Teradici PCoIP® Management Console

Version 3.0

Administrators' Guide

TER1401005/A-3.0

Teradici Corporation
#301-4601 Canada Way, Burnaby, BC V5G 4X7 Canada
phone +1.604.451.5800 fax +1.604.451.5818
www.teradici.com

The information contained in this documentation represents the current view of Teradici Corporation as of the date of publication. Because Teradici must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Teradici, and Teradici cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. TERADICI MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Teradici may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Teradici, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property. Visit Notice of Intellectual Property Rights for more information.

Contents

Who Should Read This Guide?

This guide is intended for administrators who are installing and using PCoIP Management Console release 3.0 to discover, configure, and manage zero client endpoints.

Note: Understanding terms and conventions in Teradici guides
For information on the industry specific terms, abbreviations, text conventions, and graphic symbols used in this guide, see Using Teradici Product and Component Guides and the Teradici Glossary.

PCoIP Management Console Overview

Welcome to the Teradici PCoIP® Management Console Administrators' Guide. This documentation explains how to install and use your PCoIP Management Console to discover, configure, and manage your zero client endpoints.

PCoIP Management Console works with the Tera2 PCoIP Zero Client (firmware 5.0 and later). For more information about these zero clients, see the *Tera2 PCoIP Zero Client Firmware Administrators' Guide*.

Related: Support for Tera2 PCoIP Zero Client firmware 4.x and earlier
If you are using Tera2 PCoIP Zero Client 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 zero client endpoints. You can quickly provision new endpoints, configure settings, and update firmware.

Info: PCoIP Management Console no longer storing firmware logs
As of PCoIP Management Console release 2.5.1 and PCoIP Firmware 5.5.0, the zero client no longer sends logs to the PCoIP Management Console and the PCoIP Management Console no longer stores these logs.

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 profiles
- Reset endpoints to factory defaults and control their power settings
- Use custom certificates to secure your PCoIP system

PCoIP Management Console is packaged as an Open Virtualization Format (OVA) file for quick and easy deployment on a VMware Horizon ESXi host.

About PCoIP Management Console Releases

PCoIP Management Console release 1.x is recommended for managing deployments of Tera1 PCoIP zero clients, Tera1 PCoIP Remote Workstation Cards, and Tera2 PCoIP Remote Workstation Cards operating on firmware up to and including 4.9.

PCoIP Management Console went through a technical upgrade which was implemented in release 2.0. Since this release, PCoIP Management Console only administers PCoIP endpoints that operate with firmware 5.0 or newer.

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 (previously called Standard). PCoIP Management Console Enterprise which 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.

PCoIP Management Console Free

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

For information about PCoIP Management Console Free, see PCoIP Management Console on the Teradici 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* on page 11.

PCoIP Management Console Enterprise

PCoIP Management Console Enterprise enables large enterprise deployments to manage up to 20,000 zero clients 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 the Tera2 PCoIP Zero Client firmware, and PCoIP Management Console Enterprise. PCoIP Management Console Enterprise is available through Desktop Access subscription licensing. For more information, see *Comparison of*

PCoIP Management Console Enterprise and PCoIP Management Console Free on page 11.

For information on license offers, term lengths, trial licenses, and the Teradici Support and Maintenance program, see PCoIP Management Console on the Teradici web site.

Comparison of PCoIP Management Console Enterprise and PCoIP Management Console Free

Feature Name	Enterprise	Free
Number of devices supported	Up to 20,000	Up to 100
Supported device types	Tera2 PCoIP Zero Clients	Tera2 PCoIP Zero Clients
Device discovery	DNS SRV records DHCP options Manual discovery Manual entry	DNS SRV records DHCP options Manual discovery Manual entry
Scheduling	One time Daily & weekly recurring Delaying reboots	N/A
Dashboard	General deployment SCEP Schedule Auto Configuration	General deployment N/A N/A N/A
Compatible firmware versions	Tera2 PCoIP Zero Client firmware 5.0 and later	Tera2 PCoIP Zero Client firmware 5.0 and later
Device inventory reports	Yes	No
Support & Maintenance	Paid support included	Complimentary support

Feature Name	Enterprise	Free
Security	Management Console User Session Timeout	No Management Console User Session Timeout
Remote Endpoint Configuration	Yes	No

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* on page 15.
- For instructions on how to activate your license, see *Activating Licenses* on page 27.
- For instructions on how to get up and running quickly, see *Installing the PCoIP Management Console and Configuring Your System* on page 18.
- For instructions on how to migrate your PCoIP Management Console 1 to PCoIP Management Console release 2.x or newer, see *Migrating from PCoIP Management Console 1* on page 44.

Package Contents

The PCoIP Management Console package zip file contains the following files:

File Name	Description
readme.htm	File describing the contents of the zip file.
TER1509005_Issue_3-Teradici_End_User_License_Agreement	Teradici PCoIP Management Console End User License Agreement (EULA).
mc_va-3.*x*.*x*.ova	Teradici PCoIP Management Console OVA file for the virtual machine that hosts the PCoIP Management Console.

What's New

PCoIP Management Console release 3.0 offers new features additions, performance improvements and user interface changes over past releases and are described in this section.

Info: Information on previous version releases
For features and release details associated with previous releases of the PCoIP Management Console, consult the Teradici PCoIP Management Console Life Cycle Table (KB 15134-2838).

Feature Additions or Changes

Introducing PCoIP Management Console Free

PCoIP Management Console now has a Free offering. Standard is no longer available as of release 3.0 and higher.

Management Console Free supports up to 100 endpoints and basic configuration of those devices. Advanced features are now exclusive to PCoIP Management Console Enterprise. See *Comparison of PCoIP Management Console Enterprise and PCoIP Management Console Free* on page 11

Amazon WorkSpaces Session Type

For Tera2 Zero Clients on firmware version 6.0, PCoIP Management Console can now configure the Amazon WorkSpaces session type from within the profile settings. This session type enables Tera2 Zero Clients to connect directly to Amazon WorkSpaces without the use of the PCoIP Connection Manager for Amazon WorkSpaces. Amazon Web Services will instruct the zero client to present which authentication fields are required to log into Amazon WorkSpaces.

Remote Endpoint Management (Enterprise only)

Administrators can control and manage PCoIP Zero Clients for at-home workers in the same way they do for those in the office, without the expense of a VPN. Zero clients can be remotely placed and will receive profile updates and firmware updates provided the latency to the zero client is within 100ms. See *PCoIP Management Console Remote Endpoint Management (Enterprise)* on page 102.

Offline License Activation (Enterprise only)

Enabling licenses for Enterprise capabilities can now be done in highly secured environments that do not permit access to the Internet. In order to do so, Offline activation license SKUs must be purchased instead of the standard Desktop Access SKUs. Activation occurs in the command line of the operating system. See *Activating Your PCoIP Management Console License from a Location Without Internet Access* on page 30.

Unified Communications Options Removed

As of firmware 6.0, CounterPath's Unified Communication (UC) is no longer available in zero client firmware. As such, the ability to configure UC or enhanced logging for

UC has been removed from the Management Console.

System Network Configuration tool has been replaced with NetworkManager TUI

As of CentOS 7, the System Network Configuration tool has been replaced with NetworkManager textual user interface (nmtui). NetworkManager TUI is now the default tool for configuring IPv4 static addresses. See *Changing the Default Network Configuration* on page 153.

Added endpoint serial number to the Endpoint page

The serial number of the endpoint is now an available property for the endpoints table. It can also be exported into the Inventory Report, enabling administrators to better track their endpoint inventory

Updated Profile assignment in the endpoints table

Profile assignments are now listed in the same row as an endpoint in the endpoint table. Previously profile assignments were only listed when the row represented a group. This facilitates a quicker identification of an endpoint, and the associated profile.

Session Timeout setting

The session timeout is now configurable from a tab in the security settings page for PCoIP Management Console Enterprise. This enables administrators to configure how long a user’s session in the PCoIP Management Console can be idle for before it logs the user out. See *Configuring PCoIP Management Console Session Timeout (Enterprise)* on page 150.

Sudo console commands require password

To improve the security of the virtual appliance, the Linux console admin account password is now required when enacting any elevated privilege commands using sudo.

Manual request Get All Settings for arbitrary sets of Endpoints

The Endpoint page's ENDPOINTS -> GET ALL SETTINGS menu option now supports arbitrary sets of devices.

Improved IP Address sorting

Columns in tables that contain IP Addresses are now sorted based on the numerical value of each octet of the IP address as opposed to being sorted as if they were a string. Now 1.1.1.10 would be considered greater than 1.1.1.2. Previously it was the reverse.

Zero Client session status information updated dynamically on session state change

The PCoIP Management Console now updates the zero client's PCoIP session status when it changes, based on an alert sent by the endpoint every time its session has been changed, rather than waiting for the next periodic 'get all settings' event.

Upgraded to CentOS 7

Upgraded installation OS to CentOS 7.4.1708 64-bit.

Improved search now supports sub groups

When moving groups, the search field will now use the entered text to search within group names of any group in the hierarchy. This enables search based on the name of a parent or intermediary group in order to find the desired child group.

Hide Sub Group can be checked if only the group that matches the search text is desired.

System Requirements

The PCoIP Management Console is intended for deployment within a secured corporate network for the management of PCoIP zero clients 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.

Deployment

PCoIP Management Console is released in Open Virtual Appliance (OVA) format. The supported hypervisor platforms are VMware ESXi 5.5 and 6.0.

System Configuration

PCoIP Management Console features the following system configuration:

- CPU: 4 CPUs
- RAM: 12 GB
- Disk: 62 GB
- Installation OS: CentOS 7.3, 64-bit

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 *Activating Licenses* on page 27.

Port Numbers

The PCoIP Management Console uses the following ports:

- **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.

IP Address Configuration

The PCoIP Management Console supports IPv4 and can join any network that is using DHCP. The PCoIP Management Console also supports static IP addressing. Teradici 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* on page 155

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
- Internet Explorer
- Chrome
- Microsoft Edge

PCoIP Endpoint Firmware

Teradici recommends using the latest version of firmware for Tera2 PCoIP Zero Clients. For the latest information on current and supported versions, see the Teradici PCoIP Management Console support page.

Note:PCoIP Management Console requires Tera2 PCoIP Zero Clients have firmware release 5.0 or later installed

Tera2 PCoIP Zero Clients managed by PCoIP Management Console release 2 or later, require endpoints to have firmware release 5.0 or later installed. If you have endpoints running previous firmware versions, please use PCoIP Management Console 1.10.3 to 1.10.8 or each endpoint’s Administrative Web Interface (AWI) to upgrade to the latest 5.x firmware. For instructions, see *Upgrading Endpoints to Firmware 5.0 or Later* on page 56.

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.

Note: Migrating, upgrading, or downgrading from other versions
If you are migrating to a new PCoIP Management Console version from PCoIP Management Console 1, see *Migrating from PCoIP Management Console 1*. If you are upgrading from PCoIP Management Console 2 to a newer version, see *Upgrading PCoIP Management Console 2 to a New Version*. If you need to downgrade endpoints from firmware 5.0 or later to 4.8, see *Downgrading Endpoints to Firmware 4.x* on page 58.

Installing PCoIP Management Console

Once you have PCoIP Management Console, deploy it as an Open Virtual Appliance (OVA) using vSphere Client.

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 *Activating Licenses* on page 27.

Note: Ensure different IP addresses when running parallel versions
If you are running PCoIP Management Console 1 in parallel with PCoIP Management Console releases 2.x and newer, ensure the two versions of the PCoIP Management Console have different IP addresses.

Getting Started

Getting Started

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, *Changing the Default Network Configuration* on page 153 for instructions prior to continuing.

Log in to the PCoIP Management Console Web User Interface

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* on page 29.
- 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

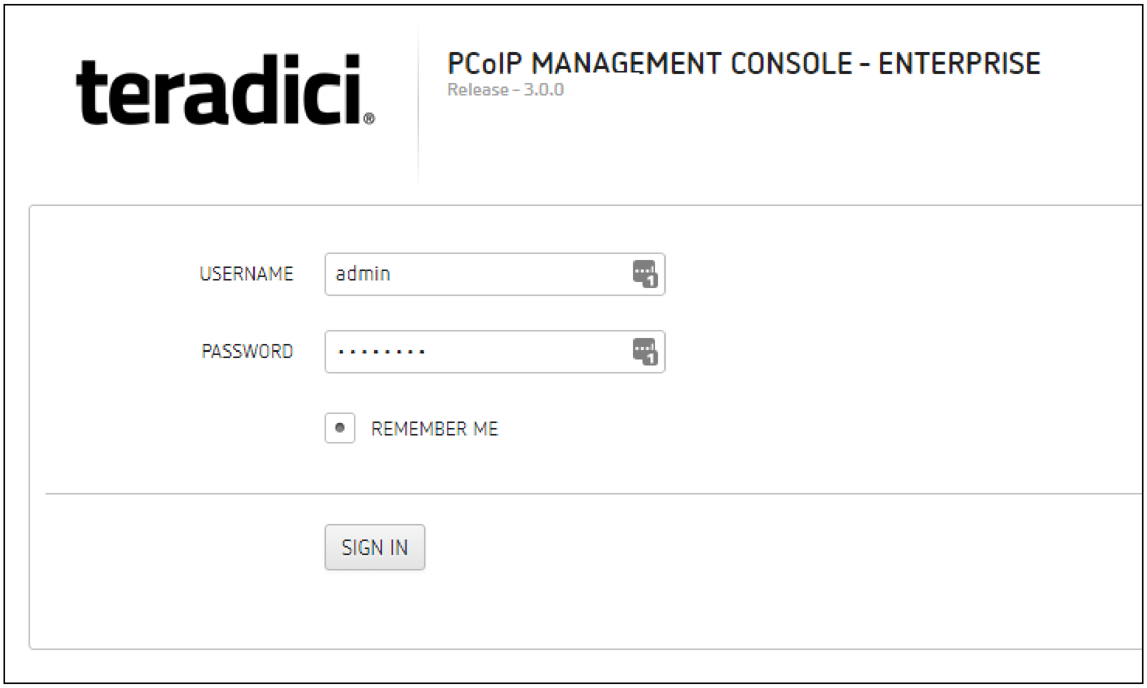
Note: The Web UI admin account for PCoIP Management Console is different from the virtual machine admin account

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* on page 18.
2. At the PCoIP Management Console login screen, enter the web interface credentials.

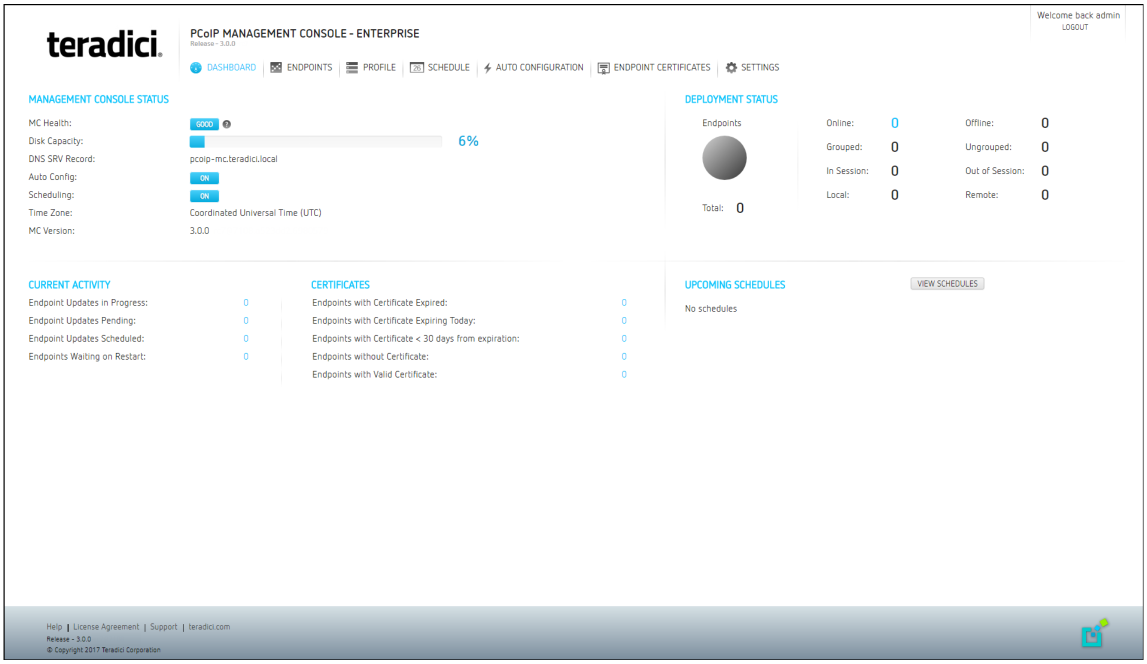
USERNAME **admin**
PASSWORD **password**



Note: Changing default settings and activating licenses
In order to change the PCoIP Management Console's default settings and run various scripts such as licensing 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* on page 38

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

Note: Example shows 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.



MANAGEMENT CONSOLE STATUS

MC Health:	GOOD
Disk Capacity:	6%
DNS SRV Record:	pcoip-mc.teradici.local
Auto Config:	ON
Scheduling:	ON
Time Zone:	Coordinated Universal Time (UTC)
MC Version:	3.0.0

DEPLOYMENT STATUS

Endpoints

Total: 0

Online:	0	Offline:	0
Grouped:	0	Ungrouped:	0
In Session:	0	Out of Session:	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

CERTIFICATES

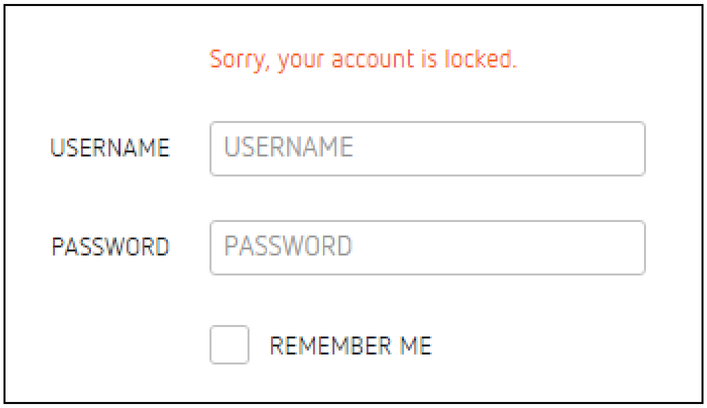
Endpoints with Certificate Expired:	0
Endpoints with Certificate Expiring Today:	0
Endpoints with Certificate < 30 days from expiration:	0
Endpoints without Certificate:	0
Endpoints with Valid Certificate:	0

UPCOMING SCHEDULES

No schedules

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 10 times within a 10-minute period, that user account will be locked out for 10 minutes. If this occurs, the login screen will display the message shown next.



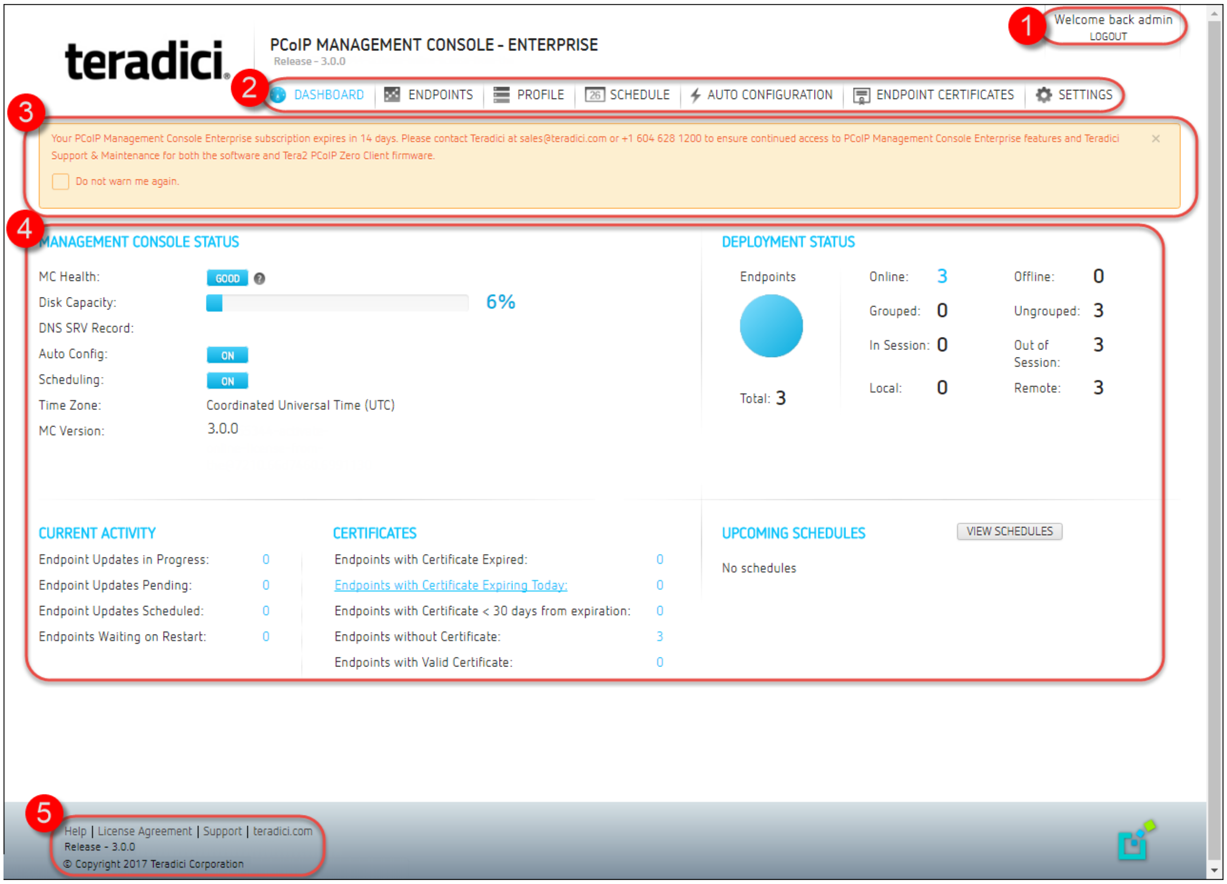
Sorry, your account is locked.

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.



Your PCoIP Management Console Enterprise subscription expires in 14 days. Please contact Teradici at sales@teradici.com or +1 604 628 1200 to ensure continued access to PCoIP Management Console Enterprise features and Teradici Support & Maintenance for both the software and Tera2 PCoIP Zero Client firmware.

□ Do not warn me again.

MANAGEMENT CONSOLE STATUS

MC Health:	GOOD
Disk Capacity:	6%
DNS SRV Record:	
Auto Config:	ON
Scheduling:	ON
Time Zone:	Coordinated Universal Time (UTC)
MC Version:	3.0.0

DEPLOYMENT STATUS

Endpoints

Total: 3

Online:	3	Offline:	0
Grouped:	0	Ungrouped:	3
In Session:	0	Out of Session:	3
Local:	0	Remote:	3

CURRENT ACTIVITY

Endpoint Updates in Progress:	0
Endpoint Updates Pending:	0
Endpoint Updates Scheduled:	0
Endpoints Waiting on Restart:	0

CERTIFICATES

Endpoints with Certificate Expired:	0
Endpoints with Certificate Expiring Today:	0
Endpoints with Certificate < 30 days from expiration:	0
Endpoints without Certificate:	3
Endpoints with Valid Certificate:	0

UPCOMING SCHEDULES

No schedules

Help | License Agreement | Support | teradici.com
Release - 3.0.0
© Copyright 2017 Teradici Corporation

PCoIP Management Console Dashboard Description

Area	Dashboard	Description
1	Welcome message	Displays the PCoIP Management Console user account for the logged in user.
	LOGOUT	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 pages.
	PROFILE	Navigates to the **PROFILE** page. From this page you can create, edit, duplicate, and delete profiles. The **PROFILE** link occurs at the top of all PCoIP Management Console pages.
	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.

Area	Dashboard	Description
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.

Area	Dashboard	Description
4	MANAGEMENT CONSOLE STATUS	Shows the PCoIP Management Console's status and contains information about how the PCoIP Management Console is configured: • **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, and scheduled, and the number of endpoints waiting to restart.
	UPCOMING SCHEDULES	Displays information about upcoming schedules, including the date and time they will apply.
	CERTIFICATES	Identifies the number of endpoints with: • 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.

Area	Dashboard	Description
5	Footnote Information	The following links occur at the bottom of every PCoIP Management Console page: • **Help**: Opens the PCoIP Management Console support page where you can find information about the PCoIP Management Console. • **License Agreement**: Opens the Teradici 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.

Activating Licenses

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 http://connect.teradici.com/mc-trial to request a free PCoIP Management Console Enterprise trial license. For more information on license options and packaging, see http://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.

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

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

Important: Deactivate expired licenses for PCoIP Management Console Free

If licenses expire and the you wish to use PCoIP Management Console Free, then all licenses must be deactivated.

- 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 Teradici support at Teradici Support Center.
- Only one license can be activated on one PCoIP Management Console Enterprise at one 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 Teradici Support and Maintenance.

For more information on Teradici support and maintenance, see http://www.teradici.com/products-and-services/global-support-services/pcoip-product-support-maintenance.

License Scripts

Teradici 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 Virtual Machine Console* on page 38.

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 and port number of your proxy server.

Activating Your PCoIP Management Console License

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 Virtual Machine Console* on page 38.
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
   ```

Activating Your PCoIP Management Console License from behind a Proxy Server

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.

To activate your PCoIP Management Console Enterprise license when the PCoIP Management Console is located behind a proxy server:

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
     ```

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

Important: Offline activation requirement
In order to activate your PCoIP Management Console from a location without internet access, you require offline licenses that are purchased via a specific SKU. Contact your reseller or Teradici sales for more information.

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 darksite), 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.

Requesting Offline Activation

Go to the support site https://techsupport.teradici.com 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 Teradici 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. See: *Temporarily Enabling SSH Access* on page 39
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=/opt/teradici/licensing
```

7. Process offline_activation.asr with appactutil.

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

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

8. Copy the *Activation short code* returned by the last command 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* on page 39
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 appactuti.

```
[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

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 dashboard, navigate to SETTINGS > LICENSE. This method does not display the fulfillment ID.

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 Virtual Machine Console* on page 38.
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: 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

To deactivate your 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*.

Deactivating Your PCoIP Management Console License from behind a Proxy Server

Deactivating 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.

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 Virtual Machine Console* on page 38.
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
  ```

Note: Finding fulfillment ID

To find your fulfillment ID, see *Viewing Installed Licenses*.

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* on page 39
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 Fullfillment 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 Teradici.

10. Teradici will return a response file where you must finish the deactivation by following the *Completing the Offline Activation* on page 32

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 Tera2 PCoIP Zero Clients, 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.

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. For security reasons, the SSH server on the PCoIP Management Console virtual machine CentOS operating system is disabled, therefore the VMware vSphere Client will be required to access the virtual machine console. 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.

Logging in to the PCoIP Management Console 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 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
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 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 virtual machine console from your vSphere Client. See *Accessing the PCoIP Management Console Virtual Machine Console* on page 38.
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 *Accessing the PCoIP Management Console Virtual Machine Console* on page 38.
2. Run the following command at the command line:
   ```
   sudo /sbin/service sshd stop
   ```

Note: Permanent SSH configuration will activate after rebooting

Permanently Enabling SSH Access

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

1. Log in as **admin** to the PCoIP Management Console virtual machine console from your vSphere Client. See *Accessing the PCoIP Management Console Virtual Machine Console* on page 38.
2. Run the following command at the command line:
   sudo chkconfig sshd on
3. Reboot the PCoIP Management Console virtual machine from your vSphere Client:
   a. Right-click the PCoIP Management Console virtual machine in the *Inventory* list.
   b. Select **Power > Restart Guest**.

Permanently Disabling SSH Access

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

1. Log in as **admin** to the PCoIP Management Console virtual machine console from your vSphere Client. See *Accessing the PCoIP Management Console Virtual Machine Console* on page 38.
2. Run the following command at the command line:
   sudo chkconfig sshd off
3. Reboot the PCoIP Management Console virtual machine from your vSphere Client:
   a. Right-click the PCoIP Management Console virtual machine in the Inventory list.
   b. Select **Power > Restart Guest**.

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:
   user name: **admin**
   password: **ManagementConsole2015** (default) or the password you have

assigned to the **admin** user. See *Changing the PCoIP Management Console Virtual Machine Default User Password* on page 41.

5. When you are finished using the console, type **exit** to log out and exit the application.
6. If desired, disable SSH again for the **admin** user. See *Enabling/Disabling SSH Access* on page 39.

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:
passwd: password updated successfully.
```

4. Store your password in a secure location.

Changing the PCoIP Management Console Web Interface Default Password

Important: Change default password and disable *admin* user
The **admin** user name cannot be changed, but for security reasons it is critical to change the default password when you first log in. Teradici also recommends that you disable the **admin** user and create a different administrative user with a new name and password (Enterprise only). See *Displaying User Information* on page 131.

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 that produce undesirable results.

The PCoIP Management Console web user account has the following default user name and password when it is first deployed:

- User name: **admin**
- Default password: **password**

To change the *admin* account password:

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

Re-enabling the PCoIP Management Console's Web 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. Open the PCoIP Management Console console from vSphere Client. See *Logging in to the PCoIP Management Console Virtual Machine Console* on page 38.
2. Log in using the PCoIP Management Console console **admin** user name and password.
3. Change to the **teradici** directory:
   ```
   cd /opt/teradici
   ```
4. Type the following command to run the script:
   ```
   ./enable_admin.sh
   ```

Reverting the PCoIP Management Console’s Web 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 Virtual Machine Console* on page 38.
2. Log in using the PCoIP Management Console console **admin** user name and password.
3. Change to the **teradici** directory:
   `cd /opt/teradici`
4. Type the following command to run the script:
   `./reset_admin_password.sh`

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.

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.
```

Migrating PCoIP Management Console

This section provides details of how to migrate PCoIP Management Console to another version of the software.

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 newer. This section only applies to Tera2 PCoIP Zero Clients.

Step 1: Install and configure PCoIP Management Console release 2.0 or newer

To install and configure PCoIP Management Console release 2.0 or newer:

1. Install PCoIP Management Console 2.0 or newer on your ESXi host.
2. Log in to the PCoIP Management Console virtual machine console.
3. Change the PCoIP Management Console virtual machine default user password.
4. Set the PCoIP Management Console network properties.
5. Activate your PCoIP Management Console Enterprise license (optional).
6. If you are using an auto discovery method, update your DHCP or DNS server with the new PCoIP Management Console information:
   - PCoIP Management Console DHCP options (for DHCP discovery)
   - PCoIP Management Console DNS SRV records (for DNS discovery)
   - PCoIP Management Console DNS TXT records (for DNS discovery)
7. Log in to the PCoIP Management Console web UI.
8. Change the PCoIP Management Console web UI admin user password.
   Teradici 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 5.0 or later firmware file for your endpoints.
   At least one 5.0 or later firmware image must be uploaded to PCoIP Management Console before a profile can be created. When profiles are migrated from PCoIP Management Console 1, they will be assigned the highest firmware version that is present on the newly installed PCoIP Management Console.

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

To import profiles, create and assign profiles to groups:

1. Log in to your PCoIP Management Console 1 web UI and make a note of the names of the profiles you want to import.
   Note that profile names are case- and white space sensitive.
2. Ensure that you can connect to your PCoIP Management Console 1 SSH server from your PCoIP Management Console 2.0 or newer virtual machine. To test:
   a. From the PCoIP Management Console 2 virtual machine command line, type **ssh teradici@<*MC 1 IP address*>**.
   b. Enter your PCoIP Management Console 1 virtual machine password.
   c. Type **exit** to close the session and return to PCoIP Management Console 2.
3. Import profiles into your PCoIP Management Console release 2.0 or newer.
4. From the PCoIP Management Console release 2.0 or newer web UI, refresh the **PROFILE page** and check that your profiles have been moved over.

   Note: Importing process creates tab for zero clients
   The profile import process will create a tab for both Tera2 Dual and Quad Zero Clients . If you are only migrating one type of zero client, 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 zero clients and you set properties in the **QUAD** tab, the profile will not be applied.

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 *Appendix B: PCoIP Management Console 1 Profile Properties Renamed or Not Migrated* on page 168.

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.

Step 3: Migrate each group of PCoIP Management Console 1 endpoints to PCoIP Management Console release 2.0 or newer

If you have a large deployment, Teradici 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 Tera2 PCoIP Client endpoints to firmware 5.0 or later.
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.

Importing Profiles from PCoIP Management Console 1

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

Before You Import Your Profiles

Before beginning, ensure the following prerequisites are in place:

- For Tera2 PCoIP Zero Clients, you have uploaded at least one firmware 5.0 or later firmware image to PCoIP Management Console. Migrated profiles will be assigned the latest firmware version that is present on PCoIP Management Console.
- 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).
  Note that inPCoIP 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:
  - From your PCoIP Management Console VM console, type **ssh teradici@<*PCoIP Management Console 1 IP address or domain name*>**.
  - Enter your PCoIP Management Console 1 VM password.
  - Type **exit** to close the session and return to your PCoIP Management Console.

Importing Individual PCoIP Management Console 1 Profiles

To import profiles to PCoIP Management Console release 2 or newer, 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').
   Important: In PCoIP Management Console 1, profile names are case and white space sensitive.
4. Load (or reload) the newPCoIP Management Console *PROFILE* page to see the migrated profiles. See *Managing Profiles* on page 82.

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.

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.

For 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

Note: 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* on page 82.

Profile Properties Renamed in PCoIP Management Console or Not Migrated

The list of PCoIP Management Console 1 profile properties that have been renamed in PCoIP Management Console, or are not migrated when you import a PCoIP Management Console 1 profile to PCoIP Management Console, is in *Appendix B*.

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 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 5.0 or later.

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 for Auto Discovery Using DHCP* on page 68 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.

PCoIP Management Console release 2.0 or newer and PCoIP Management Console 1 Interoperability

Category	Interoperability
Endpoint firmware	• **PCoIP Management Console release 2.0 or newer**: For Tera2 PCoIP Zero Clients, zero clients must run firmware 5.0 or later. PCoIP Management Console cannot discover and manage endpoints running previous versions of the firmware. • **PCoIP Management Console 1**: Zero clients must run a 4.x firmware version. PCoIP Management Console 1 cannot discover and manage devices running firmware 5.0 or later.
DHCP/DNS discovery	Newer releases of PCoIP Management Console use a different format for DHCP options and DNS SRV records from PCoIP Management Console 1. **Related Information: DHCP and DNS discovery** For information on DHCP and DNS discovery for PCoIP Management Console 1, see the *PCoIP Management Console 1.x User Manual*.
Management	• **PCoIP Management Console release 2.0 or newer**: Zero clients are managed by at most one PCoIP Management Console. • **PCoIP Management Console 1**: Zero clients can be managed by more than one PCoIP Management Console 1 simultaneously.
Database	The PCoIP Management Console 1 database cannot be imported into the newer versions of PCoIP Management Console and vice versa. However, you can import PCoIP Management Console 1.10.x profiles into PCoIP Management Console.
Communication	Newer releases of PCoIP Management Console and PCoIP Management Console 1 do not communicate with each other.

Migrating PCoIP Management Console to a Newer Release

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 newer release. This enables a seamless transition to the new PCoIP Management Console 3 and eliminates unnecessary PCoIP endpoint configuration as each endpoint is configured to report to the existing PCoIP Management Console 3 IP address.

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

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* on page 38.
   - PCoIP Management Console 2.x users go to step 2.
   - PCoIP Management Console 3.x users 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* on page 1.
   e. Select **Ok**.
   f. In the next screen, select **Cancel**.
   g. In the next screen, select **Quit**. Teradici does not recommend changing the PCoIP Management Console 2 DNS configuration.

3. PCoIP Management Console 3 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 `Enter`.
   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* on page 155
   e. Select **<OK>** or **<Cancel>** and press `Enter`.
   f. Select **<Back>** to return to the main screen.
   Teradici 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 (applies to custom PCoIP Management Console certificates only):

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

Skip this step if you are using the default Teradici self-signed PCoIP Management Console certificate.

- If you plan to use your custom PCoIP Management Console certificate after upgrading, Teradici 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* on page 136.
- 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 Profiles* on page 82.

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.

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.
6. If you are using PCoIP Management Console Enterprise, record the following licensing information by running the `/opt/teradici/licensing/mc_view_lic.sh` script:
   - Fulfillment ID
   - Entitlement ID (activation code)
7. If you are using PCoIP Management Console Enterprise, from it's console, deactivate the PCoIP Management Console Enterprise license by running one of the following commands:

```
/opt/teradici/licensing/mc_return_lic.sh -f <fulfillment_ID>
```

   If behind a proxy:

```
/opt/teradici/licensing/mc_return_lic.sh -f <fulfillmentId> -p
[<user:password>@] <proxyhost:port>
```

8. From vSphere Client, shut down the PCoIP Management Console virtual appliance.
9. Follow the instructions in deploying PCoIP Management Console to deploy the new PCoIP Management Console release. See *Installing PCoIP Management Console* on page 18
10. Connect to your PCoIP Management Console virtual machine console. See *Logging in to the PCoIP Management Console Virtual Machine Console* on page 38.

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* on page 38.
12. Modify the upgraded PCoIP Management Console to use the same network settings as the previous PCoIP Management Console release. See *Changing the Default Network Configuration* on page 153.

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* on page 155 for instructions.

13. From vSphere Client, restart the PCoIP Management Console and ensure it has the correct addressing information.
14. If you are using PCoIP Management Console Enterprise, activate it's license by running one of the following commands:

```
/opt/teradici/licensing/mc_activate_lic.sh -k <entitlementID>
```

From behind a proxy:

```
/opt/teradici/licensing/mc_activate_lic.sh -k <entitlementID> -p
[<user:password>@ <proxyhost:port>
```

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* on page 136.

Note: Skip this step if using the default Teradici signed certificate
If you are using the default Teradici 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* on page 160.

    ⚠ **Important: 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 Teradici 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's Web User Password* on page 43.

18. Log in again using your standard user account.
19. Check the *MC Health* field on the DASHBOARD page to ensure the PCoIP Management Console status is **GOOD**. See *Understanding the PCoIP Management Console Dashboard* on page 23.
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* on page 81.

Managing Tera2 PCoIP Zero Client Firmware

This section provides an overview of how to upgrade or downgrade your version of the Tera2 PCoIP Zero Client firmware.

Upgrading Endpoints to Firmware 5.0 or Later

For Tera2 PCoIP Zero Clients, PCoIP Management Console cannot upgrade endpoints running firmware versions prior to 5.0.0. 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.

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.

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 newer home page, click **Update Firmware**.
3. Click the **Import Firmware** link to transfer the firmware 5.0 or later 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 5.0 or later 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 Teradici processor family used by the endpoint **Tera2**.
- **Version Number** represents the currently applied firmware on the endpoints you want to update (for example, **4.8.0**).
- **Group** lists any groups you have previously configured for endpoint management.

Tip: Upgrade firmware one group at a time
Teradici 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 newerPCoIP 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**.

For more information about the AWI, see *Tera2 PCoIP Zero Client Firmware 4.x and Remote Workstation Card Firmware 4.9 Administrators' Guide* (for endpoints prior to firmware version 5.0) or *Tera2 PCoIP Zero Client Firmware Administrators' Guide* (for Tera2 PCoIP Zero Clients running firmware version 5.0 or later).

Downgrading Endpoints to Firmware 4.x

This section applies only to Tera2 PCoIP Zero Clients.

From PCoIP Management Console release 2.0 and newer, you can apply a profile to a group of endpoints running firmware 5.0 or later to remotely downgrade their firmware to version 4.x. 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 zero client

For Tera2 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 firmware 4.8.x the second firmware upload will need to be completed using PCoIP Management Console 1. Alternatively, you can upload the firmware *twice* from the zero client AWI. For more details about recovery mode, please see *Tera2 PCoIP Zero Client Firmware Administrators' Guide* .

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* on page 88 to find out more.

Uploading the Firmware to the PCoIP Management Console

To upload the firmware to the PCoIP Management Console:

1. Using a browser, log in to the Teradici Support Center.
2. Select any of the **Zero Client Firmware** buttons from an All Access offering, and from the Previous Firmware section, select the download firmware button for PCoIP Management Console 1 users.
3. Download the firmware 4.8 zip file, and extract the package contents.
4. From PCoIP Management Console, click **SETTINGS > SOFTWARE** to display the SOFTWARE MANAGEMENT window.
5. Click **Add Software/Firmware**.
6. 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 Firmware 4.8.x Profile with a Group

To associate a Firmware 4.8.x 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 4.8.x firmware profile.
3. Click the **+** tab, select the **TERA2: CLIENT [DUAL] (5.0.0)** profile or the **TERA2: CLIENT [QUAD] (5.0.0)** profile, and click **ADD**.
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 endpoints will automatically restart and upload the 4.8.x firmware image. They will either no longer appear in the ENDPOINTS table or may appear as offline. The PCoIP Management Console will not be able to manage them. To synchronize the recovery image 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.Recurrence**
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 *Changing the Web Interface Time Zone* on page 81.

   - 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.

Note: Synchronize firmware image after applying profile
After the profile applies, the selected endpoints will automatically restart and upload the 4.8.x firmware image. They will either no longer appear in the ENDPOINTS table or may appear as offline. The PCoIP Management Console will not be able to manage them. To synchronize the recovery image 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*.

Discovering Endpoints

This section provides an overview of how to discover endpoints with PCoIP Management Console.

Discovery Process Overview

Before endpoints can be managed by the PCoIP Management Console, they must first be discovered. This topic provides an overview of the main steps of the PCoIP endpoint discovery process.

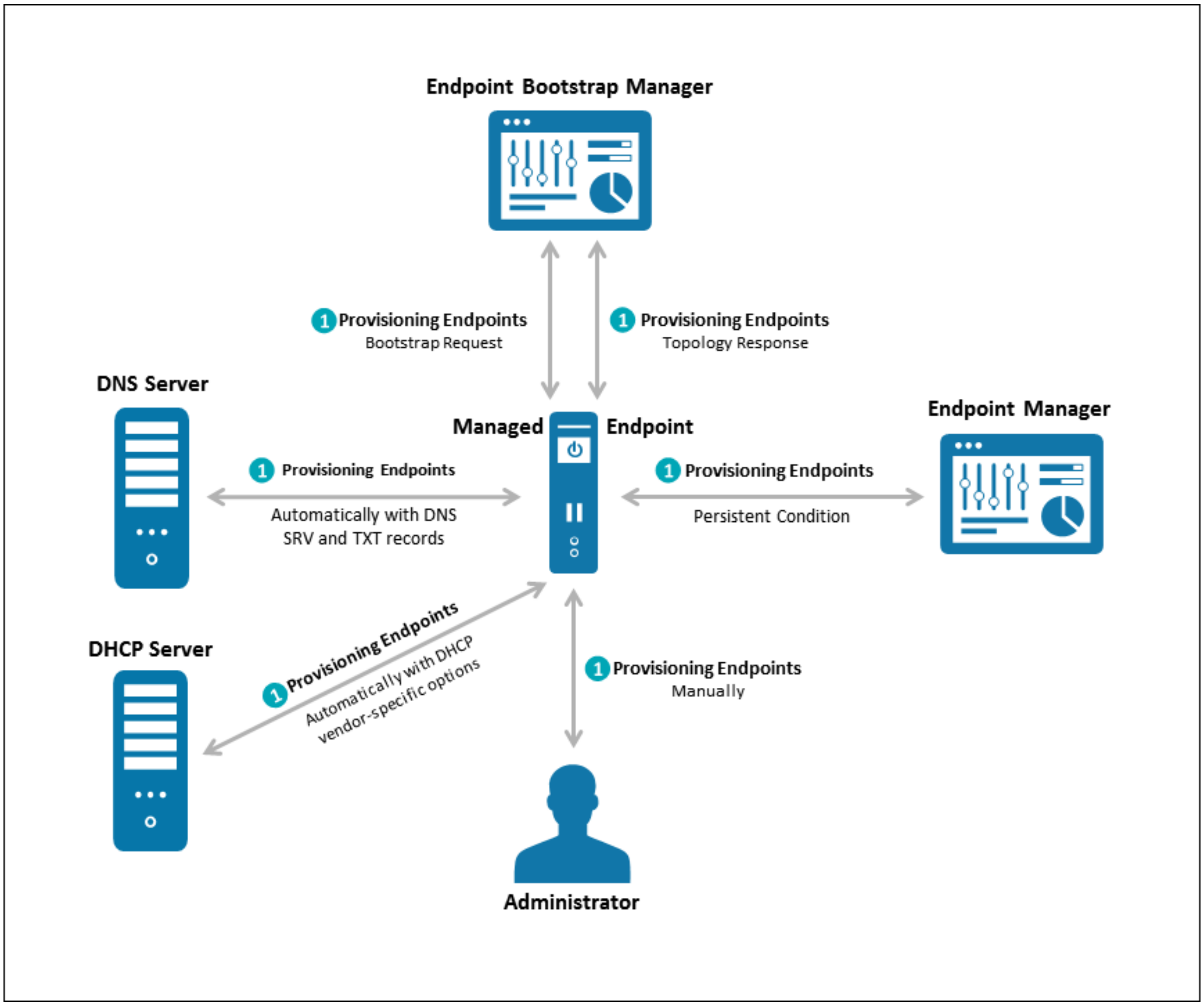
Important: Replace the default self-signed certificate with your own before configuring a discovery method and adding endpoints

Teradici strongly recommends 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* on page 136 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 or future releases 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 *Tera2 PCoIP Zero Client Firmware Administrators' Guide* for details. See also *Configuring an Endpoint Manager Manually from an Endpoint* on page 157 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, and 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.

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 or future releases of the PCoIP Management Console may separate these roles.

Discovery Methods

For automatic discovery, endpoints are populated with the IP address or FQDN of the Endpoint Bootstrap Manager to which they should connect via DHCP vendor-specific options or DNS service and text records. Optionally, endpoints can also be configured with the Endpoint Bootstrap Manager 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 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 Endpoint Bootstrap Manager/Endpoint Manager certificate.

Endpoints configured for medium or high security must have a trusted certificate in their certificate store before they can connect to an Endpoint Bootstrap Manager or Endpoint Manager. 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 Endpoint Bootstrap Manager certificate's fingerprint.
- They are discovered using the PCoIP Management Console's manual discovery method. See *Discovering Endpoints Manually from PCoIP Management Console* on page 115.

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

Discovery Method	Low Security	Medium Security	High Security
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* on page 115.

Endpoints can use DHCP or DNS auto discovery. 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 auto discovery.

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 for Auto Discovery Using DHCP* on page 68: Explains how to configure your DHCP server to provision endpoints with Endpoint Bootstrap Manager information.
- *Configuring Endpoints for Auto Discovery Using DNS* on page 74: Explains how to configure your DNS server to provision endpoints with Endpoint Bootstrap Manager information.
- *Configuring an Endpoint Manager Manually from an Endpoint* on page 157: Explains how to manually configure an Endpoint Manager for an endpoint in a high security environment.
- *Discovering Endpoints Manually from PCoIP Management Console* on page 115: Explains how to manually initiate discovery from the PCoIP Management Console. Endpoints must be configured for low security if you use this method.

Configuring Endpoints for Auto Discovery Using DHCP

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

When PCoIP Management Console 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. A zero client 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 PCoIP Management Console 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: Configure 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 two PCoIP Management Console PCoIP Endpoint DHCP options.

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* on page 70.

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:

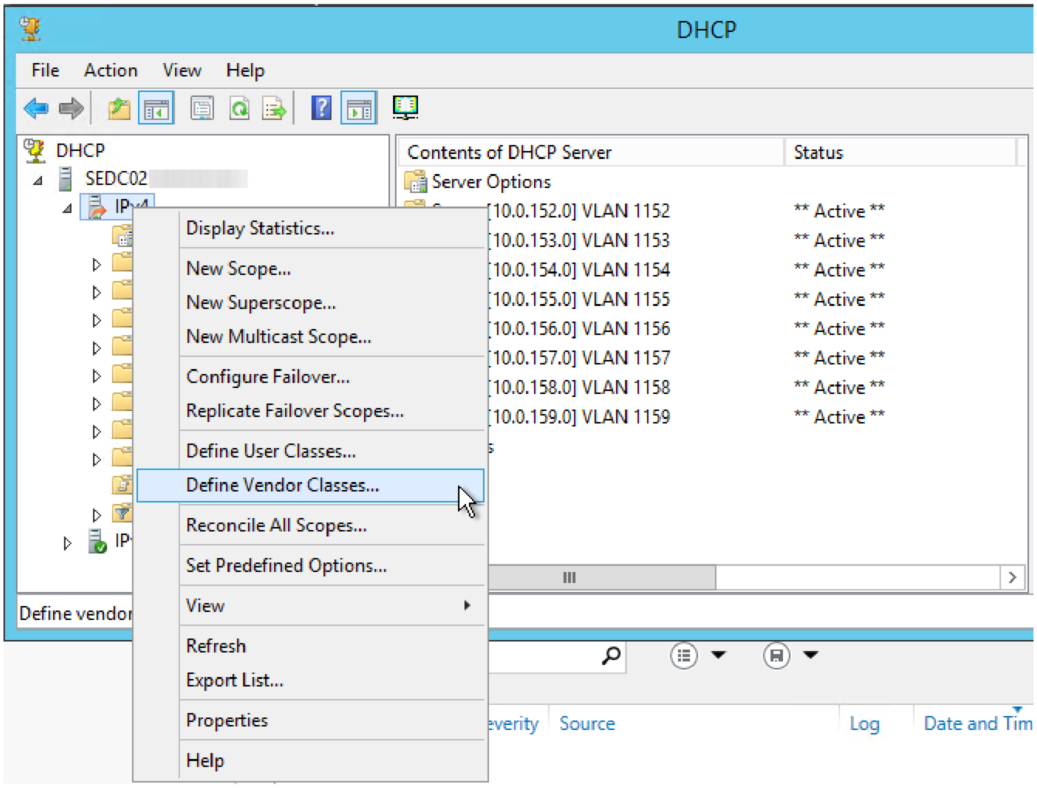
1. Use Mozilla Firefox to log in to the PCoIP Management Console 2 web interface.
2. Click the padlock icon in the browser's address bar.
3. Click **More Information**.
4. Click **View Certificate**.
5. In the **Fingerprints** section, copy and paste the SHA-256 fingerprint into a text editor.

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

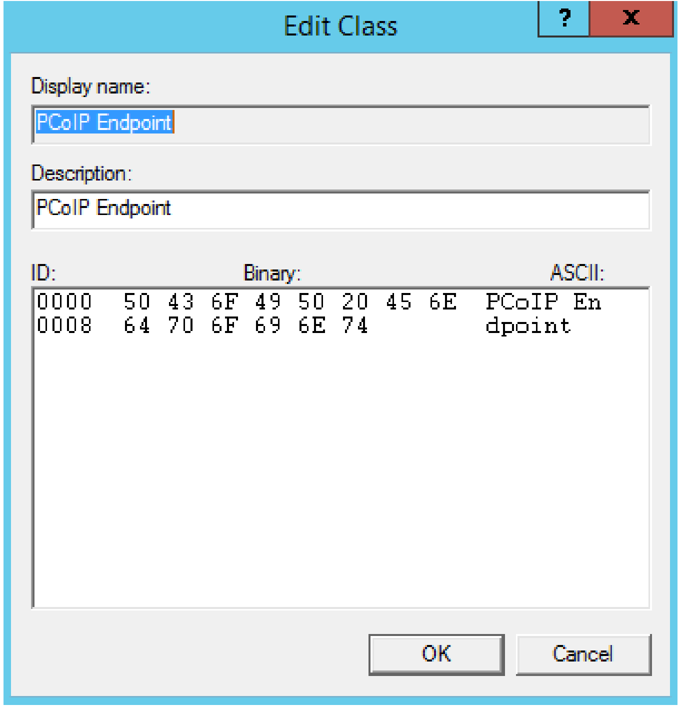
To add the PCoIP DHCP vendor class to your DHCP server:

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**.



Contents of DHCP Server	Status
Server Options	
[10.0.152.0] VLAN 1152	** Active **
[10.0.153.0] VLAN 1153	** Active **
[10.0.154.0] VLAN 1154	** Active **
[10.0.155.0] VLAN 1155	** Active **
[10.0.156.0] VLAN 1156	** Active **
[10.0.157.0] VLAN 1157	** Active **
[10.0.158.0] VLAN 1158	** Active **
[10.0.159.0] VLAN 1159	** Active **

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.



Display name:
PCoIP Endpoint

Description:
PCoIP Endpoint

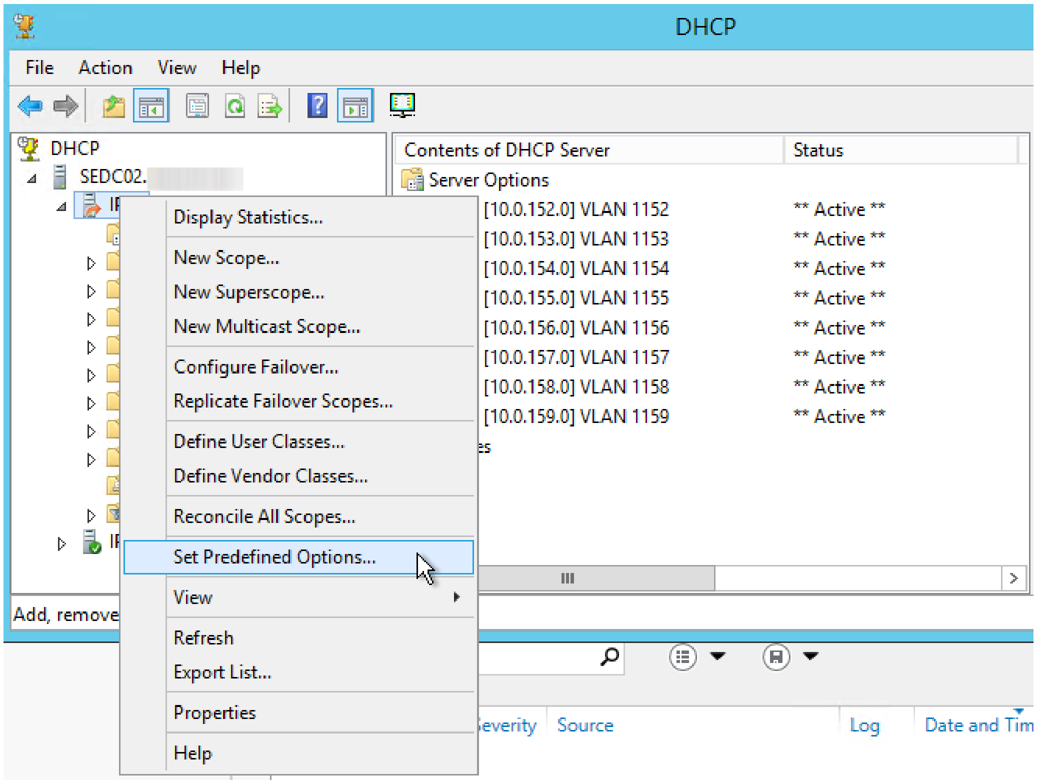
```
ID:              Binary:                     ASCII:
0000   50 43 6F 49 50 20 45 6E   PCoIP En
0008   64 70 6F 69 6E 74         dpoint
```

7. Click **OK** to save and close the dialog.

Configuring DHCP Options

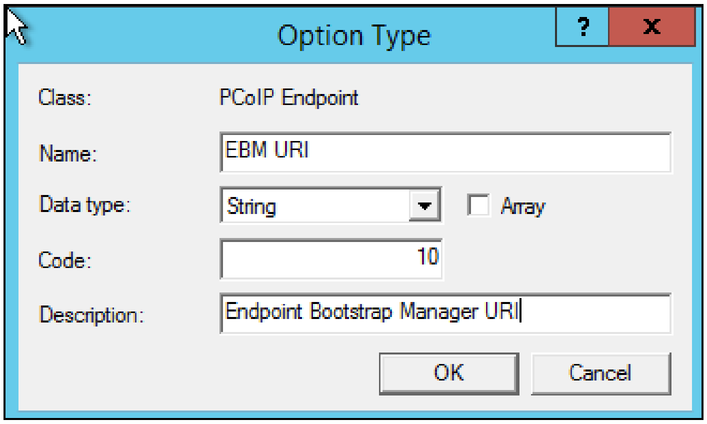
To add two PCoIP Management Console DHCP options and apply them to a scope:

1. Right-click on **IPv4** in the tree and select **Set Predefined Options**.



Contents of DHCP Server	Status
Server Options	
[10.0.152.0] VLAN 1152	** Active **
[10.0.153.0] VLAN 1153	** Active **
[10.0.154.0] VLAN 1154	** Active **
[10.0.155.0] VLAN 1155	** Active **
[10.0.156.0] VLAN 1156	** Active **
[10.0.157.0] VLAN 1157	** Active **
[10.0.158.0] VLAN 1158	** Active **
[10.0.159.0] VLAN 1159	** Active **

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**.



Class: PCoIP Endpoint

Name: EBM URI

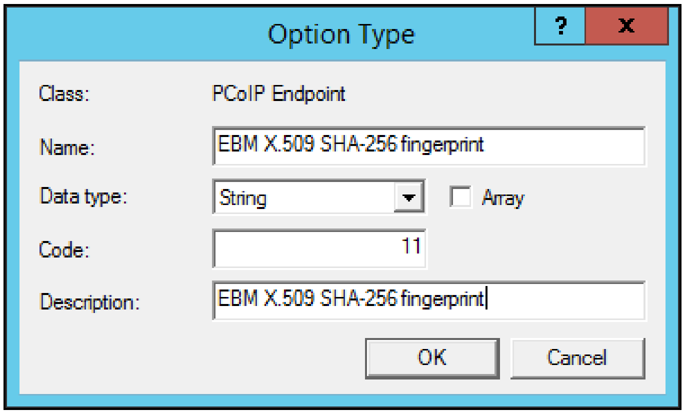
Data type: String ☐ Array

Code: 10

Description: Endpoint Bootstrap Manager URI

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**.



Class: PCoIP Endpoint

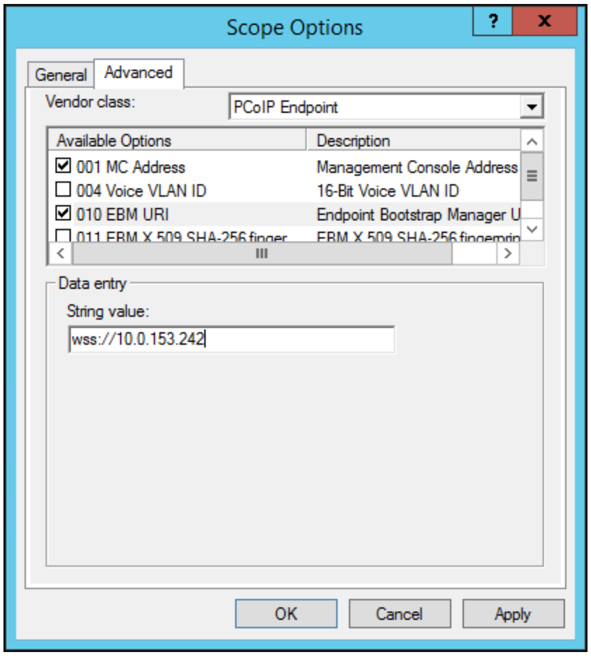
Name: EBM X.509 SHA-256 fingerprint

Data type: String ☐ Array

Code: 11

Description: EBM X.509 SHA-256 fingerprint

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://<MC IP address>:[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.



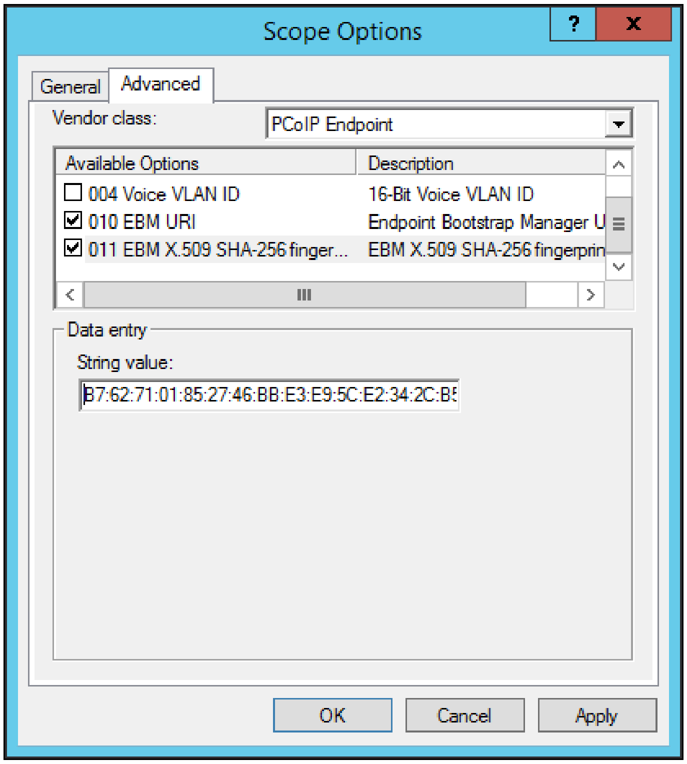
Vendor class: PCoIP Endpoint

Available Options	Description
☑ 001 MC Address	Management Console Address
☐ 004 Voice VLAN ID	16-Bit Voice VLAN ID
☑ 010 EBM URI	Endpoint Bootstrap Manager U
☐ 011 EBM X.509 SHA-256 finger	EBM X.509 SHA-256 fingerprin

Data entry

String value: wss://10.0.153.242

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.



Vendor class: PCoIP Endpoint

Available Options	Description
☐ 004 Voice VLAN ID	16-Bit Voice VLAN ID
☑ 010 EBM URI	Endpoint Bootstrap Manager U
☑ 011 EBM X.509 SHA-256 finger...	EBM X.509 SHA-256 fingerprin

String value: B7:62:71:01:85:27:46:BB:E3:E9:5C:E2:34:2C:B5

12. Click **OK** to save and close the dialog.

Configuring Endpoints for Auto Discovery Using DNS

This section explains how to configure your DNS server to provision endpoints with Endpoint Bootstrap Manager information, as part of the endpoint 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)** that 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)** that 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 the following example.
- **A DNS TXT record** that 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 2 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.

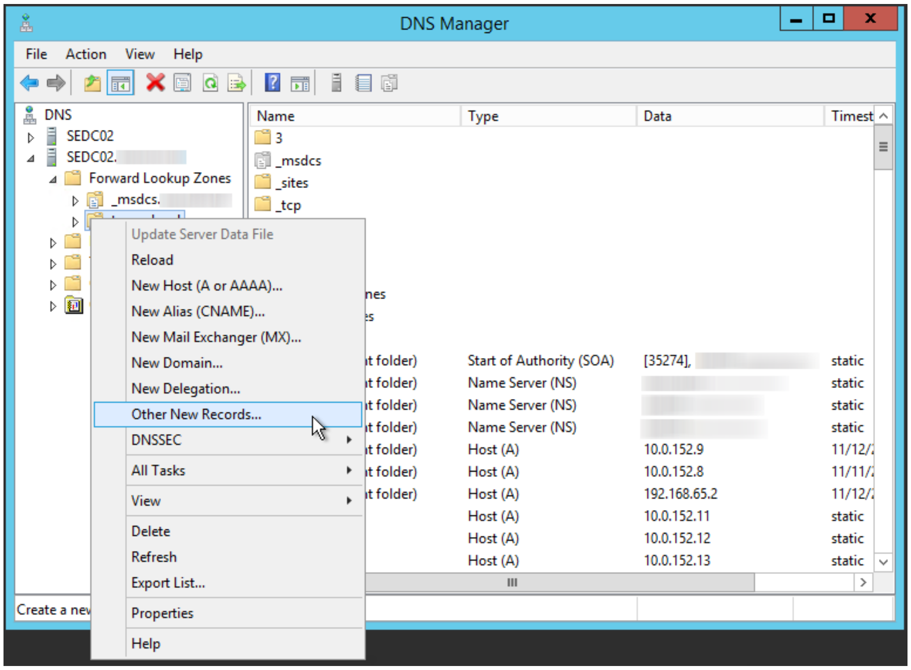
Note: Examples shown use Windows Server 2012 R2
The instructions provided may change slightly depending on your specific server version.

Adding the DNS SRV Record

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

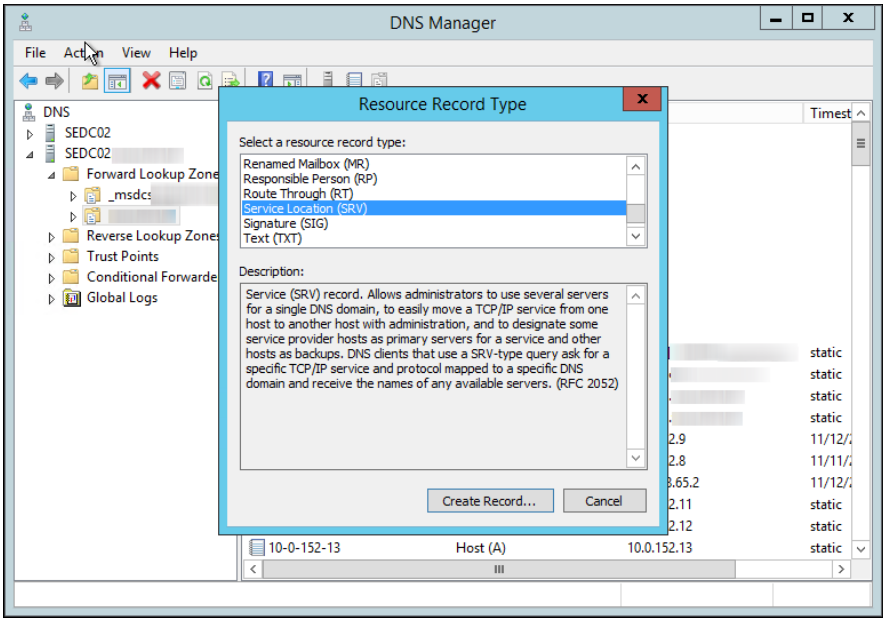
1. Log in to your Windows Server and select **DNS**.
2. Right-click on your DNS server in the SERVERS pane and select **DNS Manager** from the context menu.

3. In *Forward Lookup Zones*, right-click on your domain and select **Other New Records** from the context menu.



Name	Type	Data	Timest
3			
_msdcs			
_sites			
_tcp			
...nes			
...s			
...t folder)	Start of Authority (SOA)	[35274], [redacted]	static
...t folder)	Name Server (NS)	[redacted]	static
...t folder)	Name Server (NS)	[redacted]	static
...t folder)	Name Server (NS)	[redacted]	static
...t folder)	Host (A)	10.0.152.9	11/12/2
...t folder)	Host (A)	10.0.152.8	11/11/2
...t folder)	Host (A)	192.168.65.2	11/12/2
	Host (A)	10.0.152.11	static
	Host (A)	10.0.152.12	static
	Host (A)	10.0.152.13	static

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



Select a resource record type:

- Renamed Mailbox (MR)
- Responsible Person (RP)
- Route Through (RT)
- Service Location (SRV)
- Signature (SIG)
- Text (TXT)

Description:

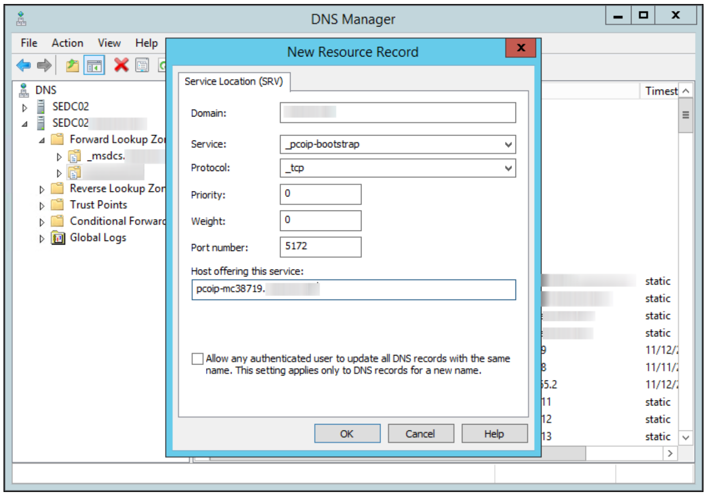
Service (SRV) record. Allows administrators to use several servers for a single DNS domain, to easily move a TCP/IP service from one host to another host with administration, and to designate some service provider hosts as primary servers for a service and other hosts as backups. DNS clients that use a SRV-type query ask for a specific TCP/IP service and protocol mapped to a specific DNS domain and receive the names of any available servers. (RFC 2052)

Name	Type	Data	Timest
		[redacted]	static
		[redacted]	static
		[redacted]	static
		[redacted]	static
		...2.9	11/12/2
		...2.8	11/11/2
		...3.65.2	11/12/2
		...2.11	static
		...2.12	static
10-0-152-13	Host (A)	10.0.152.13	static

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.



New Resource Record

Service Location (SRV)

Domain: [redacted]

Service: _pcoip-bootstrap

Protocol: _tcp

Priority: 0

Weight: 0

Port number: 5172

Host offering this service:
pcoip-mc38719.[redacted]

☐ Allow any authenticated user to update all DNS records with the same name. This setting applies only to DNS records for a new name.

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.

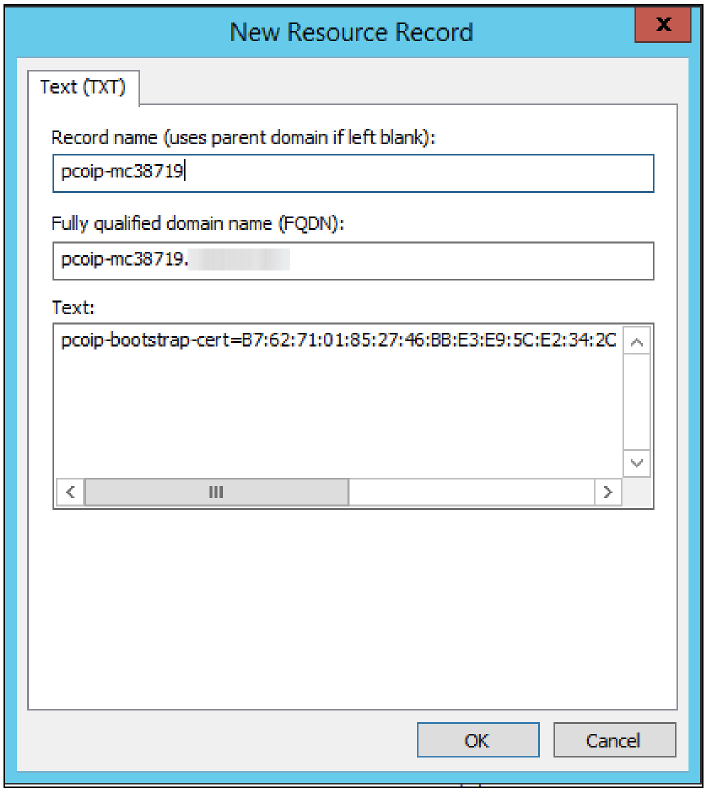
Adding a DNS TXT Record

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.



Record name (uses parent domain if left blank):
pcoip-mc38719

Fully qualified domain name (FQDN):
pcoip-mc38719.[redacted]

Text:
pcoip-bootstrap-cert=B7:62:71:01:85:27:46:BB:E3:E9:5C:E2:34:2C

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* on page 94 and *Auto Configuring Endpoints (Enterprise)* on page 91 for details.

See *Appendix A: Troubleshooting DNS* on page 165 to verify that your DNS server is configured correctly for the PCoIP Management Console.

Discovering Endpoints Manually

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. For complete instructions, see *Discovering Endpoints Manually from PCoIP Management Console* on page 115.

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.

Managing Endpoints

This section contains the following topics:

- *Understanding the PCoIP Management Console Dashboard* on page 23: Describes the information you can view from the PCoIP Management Console **DASHBOARD** page.
- *Changing the Web Interface Time Zone* on page 81: 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.
- *Using the Endpoints Page* on page 105: Lists all the actions you can perform from the **ENDPOINTS** page and provides links to instructions for each one.
- *Displaying Endpoint Properties* on page 107: Shows how to select the endpoint properties you wish to include in a **GROUPED** or **UNGROUPED** endpoint table.
- *Using the ENDPOINT DETAILS Page* on page 118: Lists all the actions you can perform from the **ENDPOINT DETAILS** page and provides instructions for each one.
- *Performing Power Management* on page 121: Explains how to power down and reset endpoints remotely.
- *Renaming Endpoints* on page 124: Explains how to rename an endpoint from the **ENDPOINTS** page.
- *Deleting Endpoints* on page 124: This topic explains how to delete endpoints.
- *Discovering Endpoints Manually* on page 80: Provides information about how to use the PCoIP Management Console’s manual endpoint discovery feature.
- *Searching an Endpoint Table* on page 125: Explains how to use a text search to locate endpoints in a **GROUPED** or **UNGROUPED** endpoint table.
- *Filtering the Endpoint List* on page 126: 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)* on page 96: 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.

Changing the Web Interface Time Zone

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 **USERS** 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**.

Note: Time zone selection/setting displays 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').

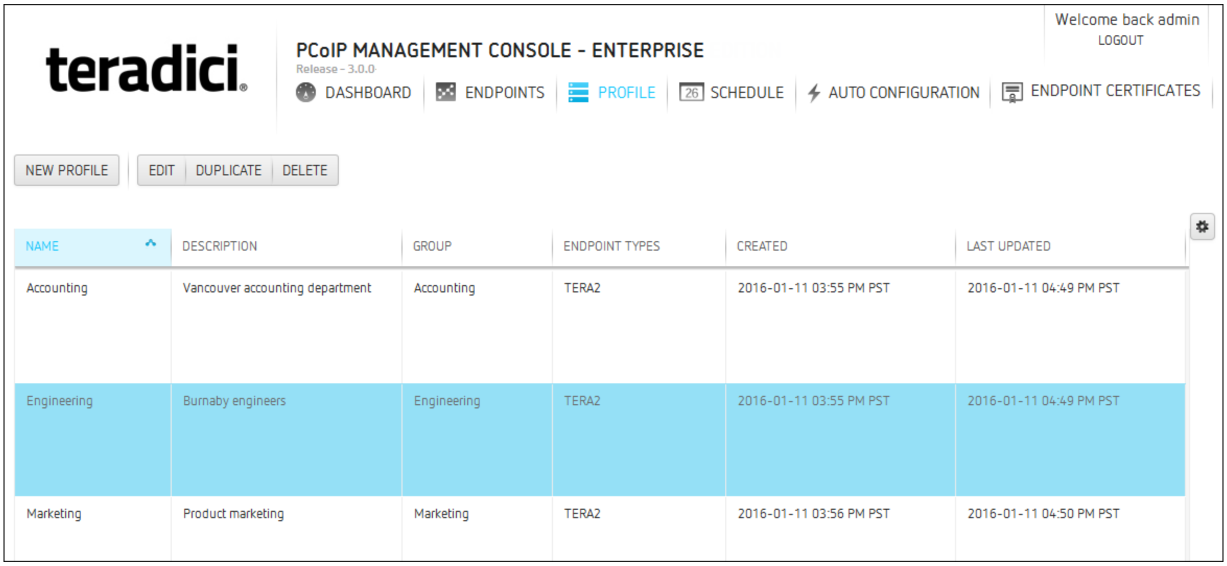
Managing Profiles

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.

See firmware version from **SETTINGS > SOFTWARE MANAGEMENT** page. When you add a profile, the firmware version that displays in the **PROFILE > ADD PROFILE** drop-down list may not directly correlate to the firmware version you associate with the profile. You will see the actual version number of the firmware file when you select it from the **SETTINGS > SOFTWARE MANAGEMENT** page.

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 MANAGEMENT** page before you can create a profile.

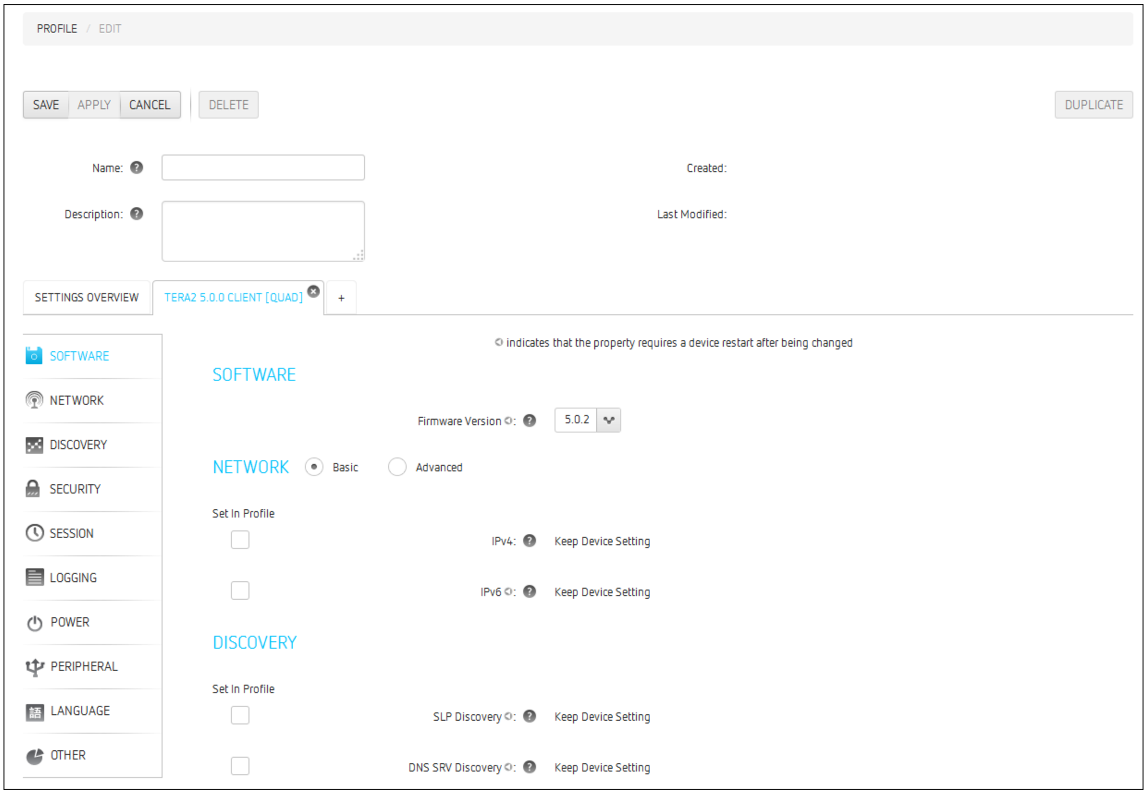
For the Tera2 PCoIP Zero Client, you can configure profiles for dual and quad endpoint types. The dual zero client supports two monitors. The quad zero client supports four monitors. You need to create a separate profile for each endpoint type.

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.
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.



Name:

Description:

Created:

Last Modified:

◌ indicates that the property requires a device restart after being changed

SOFTWARE

Firmware Version ◌: 5.0.2

NETWORK ● Basic ○ Advanced

Set In Profile

□ IPv4: Keep Device Setting

□ IPv6 ◌: Keep Device Setting

DISCOVERY

Set In Profile

□ SLP Discovery ◌: Keep Device Setting

□ DNS SRV Discovery ◌: Keep Device Setting

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* on page 99.

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:

Note: See firmware version from SETTINGS > SOFTWARE MANAGEMENT page
When you add a profile, the firmware version that displays in the **PROFILE > ADD PROFILE** drop-down list may not directly correlate to the firmware version you associate with the profile. You will see the actual version number of the firmware file when you select it from the **SETTINGS > SOFTWARE MANAGEMENT** page.

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* on page 83.
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* on page 85 to choose how to apply the updated profile.

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

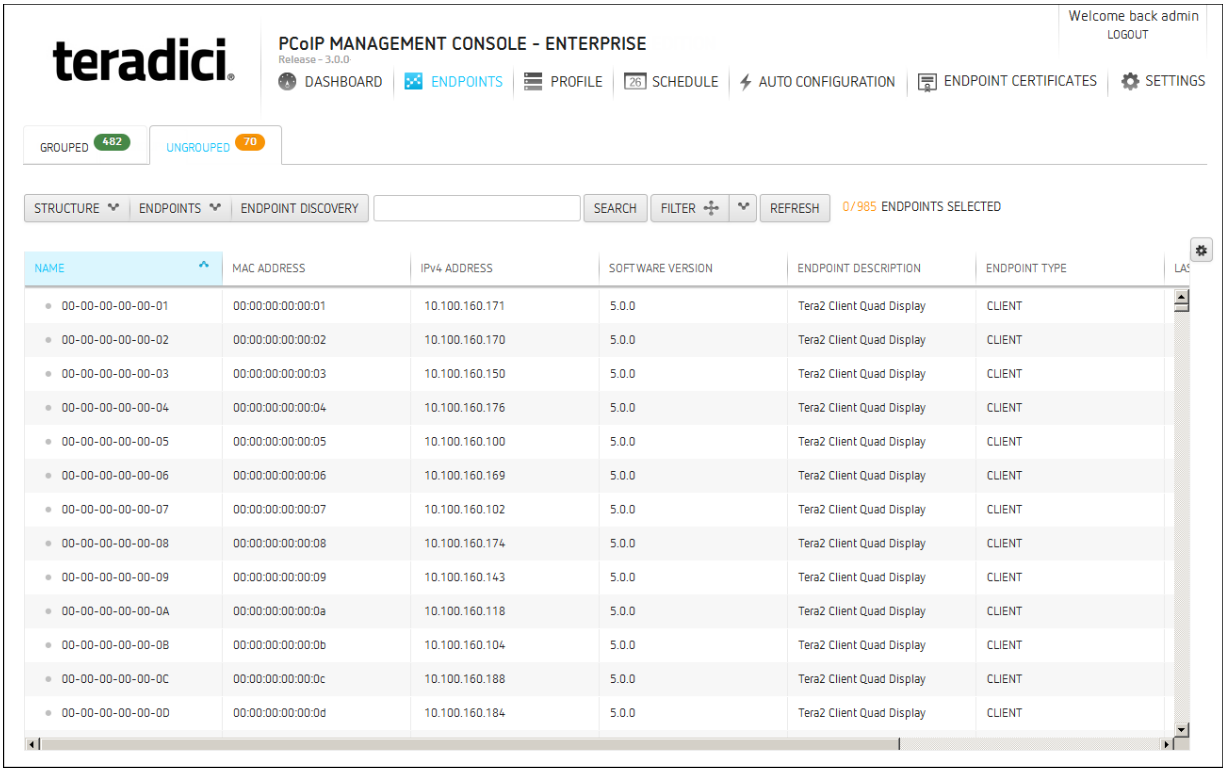
To view profile details:

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.



NAME	MAC ADDRESS	IPv4 ADDRESS	SOFTWARE VERSION	ENDPOINT DESCRIPTION	ENDPOINT TYPE	LAS
00-00-00-00-00-01	00:00:00:00:00:01	10.100.160.171	5.0.0	Tera2 Client Quad Display	CLIENT	
00-00-00-00-00-02	00:00:00:00:00:02	10.100.160.170	5.0.0	Tera2 Client Quad Display	CLIENT	
00-00-00-00-00-03	00:00:00:00:00:03	10.100.160.150	5.0.0	Tera2 Client Quad Display	CLIENT	
00-00-00-00-00-04	00:00:00:00:00:04	10.100.160.176	5.0.0	Tera2 Client Quad Display	CLIENT	
00-00-00-00-00-05	00:00:00:00:00:05	10.100.160.100	5.0.0	Tera2 Client Quad Display	CLIENT	
00-00-00-00-00-06	00:00:00:00:00:06	10.100.160.169	5.0.0	Tera2 Client Quad Display	CLIENT	
00-00-00-00-00-07	00:00:00:00:00:07	10.100.160.102	5.0.0	Tera2 Client Quad Display	CLIENT	
00-00-00-00-00-08	00:00:00:00:00:08	10.100.160.174	5.0.0	Tera2 Client Quad Display	CLIENT	
00-00-00-00-00-09	00:00:00:00:00:09	10.100.160.143	5.0.0	Tera2 Client Quad Display	CLIENT	
00-00-00-00-00-0A	00:00:00:00:00:0a	10.100.160.118	5.0.0	Tera2 Client Quad Display	CLIENT	
00-00-00-00-00-0B	00:00:00:00:00:0b	10.100.160.104	5.0.0	Tera2 Client Quad Display	CLIENT	
00-00-00-00-00-0C	00:00:00:00:00:0c	10.100.160.188	5.0.0	Tera2 Client Quad Display	CLIENT	
00-00-00-00-00-0D	00:00:00:00:00:0d	10.100.160.184	5.0.0	Tera2 Client Quad Display	CLIENT	

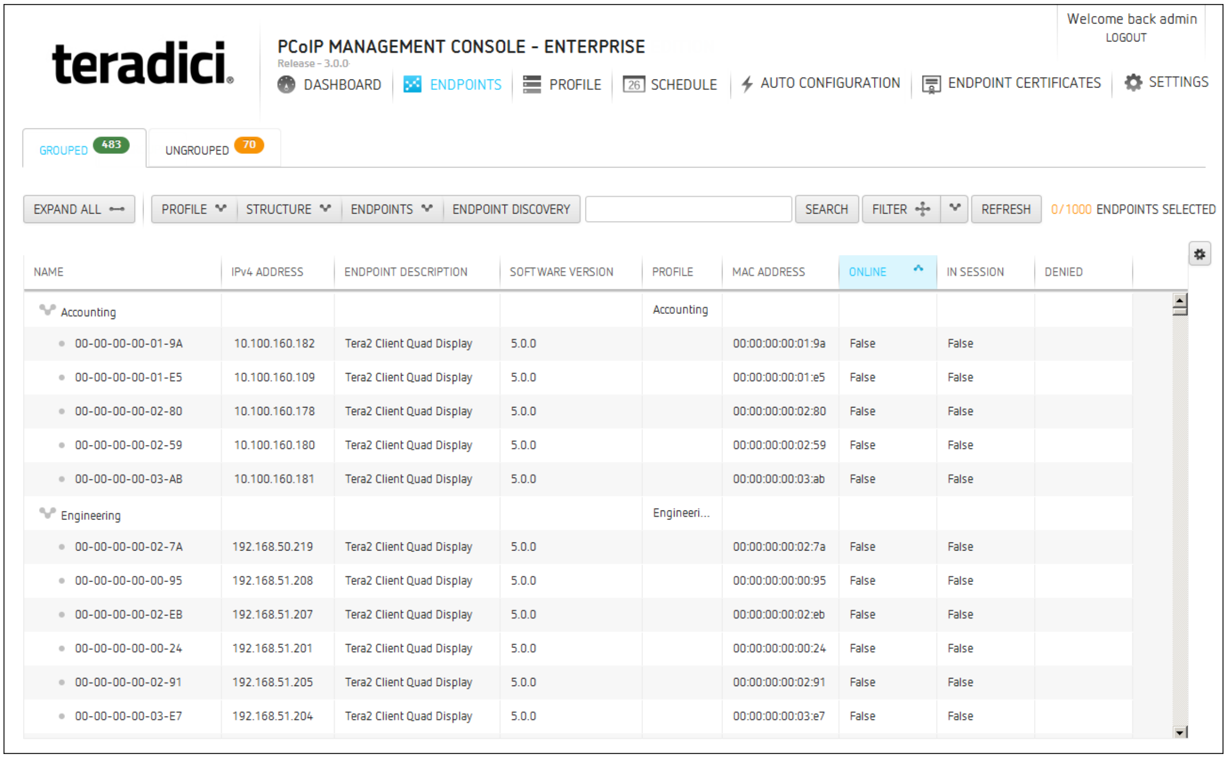
The ENDPOINTS page - UNGROUPED

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.



NAME	IPv4 ADDRESS	ENDPOINT DESCRIPTION	SOFTWARE VERSION	PROFILE	MAC ADDRESS	ONLINE	IN SESSION	DENIED
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	False	False	
00-00-00-00-01-E5	10.100.160.109	Tera2 Client Quad Display	5.0.0		00:00:00:00:01:e5	False	False	
00-00-00-00-02-80	10.100.160.178	Tera2 Client Quad Display	5.0.0		00:00:00:00:02:80	False	False	
00-00-00-00-02-59	10.100.160.180	Tera2 Client Quad Display	5.0.0		00:00:00:00:02:59	False	False	
00-00-00-00-03-AB	10.100.160.181	Tera2 Client Quad Display	5.0.0		00:00:00:00:03:ab	False	False	
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	False	False	
00-00-00-00-00-95	192.168.51.208	Tera2 Client Quad Display	5.0.0		00:00:00:00:00:95	False	False	
00-00-00-00-02-EB	192.168.51.207	Tera2 Client Quad Display	5.0.0		00:00:00:00:02:eb	False	False	
00-00-00-00-00-24	192.168.51.201	Tera2 Client Quad Display	5.0.0		00:00:00:00:00:24	False	False	
00-00-00-00-02-91	192.168.51.205	Tera2 Client Quad Display	5.0.0		00:00:00:00:02:91	False	False	
00-00-00-00-03-E7	192.168.51.204	Tera2 Client Quad Display	5.0.0		00:00:00:00:03:e7	False	False	

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**.

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

To remove 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.

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)

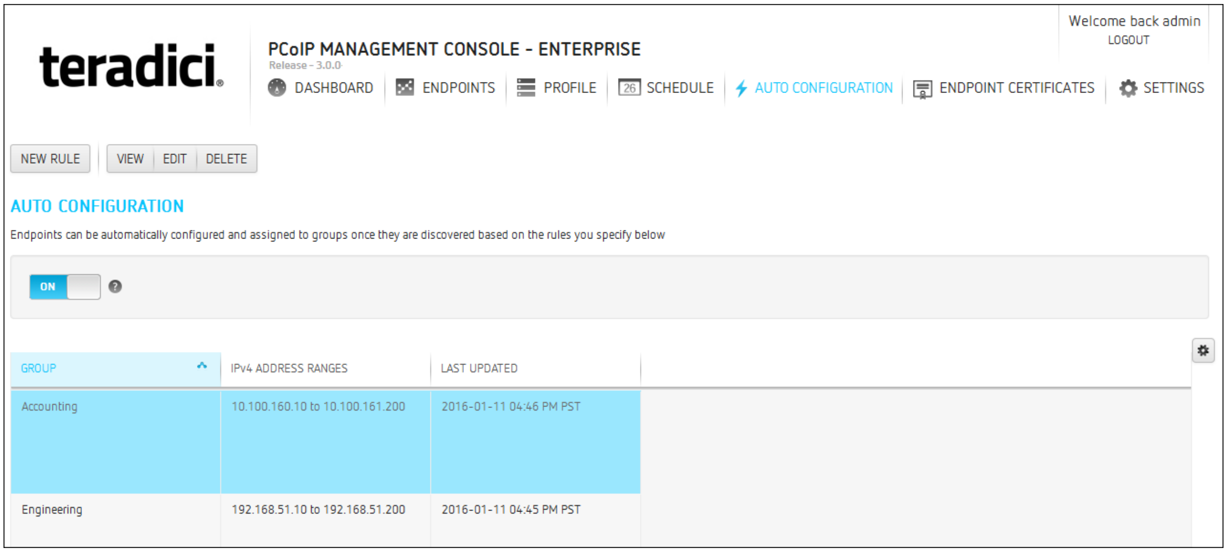
The PCoIP Management Console Enterprise lets you create rules to automatically move endpoints into a specific group when they are first discovered. After discovery, you can find the endpoints in the GROUPED table on the **ENDPOINTS** page. If you are using PCoIP Management Console Free, you will be able to view 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 view, 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.

Caution: 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.



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

GROUP	IPv4 ADDRESS RANGES	LAST UPDATED
Accounting	10.100.160.10 to 10.100.161.200	2016-01-11 04:46 PM PST
Engineering	192.168.51.10 to 192.168.51.200	2016-01-11 04:45 PM PST

AUTO CONFIGURATION page and switch button

Creating an Auto Configuration Rule

To create an auto configuration rule:

Note: Help with settings

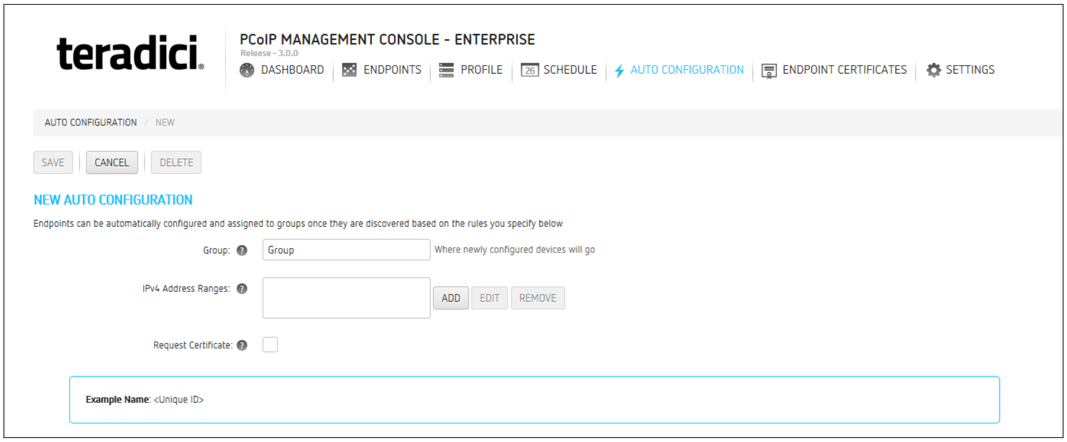
Click the **?** button beside each field for help with any of the settings.

1. From the PCoIP Management Console's top menu, click **AUTO CONFIGURATION**.
2. Click **NEW RULE** and configure the rule as follows:
   - **Group**: Click in this field, select the desired group, and then click **OK**.
   - **IPv4 Address Ranges**: 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, that is, from x.0.0.0 to x.255.255.255.

     Note: Example 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* on page 95.

- **Request Certificate**: Select to automatically retrieve a Simple Certificate Enrollment Protocol (SCEP) digital certificate from a SCEP server.



teradici.

PCoIP MANAGEMENT CONSOLE - ENTERPRISE

Release - 3.0.0

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

AUTO CONFIGURATION / NEW

SAVE | CANCEL | DELETE

NEW AUTO CONFIGURATION

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

Group: Group Where newly configured devices will go

IPv4 Address Ranges: ADD EDIT REMOVE

Request Certificate: □

Example Name: <Unique ID>

3. Click **SAVE**.

Note: 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 Auto Configuration Rule Details

To view auto configuration rule details:

1. Select the rule in the *AUTO CONFIGURATION* list.
2. Click **VIEW**.
3. If desired, you choose to view the previous or next rule in the list, or you can click **EDIT** to edit the rule.
4. Click **AUTO CONFIGURATION** in the navigation link at the top to return to the main page.

Editing an Auto Configuration Rule

To edit an auto configuration rule:

1. Select the rule in the *AUTO CONFIGURATION* list.
2. Click **EDIT**.
3. Make the 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.

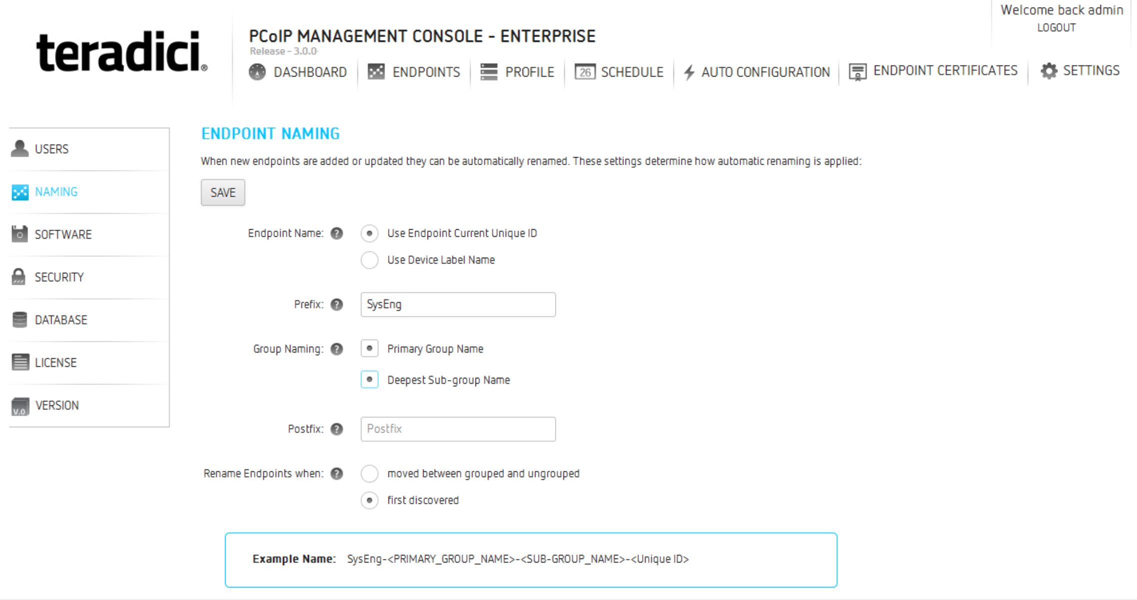
Creating a Global Endpoint Naming Convention

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-<*MAC address*>) 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.



ENDPOINT NAMING

When new endpoints are added or updated they can be automatically renamed. These settings determine how automatic renaming is applied:

Endpoint Name: ● Use Endpoint Current Unique ID ○ Use Device Label Name

Prefix: SysEng

Group Naming: ☑ Primary Group Name ☑ Deepest Sub-group Name

Postfix: Postfix

Rename Endpoints when: ○ moved between grouped and ungrouped ● first discovered

Example Name: SysEng-<PRIMARY_GROUP_NAME>-<SUB-GROUP_NAME>-<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. Tera2 zero clients support 802.1X authentication, which prevents unauthorized devices from gaining access to local area networks (LANs).

Tip: Organize endpoints into groups

Before you create an endpoint certificate, organize your endpoints into groups. See *Organizing Endpoints into Groups* on page 88.

Info: View certificate information

PCoIP Management Console Enterprise Edition release 2.5+ users can reference certificate information displayed on the dashboard.

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. In the **Server URI**, field, type the Uniform Resource Identifier (URI) of the SCEP server that is configured to issue certificates for the group.
5. In the **Server Password** field, type the password for the SCEP server.
6. 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).
7. In the **Use Certificate for 802.1X** field, select **True** to have the endpoint present this certificate to the 802.1x authenticator.
8. Click **SAVE**.

To view an endpoint certificate rule:

1. Click **ENDPOINT CERTIFICATES** to display the *CERTIFICATE MANAGEMENT* window.
2. Click **VIEW** to review the details of an endpoint certificate rule.
3. If there is more than one endpoint certificate rule, click **PREV** or **NEXT** to view additional certificate rules.

To edit an endpoint certificate rule:

1. Click **ENDPOINT CERTIFICATES** to display the *CERTIFICATE MANAGEMENT* window.
2. Highlight a certificate rule that you want to edit.
3. Click **EDIT** to revise an endpoint certificate rule.

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** to delete an endpoint certificate rule.
4. In the *DELETE CERTIFICATE RULE* dialog box, click **DELETE**.

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. In this release, 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. If you are using PCoIP Management Console Free, you will be able to view existing configurations.

Displaying Schedule Information

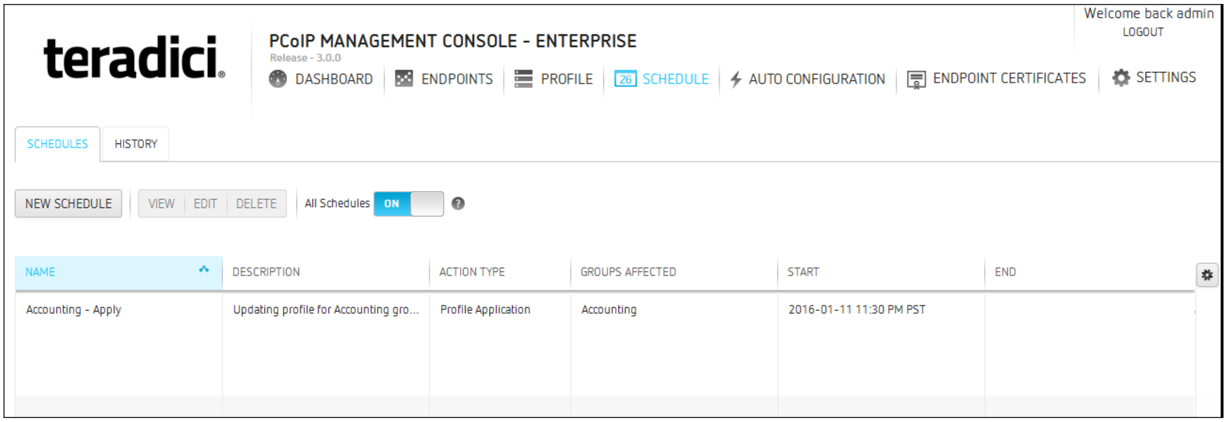
All configured schedules are displayed on the PCoIP Management Console’s **SCHEDULES** page. You can view information about schedules that have previously run by clicking the **HISTORY** tab. Any configured schedules that have yet to run are also displayed on the PCoIP Management Console dashboard in its **UPCOMING SCHEDULES** area.

SCHEDULES Page

This 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. The **All Schedules**

ON/OFF switch ON at the top of the page lets you globally enable or disable all schedules 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.



NAME	DESCRIPTION	ACTION TYPE	GROUPS AFFECTED	START	END
Accounting - Apply	Updating profile for Accounting gro...	Profile Application	Accounting	2016-01-11 11:30 PM PST	

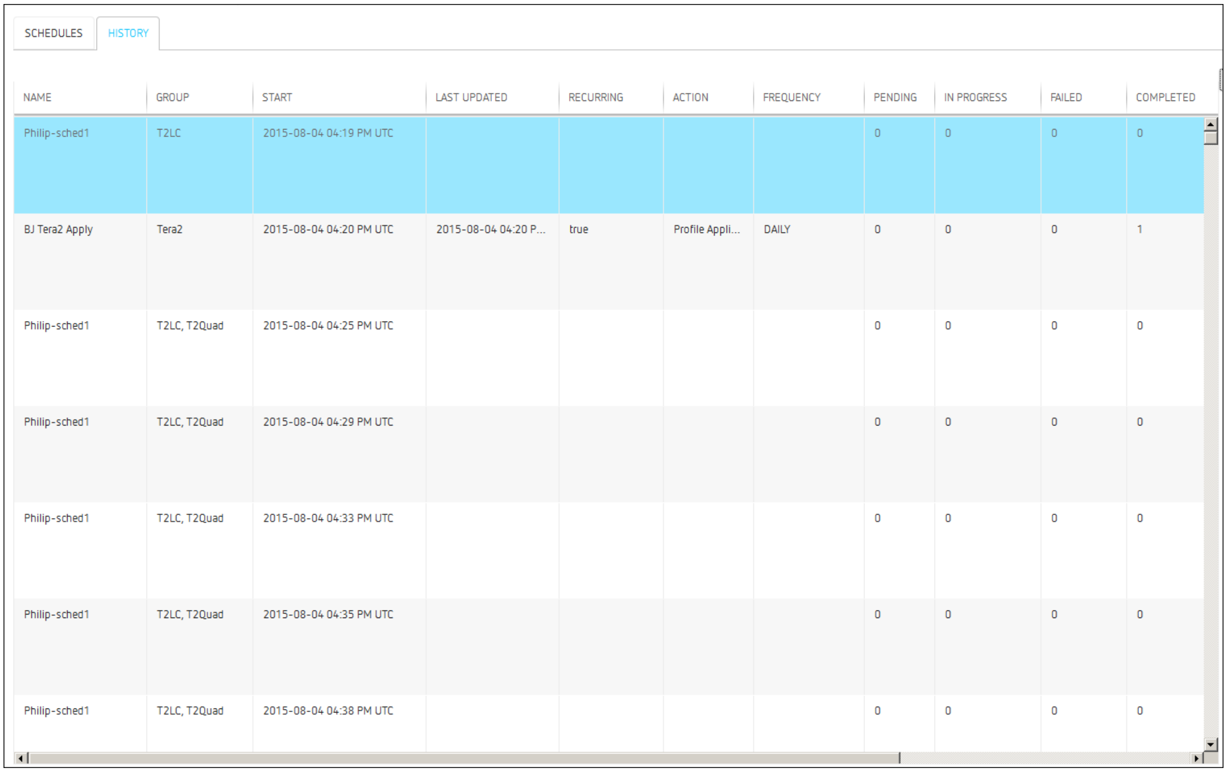
SCHEDULES Page

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.



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.

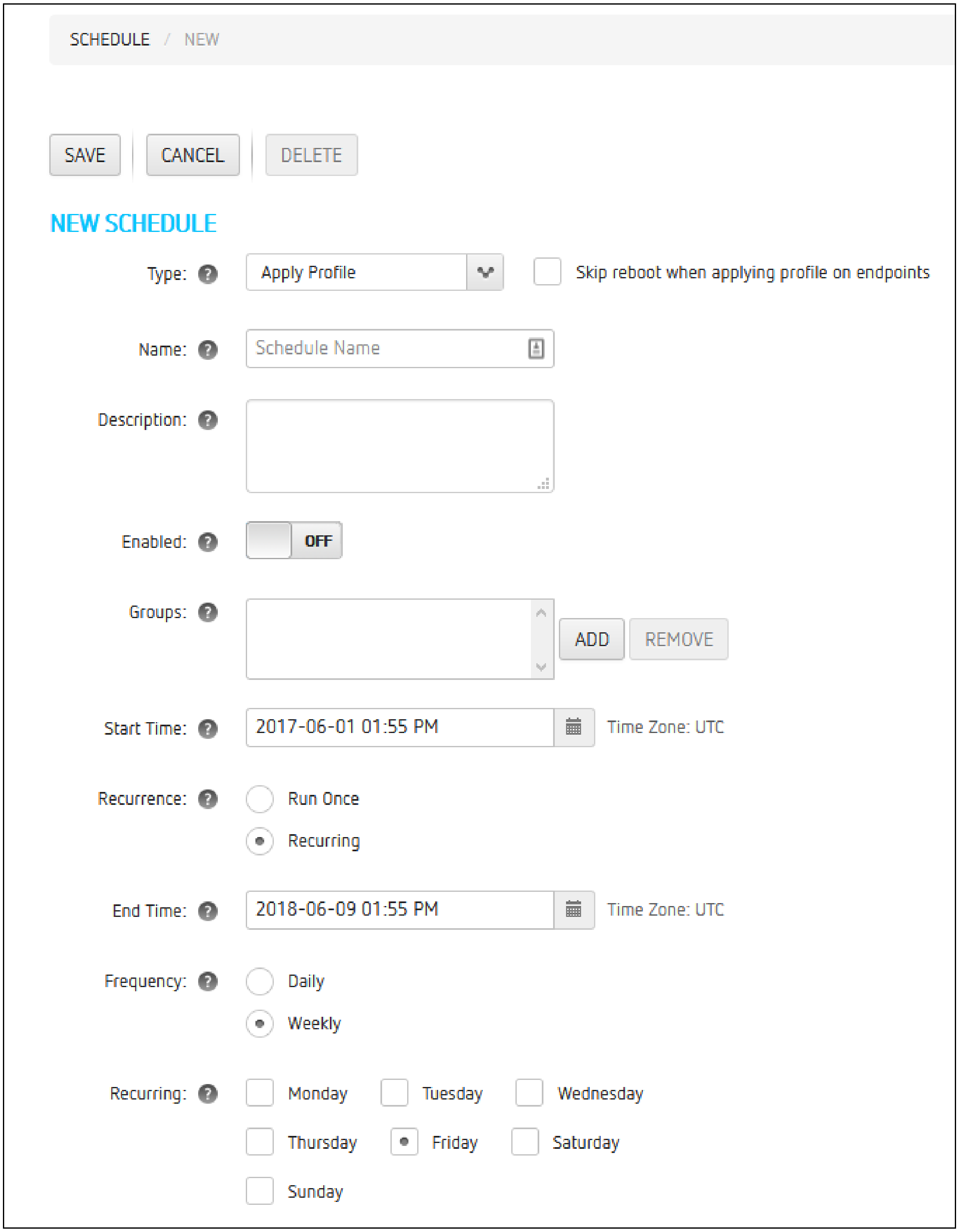
To create a schedule:

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.
    - **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

NEW SCHEDULE

Type: Apply Profile □ Skip reboot when applying profile on endpoints

Name: Schedule Name

Description:

Enabled: OFF

Groups:

Start Time: 2017-06-01 01:55 PM Time Zone: UTC

Recurrence: ○ Run Once ● Recurring

End Time: 2018-06-09 01:55 PM Time Zone: UTC

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**.

PCoIP Management Console Remote Endpoint Management (Enterprise)

The PCoIP Management Console must be licensed with a trial or enterprise license to use remote device management. See *Activating Licenses* on page 27 the administrators' guide for more information on licensing. You will also need to deploy a reverse proxy and ensure the network connection between the PCoIP Management Console and the remote endpoint has a latency of approximately 100ms or less.

Administration of remote endpoints requires the configuration of the proxy, the PCoIP Management Console, and the remote endpoint. Each configuration can be found in the following topics:

Reverse Proxy Configuration on page 103

Configuring PCoIP Management Console Remote Management on page 103

Connecting to a Remote Endpoint on page 104

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 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://** preceeding the FQDN.
- It must be configured with a publicly accessible address, including DNS SRV and DNS TXT records.
  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 certificates added to its configuration.
  This certificates SHA256 fingerprint is entered in the PCoIP Management Console **External Certificate Fingerprint** field on the *REMOTE CONFIGURATION* page, in **SETTINGS > REMOTE**.

Teradici has provided a sample configuration using nginx for a reverse proxy, and is provided as-is, with no warranty. This sample configuration resides on the 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

PCoIP Management Console. This is how "remote" devices will access the PCoIP Management Console.

> **Important: DNS SRV and TXT records**
> The public IP address of the reverse proxy server requires both DNS SRV and DNS TXT records.

- **External Certificate Fingerprint:** Here you can enter the PCoIP Management Console certificate fingerprint. Endpoints may require the fingerprint of the certificate used for external access to the PCoIP Management Console. This is usually the certificate fingerprint of the reverse proxy.
- **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

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 zero client this can be done by either configuring and uploading the required certificates onto the zero client via the AWI, or by creating an external DNS entry for the Proxy server via the zero client OSD.

Connecting to a Remote Endpoint from OSD

This is the commended method which requires the OSD be accessible and the end user knows the password, and that there is a properly configured public DNS server that will provide the address of the reverse proxy and the SHA256 certificate fingerprint of the reverse proxy to the endpoint. (*Configuring Endpoints for Auto Discovery Using DNS* on page 74

1. From your zero client OSD, navigate to **Options > Configuration > Network.**
2. `Unlock` your 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 zero client, select `Reset` to restart your zero client.

The 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 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 to a Remote Endpoint via AWI

This method requires the AWI be enabled and accessible on the zero client, and the zero client user knows the AWI password.

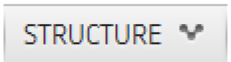
1. From the zero client AWI navigate to **Configuration > Management.**
2. Set the Manager Discovery Mode to *Manual* and enter in the address of the reverse proxy into the **Endpoint Bootstrap Manager URI**.
3. Install the certificate of the reverse proxy into the endpoint via the *Certificate Upload* page, by navigating the AWI to **Upload > Certificate.** See *Installing Your Own Certificates* on page 1.

Using the Endpoints Page

The actions you can perform from the **ENDPOINTS** page are listed in the following table.

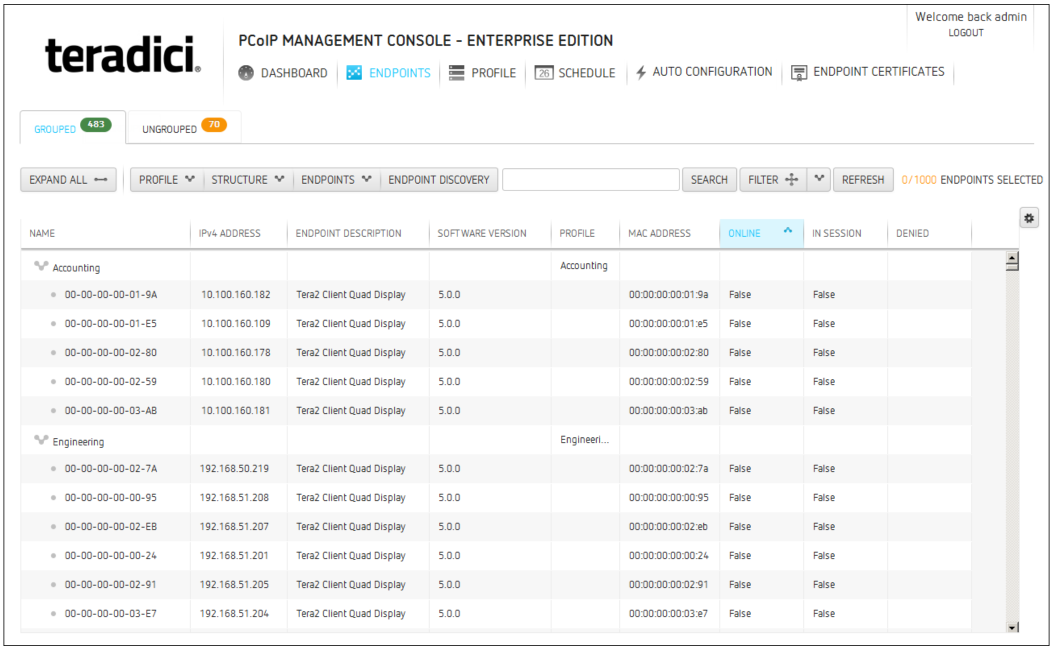
ENDPOINTS Page Features

Menu	Action
	Toggles to display the following: • Expand top-level and parent groups to display all child level groups and endpoints. • Collapse the group hierarchy and display only top-level groups.
	Displays on the **GROUPED** table and provides the following menus: • **DETAILS**: View details about a profile assigned to a group. See *Viewing Profile Details* on page 87. • **CHANGE**: Change the profile assigned to a group. See *Changing a Profile Association* on page 85. • **APPLY**: Apply a profile to a group. See *Applying a Profile* on page 85.

Menu	Action
 STRUCTURE	Provides the following menus: - **MOVE**: Move endpoints or groups to a group. See *Moving Endpoints into Groups* on page 89. - **RENAME**: Rename a group or endpoint. See *Renaming a Group* on page 90. - **NEW GROUP**: Create a new group. *Creating Groups* on page 89 - **REMOVE GROUP**: Remove a group. *Removing a Group* on page 90.
ENDPOINTS	Provides the following menus: - **DETAILS**: View details about an endpoint. See *Using the ENDPOINT DETAILS Page* on page 118. - **POWER DOWN**: Power down one or more endpoints. See *Powering Down Endpoints* on page 122. - **POWER RESET**: Reset (reboot) one or more endpoints. See *Resetting Endpoints* on page 122. - **RESET TO DEFAULT**: Reset endpoint properties to their default values. See *Resetting Endpoint Properties to Their Defaults* on page 123. **Note: 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* on page 124.
ENDPOINT DISCOVERY	Lets you manually discover endpoints by their IP address. See *Discovering Endpoints Manually from PCoIP Management Console* on page 115.
SEARCH	Lets you search for one or more endpoints in the endpoint table. See *Searching an Endpoint Table* on page 125.
FILTER	Lets you create and manage filters to display only specified endpoints. See *Filtering the Endpoint List* on page 126.
REFRESH	Refreshes the endpoint table with the current configuration. **Note: 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	ONLINE	IN SESSION	DENIED
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	False	False	
00-00-00-00-01-E5	10.100.160.109	Tera2 Client Quad Display	5.0.0		00:00:00:00:01:e5	False	False	
00-00-00-00-02-80	10.100.160.178	Tera2 Client Quad Display	5.0.0		00:00:00:00:02:80	False	False	
00-00-00-00-02-59	10.100.160.180	Tera2 Client Quad Display	5.0.0		00:00:00:00:02:59	False	False	
00-00-00-00-03-AB	10.100.160.181	Tera2 Client Quad Display	5.0.0		00:00:00:00:03:ab	False	False	
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	False	False	
00-00-00-00-00-95	192.168.51.208	Tera2 Client Quad Display	5.0.0		00:00:00:00:00:95	False	False	
00-00-00-00-02-EB	192.168.51.207	Tera2 Client Quad Display	5.0.0		00:00:00:00:02:eb	False	False	
00-00-00-00-00-24	192.168.51.201	Tera2 Client Quad Display	5.0.0		00:00:00:00:00:24	False	False	
00-00-00-00-02-91	192.168.51.205	Tera2 Client Quad Display	5.0.0		00:00:00:00:02:91	False	False	
00-00-00-00-03-E7	192.168.51.204	Tera2 Client Quad Display	5.0.0		00:00:00:00:03:e7	False	False	

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
AUTO CONFIGURATION STATUS	Displays an endpoint's auto configuration status. Possible values: • 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
	• COMPLETED			
APPLY PROFILE	Displays the status of endpoint's profile update. Possible values: • NOT STARTED • IN PROGRESS • COMPLETED • SKIPPED • FAILED 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.	✓		
CERTIFICATE EXPIRY DATE	Displays the date the SCEP certificate will expire and become not valid.	✓	✓	
CERTIFICATE NAME	Displays the SCEP certificate subject name.	✓	✓	

Property	Information	Grouped	Ungrouped	MC Enterprise Only
CERTIFICATE RULE	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.	✓		
CERTIFICATE START DATE	Displays the date the SCEP certificate becomes valid.	✓	✓	
CERTIFICATE STATUS	Displays the status of the SCEP certificate. Possible values: • Active • About To Expire • Expiring Today • Expired • Not Requested	✓	✓	
CLEAR MANAGEMENT STATE	Indicates if devices now have all management settings cleared and set back to a default state.	✓		
CONNECTED BY	Identifies where in the deployment the PCoIP endpoint is placed. Possible Values: • Local • Remote	✓	✓	✓

Property	Information	Grouped	Ungrouped	MC Enterprise Only
DENIED	Indicates whether or not the PCoIP Management Console has enough licenses to manage all the discovered endpoints. Possible values: • 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.	✓	✓	
DISPLAY TYPE	Displays the maximum number of monitors an endpoint supports. Possible values for a Tera2 PCoIP Zero Client: • Dual: The endpoint supports up to two monitors. • Quad: The endpoint supports up to four monitors.	✓	✓	
ENDPOINT DESCRIPTION	Displays information about the Teradici family and endpoint type for the endpoint.	✓	✓	

Property	Information	Grouped	Ungrouped	MC Enterprise Only
ENDPOINT PLATFORM	Displays the endpoint’s PCoIP family. In this release, only endpoints that support the Tera2 platform can be managed by the PCoIP Management Console.	✓	✓	
ENDPOINT TYPE	Displays the endpoint type. Possible values: • Client	✓	✓	
FIRMWARE BUILD ID	Lists the firmware build number in use on the PCoIP endpoint	✓	✓	
FQDN	Displays an endpoint’s fully-qualified domain name.	✓	✓	
IPv4 ADDRESS	Displays an endpoint's IPv4 address	✓	✓	
IN SESSION	Indicates whether or not an endpoint is in a PCoIP session with another PCoIP software or hardware endpoint. Possible values: • True • False	✓	✓	

Property	Information	Grouped	Ungrouped	MC Enterprise Only
INTERNAL IPv4	Displays an endpoint's IPv4 address for the network the endpoint is part of. For remote endpoints, this will be their internal network addresses.	✓	✓	✓
LAST POLLED	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.	✓	✓	
MAC ADDRESS	Displays an endpoint's MAC address.	✓	✓	
ONLINE	Indicates whether or not an endpoint is connected to the PCoIP Management Console. Possible values: • True • False	✓	✓	
Reset to Default Columns	Resets the table to display the default columns.	✓	✓	

Property	Information	Grouped	Ungrouped	MC Enterprise Only
SERIAL NUMBER	The serial number of the endpoint is now available from the endpoints table. It can also be exported into the Inventory Report	✓	✓	
SOFTWARE VERSION	Firmware file name used in the PCoIP firmware build minus the build number	✓	✓	
UNIQUE ID	Displays an endpoint's MAC address delimited with hyphens instead of colons. This field can be incorporated into the automatic naming convention for endpoints.	✓	✓	

Discovering Endpoints Manually from PCoIP Management Console

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 a Endpoint Manager and has a **Idle** management status (that is, is not engaged in any kind of PCoIP Management Console activity).

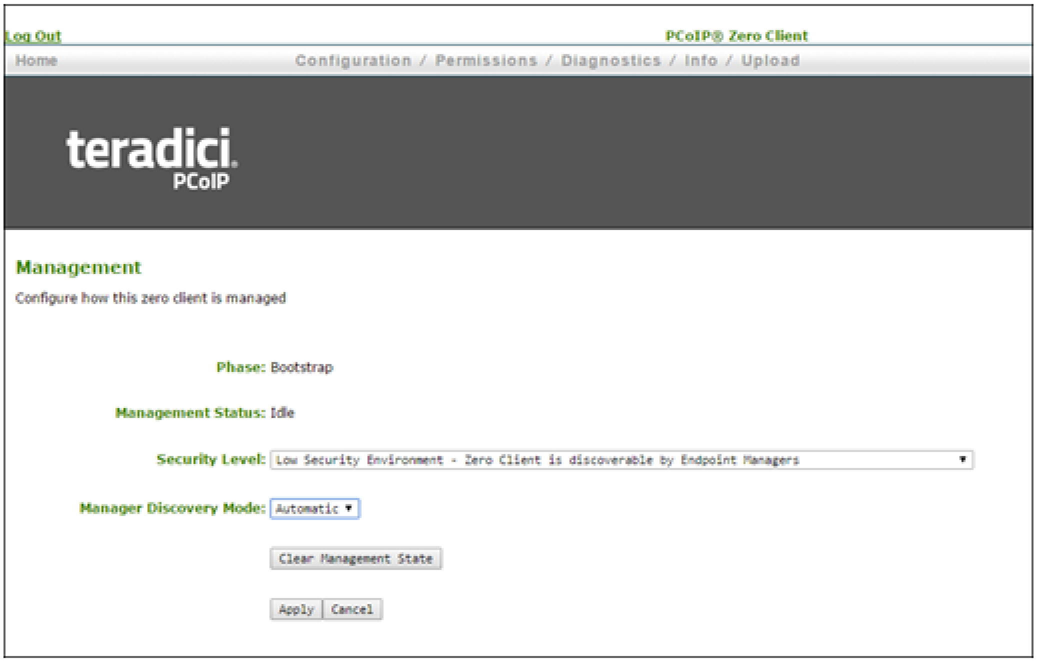
- The endpoint is configured for a Low Security Environment from its AWI Management page.

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 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**.



Management

Configure how this zero client is managed

Phase: Bootstrap

Management Status: Idle

Security Level: Low Security Environment - Zero Client is discoverable by Endpoint Managers

Manager Discovery Mode: Automatic

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

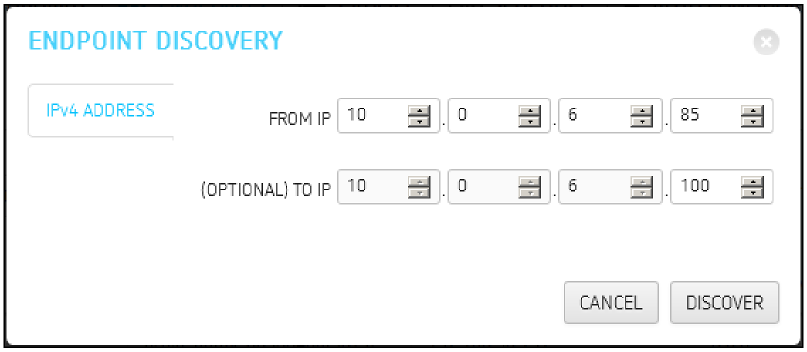
To discover endpoints manually:

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 only (for example, 10.0.0.1 to 10.0.0.255). It cannot support a range such as 10.0.0.1 to 10.0.255.255.

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



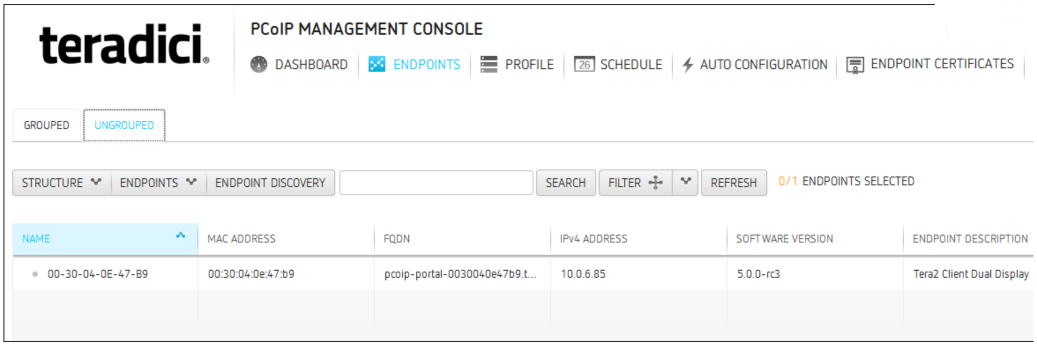
ENDPOINT DISCOVERY

IPv4 ADDRESS

FROM IP 10 . 0 . 6 . 85

(OPTIONAL) TO IP 10 . 0 . 6 . 100

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).



PCoIP MANAGEMENT CONSOLE

0/1 ENDPOINTS SELECTED

NAME	MAC ADDRESS	FQDN	IPv4 ADDRESS	SOFTWARE VERSION	ENDPOINT DESCRIPTION
00-30-04-0E-47-B9	00:30:04:0e:47:b9	pcoip-portal-0030040e47b9.t...	10.0.6.85	5.0.0-rc3	Tera2 Client Dual Display

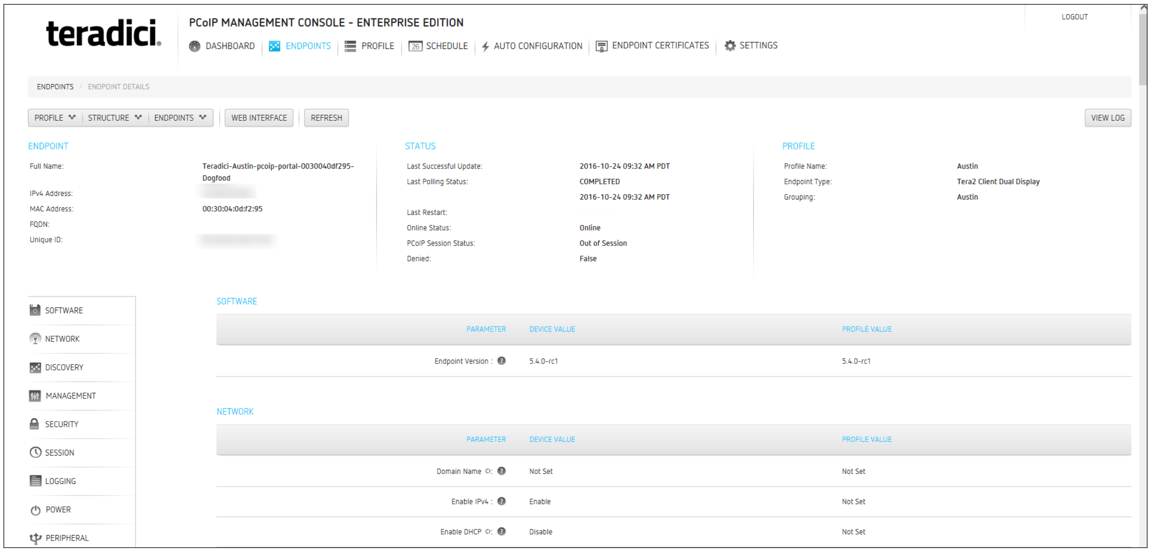
Note: Automatically name and group endpoints
You can configure the PCoIP Management Console to automatically name endpoints and place them in a specific group when they are discovered. See *Auto Naming Endpoints* on page 94 and *Auto Configuring Endpoints (Enterprise)* on page 91 for details.

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 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.
- Reset (reboot) the endpoint.
- Restore the endpoint’s default configuration.
- Access the endpoint’s web interface.
- View the endpoint’s device log.
- Refresh.



ENDPOINT

Full Name:	Teradici-Austin-pcoip-portal-0030040df295-Dogfood
IPv4 Address:	[redacted]
MAC Address:	00:30:04:0d:f2:95
FQDN:	
Unique ID:	[redacted]

STATUS

Last Successful Update:	2016-10-24 09:32 AM PDT
Last Polling Status:	COMPLETED 2016-10-24 09:32 AM PDT
Last Restart:	[redacted]
Online Status:	Online
PCoIP Session Status:	Out of Session
Denied:	False

PROFILE

Profile Name:	Austin
Endpoint Type:	Tera2 Client Dual Display
Grouping:	Austin

SOFTWARE

PARAMETER	DEVICE VALUE	PROFILE VALUE
Endpoint Version :	5.4.0-rc1	5.4.0-rc1

NETWORK

PARAMETER	DEVICE VALUE	PROFILE VALUE
Domain Name :	Not Set	Not Set
Enable IPv4 :	Enable	Not Set
Enable DHCP :	Disable	Not Set

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 **ENDPOINT** 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* on page 94.

Powering Down an Endpoint

The **POWER DOWN** option causes an endpoint to power down right away, or after any currently running scheduled actions for this endpoint have completed. You can power down an endpoint 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.

Resetting an Endpoint

The **POWER RESET** option causes an endpoint to reset (reboot) right away, or after any currently running scheduled actions have completed. You can reset an endpoint 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 Their Defaults

The **RESET TO DEFAULT** option causes an endpoint to reset to its default configuration right away, or after any currently running scheduled actions have completed. You can reset an endpoint to its default configuration either from the **ENDPOINTS** page or the **ENDPOINT DETAILS** page.

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.

Deleting an Endpoint

The **DELETE** option enables removal of one or more endpoints from 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 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 is 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 **ENDPOINT** and then **DELETE**.
4. Click **I AM SURE** at the message prompt.

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.

For information about the AWI, please see *Tera2 PCoIP Zero Client 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 endpoints from the PCoIP Management Console. These actions are performed on one or more individual endpoints and occur as soon as you apply them from the **ENDPOINTS** menu, or after any currently running scheduled actions for this endpoint have completed. Alternatively, you can create a schedule to power down or reset one or more groups of endpoints in the future. See *Creating a Schedule* on page 99.

Powering Down Endpoints

The **POWER DOWN** option causes an endpoint to power down right away, or after any currently running scheduled actions have completed. You can power down an endpoint either from its **ENDPOINT DETAILS** page or from the **ENDPOINTS** page.

To power down 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 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 endpoints 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 **ENDPOINT** and then **POWER RESET**.
    d. Click **OK** at the message prompt.
3. Click **ENDPOINT** and then **POWER DOWN**.
4. Click **OK** at the message prompt.

Resetting Endpoints

The **POWER RESET** option causes an endpoint to reboot right away, or after any currently running scheduled actions for this endpoint 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 endpoints 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.

3. Click **ENDPOINT** and then **POWER RESET**.
4. Click **OK** at the message prompt.

Resetting Endpoint Properties to Their Defaults

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.

Note: Resetting an endpoint clears the management state
Resetting an endpoint will clear the management state of the endpoint. The bootstrap and endpoint discovery will need to be done automatically or manually.

To reset endpoint properties to their defaults:

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 reset.
    a. From the PCoIP Management Console’s top menu, click **ENDPOINTS**.
    b. In either the *GROUPED* or *UNGROUPED* table, select one or more endpoints 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 **ENDPOINT** and then **POWER RESET**.
    d. Click **OK** at the message prompt.
3. Click **ENDPOINT** and then **RESET TO DEFAULT**.
4. Click **OK** at the message prompt.
5. Confirm the endpoint rebooted automatically. If the endpoint has not rebooted, you must reboot the endpoint manually or from the PCoIP Management Console using the **POWER RESET** command.

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* on page 94.

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 is 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.
   Use `Shift`+Click to select contiguous elements and `Ctrl`+Click to select non-contiguous elements.
3. Click **ENDPOINT** and then **DELETE**.
4. 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.

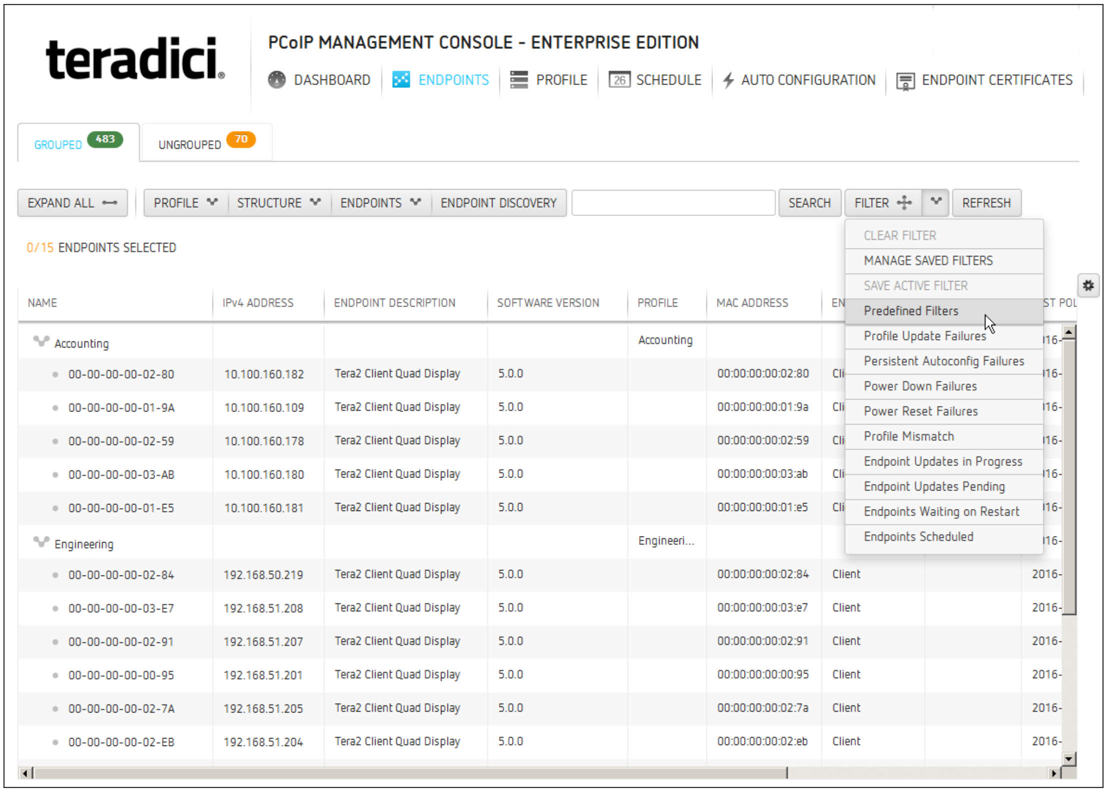
To perform a search:

1. Enter the desired search text in the search text box.
2. Press `Enter` 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.



0/15 ENDPOINTS SELECTED

NAME	IPv4 ADDRESS	ENDPOINT DESCRIPTION	SOFTWARE VERSION	PROFILE	MAC ADDRESS	EN	ST POL
Accounting				Accounting			16-
00-00-00-00-02-80	10.100.160.182	Tera2 Client Quad Display	5.0.0		00:00:00:00:02:80	Cli	16-
00-00-00-00-01-9A	10.100.160.109	Tera2 Client Quad Display	5.0.0		00:00:00:00:01:9a	Cli	16-
00-00-00-00-02-59	10.100.160.178	Tera2 Client Quad Display	5.0.0		00:00:00:00:02:59	Cli	16-
00-00-00-00-03-AB	10.100.160.180	Tera2 Client Quad Display	5.0.0		00:00:00:00:03:ab	Cli	16-
00-00-00-00-01-E5	10.100.160.181	Tera2 Client Quad Display	5.0.0		00:00:00:00:01:e5	Cli	16-
Engineering				Engineeri...			16-
00-00-00-00-02-84	192.168.50.219	Tera2 Client Quad Display	5.0.0		00:00:00:00:02:84	Client	2016-
00-00-00-00-03-E7	192.168.51.208	Tera2 Client Quad Display	5.0.0		00:00:00:00:03:e7	Client	2016-
00-00-00-00-02-91	192.168.51.207	Tera2 Client Quad Display	5.0.0		00:00:00:00:02:91	Client	2016-
00-00-00-00-00-95	192.168.51.201	Tera2 Client Quad Display	5.0.0		00:00:00:00:00:95	Client	2016-
00-00-00-00-02-7A	192.168.51.205	Tera2 Client Quad Display	5.0.0		00:00:00:00:02:7a	Client	2016-
00-00-00-00-02-EB	192.168.51.204	Tera2 Client Quad Display	5.0.0		00:00:00:00:02:eb	Client	2016-

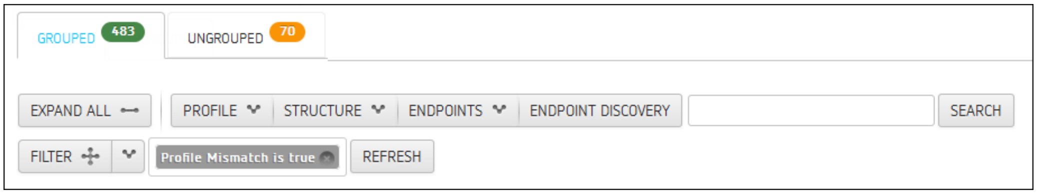
Endpoint predefined filters

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.



Profile Mismatch is true

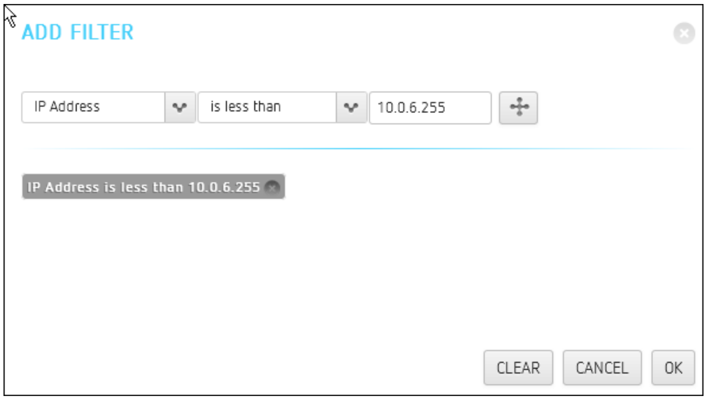
5. To return to the unfiltered endpoint list, click the **x** on the filter icon, or select **CLEAR FILTER** from the **FILTER** drop-down list.

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.
   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.



IP Address | is less than | 10.0.6.255

IP Address is less than 10.0.6.255

5. Click **OK**.
6. To save your filter, select **SAVE ACTIVE FILTER** from the *FILTER* drop-down list on the main *ENDPOINTS* page.
7. 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 **ENDPOINT** 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.

Troubleshooting Endpoints in Recovery Mode

Recovery mode is a special version of the 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.

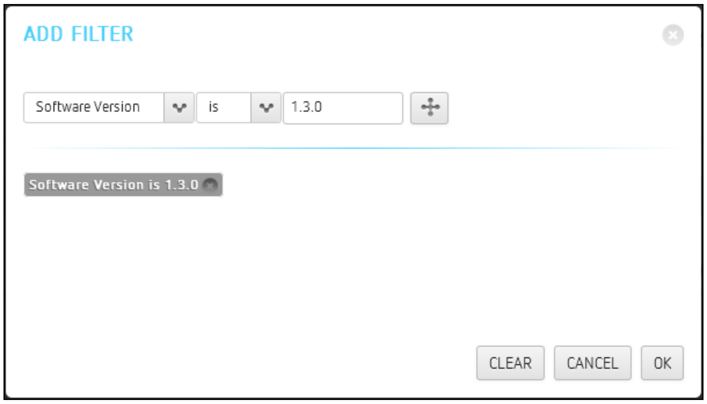
Locating Endpoints in Recovery Mode

Note: Recovery mode is only available for Tera2 PCoIP Zero Clients

Recovery mode is only available for Tera2 PCoIP Zero Clients.

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

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:

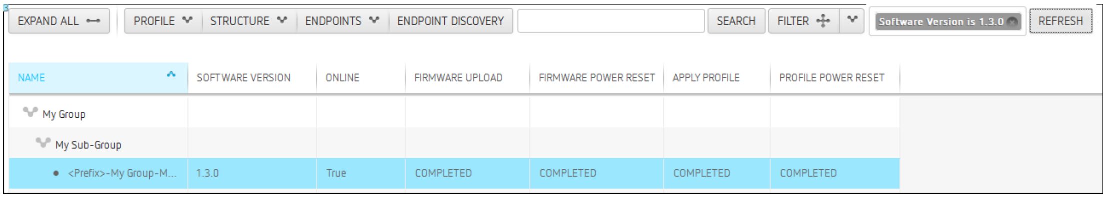
- The client may have been forced into recovery mode by a user repeatedly tapping the power button when turning on the endpoint. If so, rebooting (resetting) the zero client may return it to the main firmware.
- If the client does not load the main firmware but boots into the recovery image immediately 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 zero client and reboot the client to return to working firmware.

- If the 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* on page 123 to clear this problem and then re-provision the endpoint.

Recovery Mode Examples

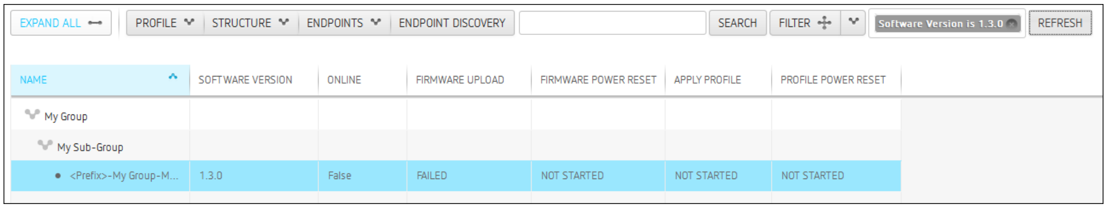
The following example shows a client with a completed firmware upload status. It may have switched to recovery mode by a user repeatedly tapping its power button. In this case, simply performing a power reset may recover the endpoint.



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.



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* on page 121.

Managing Your PCoIP Management Console System

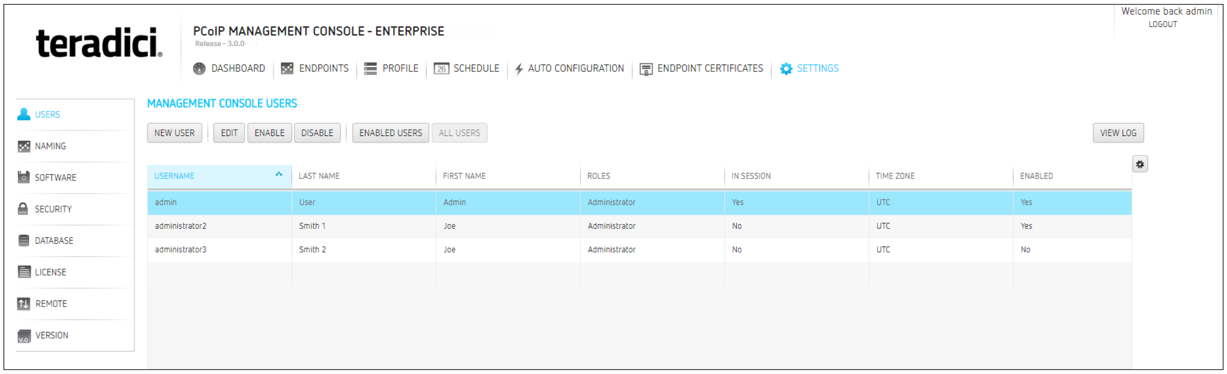
PCoIP Management Console Enterprise supports multiple concurrent administrative users. All users have the same administrative capabilities. PCoIP Management Console Free supports one administrative user.

You can manage PCoIP Management Console Enterprise user accounts by clicking **SETTINGS** from the top menu and then clicking the **USERS** menu in the left pane.

Displaying User Information

The **PCoIP Management Console Enterprise USERS** page contains a table showing all the users that are currently configured to use PCoIP Management Console. PCoIP Management Console Enterprise allows you to create, edit, enable or disable one or more user accounts, 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.

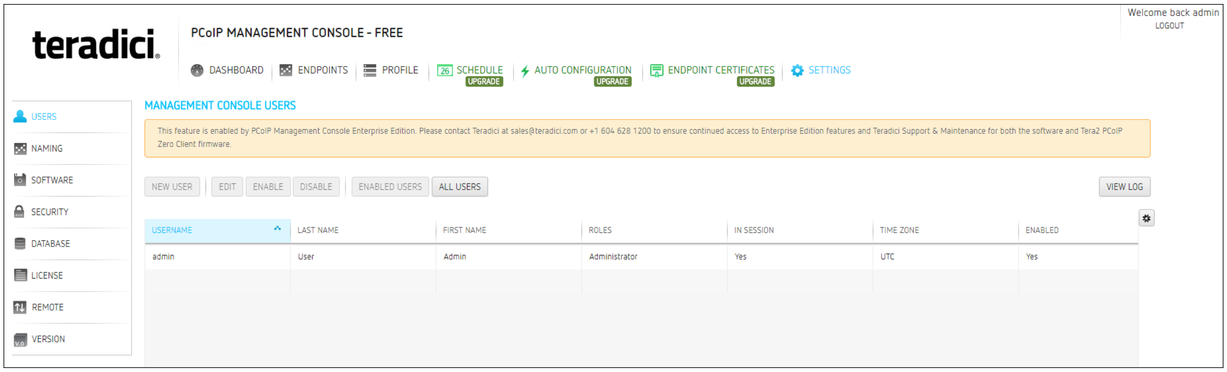
Click the gear icon ⚙ to the right of the table to change the information you want to display in the table columns. Your customized settings are saved in your browser and will be used for any user who subsequently logs in from that browser.



USERNAME	LAST NAME	FIRST NAME	ROLES	IN SESSION	TIME ZONE	ENABLED
admin	User	Admin	Administrator	Yes	UTC	Yes
administrator2	Smith 1	Joe	Administrator	No	UTC	Yes
administrator3	Smith 2	Joe	Administrator	No	UTC	No

PCoIP Management Console Enterprise USERS Page

PCoIP Management Console Free supports only one administrative user. Enabling and disabling this user is not supported.



MANAGEMENT CONSOLE USERS

This feature is enabled by PCoIP Management Console Enterprise Edition. Please contact Teradici at sales@teradici.com or +1 604 628 1200 to ensure continued access to Enterprise Edition features and Teradici Support & Maintenance for both the software and Tera2 PCoIP Zero Client firmware.

USERNAME	LAST NAME	FIRST NAME	ROLES	IN SESSION	TIME ZONE	ENABLED
admin	User	Admin	Administrator	Yes	UTC	Yes

PCoIP Management Console Free USERS Page

Creating a New User Account in PCoIP Management Console Enterprise

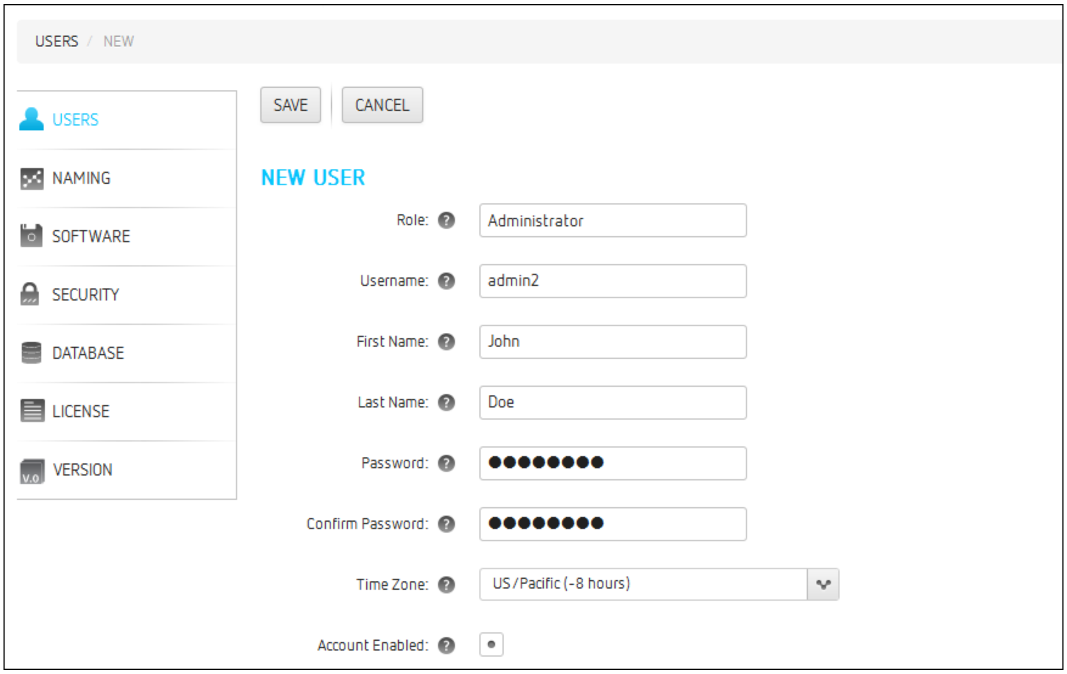
Note: Help with settings

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

To create a new user account in PCoIP Management Console Enterprise:

1. From the PCoIP Management Console's top menu, click **SETTINGS**.
2. Click **USERS** in the left pane.
3. Click **NEW USER**.
4. Configure the parameters as follows:
   - **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.

- **Account Enabled**: Select to enable the account.



NEW USER

Role: Administrator

Username: admin2

First Name: John

Last Name: Doe

Password: ●●●●●●●●

Confirm Password: ●●●●●●●●

Time Zone: US/Pacific (-8 hours)

Account Enabled: ☑

5. Click **SAVE**.

Note: 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**.

Note: 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

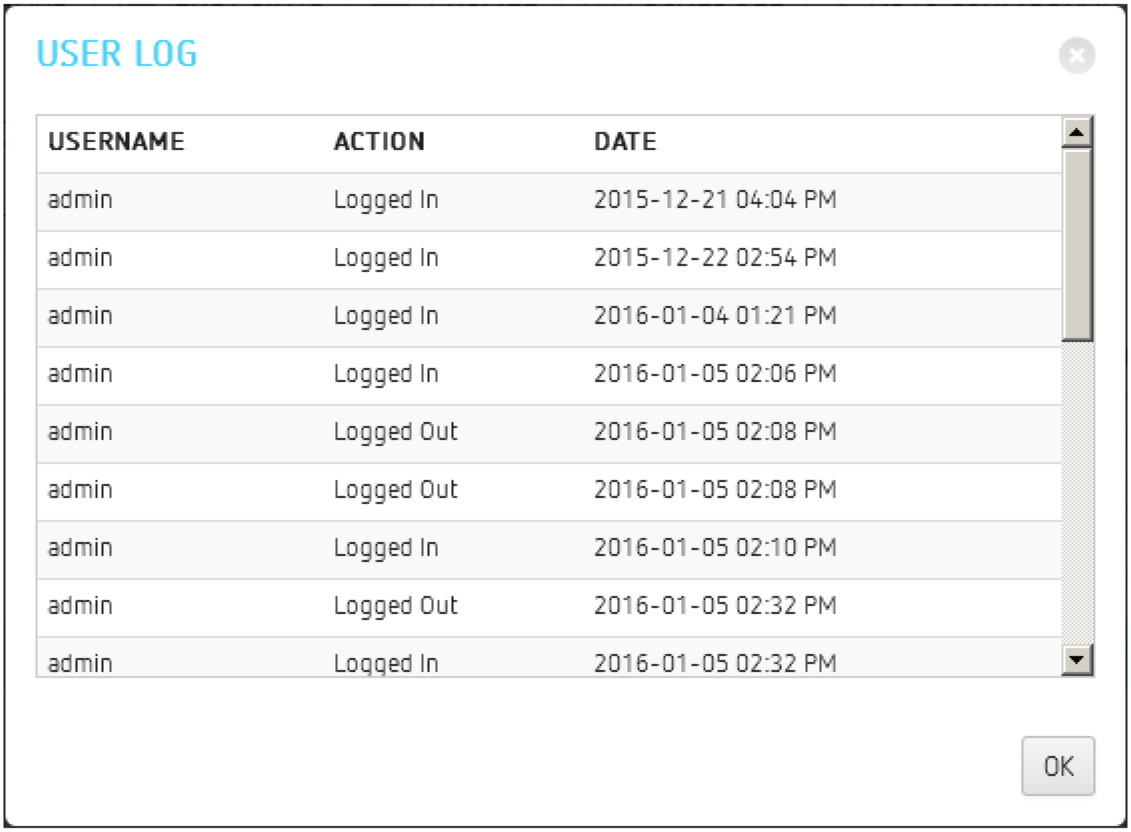
To enable or disable user accounts in PCoIP Management Console Enterprise:

1. From the table on the *MANAGEMENT CONSOLE USERS* page, select one or more users.
   Use `Shift`+Click to select contiguous elements and `Ctrl`+Click to select non-contiguous elements.
2. 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:



USER LOG

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

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.

Note: Release version can be viewed on dashboard
The PCoIP Management Console 2 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.<*date*>**: 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 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.

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’s daemon process has two log levels that you can set:

- **Info**: Logs informational messages and events at a coarse-grained level.
- **Trace**: Logs finer-grained informational messages and events.

Managing PCoIP Management Console Certificates

This section contains information on how to manage your PCoIP Management Consolecertificates, including custom certificate requirements, creation, upload, update, and general management of certificates.

Important: Generate your own custom certificate
The PCoIP Management Console is shipped with a default Teradici self-signed certificate. Teradici strongly recommends 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.

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.
  - The second file contains only the PCoIP Management Console certificate’s private key.
  - The third file contains the PCoIP Management Console certificate’s issuing chain (intermediate CAs, if applicable, and 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.

- The PCoIP Management Console 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.
- The certificate must have an entire verifiable chain. Any certificate used to sign the leaf certificate must be present in the chain.

Creating and Preparing Your Own PCoIP Management Console Certificate

This section demonstrates how to create and submit your own certificate using OpenSSL and your own CA.

Note: 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** and confirm the following information:

Step 2: Connect and Enable SSH to Create Your Certificate

Note: vSphere needed to connect and enable SSH for version 2.1 and higher

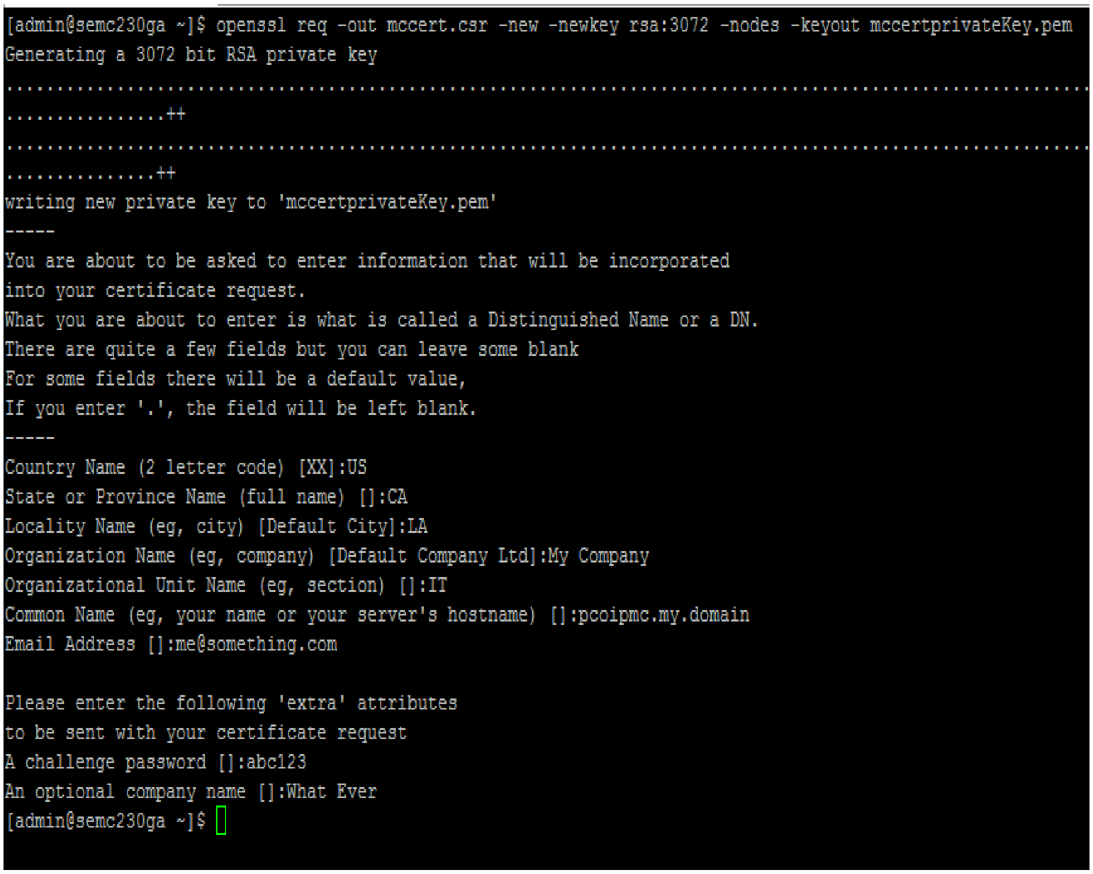
vSphere is needed to enabled SSH in PCoIP Management Console 2.1 and newer. See *Accessing the PCoIP Management Console Virtual Machine Console* on page 38.

Note: Run OpenSSL on a 'Trusted' computer

OpenSSL can be run on any 'Trusted' computer.

To create your certificate:

1. SSH into the PCoIP Management Console 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 privateKey.pem
3. You will get the following response and be asked a series of questions, as shown next:



```
[admin@semc230ga ~]$ openssl req -out mccert.csr -new -newkey rsa:3072 -nodes -keyout mccertprivateKey.pem
Generating a 3072 bit RSA private key
...........................................................................................................
...............++
...........................................................................................................
..............++
writing new private key to 'mccertprivateKey.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 ~]$
```

4. 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 - *se-pcoip-mc-200*)
- **Email Address:** you@yourcompany.com
- **A challenge password:** Your password
- **An optional company name:** Optional

5. Press `Enter`.
6. Two files will be generated in the admin folder: **privateKey.pem** and **CSR.csr**.

Step 3: Submit Your Certificate

To submit your certificate:

1. Using a file management tool of your choice, copy the two files off of your PCoIP Management Console.
2. Take the generated **CSR.csr** and send it to your CA (https://mycertserver.mydomain.local/certsrv).
3. Select **Request a Certificate**.
4. Select **Advanced Certificate Request**.
5. Copy the **CSR.csr** certificate and send it to the CA. The content will be Base-64 encoded.

Note: Using text editor to copy the Certificate Signing Request
You can rename **CSR.csr** to **CSR.csr.txt** to open it in Notepad and copy the content.

6. For *Certificate Template*, select **Web Server**.
7. Do not add anything in the attributes box.
8. Click **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. However, do *not* download the certificate chain as it is still in the wrong format. The certificate will show up as **certnew.cer**.
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.

4. Create a new certificate called **chain.pem** by combining the contents of **certnew.pem** with **CA.pem**.

   Note: Using Notepad to combine the certificates
   You can create text file of each certificate to help combine the two certificates. To edit certificates, change their extension to **.txt**. Teradici recommends creating a new file with **.txt** extension. Place the **CA.pem** content under the **certnew.pem** content in the combined certificate.

5. Rename the combine certificate back to **.pem**. All certificates must be in **.pem** format before uploading into the PCoIP Management Console.
6. Now, you will have three certificates:

   certnew.pem: The certificate returned from the CA
   privateKey.pem: The certificate from the Linux command
   chain.pem: The combination of **certnew.pem** and **CA.pem**

   Note: CA.pem is not uploaded into the PCoIP Management Console
   The **CA.pem** creates the chain certificate (**chain.pem**). While uploading **CA.pem** into PCoIP Management Console is not required, ensure its content is correct.

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* on page 145 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.
- **PCoIP Management Console server's private key certificate** (***.pem**): Contains the private key.
- **PCoIP Management Console chain certificate** (***.pem**): Contains the root certificate and any intermediate certificates used to issue PCoIP Management Console server certificates.

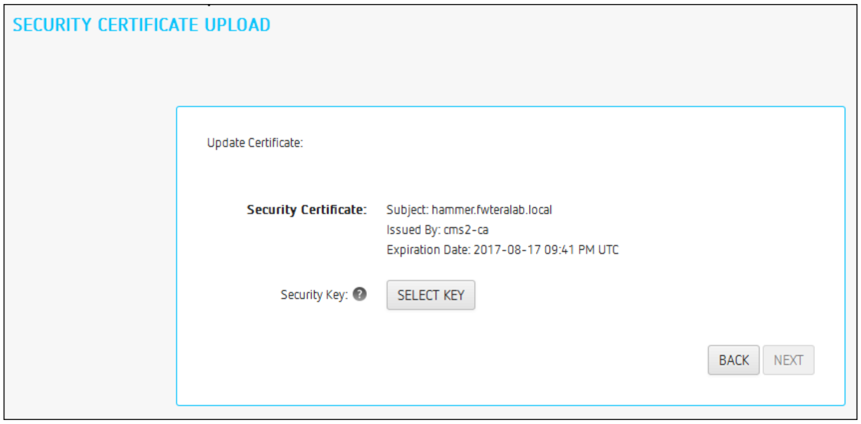
Step 1: Upload Your PCoIP Management Console Certificates to the PCoIP Management Console

Note: Uploading with disable users and cause application to restart
Uploading a 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 upload your certificates to the PCoIP Management Console:

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 key certificate file (***.pem**), and then click **NEXT**.

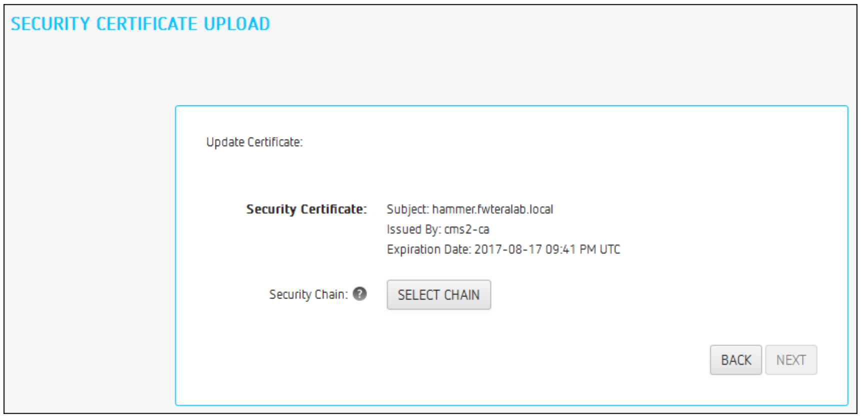

SECURITY CERTIFICATE UPLOAD

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 key certificate file (***.key**), and then click **NEXT**.

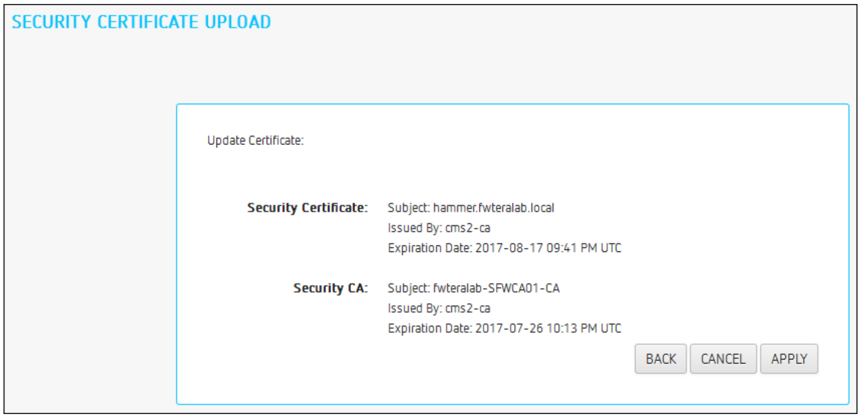

SECURITY CERTIFICATE UPLOAD

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 (***.pem**), and then click **NEXT**.

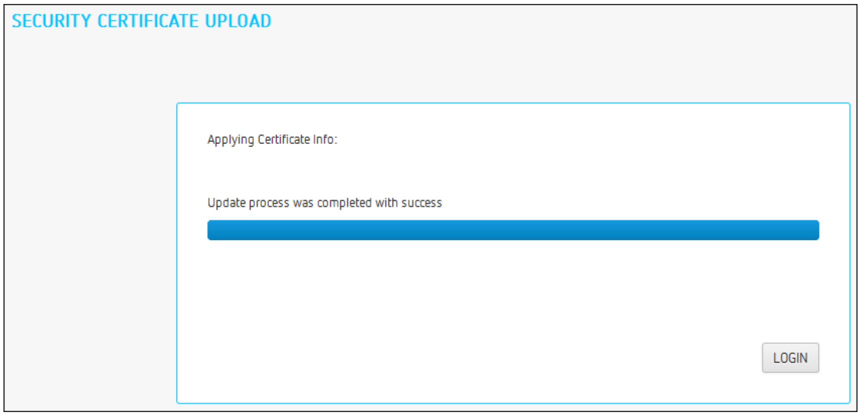

SECURITY CERTIFICATE UPLOAD

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**.



SECURITY CERTIFICATE UPLOAD

Applying Certificate Info:

Update process was completed with success

9. When the update process completes, click **LOGIN** to log in to the PCoIP Management Console again.

Step 2: Update Your DHCP/DNS Server with the PCoIP Management Console Server's Public Key Certificate Fingerprint

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* on page 71.
- **DNS server**: Edit the **EBM-SHA-256-fingerprint** DNS text record. For details, see *Adding a DNS TXT Record* on page 78.

Step 3: Upload a 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.

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 install the PCoIP Management Console certificate in a browser? (KB 15134-3043).

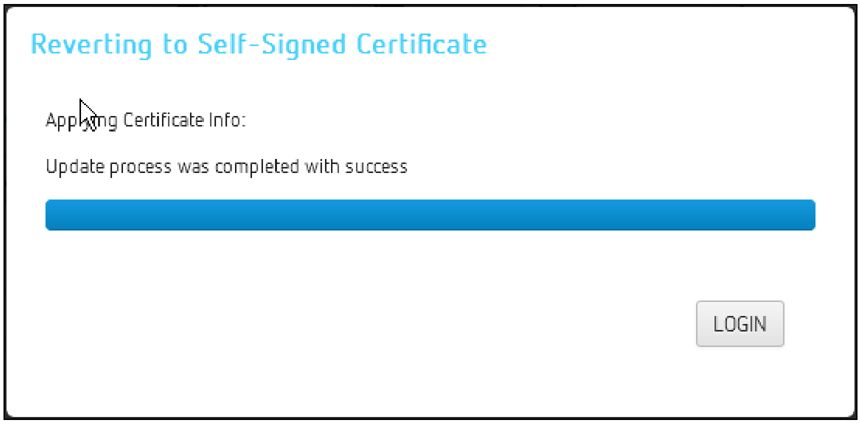
Reverting to the Default Self-signed PCoIP Management Console Certificate

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**.



Reverting to Self-Signed Certificate

Applying Certificate Info:

Update process was completed with success

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 2 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

To update endpoints with the new PCoIP Management Console certificate:

1. Ensure that all ungrouped endpoints are moved from the ungrouped category into a group.
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. From the profile table, select the profile and click **EDIT**.
    c. Click the profile's device type tab.
    d. In the *SOFTWARE* section, ensure that the right firmware version is selected for your endpoints.
    e. Click **SECURITY** in the left navigation pane, scroll down to **Certificate Store**, and select **Set in Profile**.
    f. Click **Add New**, select your new PCoIP Management Console public key certificate, and click **Open**.
    This certificate must have a **.pem** extension.
    g. Click **Upload**.
    h. Click **SAVE** at the top of the page.
    i. Click **PROFILE** in the navigation link at the top to return to the main page.

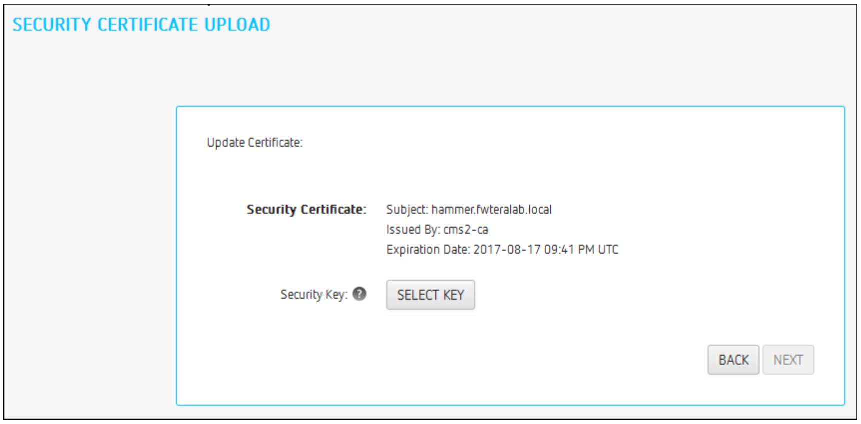
4. Apply the profile immediately or create a schedule to update your group(s) with the profile.

Step 2: Upload the New PCoIP Management Console Certificate to the PCoIP Management Console

To upload the new PCoIP Management Console to the PCoIP Management Console:

Note: Uploading disables users and causes application to restart
Uploading a 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.

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 key certificate file (***.pem**), and then click **NEXT**.

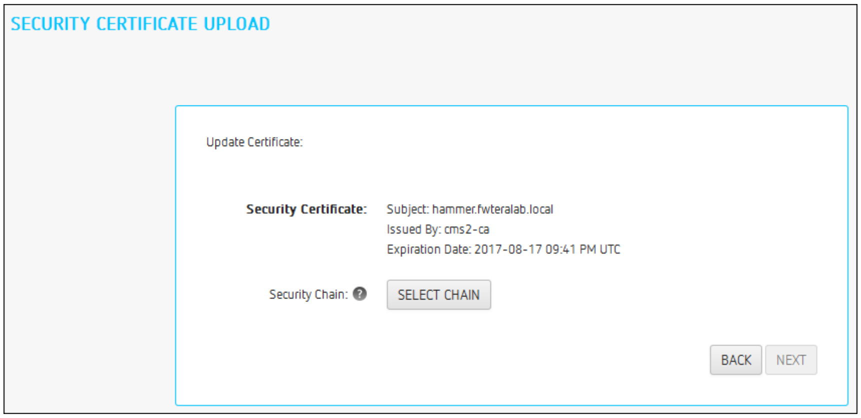


SECURITY CERTIFICATE UPLOAD

Update Certificate:

Security Certificate: Subject: hammer.fwteralab.local
Issued By: cms2-ca
Expiration Date: 2017-08-17 09:41 PM UTC

5. Click **SELECT KEY**, select the PCoIP Management Console's private key certificate file (***.key**), and then click **NEXT**.



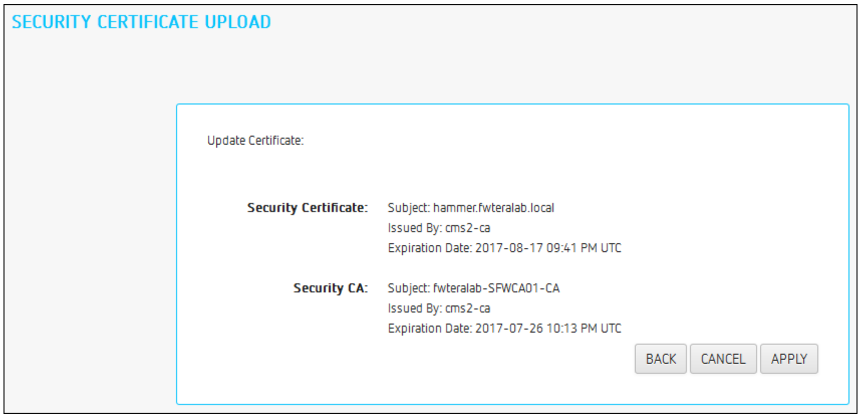
SECURITY CERTIFICATE UPLOAD

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 (***.pem**), and then click **NEXT**.



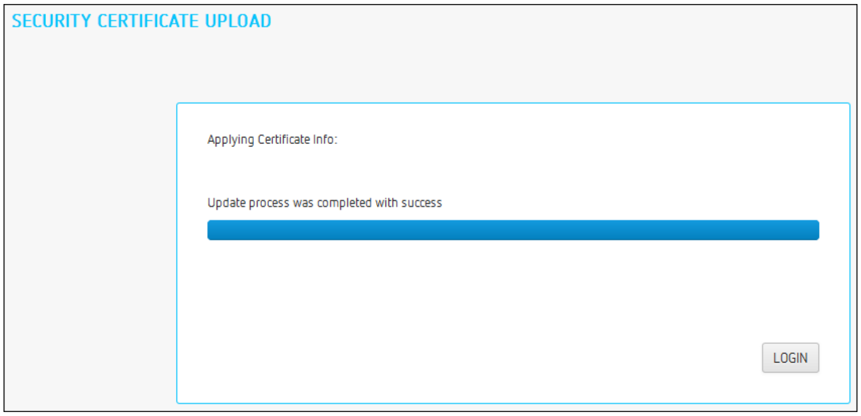
SECURITY CERTIFICATE UPLOAD

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**.



SECURITY CERTIFICATE UPLOAD

Applying Certificate Info:

Update process was completed with success

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* on page 71.
- **DNS server**: Edit the **EBM-SHA-256-fingerprint** DNS text record. For details, see *Adding a DNS TXT Record* on page 78.

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 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.

For information on PCoIP Management Console certificates, see *Managing PCoIP Management Console Certificates* on page 136.

Upgrading Endpoint PCoIP Management Console Certificates Using PCoIP Management Console

Note: All certificates should be in PEM format

All PCoIP Management Console certificates must be issued in PEM format.

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

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.
2. From the PCoIP Management Console home page, click the **PROFILES** tab.
3. Click **Add New**.
4. Enter a name and description and then click **Save**.
5. In the **Profile Management** page, click the profile's **Set Properties** link.
6. Scroll down to the profile's **Certificate Store** section and click **Add New**.
7. Click **Browse**, select your PCoIP Management Console certificate file (***.pem**), and then click **Add**.
8. From the main menu, click the **GROUPS** tab.
9. In the **Group Management** page, click the **Edit** link for group containing your endpoints.
10. Select the profile you created in the **Profile** drop-down list and click **Save**.
11. Click the **Apply Profile** link for the group containing your endpoints.
12. Enter the date and time to apply your profile in the **Apply Profile at Date/Time** text box and then click **OK**.

Upgrading the PCoIP Management Console Certificate Using the Endpoint's AWI

To update the PCoIP Management Console certificate 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 > Certificate** menu.
3. From the **Certificate Upload** page, browse to the folder containing the PCoIP Management Console certificate file (***.pem**).
4. Double-click the file and then click **Upload**.
5. Click **OK** and then **Continue**.

For more information about the AWI, see *Tera2 PCoIP Zero Client Firmware 4.x and Remote Workstation Card Firmware 4.9 Administrators' Guide* (for endpoints prior to firmware version 5.0) or *Tera2 PCoIP Zero Client Firmware Administrators' Guide* (for Tera2 PCoIP Zero Clients running firmware version 5.0 or later).

Configuring PCoIP Management Console Settings

This section provides an overview of how to configure PCoIP Management Console. Configuration requires that you are familiar with *Accessing the PCoIP Management Console Virtual Machine Console* on page 38

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 in its own tab on the settings security page. Once a period of inactivity reaches the set time, the administrator will be logged out of PCoIP Management Console Enterprise.

Configuring Your 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 **USERS** 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 *Securing the PCoIP Management Console*.

Default PCoIP Management Console CentOS Configuration

Configuration	Description
Installed packages	The following applications have been installed on the CentOS operating system for PCoIP Management Console: • Text editors (from the CentOS project): nano, vim • Wget, unzip, man, gcc, patch, python-argparse, redhat-lsb, sshpass, nmtui • Python (from the Python project) • Java Platform: OpenJDK configured with weak ciphers and hashes disabled • Jetty (from the Jetty project) • PostgreSQL (from the PostgreSQL project) • VMware Tools (from VMware) • FlexNet Publisher and Java tools (from Flexera)

Configuration	Description
PCoIP Management Console users	**Note: Root user is not used for PCoIP Management Console administration** 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. The following PCoIP Management Console virtual machine users are created by default: • **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. • **jetty**: No login shell; can use restricted **sudo** to manage PCoIP Management Console web UI components; has no password. • **mcdaemon**: No login shell; has no password. • **postgres**: Has login shell due to PostgreSQL limitations; has no password.
Security	Security-Enhanced Linux (SELinux) is enabled with a default configuration.
	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. **Note: SSH access for the admin user** Although the PCoIP Management Console permits you to re-enable the SSH server (temporarily or permanently), for security reasons it only allows SSH access for the **admin** user while the SSH server is enabled.
	Default firewall port settings are as follows: • 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.

Configuration	Description
Open file limit	The maximum number of open files for all OS processes is 65,535.
IPv6	IPv6 is disabled.
PCoIP Management Console directories and scripts	The following scripts and files are included on the PCoIP Management Console virtual machine: **/opt/teradici** • ***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. • **port80_disable.sh**: Disables the PCoIP Management Console's HTTP port (port 80). • **port80_enable.sh**: Enables the PCoIP Management Console's HTTP port (port 80). • **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. **/opt/teradici/database/legacy/migration_script** • ***migrate_mc1_profile.sh***: Imports individual PCoIP Management Console 1 profiles into your PCoIP Management Console release 2 or newer. **/opt/teradici/log** • Contains *PCoIP Management Console console and daemon log files*.

Changing the Default Network Configuration

The PCoIP Management Console virtual machine includes a network configuration tool called NetworkManager TUI (textual user interface) that lets you change the PCoIP Management Console's default network configuration. You can use this tool to assign a static IP address to the PCoIP Management Console. Do **NOT** modify the DNS configuration with this tool.

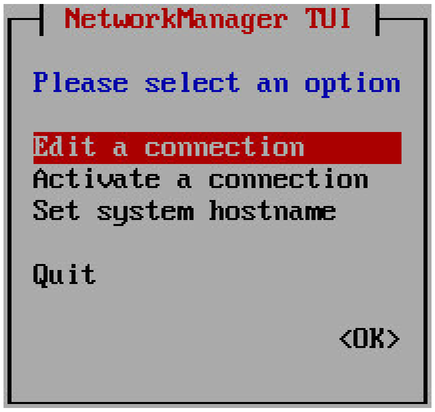
Tip: Ensure you have correct DNS A and DNS PTR records set
Before you run the Network Configuration Tool, be sure to set the correct DNS A record and DNS PTR record in your DNS server for the PCoIP Management Console. If the records are already set, ensure you use the same IP address associated with the DNS records.

Note: Give PCoIP Management Console a fixed IP address
Teradici recommends that you give the PCoIP Management Console a fixed "static" IP address, either through a DHCP reservation or by *Assigning a Static IP Address* on page 155 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:

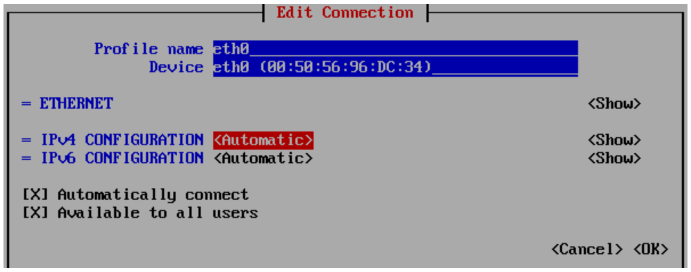
1. Log in to the PCoIP Management Console virtual machine console. For instructions, see *Accessing the PCoIP Management Console Virtual Machine Console* on page 38.
2. Type the following command at the command line to launch the network configuration tool:
`sudo nmtui`



```
NetworkManager TUI

Please select an option

Edit a connection
Activate a connection
Set system hostname

Quit

                  <OK>
```

Network Manager Configuration Tool

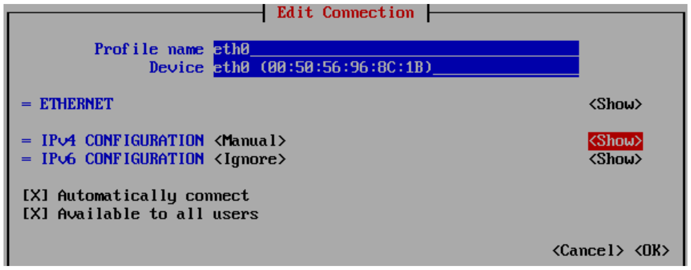
Info: Default configuration
The default configuration for IPv4 is DHCP based, identified by <Automatic>.



```
                      ┤ Edit Connection ├

          Profile name eth0_________________________________
                Device eth0 (00:50:56:96:DC:34)_____________

 = ETHERNET                                               <Show>

 = IPv4 CONFIGURATION <Automatic>                         <Show>
 = IPv6 CONFIGURATION <Automatic>                         <Show>

 [X] Automatically connect
 [X] Available to all users

                                                    <Cancel> <OK>
```

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 **<Show>** to access additional configurable elements.



```
                      ┤ Edit Connection ├

          Profile name eth0_________________________________
                Device eth0 (00:50:56:96:8C:1B)_____________

 = ETHERNET                                               <Show>

 = IPv4 CONFIGURATION <Manual>                            <Show>
 = IPv6 CONFIGURATION <Ignore>                            <Show>

 [X] Automatically connect
 [X] Available to all users

                                                    <Cancel> <OK>
```

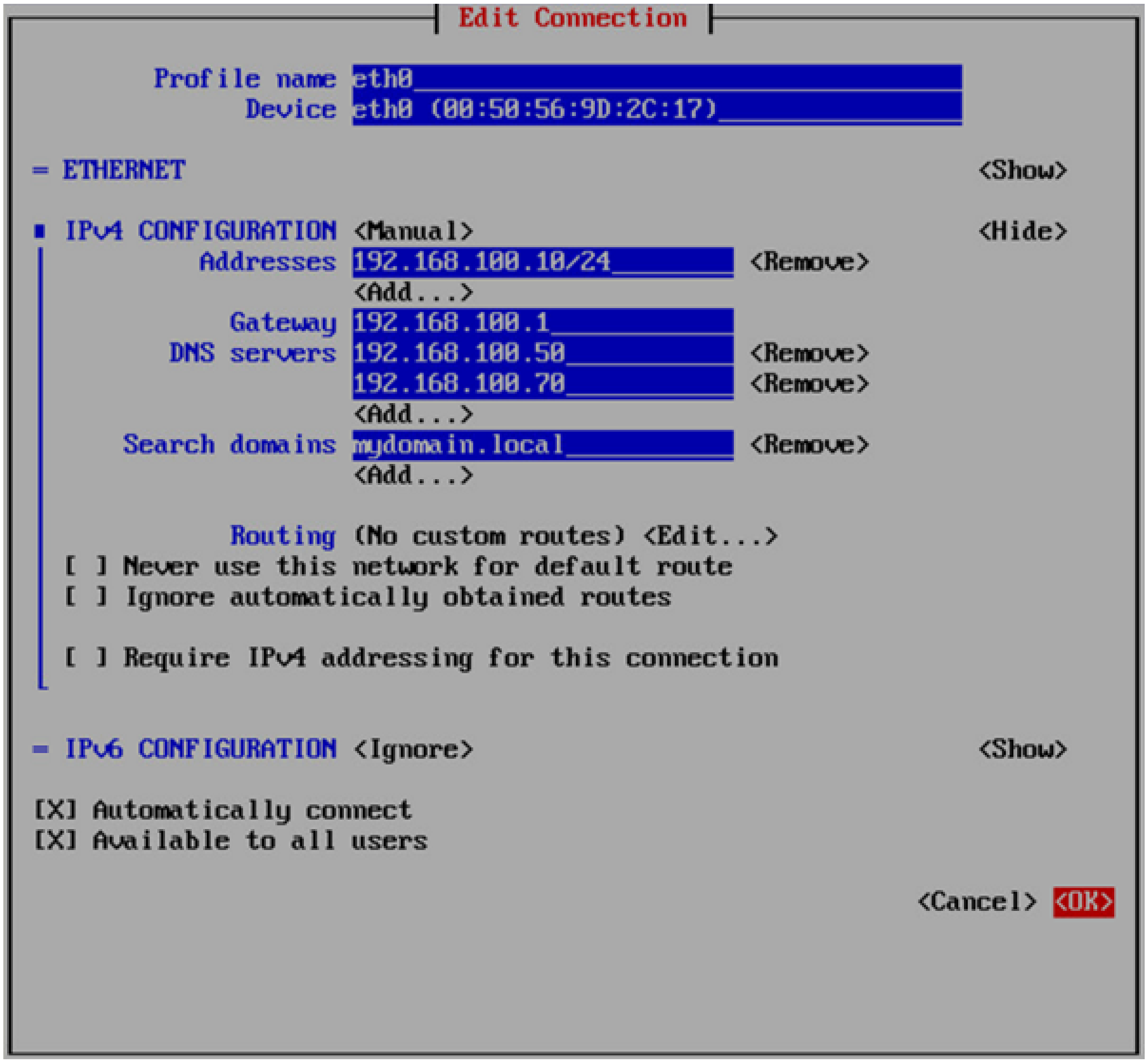
Assigning a Static IP Address

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.
2. Select **Edit a connection**.
3. Select **eth0** then tab and select **<Edit...>**.

4. Tab to **<Show>** to access and configure your IPv4 parameters:
   - **IPv4 CONFIGURATION**: Set to **Manual** for a static IP configuration.
   - **Addresses:** Enter the IP address you selected for your Management Console.
   - **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.
5. Tab to **IPv6 CONFIGURATION** and change automatic to **Ignore**.
6. Tab to **<OK>** and press `Enter`.
7. Tab to **<Back>** and press `Enter` to get to the main screen of the network configuration tool.
8. To have the settings take affect immediately, type the following command from the CentOS command line:
   ```
   sudo systemctl restart network
   ```

Note: Shown next are example IP addresses
The IP addresses shown next are for example purposes only. Enter your own information.



```
                      ┤ 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>

[X] Automatically connect
[X] Available to all users

                                                   <Cancel> <OK>
```

Configuring an Endpoint Manager Manually from an Endpoint

For environments that do not use automatic DHCP or DNS discovery, you can manually configure each 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. SeePCoIP Management Console *Discovering Endpoints Manually from PCoIP Management Console* on page 115.

This example shows how to configure a 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 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 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 - 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.

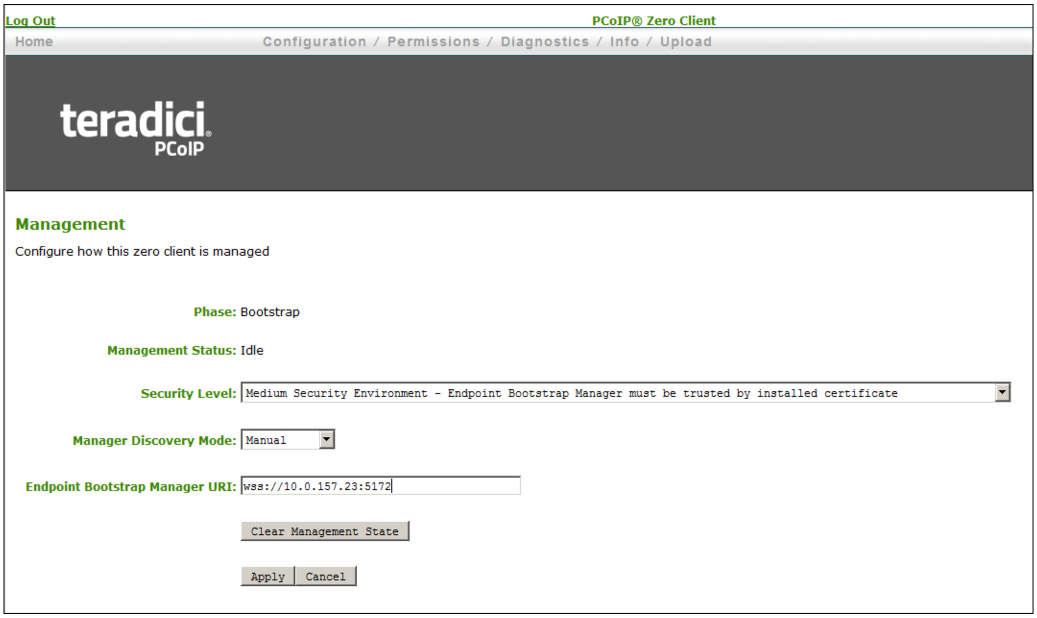
   - **Medium Security Environment - Endpoint Bootstrap Manager must be trusted by installed certificate**: When this security level is selected, the endpoint must have a trusted PCoIP Management Console certificate in its certificate store in order for discovery to succeed. The certificate can be provisioned 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* on page 148.

- **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.

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.



Management

Configure how this zero client is managed

Phase: Bootstrap

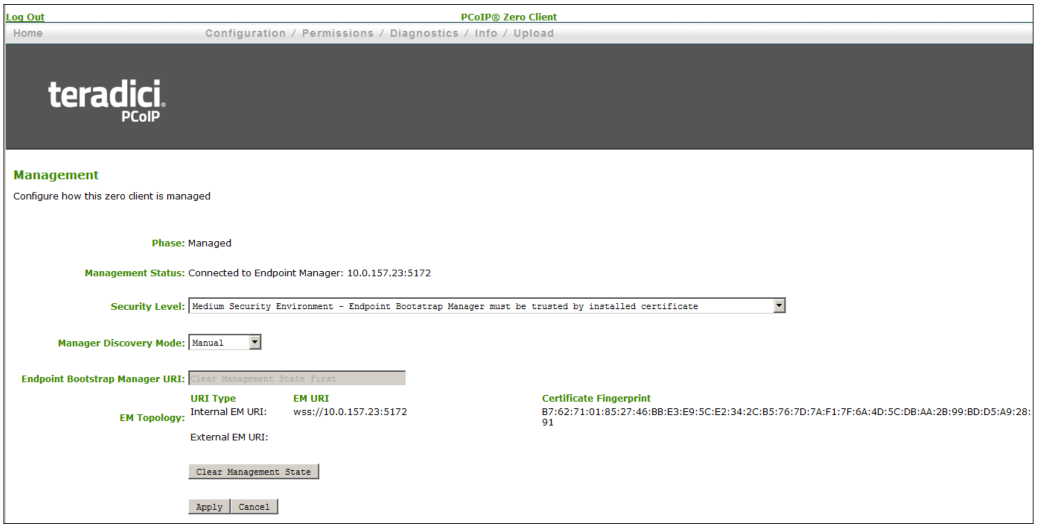
Management Status: Idle

Security Level: Medium Security Environment - Endpoint Bootstrap Manager must be trusted by installed certificate

Manager Discovery Mode: Manual

Endpoint Bootstrap Manager URI: wss://10.0.157.23:5172

7. Click **Apply** and then **Continue** once more.
   If discovery succeeds, the endpoint's **Management** page will show the following information:



Management

Configure how this zero client is managed

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: Clear Management State First

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:		

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* on page 94 and *Auto Configuring Endpoints (Enterprise)* on page 91 for details.

Managing PCoIP Management Console Databases

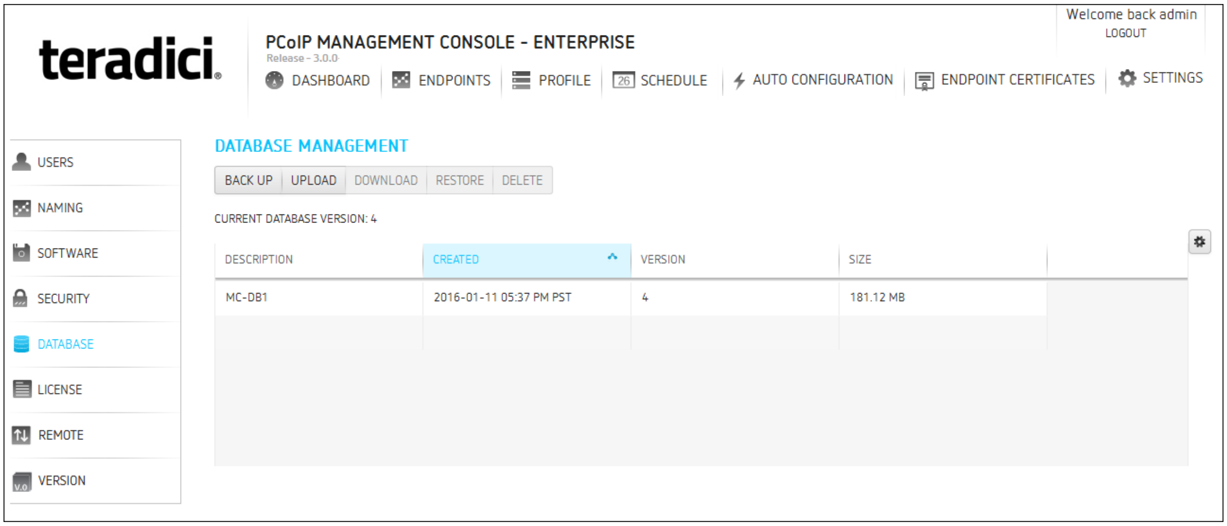
The PCoIP Management Console maintains a database containing its configuration data, information about the PCoIP endpoints it has discovered, and console and daemon log files. You can archive multiple snapshots of these PCoIP Management Console database settings and store them on your PCoIP Management 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.

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.

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.



CURRENT DATABASE VERSION: 4

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 Settings to the PCoIP Management Console Virtual Machine

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 and click **BACK UP**. 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 a Database Archive from the PCoIP Management Console Virtual Machine

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 a Database Archive from the PCoIP Management Console Virtual Machine

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**: 7
- **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. Teradici 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.

Disk Sizing Guidelines for Larger Deployment

The following table contains sizing guidelines based on working with deployments from 1,500 to 20,000 endpoints.

Note: The following are recommendations only
Your environment may require different configurations based on the ESXi environment you are using.

Disk Sizing Recommended Sizing Guidelines Table

Deployment Size	Virtual Machine Hardware Version	CPU	Memory	Provisioned Storage
1500 - 5000 endpoints	7 to 11	4 x vCPU	8192 MB	30 GB
5000 - 10,000 endpoints	7 to 11	4 x vCPU	12 GB	60 GB
10,000 - 15,000 endpoints	7 to 11	4 x vCPU	12 GB	100 GB
15,000 - 20,000 endpoints	7 to 11	4 x vCPU	12 GB	130 GB

Note: Keep logging level set to *Info*

The PCoIP Management Console by default has its logging level set to *Info*. If changed to *Trace*, the amount of logging information will increase significantly. Teradici recommends leaving the logging level of the PCoIP Management Console set to *Info* unless you are actively investigating an issue with the PCoIP Management Console where additional logging information is required.

Appendix A: Troubleshooting DNS

This appendix 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 **_bootstrap-pcoip** 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
- 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

Appendix B: PCoIP Management Console 1 Profile Properties Renamed or Not Migrated

The following table lists PCoIP Management Console 1 profile properties that have been renamed in PCoIP Management Console release 2 or newer and are not migrated when you import a PCoIP Management Console 1 profile to a PCoIP Management Console release 2 or newer.

Reference to PCoIP Management Console refer to releases 2.0 or newer, 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	Release 2+ Category	Release 2+ 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**.

Release 1 Category	Release 1 Property Name	Release 2+ Category	Release 2+ Property Name	Migration Notes
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 Static IP Fallback** 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 Static IP Fallback** 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 Static IP Fallback** is not **Set in Profile** or is set to **False**.

Release 1 Category	Release 1 Property Name	Release 2+ Category	Release 2+ Property Name	Migration Notes
Network Configuration	Static Fallback Timeout	Network	Static Fallback IPv4 Timeout	Not migrated when PCoIP Management Console 1 property **Network Configuration > Enable Static IP Fallback** is not **Set in Profile** or is set to **False**.
Discovery Configuration	PCoIP Management Console DNS-Based Discovery Prefix			Never migrated. Not used in firwmare 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: • **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**.
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: • **View Connection Server + Auto-Logon** • **PCoIP Connection Manager + Auto-Logon**

Release 1 Category	Release 1 Property Name	Release 2+ Category	Release 2+ Property Name	Migration Notes
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: - **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: - **View Connection Server + Auto-Logon** - **PCoIP Connection Manager + Auto-Logon**
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**.

Release 1 Category	Release 1 Property Name	Release 2+ Category	Release 2+ Property Name	Migration Notes
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-Round12 Encryption			Never migrated. Applies to Tera1 endpoints only.
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	

Release 1 Category	Release 1 Property Name	Release 2+ Category	Release 2+ Property Name	Migration Notes
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 *Appendix C: Time Zone Definitions for PCoIP Management Console 1 and newer releases* on page 179.
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	

Release 1 Category	Release 1 Property Name	Release 2+ Category	Release 2+ Property Name	Migration Notes
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			Never migrated. Currently not included in PCoIP Management Console.
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 Permissions	Audio Out Preferred USB 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 Mode	Power	Power On After Power Loss	

Release 1 Category	Release 1 Property Name	Release 2+ Category	Release 2+ Property Name	Migration Notes
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 Configuration	Enable USB EHCI	Peripheral	EHCI	
Peripheral Configuration	Force Local Cursor Visible			Never migrated. Currently not included in PCoIP Management Console.
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**.

Release 1 Category	Release 1 Property Name	Release 2+ Category	Release 2+ Property Name	Migration Notes
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	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 Primary DNS Address & IPv6 Primary DNS Address Prefix Length	Network	Primary IPv6 DNS	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 Secondary DNS Address & IPv6 Secondary DNS Address Prefix Length	Network	Secondary IPv6 DNS	Not migrated when PCoIP Management Console 1 property **IPv6 Configuration > Enable IPv6** is not **Set in Profile** or is set to **False**.
SCEP Configuration	SCEP Server URI			Never migrated. Currently not included in PCoIP Management Console.
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.

Release 1 Category	Release 1 Property Name	Release 2+ Category	Release 2+ Property Name	Migration Notes
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**.
Display Topology Configuration (Dual and Quad)	Resolution	Session > Display Configuration: Dual/Quad Display Topology	Resolution	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.

Release 1 Category	Release 1 Property Name	Release 2+ Category	Release 2+ Property Name	Migration Notes
Profile Firmware		Software	Firmware Version	Never migrated. For the Tera2 PCoIP Zero Client, all migrated profiles are assigned to a zero client.

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.

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 newer releases of PCoIP Management Console.
IPv6 Address Resolution	4.8.0	Not managed by PCoIP Management Console 1.x or newer releases of PCoIP Management Console.
OSD Region Tab Lockout	5.0.0	Never managed by PCoIP Management Console 1.x.

Appendix C: Time Zone Definitions for PCoIP Management Console 1 and newer releases

Reference to PCoIP Management Console refer to releases 2.0 or newer, 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: Endpoints use IANA time zone definitions as of zero point firmware 5.0.0
As of firmware 5.0.0, Tera2 PCoIP Zero Client endpoints also use IANA time zone definitions for setting the endpoint's local time. If endpoints are downgraded from firmware 5.0 or later to a version older than 5.0.0, the older Windows time zones will be used, and the endpoint's local time setting will revert to **(GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London**. To reset the local time, you can use PCoIP Management Console 1.x to configure a group of endpoints, or you can use an individual endpoint's AWI to manually configure its local time.

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

PCoIP Management Console 1 Time Zone Definition	PCoIP Management Console Time Zone Definition
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
gmt_minus_0200_mid_atlantic	Atlantic/South_Georgia
gmt_minus_0100_azores	Atlantic/Azores

PCoIP Management Console 1 Time Zone Definition	PCoIP Management Console Time Zone Definition
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
gmt_plus_0430_kabul	Asia/Kabul

PCoIP Management Console 1 Time Zone Definition	PCoIP Management Console Time Zone Definition
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