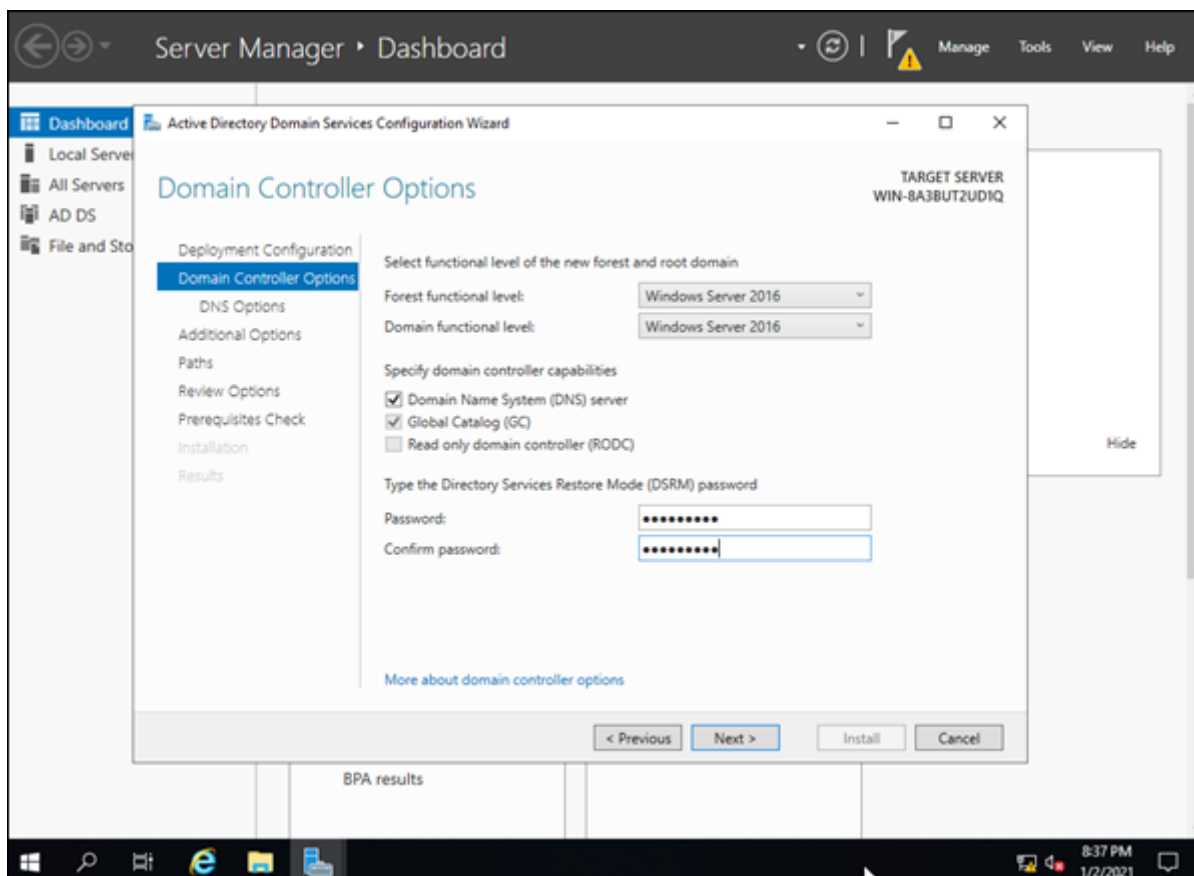


3. Click the flag and select **Promote this Server to a DC** (Domain Control).

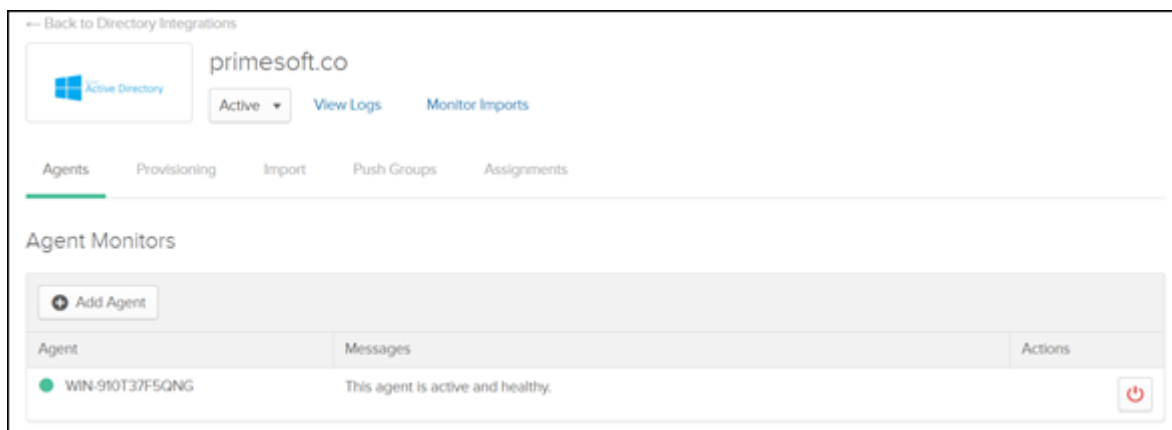


4. Select **Add a new forest** and create a domain name and click **Next**.

5. Create a password and select **Next** until the install button shows.



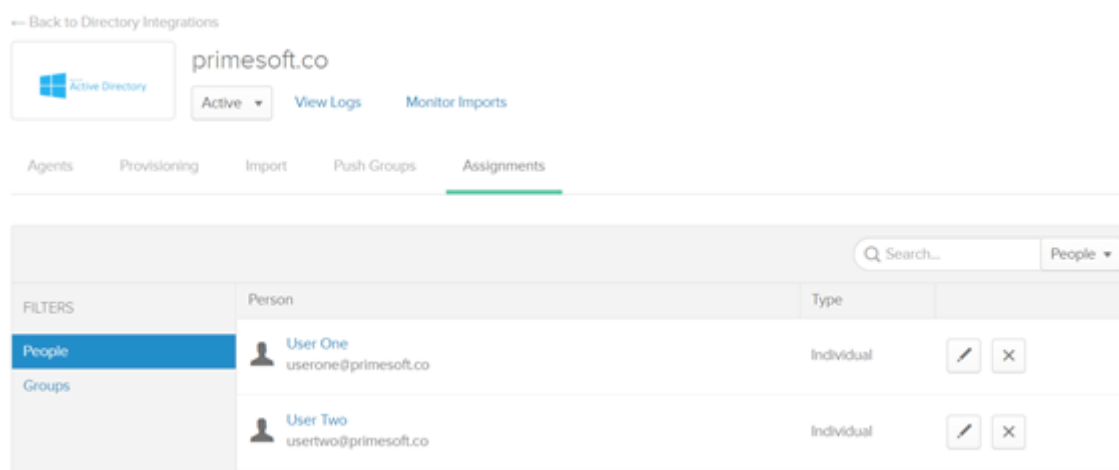
6. Select **Install**.
7. Restart the server and create some users and groups in Active Directory Users and Computers.
8. From the Domain Controller that was just created, login to Okta, navigate to **Settings > Downloads** and download the Okta AD Agent and install it.
9. Enter the AD Domain Name.
10. Create an Okta Service Account as recommended and enter the password.
11. Enter the Okta URL, once redirected to the Okta page, enter the Okta credentials and select **Allow access**.
12. From the Okta dashboard, navigate to **Directory > Directory Integrations**.
13. Select the AD Server name and configure it using the default settings. Once completed, the agent displays as active.



14. Click on the **Import** tab and Import now with full import.

15. After the import, highlight the users and select **Assign the users**.

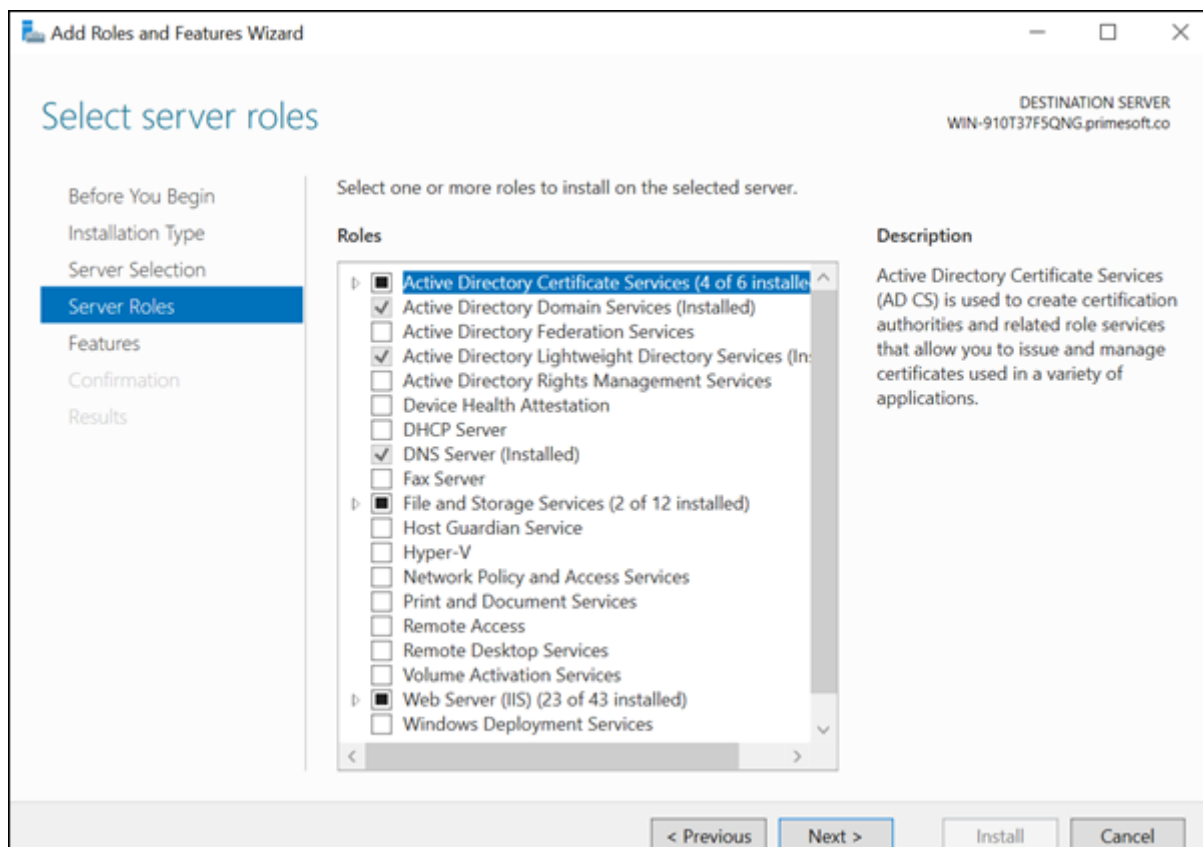
After assigning the users you can see the AD users in the *Assignments* tab.



16. Navigate to **Directory > People** and **Activate** the imported AD users.

After activating the AD users, try to login Okta with the AD credentials to verify a working configuration.

17. From the Domain Controller server, navigate to **Server Manager > Manage > Add Roles and Features**, select **Active Directory Certificate Services** and select **Next**.

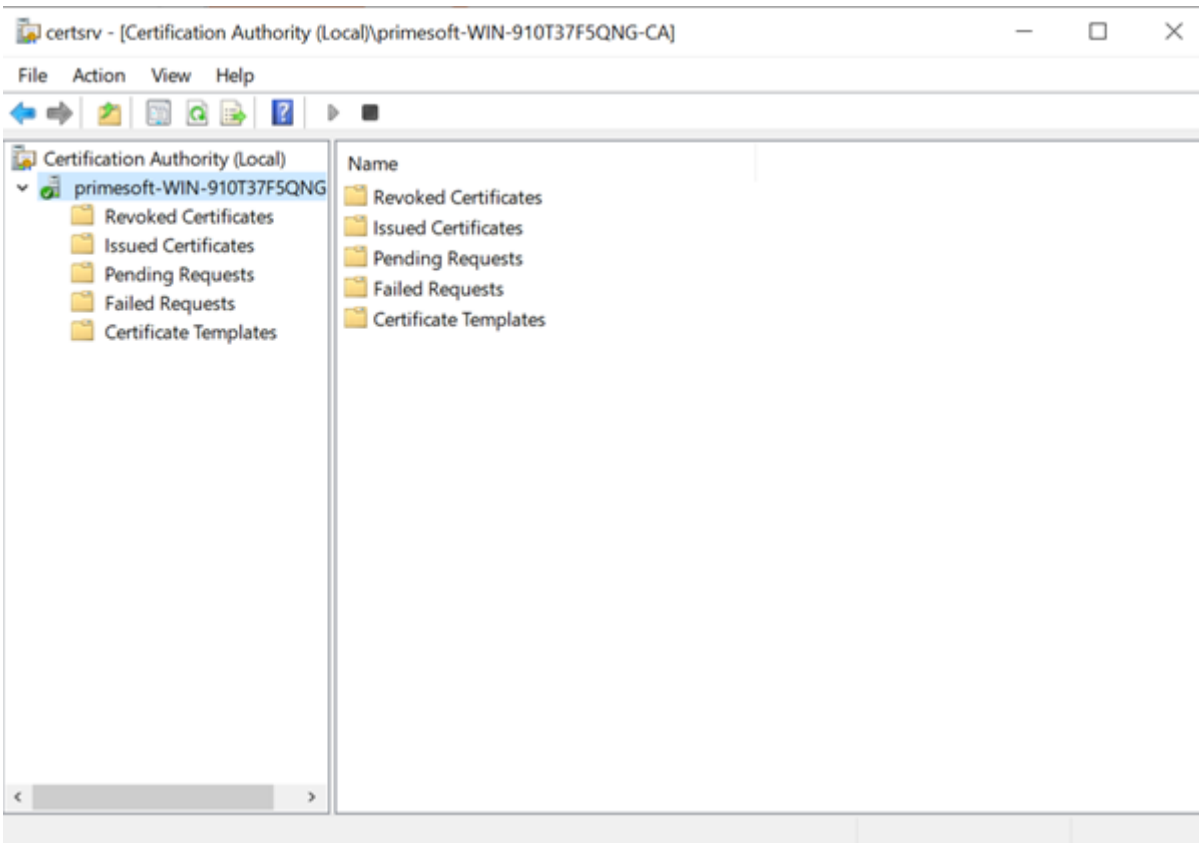


18. Select **Certificate Authority** and **Certificate Authority Web Enrollment** and click **Install**.

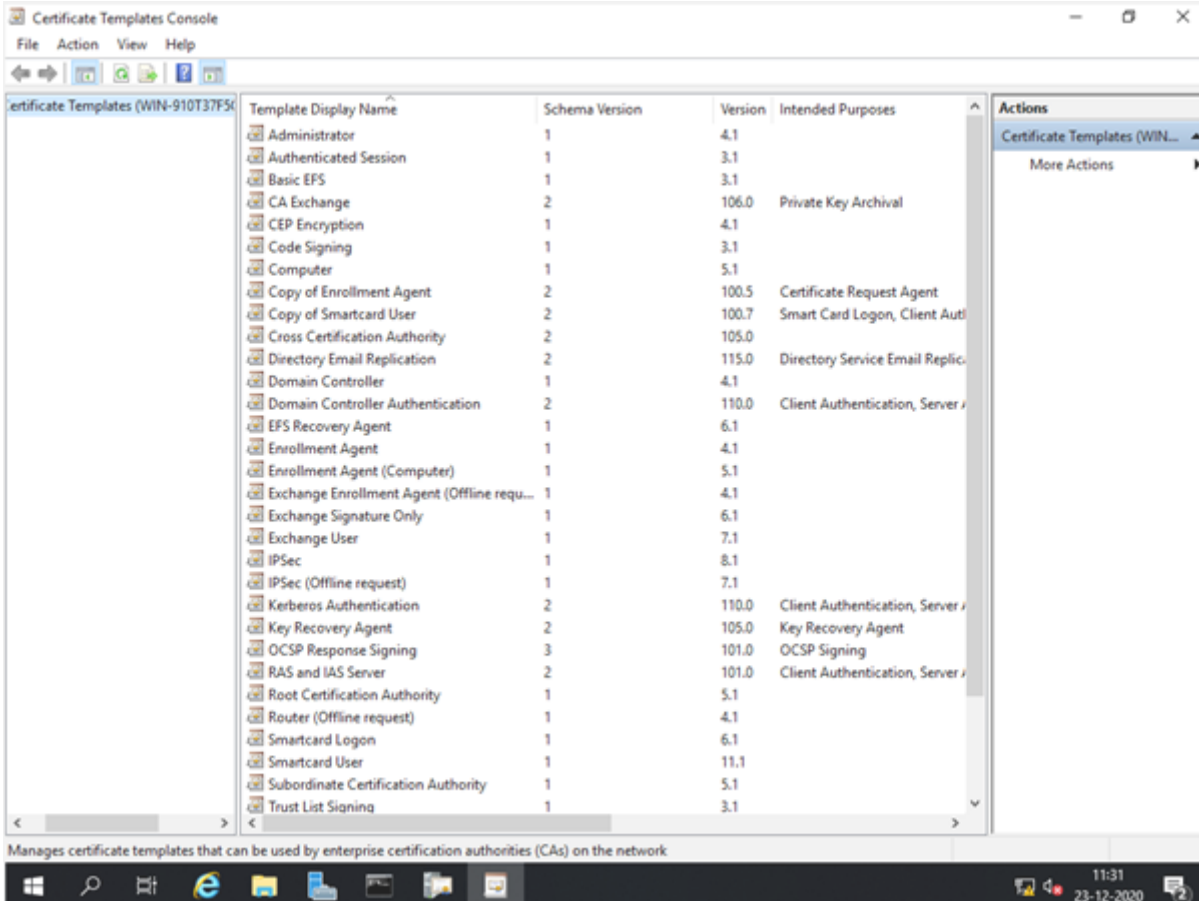
19. (22) From the Server Manager header, click the flag icon and click **Promote this Server to a certificate server**.

While Configuring Certificate Authority select Enterprise and Root CA

20. In the search bar, type **Certification Authority** and select your local CA.



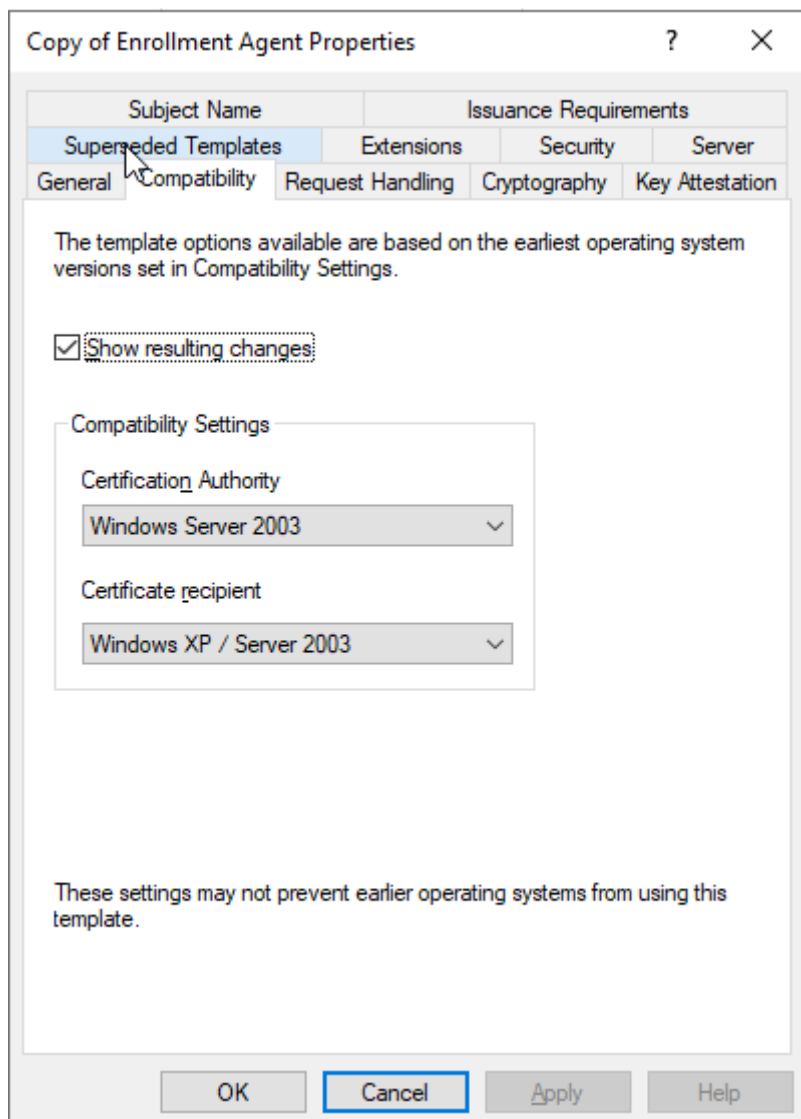
21. Right click **Certificate Template** and click **Manage**.



22. Right click **Enrollment Agent** and click **Duplicate Template**.
23. Right click **Duplicated Template** and click **Properties**.
24. From the **General** tab, select the **Publish Certificate in Active Directory** checkbox.

The screenshot shows a dialog box titled "Copy of Enrollment Agent Properties" with a question mark icon and a close button. The dialog has several tabs: "General", "Compatibility", "Request Handling", "Cryptography", and "Key Attestation". The "General" tab is selected. The "Subject Name" and "Issuance Requirements" sections are visible at the top. Below the tabs, there are two text input fields: "Template display name:" and "Template name:", both containing the text "Copy of Enrollment Agent". Below these fields are two dropdown menus: "Validity period:" set to "2 years" and "Renewal period:" set to "6 weeks". At the bottom of the dialog, there are four checkboxes: "Publish certificate in Active Directory" (checked), "Do not automatically reenroll if a duplicate certificate exists in Active Directory" (unchecked), and two other unchecked checkboxes. At the very bottom of the dialog are four buttons: "OK", "Cancel", "Apply", and "Help".

25. From the **Compatibility** tab and ensure **Windows Server 2003** is selected for *Certificate Authority* and *Certificate recipient* compatibility settings.



26. From the **Request Handling** tab, select **Signature** from the *Purpose* drop-down list and select the **Prompt the user during enrollment and require user input when the private key is used** radio button.
27. From the **Cryptography** tab, ensure the **Microsoft Base Smart Card Crypto Provider** checkbox is selected.

Copy of Enrollment Agent Properties ? X

Subject Name		Issuance Requirements		
Superseded Templates		Extensions	Security	Server
General	Compatibility	Request Handling	Cryptography	Key Attestation

Provider Category: Legacy Cryptographic Service Provider

Algorithm name: Determined by CSP

Minimum key size: 2048

Choose which cryptographic providers can be used for requests

Requests can use any provider available on the subject's computer

Requests must use one of the following providers:

Providers:

<input checked="" type="checkbox"/> Microsoft Enhanced Cryptographic Provider v1.0	▲	▲
<input checked="" type="checkbox"/> Microsoft Base Cryptographic Provider v1.0		
<input checked="" type="checkbox"/> Microsoft Base Smart Card Crypto Provider		
<input type="checkbox"/> Microsoft Enhanced RSA and AES Cryptographic Provider		▼
<input type="checkbox"/> Microsoft Strong Cryptographic Provider	▼	▼

Request hash: Determined by CSP

Use alternate signature format

OK Cancel Apply Help

28. From the **Subject** tab, ensure the **Include e-mail name in subject name** and **E-mail name** checkboxes are cleared.

Copy of Enrollment Agent Properties ? X

Superseded Templates	Extensions	Security	Server	
General	Compatibility	Request Handling	Cryptography	Key Attestation
Subject Name		Issuance Requirements		

Supply in the request

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

Build from this Active Directory information

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

Subject name format:

Fully distinguished name

Include e-mail name in subject name

Include this information in alternate subject name:

E-mail name

DNS name

User principal name (UPN)

Service principal name (SPN)

* Control is disabled due to [compatibility settings](#).

OK Cancel Apply Help

29. From the **Security** tab, ensure **Full Control** is selected for **Authenticated Users** and click OK.
30. Create a Group in Active Directory with one or two users and add them in the security tab with **Full Control** permissions and click OK.
31. From the **Certification Authority**, right click the **Certificate Template** folder and select **Manage**, then right click on **Smartcard User** and select **Duplicate Template**.
32. From the **General** tab of the Smartcard user properties dialog, set the *Validity* and *Renewal* periods and ensure **Publish certificate in Active Directory** is selected.

Copy of Smartcard User Properties ? X

Subject Name		Issuance Requirements		
Superseded Templates	Extensions	Security	Server	
General	Compatibility	Request Handling	Cryptography	Key Attestation

Template display name:
Copy of Smartcard User

Template name:
Copy of Smartcard User

Validity period: 1 years
Renewal period: 6 weeks

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

OK Cancel Apply Help

33. From the **Compatibility** tab, ensure **Windows Server 2003** is set for *Certificate Authority* and *Certificate recipient* compatibility options and that *Show resulting changes* is selected.

Copy of Smartcard User Properties ? X

Subject Name		Issuance Requirements		
Superseded Templates	Extensions	Security	Server	
General	Compatibility	Request Handling	Cryptography	Key Attestation

The template options available are based on the earliest operating system versions set in Compatibility Settings.

Show resulting changes

Compatibility Settings

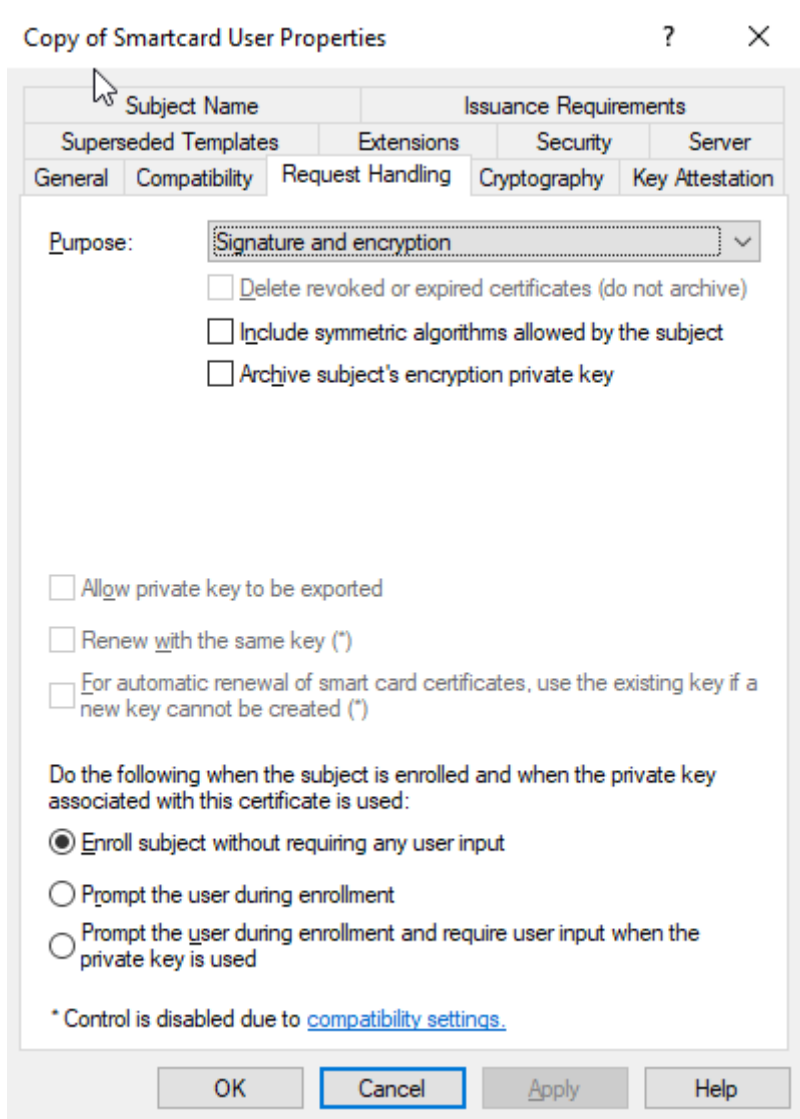
Certification Authority
Windows Server 2003

Certificate recipient
Windows XP / Server 2003

These settings may not prevent earlier operating systems from using this template.

OK Cancel Apply Help

34. From the **Request Handling** tab, select **Signature and encryption** from the *Purpose* option drop-down list and select the **Enroll subject without requiring any user input** radio button.



35. From the **Cryptography** tab, ensure the **Microsoft Base Smart Card Crypto Provider** option is selected.

Copy of Smartcard User Properties ? X

Subject Name		Issuance Requirements		
Superseded Templates	Extensions	Security	Server	
General	Compatibility	Request Handling	Cryptography	Key Attestation

Provider Category: Legacy Cryptographic Service Provider

Algorithm name: Determined by CSP

Minimum key size: 2048

Choose which cryptographic providers can be used for requests

Requests can use any provider available on the subject's computer

Requests must use one of the following providers:

Providers:

- Microsoft Base Smart Card Crypto Provider
- Microsoft DH SChannel Cryptographic Provider
- Microsoft Enhanced Cryptographic Provider v1.0
- Microsoft Enhanced DSS and Diffie-Hellman Cryptographic Pr
- Microsoft Enhanced RSA and AES Cryptographic Provider

Request hash: Determined by CSP

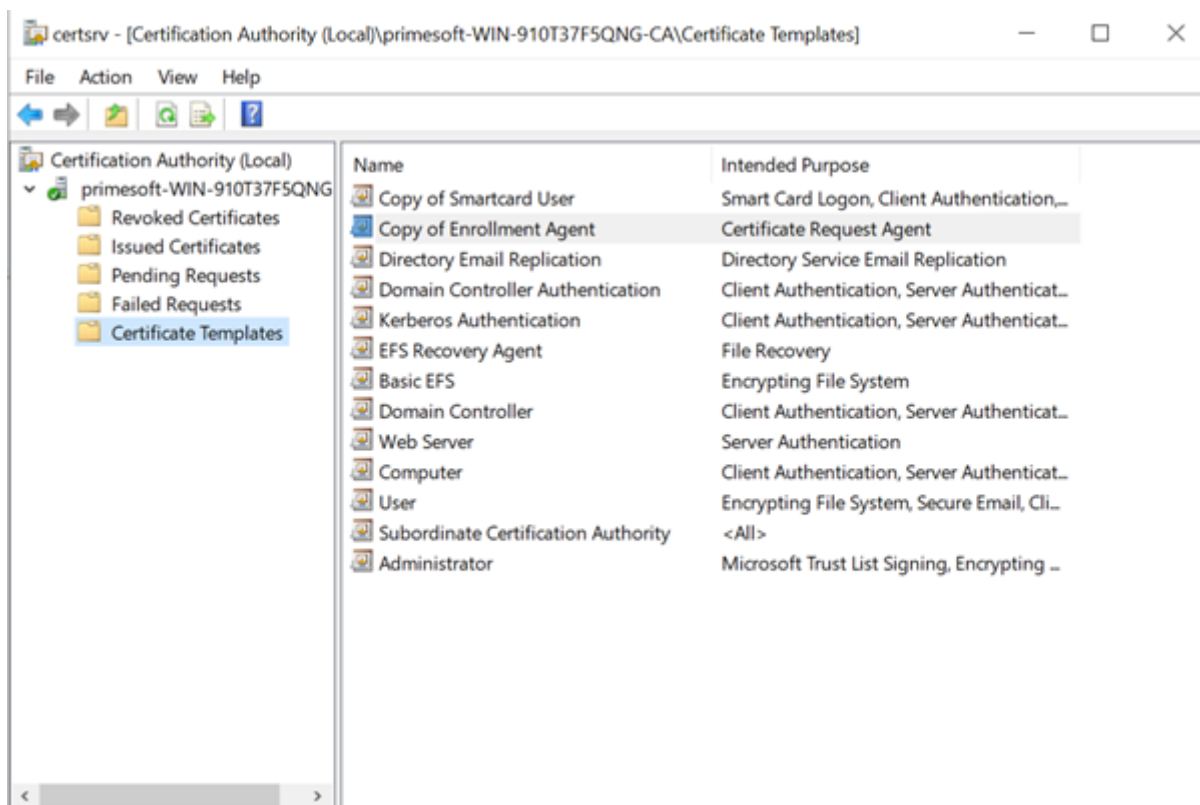
Use alternate signature format

OK Cancel Apply Help

36. From the **Subject** tab, clear the **Include e-mail name in subject name** and **E-mail name** options.

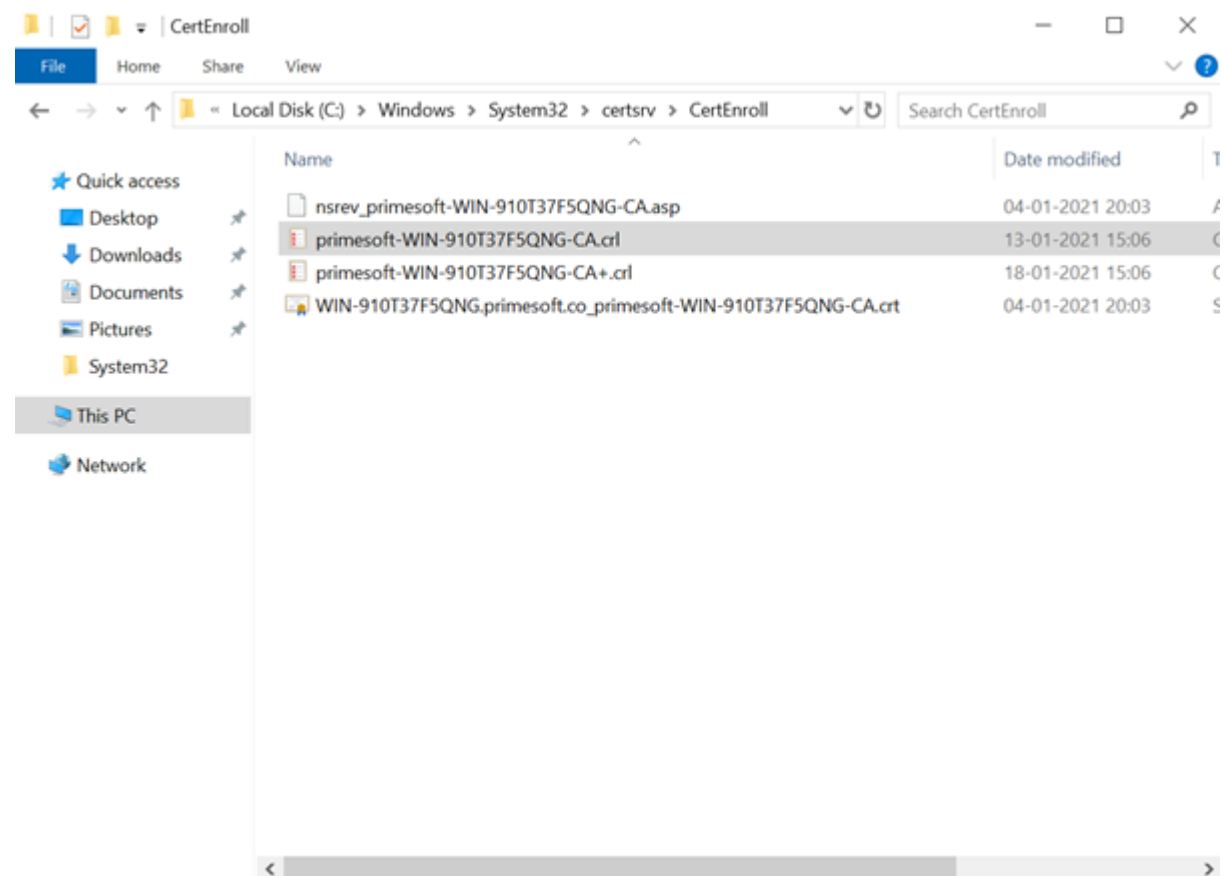
The screenshot shows a dialog box titled "Copy of Smartcard User Properties" with a question mark and a close button. The dialog has several tabs: "Superseded Templates", "Extensions", "Security", and "Server". The "Security" tab is active, and within it, the "Issuance Requirements" section is selected. This section contains two radio buttons: "Supply in the request" (unselected) and "Build from this Active Directory information" (selected). Under "Build from this Active Directory information", there is a text box for "Subject name format" with a dropdown menu set to "Fully distinguished name". Below this are several checkboxes: "Include e-mail name in subject name" (unselected), "Include this information in alternate subject name:" (with sub-options for "E-mail name", "DNS name", "User principal name (UPN)" which is checked, and "Service principal name (SPN)" which is unselected). At the bottom left, a note states: "* Control is disabled due to [compatibility settings](#)." The bottom of the dialog features four buttons: "OK", "Cancel" (highlighted with a blue border), "Apply", and "Help".

37. From the **Security** tab, select **Read, Write** and **Enroll** permissions for Authenticated Users.
38. Create a Group for smart card users in Active Directory with one or two users and add them in the Security tab with **Read, Write** and **Enroll** permissions and click OK.
39. (41) From the **Certification Authority**, right click the **Certificate Templates** and click **New > Certificate Template to issue** and select the two duplicated templates—**Copy of Enrollment Agent** and **Copy of Smartcard User**. After adding the templates, they are visible in the Certificate Templates folder.



40. Find the Certificate Revocation List certificate (extension is .crl) in **C:\Windows\System32\certsrv\CertEnroll** and create a customized link to this certificate using a format of **FQDN/Path/Certificate_Name**. The link must be reachable from both inside and outside of the server's network.

Example



Name	Date modified	Type
nsrev_primesoft-WIN-910T37F5QNG-CA.asp	04-01-2021 20:03	A
primesoft-WIN-910T37F5QNG-CA.crl	13-01-2021 15:06	C
primesoft-WIN-910T37F5QNG-CA+.crl	18-01-2021 15:06	C
WIN-910T37F5QNG.primesoft.co_primesoft-WIN-910T37F5QNG-CA.crt	04-01-2021 20:03	S

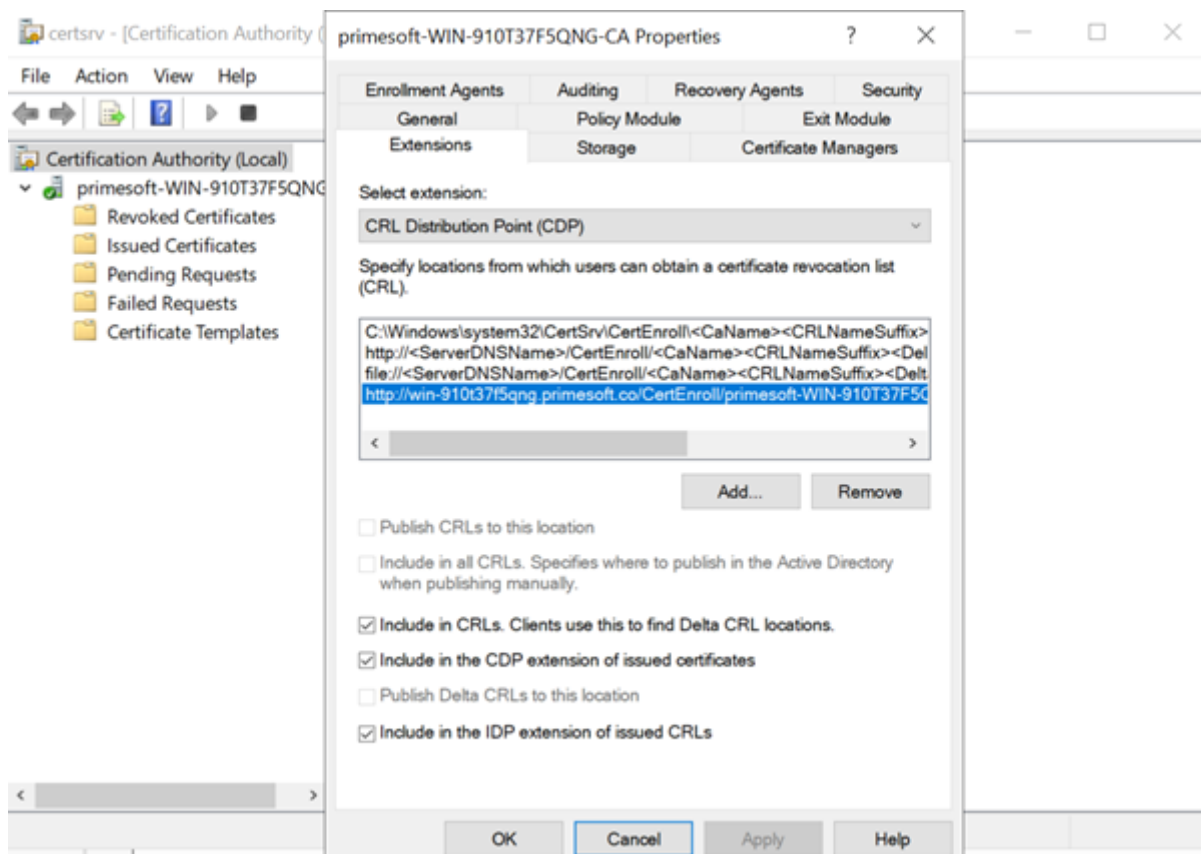
Certificate Revocation List Certificate Path

From the Certificate Revocation List Certificate Path image and the format criteria, this sample path would be:

<http://win-ti9upfujb93.primesoft.us/CertEnroll/primesoft-WIN-TI9UPFUJB93-CA.crl>

41. From the Certification Authority, right click on your **Domain Name** and click on **Properties**.
42. From the **Extensions** tab, select **CRL Distribution Point (CDP)** from the *Select extension* drop-down list, click Add to add the customized Certificate Revocation List certificate link, and ensure the following checkboxes are selected.
 - **Include in CRLs. Clients use this to find Delta CRL locations.**
 - **Include in the CDP extension of issued certificates.**
 - **Include in the IDP extension of issued CRLs**

Confirm the path has been added.



43. Restart the Certificate Authority Server.

Download the Chain Certificate from the Certificate Authority Server

1. Use the URL of the Certificate Authority Server to download the certificate. The URL will have the format similar to **http://<server_IP_address>/certsrv/**.
2. Click on the **Download CA certificate chain** link and download your certificate.

Microsoft Active Directory Certificate Services -- primesoft-WIN-910T37F5QNG-CA

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, install this CA certificate chain.

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.

CA certificate:

Current [primesoft-WIN-910T37F5QNG-CA]

Encoding method:

DER

Base 64

[Download CA certificate](#)

[Download CA certificate chain](#)

[Download latest base CRL](#)

[Download latest delta CRL](#)

Okta Configuration

1. Login to Okta and navigate to **Security > Identity Providers > Add Identity Providers > Add Smart Card** and upload the certificate chain that was downloaded in the previous steps.

Edit Identity Provider

GENERAL SETTINGS

Name

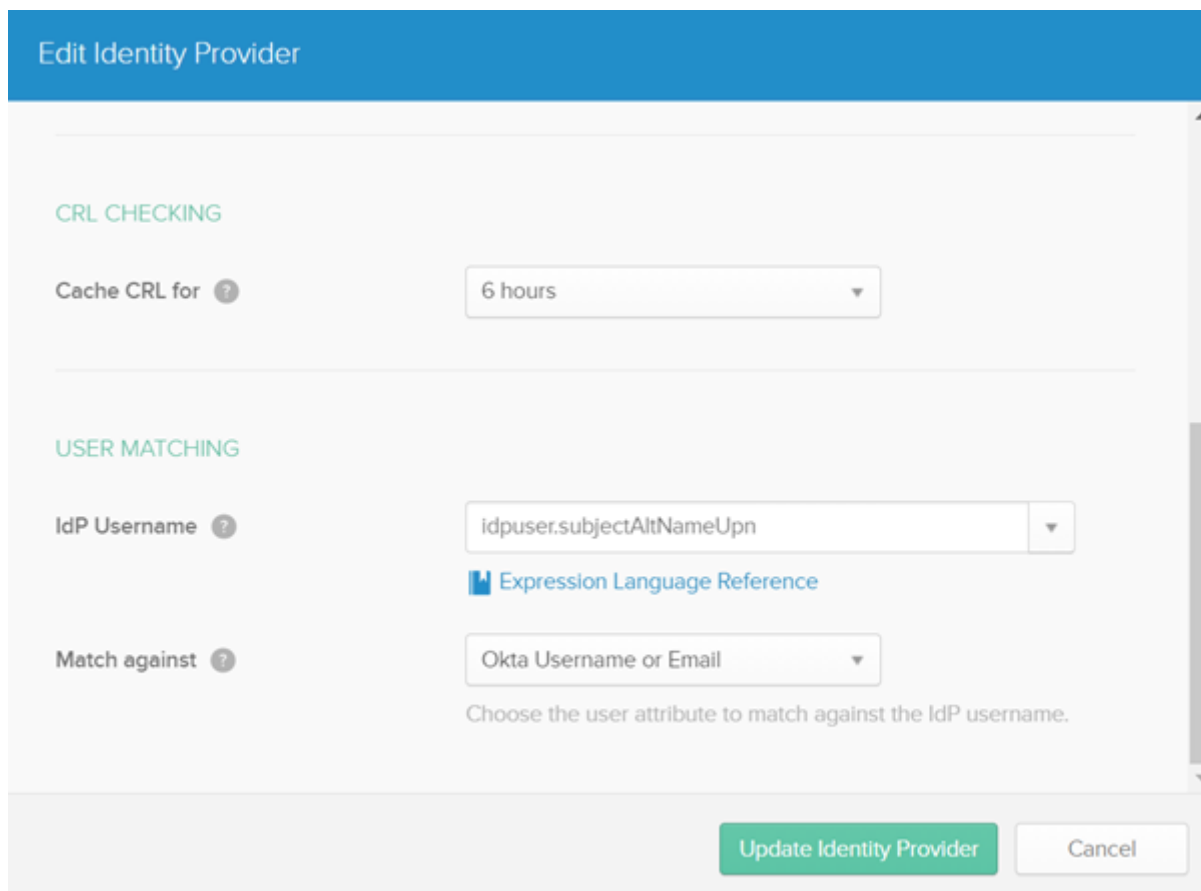
Protocol Smart Card

CERTIFICATE CHAIN

Certificate Chain ?

CN=primesoft-WIN-910T37F5QNG-CA, DC=primesoft, DC=co
Certificate expires in 1811 daysX

2. In the USER MATCHING section ensure **idpuser.subjectAltNameUpn** is entered in the *IdP Username* field and **Okta Username or Email** is selected in the *Match against* drop-down fields and click the Update Identity Provider button.



Edit Identity Provider

CRL CHECKING

Cache CRL for ? 6 hours

USER MATCHING

IdP Username ? idpuser.subjectAltNameUpn

[Expression Language Reference](#)

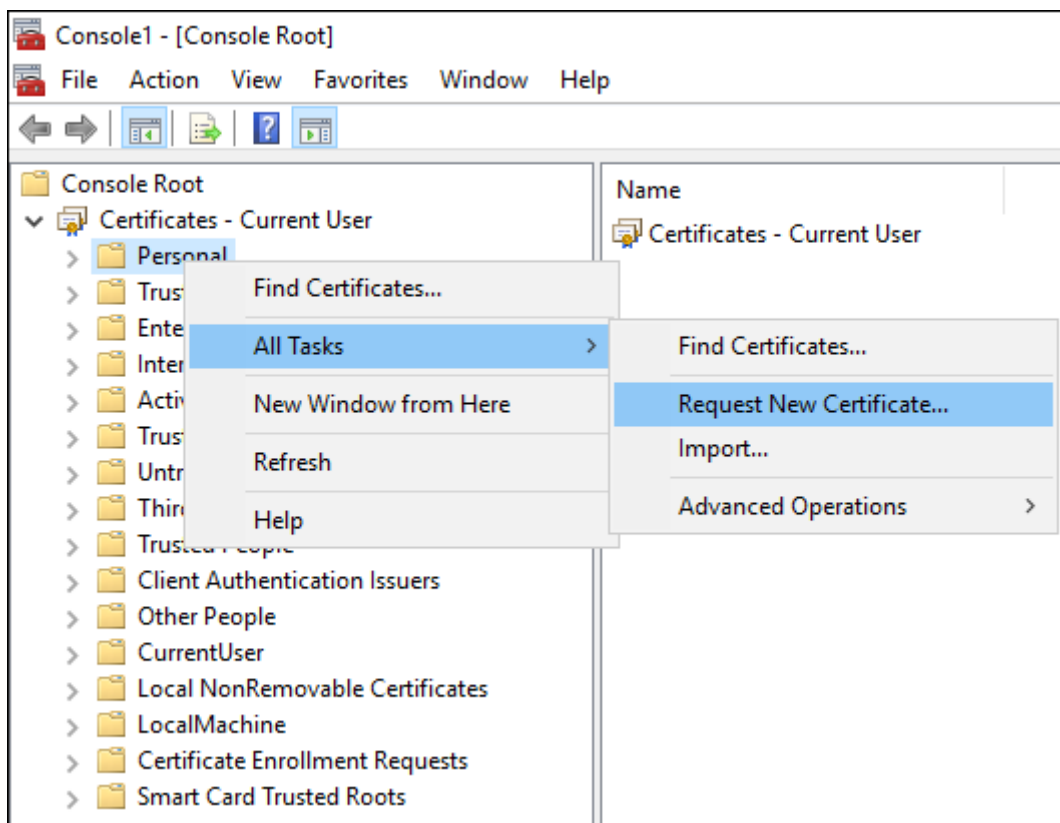
Match against ? Okta Username or Email

Choose the user attribute to match against the IdP username.

Update Identity Provider Cancel

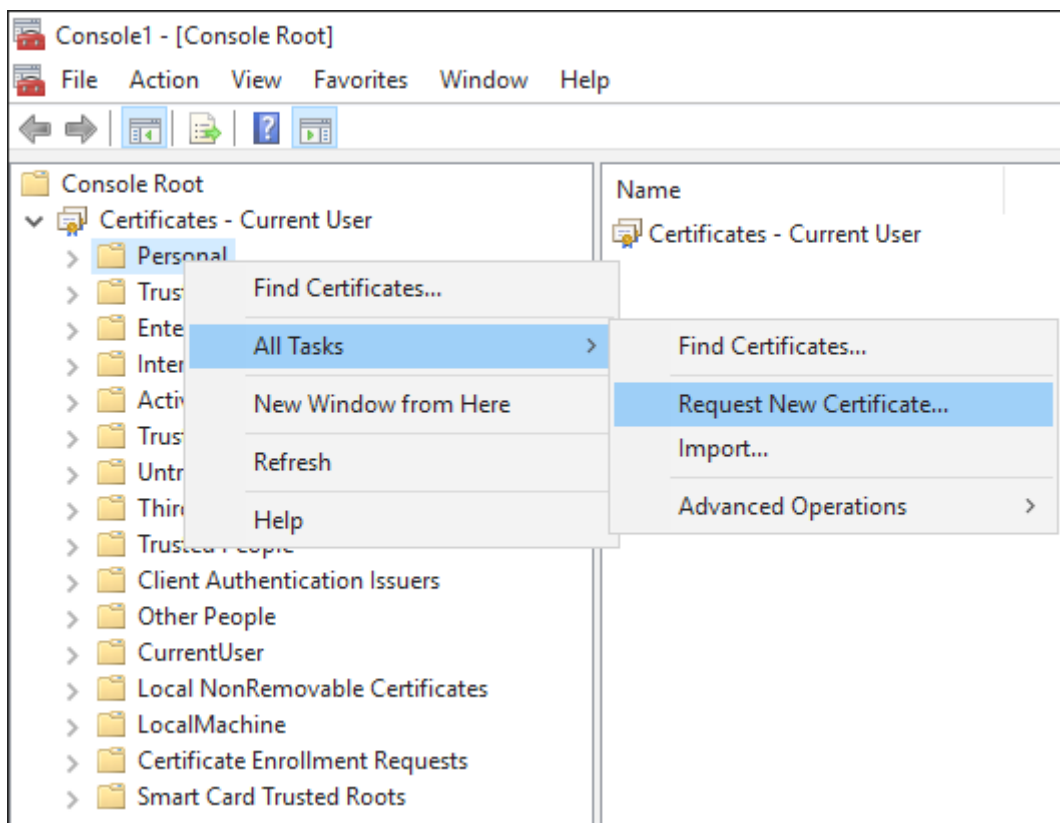
Workstation Configuration

1. Login to the workstation as >DOMAIN_NAME<\Administrator and join the domain.
2. Install smart card drivers and minidrivers. Such as the PIVKEY Administrators Kit <https://pivkey.com/pkadmin.zip>.
3. Run Microsoft Management Console (mmc.exe).
4. Click **File > Add or Remove Snap-in**, select **Certificates** and click **Add**.
5. Select the **My User Account** radio button and click **Finish** and then **OK**.
6. From the Console root expand **Certificates - Current User**, right click **Personal** and select **All Tasks > Request a New Certificate....**



7. Click **Next** on the *Before you Begin* and **Next** on the *Certificate Enrollment Policy* dialogs.

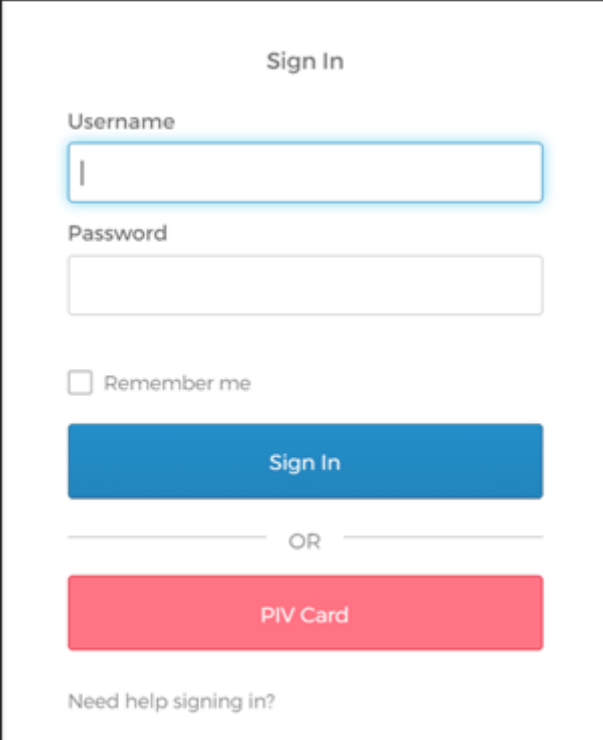
8. Select the **Copy of Smartcard User** checkbox and then click **Enroll**.



9. Enter the smart card PIN to enroll the certificate to the smart card.

Login to Okta Using PIV Card

1. Browse to the Okta URL where the smartcard is configured.
2. Click on PIV Card button.



The screenshot shows the Okta 'Sign In' page. It features a 'Username' field with a cursor, a 'Password' field, and a 'Remember me' checkbox. Below these is a blue 'Sign In' button. Underneath the button is an 'OR' separator, followed by a red 'PIV Card' button. At the bottom, there is a link that says 'Need help signing in?'.

3. Select your user Certificate.
4. Click **OK**.
5. Enter your smart card PIN.

You are now logged into Okta using smart card authentication.

Browser Configuration for use with Smartcards

Chrome and Edge (version 88.0 or newer) browsers are not known to require additional configurations at the time this article was written. Firefox requires the following configuration to display the certificate popup dialog box.

Open a Firefox browser and enter **about:config** in the URL field and configure the following options. If the option does not exist, it can be added.

- security.cert_pinning.max_max_age_seconds: 30

- security.remember_cert_checkbox_default_setting: false
- network.ssl_tokens_cache_enabled: true
- security.osclientcerts.autoload: true

[Return to the Okta configuration reference](#)

PingFederate Installation Reference

1. Register for trial and download the PingFederate Windows Installer MSI from [here](#). From the same site select the **Add-ons** tab and download Duo Security Integration Kit 3.0.
2. [Request a license key from PingIdentity](#) and download the key.
3. Download and install OpenJDK 11 and set the JAVA_HOME environment variable to the Java installation directory path, and add its bin directory to the PATH environment variable.
4. Install PingFederate using the downloaded MSI installer and select **Standalone** mode. The rest of the values during installation can be left default.
5. After installation the admin console can be accessed via **https://>FQDN<:9999/pingfederate/app**.
6. Access the admin console link in the browser and follow the onscreen instructions. Select **No, setup PingFederate Without PingOne** when prompted.
7. In the next window, browse to the downloaded license file and click Next.
8. Select **Identity Provider** and click **Next**.
9. Click **Next**.
10. Create an Administrator account.
11. Follow the instructions to install the Duo Security Integration Kit from <https://docs.pingidentity.com/bundle/integrations/page/kzh1602706841985.html>.

Before installing the integration kit

Before installing the integration kit, stop the pingfederate service from the **Services** window and start the service after the kit is deployed.

12. To integrate existing local active directory to PingFederate. Please follow the steps [at https://www.coreblox.com/blog/2015/02/add-ms-activedirectory-authentication-to-pingfederate](https://www.coreblox.com/blog/2015/02/add-ms-activedirectory-authentication-to-pingfederate).

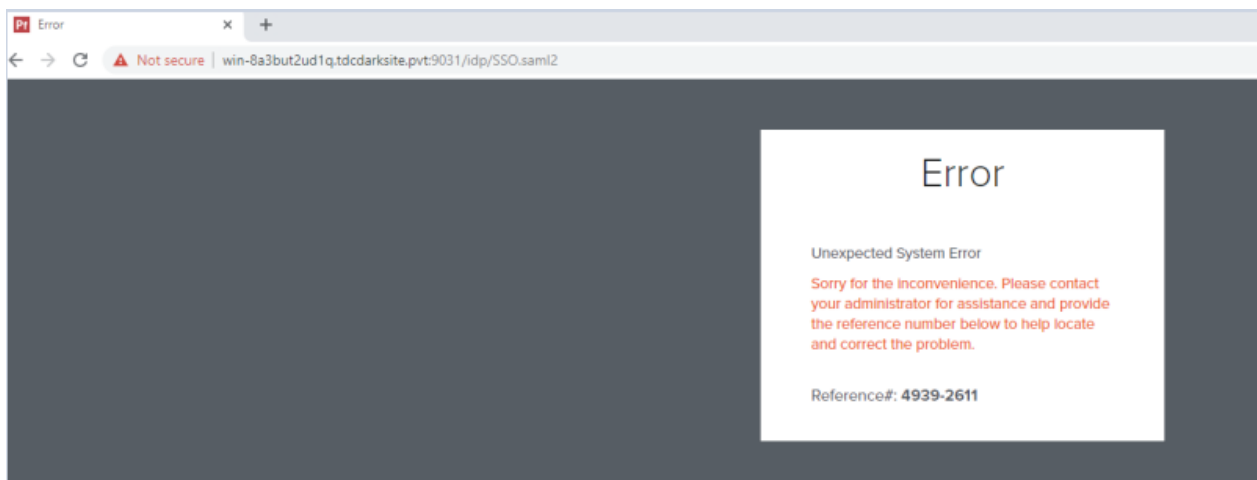
PingFederate Configuration for Management Console

Install PingFederate IDP on local system. [See PingFederate install reference.](#)

Limitations

- If we are accessing a PingFederate URL created with a hostname from a different domain, it has to be added to the **C:\Windows\System32\drivers\etc\hosts** file.
- MFA and SSO are not support with IPv6.
- PingFederate throws an unexpected system error when the entityID in SP connection is different from **<MC_URL>/saml2/service-provider-metadata/idp**. This behavior is also seen in PingOne (cloud).

This can be seen in the server.log messages located at **<pf_server>\Program Files\Ping Identity\pingfederate-10.1.2\pingfederate\log\server.log**.

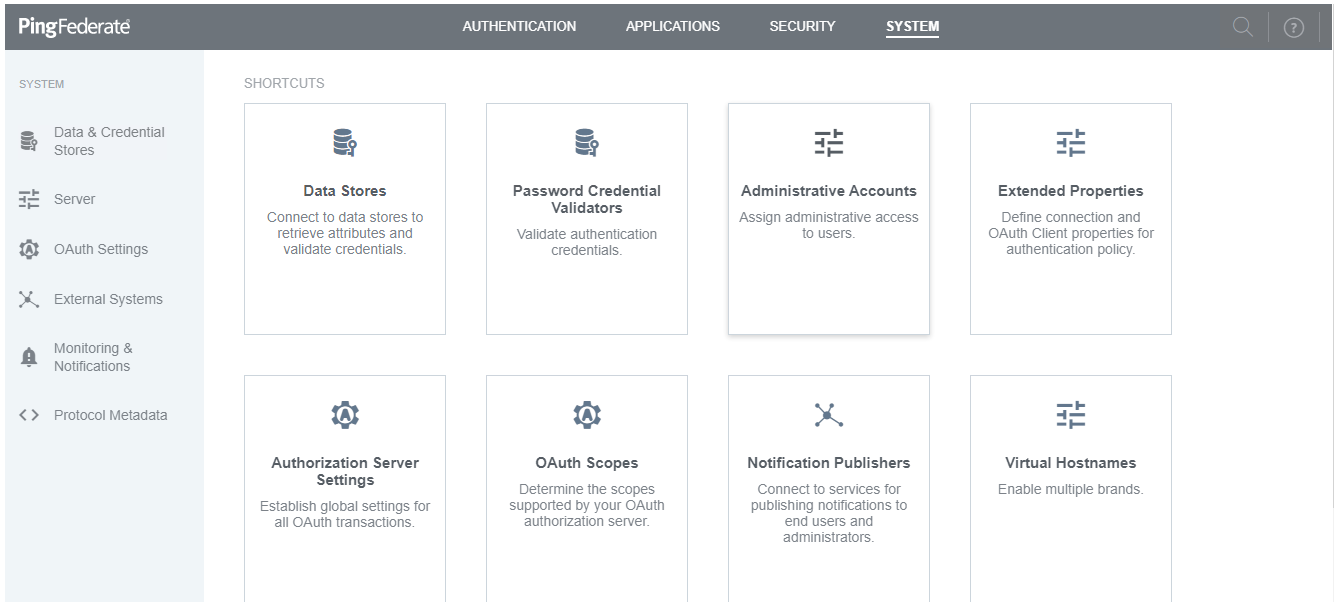


The following configurations are required to create a **SPConnection** in PingFederate (Reference links can be found [here](#) and [here](#))

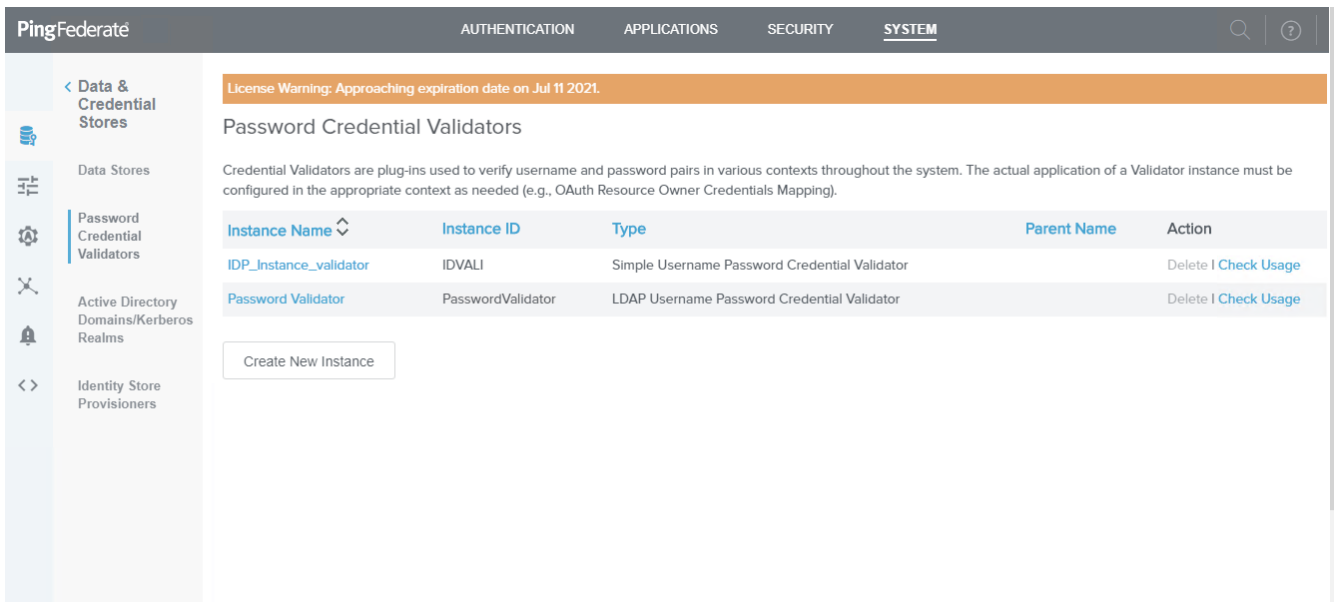
- [Create a Password Credential Validator](#)
- [Create an AD Adapter \(For first factor authentication\)](#)
- [Create a Smartcard Implementation with PingFederate](#)
- [Create a MFA Policy Contract](#)

Create a Password Credential Validator

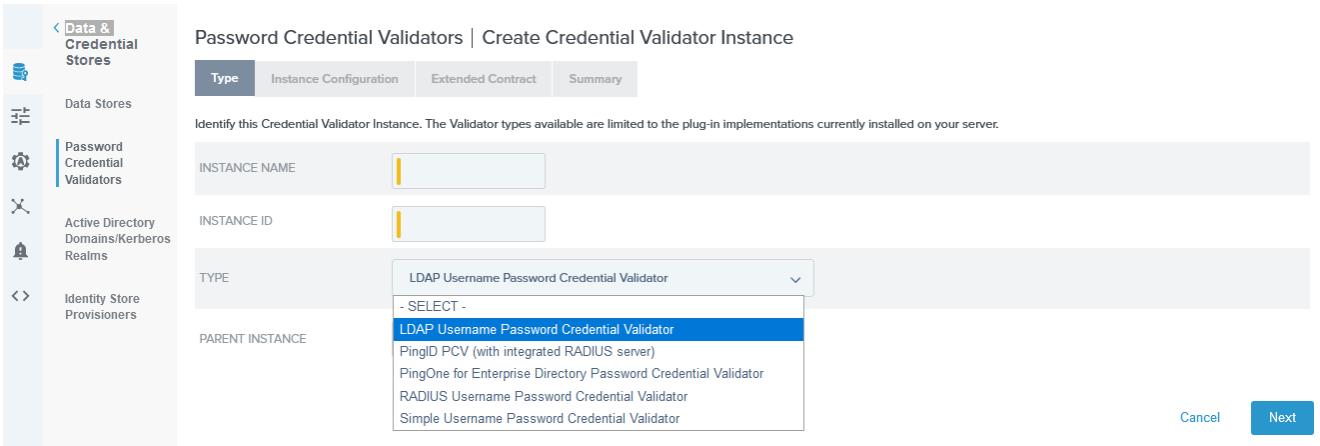
1. Navigate to **PingFederate > SYSTEM** and select **Password Credential Validators** (See reference [here](#)).



2. Click on **Create New Instance** to create a new password validator with desired name. This will be used in the AD adapter.

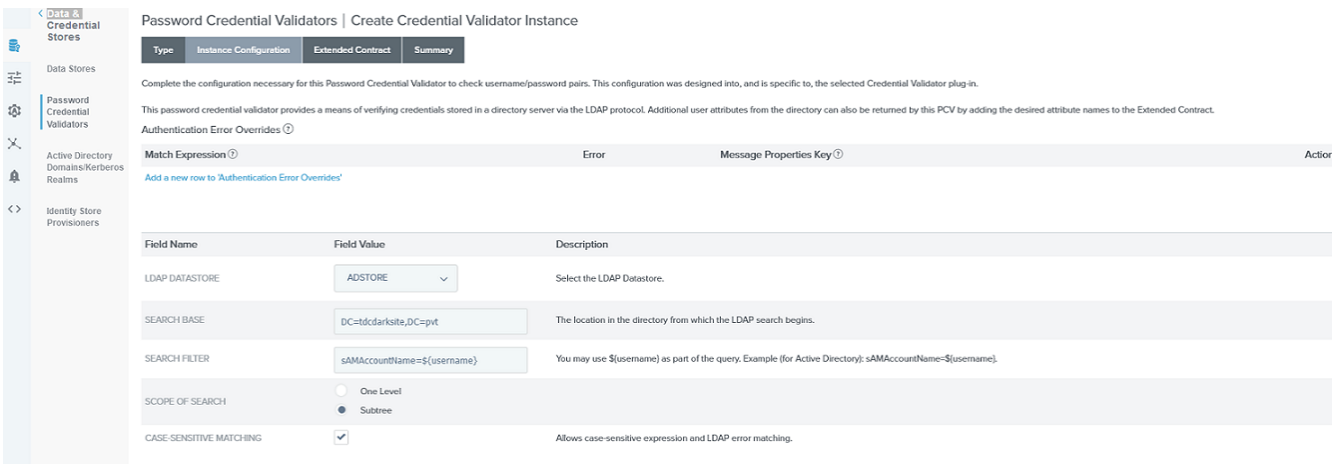


3. Select password credential validator type as **LDAP Username Password Credential Validator** and fill required fields to configure an AD Datastore.
 - a. Enter the **INSTANCE NAME**, **INSTANCE ID** and select *LDAP Username Password Credential Validator* for **TYPE** and click on **Next**.



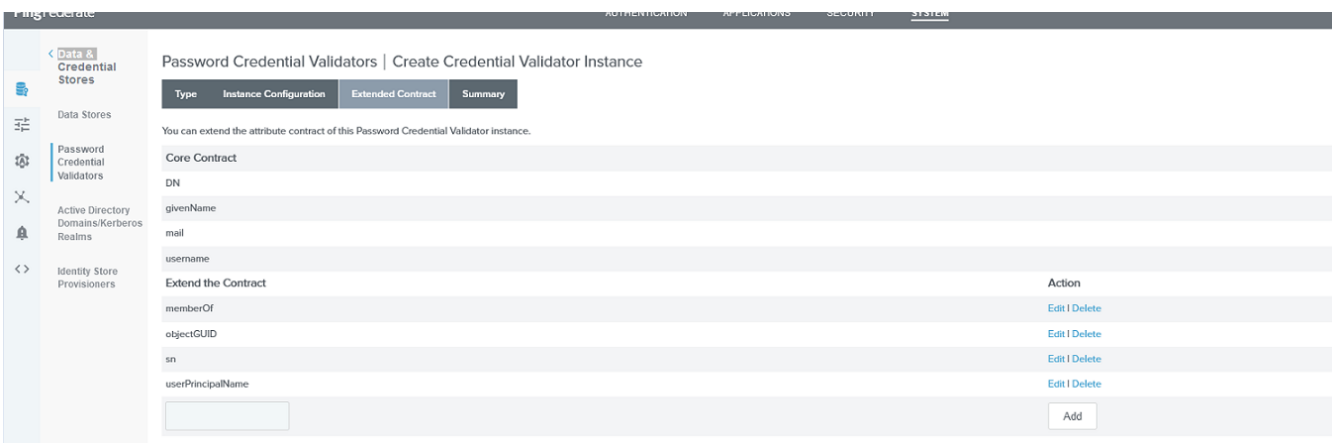
Password Credential Validator Type

a. Configure the LDAP datastore information similarly to what is displayed in the next image.



Password Credential Validator Instance Configuration

a. From the Extended Contract tab, configure similarly to the next displayed image and **SAVE**.



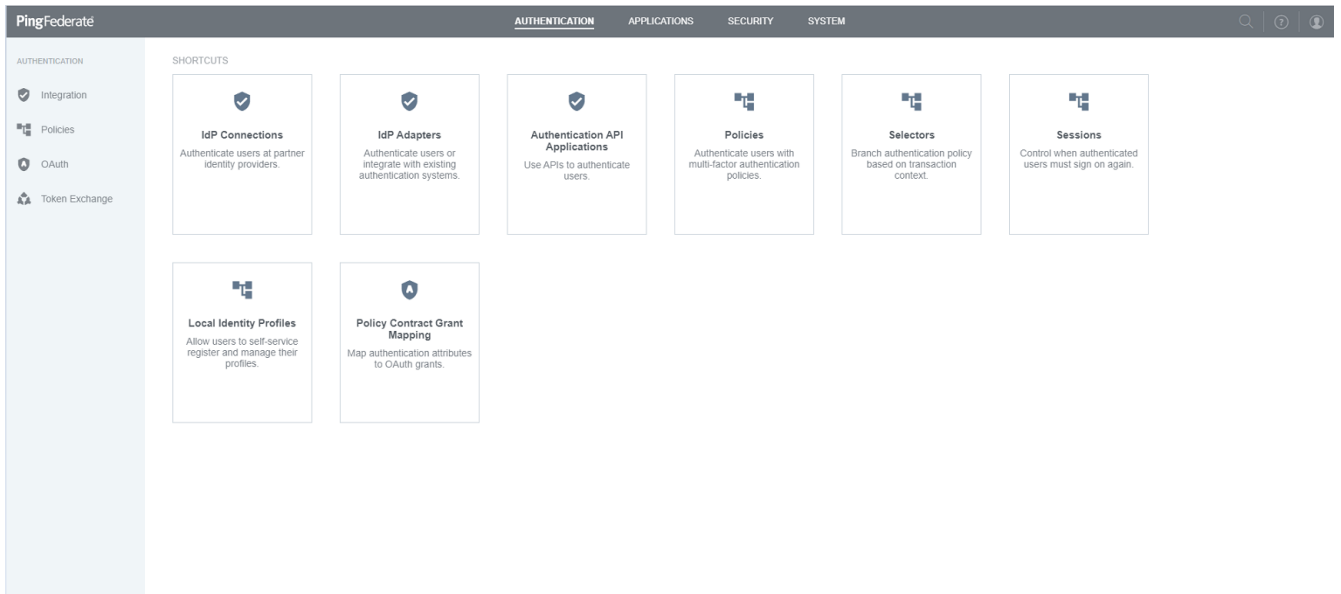
Password Credential Validator Extended Contract

4. Summary of password credential validator.

<ul style="list-style-type: none"> < Data & Credential Stores Data Stores Password Credential Validators Active Directory Domains/Kerberos Realms Identity Store Provisioners 	Scope of Search	Subtree
	Case-Sensitive Matching	true
	Display Name Attribute	displayName
	Mail Attribute	mail
	SMS Attribute	
	PingID Username Attribute	
	Mail Search Filter	
	Username Attribute	
	Trim Username Spaces For Search	true
	Mail Verified Attribute	
	Enable PingDirectory Detailed Password Policy Requirement Messaging	true
	Extended Contract	
	Attribute	DN
	Attribute	givenName
	Attribute	mail
Attribute	username	
Attribute	memberOf	
Attribute	objectGUID	

Create an AD adapter (For first factor authentication)

1. Navigate to **PingFederate > AUTHENTICATION** and click the **IDP Adapters** shortcut.



2. Click on **Create New Instance** to create a new adapter with a unique name to configure AD. This will be used in the SPConnection configuration.

Integration

- IdP Connections
- IdP Adapters**
- Authentication API Applications
- IdP Default URL

License Warning: Approaching expiration date on Jul 11 2021.

IdP Adapters

IdP adapters look up session information and provide user identification to PingFederate. Here you can manage instances of adapters that may be used to fulfill attribute contracts in protocol mappings.

Instance Name	Instance ID	Type	Parent Name	Action
AD-KERBEROS-IWA	ADIWA	IWA IdP Adapter 3.2.1		Delete
AdAuth	HTMLFormAdapter	HTML Form IdP Adapter		Delete Check Usage
IDP_ADP	IDAD	HTML Form IdP Adapter		Delete Check Usage
SmartcardAuth	Check1	X.509 Certificate IdP Adapter 1.3		Delete Check Usage
tesing sso	test123	HTTP Basic IdP Adapter		Delete Check Usage

[Create New Instance](#)

3. Select the adapter TYPE as **HTML Form IDP Adapter** and use the images showing the adapter mappings for your configuration.

IdP Adapters | Create Adapter Instance

The values of the selected Adapter.

INSTANCE NAME	AdAuth
INSTANCE ID	HTMLFormAdapter
TYPE	HTML Form IdP Adapter
CLASS NAME	com.pingidentity.adapters.htmlform.idp.HtmlFormIdpAuthnAdapter
PARENT INSTANCE	None

PingFederate Type HTML Form IDP Adapter

The screenshot shows the 'Create Adapter Instance' page for a Password Credential Validator Instance. The page is divided into several sections: 'Type' (set to IDP Adapter), 'Extended Contract', 'Adapter Attributes', 'Adapter Contract Mapping', and 'Summary'. The 'Adapter Attributes' section is active, showing a table of configuration fields. Below the table, there are several checkboxes for enabling features like 'Remember My Username' and 'This is My Device'. The table contains the following data:

Field Name	Field Value	Description
CHALLENGE RETRIES	3	Number of failed user authentications after which the PingFederate account locking service blocks future attempts.
SESSION STATE	<input type="radio"/> Globally <input type="radio"/> Per Adapter <input checked="" type="radio"/> None	Determines how state is maintained within one adapter or between different adapter instances. To take advantage of additional features, it is recommended to use a PingFederate Authentication Session rather than this adapter's internal Session State capability.
SESSION TIMEOUT	60	Session Idle Timeout (in minutes). If left blank the timeout will be the Session Max Timeout. Ignored if 'None' is selected for Session State.
SESSION MAX TIMEOUT	180	Session Max Timeout (in minutes). Leave blank for inactivity sessions. Ignored if 'None' is selected for Session State.
ALLOW PASSWORD CHANGES	<input type="checkbox"/>	Allows users to change their password using this adapter.
PASSWORD MANAGEMENT SYSTEM		A fully-qualified URL to your password management system where users can change their password. If left blank, password changes are handled by this adapter.
ENABLE 'REMEMBER MY USERNAME'	<input type="checkbox"/>	Allows users to store their username as a cookie when authenticating with this adapter. Once stored, the username is pre-populated in the login form's username field on subsequent transactions.
ENABLE 'THIS IS MY DEVICE'	<input type="checkbox"/>	Allows users to indicate whether their device is shared or private. In this mode, PingFederate Authentication Sessions will not be stored unless the user indicates the device is private. This adapter's internal session tracking (if enabled) will not be affected by the user's selection.

PingFederate Adapter Authentication IDP

The screenshot shows the configuration page for the Password Management System. It includes several checkboxes for enabling features like 'Remember My Username', 'This is My Device', 'Change Password Notification', and 'Show Password Expiring Warning'. There is a section for 'PASSWORD RESET TYPE' with radio buttons for 'Authentication Policy', 'Email One-Time Link', 'Email One-Time Password', 'PingID', 'Text Message', and 'None'. Below this is a dropdown for 'PASSWORD RESET POLICY CONTRACT' set to 'select'. At the bottom, there are several management buttons: 'Manage Password Credential Validators', 'Manage RMS Provider Settings', 'Manage Local Identity Profiles', 'Manage Notification Publishers', 'Manage CAPTCHA Settings', and 'Manage Policy Contracts'. There are also 'Cancel', 'Previous', 'Next', and 'Save' buttons at the bottom right.

PingFederate Adapter Authentication IDP 2

IdP Connections

- IdP Adapters
- Authentication API Applications
- IdP Default URL

Type	IdP Adapter	Extended Contract	Adapter Attributes	Adapter Contract Mapping	Summary
<p>This adapter type supports the creation of an extended adapter contract after initial deployment of the adapter instance. This adapter contract may be used to fulfill the attribute contract, look up additional attrib user passed to your SP partners.</p> <p>Core Contract</p> <p>policy.action</p> <p>username</p> <p>Extend the Contract Action</p> <p>givenName Edit I De</p> <p>mail Edit I De</p> <p>memberOf Edit I De</p> <p>objectGUID Edit I De</p> <p>sn Edit I De</p> <p>userPrincipalName Edit I De</p> <p><input type="text"/> Add</p>					

PingFederate Adapter Authentication Extended Contract

IdP Connections

- IdP Adapters
- Authentication API Applications
- IdP Default URL

Type	IdP Adapter	Extended Contract	Adapter Attributes	Adapter Contract Mapping	Summary																											
<p>As an IdP, some of your SP partners may choose to receive a pseudonym to uniquely identify a user. From the attributes in this authentication adapter, please select the values that you would like to use in con files.</p> <table border="1"> <thead> <tr> <th>Attribute</th> <th>Pseudonym</th> <th>M</th> </tr> </thead> <tbody> <tr> <td>givenName</td> <td><input type="checkbox"/></td> <td></td> </tr> <tr> <td>mail</td> <td><input type="checkbox"/></td> <td></td> </tr> <tr> <td>memberOf</td> <td><input type="checkbox"/></td> <td></td> </tr> <tr> <td>objectGUID</td> <td><input type="checkbox"/></td> <td></td> </tr> <tr> <td>policy.action</td> <td><input type="checkbox"/></td> <td></td> </tr> <tr> <td>sn</td> <td><input type="checkbox"/></td> <td></td> </tr> <tr> <td>username</td> <td><input checked="" type="checkbox"/></td> <td></td> </tr> <tr> <td>userPrincipalName</td> <td><input checked="" type="checkbox"/></td> <td></td> </tr> </tbody> </table> <p><input type="checkbox"/> MASK ALL OGNL-EXPRESSION GENERATED LOG VALUES</p>						Attribute	Pseudonym	M	givenName	<input type="checkbox"/>		mail	<input type="checkbox"/>		memberOf	<input type="checkbox"/>		objectGUID	<input type="checkbox"/>		policy.action	<input type="checkbox"/>		sn	<input type="checkbox"/>		username	<input checked="" type="checkbox"/>		userPrincipalName	<input checked="" type="checkbox"/>	
Attribute	Pseudonym	M																														
givenName	<input type="checkbox"/>																															
mail	<input type="checkbox"/>																															
memberOf	<input type="checkbox"/>																															
objectGUID	<input type="checkbox"/>																															
policy.action	<input type="checkbox"/>																															
sn	<input type="checkbox"/>																															
username	<input checked="" type="checkbox"/>																															
userPrincipalName	<input checked="" type="checkbox"/>																															

PingFederate Adapter Authentication Attributes

PingFederate AUTHENTICATION APPLICATIONS SECURITY SYSTEM

Integration

- IdP Connections
- IdP Adapters
- Authentication API Applications
- IdP Default URL

IdP Adapters | Create Adapter Instance

Type	IdP Adapter	Extended Contract	Adapter Attributes	Adapter Contract Mapping	Summary
<p>An Adapter Contract may be used to fulfill the Attribute Contract passed to your SP partners. By default, the adapter contract is fulfilled by the adapter itself. Optionally, additional attributes from local data store</p> <p><input type="text" value="Configure Adapter Contract"/></p>					

PingFederate Adapter Authentication Contract Mapping

License Warning: Approaching expiration date on Jul 11 2021

Integration > IdP Adapters | Create Adapter Instance

IdP adapter instance summary information.

Create Adapter Instance	
Type	
Instance Name	AdAuth
Instance ID	HTMLFormAdapter
Type	HTML Form IdP Adapter
Class Name	com.pingidentity.adapters.htmlform.idp.HtmlFormIdpAuthnAdapter
Parent Instance Name	None
IdP Adapter	
Credential Validators	Password Validator
Challenge Retries	3
Session State	None
Session Timeout	60
Session Max Timeout	480
Allow Password Changes	false
Password Management System	
Enable 'Remember My Username'	false
Enable 'This is My Device'	false
Change Password Notification	false
Show Password Expiring Warning	false
Password Reset Type	None

PingFederate Adapter Authentication Summary

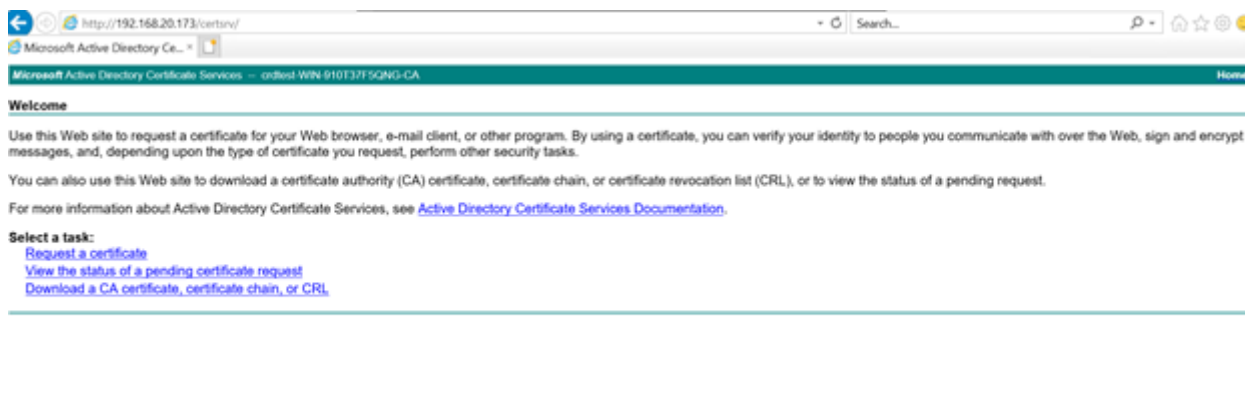
Create a Smartcard Implementation with PingFederate

The following configurations are required to implement use of a smartcard system with PingFederate.

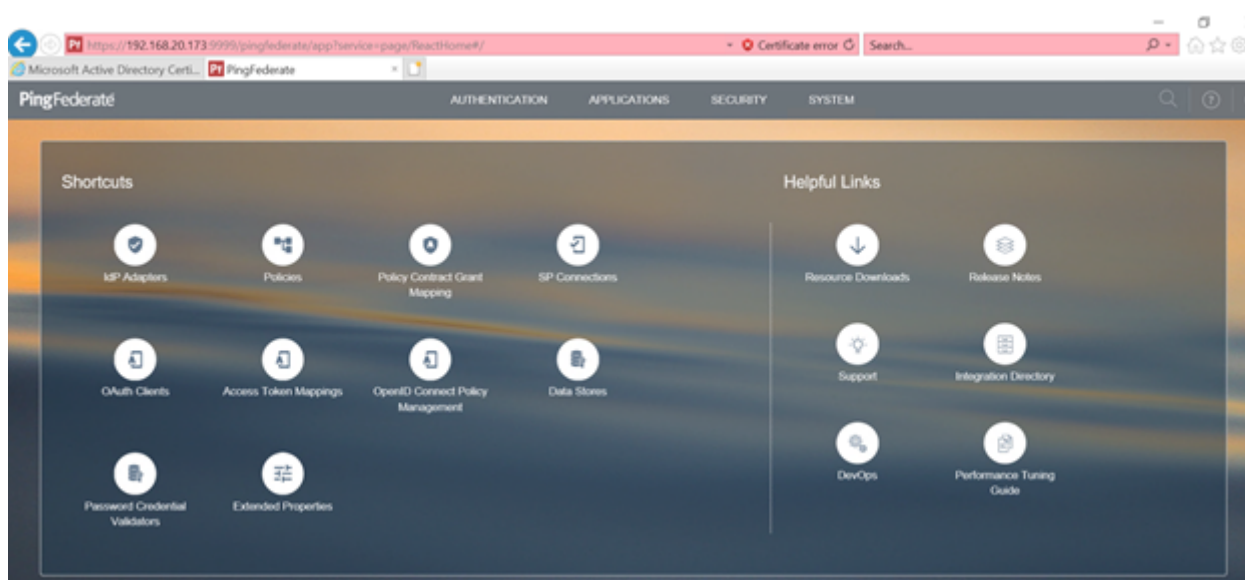
- [Download CA certificate chain file from Active Directory Server](#)
- [Install the X.509 Certificate Adapter \(Integration Kit\) in PingFederate](#)
- [Port Number for X.509 Certificate Authentication Configuration](#)
- [X.509 Certificate Adapter Configuration](#)
- [System with USB Card Reader Configuration](#)
- [Browser Configuration for use with Smartcards](#)

DOWNLOAD CA CERTIFICATE CHAIN FILE FROM ACTIVE DIRECTORY SERVER

1. In Windows Server configure the domain service with a Domain Name and Install certificate authority with web enrollment.
2. Download the CA certificate chain at http://<ActiveDirectory_IP or FQDN>/certsrv/ and upload the certificate chain to the PingFederate server.
3. Click on the **Download a CA certificate, certificate chain, or CRL** link.



4. Click on **Download CA certificate chain** to download the certificate.
5. Login to the PingFederate admin console.



6. Click **Security > Trusted CA > Import** and select the downloaded chain certificate file.

Note: Make sure the web enrollment certificate features is installed in Active directory certificate services in Windows Server.

INSTALL THE X.509 CERTIFICATE ADAPTER (INTEGRATION KIT) IN PINGFEDERATE

This section describes how to install and configure the X.509 Certificate Adapter for smart card.

1. From the system where PingFederate is installed, download the **X.509 Certificate Integration Kit 1.3.1** PingFederate add-on. You can find the **X.509 Certificate Integration Kit 1.3.1** from the **Add-ons** tab at the [PingFederate download site](#) and search the Integration Kits section.
2. Unzip and install **X.509 Certificate Integration Kit 1.3.1**.

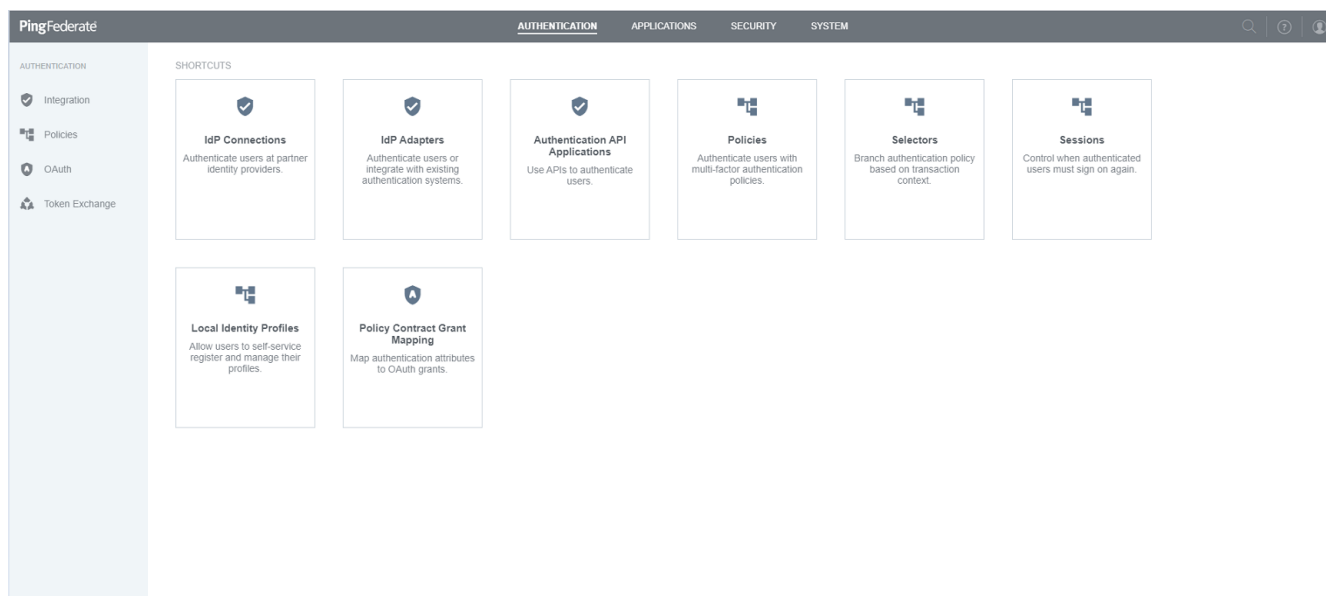
3. Copy the x509-certificate-adapter-1.1.jar file in the **dist** directory of the distribution ZIP file to the <pf-install>/pingfederate/server/default/deploy directory of your PingFederate server installation.

PORT NUMBER FOR X.509 CERTIFICATE AUTHENTICATION CONFIGURATION

1. In the <pf-install>/pingfederate/bin directory, edit the file **run.properties** and change the value of pf.secondary.https.port to a valid port number.(For this example we will configure it as 9032).
2. Press the Windows key, type **services** and press the Enter key and the Services dialog displays.
3. Right click the PingFederate service and restart it.

X.509 CERTIFICATE ADAPTER CONFIGURATION

1. From PingFederate **AUTHENTICATION** tab select the **IDP Adapters** shortcut.



2. Click on **Create New Instance** to create a new adapter with a descriptive name. This will be used in the smart card SPConnection.

Integration

- IdP Connections
- IdP Adapters**
- Authentication API Applications
- IdP Default URL

License Warning: Approaching expiration date on Jul 11 2021.

IdP Adapters

IdP adapters look up session information and provide user identification to PingFederate. Here you can manage instances of adapters that may be used to fulfill attribute contracts in protocol mappings.

Instance Name	Instance ID	Type	Parent Name	Action
AD-KERBEROS-IWA	ADIWA	IWA IdP Adapter 3.2.1		Delete
AdAuth	HTMLFormAdapter	HTML Form IdP Adapter		Delete Check Usage
IDP_ADP	IDAD	HTML Form IdP Adapter		Delete Check Usage
SmartcardAuth	Check1	X.509 Certificate IdP Adapter 1.3		Delete Check Usage
tesing sso	test123	HTTP Basic IdP Adapter		Delete Check Usage

Create New Instance

- Select type as **X509 Certificate IDP Adapter 1.3** and enter the Client Auth Port specified for the pf.secondary.https.port (see Configure port number for x509 certificate authentication) and for client hostname enter the fqdn of the PingFederate system.

IdP Adapters | Create Adapter Instance

Type | **IdP Adapter** | Extended Contract | Adapter Attributes | Adapter Contract Mapping | Summary

The values of the selected Adapter:

INSTANCE NAME: SmartcardAuth

INSTANCE ID: Check1

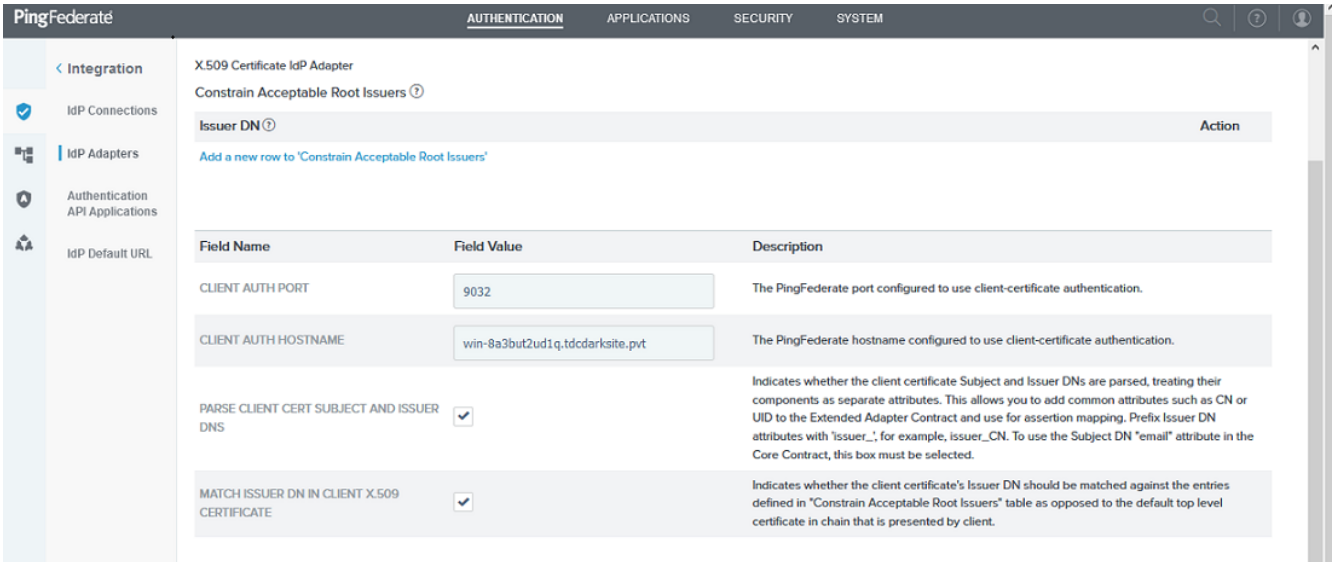
TYPE: X.509 Certificate IdP Adapter 1.3

CLASS NAME: com.pingidentity.adapters.idp.clientcert.ClientCertIdpAuthnAdapter

PARENT INSTANCE: None

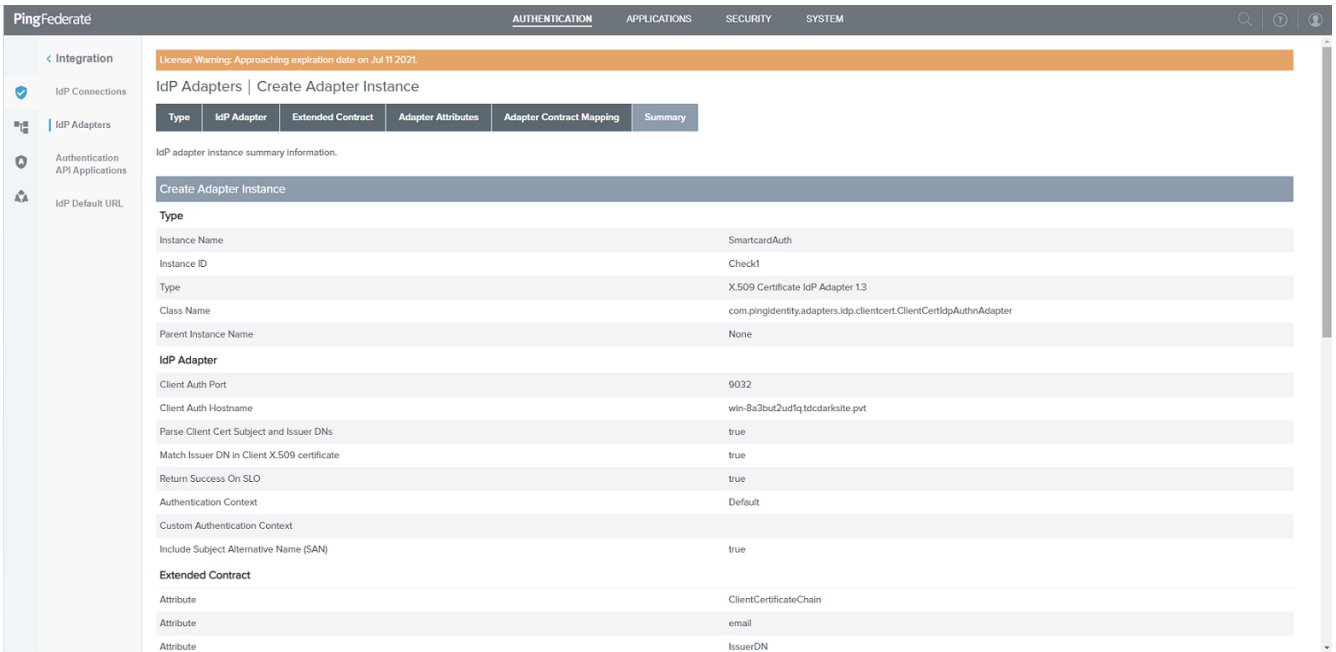
Cancel Next Save

PingFederate IDP Adapter Type Settings



PingFederate IDP Adapter Port Settings **PingFederate IDP Adapter Attributes Settings**

4. Review the smart card adapter summary.



PingFederate IDP Adapter Summary

Browser Configuration for use with Smartcards

Chrome and Edge (version 88.0 or newer) browsers are not known to require additional configurations at the time this article was written. Firefox requires the following configuration to display the certificate popup dialog box.

Open a Firefox browser and enter **about:config** in the URL field and configure the following options. If the option does not exist, it can be added.

- security.cert_pinning.max_max_age_seconds: 30
- security.remember_cert_checkbox_default_setting: false
- network.ssl_tokens_cache_enabled: true
- security.osclientcerts.autoload: true

SYSTEM WITH USB CARD READER CONFIGURATION

This configuration is required on the computer that has a USB Smart Card Reader attached.

1. Login to the workstation as >DOMAIN_NAME<\Administrator and join the domain.
2. Install smart card drivers and minidrivers from the PIVKEY Administrators Kit <https://pivkey.com/pkadmin.zip>.
3. Insert a smart card into the smart card reader.
4. Run Microsoft Management Console (mmc.exe).
5. Click **File > Add or Remove Snap-in**, select **Certificates** and click **Add**.
6. Select the **My User Account** radio button and click **Finish** and then **OK**.
7. From the Console root expand **Certificates - Current User**, right click **Personal** and select **All Tasks > Request a New Certificate....**
8. Click **Next** on the *Before you Begin* and **Next** on the *Certificate Enrollment Policy* dialogs.
9. Select the **Copy of Smartcard User** checkbox and then click **Enroll**.
10. Enter the smart card PIN to enroll the certificate to the smart card. The Certificate is enrolled to the Smartcard.
11. Make sure the smart card services is up and running. (verify through mmc services)
12. Make sure that the smart card has the certificate issued by the local AD server certificate authority.
13. Browse to the Management Console login page using the FQDN of the application (i.e. https://mccapplication.domain.name) and click on **SIGN IN WITH IDP**.
You will be prompted to select the smart card certificate and once selected you will be prompted to enter the PIN.

Browser Configuration for use with Smartcards

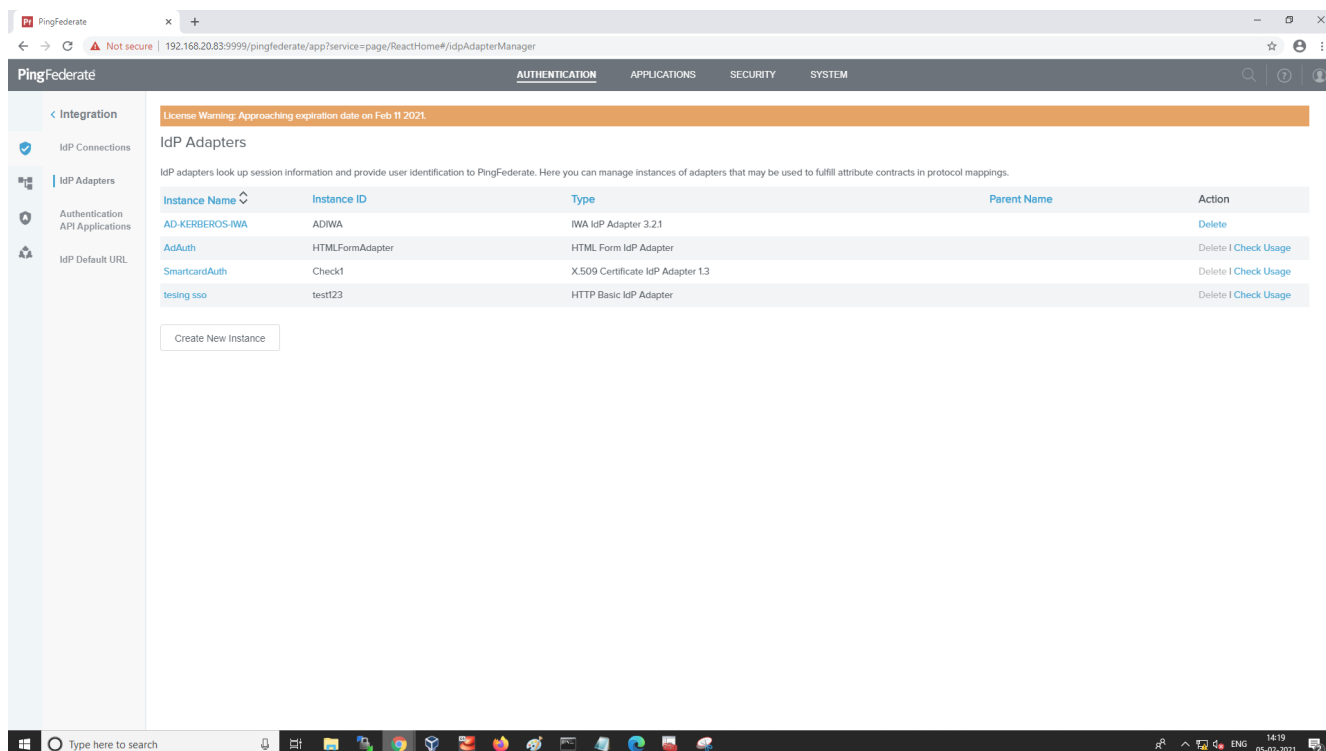
Chrome and Edge (version 88.0 or newer) browsers are not known to require additional configurations at the time this article was written. Firefox requires the following configuration to display the certificate popup dialog box.

Open a Firefox browser and enter **about:config** in the URL field and configure the following options. If the option does not exist, it can be added.

- security.cert_pinning.max_max_age_seconds: 30
- security.remember_cert_checkbox_default_setting: false
- network.ssl_tokens_cache_enabled: true
- security.osclientcerts.autoload: true

Create a MFA Policy Contract

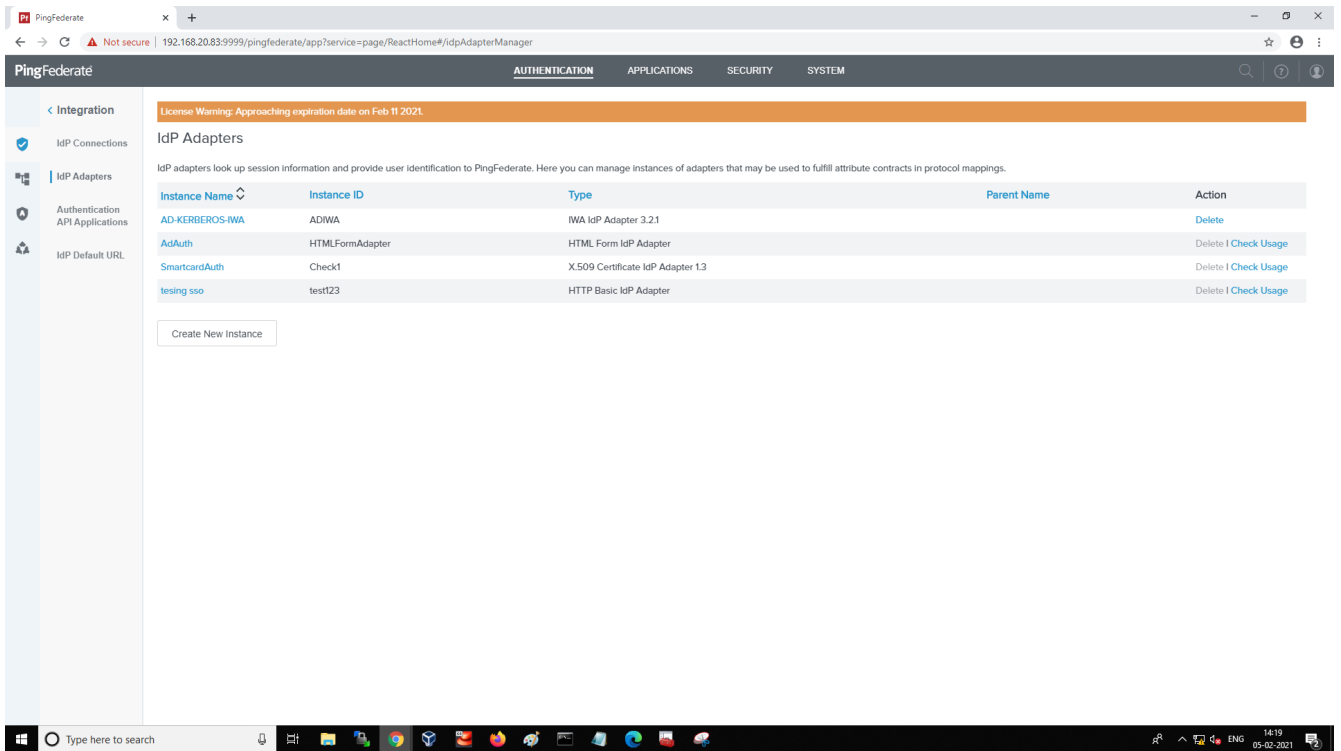
1. Select the smart card adapter from **Authentication > IDP Adapters**



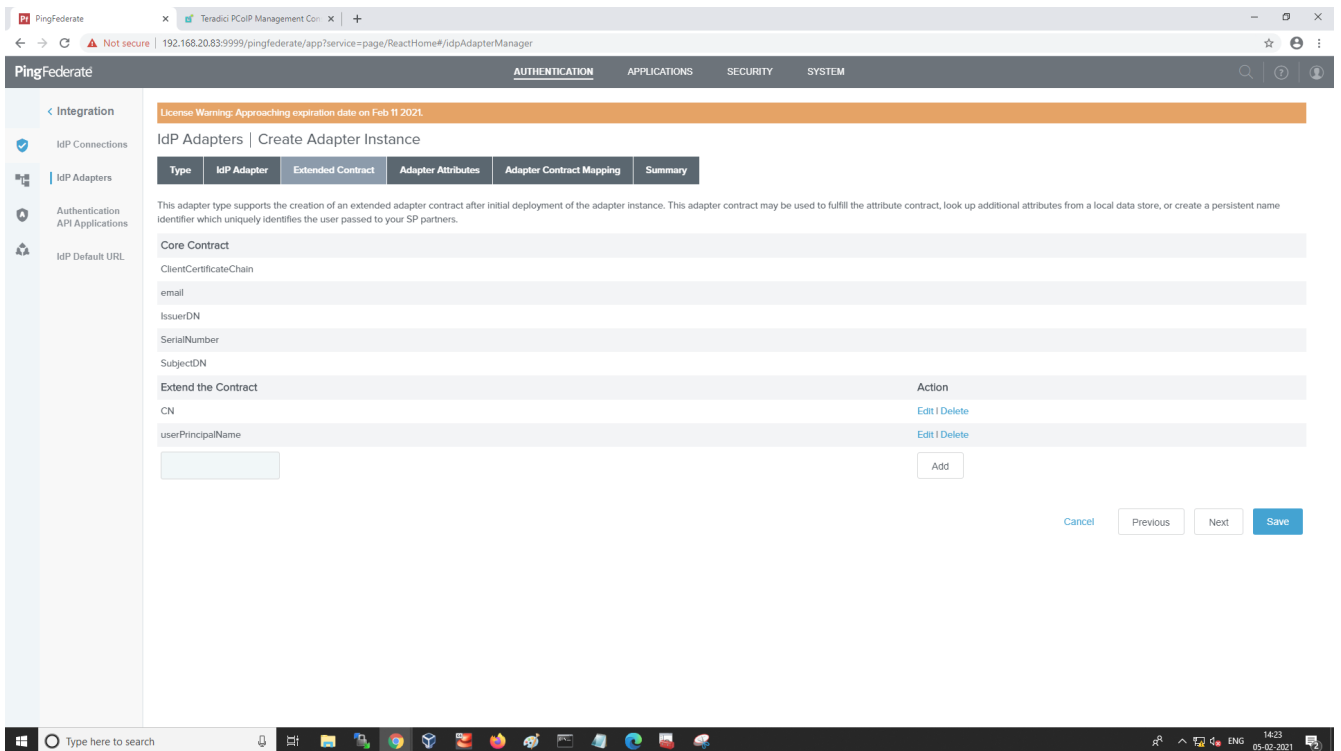
The screenshot shows the PingFederate management console interface. The left sidebar is set to 'Integration' > 'IdP Adapters'. The main content area shows a 'License Warning: Approaching expiration date on Feb 11 2021.' and a table of 'IdP Adapters'. Below the table is a 'Create New Instance' button.

Instance Name	Instance ID	Type	Parent Name	Action
AD-KERBEROS-IWA	ADIWA	IWA IdP Adapter 3.2.1		Delete
AdAuth	HTMLFormAdapter	HTML Form IdP Adapter		Delete Check Usage
SmartcardAuth	Check1	X.509 Certificate IdP Adapter 1.3		Delete Check Usage
tesing sso	test123	HTTP Basic IdP Adapter		Delete Check Usage

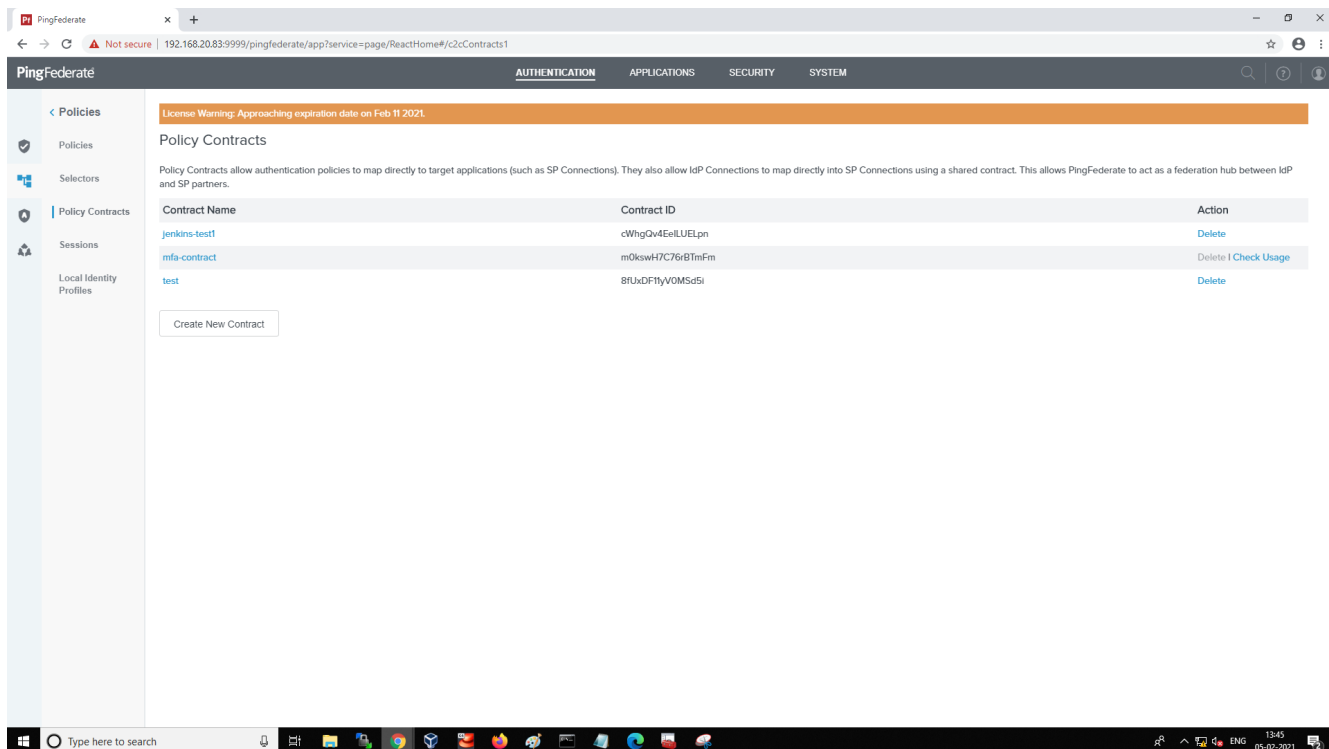
2. Ensure the **INCLUDE SUBJECT ALTERNATIVE NAME (SAN)** checkbox is selected to get the userPrincipalName in the IDP adapter and click **Save**.



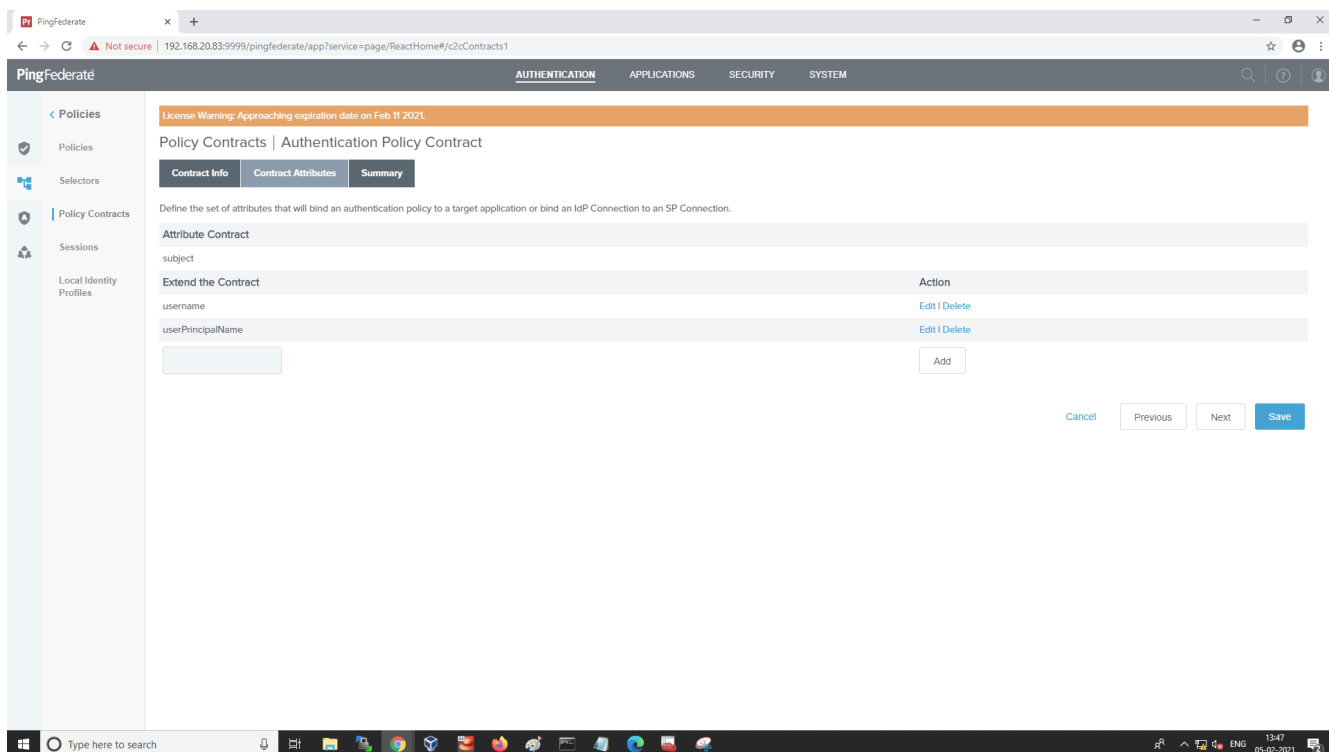
3. Select the **Extended Contract** tab, use the Add button to enter **userPrincipalName** and click **Save**.



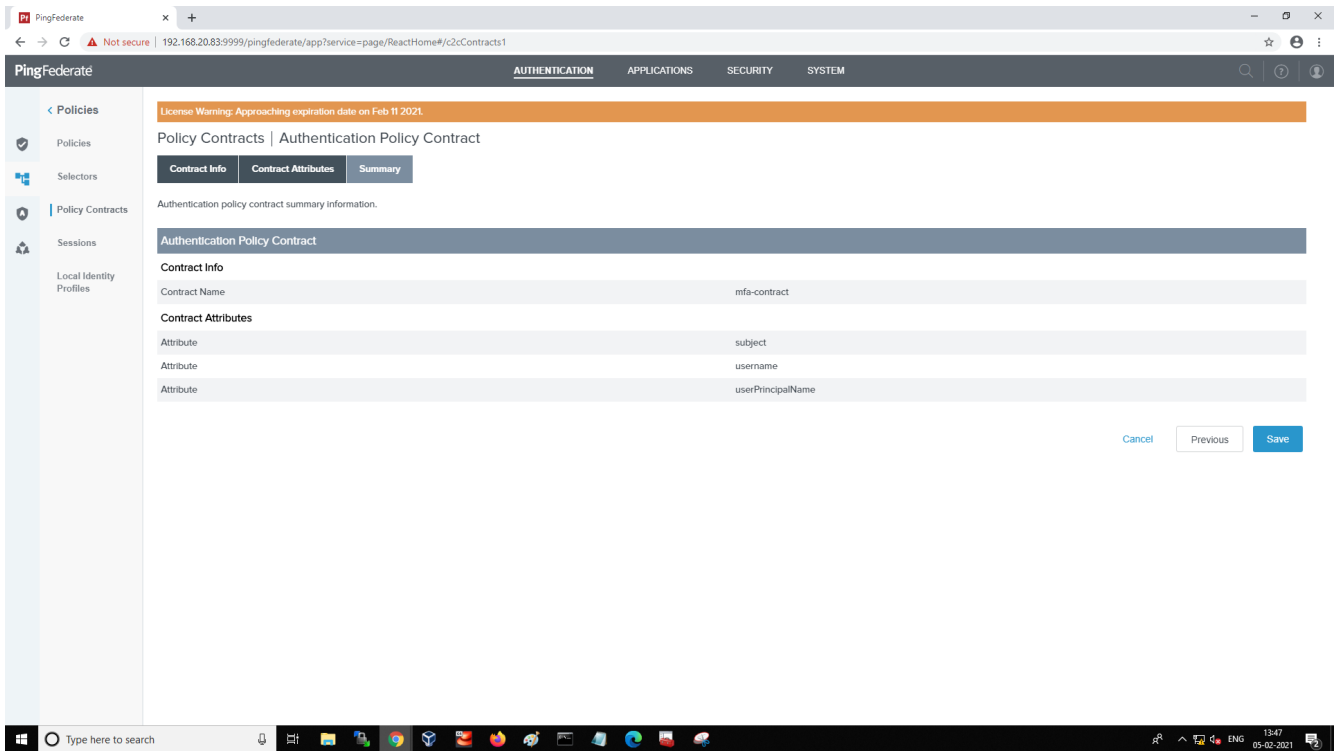
4. Click **Create New Contract**.



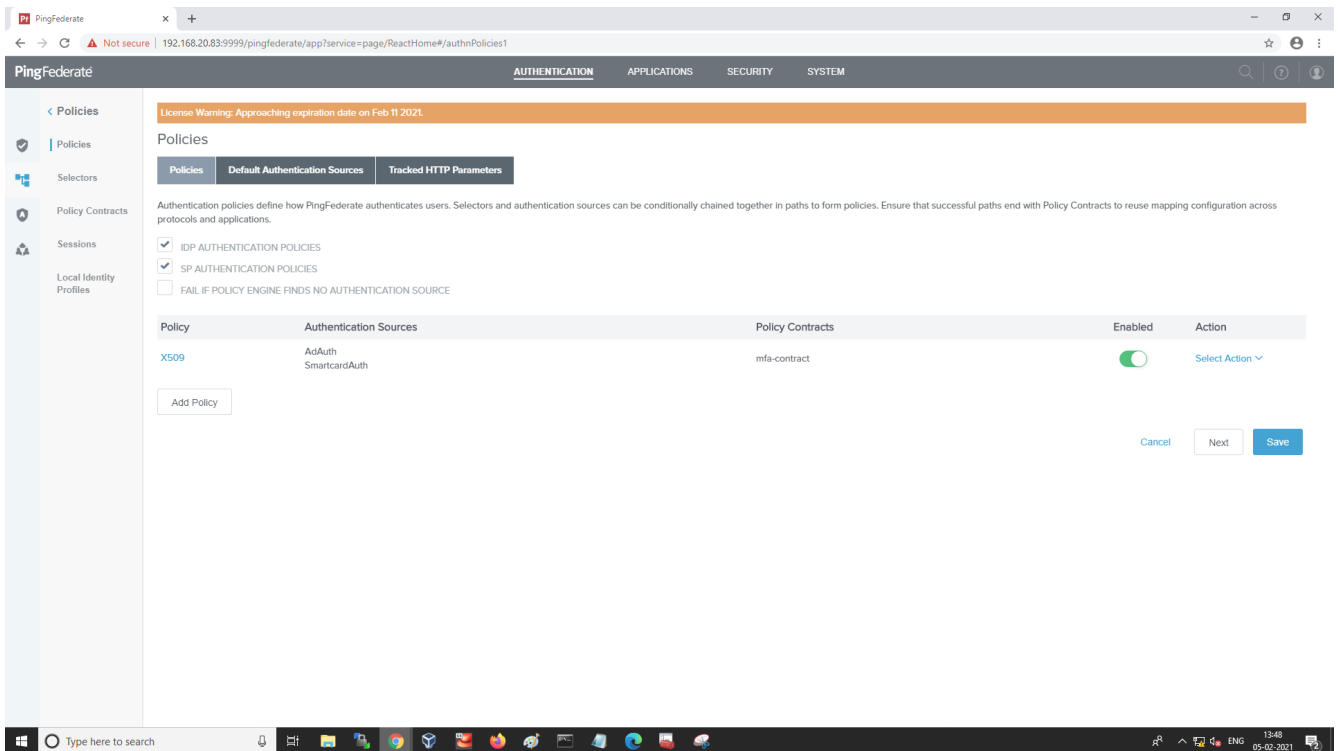
5. Add **userPrincipalName** by extending the contract in *Contract Attributes* and **Save**.



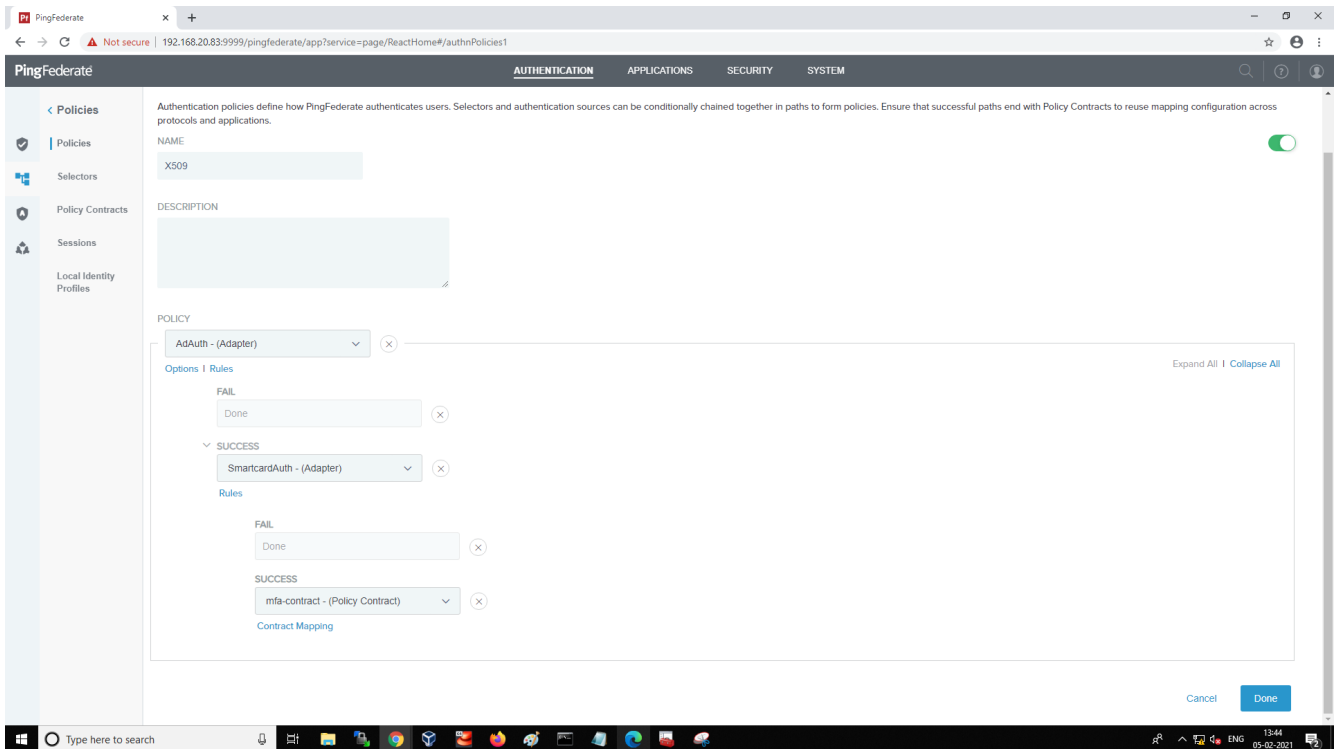
6. Review the **Summary** of the Authentication Policy Contract.



7. Select **Authentication > Policies** to add the created policy contract.

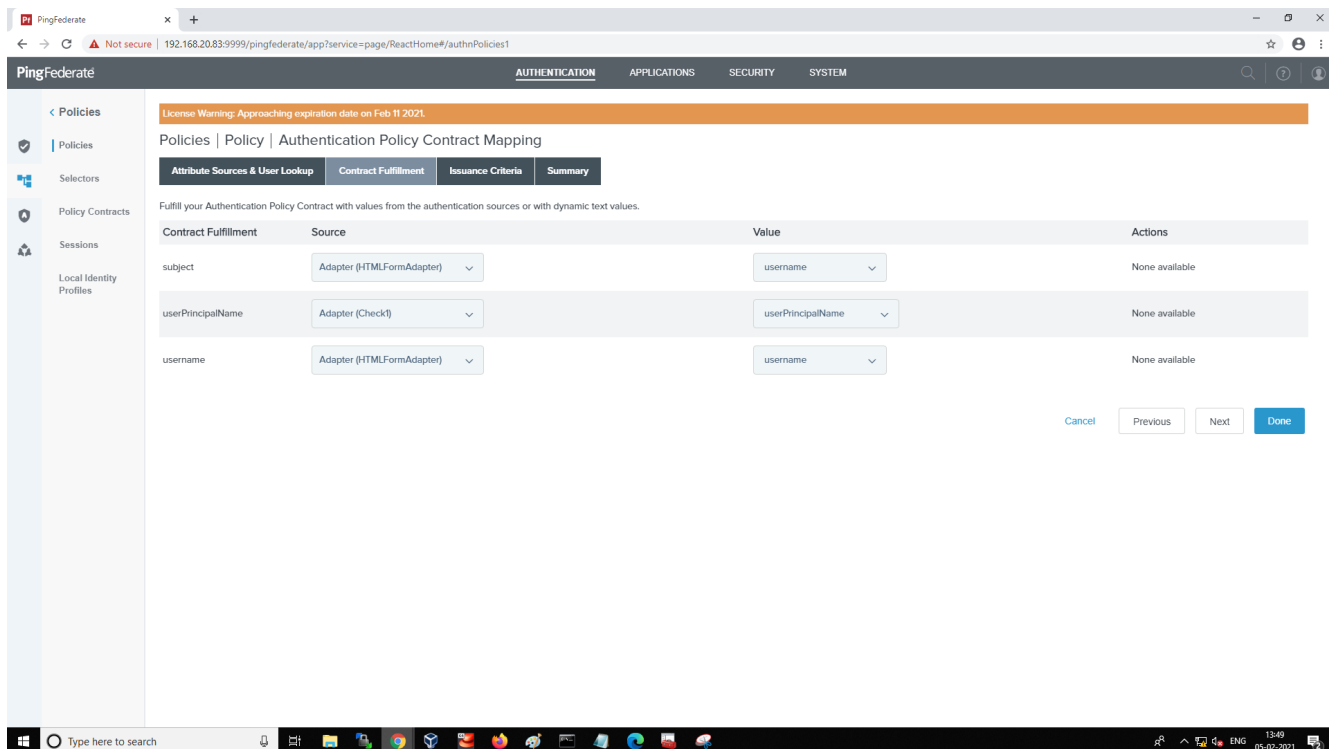


8. Review the policy and select the **Contract Mapping** link for the **mfa-contract** Policy Contract.



- **AD adapter(AdAuth)** is configured for first factor authentication.
- **X509 adapter(SmartCardAuth)** is configured for smart card as second factor authentication.
- The Policy Contract(**mfa-contract**) is configured to validate first factor username with smart card certificate username.

9. Select the **Contract Fulfillment** tab and map the attributes

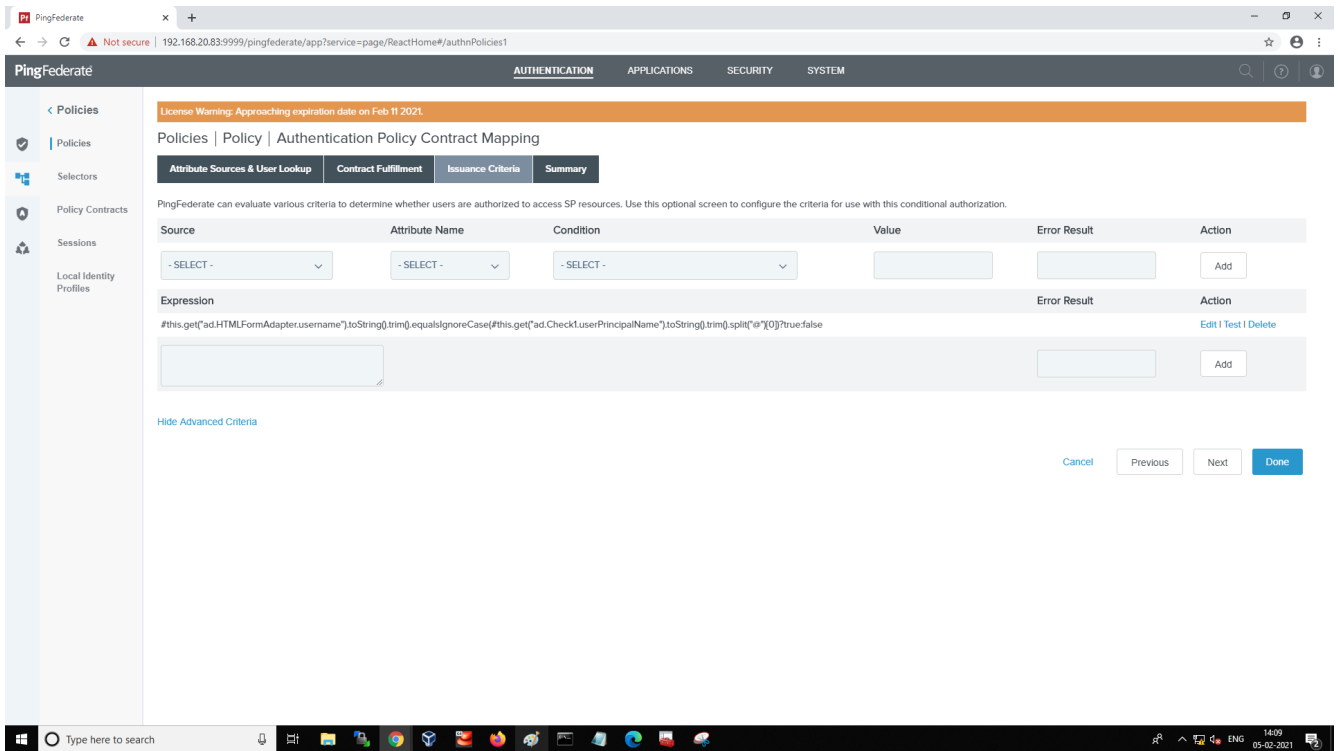


10. Select the **Issuance Criteria** tab and add the following ONGL expression to validate the username of the first factor with the smart card certificate username. The ONGL expression will be changed based on AD configurations in the AD adapter.

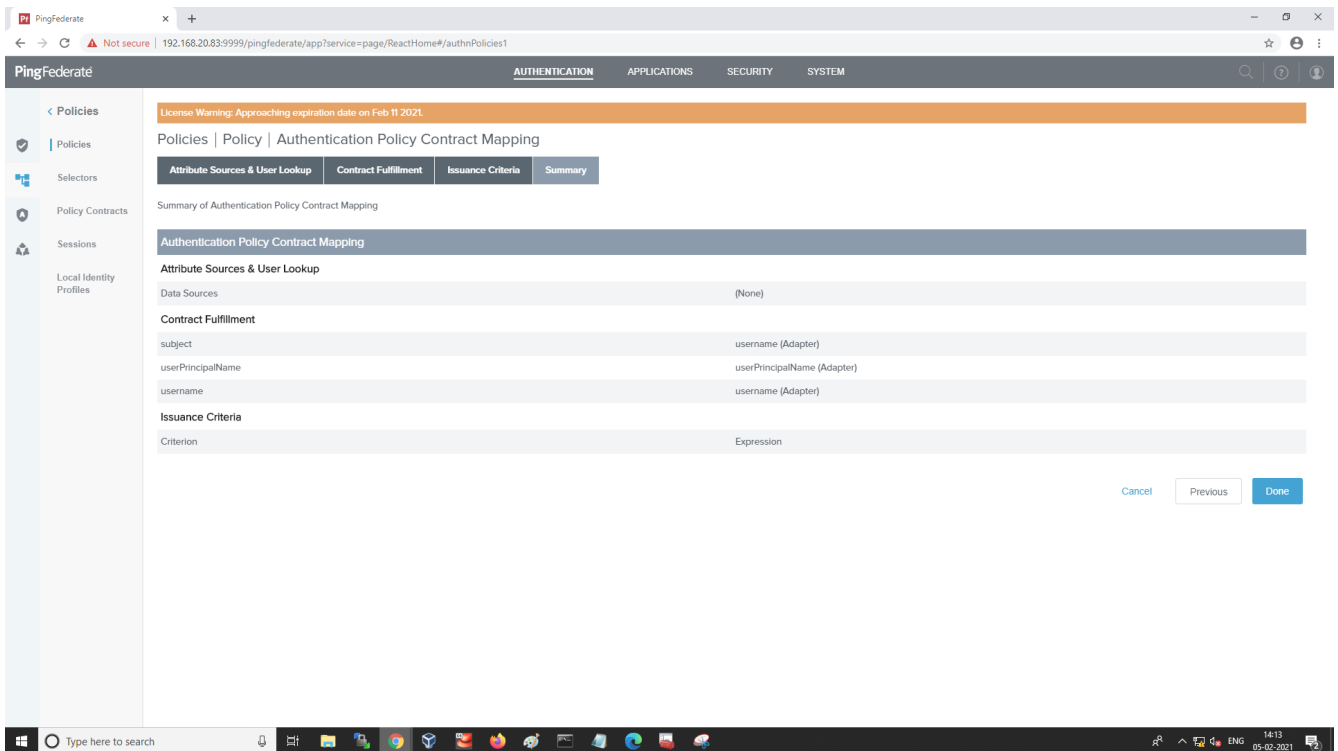
```
#this.get("ad.HTMLFormAdapter.username").toString().trim().equalsIgnoreCase(#[0])?true:false
```

You can test the ONGL expression by clicking the **Test** link and providing sample values. The test results will return true if the username is the same in both AD Adapter and Smartcard adapter and false if not.

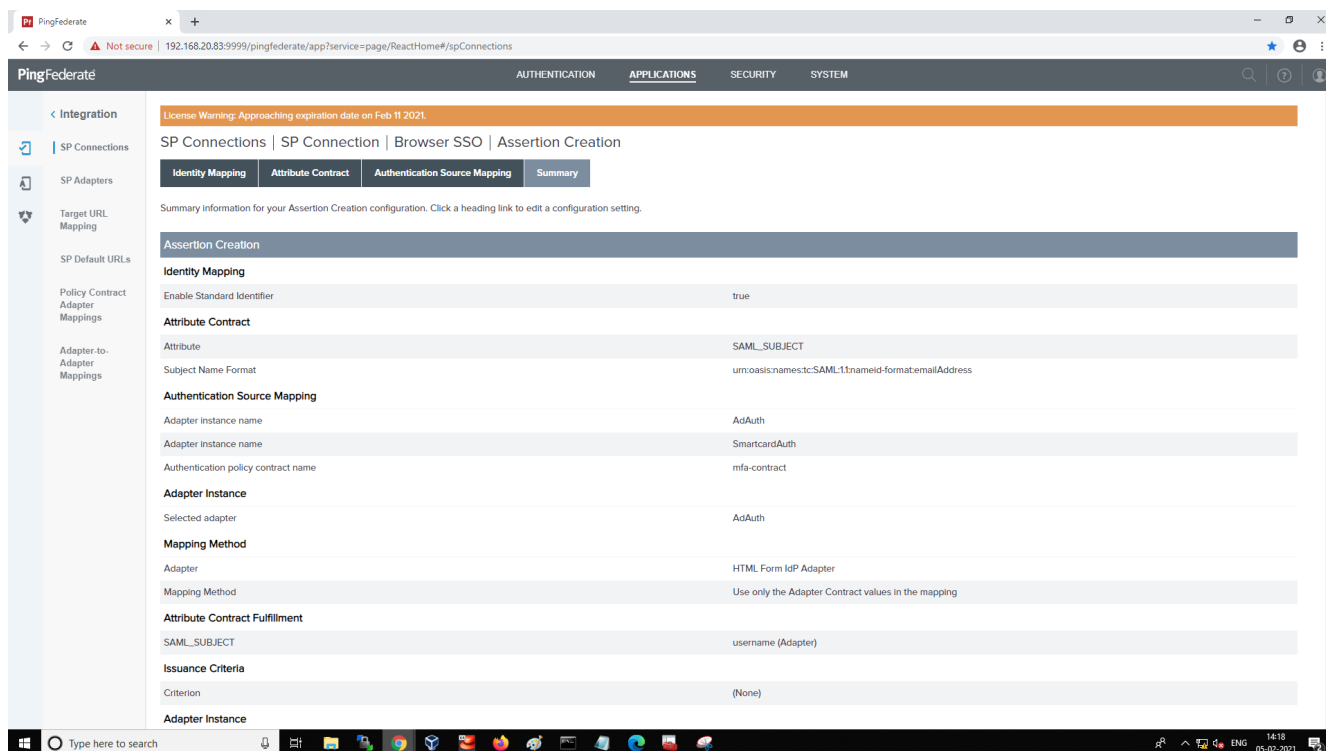
After testing, ensure the ONGL entered expression is correct and click **Done**.



11. Select the **Summary** tab and review the Policy Contract Mapping.



12. Select the **Applications** tab and review Summary for **SP Connections**.



CREATING A SP CONNECTION

An SP Connection is comprised of the following configurations.

- [SP Connection](#)
- [Configure Browser SSO](#)
- [Configure Assertion Creation](#)
- [Configure Protocol Settings](#)
- [Configure Credentials](#)

SP Connection

1. Navigate to **APPLICATIONS** → **SP Connections**
2. Click **Create Connection**.
3. Select the **DO NOT USE A TEMPLATE FOR THIS CONNECTION** radio button and click **Next**.
4. Select the **Connection Type** tab and select the **BROWSER SSO PROFILES** check box and select **SAML2.0** as the Protocol.
5. Select the **BROWSER SSO** checkbox and click **Next**.
6. Select the **FILE** radio button to upload SP metadata XML or select **NONE** to configure the required fields manually and click **Next**.

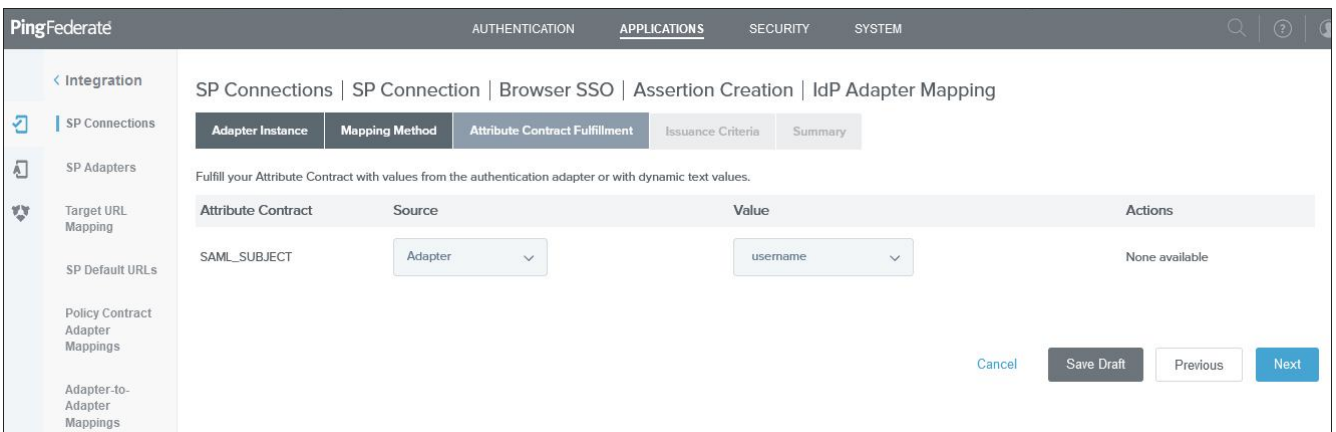
7. Enter **/saml2/service-provider-metadata/idp** for the *PARTNER'S ENTITY ID (CONNECTION ID)* field.
8. Enter a descriptive connection name.
9. Enter the Management Console's URL in the **BASE URL** field and click **Next**.

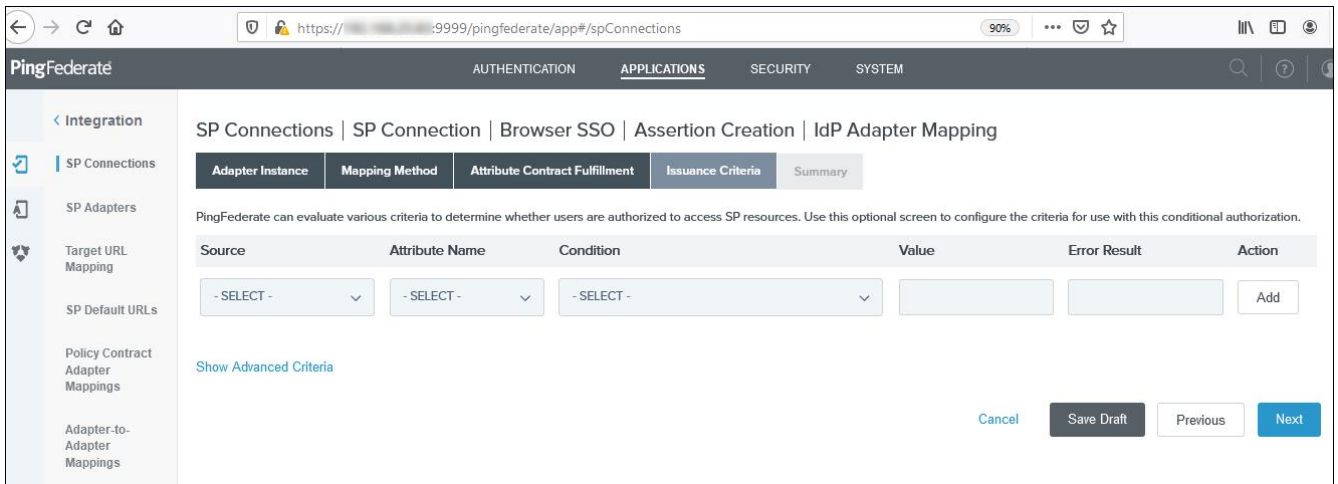
Configure Browser SSO

1. Click the **Configure Browser SSO** button.
2. From the *SAML Profiles* page, select the **IDP-INITIATED SSO** and **SP-INITIATED SSO** checkboxes and click **Next**. (Management Console does not support SLO)
3. Enter **Assertion Lifetime** values and click **Next**.

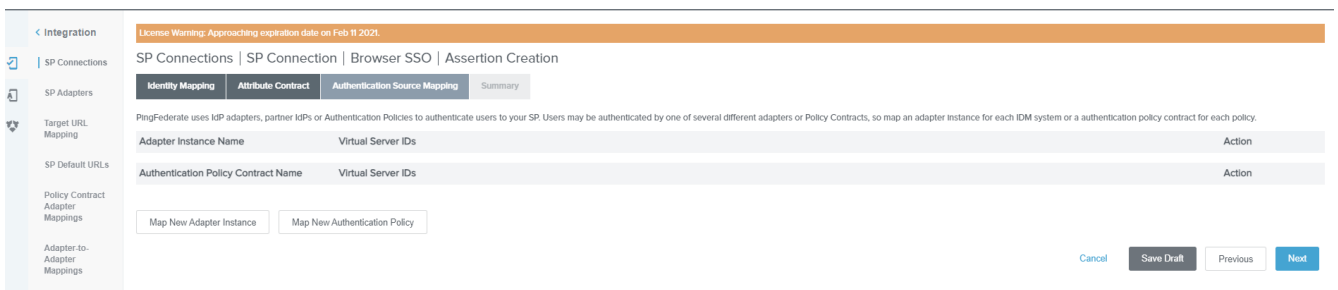
Configure Assertion Creation

1. Click the **Configure Assertion Creation** button on the Assertion Creation page.
2. Select the **STANDARD:** radio button and click **Next** and **Next** again.
3. Click the **Map New Adapter Instance** button on the *Authentication Source Mapping* page and click **Next**.
4. Select **Create AD/Smartcard adapters** from the **ADAPTER INSTANCE** drop-down list and click **Next**.
5. Select the **Manage Adapter Instances** button to create a new adapter and then **Next > Next > Next**.
6. Select **USE ONLY THE ADAPTER CONTRACT VALUES IN THE SAML ASSERTION** and click on **Next**.
7. Select the username as **SAMLSUBJECT** and click on **Next** and **Next** again.

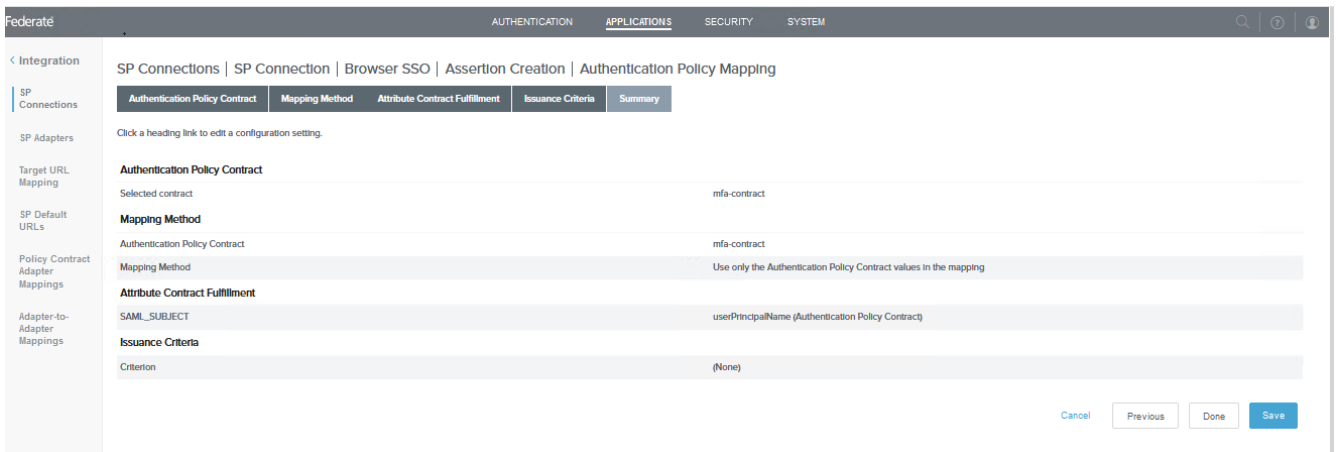




8. Click the **Map New Authentication Policy** button and select the created policy contract(mfa-contract)



9. Click **Next** until the summary tab and click **Save** to save the New Authentication Policy.



10. Click Save to save the adapters and policy contract.

License Warning: Approaching expiration date on Aug 10 2021.

SP Connections | SP Connection | Browser SSO | Assertion Creation

Identity Mapping | Attribute Contract | Authentication Source Mapping | **Summary**

PingFederate uses IdP adapters, partner IdPs or Authentication Policies to authenticate users to your SP. Users may be authenticated by one of several different adapters or Policy Contracts, so map an adapter instance for each IDM system or a authentication policy contract for each policy.

Adapter Instance Name	Virtual Server IDs	Action
AdAuth		Delete
SmartcardAuth		Delete
Authentication Policy Contract Name	Virtual Server IDs	Action
mfa-contract		Delete

Map New Adapter Instance Map New Authentication Policy

Cancel Previous Next Done **Save**

11. Click **Next** to review the authentication policy *Summary* page and click **Done**.

License Warning: Approaching expiration date on Aug 10 2021.

SP Connections | SP Connection | Browser SSO | Assertion Creation

Identity Mapping | Attribute Contract | Authentication Source Mapping | Summary

Summary information for your Assertion Creation configuration. Click a heading link to edit a configuration setting.

Assertion Creation

Identity Mapping

Enable Standard Identifier: true

Attribute Contract

Attribute: SAML_SUBJECT

Subject Name Format: urn:oasis:names:tc:SAML:1:nameid-format:emailAddress

Attribute: firstName

Attribute Name Format: urn:oasis:names:tc:SAML:2.0:attribute-format:unspecified

Attribute: lastName

Attribute Name Format: urn:oasis:names:tc:SAML:2.0:attribute-format:unspecified

Authentication Source Mapping

Adapter instance name: AdAuth

Adapter instance name: SmartcardAuth

Authentication policy contract name: mfa-contract

Adapter Instance

Selected adapter: AdAuth

Mapping Method

Adapter: HTML Form IDP Adapter

Mapping Method: Use only the Adapter Contract values in the mapping

Attribute Contract Fulfillment

firstName: givenName (Adapter)

lastName: sn (Adapter)

SAML_SUBJECT: username (Adapter)

Issuance Criteria

Criterion: (None)

Adapter Instance

Selected adapter: SmartcardAuth

Mapping Method

Adapter: X.509 Certificate IDP Adapter 1.3

Mapping Method: Use only the Adapter Contract values in the mapping

Attribute Contract Fulfillment

firstName: givenName (Adapter)

lastName: sn (Adapter)

SAML_SUBJECT: userPrincipalName (Adapter)

Issuance Criteria

Criterion: (None)

Authentication Policy Contract

Selected contract: mfa-contract

Mapping Method

Authentication Policy Contract: mfa-contract

Mapping Method: Use only the Authentication Policy Contract values in the mapping

Attribute Contract Fulfillment

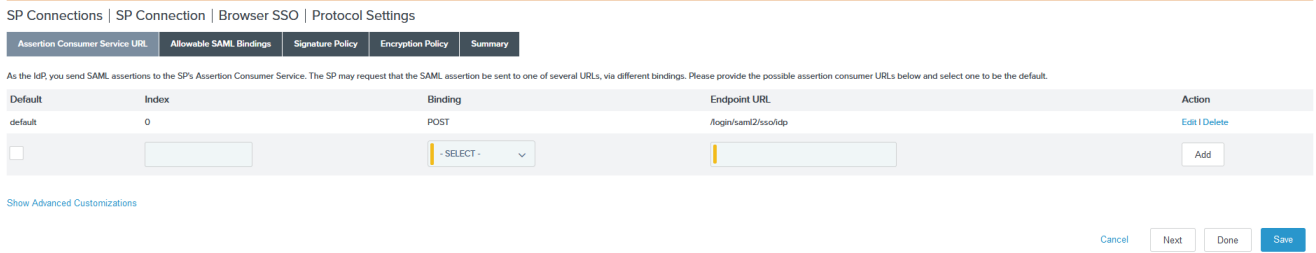
firstName: firstName (Authentication Policy Contract)

lastName: lastName (Authentication Policy Contract)

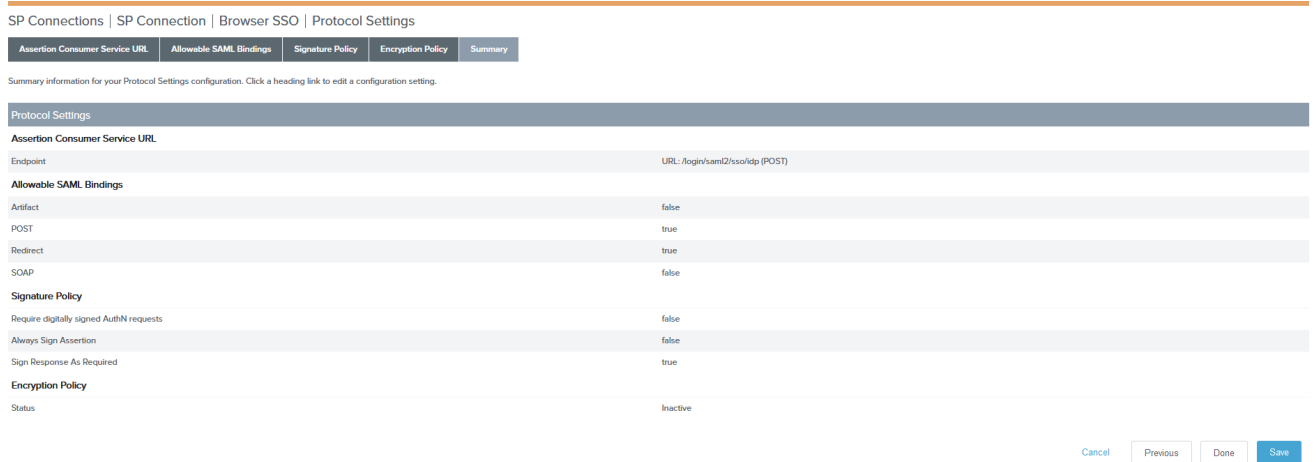
Configure Protocol Settings

1. Click the **Configure Protocol Settings** button.

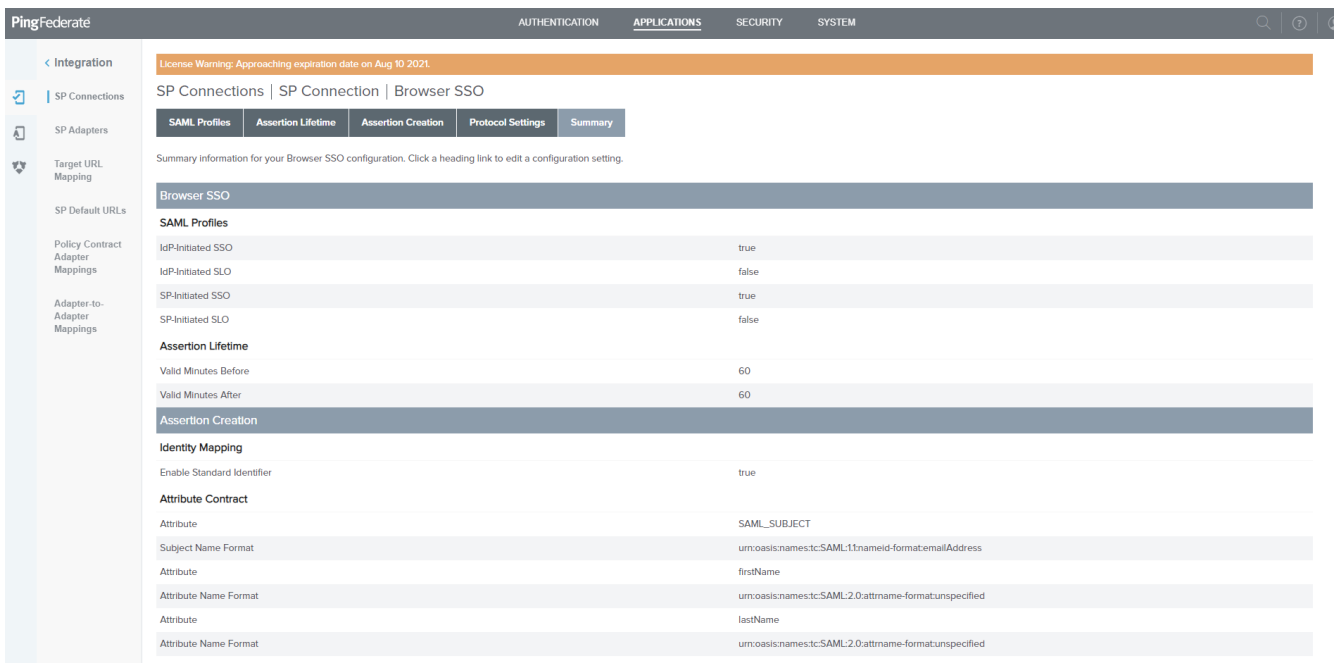
2. Select **POST** from the Binding drop-down list and enter the SAML Endpoint URL `/login/saml2/sso/idp` copied from Management Console in the Endpoint URL field click **Add > Next**.



3. Select the **POST/REDIRECT** checkboxes on the *Allowable SAML Bindings* page and click **Next**.
4. Click **Next** on the Signature Policy page, click **Next** again on the Encryption Policy page, then click **Done** on the protocol settings Summary page.

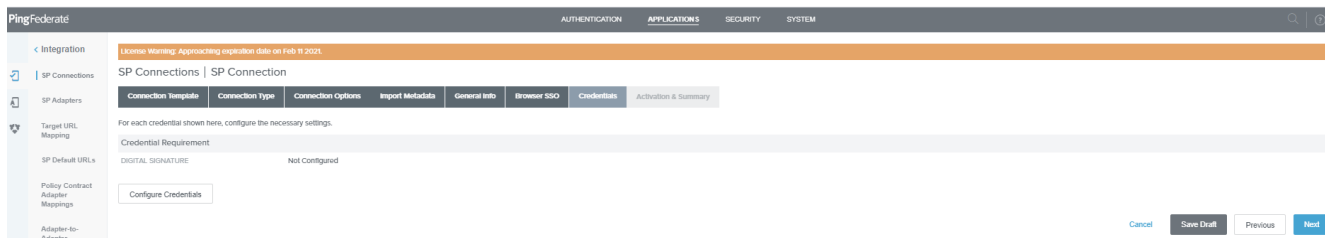


5. Click **Done** on the Browser SSO Summary page and click **Next** on the Browser SSO page.

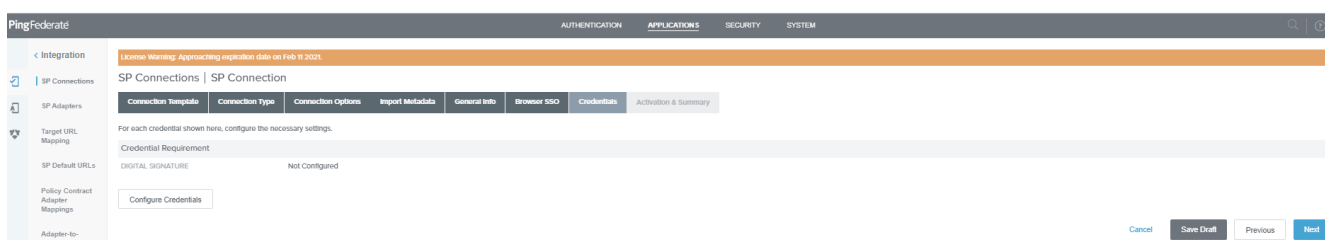


Configure Credentials

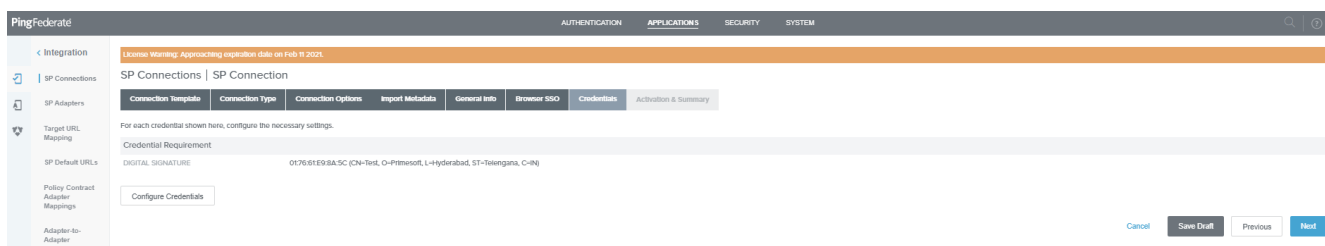
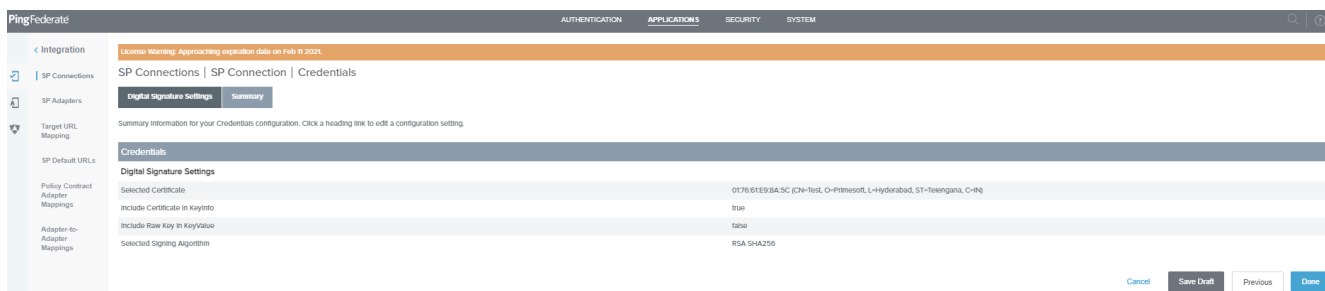
1. Click the **Configure Credentials** button on the SP Connection Credentials page.



2. Select the certificate you want to use with Management Console from the SIGNING CERTIFICATE drop-down list and select **INCLUDE THE CERTIFICATE IN THE SIGNATURE ELEMENT** and click **Next**.



3. Click **Done** on the Credentials Digital Signature Summary page and then click **Next** on the Credentials page.



4. Toggle the SSO Application Endpoint slider button to **Active** on the *Activation & Summary* page, then scroll down and click **Save**.

Integration

- SP Connections
- SP Adapters
- Target URL Mapping
- SP Default URLs
- Policy Contract Adapter Mappings
- Adapter-to-Adapter Mappings

License Warning: Approaching expiration date on Jul 11 2021.

SP Connections | SP Connection

Connection Type | **Connection Options** | **Metadata URL** | **General Info** | **Browser SSO** | **Credentials** | **Activation & Summary**

Summary information for your SP connection. Click a heading in a section to edit a particular configuration setting.

SSO Application Endpoint: <https://win-8a3but2ud1q.tdcdarksite.pvt:9031/dp/startSSO.ping?PartnerSpld=https%3A%2F%2F192.168.20.197%2Fsaml2%2Fservice-provider-metadata%2Fidp>

Summary

SP Connection

Connection Type	
Connection Role	SP
Browser SSO Profiles	true
Protocol	SAML 2.0
Connection Template	No Template
WS-Trust STS	false
Outbound Provisioning	false

Connection Options

5. From **APPLICATIONS > SP Connections**, select **Export Metadata** from the **Select Action** drop-down list for Management Console and upload it to Management Console.

pingFederate AUTHENTICATION APPLICATIONS SECURITY SYSTEM

Integration

- SP Connections
- SP Adapters
- Target URL Mapping
- SP Default URLs
- Policy Contract Adapter Mappings
- Adapter-to-Adapter Mappings

License Warning: Approaching expiration date on Feb 11 2021.

SP Connections

On this screen you can manage connections to your partner SPs.

Search Clear Narrow By

Connection Name	Connection ID	Virtual ID	Protocol	Enabled	Action
isaConnection	http://172.16.4.103:8080/pingfederate/samlso		SAML 2.0	<input checked="" type="checkbox"/>	Select Action
MC	mcEntity		SAML 2.0	<input checked="" type="checkbox"/>	Select Action
MC_test	Test		SAML 2.0	<input checked="" type="checkbox"/>	Select Action

Create Connection Import Connection

- Export Metadata
- Update with Metadata
- Export Connection
- Copy
- Delete

← → ↻ 🏠 <https://192.168.20.83:9999/pingfederate/app#/spConnections> 90%

pingFederate AUTHENTICATION APPLICATIONS SECURITY SYSTEM

Integration

- SP Connections
- SP Adapters
- Target URL Mapping
- SP Default URLs
- Policy Contract Adapter Mappings
- Adapter-to-Adapter Mappings

SP Connections | Metadata Export

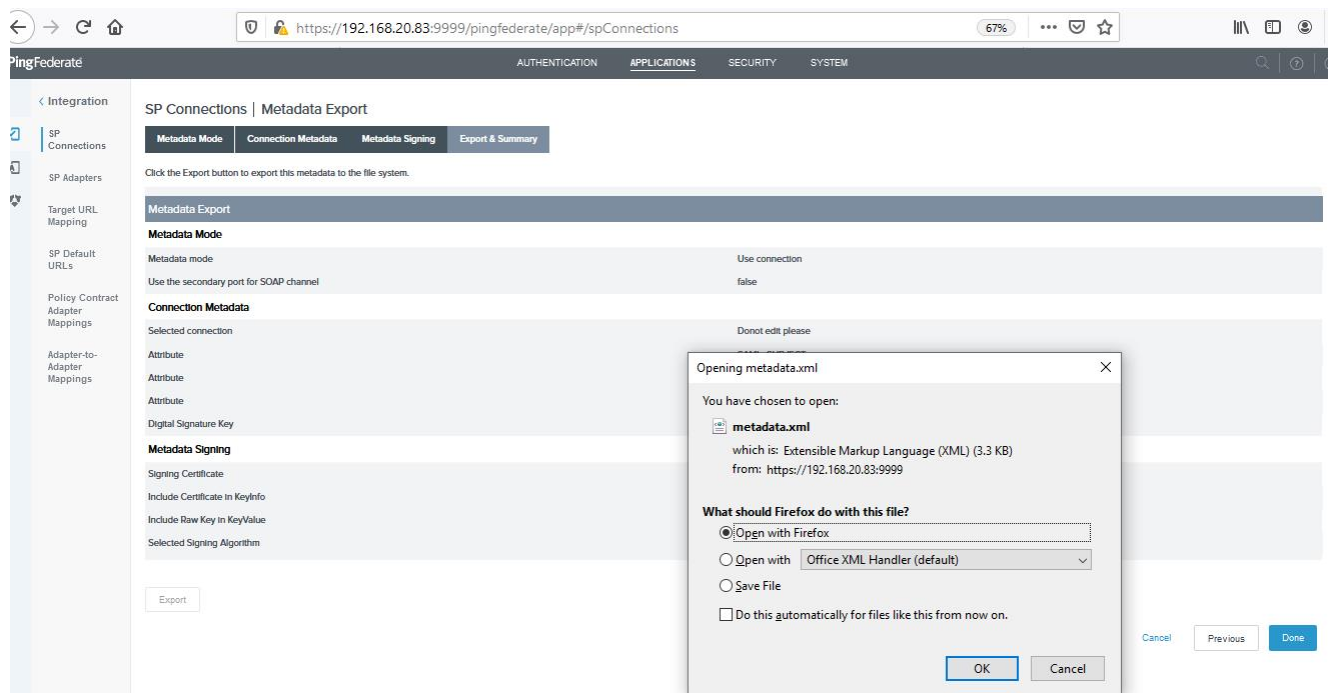
Metadata Mode | **Connection Metadata** | **Metadata Signing** | **Export & Summary**

From this list of certificates, choose which one to use for signing the selected file.

SIGNING CERTIFICATE:

Manage Certificates

Cancel Previous **Next**



6. Upload the downloaded metadata XML file to **Management Console > SETTINGS > AUTHENTICATION > IDP CONFIGURATION** tab.

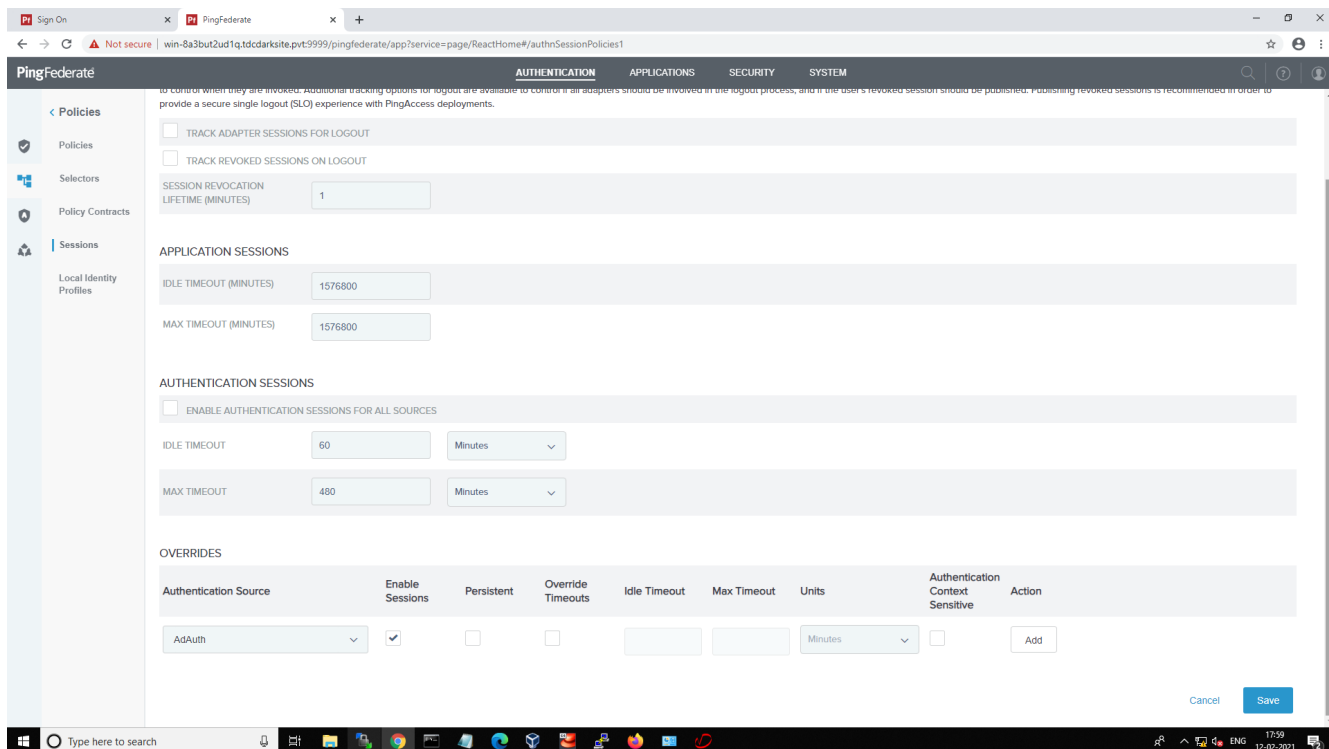
LINK TO MC GUIDE REQUIRED HERE (Please check Identity Provider Metadata Upload functionality in Management Console section). IDP user can able to login to MC using PingFederate IDP.

7. Test IDP login. The login flow will be as follows:

- a. Select the Management Console **SIGN IN WITH IDP** button.
- b. You will be redirected to the PingFederate login page.
- c. Enter your IDP user login credentials.
- d. Select your smart card certificate.
- e. Enter your smart card PIN number.
- f. You are now logged into Management Console using your smart card issued credentials.

SSO POLICY CREATION

1. To support SSO in PingFederate, Navigate to **Authentications > Policies > Sessions** and in the **VERRIDES** section, select **AD Adapter(AdAuth)** from the Authentication Source drop-down list and select the **Enable Sessions** checkbox and click **Save**.

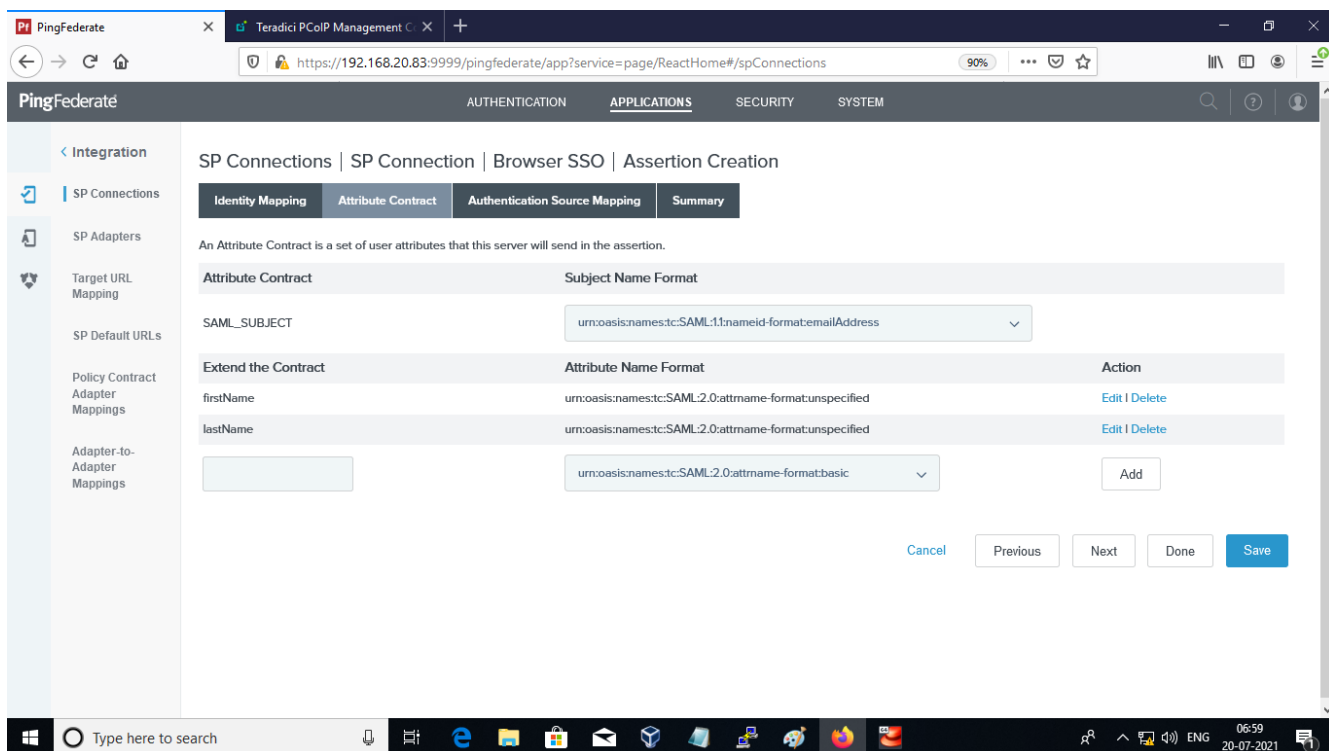


FIRSTNAME AND LASTNAME CONFIGURATIONS

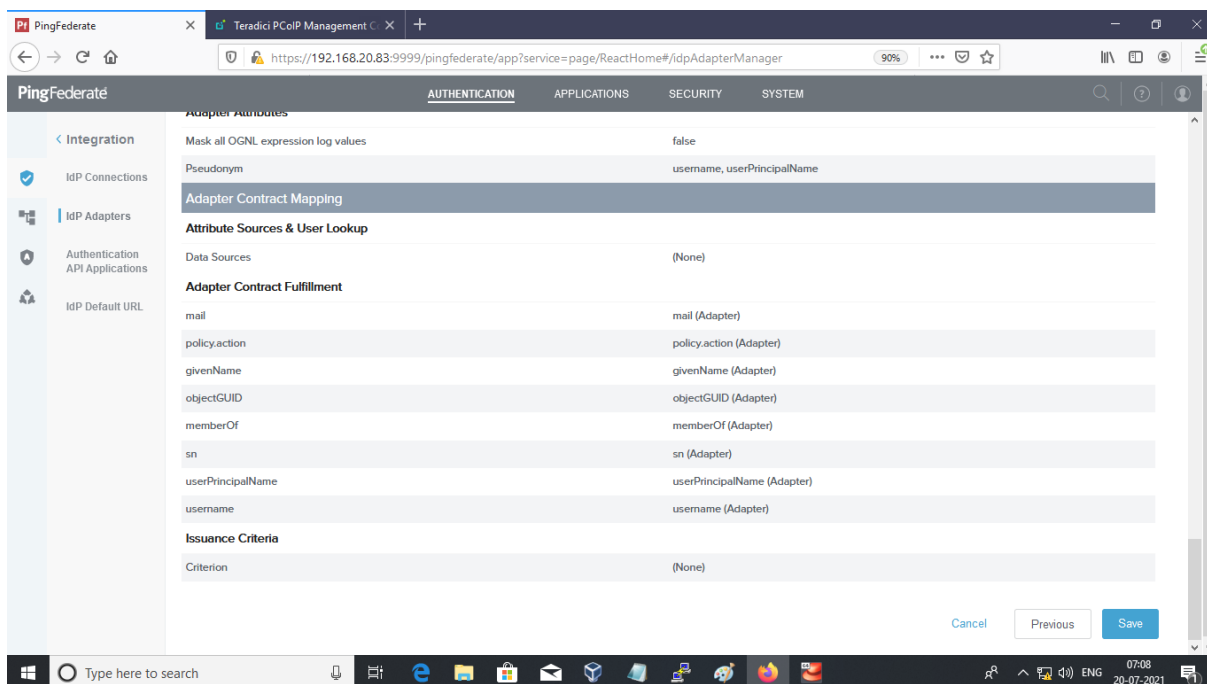
Configuration of firstName and lastName is optional. By default, Management Console saves usernames as firstname and lastname.

The following steps are required to map Management Console user credentials in PingFederate.

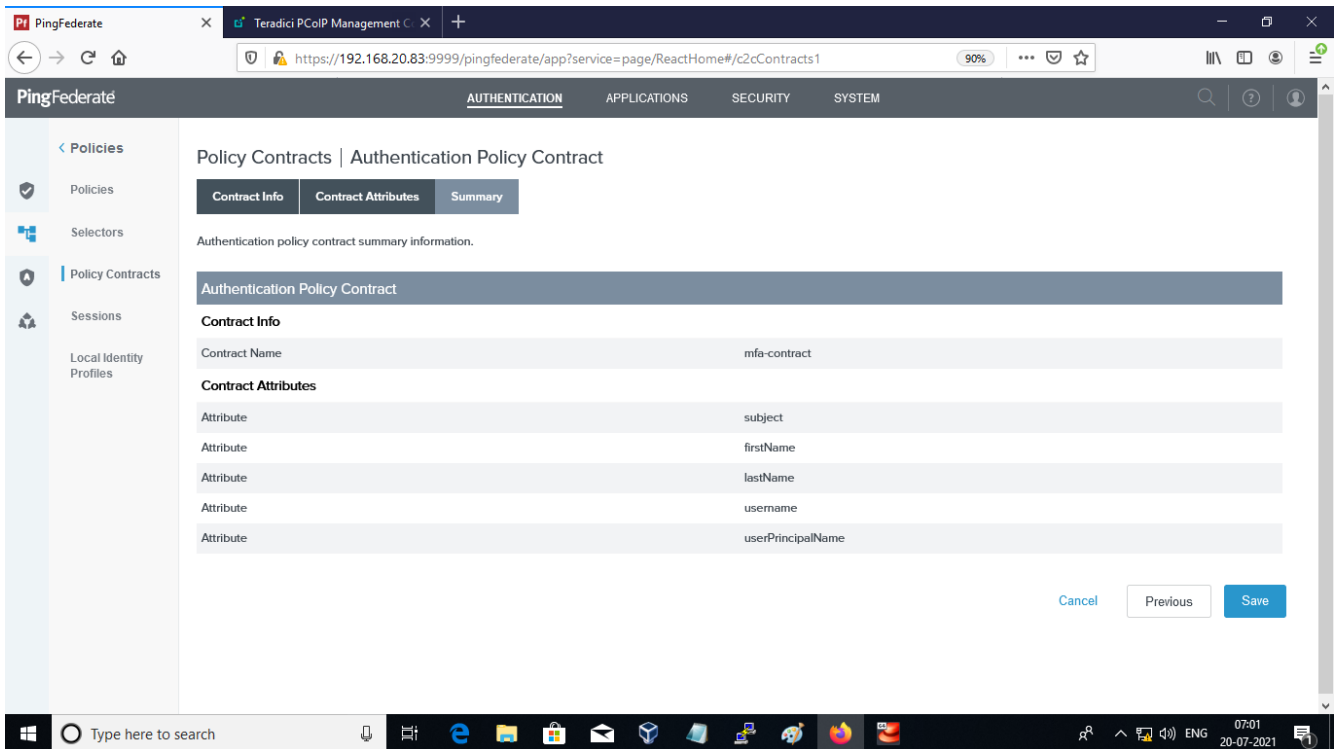
1. Map the Active Directory **givenName** as firstName, and **sn** as lastName of a user in the ADadapter, smart card adapter, and contract policy.



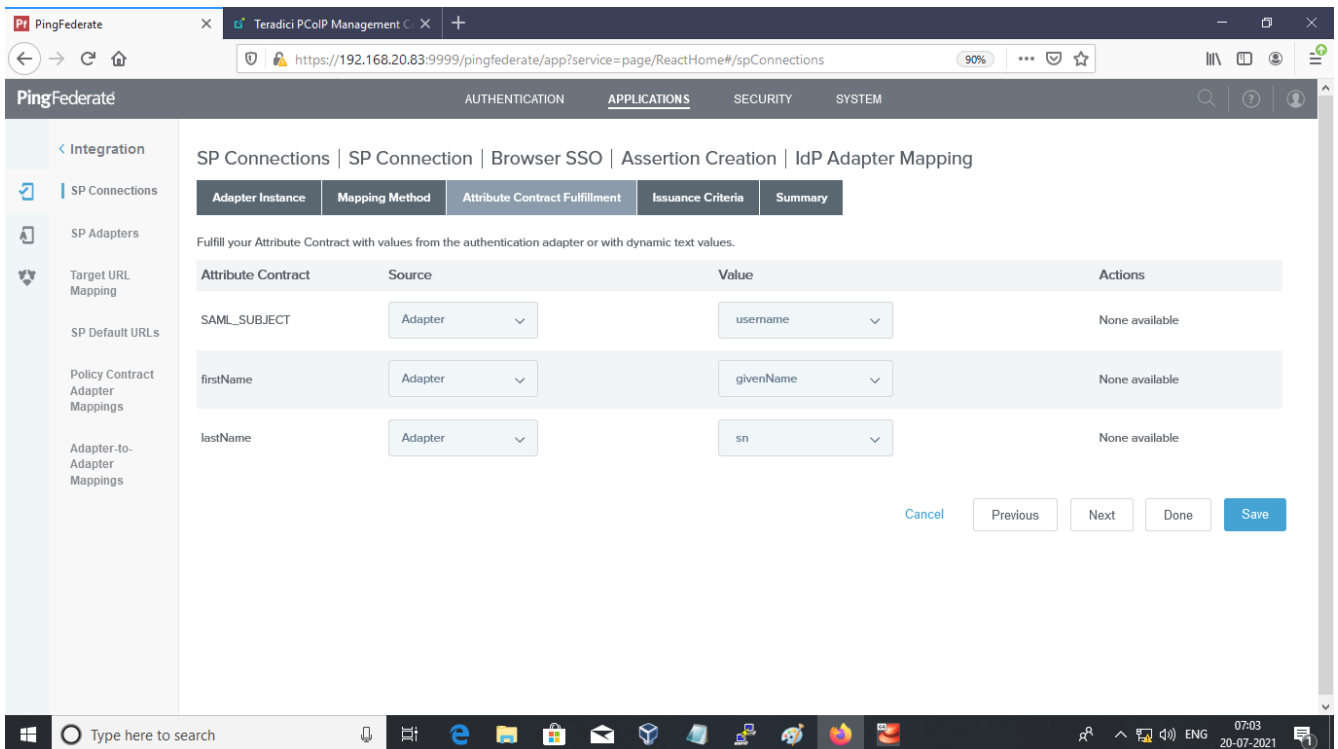
2. Review the summary and click **Save**.



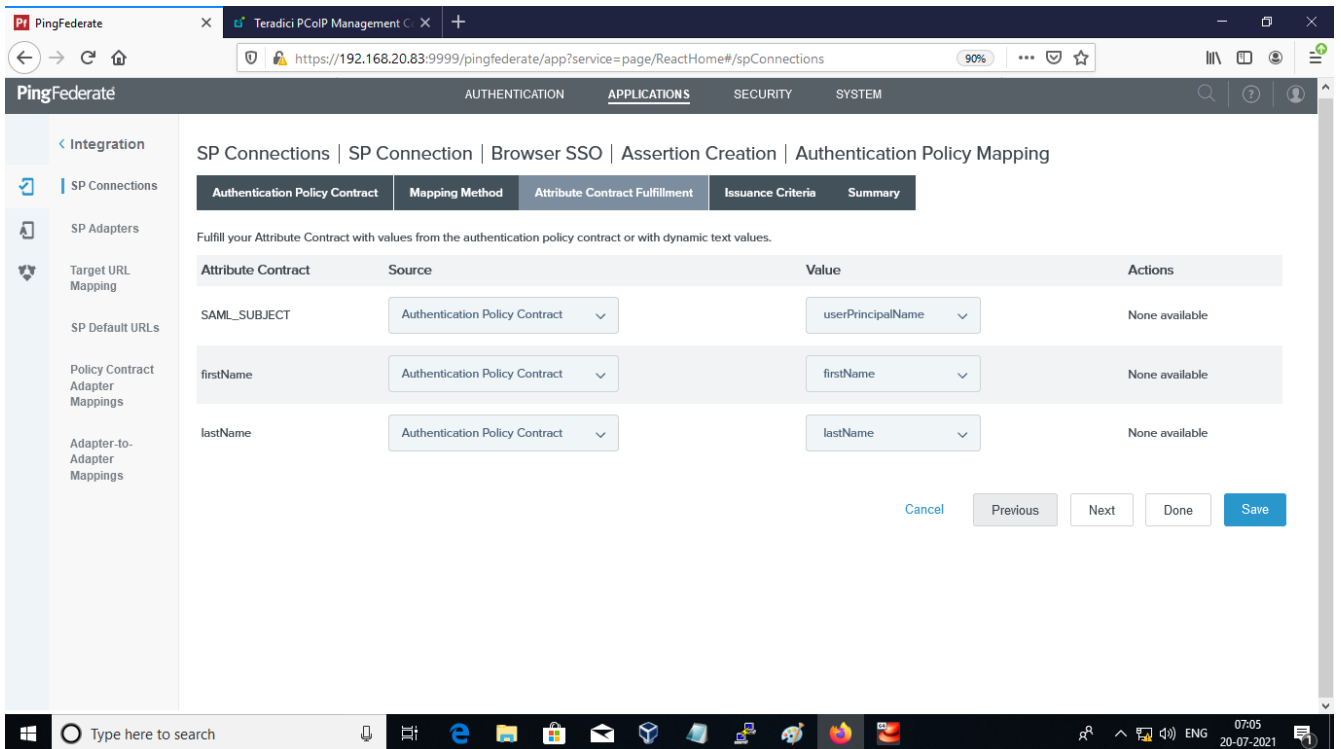
3. Add the `firstName` and `lastName` in the *Authentication Policy Contract* and click **Save**.



4. Add the firstName and lastName in the *SPConnection > IDP Adapter Mapping* and click **Save**.

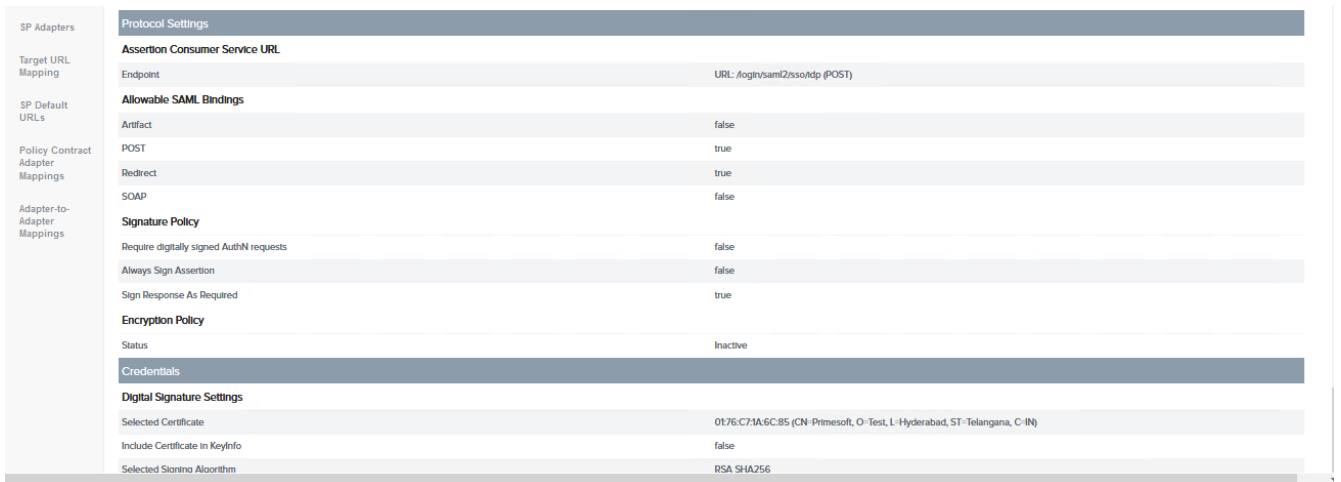


5. Add the firstName and lastName in the *Authentication Policy Mapping* and click **Save**.

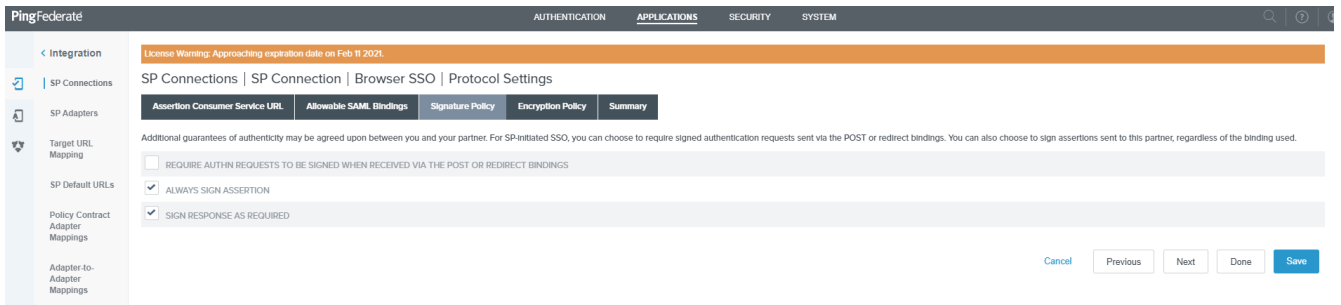


UPLOAD ASSERTION ENCRYPTION CERTIFICATE IN PINGFEDERATE

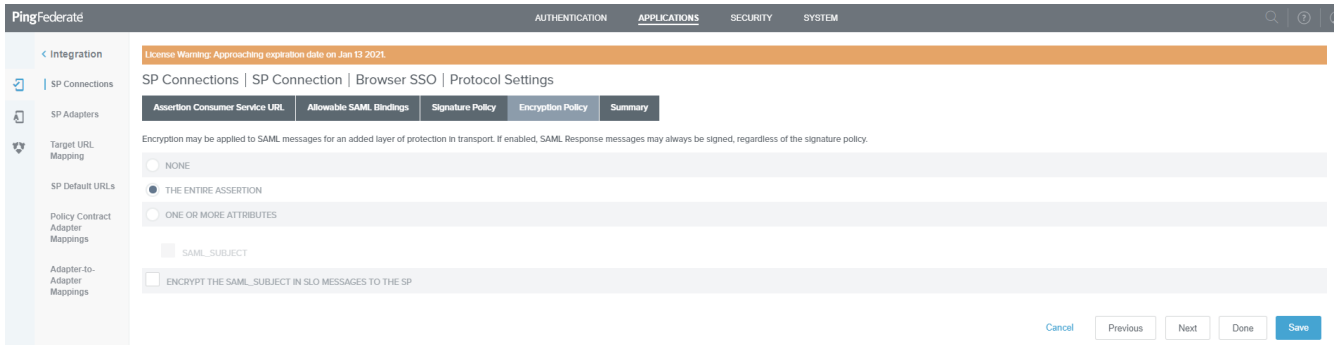
1. In SP Connection details, navigate to the Protocol Settings section and click on **Signature policy**.



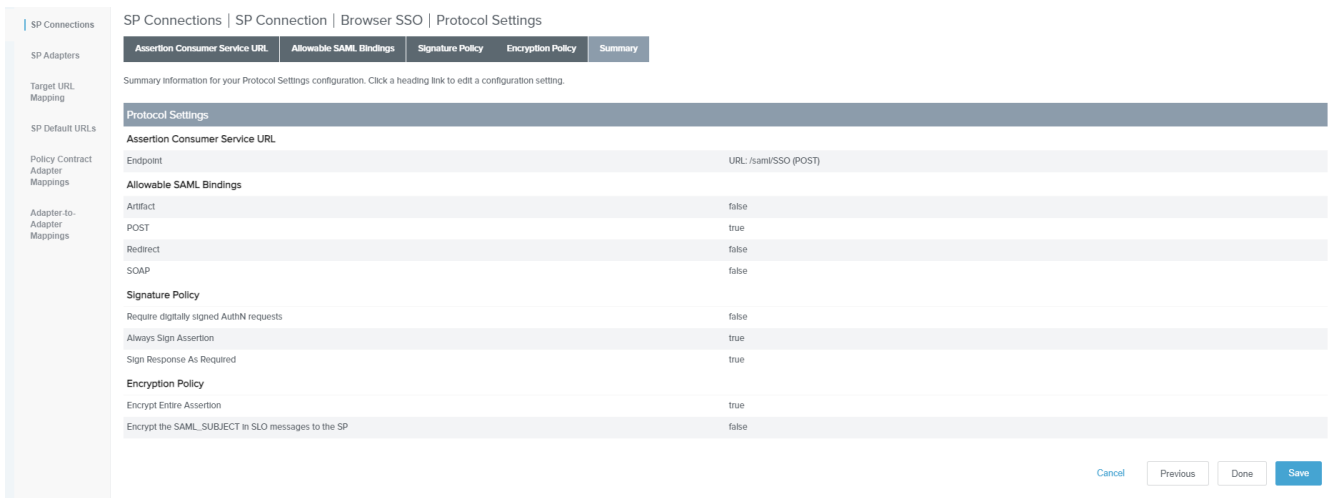
2. From the Browser SSO Protocol Settings Page, select the **Signature Policy** tab and select the **ALWAYS SIGN ASSERTION** and **SIGN RESPONSE AS REQUIRED** checkboxes and click on **Next**.



3. Select **THE ENTIRE ASSERTION** radio button on the *Encryption Policy* page and click **Next**.



4. Review the *Protocol Settings Summary* page and click **Save**.



5. In the *Credentials* section, click the **Select XML Encryption Certificate** link.

Assertion Consumer Service URL

Endpoint URL: /saml/SSO (POST)

Allowable SAML Bindings

Artifact false
 POST true
 Redirect false
 SOAP false

Signature Policy

Require digitally signed AuthN requests false
 Always Sign Assertion true
 Sign Response As Required true

Encryption Policy

Encrypt Entire Assertion true
 Encrypt the SAML_SUBJECT in SLO messages to the SP false

Credentials

Digital Signature Settings

Selected Certificate 0176:61E9:8A:5C (CN=Test, O=Primesoft, L=Hyderabad, ST=Telengana, C=IN)
 Include Certificate in KeyInfo false
 Selected Signing Algorithm RSA SHA256

Select XML Encryption Certificate

Selected Block Encryption Algorithm AES-256
 Selected Key Transport Algorithm RSA-OAEP
 Selected Encryption Certificate 3A:0B:24:AD (CN=MC SAML SECURITY)

6. (Optional) Click on the **Manage Certificates** button if you want to upload a new certificate.

PingFederate AUTHENTICATION APPLICATIONS SECURITY SYSTEM

License Warning: Approaching expiration date on Feb 11 2021.

SP Connections | SP Connection | Credentials

Digital Signature Settings | Select XML Encryption Certificate | Summary

Please select the partner certificate to use when encrypting message content as well as the preferred block encryption and key transport algorithms. Only RSA keys can be used for XML encryption.

Block Encryption Algorithm: AES-128, AES-256 (HELP), TRIPLE DES
 Key Transport Algorithm: RSA-V1.5, RSA-OAEP

3A:0B:24:AD (CN=MC SAML SECURITY)

Manage Certificates

Cancel Previous Next Done Save

7. Click on the **Import** button.

PingFederate AUTHENTICATION APPLICATIONS SECURITY SYSTEM

License Warning: Approaching expiration date on Feb 11 2021.

SP Connections | SP Connection | Credentials | XML Encryption Certificate Management

Import and manage the XML encryption certificate.

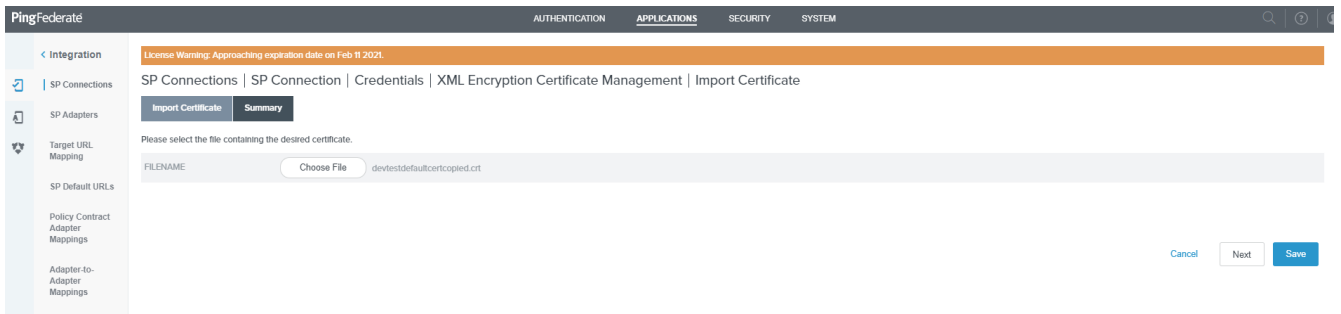
SERIAL	SUBJECT DN	EXPIRES	SIGNATURE VERIFICATION	XML ENCRYPTION	ACTION
119:D0:6D:00:02:00:00:05:A6	CN=*,autolab.local, OU=Orion, O=Teradici, L=Burnaby, ST=BC, C=CA	Fri Jun 25 04:06:06 IST 2021 Status: Valid			Select Action
3A:0B:24:AD	CN=MC SAML SECURITY	Tue Jan 07 22:10:10 IST 2031 Status: Valid			Select Action

Import

Done

8. Select the **Choose File** and select the encryption certificate and click on **Next**.

!!! tip "Encryption Certificate" The encryption certificate is downloaded from the **Management Console > AUTHENTICATION > IDP CONFIGURATION** tab.



9. On the *Import Certificate* summary page click on **Save**.



10. On the **XML Encryption Certificate Management** page click on **Done**.



11. On the Select XML Encryption Certificate tab of the *Credentials* page, select the **AES-256** and **RSA-OAEP** radio buttons, then select the uploaded certificate from the drop-down list and click **Next**.

Integration

SP Connections | SP Connection | Credentials

Digital Signature Settings | Select XML Encryption Certificate | Summary

Please select the partner certificate to use when encrypting message content as well as the preferred block encryption and key transport algorithms. Only RSA keys can be used for XML encryption.

Block Encryption Algorithm: AES-128 AES-256 (HELP) TRIPLE DES

Key Transport Algorithm: RSA-V1.5 RSA-OAEP

3A:0B:24:AD (CN=MC SAML SECURITY)

Manage Certificates

Cancel Previous Next Done Save

12. Verify the details on the *Summary* page and click on **Save**.

Protocol Settings

Assertion Consumer Service URL

Endpoint: URL:/saml/SSO (POST)

Allowable SAML Bindings

Artifact: false

POST: true

Redirect: false

SOAP: false

Signature Policy

Require digitally signed AuthN requests: false

Always Sign Assertion: true

Sign Response As Required: true

Encryption Policy

Encrypt Entire Assertion: true

Encrypt the SAML_SUBJECT in SLO messages to the SP: false

Credentials

Digital Signature Settings

Selected Certificate: 0176:61E9:8A:5C (CN=Test, O=Primesoft, L=Hyderabad, ST=Telengana, C=IN)

Include Certificate in KeyInfo: false

Selected Signing Algorithm: RSA SHA256

Select XML Encryption Certificate

Selected Block Encryption Algorithm: AES-256

Selected Key Transport Algorithm: RSA-OAEP

Selected Encryption Certificate: 3A:0B:24:AD (CN=MC SAML SECURITY)

Firewall References

Configuring firewalld for New Installs of Management Console 20.04 or newer

As of release 20.04, Management Console was upgraded for use with firewalld. Current versions of Management Console do not configure any firewall settings, but instead leaves firewall configurations in control of the administrator. In earlier versions of Management Console, the installer would enable **iptables**, create and apply a new set of rules that would allow the Management Console to communicate properly. Therefore, firewall configurations were not required for releases 20.01 or older.

If you are using a firewall with Management Console on your Linux system, you must follow the recommended instructions that show how to create the rules required for Management Console communications. You must also add additional rules required to meet the requirements of your corporate security policy.

The steps below are instructions for configuring firewalld, grouped by IPv4 and IPv6 environments.

[To configure firewalld in IPv4 environment](#)

[IPv4 firewalld script](#)

[RPM New Installations: To configure firewalld in IPv6 environment](#)

[OVA New Installations: To configure firewalld in IPv6 environment](#)

Firewalld default behaviors when enabled

- All inbound connections are tested against configured rules that have been applied
- All outbound connections are allowed
- Rules to allow traffic are added to the default zone. All other traffic will be blocked.

Uninstalling RPM

Uninstalling the Management Console RPM does not completely remove the firewall rules.

New Installs in IPv4 Environment

To configure firewalld for Management Console communication in an IPv4 environment perform the following steps:

1. Login to the Management Console host operating system console.
2. Enable firewalld.

```
sudo systemctl enable firewalld --now
```

3. Get the default zone. If the default zone is trusted it will allow all packets. It is recommended that the default zone is set to public.

```
sudo firewall-cmd --get-default
```

If default zone is not public, execute the following commands to set the default zone to public.

```
sudo firewall-cmd --permanent --zone=trusted --remove-service=pcoip-agent
sudo firewall-cmd --set-default=public
sudo firewall-cmd --reload
```

4. Get the default zone and assign it to a variable.

```
def_zone=$(firewall-cmd --get-default)
```

5. Set the log (all denied packets logged together).

```
sudo firewall-cmd --set-log-denied=all
```

6. Add an interface.

```
sudo firewall-cmd --zone=$(echo $def_zone) --change-interface=$(ip addr show |
grep "state UP" | head -1 | awk -F': ' '{print $2}')
```

7. Enable required ports.

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --add-
port={80,443,22,5172}/tcp
```

8. Allow pings.

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --remove-icmp-
block={echo-reply,echo-request} 2>/dev/null
```

9. Redirect port 443 to 8443.

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --add-forward-  
port=port=443:proto=tcp:toport=8443
```

10. Enable IP Masquerading.

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --add-masquerade
```

11. Redirect Port 80 to 8080.

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --add-forward-  
port=port=80:proto=tcp:toport=8080
```

12. Drop incoming packets to 127/8 from other interfaces other than loopback interface.

```
sudo firewall-cmd --permanent --new-zone loopback 2>/dev/null  
sudo firewall-cmd --permanent --zone=loopback --change-interface=lo 2>/dev/  
null  
sudo firewall-cmd --zone=loopback --permanent --set-target=ACCEPT  
sudo firewall-cmd --zone=loopback --permanent --add-source=127.0.0.0/8
```

13. Reload the firewall.

```
sudo firewall-cmd --reload
```

14. Confirm the rules are applied.

a. Check the firewalld status is active.

```
sudo systemctl status firewalld
```

```
[autorunner@gcp892b829c82864a9aa9b870e795e74383 ~]$ sudo systemctl status firewalld  
● firewalld.service - firewalld - dynamic firewall daemon  
  Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor preset: enabled)  
  Active: active (running) since Fri 2020-02-14 10:24:12 UTC; 34min ago  
  Docs: man:firewalld(1)  
 Main PID: 730 (firewalld)  
  CGroup: /system.slice/firewalld.service  
          └─730 /usr/bin/python2 -Es /usr/sbin/firewalld --nofork --nopid
```


b. Verify all rules are added in firewalld or not, all rules should be applied.

```
sudo firewall-cmd --list-all
```

```
[autorunner@gcp8ccbf5e557cd4a089155360bfe8c794b ~]$ sudo firewall-cmd --list-all
trusted (active)
  target: ACCEPT
  icmp-block-inversion: no
  interfaces: eth0
  sources:
  services: ncoip-agent
  ports: 80/tcp 443/tcp 22/tcp 5172/tcp
  protocols:
  masquerade: yes
  forward-ports: port=443:proto=tcp:toport=8443:toaddr=
                 port=80:proto=tcp:toport=8080:toaddr=
  source-ports:
  icmp-blocks:
  rich rules:

[autorunner@gcp8ccbf5e557cd4a089155360bfe8c794b ~]$
```

Firewalld Script for New Installations of Management Console 20.04 or newer Using IPv4

HP has provided instructions to create a script that stops the iptables service, and enables firewalld with the required IPv4 rules for Management Console to work correctly.

The script file is created and executed using the following steps:

1. Copy the script content and save into firewalld.sh

```
sudo vi firewalld.sh
```

```
#!/bin/bash
val1=1
if [ $val1 -eq 1 ]; then
systemctl stop iptables || service iptables stop
systemctl enable firewalld --now
def_zone=$(firewall-cmd --get-default)
if [ $def_zone != "public" ] ; then
    firewall-cmd --permanent --zone=trusted --remove-service=pcoip-agent
    firewall-cmd --set-default=public
    firewall-cmd --reload
    def_zone=$(firewall-cmd --get-default)
fi
firewall-cmd --set-log-denied=all
firewall-cmd --permanent --zone=$(echo $def_zone) --change-interface=`ip
addr show | grep "state UP" | head -1 | awk -F': ' '{print $2}'`
firewall-cmd --zone=$(echo $def_zone) --permanent --add-
port={22,443,80,5172}/tcp
firewall-cmd --zone=$(echo $def_zone) --permanent --remove-icmp-
block={echo-reply,echo-request}
firewall-cmd --zone=$(echo $def_zone) --permanent --add-forward-
port=port=443:proto=tcp:toport=8443
firewall-cmd --zone=$(echo $def_zone) --permanent --add-forward-
port=port=80:proto=tcp:toport=8080
firewall-cmd --permanent --new-zone loopback
firewall-cmd --permanent --zone=loopback --change-interface=lo
firewall-cmd --zone=loopback --permanent --set-target=ACCEPT
firewall-cmd --zone=loopback --permanent --add-source=127.0.0.0/8
firewall-cmd --reload
fi 2> /dev/null
```

1. Provide permissions for the script to execute.

```
sudo chmod +x ./firewalld.sh
```

2. Run firewalld.sh:

```
sudo ./firewalld.sh
```

New Installs in IPv6 Environment¶

To configure firewalld for new RPM installation of Management Console allowing communication in an IPv6 environment perform the following steps:

1. Login to the Management Console host operating system console.
2. Enable firewalld.

```
sudo systemctl enable firewalld --now
```

3. Get the default zone. If the default zone is trusted it will allow all packets. It is recommended that the default zone is set to public.

```
sudo firewall-cmd --get-default
```

If default zone is not public, execute the following commands to set the default zone to public.

```
sudo firewall-cmd --permanent --zone=trusted --remove-service=pcoip-agent
sudo firewall-cmd --set-default=public
sudo firewall-cmd --reload
```

4. Get the default zone and assign it to a variable.

```
def_zone=$(firewall-cmd --get-default)
```

5. Set the log (all denied packets logged together).

```
sudo firewall-cmd --set-log-denied=all
```

6. Add an interface.

```
```
sudo firewall-cmd --permanent --zone=$(echo $def_zone) --change-
interface=`ip addr show | grep "state UP" | head -1 | awk -F': ' '{print
$2}`
```
```

7. Enable required IPv6 ports.

- Open port 443

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --add-rich-rule='rule family=ipv6 port port=443 protocol=tcp accept'
```

- Open port 22

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --add-rich-rule='rule family=ipv6 port port=22 protocol=tcp accept'
```

- Open port 5172

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --add-rich-rule='rule family=ipv6 port port=5172 protocol=tcp accept'
```

- Open port 80

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --add-rich-rule='rule family=ipv6 port port=80 protocol=tcp accept'
```

8. Allow pings.

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --remove-icmp-block={echo-reply,echo-request} 2>/dev/null
```

9. Redirect IPv6 port 443 to 8443.

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --add-rich-rule='rule family=ipv6 forward-port to-port=8443 protocol=tcp port=443'
```

10. Redirect IPv6 Port 80 to 8080.

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --add-rich-rule='rule family=ipv6 forward-port to-port=8080 protocol=tcp port=80'
```

11. Drop incoming packets to 127/8 from other interfaces other than loopback interface.

```
sudo firewall-cmd --permanent --new-zone loopback 2>/dev/null
sudo firewall-cmd --permanent --zone=loopback --change-interface=lo 2>/dev/null
sudo firewall-cmd --zone=loopback --permanent --set-target=ACCEPT
sudo firewall-cmd --zone=loopback --permanent --add-source=127.0.0.0/8
```

12. Reload the firewall.

```
sudo firewall-cmd --reload
```

13. Confirm the rules are applied.

a. Check the firewalld status is active.

```
sudo systemctl status firewalld
```

```
[autorunner@gcp892b829c82864a9aa9b870e795e74383 ~]$ sudo systemctl status firewalld
● firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2020-02-14 10:24:12 UTC; 34min ago
     Docs: man:firewalld(1)
   Main PID: 730 (firewalld)
    CGroup: /system.slice/firewalld.service
           └─730 /usr/bin/python2 -Es /usr/sbin/firewalld --nofork --nopid
```

b. Verify all rules are added in firewalld or not, all rules should be applied.

```
sudo firewall-cmd --list-all
```

```
[primeuser@localhost ~]$ sudo firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: emp0s25 wlp2s0
  sources:
  services: dhcpv6-client ssh
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
    rule family="ipv6" port port="443" protocol="tcp" accept
    rule family="ipv6" port port="22" protocol="tcp" accept
    rule family="ipv6" port port="5172" protocol="tcp" accept
    rule family="ipv6" port port="80" protocol="tcp" accept
    rule family="ipv6" forward-port port="443" protocol="tcp" to-port="8443"
    rule family="ipv6" forward-port port="80" protocol="tcp" to-port="8080"
[primeuser@localhost ~]$
```

To configure firewalld for new OVA installation of Management Console allowing communication in an IPv6 environment perform the following steps:

PCoIP Management Console OVA comes ready for an IPv4 deployment. When deploying into an IPv6 environment, the firewalld IPv4 rules must be replaced with IPv6 rules. Perform the following steps to ensure Management Console only has IPv6 rules enabled after deploying Management Console OVA in an IPv6 environment.

1. Login to the Management Console host operating system console.
2. Close IPv4 22, 443, 80, 5172 ports.

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --remove-port={22,443,80,5172}/tcp
```

3. Remove IPv4 internal port forwarding from 443 to 8443.

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --remove-forward-port=port=443:proto=tcp:toport=8443
```

4. Remove IPv4 internal port forwarding from 80 to 8080.

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --remove-forward-port=port=80:proto=tcp:toport=8080
```

5. Open IPv6 port 443.

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --add-rich-rule='rule family=ipv6 port port=443 protocol=tcp accept'
```

6. Open IPv6 port 22.

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --add-rich-rule='rule family=ipv6 port port=22 protocol=tcp accept'
```

7. Open IPv6 port 5172.

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --add-rich-rule='rule family=ipv6 port port=5172 protocol=tcp accept'
```

8. Open IPv6 port 80

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --add-rich-rule='rule family=ipv6 port port=80 protocol=tcp accept'
```

9. Redirect IPv6 port 443 to 8443.

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --add-rich-r
```

10. Redirect IPv6 port 80 to 8080.

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --add-rich-rule='rule family=ipv6 forward-port to-port=8080 protocol=tcp port=80'
```

11. Reload the firewall rules.

```
Reload firewall rules
```

12. Confirm the rules are applied.

a. Check the firewalld status is active.

```
sudo systemctl status firewalld
```

```
[autorunner@gcp892b829c82864a9aa9b870e795e74383 ~]$ sudo systemctl status firewalld
● firewalld.service - firewalld - dynamic firewall daemon
  Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor preset: enabled)
  Active: active (running) since Fri 2020-02-14 10:24:12 UTC; 34min ago
  Docs: man:firewalld(1)
  Main PID: 730 (firewalld)
  CGroup: /system.slice/firewalld.service
          └─730 /usr/bin/python2 -Es /usr/sbin/firewalld --nofork --nopid
```

b. Verify all rules are added in firewalld or not, all rules should be applied.

```
sudo firewall-cmd --list-all
```

```
[primeuser@localhost ~]$ sudo firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: emp0s25 wlp2s0
  sources:
  services: dhcpv6-client ssh
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
    rule family="ipv6" port port="443" protocol="tcp" accept
    rule family="ipv6" port port="22" protocol="tcp" accept
    rule family="ipv6" port port="3172" protocol="tcp" accept
    rule family="ipv6" port port="80" protocol="tcp" accept
    rule family="ipv6" forward-port port="443" protocol="tcp" to-port="8443"
    rule family="ipv6" forward-port port="80" protocol="tcp" to-port="8080"
[primeuser@localhost ~]$
```

Configuring firewalld after a Management Console Upgrade

In Management Console releases 19.05 through 20.01, installation disabled **firewalld**, enabled **iptables** and created rules that allowed Management Console to work as expected. Starting with release 20.04, Management Console upgraded to firewalld, and leaves the firewall configuration in the hands of the local administrator.

If you are upgrading from Management Console release 19.05 through 20.01 to release 20.04 or newer using Management Console RPM, existing firewall configurations can be left intact or if moving to firewalld they will have to be re-applied to the upgraded version of Management Console.

If you decide to use firewalld, the following instructions provide the steps to remove the iptables configuration applied by Management Console and steps to add firewalld rules required by Management Console to operate properly. Additional rules required to comply to your corporate security policy must be added by the administrator.

Upgrade Scenarios discussed in this topic are:

[Firewall changes after a RPM Upgrade from Management Console 20.01 or older using IPv4](#)

[Firewall changes for RPM Upgrades from Management Console 20.04 to Management Console 20.07 or newer in IPv4 Deployments](#)

[Firewalld IPv4 Script](#)

[Firewall changes required after an Upgrade from Management Console 20.01 or older to Management Console 20.07 or newer in an IPv6 Deployment](#)

[Firewalld Script for IPv6](#)

[Firewall changes required after an RPM Upgrade from Management Console 20.04 to Management Console 20.07 or newer in IPv6 Deployment](#)

[Firewall changes required after updating a Management Console OVA IPv4 deployment to an IPv6 Deployment](#)

[Firewall changes required when changing an existing Management Console IPv4 deployment to an IPv6 Deployment](#)

Upgrades in IPv4 Environments

Firewall changes after a RPM Upgrade from Management Console 20.01 or older using IPv4

When upgrading from a Management Console 20.01 or older installation using RPM, consideration for all previous installation firewall rules must be considered. The following steps will remove previously installed Management Console iptables IPv4 rules and add firewalld IPv4 rules so Management Console can operate properly in an IPv4 environment.

1. Login to Management Console host operating system console.
2. Check iptables status(which should be active).

```
sudo systemctl status iptables
```

```
[admin@ip-10-12-56-215 ~]$ sudo systemctl status iptables
● iptables.service - IPv4 firewall with iptables
   Loaded: loaded (/usr/lib/systemd/system/iptables.service; enabled; vendor preset: disabled)
   Active: active (exited) since Fri 2020-02-14 11:46:49 UTC; 12min ago
   Process: 889 ExecStart=/usr/libexec/iptables/iptables.init start (code=exited, status=0/SUCCESS)
  Main PID: 889 (code=exited, status=0/SUCCESS)
   CGroup: /system.slice/iptables.service
```

3. Check the applied iptables rules.

```
sudo iptables -L
```

```
[admin@ip-10-12-56-215 ~]$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination
ACCEPT     tcp  --  anywhere              anywhere             state NEW tcp dpt:ssh
ACCEPT     tcp  --  anywhere              anywhere             state NEW tcp dpt:pcsync-https
ACCEPT     tcp  --  anywhere              anywhere             state NEW tcp dpt:5172
ACCEPT     icmp --  anywhere              anywhere             icmp echo-request
ACCEPT     icmp --  anywhere              anywhere             icmp echo-reply
ACCEPT     all  --  anywhere              anywhere
REJECT     all  --  anywhere              loopback/8          reject-with icmp-port-unreachable
ACCEPT     all  --  anywhere              anywhere             state RELATED,ESTABLISHED
LOG        all  --  anywhere              anywhere             limit: avg 5/min burst 5 LOG level debug prefix "iptables denied"
DROP      all  --  anywhere              anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination
REJECT     all  --  anywhere              anywhere             reject-with icmp-port-unreachable

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
ACCEPT     icmp --  anywhere              anywhere             icmp echo-reply
ACCEPT     icmp --  anywhere              anywhere             icmp echo-request
ACCEPT     all  --  anywhere              anywhere

Chain LOGDROP (0 references)
target     prot opt source                destination
[admin@ip-10-12-56-215 ~]$
```

4. Remove rule which enabled port 8080.

```
sudo iptables -D INPUT -p tcp -m state --state NEW --dport 8080 -j ACCEPT
```

5. Remove rule which enabled port 8443.

```
sudo iptables -D INPUT -p tcp -m state --state NEW --dport 8443 -j ACCEPT
```

6. Remove rule which enabled port 5172.

```
sudo iptables -D INPUT -p tcp -m state --state NEW --dport 5172 -j ACCEPT
```

7. Remove rule which allowed incoming and outgoing pings.

```
sudo iptables -D INPUT -p icmp --icmp-type echo-request -j ACCEPT
sudo iptables -D OUTPUT -p icmp --icmp-type echo-reply -j ACCEPT
sudo iptables -D OUTPUT -p icmp --icmp-type echo-request -j ACCEPT
sudo iptables -D INPUT -p icmp --icmp-type echo-reply -j ACCEPT
```

8. Remove PREROUTING rule.

```
sudo iptables -t nat -D PREROUTING -i `ip addr show | grep "state UP" |
head -1 | awk -F': ' '{print $2}'` -p tcp --dport 443 -j REDIRECT --to-port
8443
```

9. Drop incoming packets to 127/8 from other interfaces other than loopback interface.

```
sudo iptables -D INPUT -i lo -j ACCEPT
sudo iptables -D INPUT -i lo -d 127.0.0.0/8 -j REJECT
```

10. Remove outbound traffic rule.

```
sudo iptables -D OUTPUT -j ACCEPT
```

11. Remove logging rule.

```
sudo iptables -D INPUT -m limit --limit 5/min -j LOG --log-prefix "iptables
denied: " --log-level 7
```

12. Remove rule which dropped packets not matching any other rule.

```
sudo iptables -D INPUT -j DROP
sudo iptables -D FORWARD -j REJECT
```

13. Save iptables service to save your changes (should show status OK).

```
sudo service iptables save
```

14. Restart iptables to apply your changes.

```
sudo systemctl restart iptables
```

15. Check iptables rules (should not contain rules which Management Console install previously added).

```
sudo iptables -L
```

```
[admin@ip-10-12-56-215 ~]$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination
ACCEPT    tcp  --  anywhere              anywhere           state NEW tcp dpt:ssh
ACCEPT    all  --  anywhere              anywhere           state RELATED,ESTABLISHED

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination

Chain LOGDROP (0 references)
target     prot opt source                destination
[admin@ip-10-12-56-215 ~]$
```

16. Mask iptables.

```
sudo systemctl mask iptables
```

17. Stop iptables service.

```
sudo systemctl stop iptables
```

18. Unmask firewalld, (should show removed symlink).

```
sudo systemctl unmask firewalld
```

```
[admin@ip-~]$ sudo systemctl unmask firewalld
Removed symlink /etc/systemd/system/firewalld.service.
[admin@ip-~]$
```

19. Enable firewalld.

```
sudo systemctl enable firewalld --now
```

20. Start firewalld.

```
sudo systemctl start firewalld
```

21. Check firewalld status (should be active).

```
sudo systemctl status firewalld
```

```
[autorunner@gcp892b829c82864a9aa9b870e795e74383 ~]$ sudo systemctl status firewalld
● firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2020-02-14 10:24:12 UTC; 34min ago
     Docs: man:firewalld(1)
  Main PID: 730 (firewalld)
    CGroup: /system.slice/firewalld.service
           └─730 /usr/bin/python2 -Es /usr/sbin/firewalld --nofork --nopid
```

- a. Get the default zone. If the default zone is trusted it will allow all packets. It is recommended that the default zone is set to public.

```
sudo firewall-cmd --get-default
```

If default zone is not public, execute the following commands to set the default zone to public.

- i. `sudo firewall-cmd --permanent --zone=trusted --remove-service=pcoip-agent`
- ii. `sudo firewall-cmd --set-default=public`
- iii. `sudo firewall-cmd --reload`

22. Get the default zone and assign it to a variable.

```
def_zone=$(firewall-cmd --get-default)
```

23. Set the log.(all denied packets logged together)

```
sudo firewall-cmd --set-log-denied=all
```

24. Add an interface.

```
sudo firewall-cmd --zone=$(echo $def_zone) --change-interface=$(ip addr show |  
grep "state UP" | head -1 | awk -F': ' '{print $2}')
```

25. Enable required ports.

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --add-  
port={80,443,22,5172}/tcp
```

26. Allow pings.

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --remove-icmp-  
block={echo-reply,echo-request} 2>/dev/null
```

27. Redirect port 443 to 8443.

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --add-forward-  
port=port=443:proto=tcp:toport=8443
```

28. Enable IP Masquerading.

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --add-masquerade
```

29. Redirect Port 80 to 8080.

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --add-forward-  
port=port=80:proto=tcp:toport=8080
```

30. Drop incoming packets to 127/8 from other interfaces other than loopback interface.

```
sudo firewall-cmd --permanent --new-zone loopback 2>/dev/null  
sudo firewall-cmd --permanent --zone=loopback --change-interface=lo 2>/dev/  
null  
sudo firewall-cmd --zone=loopback --permanent --set-target=ACCEPT  
sudo firewall-cmd --zone=loopback --permanent --add-source=127.0.0.0/8
```

31. Reload the firewall rules.

```
sudo firewall-cmd --reload
```

32. Confirm the rules are applied.

a. Check the firewalld status is active.

```
sudo systemctl status firewalld
```

```
[autorunner@gcp892b829c82864a9aa9b870e795e74383 ~]$ sudo systemctl status firewalld
● firewalld.service - firewalld - dynamic firewall daemon
  Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor preset: enabled)
  Active: active (running) since Fri 2020-02-14 10:24:12 UTC; 34min ago
  Docs: man:firewalld(1)
  Main PID: 730 (firewalld)
  CGroup: /system.slice/firewalld.service
          └─730 /usr/bin/python2 -Es /usr/sbin/firewalld --nofork --nopid
```

b. Verify all rules are added in firewalld, all rules should be applied.

```
sudo firewall-cmd --list-all
```

```
[autorunner@gcp8ccb5e557cd4a089155360bfe8c794b ~]$ sudo firewall-cmd --list-all
trusted (active)
  target: ACCEPT
  icmp-block-inversion: no
  interfaces: eth0
  sources:
  services: ncoin-agent
  ports: 80/tcp 443/tcp 22/tcp 5172/tcp
  protocols:
  masquerade: yes
  forward-ports: port=443:proto=tcp:toport=8443:toaddr=
                 port=80:proto=tcp:toport=8080:toaddr=
  source-ports:
  icmp-blocks:
  rich rules:
```

Firewall changes for RPM Upgrades from Management Console 20.04 to Management Console 20.07 or newer in IPv4 Deployments

Upgrading from an operational Management Console 20.04 to Management Console 20.07 or newer in an IPv4 environment does not require any firewalld rule changes.

Confirm iptables service has been disabled

It is a good idea to confirm any previous Management Console iptables installation has been removed if your 20.04 version has been previously upgraded from an older version.

Firewalld IPv4 Script

HP has provided instructions to create a script that will apply firewalld rules that allow Management Console to work correctly in an IPv4 environment.

Instructions on creating and executing the script can be found [here](#)

Upgrades in IPv6 Environments

Firewall changes required after an Upgrade from Management Console 20.01 or older to Management Console 20.07 or newer in an IPv6 Deployment

When upgrading from a Management Console 20.01 or older installation using RPM, consideration for previous installation firewall rules must be considered. The following steps will remove previously installed iptables IPv4 rules and add firewalld IPv6 rules so Management Console can operate properly in an IPv6 environment.

1. Login to Management Console host operating system console.
2. Check iptables status(which should be active).

```
sudo systemctl status iptables
```

```
[admin@ip-10-12-56-215 ~]$ sudo systemctl status iptables
● iptables.service - IPv4 firewall with iptables
   Loaded: loaded (/usr/lib/systemd/system/iptables.service; enabled; vendor preset: disabled)
   Active: active (exited) since Fri 2020-02-14 11:46:49 UTC; 12min ago
     Process: 889 ExecStart=/usr/libexec/iptables/iptables.init start (code=exited, status=0/SUCCESS)
    Main PID: 889 (code=exited, status=0/SUCCESS)
      CGroup: /system.slice/iptables.service
```

3. Check the applied iptables rules.

```
sudo iptables -L
```

```
[admin@ip- ~]$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination           state NEW tcp dpt:ssh
ACCEPT    tcp  --  anywhere              anywhere              state NEW tcp dpt:pcsync-https
ACCEPT    tcp  --  anywhere              anywhere              state NEW tcp dpt:5172
ACCEPT    icmp --  anywhere              anywhere              icmp echo-request
ACCEPT    icmp --  anywhere              anywhere              icmp echo-reply
ACCEPT    all  --  anywhere              anywhere
REJECT    all  --  anywhere              loopback/8           reject-with icmp-port-unreachable
ACCEPT    all  --  anywhere              anywhere              state RELATED,ESTABLISHED
LOG       all  --  anywhere              anywhere              limit: avg 5/min burst 5 LOG level debug prefix "iptables denied"
DROP     all  --  anywhere              anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination           reject-with icmp-port-unreachable

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination           icmp echo-reply
ACCEPT    icmp --  anywhere              anywhere              icmp echo-request
ACCEPT    all  --  anywhere              anywhere

Chain LOGDROP (0 references)
target     prot opt source                destination
```

- Remove rule which enabled port 8080.

```
sudo iptables -D INPUT -p tcp -m state --state NEW --dport 8080 -j ACCEPT
```

- Remove rule which enabled port 8443.

```
sudo iptables -D INPUT -p tcp -m state --state NEW --dport 8443 -j ACCEPT
```

- Remove rule which enabled port 5172.

```
sudo iptables -D INPUT -p tcp -m state --state NEW --dport 5172 -j ACCEPT
```

- Remove rule which allowed incoming and outgoing pings.

```
sudo iptables -D INPUT -p icmp --icmp-type echo-request -j ACCEPT
sudo iptables -D OUTPUT -p icmp --icmp-type echo-reply -j ACCEPT
sudo iptables -D OUTPUT -p icmp --icmp-type echo-request -j ACCEPT
sudo iptables -D INPUT -p icmp --icmp-type echo-reply -j ACCEPT
```

- Remove PREROUTING rule.

```
sudo iptables -t nat -D PREROUTING -i `ip addr show | grep "state UP" |
head -1 | awk -F: ' '{print $2}` -p tcp --dport 443 -j REDIRECT --to-port
8443
```

- Drop incoming packets to 127/8 from other interfaces other than loopback interface.

```
sudo iptables -D INPUT -i lo -j ACCEPT
sudo iptables -D INPUT -i lo -d 127.0.0.0/8 -j REJECT
```

- Remove outbound traffic rule.

```
sudo iptables -D OUTPUT -j ACCEPT
```

11. Remove logging rule.

```
sudo iptables -D INPUT -m limit --limit 5/min -j LOG --log-prefix "iptables  
denied: " --log-level 7
```

12. Remove rule which dropped packets not matching any other rule.

```
sudo iptables -D INPUT -j DROP  
sudo iptables -D FORWARD -j REJECT
```

13. Save iptables service to save your changes (should show status OK).

```
sudo service iptables save
```

14. Restart iptables to apply your changes.

```
sudo systemctl restart iptables
```

15. Check iptables rules (should not contain rules which Management Console install previously added).

```
sudo iptables -L
```

```
[admin@ip-10-12-56-215 ~]$ sudo iptables -L  
Chain INPUT (policy ACCEPT)  
target      prot opt source                destination  
ACCEPT     tcp  --  anywhere              anywhere           state NEW tcp dpt:ssh  
ACCEPT     all  --  anywhere              anywhere           state RELATED,ESTABLISHED  
  
Chain FORWARD (policy ACCEPT)  
target      prot opt source                destination  
  
Chain OUTPUT (policy ACCEPT)  
target      prot opt source                destination  
  
Chain LOGDROP (0 references)  
target      prot opt source                destination  
[admin@ip-10-12-56-215 ~]$
```

16. Mask iptables.

```
sudo systemctl mask iptables
```

17. Stop iptables service.

```
sudo systemctl stop iptables
```

18. Unmask firewalld, (should show removed symlink).

```
sudo systemctl unmask firewalld
```

```
[admin@ip-~]$ sudo systemctl unmask firewalld  
Removed symlink /etc/systemd/system/firewalld.service.  
[admin@ip-~]$
```


19. Enable firewalld.

```
sudo systemctl enable firewalld --now
```

20. Start firewalld.

```
sudo systemctl start firewalld
```

21. Check firewalld status (should be active).

```
sudo systemctl status firewalld
```

```
[autorunner@gcp892b829c82864a9aa9b870e795e74383 ~]$ sudo systemctl status firewalld
● firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2020-02-14 10:24:12 UTC; 34min ago
     Docs: man:firewalld(1)
  Main PID: 730 (firewalld)
   CGroup: /system.slice/firewalld.service
           └─730 /usr/bin/python2 -Es /usr/sbin/firewalld --nofork --nopid
```

- a. Get the default zone. If the default zone is trusted it will allow all packets. It is recommended that the default zone is set to public.

```
sudo firewall-cmd --get-default
```

If default zone is not public, execute the following commands to set the default zone to public.

- i. `sudo firewall-cmd --permanent --zone=trusted --remove-service=pcoip-agent`
- ii. `sudo firewall-cmd --set-default=public`
- iii. `sudo firewall-cmd --reload`

22. Get the default zone and assign it to a variable.

```
def_zone=$(firewall-cmd --get-default)
```

23. Set the log.(all denied packets logged together)

```
sudo firewall-cmd --set-log-denied=all
```

24. Add an interface.

```
sudo firewall-cmd --permanent --zone=$(echo $def_zone) --change-interface=`ip addr show | grep "state UP" | head -1 | awk -F': ' '{print $2}'`
```

25. Enable required ports.

26. Open required ports.

- IPv6 Port 443

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --add-rich-rule='rule
family=ipv6 port port=443 protocol=tcp accept'
```

- IPv6 Port 22

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --add-rich-rule='rule
family=ipv6 port port=22 protocol=tcp accept'
```

- IPv6 Port 5172

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --add-rich-rule='rule
family=ipv6 port port=5172 protocol=tcp accept'
```

- IPv6 Port 80

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --add-rich-rule='rule
family=ipv6 port port=80 protocol=tcp accept'
```

27. Allow pings.

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --remove-icmp-
block={echo-reply,echo-request} 2>/dev/null
```

28. Redirect port 443 to 8443.

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --add-rich-rule='rule
family=ipv6 forward-port to-port=8443 protocol=tcp port=443'
```

29. Redirect Port 80 to 8080.

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --add-rich-rule='rule
family=ipv6 forward-port to-port=8080 protocol=tcp port=80'
```

30. Drop incoming packets to 127/8 from other interfaces other than loopback interface.

```
sudo firewall-cmd --permanent --new-zone loopback 2>/dev/null
sudo firewall-cmd --permanent --zone=loopback --change-interface=lo 2>/dev/
null
sudo firewall-cmd --zone=loopback --permanent --set-target=ACCEPT
sudo firewall-cmd --zone=loopback --permanent --add-source=127.0.0.0/8
```

31. Reload the firewall rules.

```
sudo firewall-cmd --reload
```

32. Confirm the rules are applied.

a. Check the firewalld status is active.

```
sudo systemctl status firewalld
```

```
[autorunner@gcp892b829c82864a9aa9b870e795e74383 ~]$ sudo systemctl status firewalld
● firewalld.service - firewalld - dynamic firewall daemon
  Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor preset: enabled)
  Active: active (running) since Fri 2020-02-14 10:24:12 UTC; 34min ago
  Docs: man:firewalld(1)
  Main PID: 730 (firewalld)
  CGroup: /system.slice/firewalld.service
         └─730 /usr/bin/python2 -Es /usr/sbin/firewalld --nofork --nopid
```

b. Verify all rules are added in firewalld, all rules should be applied.

```
sudo firewall-cmd --list-all
```

```
[primeuser@localhost ~]$ sudo firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: emp0s25 wlp2s0
  sources:
  services: dhcpv6-client ssh
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
  rule family="ipv6" port port="443" protocol="tcp" accept
  rule family="ipv6" port port="22" protocol="tcp" accept
  rule family="ipv6" port port="5172" protocol="tcp" accept
  rule family="ipv6" port port="80" protocol="tcp" accept
  rule family="ipv6" forward-port port="443" protocol="tcp" to-port="8443"
  rule family="ipv6" forward-port port="80" protocol="tcp" to-port="8080"
```

Firewalld Script for IPv6

HP has provided instructions to create a script that removes Management Console iptables rules, stops the iptables service, and enables firewalld with the required rules for Management Console to work correctly in an IPv6 deployment.

The script file is created and executed using the following steps:

1. Copy the script content and save into firewalld.sh

```
sudo vi firewalld.sh
```

```

#!/bin/bash
val1=1
if [ $val1 -eq 1 ]; then
systemctl stop iptables || service iptables stop
systemctl enable firewalld --now
def_zone=$(firewall-cmd --get-default)
if [ $def_zone != "public" ] ; then
    firewall-cmd --permanent --zone=trusted --remove-service=pcoip-agent
    firewall-cmd --set-default=public
    firewall-cmd --reload
    def_zone=$(firewall-cmd --get-default)
fi
firewall-cmd --zone=$(echo $def_zone) --permanent --remove-
port={22,443,80,5172}/tcp # Closes 22, 443, 80, 5172 port IPv4 rules
firewall-cmd --zone=$(echo $def_zone) --permanent --remove-forward-
port=port=443:proto=tcp:toport=8443 # Removes IPv4 internal port
forwarding from 443 to 8443
firewall-cmd --zone=$(echo $def_zone) --permanent --remove-forward-
port=port=80:proto=tcp:toport=8080 # Removes IPv4 internal port
forwarding from 80 to 8080
firewall-cmd --set-log-denied=all
firewall-cmd --permanent --zone=$(echo $def_zone) --change-interface=`ip
addr show | grep "state UP" | head -1 | awk -F': ' '{print $2}`
firewall-cmd --zone=$(echo $def_zone) --permanent --add-rich-rule='rule
family=ipv6 port port=443 protocol=tcp accept' # Open 443
port IPv6 rules
firewall-cmd --zone=$(echo $def_zone) --permanent --add-rich-rule='rule
family=ipv6 port port=22 protocol=tcp accept' # Open 22
port IPv6 rules
firewall-cmd --zone=$(echo $def_zone) --permanent --add-rich-rule='rule
family=ipv6 port port=5172 protocol=tcp accept' # Open 5172
port IPv6 rules
firewall-cmd --zone=$(echo $def_zone) --permanent --add-rich-rule='rule
family=ipv6 port port=80 protocol=tcp accept' # Open 80
port IPv6 rules
firewall-cmd --zone=$(echo $def_zone) --permanent --remove-icmp-
block={echo-reply,echo-request} #
Allow icmp ping reply and request
firewall-cmd --zone=$(echo $def_zone) --permanent --add-rich-rule='rule
family=ipv6 forward-port to-port=8443 protocol=tcp port=443' # Forward
IPv6 443 port to 8443
firewall-cmd --zone=$(echo $def_zone) --permanent --add-rich-rule='rule
family=ipv6 forward-port to-port=8080 protocol=tcp port=80' # Forward
IPv6 80 port to 8080
firewall-cmd --permanent --new-zone loopback
firewall-cmd --permanent --zone=loopback --change-interface=lo
firewall-cmd --zone=loopback --permanent --set-target=ACCEPT
firewall-cmd --zone=loopback --permanent --add-source=127.0.0.0/8 # Not

```

```
removing loopback as some services require loopback address to function properly
firewall-cmd --reload          # Reload the firewall tables
firewall-cmd --list-all
fi 2> /dev/null
```

2. Provide permissions for the script to execute.

```
sudo chmod +x ./firewalld.sh
```

3. Run firewalld.sh:

```
sudo ./firewalld.sh
```

Firewall changes required after an RPM Upgrade from Management Console 20.04 to Management Console 20.07 or newer in an IPv6 Deployment

When upgrading from IPv4 to IPv6, firewalld IPv4 rules must be replaced with IPv6 rules.

Perform the following steps to ensure Management Console only has IPv6 rules enabled after upgrading from an IPv4 environment.

1. Login to Management Console operating system console using an SSH client (e.g. PuTTY).
2. Ensure firewalld is enabled.

```
sudo systemctl enable firewalld --now
```

3. Get the default zone. If the default zone is trusted it will allow all packets. It is recommended that the default zone is set to public.

```
sudo firewall-cmd --get-default
```

If default zone is not public, execute the following commands to set the default zone to public.

- a. `sudo firewall-cmd --permanent --zone=trusted --remove-service=pcoip-agent`
- b. `sudo firewall-cmd --set-default=public`
- c. `sudo firewall-cmd --reload`

4. Get the default zone and assign it to a variable.

```
def_zone=$(firewall-cmd --get-default)
```

5. Close IPv4 ports 22, 443, 80, and 5172.

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --remove-port={22,443,80,5172}/tcp
```

6. Remove IPv4 internal port forwarding from 443 to 8443.

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --remove-forward-port=port=443:proto=tcp:toport=8443
```

7. Remove IPv4 internal port forwarding from 80 to 8080.

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --remove-forward-port=port=80:proto=tcp:toport=8080
```

8. Set the log. (all denied packets are logged together)

```
sudo firewall-cmd --set-log-denied=all
```

9. Add an interface.

```
sudo firewall-cmd --permanent --zone=$(echo $def_zone) --change-interface=`ip addr show | grep "state UP" | head -1 | awk -F': ' '{print $2}'`
```

10. Open required ports.

• IPv6 Port 443

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --add-rich-rule='rule family=ipv6 port port=443 protocol=tcp accept'
```

• IPv6 Port 22

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --add-rich-rule='rule family=ipv6 port port=22 protocol=tcp accept'
```

• IPv6 Port 5172

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --add-rich-rule='rule family=ipv6 port port=5172 protocol=tcp accept'
```

• IPv6 Port 80

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --add-rich-rule='rule family=ipv6 port port=80 protocol=tcp accept'
```

11. Allow pings.

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --remove-icmp-block={echo-reply,echo-request} 2>/dev/null
```

12. Redirect port 443 to 8443.

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --add-rich-rule='rule
family=ipv6 forward-port to-port=8443 protocol=tcp port=443'
```

13. Redirect Port 80 to 8080.

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --add-rich-rule='rule
family=ipv6 forward-port to-port=8080 protocol=tcp port=80'
```

14. Drop incoming packets to 127/8 from other interfaces other than loopback interface.

```
sudo firewall-cmd --permanent --new-zone loopback 2>/dev/null
sudo firewall-cmd --permanent --zone=loopback --change-interface=lo 2>/dev/
null
sudo firewall-cmd --zone=loopback --permanent --set-target=ACCEPT
sudo firewall-cmd --zone=loopback --permanent --add-source=127.0.0.0/8
```

15. Reload the firewall rules.

```
sudo firewall-cmd --reload
```

16. Confirm the rules are applied.

a. Check the firewalld status is active.

```
sudo systemctl status firewalld
```

```
[autorunner@gcp892b829c82864a9aa9b870e795e74383 ~]$ sudo systemctl status firewalld
● firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2020-02-14 10:24:12 UTC; 34min ago
     Docs: man:firewalld(1)
   Main PID: 730 (firewalld)
    CGroup: /system.slice/firewalld.service
           └─730 /usr/bin/python2 -Es /usr/sbin/firewalld --nofork --nopid
```

b. Verify all rules are added in firewalld, all rules should be applied.

```
sudo firewall-cmd --list-all
```

```
[primeuser@localhost ~]$ sudo firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: emp0s25 wlp3s0
  sources:
  services: dhcpv6-client ssh
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
    rule family="ipv6" port port="443" protocol="tcp" accept
    rule family="ipv6" port port="22" protocol="tcp" accept
    rule family="ipv6" port port="8172" protocol="tcp" accept
    rule family="ipv6" port port="80" protocol="tcp" accept
    rule family="ipv6" forward-port port="443" protocol="tcp" to-port="8443"
    rule family="ipv6" forward-port port="80" protocol="tcp" to-port="8080"
```

Firewall changes required after updating a Management Console OVA IPv4 deployment to an IPv6 Deployment

To use Management Console OVA in an IPv6 environment, the firewall rules for IPv4 should be removed and the IPv6 rules must be added so Management Console can communicate properly.

Once Management Console 20.07 or newer is deployed, log into its host operating system console and perform the following steps.

1. Close IPv4 ports 22, 443, 80, and 5172.

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --remove-port={22,443,80,5172}/tcp
```

2. Remove IPv4 internal port forwarding rules.

- From port 443 to 8443.

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --remove-forward-port=port=443:proto=tcp:toport=8443
```

- From port 80 to 8080.

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --remove-forward-port=port=80:proto=tcp:toport=8080
```

3. Open required IPv6 ports.

- IPv6 Port 443

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --add-rich-rule='rule family=ipv6 port port=443 protocol=tcp accept'
```

- IPv6 Port 22

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --add-rich-rule='rule family=ipv6 port port=22 protocol=tcp accept'
```

- IPv6 Port 5172

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --add-rich-rule='rule family=ipv6 port port=5172 protocol=tcp accept'
```

- IPv6 Port 80

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --add-rich-rule='rule family=ipv6 port port=80 protocol=tcp accept'
```

4. Redirect required ports.

- Port 443 to 8443

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --add-rich-rule='rule
family=ipv6 forward-port to-port=8443 protocol=tcp port=443'
```

- Port 80 to 8080

```
sudo firewall-cmd --zone=$(echo $def_zone) --permanent --add-rich-rule='rule
family=ipv6 forward-port to-port=8080 protocol=tcp port=80'
```

5. Reload firewall rules.

```
sudo firewall-cmd --reload
```

6. Confirm the rules are applied.

- Check the firewalld status is active.

```
sudo systemctl status firewalld
```

```
[autorunner@gcp892b829c82864a9aa9b870e795e74383 ~]$ sudo systemctl status firewalld
● firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2020-02-14 10:24:12 UTC; 34min ago
     Docs: man:firewalld(1)
   Main PID: 730 (firewalld)
   CGroup: /system.slice/firewalld.service
           └─730 /usr/bin/python2 -Es /usr/sbin/firewalld --nofork --nopid
```

- Verify all rules are added in firewalld, all rules should be applied.

```
sudo firewall-cmd --list-all
```

```
[primeuser@localhost ~]$ sudo firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0e2s wlp2s0
  sources:
  services: dhcpv6-client ssh
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
    rule family="ipv6" port port="443" protocol="tcp" accept
    rule family="ipv6" port port="22" protocol="tcp" accept
    rule family="ipv6" port port="5172" protocol="tcp" accept
    rule family="ipv6" port port="80" protocol="tcp" accept
    rule family="ipv6" forward-port port="443" protocol="tcp" to-port="8443"
    rule family="ipv6" forward-port port="80" protocol="tcp" to-port="8080"
```

Migrating PCoIP Management Console to a Newer Release Using firewalld

HP recommends using firewalld and thus has provisioned scripts and instructions to enable and configure firewalld. The instructions contained in this topic are for administrators who would like to use firewalld with Management Console and are making changes to an existing deployment.

Backup Your Database

Always ensure you have a working backup of your Management Console data when performing a Management Console removal, upgrade, or installation. Considerations should include:

- having a current snapshot of your virtual machine
- having a complete backup or clone of your Linux PC
- having a current backup of your Management Console database.

This topic is separated into different scenarios that differ slightly from one another based on the initial version of Management Console in use. Management Console 20.04 and newer has moved to using **firewalld** as its firewall. RPM upgrades to versions 20.04 or newer do not administer any firewall configurations thus leaving the administrator in complete control of the installation. In Management Console releases 19.05 through 20.01, RPM upgrades disabled firewalld, enabled iptables and created rules that allowed Management Console to work as expected.

- [Migrating PCoIP Management Console to a Newer Release Using firewalld](#)
- [Upgrades in IPv4 Environments](#)
 - [To Upgrade from Management Console 20.01 or older to 20.07 or newer in an IPv4 environment perform the following steps:](#)
 - [To upgrade from Management Console 20.04 to 20.07 or newer in an IPv4 environment perform the following steps:](#)
- [Upgrades in IPv6 Environments](#)
 - [To upgrade from Management Console 20.01 or older to 20.07 or newer in an IPv6 environment perform the following steps:](#)
 - [To upgrade from Management Console 20.04 to 20.07 or newer in an IPv6 environment perform the following steps:](#)

- [To Migrate Management Console 20.07 or newer between IPv4 and IPv6 Networks using a static IP address perform the following steps:](#)

Upgrades in IPv4 Environments

To Upgrade from Management Console 20.01 or older to 20.07 or newer in an IPv4 environment perform the following steps:

The following instructions provide the steps to remove the iptables configuration applied by Management Console and steps to add firewalld rules required by Management Console to operate properly. Additional rules required to comply to your corporate security policy must be added by the administrator.

1. Login to the Management Console host operating system console.
2. Configure your firewall. See [Firewall changes after a RPM Upgrade from Management Console 20.01 or older using IPv4](#)

3. Upgrade existing Management Console to 20.07 or newer.

```
sudo yum install teradicihc-<mc_version>.rpm
```

4. Access Management Console Web UI with IPv4 address.

To upgrade from Management Console 20.04 to 20.07 or newer in an IPv4 environment perform the following steps:

Upgrades from an existing Management Console 20.04 deployment should not require additional firewall configurations as new installs use firewalld.

1. Login to the Management Console host operating system console.
2. Upgrade the existing Management Console to new version using RPM in IPv4 environment.

```
sudo yum install teradicihc-<mc_version>.rpm
```

3. Access Management Console Web UI with IPv4 address.

Upgrades in IPv6 Environments

Loss of Data

When migrating between IPv4 and IPv6, the older unrelated data will be permanently deleted. See [Deleted Data](#) for further details.

To upgrade from Management Console 20.01 or older to 20.07 or newer in an IPv6 environment perform the following steps:

1. Login to the Management Console host operating system console.
2. Upgrade existing 20.01 or later Management Console to 20.07 or newer.

```
sudo yum install teradicimc-<mc_version>.rpm
```

3. After RPM upgrade, perform the steps [Moving between IPv4 and IPv6](#) for switching between IPv4 and IPv6.

Error Message

The error message **connecting to INET family : ipv4 socket. Error No: 101, Reason: Network is unreachable** is expected behavior when upgrading to IPv6. It is OK to ignore this message.

Verify your using the new rpm

Verify your using the new rpm with this command.

```
sudo rpm -qa | grep teradici
```

```
[admin@localhost ~]# sudo rpm -qa | grep teradici
teradicimc-20.07-11780.e17.x86_64
[admin@localhost ~]#
```

4. Access Management Console Web UI with IPv6 address. Depending on your network configuration, this can be either a manual, DHCP, or SLAAC provided IPv6 address.

To upgrade from Management Console 20.04 to 20.07 or newer in an IPv6 environment perform the following steps:

Deleted data when moving between IP versions

When Management Console migrates between IPv4 to IPv6 using RPM, only the common data between IPv4 and IPv6 will be restored. The rest of the data will be deleted. For further details see [Deleted Data When Migrating between IP Protocols](#)

1. Login to the Management Console host operating system console.
2. Upgrade existing 20.04 Management Console to 20.07 or newer. (See tip above)

```
sudo yum install teradici-mc-<mc_version>.rpm
```

Error Message

The error message **connecting to INET family : ipv4 socket. Error No: 101, Reason: Network is unreachable** is expected behavior when upgrading to IPv6. It is OK to ignore this message.

3. After RPM upgrade, perform the steps [Moving between IPv4 and IPv6](#) for switching between IPv4 and IPv6.
4. Access Management Console Web UI with a configured IPv6 address. Depending on your network configuration, this can be either a manual, DHCP, or SLAAC provided IPv6 address.

To Migrate Management Console 20.07 or newer between IPv4 and IPv6 Networks using a static IP address perform the following steps:

These steps must be performed in order for Management Console to operate successfully in a pure IPv6 environment when moving from an IPv4 environment.

1. Login to the Management Console host operating system console.
2. Stop mcconsole and mcdaemon services

```
sudo systemctl stop mcconsole
sudo systemctl stop mcdaemon
```

3. Change IP address from IPv4 to IPv6 [using nmtui](#).
4. Reboot Management Console host operating system.

```
sudo init 6
```

5. [Configure your firewall for IPv6](#)
6. Run scripts to delete unrelated data.

```
cd /opt/teradici/database
sudo python mc_env_db.py
```

Error Message when migrating from IPv4 to IPv6

The error message **connecting to INET family : ipv4 socket. Error No: 101, Reason: Network is unreachable** is expected behavior when migrating from IPv4 to IPv6. It is OK to ignore this message.

7. Start mcconsole and mcdaemon services.

```
sudo systemctl start mcconsole
sudo systemctl start mcdaemon
```

Data deleted

When migrating from IPv4 to IPv6, the data from IPv4 will be deleted during the migration and vice versa.

Deleted data information can be found [here](#)

1. Access Management Console Web UI with the address you configured for IPv6 in step 3.

Removing Management Console iptables Configuration

This reference applies to RPM installations and upgrades from Management Console release 20.01 and older as well as all OVA and AMI installations. The following instructions, provide commands to remove the rules created for iptables by Management Console and instructions to disable the iptables service.

To remove the iptables configuration Management Console applied during installation perform these steps:

1. Login to Management Console host operating system console.
2. Check iptables status (which should be active).

```
sudo systemctl status iptables
```

```
[admin@ip-10-12-56-215 ~]$ sudo systemctl status iptables
● iptables.service - IPv4 firewall with iptables
   Loaded: loaded (/usr/lib/systemd/system/iptables.service; enabled; vendor preset: disabled)
   Active: active (exited) since Fri 2020-02-14 11:46:49 UTC; 12min ago
   Process: 889 ExecStart=/usr/libexec/iptables/iptables.init start (code=exited, status=0/SUCCESS)
  Main PID: 889 (code=exited, status=0/SUCCESS)
   CGroup: /system.slice/iptables.service
```

3. Check the applied iptables rules.

```
sudo iptables -L
```

```
[admin@ip-10-12-56-215 ~]$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination
ACCEPT    tcp  --  anywhere              anywhere             state NEW tcp dpt:ssh
ACCEPT    tcp  --  anywhere              anywhere             state NEW tcp dpt:pcsync-https
ACCEPT    tcp  --  anywhere              anywhere             state NEW tcp dpt:5172
ACCEPT    icmp --  anywhere              anywhere             icmp echo-request
ACCEPT    icmp --  anywhere              anywhere             icmp echo-reply
ACCEPT    all  --  anywhere              anywhere
REJECT    all  --  anywhere              loopback/8          reject-with icmp-port-unreachable
ACCEPT    all  --  anywhere              anywhere             state RELATED,ESTABLISHED
LOG        all  --  anywhere              anywhere             limit: avg 5/min burst 5 LOG level debug prefix "iptables denied"
DROP      all  --  anywhere              anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination
REJECT    all  --  anywhere              anywhere             reject-with icmp-port-unreachable

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
ACCEPT    icmp --  anywhere              anywhere             icmp echo-reply
ACCEPT    icmp --  anywhere              anywhere             icmp echo-request
ACCEPT    all  --  anywhere              anywhere

Chain LOGDROP (0 references)
target     prot opt source                destination
[admin@ip-10-12-56-215 ~]$
```

4. Remove rule which enabled port 8080.

```
sudo iptables -D INPUT -p tcp -m state --state NEW --dport 8080 -j ACCEPT
```

5. Remove rule which enabled port 8443.


```
sudo iptables -D INPUT -p tcp -m state --state NEW --dport 8443 -j ACCEPT
```

6. Remove rule which enabled port 5172.

```
sudo iptables -D INPUT -p tcp -m state --state NEW --dport 5172 -j ACCEPT
```

7. Remove rule which allowed incoming and outgoing pings.

```
sudo iptables -D INPUT -p icmp --icmp-type echo-request -j ACCEPT
sudo iptables -D OUTPUT -p icmp --icmp-type echo-reply -j ACCEPT
sudo iptables -D OUTPUT -p icmp --icmp-type echo-request -j ACCEPT
sudo iptables -D INPUT -p icmp --icmp-type echo-reply -j ACCEPT
```

8. Remove PREROUTING rule.

```
sudo iptables -t nat -D PREROUTING -i `ip addr show | grep "state UP" |
head -1 | awk -F': ' '{print $2}'` -p tcp --dport 443 -j REDIRECT --to-port
8443
```

9. Drop incoming packets to 127/8 from other interfaces other than loopback interface.

```
sudo iptables -D INPUT -i lo -j ACCEPT
sudo iptables -D INPUT -i lo -d 127.0.0.0/8 -j REJECT
```

10. Remove outbound traffic rule.

```
sudo iptables -D OUTPUT -j ACCEPT
```

11. Remove logging rule.

```
sudo iptables -D INPUT -m limit --limit 5/min -j LOG --log-prefix "iptables
denied: " --log-level 7
```

12. Remove rule which dropped packets not matching any other rule.

```
sudo iptables -D INPUT -j DROP
sudo iptables -D FORWARD -j REJECT
```

13. Save iptable service to save your changes (should show status OK).

```
sudo service iptables save
```

14. Restart iptables to apply your changes.

```
sudo systemctl restart iptables
```

15. Check iptables rules (should not contain rules which Management Console install previously added).

```
sudo iptables -L
```

```
[admin@ip-10-12-56-215 ~]$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination
ACCEPT    tcp  --  anywhere              anywhere           state NEW tcp dpt:ssh
ACCEPT    all  --  anywhere              anywhere           state RELATED,ESTABLISHED

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination

Chain LOGDROP (0 references)
target     prot opt source                destination
[admin@ip-10-12-56-215 ~]$
```

16. Mask iptables.

```
sudo systemctl mask iptables
```

17. Stop iptables service.

```
sudo systemctl stop iptables
```

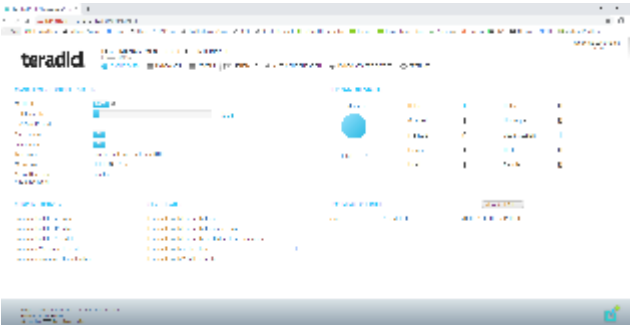
Deleted Data When Migrating between IP Protocols

After migrating from an IPv4 network to an IPv6 network (or vice versa), Management Console deletes data related to the removed IP version.

This table provides descriptions of data that is deleted and uses an example of a migration from IPv4 to IPv6.

 **IPv6 to IPv4 migrations**

Similarly, IPv6 data is deleted when migrating from IPv6 to IPv4.

Tab Name Migration Behavior	Display Before Migration
<p>Dashboard</p> <p>The data related to IPv4 endpoints will not be restored. Schedule data is restored.</p>	
<p>Endpoints</p> <p>All the groups will be restored. IPv4 endpoints will be deleted.</p>	

Tab Name Migration Behavior	Display Before Migration
---------------------------------------	------------------------------------



PCoIP MANAGEMENT CONSOLE
Release - 20.01.0

DASHBOARD | ENDPOINTS

GROUPED 1 | UNGROUPED

EXPAND ALL | PROFILE | STRUCTURE | ENDPOINTS | ENDPOINTS

NAME	IPv4 ADDRESS	ENDPOINT DESCRIPTI...
Group 1		
• 00-30-04-12-14-04	10.100.1.122	Tera2 Client Dual Display
Group 2		
Group 3		

Profile

All profiles will be restored

Tab Name Migration Behavior	Display Before Migration
---------------------------------------	------------------------------------

← → ↻ ⚠ Not secure | 10.12.56.110/profile/index

Apps Teradici Slack JetBrains Account Repo Home - PCoIP Man..

teradici®

PCoIP MANAGEMENT CONSOLE
Release - 20.01.0

DASHBOARD | ENDPOINT

NEW PROFILE | EDIT | DUPLICATE | DELETE

NAME	DESCRIPTION	GROUP
Profile 1		Group

Schedule

All schedules will be restored

Tab Name	Display
Migration Behavior	Before Migration

← → ↻ ⚠ Not secure | 10.12.56.110/schedule/index

Apps Teradici Slack JetBrains Account Repo Home - PCoIP Man

teradici

PCoIP MANAGEMENT CONSOLE
Release - 20.01.0

DASHBOARD ENDPOINTS

SCHEDULES HISTORY

NEW SCHEDULE VIEW EDIT DELETE All Schedules ON ?

NAME	DESCRIPTION	ACTION
Schedule 1		Profile

Auto Configuration

Autoconfig rules related to **IPv4 IP Ranges** will be deleted. Autoconfig rules related to **password** and **generic** tag will be restored.

Tab Name Migration Behavior	Display Before Migration



PCoIP MANAGEMENT CO
Release - 20.01.0

DASHBOARD | ENDPO

NEW RULE | VIEW | EDIT | DELETE

AUTO CONFIGURATION

Endpoints can be automatically configured and assigned to groups once they are discovered.

ON ?

GROUP	RULE TYPE	IPv4
Group 1	IP ADDRESS	10.1
Group 2	PASSWORD	
Group 3	GENERIC TAG	

Endpoint Certificates

Tab Name Migration Behavior	Display Before Migration
--------------------------------	-----------------------------

All Endpoint
Certificates will be
restored.

teradici PCoIP MANAGEMENT CONSOLE
Release - 20.01.0

DASHBOARD | ENDPOINTS

NEW CERTIFICATE RULE | VIEW | EDIT | DELETE

CERTIFICATE MANAGEMENT

Certificates can be automatically requested on Zero Clients only

ON ?

ID	GROUPS	SERVERS
1	Group 1	http://10...

Authentication

All users will be
restored.

**If any AD users are
present they will be
disabled.**

Tab Name
Migration Behavior

Display
Before Migration






← → ↻ ⚠ Not secure | 10.12.56.110/settings/users

📱 Apps 🗨 Teradici Slack 🗑 JB JetBrains Account 📄 Repo 🎓 Home - PCoIP Man.



PCoIP MANAGEMENT CONSOLE
Release - 20.01.0

🕒 DASHBOARD | 📱 ENDPON

-  AUTHENTICATION
-  NAMING
-  SOFTWARE
-  SECURITY
-  DATABASE
-  LICENSE
-  REMOTE
-  VERSION

AUTHENTICATION

USERS ROLES AND PERMISSIONS ACTIVE

NEW USER EDIT ENABLE DISABLE

USERNAME	LAST M
admin	User
user	1

Active Directory Configuration

IPv4 Active Directory Configuration will not be restored

Tab Name
Migration Behavior

Display
Before Migration

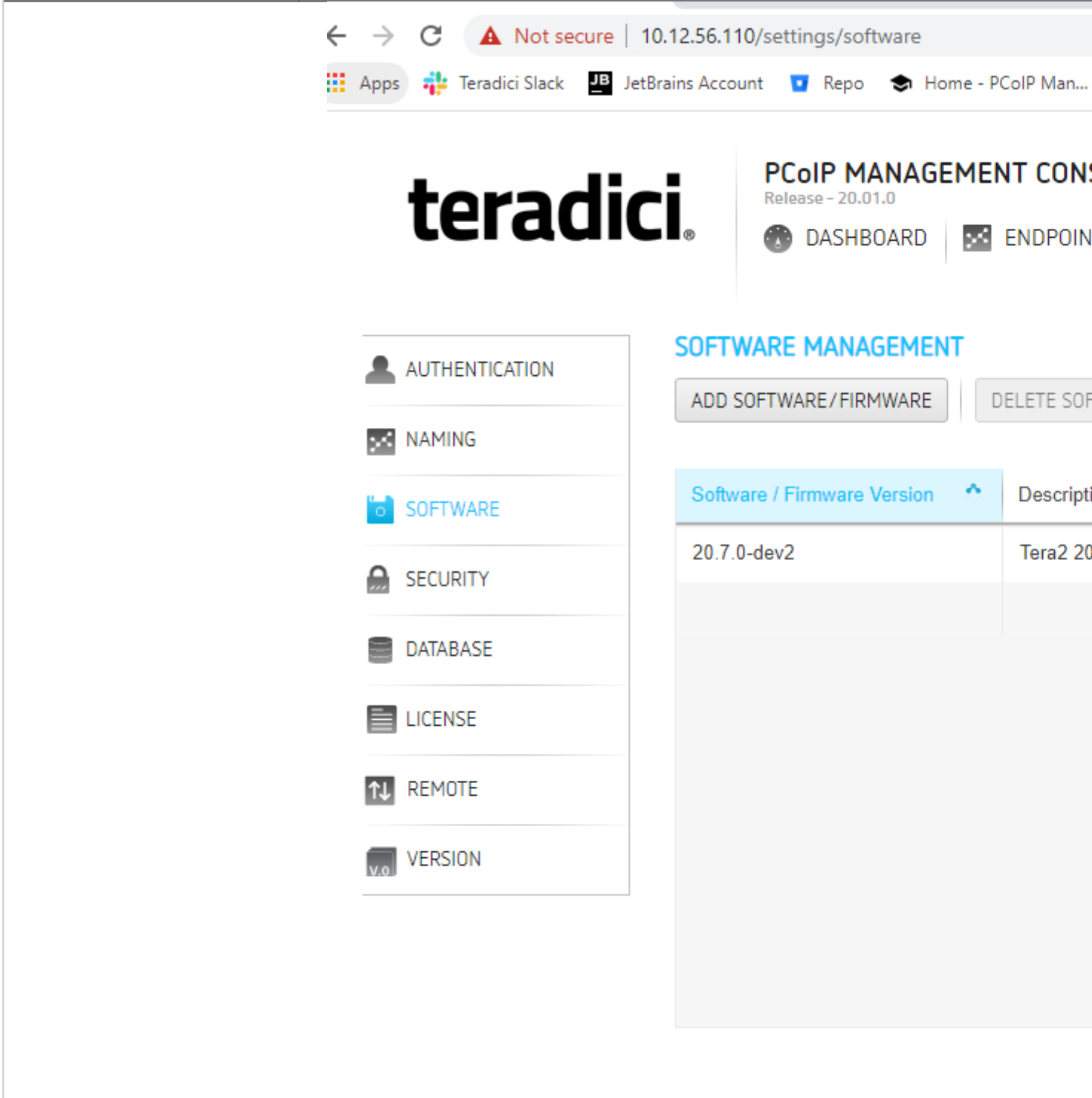
Remote Configuration

In Remote Configuration, IPv4 related Local IP Address ranges will not be restored

Tab Name Migration Behavior	Display Before Migration
--------------------------------	-----------------------------

Software

All softwares will be restored.

Tab Name Migration Behavior	Display Before Migration
 <p>The screenshot shows a web browser window with the URL 10.12.56.110/settings/software. The page features the Teradici logo and navigation links for Dashboard and Endpoints. A sidebar menu includes Authentication, Naming, Software (highlighted), Security, Database, License, Remote, and Version. The main content area is titled 'SOFTWARE MANAGEMENT' and contains buttons for 'ADD SOFTWARE/FIRMWARE' and 'DELETE SOFTWARE'. A table below shows a list of software versions, with the first entry being '20.7.0-dev2' with a description 'Tera2 20...'. The browser's address bar shows a 'Not secure' warning.</p>	

Troubleshooting

Troubleshooting

The troubleshooting section of this guide allows users to easily find the topics and links that are required for various aspects of troubleshooting your PCoIP Management Console.

- The PCoIP Management Console records logs of its activity on a rotational basis. Logs also have two levels which can be set depending on how much details is required to solve an issue. For further information, see [Managing PCoIP Management Console Logs](#).


Troubleshooting Endpoints in Recovery Mode

Recovery mode is a special version of the PCoIP Zero Client firmware that takes effect when the client experiences a problem that renders it unable to operate. Recovery mode automatically becomes active under the following conditions:

- A firmware update fails.
- The client has an invalid configuration.
- The client has been unable to complete its boot sequence after a number of attempts.

This mode lets you correct the configuration, or upload a replacement firmware or certificate file. You can do this directly from a client's AWI or you can use a PCoIP Management Console profile to correct the problem.

Locating Endpoints in Recovery Mode

 **Note: Recovery mode is only available for PCoIP Zero Clients**

Recovery mode is not available on Remote Workstation Cards.

If you have an endpoint in recovery mode, make a note of its firmware version number. You can then locate all endpoints in recovery mode from the PCoIP Management Console ENDPOINTS page by creating a filter to display endpoints running this firmware version.

The following example creates a filter for firmware version earlier than 5.0.0.



ADD FILTER

Software Version is 1.3.0

Software Version is 1.3.0

CLEAR CANCEL OK

Filter criterion for finding endpoints in recovery mode

Recovery Mode Causes and Solutions

The following problems can cause an endpoint to be in recovery mode:

- The client may have been forced into recovery mode by a user repeatedly tapping the power button when turning on the endpoint. If so, rebooting (resetting) the PCoIP Zero Client may return it to the main firmware.
- If the client does not load the main firmware but boots into the recovery image immediately when powered up, then it is likely that a firmware upload operation was interrupted and the client does not contain a valid firmware image. Apply a profile to upload a new firmware image to the PCoIP Zero Client and reboot the client to return to working firmware.
- If the PCoIP Zero Client attempts to boot to the main firmware images a few times (the splash screen is displayed for a bit) but eventually switches to the recovery image, then it is likely that the firmware configuration is not valid. See [Resetting Endpoint Properties to Their Defaults](#) to clear this problem and then re-provision the endpoint.

Recovery Mode Examples

The following example shows a client with a completed firmware upload status. It may have switched to recovery mode by a user repeatedly tapping its power button. In this case, simply performing a power reset may recover the endpoint.

EXPAND ALL								PROFILE	STRUCTURE	ENDPOINTS	ENDPOINT DISCOVERY	SEARCH	FILTER	Software Version is 1.3.0	REFRESH	
NAME	SOFTWARE VERSION	ONLINE	FIRMWARE UPLOAD	FIRMWARE POWER RESET	APPLY PROFILE	PROFILE POWER RESET										
My Group																
My Sub-Group																
• <Prefix>-My Group-M...	1.3.0	True	COMPLETED	COMPLETED	COMPLETED	COMPLETED										

Client in Recovery Mode with Completed Firmware Upload

The next example shows a client in recovery mode because a firmware upload was interrupted. In this case, applying the profile will download the firmware again and may recover the endpoint.

EXPAND ALL								PROFILE	STRUCTURE	ENDPOINTS	ENDPOINT DISCOVERY	SEARCH	FILTER	Software Version is 1.3.0	REFRESH	
NAME	SOFTWARE VERSION	ONLINE	FIRMWARE UPLOAD	FIRMWARE POWER RESET	APPLY PROFILE	PROFILE POWER RESET										
My Group																
My Sub-Group																
• <Prefix>-My Group-M...	1.3.0	False	FAILED	NOT STARTED	NOT STARTED	NOT STARTED										

Client in Recovery Mode with Failed Firmware Upload

Client in Recovery Mode with Failed Firmware Upload

If rebooting a client or uploading firmware again does not recover the endpoint, you must reset parameters to factory defaults and re-provision the endpoint.

Note: Use the client's AWI to reset and configure parameters

You can also use the client's AWI to reset parameters and reconfigure it. See [Accessing an Endpoint's AWI](#).

Troubleshooting DNS

This troubleshooting reference provides some steps to perform to ensure that you have the correct PCoIP Management Console information configured in your DNS server.

 **Note: Instructions are for Windows only**

These instructions apply to the Windows platform.

The procedure shown next checks that you have a DNS A record that maps the PCoIP Management Console's host name to its IP address for forward lookups, and a DNS PTR record that maps the PCoIP Management Console's IP address to its host name for reverse lookups. In addition, it checks that a DNS SRV record for **_pcoip-bootstrap** exists, and that the DNS TXT record containing the PCoIP Management Console's certificate fingerprint exists and is located in the right place.

Also note that:

- DNS records have a time-to-live value that dictates how long the records are cached. If your **nslookup** results show old information, please try clearing the PC's DNS cache using the `ipconfig /flushdns` command before running the **nslookup** commands in this example again.

For example,

```
C:\Users\username> ipconfig /flushdns
```

```
Windows IP Configuration
Successfully flushed the DNS Resolver Cache
```

- PCoIP Zero Client endpoints will cache DNS results for the entire time-to-live period. You can clear this cache by power cycling the endpoint.
- The following SHA-256 fingerprint shown is the default PCoIP Management Console certificate fingerprint. If you have created your own certificates, this value will be different.
- The following example uses sample IP addresses and host names for the primary DNS server and PCoIP Management Console. Please substitute your own server and PCoIP Management Console 2 information for these names and addresses.
- The information returned by the **nslookup** commands is shown in gray text after each command.

To verify DNS PCoIP Management Console information:

1. Log in to your Windows server.
2. Launch a command prompt window by clicking the **Start** button and typing **cmd** in the *Search* box.
3. Launch **nslookup** from the command line prompt:

```
C:\Users\username> nslookup
```

```
Default Server: mydnsserver.mydomain.local
```

```
Address: 172.15.25.10
```

4. Instruct **nslookup** to connect to the DNS server under which you created the records. This address should match the primary DNS server address configured in the endpoint's network settings.

```
> server 172.15.25.10
```

```
Default Server: mydnsserver.mydomain.local
```

```
Address: 172.15.25.10
```

5. Enter the FQDN of your PCoIP Management Console to perform a forward lookup to verify that a DNS A record that maps the PCoIP Management Console host name to its IP address is present:

```
> pcoip-mc.mydomain.local
```

```
Server: mydnsserver.mydomain.local
```

```
Address: 172.15.25.10
```

```
Name: pcoip-mc.mydomain.local
```

```
Address: 172.25.15.20
```

6. Enter the PCoIP Management Console's IP address (found in the previous step) to perform a reverse lookup to verify that a DNS PTR record that maps the PCoIP Management Console IP address to its host name is present:

```
> 172.25.15.20
```

```
Server: mydnsserver.mydomain.local
```

```
Address: 172.15.25.10
```

```
Name: pcoip-mc.mydomain.local
```

```
Address: 172.25.15.20
```

7. Set the record type to **SRV** and check that a DNS SRV record exists to tell endpoints the FQDN of the PCoIP Management Console. In the second command, the domain name is the domain under which your endpoints are configured:

```
> set type=srv
```

```
> _pcoip-bootstrap._tcp.myendpointdomain.local
```

Server: mydnsserver.mydomain.local

Address: 172.15.25.10:

> _pcoip-bootstrap._tcp.myendpointdomain.local SRV service location:

priority =0

weight =0

port =5172

svr hostname =pcoip-mc.mydomain.local

pcoip-mc.mydomain.local internet address = 172.25.15.20

8. Set the record type to **TXT** and check that a DNS TXT record exists containing the PCoIP Management Console SHA-256 fingerprint. In the second command, the domain name is the domain under which your endpoints are configured.

> **set type=txt**

> **pcoip-mc.myendpointdomain.local**

Server: mydnsserver.mydomain.local

Address: 172.15.25.10

pcoip-mc.mydomain.local text = "pcoip-bootstrap-cert=

B7:62:71:01:85:27:46:BB:E3:E9:5C:E2:34:2C:B5:76:7D:7A:F1:7F:6A:4D:5C:DB:AA:2B:

99:BD:D5:A9:28:91"

9. Exit **nslookup**:

> `exit`

Viewing License Information via Command Line

If you need to find license information and are having issues using the Management Console web interface, you can use the **mc_view_lic.sh** script to view licensing information such as the **Fulfillment ID** and **Entitlement ID**(activation code).

You can find the script in **/opt/teradici/licensing/** folder.

Deactivating and Activating Licenses via Command Line

If you are using PCoIP Management Console Enterprise host operating system console, you can also deactivate the PCoIP Management Console Enterprise license by using the **my_return_lic.sh** script.

To deactivate your Management Console license, run the following command:

```
/opt/teradici/licensing/mc_return_lic.sh -f <fulfillment_ID>
```

To deactivate your Management Console license when it is behind a proxy, run the following command:

```
/opt/teradici/licensing/mc_return_lic.sh -f <fulfillmentId> -p [<user:password>@]  
<proxyhost:port>
```

To activate your Management Console license, run the following command:

```
'/opt/teradici/licensing/mc_activate_lic.sh -k < entitlementID >'
```

To activate your Management Console license when it is behind a proxy, run the following command.

```
/opt/teradici/licensing/mc_activate_lic.sh -k <entitlementID> -p [<user:password>@]  
<proxyhost:port>
```

FAQ

FAQs

The latest PCoIP Management Console FAQs can be found [here](#).

Support

Contacting Support

If you encounter any problems installing, configuring, or running the PCoIP Management Console, you can create a support ticket with HP.

Before creating a ticket, be prepared with the following:

- A detailed description of the problem
- The version or versions of PCoIP Management Console involved in the problem. See [Managing PCoIP Management Console Logs](#)
- Appropriate logs that capture the issue. [Locating the PCoIP Management Console's Log Files](#)

The Community Forum

The PCoIP Community Forum enables 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 Global Support Service team. HP staff are heavily involved in the forum.

To visit the community, go to <https://help.teradici.com/s/discussions>.

Finding the PCoIP Management Console Release Number

You can find your PCoIP Management Console release number using the PCoIP Management Console Dashboard.

To find your PCoIP Management Console release number:

Browse to your PCoIP Management Console and view the release number at the bottom of the left of the web interface. It will be in the format of `##.#@####`. For example, 19.05@9507