PCoIP Remote Workstation Card Overview

This guide is intended for systems administrators who are configuring, managing, and deploying Teradici PCoIP® Remote Workstation Cards in a PCoIP environment. Administrators are expected to have experience configuring PCoIP clients, and have a working knowledge of networking principals and using the PCoIP protocol.

> ✏️ **Understanding terms in Teradici guides**
>
> For information on the industry specific terms and abbreviations in this guide, see the Teradici Glossary.

A PCoIP Remote Workstation Card is a small add-in card that can be integrated into tower workstations, rack mount workstations, computer blades, and server blades. PCoIP Remote Workstation Cards are manufactured and integrated by various display card manufacturers, supporting widescreen formats, and are powered by TERA2220 or TERA2240 processors. The card's TERA-series processor uses advanced display compression algorithms to encode a user's full workstation environment and then communicated over an IP network to the user's PCoIP client endpoint. Because PCoIP Remote Workstation Cards do not have general purpose CPUs, local data storage, or application operating systems, they are very secure and easy to manage. This is separate from the host PC which does have general purpose CPUs and local data storage. PCoIP Remote Workstation Cards contain upgradable firmware that enables you to customize your PCoIP Remote Workstation Card with various features.

> ✏️ **Teradici processor**
>
> The processor name refers to the chipset used in the PCoIP device. For example, TERA2240 is the processor used in the second-generation TERA2240 PCIe Remote Workstation Card (for tower PC or rack mount workstations) and TERA2240 PCI Mezzanine Remote Workstation Card (for blade workstations). For details on how to display the processor name for your device, see Displaying Processor Information.

Supported Resolutions for PCoIP Remote Workstation Cards

Remote Workstation Card Processor Name	Maximum No. of Supported Displays and Resolutions
TERA2220	2 x 1920x1200 1 x 2560x1600 [1] 1 x 3840x2160 [2]
TERA2240	4 x 1920x1200 2 x 2560x1600 [1] 2 x 3840x2160 [2]

You can mix and match any Remote Workstation Card with any PCoIP Zero Client. However, when you connect a PCoIP Zero Client endpoint to a Remote Workstation Card, the maximum supported resolutions for any displays attached to the endpoint will equal the highest common denominator between the two devices. For example, if you connect a TERA2140 PCoIP Zero Client to a TERA2240 Remote Workstation Card, you can attach up to four 1920x1200 displays or two 3840x2160 displays. However, if you connect a TERA2321 PCoIP Zero Client to the same Remote Workstation Card, the options become up to two 1920x1200 displays or one 3840x2160 display.

Teradici Software Clients and PCoIP enabled thin clients also offer alternative client endpoints to connect to Remote Workstation Cards.

> ⚠️ **Best Security Practices**
>
> Teradici highly recommends using custom peer-to-peer certificates to create a more secure environment when connecting to your Remote Workstation Card. Teradici highly recommends using this new feature to create a more secure environment. Contact your IT department to ensure your deployment is in accordance with your Company's security policy.

Platforms

Remote Workstation Cards are supported on host PCs using Windows or Linux platforms when the host PC supports PCIe x1 required to install the PCoIP Remote Workstation Card. Additionally, Teradici provides an optional software package that can be installed on the host PC. The software package called Remote Workstation Card Software for Windows (and Linux) is specific to each platform and communicates with the Remote Workstation Card adding additional features and performance enhancements. For more information on the Remote Workstation Card Software see

PCoIP® Remote Workstation Card Software for Linux Administrators' Guide and "PCoIP® Remote Workstation Card Software for Windows Administrators' Guide.

> 🔥 **Remote Workstation Card Software and Firmware features**
>
> Some features of the Remote Workstation Card Software may require a minimum firmware version on the PCoIP Remote Workstation Card and the PCoIP Zero Client. Always review the release notes for feature requirements.

> 🔥 **Wacom Tablets on Host PCs**
>
> Wacom tablets are supported when connecting to Remote Workstation Cards using a PCoIP Zero Client with an attached Wacom tablet. Use the latest release of your Zero Client firmware, for the most up to date support of Wacom tablets. Some PCoIP enabled thin clients also support Wacom tablets. Check with your PCoIP enabled thin client manufacturer if they support Wacom tablets with PCoIP. It is recommended to use the latest release of Remote Workstation Card Software for Windows (or Linux) to maintain local cursor support on the client side, and to have best performance in sessions with the Remote Workstation Card when the latest Wacom drivers are used.

Host Driver Function

When enabled, the **Host Driver Function** allows the PCoIP Remote Workstation Card Software installed on the host computer to communicate with the PCoIP Remote Workstation Card. This setting is disabled by default. You can enable this setting by logging in to the Remote Workstation Card from the AWI page—**Configuration > Host Driver Function**.

When disabled, you will not be able to access to additional features provided by the Remote Workstation Card Software. If the Host Driver function is disabled:

- the Remote Workstation Card Software for Linux installation will alert you it cannot find a PCoIP Remote Workstation Card

- the Remote Workstation Card Software for Windows will not install

> 🔥 **Identifying PCoIP Remote Workstation Card**
>
> On your Windows host PC, use device manager to see if a PCoIP Remote Workstation Card is installed. This works if the Host Driver Function is enabled. On your Linux host PC, open the command prompt and type `lspci | grep -i tera` to see if a PCoIP Remote Workstation Card is installed.

PCoIP Remote Workstation Card Software for Windows or Linux

Optionally, once the PCoIP Remote Workstation Card is installed in the host PC, you can install the PCoIP Remote Workstation Card Software package on the host PC/workstation to allow you to manage the card directly from the PCoIP Remote Workstation Card Software UI on the workstation. The Remote Workstation Card Software lets users enable features such as the following:

- Using the local cursor and keyboard feature

- Locking the host PC when a session is terminated

- Using the Wake-on-LAN function

- Viewing host and client network parameters

- Disconnecting a session

- Viewing host statistics and connection information

- Using the client display topology settings on the host

For detailed instructions on how to install the PCoIP Remote Workstation Card Software, please see PCoIP® Remote Workstation Card Software for Windows User Guide or PCoIP® Remote Workstation Card Software for Linux User Guide.

> ⚠️ **Host Driver Function must be enabled**
>
> Before installing the Remote Workstation Card Software package for Linux or Windows on the host computer, the **Host Driver Function** must be enabled. This setting is disabled by default.

1. Remote Workstation Cards support 2560x1600 resolution on attached displays using either DVI (with Y-cable) or miniDisplayPort interfaces. For instructions on how to connect cables to Tera2 PCoIP Remote Workstation Cards with DVI and/or DisplayPort ports to support this resolution, see knowledge base article 1025.

2. Remote Workstation Cards support 3840x2160 @ 30 Hz (4K UHD) resolution at 15 FPS when the changing content is full screen. A video that takes up half of the screen can run at 30 FPS.

What's New in 22.04

This release contains security updates and bug fixes.

See Release Notes for further details.

Getting More Information

In addition to this guide, the PCoIP Remote Workstation Card documentation set includes:

- Remote Workstation Card Quick Start Guide

- Remote Workstation Card Firmware Release Notes

- Remote Workstation Card Software for Windows

- Remote Workstation Card Software for Linux

- Remote Workstation Card Agent for Windows

- Remote Workstation Card Agent for Linux

For detailed information on using the PCoIP Management Console to manage deployments, see the Teradici PCoIP® Management Console Administrators' Guide.

For help using and configuring firmware for PCoIP Zero Clients, see PCoIP Zero Client Firmware Administrators' Guide.

For information on installing and configuring additional Remote Workstation Cards and PCoIP Zero Clients so that you can use additional monitors on your desk, see Tera2 PCoIP® Multi-Monitor Deployment Guide.

About the Management Tools

The following configuration and management tools are available for PCoIP Remote Workstation Cards:

- PCoIP Administrative Web Interface (AWI): A web-based interface for configuring a specific PCoIP Remote Workstation Card's firmware remotely after typing the endpoints's IP address or FQDN into the browser's address bar. For more information, see About the PCoIP Administrative Web Interface (AWI).

- PCoIP Endpoint Management Software: A management tool for managing multiple PCoIP endpoints, such as Remote Workstation Cards remotely. Teradici's management software is the **PCoIP Management Console**. For information about the PCoIP Management Console, see the latest PCoIP Management Console Administrators' Guide.

🔥 **Management Console firmware requirements**

Remote Workstation Card firmware management may be limited to specific Management Console releases. Always review the release notes and documentation for each release.

- Firmware release 4.9.x and earlier can only be managed my Management Console 1.10.8

- Firmware 5.x - 19.11 can be managed by Management Console 3.2 - 19.11

- Firmware 20.01+ must be managed by Management Console 20.01+

Please review the lifecycle pages for up-to-date information on the life status and support of Teradici products.

PCoIP Remote Workstation Card Requirements

The PCoIP Remote Workstation Card has few requirements other than being used in a host PC that supports PCIe x1 devices.

Host Requirements

Category	Requirement	Notes
Operating System	Windows or Linux	If using features requiring the Remote Workstation Card Software, the PC must be Windows or Linux based
Hardware Interface	Available PCIe x1	• Quad Remote Workstation Card requires FHHL • Dual Remote Workstation Card requires Low Profile • 13W power
GPU	Video port	At minimum, the same number of ports to match the number of monitors in your deployment (up to 4) Ports must support dual data rates to obtain maximum Remote Workstation Card resolution
	Resolution	GPU must support the resolution used in your deployment (up to 3840x2160 @ 30 Hz)
Video Port Cables	miniDP to DP or miniDP to DVI	High resolution configurations to a GPU with DVI ports may require active cables
Remote Workstation Card Firmware	Matching client release	See release notes for compatible clients

> ⚠️ **Connecting Monitors to your Workstation**
>
> PCoIP sessions to Remote Workstation Cards when monitors are connected on the local workstation are not supported.

4K Requirements

Category	Requirement	Notes
Firmware	4K firmware 20.01 or newer	
Model	Mini DisplayPort model of a quad (TERA2240) or dual (TERA2220) Remote Workstation Card	
GPU	The GPU on the workstation must support 4K UHD	

> 🔥 **Bandwidth, Build to Lossless, and timing behavior**
>
> - For the best user experience, a 1 Gb connection between the client and host is recommended
> - With 4K firmware, the Remote Workstation Card **Build to Lossless** feature is disabled when using 4K resolutions
> - 4K @ 60 Hz timings are not supported. The client will search for a 4K @ 30 Hz timing instead.

Installing Your Remote Workstation Card

Using the PCoIP Remote Workstation Card requires installing the card into a PCIe slot on the host PC motherboard, connecting the Remote Workstation Card to the host PC GPU, and plugging it into a DHCP enabled network with PCoIP clients connected. Optionally, you can connect the PCoIP Remote Workstation Card power cable to the host PC motherboard which allows the host card to turn off and wake the host PC through wake-on-lan. Another option is to install the Remote Workstation Card Software on the host PC to enhance the PCoIP experience when using the PCoIP Remote Workstation Card.

Most PCoIP Remote Workstation Cards come with DHCP enabled and will accept a connection from any client. This allows a PCoIP connection with minimal effort when first connected to a network with PCoIP clients. All that is required is to connect the PCoIP Remote Workstation Card to a network with DHCP enabled via the card's RJ45 connector.

> 🔥 **OEM default settings**
>
> PCoIP Remote Workstation Cards default settings can be changed by OEM manufacturers. Reference your OEM documentation to ensure a smooth deployment.

> 🔥 **MAC Address**
>
> The PCoIP Remote Workstation Card's MAC address is located on a sticker on the card. It is important to write down this address before installing the card in the workstation. see KB 1360 in the Teradici Support Site for additional information. You will need this information to connect to the card using SLP discovery.

Ensure the host PC is completely powered off before installing the PCoIP Remote Workstation Card to the host PC and connecting the optional PCoIP Remote Workstation Card remote power cable.
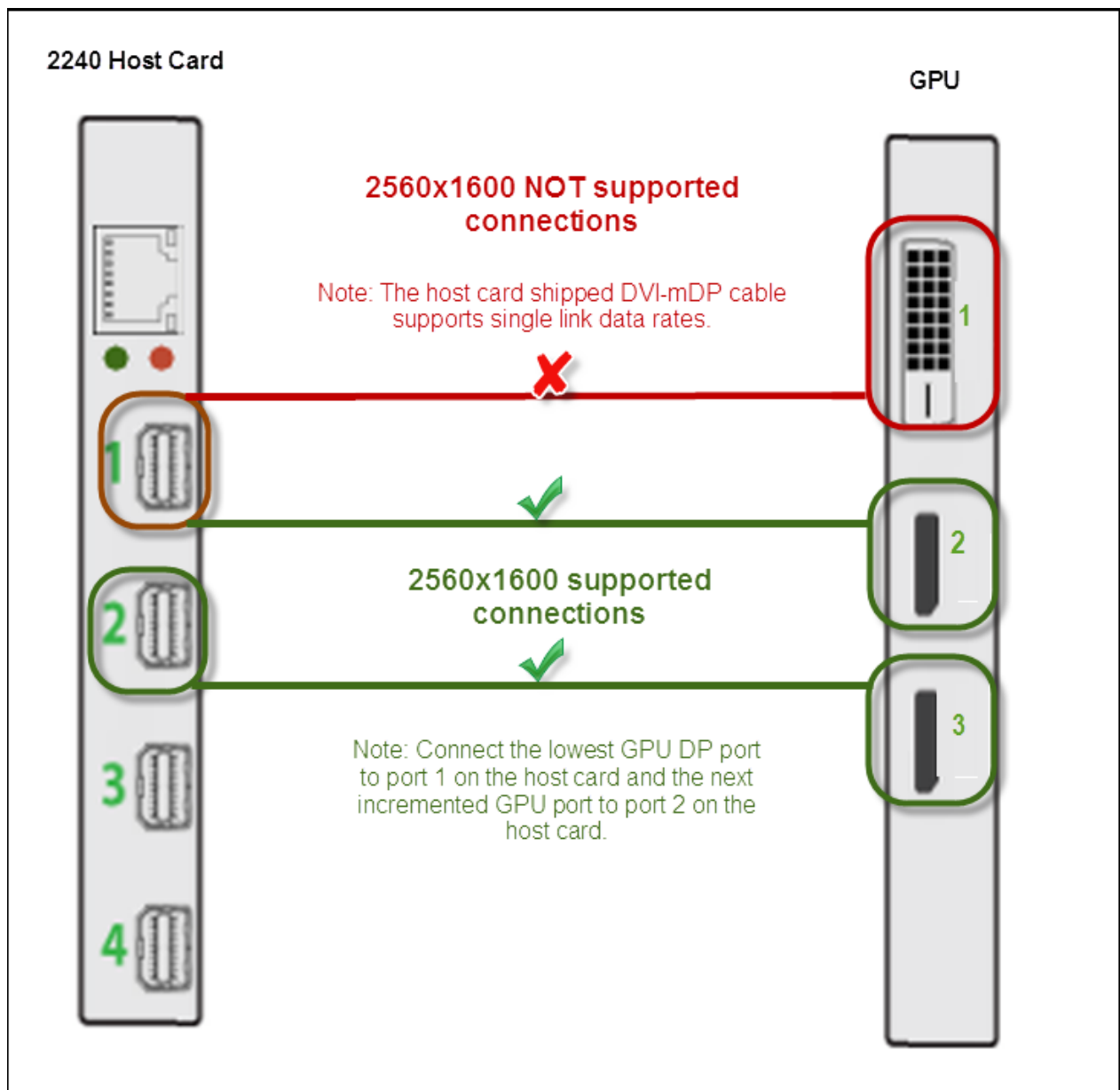
- Insert the PCoIP Remote Workstation Card into an available PCIe slot and secure the card's metal bracket.
- Connect the PCoIP Remote Workstation Card to your network using the Ethernet port.
- Connect the GPU to the PCoIP Remote Workstation Card using the cables that came with your card.

🔥 Connecting cables correctly

To get a desired resolution, all the components of your system (workstation card, GPU, PCoIP Zero Client, and monitors) must support this resolution. In addition, the cables must be connected according to the following rules:

- Always start with the lowest number GPU port (DisplayPort or DVI) and work up sequentially from there, similarly connecting to the lowest number PCoIP Remote Workstation Card port
- For 2560x1600 resolution, you must use DisplayPort ports on the workstation's GPU when connecting to the workstation card DisplayPort.

If you use DVI ports on the GPU, the maximum resolution supported is 1920x1200. The DVI-mDP cable shipped with the workstation card only supports single-link data rates. This means that if you connect the first dual-link DVI port on the GPU to a port on the workstation card, you will still only get a single-link data rate (i.e., resolutions up to 1920x1200).

- Optionally (and recommended) install the Teradici PCoIP Remote Workstation Card power button cable. This connection allows a remote user to power cycle the host PC (e.g., when the operating system is non-responsive).
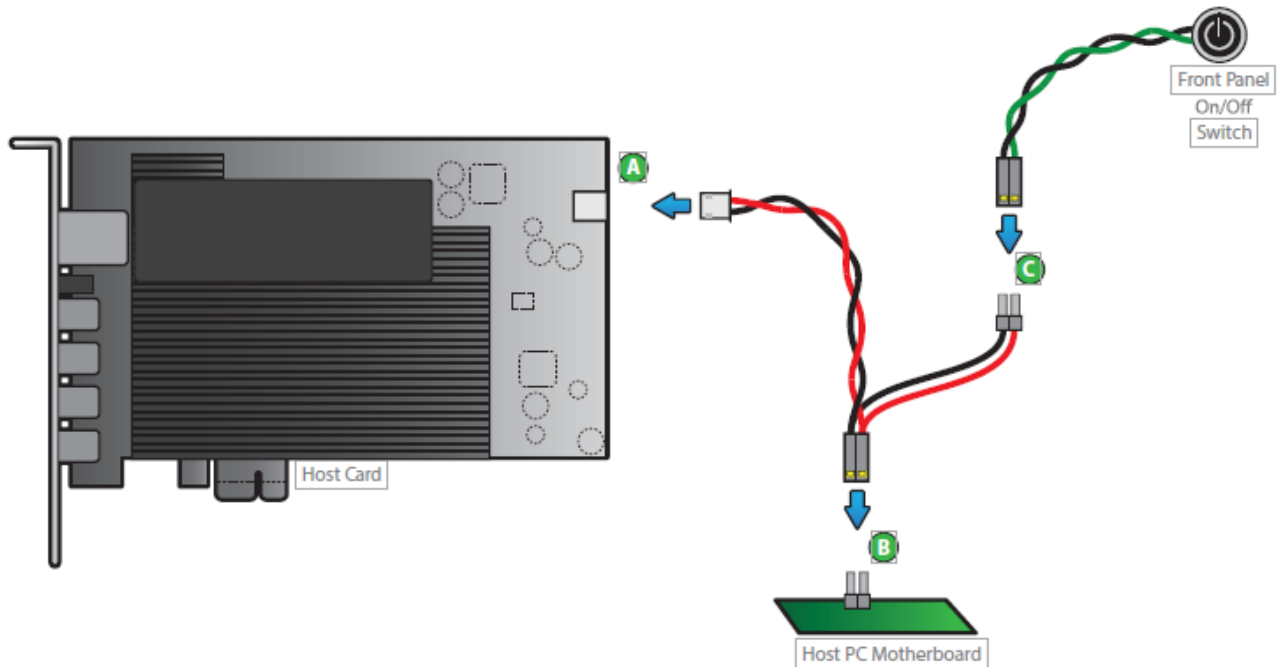
  ○ Connect the white end of the power button cable to the power button cable connector on the PCoIP Remote Workstation Card.

  ○ Locate where the host PC front-panel power button cable connects to the motherboard. Disconnect the host PC's front-panel On/Off switch cable from the motherboard's header, and locate the Power On/Off signal pins. Connect the red wire on the workstation card power button cable to the positive terminal of the Power On/Off pin. Connect the black wire to the negative terminal. The negative terminal is typically a ground pin.

> ⚠ **Motherboard power pins**
>
> The location of the Power On/Off switch pins is different from one motherboard to another. See your motherboard user manual for details. If you have the connector inversely connected, the host PC will not power up.

- Connect the host PC's front-panel On/Off switch cable to the 2-pin header on the workstation card power button cable. If this is not possible, the host PC's front-panel On/Off switch is disabled.

When powered on, the host PC will be ready to receive a PCoIP connection.

About the PCoIP Administrative Web Interface (AWI)

The PCoIP Administrative Web Interface (AWI) enables you to interact with a PCoIP endpoint. From the AWI, you can manage and configure an endpoint, view important information about it, and upload firmware and certificates to it.

After you type the device's IP address or FQDN into Microsoft Edge, Mozilla Firefox, or Google Chrome browser, the browser will use HTTPS to connect to the device's AWI web page. Access to the AWI is controlled using an administrative password, which can be optionally disabled.

The AWI's HTTPS connection is secured using a PCoIP root Certificate Authority (CA) certificate. To avoid warning messages when you log into the AWI, it is recommended that you install this certificate in your browser. The certificate file (cacert.pem) is always included in a firmware release, but you can also download it directly from Certificate management for PCoIP Zero Clients and PCoIP Remote Workstation Cards (1561). Detailed instructions on how to install the certificate are also included in the knowledge base article.

The following browsers are supported in this release:

- Firefox: current version
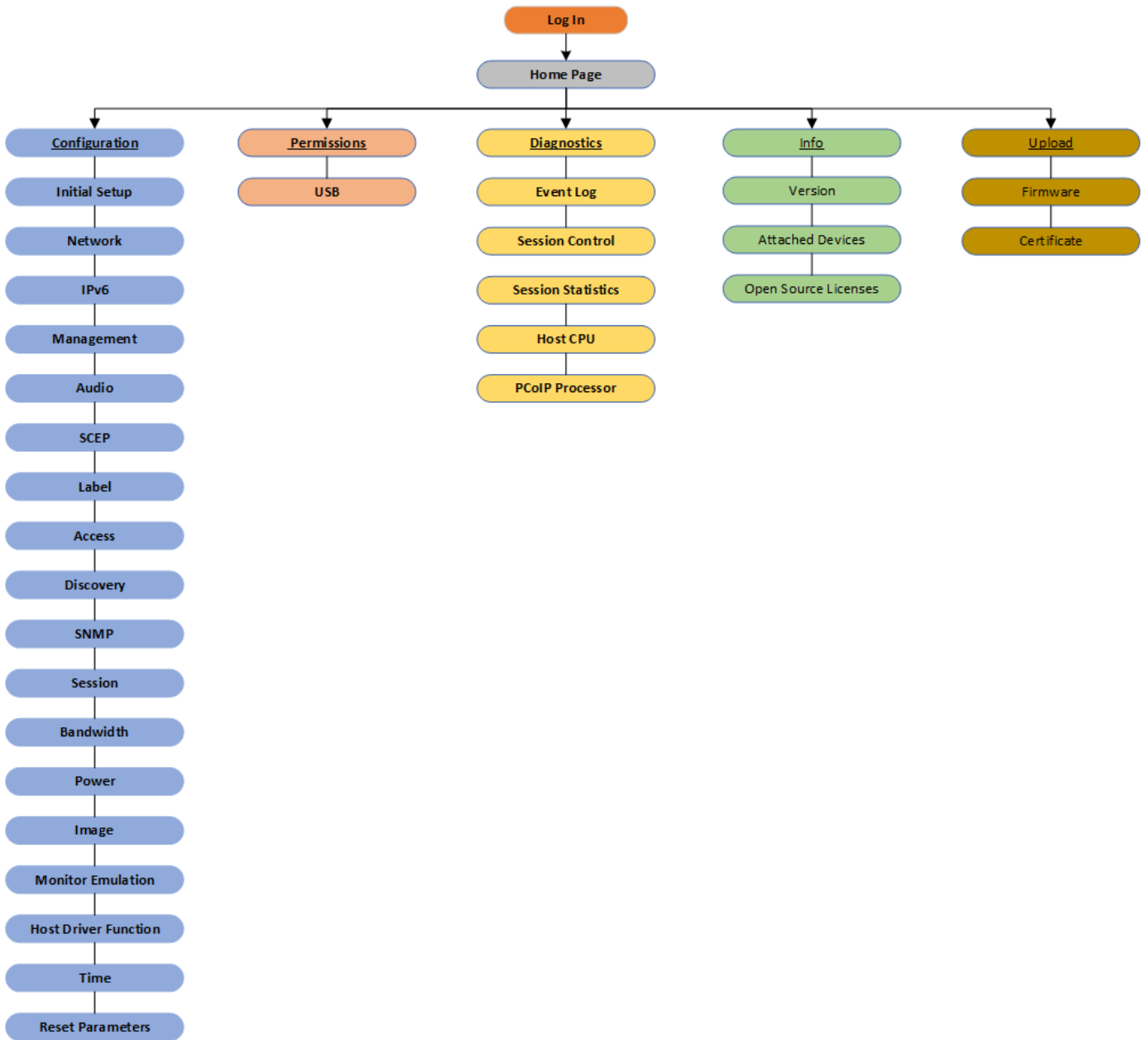- Chrome: current version
- Microsoft Edge: current version

AWI Menus

AWI Menus

The AWI has five main menus that link to the various configuration and status pages.

- **Configuration:** The pages under this menu let you configure the various aspects for the device, such as network settings, language, session parameters, etc.

- **Permissions:** The pages under this menu let you set up the permissions for USB on the client and host.

- **Diagnostics:** The pages under this menu help you troubleshoot the device.

- **Info:** The pages listed under this menu let you view firmware information, the devices currently attached to the device and the open source licenses applicable to this release.

- **Upload:** The pages under this menu let you upload a new firmware version and certificates to the device.

The following figure shows the menus and pages available in the AWI.

Log In → **Home Page**

Configuration
- Initial Setup
- Network
- IPv6
- Management
- Audio
- SCEP
- Label
- Access
- Discovery
- SNMP
- Session
- Bandwidth
- Power
- Image
- Monitor Emulation
- Host Driver Function
- Time
- Reset Parameters

Permissions
- USB

Diagnostics
- Event Log
- Session Control
- Session Statistics
- Host CPU
- PCoIP Processor

Info
- Version
- Attached Devices
- Open Source Licenses

Upload
- Firmware
- Certificate

Logging into the AWI

To log into the Administrator Web Interface web page for a PCoIP Remote Workstation Card.

1. Using a web browser, enter the PCoIP Remote Workstation Card's IP address in the address bar. According to network requirements, this address may be either a static or dynamic address as follows:

   - **Static IP Address:** The IP address is hard-coded and must be known.

   - **Dynamic IP Address:** The Dynamic Host Configuration Protocol (DHCP) server dynamically assigns the IP address. You can get it from the DHCP server.

2. From the *Log In* page, enter the administrative password. The default value is blank.

> 🔥 **OEM default settings**
>
> PCoIP Remote Workstation Cards default settings can be changed by OEM manufacturers. Reference your OEM documentation to ensure a smooth deployment.
>
> **Log In**
>
> Please enter the administrative password to access this device.
>
> Password: [   ]
>
> Idle Timeout: [Never ▼]   [Log In]
>
> **AWI Log In Page**

3. To change idle timeout (the time after which the user is automatically logged off), select an option from the **Idle Timeout** drop-down menu.

4. Click **Log In**.

> ✏️ **Some PCoIP devices do not require a password to log in**
>
> Passwords on PCoIP endpoints when manufactured are determined by the OEMs. Some have placed a default password while others do not have password protection enabled. Teradici recommends using the PCoIP Management Console to manage endpoint password configuration. You can enable/disable password protection for these endpoints from the Management Console profile page. Then complete the following tasks:
>
> - **EDIT** the profile containing your endpoint type
>
> - select the appropriate endpoint type tab (DUAL or QUAD)
>
> - from the **SECURITY** property group you will be able to configure the password options for the endpoints contained in this profile

If configured in the firmware defaults by the OEM manufacturer, the Initial Setup page appears the first time you log in. You can configure audio, network, and session parameters on this page. After you click **Apply**, the Home page appears for each subsequent session. This page provides an overview of the device status.

If a warning message appears when you try to log in, then a session is already in progress on that device. Only one user can log into a device at one time. When a new user logs in, the current session is ended and the previous user is returned to the Log In page.

Passwords

The **Password** page lets you update the local administrative password for the device. You can access this page from the **Options > Password** menu. The password can be a maximum of 20 characters.

> ⚠️ **Unknown AWI password**
>
> Take care when updating the client password as the client may become unusable if the password is lost.

> ✏️ **Contact your manufacturer for your devices AWI default password**
>
> Contact your manufacturer to obtain the default password for your device's AWI.

AWI Home Page

The AWI Home page displays a statistics summary for the PCoIP endpoint. You can display the Home page at any time by clicking the Home link at the top left section of the menu bar.

teradici.
PCoIP

PCoIP® Host Card

PCoIP® device status and statistics for the current session.

Processor:	TERA2220 revision 1.0 (512 MB)
Time Since Boot:	2 Days 1 Hours 6 Minutes 5 Seconds
PCoIP Device Name:	pcoip-host-0030040e3388
Connection State:	Disconnected
Connection Duration:	
802.1X Authentication Status:	Disabled
Session Encryption Type:	Not in Session
PCoIP Packets (Sent/Received/Lost):	7390 / 7061 / 0 (0.0 %)
Bytes (Sent/Received):	3608788 / 1917558
Round Trip Latency (Min/Avg/Max):	0 / 0 / 0 ms
Transmit Bandwidth (Min/Avg/Max/Limit):	0 / 0 / 0 / 8404 kbps
Receive Bandwidth (Min/Avg/Max):	0 / 0 / 0 kbps
Pipeline Processing Rate (Avg/Max/Limit):	0 / 0 / 0 Mpps
Endpoint Image Settings In Use:	Client
Initial Image Quality (Min/Active/Max):	40 / 45 / 90
Image Quality Preference:	25
Build To Lossless:	Enabled

Display	Maximum Rate: Refresh Rate	Input Change Rate	Output Process Rate	Image Quality
1	60 fps	0 fps	0 fps	N/A
2	0 fps	0 fps	0 fps	N/A

AWI: Home Page

The previous figure shows session statistics for devices that can support two connected displays. If your deployment only supports two displays, information for these two displays will appear in the bottom area of the page.

AWI Home Page Statistics

Statistics	Description
Processor	PCoIP processor type, version, and RAM size
Time Since Boot	Length of time that the PCoIP processor has been running.
PCoIP Device Name	The logical name for the device. This field is the name the endpoint registers with the DNS server if DHCP is enabled or the system is configured to support registering the hostname with the DNS server. (See the PCoIP Device Name parameter on the **Label** page.)
Connection State	The current state of the PCoIP session. Values include the following: • Asleep • Canceling • Connected • Connection Pending • Disconnected • Waking
Connection Duration	Displays the length of time the device has been connected to a host endpoint.
802.1X Authentication Status	Indicates whether 802.1X authentication is enabled or disabled on the device.
Session Encryption Type	The type of encryption in use when a session is active: • AES-256-GCM
PCoIP Packet Statistics	**PCoIP Packets Sent:** The total number of PCoIP packets sent in the current/last session. **PCoIP Packets Received:** The total number of PCoIP packets received in the current/last session. **PCoIP Packets Lost:** The total number of PCoIP packets lost in the current/last session.

Statistics	Description
Bytes	**Bytes Sent:** The total number of bytes sent in the current/last session. **Bytes Received:** The total number of bytes received in the current/last session.
Round Trip Latency	The minimum, average, and maximum round-trip PCoIP system and network latency in milliseconds (± 1 ms).
Bandwidth Statistics	**Transmit Bandwidth:** The minimum, average, and maximum traffic transmitted by the Tera processor. The active bandwidth limit is the maximum amount of network traffic the Tera processor may currently generate. The value is derived from the configured bandwidth parameters and the current (or last) network congestion levels. **Receive Bandwidth:** The minimum, average, and maximum traffic received by the Tera processor.
Pipeline Processing Rate	How much image data is currently being processed by the image engine (in megapixels per second).
Endpoint Image Settings In Use	Displays if the image settings being used are configured within the client or within the host. This is based on how the **Use Client Image Settings** field is configured on the **Image** page for the host device.
Initial Image Quality	The minimum and maximum quality setting is taken from the **Image** page for the device. The active setting is what's currently being used in the session and only appears on the host.
Image Quality Preference	This setting is taken from the **Image Quality Preference** field on the **Image** page. The value determines if the image is set to a smoother versus a sharper image.
Build to Lossless	Options that may appear in this field include the following: **Enabled:** The **Disable Build to Lossless** field on the Image page is unchecked. **Disabled:** The **Disable Build to Lossless** field is checked.
Display	The port number for the display.
Maximum Rate	This column shows the refresh rate of the attached display. If the **Maximum Rate** field on the **Image** page is set to 0 (i.e., there is no limit), the maximum rate is taken from the monitor's refresh rate. If the **Maximum Rate** field on the **Image** page is set to a value greater than 0, the refresh rate shows as "User Defined."

Statistics	Description
Input Change Rate	The rate of content change from the GPU. This includes everything the user is doing (such as cursor movement, email editing, or streaming video). Note: This option is only available on the host. It does not appear on the client.
Output Process Rate	The frame rate currently being sent from the image engine on the host to the client.
Initial Image Quality	Shows the current lossless state of the attached display: • Lossy • Perceptually lossless • Lossless

> ✏️ **Clicking Reset Statistics also resets statistics on Home page**

When you click the **Reset Statistics** button on a Remote Workstation Card's AWI Session Statistics page (**Diagnostics > Session Statistics**), the statistics reported in the Home page are also reset.

Configuration Parameters

This section provides descriptions for the parameters found within each menu selection. These parameters control the performance and behavior of your PCoIP Remote Workstation Card. The descriptions will help you configure and optimize your PCoIP Remote Workstation Card for your deployment. Some of the menu parameters are described in a grouped section of the guide:

- Configuring Power Options

- About USB Settings

- Host Driver Function

- Software Reset Parameters

Configuring the Initial Setup

Connecting to a PCoIP Remote Workstation Card is easy right out of the box. Default settings that are enabled include DHCP, SLP Discovery, DNS SRV Discovery and Accept Any Client allow easy first time connections for many networks. For simplicity, basic network and audio settings are available on the Initial Setup page of the AWI. You can access this page from the **Configuration > Initial Setup** menu. The AWI's Initial Setup page contains the audio, network, and session configuration parameters that you should set before a PCoIP endpoint can be used. This page helps to simplify initial setup and reduce the time for new users to establish a session between a PCoIP client and PCoIP Remote Workstation Card.

If configured in the firmware defaults by the manufacturer, the *Initial Setup* page appears the first time you log in. After you click **Apply**, the Home page appears for subsequent sessions unless the firmware parameters are reset.

✎ **Complex environments require further configuration**

More complex environments that use host discovery or endpoint management systems require further configuration than is available on the Initial Setup page.

Initial Setup Page

Audio

The two audio parameters for audio on the *Initial Setup* page will allow audio from a device attached to a PCoIP Zero Client be played from the host PC. These are the same parameters found in the separate Audio page

Enable HD Audio allows the audio hardware on the PCoIP Zero Client to be used when connecting to a PCoIP Remote Workstation Card. When disabled, the audio hardware is not available for the host operating system to enumerate.

Enable Audio Line In allows the use of the line-in connector on a PCoIP Zero Client so an audio device can be plugged into a PCoIP Zero Client and played on the host PC. When disabled you can use the line-in connector as a microphone input.

> **ℹ Microsoft Users**
>
> If using Microsoft® Windows Vista, Windows 7, & Windows 8, please ensure you do the following for this feature to function correctly:
>
> - Run **regedit**.
> - Search the registry keys for **PinConfigOverrideVerbs** and delete these registry entries.

Network

The Network parameters on the *Initial Setup* page allows you to enable DHCP or manually configure network settings, allowing you to connect to your network quickly. For more detailed network configurations, see Configuring Host Network Settings where you will have additional options.

Session

Accept Any Client allows any PCoIP Zero Client or PCoIP software client to connect to the PCoIP Remote Workstation Card. If your deployment requires a connection from a specific client, you have the option of entering its MAC address here. For more secure settings when connecting from a PCoIP client, see Configuring a Session.

Configuring Host Network Settings

This page lets you configure network settings for the PCoIP Remote Workstation Card. You can access this page from the **Configuration > Network** menu. After you update the parameters on this page, click **Apply** to save your changes.

You can also configure network information from the host's Initial Setup page.

Network

Change the network settings for the device

Enable DHCP:	☑
IP Address:	10 . 0 . 8 . 28
Subnet Mask:	255 . 255 . 255 . 0
Gateway:	10 . 0 . 8 . 1
Primary DNS Server:	192 . 168 . 1 . 50
Secondary DNS Server:	192 . 168 . 1 . 52
Domain Name:	teradici.local
FQDN:	pcoip-host-0030040e638c.teradici.local
Ethernet Mode:	Auto
Enable Gigabit Auto-Negotiation:	☑
Prefer Master for Auto-Negotiation:	☐
Maximum MTU Size:	1200 bytes
Enable 802.1X Security:	☐
Authentication:	TLS
Identity:	
Client Certificate:	Choose
Enable 802.1X Support for Legacy Switches:	☑

Apply   Cancel

AWI Network Page Parameters

Parameter	Description
Enable DHCP	When enabled, the device contacts a DHCP server to be assigned an IP address, subnet mask, gateway IP address, and DNS servers, and also requests a domain name (option 15), host name (option 12), and client fully qualified domain name (FQDN).
	When disabled, you must set these parameters manually.
IP Address	The device's IP address. If DHCP is disabled, you must set this field to a valid IP address. If DHCP is enabled, you cannot edit this field.
Subnet Mask	The device's subnet mask. If DHCP is disabled, you must set this field to a valid subnet mask. If DHCP is enabled, you cannot edit this field.
	Warning: It is possible to configure an illegal IP address/subnet mask combination (e.g., invalid mask) that leaves the device unreachable. Take care when setting the subnet mask.
Gateway	The device's gateway IP address. If DHCP is disabled, this field is required. If DHCP is enabled, you cannot edit this field.
Primary DNS Server	The device's primary DNS IP address. This field is optional. If the DNS server IP address is configured when using a connection manager, the connection manager address may be set as an FQDN instead of an IP address.
Secondary DNS Server	The device's secondary DNS IP address. This field is optional. If the DNS server IP address is configured when using a connection manager, the connection manager address may be set as an FQDN instead of an IP address.
Domain Name	The domain named of the device (e.g., "domain.local"). This field is optional.
FQDN	The fully qualified domain name for the device. The default is pcoip-host- or pcoip-portal- where is the device's MAC address. If used, the domain name is appended (for example, pcoip-host-.domain.local). This field is read-only on this page.
	Note: To use the FQDN feature, the DNS server with DHCP option 81 must be available and properly configured.

Parameter	Description
Ethernet Mode	Lets you configure the Ethernet mode of the device as follows: • Auto • 100 Mbps Full-Duplex • 10 Mbps Full-Duplex when you choose **10 Mbps Full Duplex** or **100 Mbps Full-Duplex** and then click **Apply**, the following warning message appears: "Warning: When Auto-Negotiation is disabled on the PCoIP device, it must also be disabled on the switch. Additionally, the PCoIP device and switch must be configured to use the same speed and duplex parameters. Different parameters may result in a loss of network connectivity. Are you sure you want to continue?" Click **OK** to change the parameter. Note: You should always set the Ethernet mode to Auto and only use 10 Mbps Full-Duplex or 100 Mbps Full-Duplex when the other network equipment (e.g., a switch) is also configured to operate at 10 Mbps full-duplex or 100 Mbps full-duplex. An improperly set Ethernet mode may result in the network operating at half-duplex, which is not supported by the PCoIP protocol. The session will be severely degraded and eventually dropped.
Enable Gigabit Auto-Negotiation	Lets you select the maximum negotiated speed of the network interface. When enabled (the default), the maximum possible speed is 1 Gbps. When disabled, it is 100 Mbps. Note: You may want to disable this feature on the host card if you are experiencing Ethernet packet loss (which can result in loss of network connectivity and PCoIP session loss). This scenario can be caused by Ethernet cabling that is not up to Gigabit Ethernet specification (e.g., old building wiring composed of Cat5 cable). Out-of-specification cable will often still successfully auto-negotiate to 1 Gbps speed, but may subsequently have CRC errors during normal operation. Disabling Gigabit Auto-Negotiation prevents the network interface from advertising to its peer on the network that it supports Gigabit Ethernet operation, and so the maximum possible negotiated speed drops to the next level (100 Mbps).
Prefer Master for Auto-Negotiation	When enabled, this setting makes the Remote Workstation Card the master for auto-negotiation. It can be used when a client is connected directly to a Remote Workstation Card without an intervening switch.

Parameter	Description
Maximum MTU Size	Lets you configure the **Maximum Transfer Unit** packet size. A smaller MTU may be needed for situations such as VPN tunneling because PCoIP packets cannot be fragmented. Set the **Maximum MTU Size** to a value smaller than the network path MTU for the end-to-end connection between the host and client. The **Maximum MTU Size** range is 600 to 1500 bytes for all firmware versions. The default MTU size is 1200.
Enable 802.1X Security	Enable this field for each of your devices if your network uses 802.1X security to ensure that only authorized devices access the network. If enabled, configure the **Authentication**, **Identity**, and **Client Certificate** fields.
Authentication	This field is set to TLS (Transport Layer Security) and is grayed-out. TLS is currently the only authentication protocol supported.
Identity	Enter the identity string used to identify your device to the network.
Client Certificate	Click **Choose** to select the client certificate you want to use for your 802.1X devices. The list of certificates that appears includes the certificates uploaded from the **Certificate Upload** page that contain a private key. The certificate you choose from the **Network** page is linked to the read-only **Client Certificate** field on the **Certificate Upload** page. Note: PCoIP only supports one 802.1X client certificate. Ensure your security details are all contained within the one file. The 802.1X certificate must contain a private key.
Enable 802.1X Support for Legacy Switches	When enabled, allows greater 802.1X compatibility for older switches on the network.

Configuring IPv6 Settings

The settings on this page let you enable IPv6 for PCoIP devices connected to an IPv6 network.

You can access this page from the **Configuration > IPv6** menu.

AWI IPv6 Page

> 🔥 **Reboot**
>
> When you make a change to one of the settings on this page, you must reboot your device for the change to take effect.

IPv6 Page Parameters

Parameter	Description
Enable IPv6	Enable this field to enable IPv6 for your PCoIP devices.
Link Local Address	This field is automatically populated.
Gateway	Enter the IPv6 gateway address.
Enable DHCPv6	Enable this field to set up Dynamic Host Configuration Protocol version 6 (DHCPv6) for your device.
DHCPv6 Addresses	When DHCPv6 is enabled and the device is rebooted, the server automatically populates these fields with addresses for the device.
Primary DNS	The device's primary DNS IP address. If DHCPv6 is enabled, this field is automatically populated by the DHCPv6 server.
Secondary DNS	The device's secondary DNS IP address. If DHCPv6 is enabled, this field is automatically populated by the DHCPv6 server.
Domain Name	The domain name used (e.g., "domain.local") for the host or client. If DHCPv6 is enabled, this field is automatically populated by the DHCPv6 server.
FQDN	The fully qualified domain name for the host or client. If DHCPv6 is enabled, this field is automatically populated by the DHCPv6 server.
Enable SLAAC	Enable this field to set up Stateless Address Auto-configuration (SLAAC) for your devices.
SLAAC Addresses	When SLAAC is enabled and the device is rebooted, these fields are automatically populated.
Enable Manual Address	Enable this field to set up a manual (static) address for the device.
Manual Address	Enter the IP address for the device.

Configuring the Management State

The PCoIP Remote Workstation Card can be managed by an endpoint managers such as the PCoIP Management Console should one be available on the network. The AWI Management page tells the host card how to find the manager based on predetermined network deployment security levels. Configuring the security levels for endpoint managers is described in Configuring Endpoint Management Discovery Methods with further information on certificates required for each level of secure configuration found in the PCoIP Remote Workstation Card Security Overview.

From the AWI, you can set the PCoIP Remote Workstation Card's management state to automatic or manual modes.

Management
Configure how this device is managed

Phase: Bootstrap

Management Status: Idle

Security Level: Low Security Environment - Device is discoverable by Endpoint Managers

Manager Discovery Mode: Automatic

	Discovery Method	Discovery Outcome	Endpoint Bootstrap Manager Address	Certificate Fingerprint
Discovery Information:	DHCP Options	Failed to find an Endpoint manager address		
	DNS SRV Records	Failed to find an Endpoint manager address		

Clear Management State

Apply   Cancel

AWI Management page – automatic discovery mode

AWI Management page – manual discovery mode

Clearing the Management State

Setting	Default	AWI	Management Console
Clear Management State (a button)	▬	✔	✔

Clearing the management state removes the current endpoint manager information for the PCoIP Remote Workstation Card. Once the Remote Workstation Card is managed by an endpoint manager, you must clear its management state before the PCoIP device can accept a new endpoint manager.

You clear the management state from the *AWI Management* pages.

> ℹ **Discovery settings determine what displays on the AWI Management page**
>
> The information that displays on the AWI Management page depends on whether the PCoIP Remote Workstation Card uses automatic or manual discovery.

To clear the management state:

1. From the OSD or AWI, select **Configuration > Management**.

2. From the OSD or AWI Management page, click **Clear Management State** so that the endpoint will accept a new endpoint manager.

3. To save your updates, click **OK** from the OSD, or click **Apply** from the AWI.

Configuring Audio Settings

The Audio page lets you configure audio options for the PCoIP device. You can access this page from the AWI **Configuration > Audio** menu.

> ✏️ **After configuring the desired options, click Apply and then Continue to have your changes take effect.**

The Audio settings allow audio from an audio device attached to a PCoIP Zero Client be played on the host PC operating system.

AWI Host Audio Page

Audio settings on a PCoIP Remote Workstation Card work in tandem with the audio settings on a PCoIP Zero Client. The parameters below further describe how audio works between the two devices.

Audio Page Parameters

Parameter	Description
Enable Audio	When enabled, configures audio support on the PCoIP device. Note: This property must be enabled on both the PCoIP Remote Workstation Card and the PCoIP Zero Client. When disabled, the audio hardware is not available for the host operating system to enumerate.
Enable Audio Line In	Determines the input mode the audio system advertises to the host operating system. When enabled, the line-in connector found on the client is used as a standard line-in input. When disabled, the line-in connector found on the client is used as a microphone input. Note: Follow the onscreen instructions if you have Windows 7 or 10 installed on the device.

Obtaining Certificates Automatically Using SCEP

You can simplify the retrieval and installation of digital certificates by enabling devices to obtain certificates automatically from a Simple Certificate Enrollment Protocol (SCEP) server.

You can obtain certificates using SCEP for:

- **802.1X**: Allows you to request a custom certificate to use in your 802.1X configuration.

> ✏️ **Enabling 802.1X**
>
> Enabling 802.1X also requires enabling 802.1X in the **Configuration > Networking** page of the AWI.

- **Administrative Web Interface**: Allows you to request a custom certificate for the Administrative Web Interface (AWI).

- **Peer-to-peer Max Compatibility**: Allows you to use SCEP to automatically request a custom certificate that allows secure negotiation using any of the common cipher suites offering flexibility for your network security requirements.

- **Peer-to-peer Suite B**: Used in environments requiring Suite B cryptography. Allows you to use SCEP to automatically request a custom certificate offering the greatest security for negotiating session connections with a PCoIP endpoint.

SCEP Behaviors

The following behaviors are observed when using SCEP to obtain your certificates.

- A successful SCEP request for a certificate will install the SCEP certificate in the endpoint's certificate store.

- A successful SCEP request for a certificate will no longer store the Root CA (or issuing CA) certificate in the endpoint's certificate store.

- The AWI SCEP tab will display the Subject and Issuer names of the SCEP client certificate.

- Deleting a peer-to-peer certificate will cause it to revert to using the default peer-to-peer certificate. This will take effect on next session connection.

- Deleting an AWI SCEP certificate will cause it to revert to using the default AWI certificate. A reboot is required.

- Removing a 802.1X SCEP certificate happens immediately. The endpoint will fail 802.1X authentication on the next connection attempt or on the next automatic polling of the 802.1X switch.

- Additional successful SCEP requests will overwrite any previously installed SCEP certificates for the same usage.

- Endpoint SCEP certificate requests include the following parameters:

  - **Subject Name**: PCoIP Device Name

  - **Subject Alt Name**: MAC Address, User Principal Name (UPN), and the Fully Qualified Domain Name (FQDN)

- SCEP certificate renewal requests occur sequentially in 1 hour intervals when the renewal setting has been reached. The first request must successfully complete before renewal of the next certificate is initiated. If unsuccessful, the renewal request for the first certificate is attempted again. Administrators should periodically review the validity period of the SCEP certificates to ensure that renewals were successful and the certificates do not expire.

- The PCoIP endpoint must have NTP properly configured.

- The renewal period must be less than the validity period of the certificate.

- Based on the configured renewal setting, an endpoint will automatically issue a SCEP renewal request using the existing certificate for authentication.

> ✏️ **Using Microsoft NDES**
>
> Renewal using Microsoft NDES encounters a problem when the Certificate template is configured to populate the **Subject Name** with multiple attributes from Active Directory information (e.g. CN, OU, DC), such is the case when setting the Subject Name to *Fully distinguished name*.
> To avoid this issue:
>
> - Set the Subject Name to be supplied in the request
> - Set the Subject Name to be populated with just the Common Name from the Active Directory

- Endpoint SCEP requests do not use a TLS connection. The Tera2 endpoint generates its own 3072-bit SCEP RSA private key when certificates other than **Peer-to-peer Suite B** certificates are requested. For **Peer-to-peer Suite B** certificates, the endpoint generates its own ECC P-384 SCEP private key.

The private key is used to construct parts of the PKCS#10-formatted certificate request which is then delivered to the SCEP server, and the SCEP server's Registration Authority (RA) RSA certificate's public key is used to encrypt the actual certificate request. The SCEP challenge password is encrypted as it is contained within the certificate request.

The following cryptography algorithms are used to generate a SCEP request:

- Content Key Encryption Algorithm: **RSAES-OAEP**

- Hash Algorithm: **SHA384**

- Content Encryption Algorithm: **AES-256-CBC**

🔥 **Endpoint Session TLS Security Mode settings**

Hardware endpoints have a required TLS Security Mode setting in each session configuration (i.e. AWI > Session). The SCEP request must correspond to the TLS Security Mode setting used on the endpoint.

- If the selected TLS security mode is Suite B, only ECC certs can be selected using the **Peer-to-Peer Certificate** drop down list.

- If the selected TLS security mode is Max compatibility, only RSA certs can be selected using the **Peer-to-Peer Certificate** drop down list.

- The session TLS security mode must match the selected SCEP issued peer-to-peer certificate—**Peer-to-peer Max Compatibility** or **Peer-to-peer Suite B**—to establish a successful secure peer-to-peer connection.
If the endpoint is not configured with the correct session TLS Security Mode, the *Peer-to-Peer Certificate* field in the AWI Configuration > Session page will not change and remain as **Default**, even though the Upload > Certificate page shows the active SCEP issued certificate in the *Selected Peer-to-Peer Certificate* field.

- Peered endpoints will not connect until the TLS setting matches the type of certificate being used and the peered endpoint has the matching configuration.

The following settings display on the AWI **SCEP** pages:

AWI SCEP page

SCEP Parameters

Parameter	Description
Certificate Usage	There are 4 options: • 802.1X • Administrative Web Interface • Peer-to-peer Max Compatibility • Peer-to-peer Suite B
SCEP Server URL	Enter the URL for the SCEP server that is configured to issue certificates for the device.
Challenge Password	Enter the password required by the SCEP server
CA Identifier	A string provided by your CA issuer that uniquely identifies the Certificate Authority when providing certificates for SCEP requests.

Parameter	Description
Auto Renewal Period	Number of days prior to the existing certificate expiry date to initiate a certificate SCEP renewal request. If left unconfigured, administrators must manually request a new certificate.
Issuer CA Certificate	Displays the Issuer CA certificate that signed the client certificate. (The endpoint no longer stores the Root CA certificate)
Client Certificate	Displays the name of the client certificate that has been installed in the device.
Request Certificates (button)	After entering the SCEP server address, password, certificate usage, and CA Identifier, clicking this button initiates the retrieve certificates process.
Status	Displays the status of the request (for example, requesting, successful, failed).

To obtain certificates automatically using SCEP:

1. Open the SCEP page from the AWI by browsing to **Configuration > SCEP**.

2. Select the **Certificate Usage** type.

> ⚠ **Using Peer-to-peer certificates**
>
> If using a Peer-to-peer certificate, confirm the *TLS Security Mode* in the advanced section of your Session connection matches your certificate type. A successful secure connection can only happen when the corresponding PCoIP endpoint has the correctly configured certificate applied. See Peering Zero Clients to Remote Workstation Cards

3. Enter the URL and challenge password for the SCEP server.

4. Enter the **CA Identifier** if required. Provide a valid CA Identifier or use "CAIdentifier" (default).

5. Enter the **Auto Renewal Period**.

6. Click **Request Certificates** to retrieve the certificate. The issuing CA and client certificates display after a successful SCEP request.

The **Status** section displays the status of the request such as Requesting, Request completed, or Request failed. Once the SCEP process is completed, the certificate is active.

To delete your SCEP certificate:

1. Browse to **Upload > Certificates** page.

2. Click the **Remove** button beside the certificate you wish to remove.

3. Click **Apply** and then **Continue**.

Configuring the Label Settings

The Label page lets you assign a device name to your PCoIP device for easy reference. You can access this page for the host card from the **Configuration > Label** menu.

AWI Label Page Parameters

Parameter	Description
PCoIP Device Name	Lets you give the host a logical name. The default is pcoip-host-, where is the device's MAC address. This field is the name the host registers with the DNS server if DHCP is enabled and the system is configured to support registering the hostname with the DNS server. It's important to ensure that the **PCoIP Device Name** is unique for each endpoint in the network and follows these naming conventions: • The first and last character must be a letter (A-Z or a-z) or a digit (0-9). • The remaining characters must be letters, digits, hyphens, or underscores. • The length must be 63 characters or fewer.
PCoIP Device Description	A description of the device or other information, such as the location of the device's endpoint. Note: The firmware does not use this field. It is provided for administrator use only.

Parameter	Description
Generic Tag	Generic tag information about the device. Note: The firmware does not use this field. It is provided for administrator use only.

Configuring Access Settings

The Access page lets you prevent the PCoIP device from being managed by the MC (or any other PCoIP device management tool), and lets you disable administrative access to the device's AWI. It also provides an option to force an administrative password change the next time the AWI is accessed.

You can access this page from the **Configuration > Access** menu.

AWI Access Page

These options can also be configured from the PCoIP Management Console 3.1 or newer.

> ⚠️ **Enable at least one of the configuration interfaces**
>
> At least one of the device's management configuration interfaces (AWI or MC) must remain enabled at all times. If you disable both management interfaces you will lose the option to perform a software parameter reset should you want to reuse the PCoIP Remote Workstation Card in another deployment. You will be left having to do a hardware jumper parameter reset to regain administrative access to your PCoIP Remote Workstation Card

When the **Disable Management Console Interface** is checked, the management console interface on the PCoIP Remote Workstation Card cannot be accessed or managed by the MC (or any other PCoIP device management tool).

When checked, the **Disable Administrative Web Interface** on the PCoIP Remote Workstation Card cannot be accessed or managed using the AWI.

The **Force password change at next login** causes the administrative password on the AWI to be changed the next time the AWI is accessed. The new password may be blank.

Configuring Endpoint Management Discovery Methods

From the AWI Management page, you can set the PCoIP Remote Workstation Cards security level and discovery method. See About PCoIP Remote Workstation Card Management Security Levels.

In order for DNS or SLP Discovery methods to work, they both must first be enabled on the AWI **Configuration > Discovery** page.

There are several ways to register your PCoIP Remote Workstation Card with an endpoint manager such as the PCoIP Management Console. These methods are outlined next.

The methods include:

- Automatic Endpoint Manager Discovery Using DNS

- Configuring Endpoints for Auto Discovery Using DHCP

- Discovering the PCoIP Endpoint Manually from the Endpoint Manager

- Discovering the Endpoint Manager Manually from the PCoIP Endpoint Using Low or Medium Security Mode

- Discovering the Endpoint Manager Manually from the PCoIP Remote Workstation Card Using High Security Mode

The availability of these methods are determined by the PCoIP Remote Workstation Card's security settings, and whether or not the host card has a certificate installed to trust the endpoint manager.

Automatic Endpoint Manager Discovery Using DNS

PCoIP Remote Workstation Cards can use DNS to automatically find an endpoint manager. To use automatic endpoint manager discovery, you must configure the environment for DNS service record discovery, and the PCoIP Remote Workstation Card's security level must be set to low or medium.

> ⚠ **Medium or high security requires an installed certificate**
>
> In order to use medium or high security, the PCoIP Remote Workstation Card must have been provisioned with a certificate.

> ✏ **DNS server configuration information**
>
> For details about how to configure your DNS server for automatic discovery, see the PCoIP® Management Console Administrators' Guide section Configuring DNS for Endpoints that use Autodiscovery:.

To configure the PCoIP Remote Workstation Card for automatic endpoint discovery:

1. From the AWI, select **Configuration > Management**. The AWI Management page displays.

2. Set the Security Level option to **Low** or **Medium**.

   > ⚠ **Medium security level**
   >
   > When set to medium security, the MC certificate (leaf, intermediate, or root) must be in the endpoint certificate store

3. Set the Manager Discovery Mode option to **Automatic**.

4. Click **Apply**.

After the PCoIP Remote Workstation Card discovers the endpoint manager, the automatic discovery results appear on the Management page in the Discovery Information section.

> ✏ **Configuring your system for automatic discovery**
>
> For information about how to configure your system for automatic discovery from the PCoIP Management Console, see the PCoIP® Management Console Administrators' Guide.

Discovering the PCoIP Endpoint Manually from the Endpoint Manager

Endpoint managers, such as the PCoIP Management Console, can be used to discover endpoints like the PCoIP Remote Workstation Card. This discovery requires configuration on both the PCoIP Remote Workstation Card and the endpoint manager.

To configure the PCoIP Remote Workstation Card to be discoverable by an endpoint manager:

1. From the AWI, select **Configuration > Management**. The AWI Management page displays.

2. Set the Security Level option to **Low**.

3. Set the Manager Discovery Mode to **Automatic**.

4. Click **Apply**.

This configuration allows an endpoint manager the ability to discover the PCoIP Remote Workstation Card. Once discovered, the endpoint manager topology appears on the PCoIP Remote Workstation Card Management page.

> ✏️ **Initiating discovery from the PCoIP Management Console**
>
> For more information about initiating discovery from the PCoIP Management Console, see the PCoIP® Management Console Administrators' Guide.

Discovering the Endpoint Manager Manually from the PCoIP Endpoint Using Low or Medium Security Mode

In *low* or *medium* security modes, you can manually discover the endpoint manager by manually providing the URI for its bootstrap server.

> ⚠️ **Manual discovery requires a certificate**
>
> When manual discovery mode is used, DNS cannot be used to trust the endpoint. An endpoint such as the PCoIP Remote Workstation Card must have been previously provisioned with a certificate.

To configure a PCoIP Remote Workstation Card with an endpoint manager in low or medium security mode:

1. From the AWI, select **Configuration > Management**. The AWI Management page is displayed.

2. Set the Security Level option to **Low** or **Medium**.

3. Set the Manager Discovery Mode to **Manual**.

4. In the Manual Discovery section, type the bootstrap server's URI.

> ✏️ **Bootstrap server URI must use a secured WebSocket prefix**
>
> URIs are in this format and require a secured WebSocket prefix:
>
> `wss://<internal EM IP address/FQDN>[:port number]`
>
> The PCoIP Management Console's listening port is 5172. If you omit the port number, port 5172 will be used by default.

5. Click **Apply**.

After the PCoIP Remote Workstation Card discovers the endpoint manager, the endpoint manager topology appears on the PCoIP Remote Workstation Card Management page.

Discovering the Endpoint Manager Manually from the PCoIP Remote Workstation Card Using High Security Mode

In high security mode, automatic discovery is disabled entirely; you must register the PCoIP Remote Workstation Card manually with the endpoint manager from the endpoint.

> ⚠️ **Manual discovery requires a certificate**
>
> When manual discovery mode is used, DNS cannot be used to trust the endpoint manager. The PCoIP Remote Workstation Card must have been previously provisioned with a certificate from an endpoint manager or from the AWI.

To configure a PCoIP Remote Workstation Card with an endpoint manager using high security mode:

1. From the AWI, select **Configuration > Management**. The AWI Management page displays.

2. Set the Security Level option to **High**.

3. In the *Endpoint Manager URI for Direct Connect* section, find the Internal URI field and type the endpoint manager's URI. You can also provide an external URI, if needed.

> ✏️ **Endpoint manager URI must use a secured WebSocket prefix**
>
> URIs are in this format and require a secured WebSocket prefix:
>
> `wss://<internal EM IP address/FQDN>[:port number]`
>
> The PCoIP Management Console's listening port is 5172. If you omit the port number, port 5172 will be used by default.

4. Click **Apply**.

After the PCoIP Remote Workstation Card discovers the endpoint manager, the endpoint manager topology appears on the Management page.

SNMP Overview

Knowledge of using and configuring Simple Network Management Protocol (SNMP) and an SNMP manager is required before enabling SNMP. See your SNMP manager documentation.
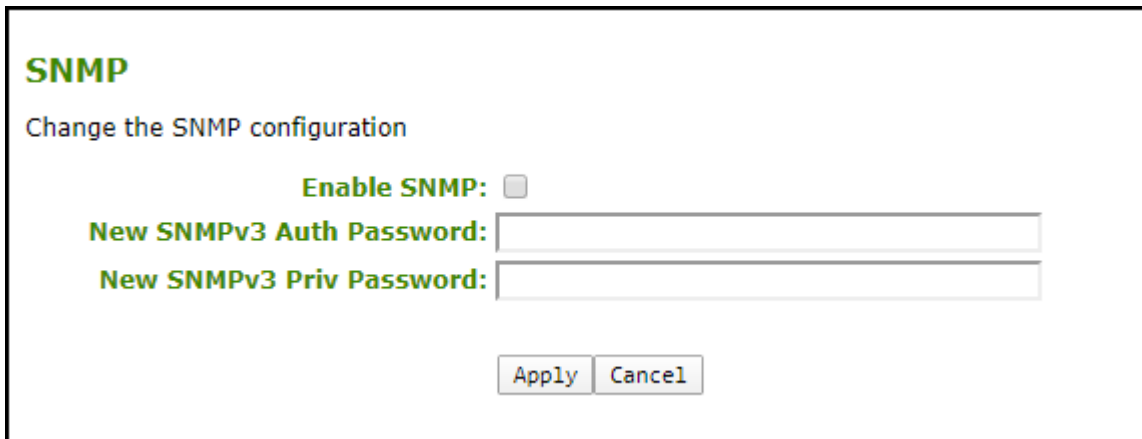
Simple Network Management Protocol (SNMP) allows an administrator to monitor hardware and software endpoints through an SNMP agent. The agent can be enabled on the device you are monitoring, and a SNMP manager can then view the data. From the AWI SNMP page you can enable or disable the SNMP agent. Once enabled, enter the auth and priv password values. The SNMP manager also requires configuration with the correct user name and protocols for SNMPv3 authentication. The SNMPv3 manager must use a username of **pcoip_authpriv**, using another value will cause the connection to fail. The **authentication password** provides user authentication using the SHA protocol while the **private password** provides the encryption key using the AES protocol.

Teradici has provided the Using SNMP with a PCoIP® Endpoint User Guide to provide additional details on SNMP and includes the TERADICI-PCOIPv2-MIB.

SNMP Configuration

Setting	Default	AWI	OSD	Management Console
Enable SNMP	Disabled	✔	✘	✔
SNMPv3 Auth Password	▬	✔	✘✘	✔
SNMPv3 Priv Password	▬	✔	✘	✔

From the AWI SNMP page, you can enable or disable the device's SNMP agent.

AWI SNMP page

To configure SNMPv3 perform the following steps:

1. From the AWI, select **Configuration > SNMP**.

2. Select **Enable SNMP** check box.

   When enabled, the device enables the PCoIP SNMP agent to respond to SNMP requests. Disabling the SNMP agent prevents it from responding to SNMP requests and from generating traps. It also ensures that the PCoIP SNMP MIB cannot be accessed.

3. For **SNMPv3 Auth Password**, enter an 8 - 16 character password to identify the agent with the manager.

4. For **SNMPv3 Priv Password**, enter an 8 - 16 character password to activate encryption of the data stream with the manager.

5. Click **Apply**.

> 🔥 **SNMPv3 Manager Tool**
>
> For connectivity from the SNMPv3 manager, configure the manager with the username of **pcoip_authpriv**. Using another value will cause the connection to fail.

Configuring a Session

The Session page on the AWI allows you to configure how a PCoIP Remote Workstation Card accepts connections from peer devices. The available connection options depend on two parameters—Accept Any Peer and TLS Security Mode. The Differentiated Services Code Point (DSCP) option allows network administrators the ability to prioritize PCoIP traffic within their networks, which can also boost PCoIP network performance.

AWI Session Page

Accept Any Peer

When enabled this parameter allows compatible clients to connect to the PCoIP Remote Workstation Card. Deselecting this setting requires you know the MAC address of a client to peer with the host card.

TLS Security Mode and Encryption Ciphers

The PCoIP data stream is always encrypted, however the PCoIP Remote Workstation Card and client must have compatible security modes to connect. The two options are:

- **Maximum Compatibility: TLS 1.2 or higher with 112-bit or higher elliptic curve encryption**: This option provides maximum compatibility with clients.

- **Suite B: TLS 1.2 with Suite B compliant 192-bit elliptic curve encryption**: This option offers an additional certificate option which must match the configuration on the connecting PCoIP Zero Client. The Suite B option offers the peer-to-peer certificate option for added security. The endpoints will use the AES-256-GCM cipher.

> 🔥 **Blacklisted Cipher Suites**
>
> The Blacklisted Cipher Suites offer maximum flexibility but should not be used if possible.
>
> The blacklist cipher suites allow an administrator the ability to disable the use of certain cipher suites due to any security concerns. The blacklist allows you to protect your system without requiring a firmware update. At least one cipher suite must remain enabled at all times.

Differentiated Services Code Point (DSCP)

DSCP provides PCoIP prioritization capability to compatible network devices, allowing for improved network performance on congested networks.

Session Parameter Options

Parameter	Description
Accept Any Peer	When enabled, the host accepts connections from any client. When disabled, you must specify the MAC address of the peer you want the host to accept.
Peer MAC Address	Enter the MAC address of the client that is allowed to connect to the host. If the **Accept Any Peer** option is enabled, this field is not required and not editable.

Parameter	Description
TLS Security Mode (Session Negotiation Cipher)	Configure the Transport Layer Security (TLS) cipher to use for negotiating the TLS session between the PCoIP client and the PCoIP host. • **Maximum Compatibility: TLS 1.2 or higher with 112-bit or higher elliptic curve encryption**: This option provides maximum compatibility. • **Suite B: TLS 1.2 with Suite B compliant 192-bit elliptic curve encryption.**: This option provides a higher level of security and offers the option of applying a PCoIP Zero Client peer-to-peer certificate.
Blacklisted Cipher Suites	The blacklist cipher suites allow an administrator the ability to disable the use of certain cipher suites due to any security concerns. The blacklist allows you to protect your system without requiring a firmware update. At least one cipher suite must remain enabled at all times. • TLS_RSA_WITH_AES_256_GCM_SHA384 • TLS_RSA_WITH_AES_128_GCM_SHA256 • TLS_RSA_WITH_AES_256_CBC_SHA256 • TLS_RSA_WITH_AES_128_CBC_SHA256 • TLS_RSA_WITH_AES_256_CBC_SHA • TLS_RSA_WITH_AES_128_CBC_SHA
PCoIP Data Encryption Ciphers: (Enabled Session Ciphers)	The enabled encryption mode must match between the host and client for a session to be established. A more secure encryption method implemented in second-generation Tera2 processors, **AES-256-GCM** offers high security and performance between hardware endpoints.
Enable DSCP	When enabled, the device populates the Differentiated Services Code Point (DSCP) field in the IP header, allowing intermediate network nodes to prioritize PCoIP traffic accordingly.
Enable Transport Congestion Notification	When enabled, transport congestion notification is enabled to allow PCoIP endpoints to react accordingly if an intermediate network node sets the congestion notification bit in either the IP header or PCoIP transport header. Note: For more information about the PCoIP transport header, see PCoIP Packet Format.

Configuring Session Bandwidth

From the AWI Bandwidth page (shown next), you can control the bandwidth that your PCoIP Remote Workstation Card uses during a PCoIP session. The following parameters display on the AWI Bandwidth page:

Bandwidth

Configure the device bandwidth limit, target and floor

Device Bandwidth Limit: 90000 kbps (0 = no limit)

Device Bandwidth Target: 0 kbps (0 = disabled)

Device Bandwidth Floor: 0 kbps (0 = use default of 1000 kbps)

Apply   Cancel

AWI Bandwidth page

Three settings found on the AWI Bandwidth page—Device Bandwidth Limit, Device Bandwidth Target, and Device Bandwidth Floor—help the PCoIP protocol use the available network bandwidth effectively.

Device Bandwidth Limit

Enter the maximum bandwidth peak for hosts or clients. When configuring hosts, this setting defines the bandwidth from the host to the client (e.g., graphics data). When configuring clients, it defines the bandwidth from the client to the host (e.g., USB data).

The usable range of the device bandwidth is 1000 to 900000 kbps for Tera2 devices.

The PCoIP processor only uses the required bandwidth up to the **Device Bandwidth Limit** maximum, and dynamically adjusts the bandwidth in response to network congestion. Setting this field to 0 configures the PCoIP processor to use the maximum rate available in the network at any time.

We recommend setting this field to the limit of the network connected to the client and host.

Device Bandwidth Target

Enter the temporary limit on the network bandwidth during periods of congestion. When the host or client detects packet loss, the device bandwidth is rapidly reduced to this value, and then more slowly reduced below it. This allows for a more even distribution of bandwidth between users sharing a congested network link.

Device Bandwidth Floor

Enter the minimum bandwidth when congestion is present and bandwidth is required. This allows you to optimize performance for a network with understood congestion or packet loss. If the bandwidth is not required, the bandwidth used drops below the floor.

When configuring hosts, this setting defines the minimum bandwidth from the host to the client (e.g., graphics data).When configuring clients, it defines the minimum bandwidth from the client to the host (e.g., USB data).

A setting of 0 configures the PCoIP processor to reduce bandwidth to 1000 Kbps during these network impairments. You should have a good understanding of the network topology before setting this to a non-zero value.

> **ℹ PCoIP Algorithm behavior**
>
> The firmware implements a slow-start algorithm that increases the bandwidth used until the required bandwidth is reached, network congestion is detected, or the **Device Bandwidth Limit** is met. It begins at the lesser of the **Device Bandwidth Limit** and 8000 Kbps, and increases the bandwidth used within seconds. The slow-start algorithm allows a graceful session startup for low bandwidth scenarios (e.g., WAN scenarios). After initiating a PCoIP session, users may temporarily notice low bandwidth video artifacts as the algorithm ramps up bandwidth use.
>
> You can avoid the slow-start algorithm by setting the bandwidth floor higher than 8000 kbps, but you must ensure your network capacity is large enough or you will create severe session degradation.

> **⚠ Bandwidth Floor incorrectly configured**
>
> If the bandwidth floor is accidentally set above the actual capacity of the network, then massive packet loss will result since the device will never drop it's active limit below the floor. This will result in severe session degradation. This is why care must be taken when choosing an appropriate bandwidth floor.

Configuring Image Quality

If desired, you can adjust the quality of the images you see during PCoIP sessions. You can set image quality preferences from the AWI Image page. Image quality and bandwidth settings help to determine the performance of your PCoIP deployment. These settings will control the amount of PCoIP data that flows through your available network bandwidth. Considerations for other network traffic should be made when adjusting these settings. The default settings (40, 90, 0) have been found to be beneficial for a wide variety of networks.

Image

Adjust the image quality.

A lower minimum image quality will allow a higher frame rate when network bandwidth is limited.

Use Client Image Settings: ☑

Minimum Image Quality: 50

Maximum Initial Image Quality: 90

Maximum Frame Rate: 0 fps (0 = no limit)

Disable Build To Lossless: ☐

Apply   Cancel

AWI Image page

✏️ **Image quality settings apply to sessions with PCoIP Zero Clients or PCoIP software clients**

Image quality settings apply to sessions between PCoIP Zero Clients or PCoIP Software Clients and PCoIP Remote Workstation Cards.

Image Parameters

Parameter	Description
Use Client Image Settings	The client image settings only take effect in a PCoIP session with a PCoIP Zero Client. This allows different PCoIP clients with different settings to configure the optimal image settings for network connections between them and the Remote Workstation Card. It is only advised to clear this checkbox and override the image settings on the Remote Workstation Card if one is unable to modify the image quality settings on the client. One example is with software clients which do not expose the image quality settings to the end user.
Minimum Image Quality (default 40)	Enables you to compromise image quality and frame rate when network bandwidth is limited. Some use cases may require lower-quality images at a higher frame rate while others need higher-quality images at a lower frame rate. In environments where the network bandwidth is constrained, reduce the number to enable higher frame rates. Increase the number to enable higher image quality through lower frame rates providing a perception-free quality. When network bandwidth is not constrained, the PCoIP system maintains perception-free quality regardless of the **Minimum Image Quality** parameter. The **Maximum Initial Image Quality** must be greater than or equal to the **Minimum Image Quality**.
Maximum Initial Image Quality (default 90)	Decreasing the number reduces the network bandwidth peaks caused by screen content changes, but produces lower quality images. Increasing this value produces higher quality images but also higher bandwidth peaks. This parameter limits the initial quality on the first display frame of a screen change. Unchanged regions of the image are built to a lossless state regardless of this parameter. The **Maximum Initial Image Quality** must be greater than or equal to the **Minimum Image Quality**.
Maximum Frame Rate (default 0)	The maximum frame rate helps you manage multiple PCoIP sessions over a single network link. This setting determines the limit that your users can reach. Set this field to 0 to set no frame limit. If you set a value, a single user is limited to that value. This helps to control the user experience for all your users.

Parameter	Description
Disable Build to Lossless	Clear this check box to retain the PCoIP protocol's build-to-lossless feature, where images continue to be refined in the background until they reach a fully lossless state (that is, identical pixel-for-pixel rendering when compared to the host image source). This is the default (recommended) setting.

Warning: Selecting the Disable Build to Lossless check box degrades images.

Selecting the **Disable Build to Lossless** check box degrades the images presented to the user. Don't select this check box unless your administrator decides that users don't require optimal image quality to perform critical functions.

If you select this check box, the PCoIP protocol rapidly builds the client image to a high quality image that may be perceptually lossless, but is not a fully lossless state. This may provide some bandwidth savings, but is not recommended for use cases that require images and desktop content to be truly lossless.

Configuring Monitor Emulation

The Monitor Emulation page lets you enable or disable monitor emulation for the video ports on your remote workstation. You can access this page from the Configuration > Monitor Emulation menu.

Some PCs and workstations do not boot if a display is not attached. The monitor emulation feature presents a generic display to ensure the boot process completes. When a session is connected, the client display information is sent to the host. For further details about Teradici's monitor emulation feature, see Monitor Emulation.

> ℹ **Monitor Emulation option**
>
> If monitor emulation is performed in hardware for a device, the AWI **Configuration** menu will not have a **Monitor Emulation** option.

AWI Monitor Emulation Page

AWI Tera2 Host Monitor Parameters

Parameter	Description
Enable Monitor Emulation on Video Port 1	When enabled, the host responds to all Display Data Channel (DDC) queries, regardless of whether a PCoIP session is active. If a session is not active, the host provides emulated DDC data. If a session is active, the host provides actual DDC data gathered from the monitor connected to the client's port 1 connector. The ports are mapped one-to-one and in sequential order (e.g., client port 1 to emulated port 1, and so on). When disabled, the host only responds to Display Data Channel (DDC) queries when a PCoIP session is active and a client display is attached. Note: Enabling this field can help resolve problems where video is not present at the client.
Enable Monitor Emulation on Video Port 2	This field affects DDC queries for the port 2 connector, and provides functionality identical to that for the port 1 connector.
Enable Monitor Emulation on Video Port 3	This field affects DDC queries for the port 3 connector, and provides functionality identical to that for the port 1 connector.
Enable Monitor Emulation on Video Port 4	This field affects DDC queries for the port 4 connector, and provides functionality identical to that for the port 1 connector.
Enable Host Hot-Plug Delay	When enabled, allows lengthier hot plug de-assert/assert profiles on the host. Enabling this feature allows the host to resolve black screen issues with certain Linux GPU driver timing expectations.
Enable Accelerated Monitor Emulation	When enabled, this property accelerates the delivery of EDID information to host systems that boot up very quickly (e.g., faster than five seconds), causing blank screens on the remote end. Typically, these are systems with solid-state drives (SSDs).

Configuring Time Settings

The Time page lets you configure Network Time Protocol (NTP) parameters to allow the host event logs to be time-stamped based on NTP time.

> ✏️ **Time Parameter Limitations**
>
> - If the host is configured for DHCP and the DHCP server provides an NTP server address, this address will override any manually configured NTP server. It will also enable NTP if it is disabled.
> - The host does not get time zone or Daylight Saving Time (DST) information from the NTP server.

You can access this page from the **Configuration > Time** menu.

Time
Change the local time configuration

Current time: 03/24/2014 16:56:09

Enable NTP: ☑
Identify NTP Host by: ○ IP address ● FQDN
NTP Host DNS Name: `ntp.teradici.local`
NTP Host Port: `123`

NTP Query Interval: `1` `Day(s)` ▾

Time Zone: `(GMT-08:00) Pacific Time (US & Canada)` ▾

Enable Daylight Saving Time: ☑

Apply | Cancel

AWI Time Page

> ꙮ **Time stamps in event logs**
>
> To simplify system troubleshooting, set the NTP parameters to allow user events to correlate with the relevant diagnostic event log entries.

AWI Time Page Parameters

Parameter	Description
Current Time	Displays the time based on the NTP.
Enable NTP	Enable or disable the NTP feature.
Identify NTP Host by	Select if the NTP host is identified by IP address or by fully qualified domain name (FQDN). If NTP is disabled, this field is not required and is not editable. If you enter an invalid IP address or DNS name, a message appears to prompt you to correct it. The parameter depends on which method you choose. • **IP Address**: Shows the NTP Host IP address • **FQDN:** Shows the NTP Host DNS name
NTP Host Port	Configure the port number of the NTP server. The default NTP server port value is 123.
NTP Query Interval	Configure the query interval. The first field is for the interval period and the second field is for the time unit in minutes, hours, days, or weeks.
Time Zone	Select the local time zone.
Enable Daylight Savings Time	Enable or disable the automatic adjustment for Daylight Saving Time (DST).

Configuring Power Options

Once your PCoIP Remote Workstation Card and remote power cable is installed on the host PC motherboard, you can configure the power settings in the AWI. There are two selections for the **Host Wake Option** and only one for the **Enable Wake-on-LAN (WoL)** parameter. These parameters determine how the PCoIP Remote Workstation Card will behave when a remote power command issued. A prerequisite for using WoL is that the workstation's PCIe slot provides sufficient standby power to the host card.

Remote Power Button: If this option is selected and you have the Remote Workstation Card power button cable installed, you will be able to change the host PC power state by asserting the workstation's front panel power button.

PCIe Wake Input: If this option is selected, you will have the option to wake the host PC by asserting the PCIe WAKEB signal.

Enable Wake-on-LAN: This parameter must be selected to provide the host PC the option to being turned on (wakened) remotely. When the workstation is asleep or shut down, the host card operates in low-power mode in which all functions are disabled except WOL Magic Packet detection. In this mode, the host card monitors the network for a WOL Magic Packet that matches its MAC address. Once the host card receives the WOL Magic Packet, it powers on the workstation by either asserting the workstation's front panel power button or the PCIe WAKEB signal. A prerequisite for using either option is that the workstation's PCIe slot can provide sufficient standby power to the host card.

> ✏️ **Activating Wake-on-LAN magic packet**
>
> PCoIP Zero Client users send Wake-on-LAN magic packets to the Remote Workstation Card by:
>
> - pressing any key on the keyboard (only if a PCoIP session is already active)
> - clicking the PCoIP Zero Client onscreen Connect button
> - by pressing the power button on the PCoIP Zero Client (only if you installed the host card's power button cable)

Resetting to Factory Defaults

You can reset your PCoIP endpoint parameters to the factory default values stored in flash memory. Before resetting your endpoint, you should have a thorough understanding of your current configuration. A factory reset may require you to perform additional configurations or it may require your endpoint to connect to a Management Console should you not be at the location of your endpoint.

If your on-premises endpoint was managed by a Management Console prior to performing a factory reset, the settings to connect to your Management Console will be lost. To get your endpoint back into the Management Console when on premises, you should have your endpoint configured for auto discovery. For further DHCP and DNS autoconfiguration directions, see PCoIP® Management Console Administrators' Guide sections Configuring DNS for Endpoints that use Autodiscovery: or Configuring DHCP for Endpoints that use Autodiscovery:. When configured for autodiscovery, your endpoint will automatically check back into the Management Console when connected to the network. After it establishes communication with the Management Console, ensure it is in the correct Management Console Group and apply any profiles that are required for that endpoint. See Configuring Endpoint Management Discovery Methods for information on where to configure your discovery settings.

If your endpoint was configured for manual discovery prior to performing a factory reset, you might have additional configurations to perform to get it back to the management state you need. For instance, when using self-signed certificates you might have to upload this certificate to the PCoIP endpoint certificate store and then enter the URL for the Management Console in the AWI *Management* page.

Using jumper 15 is generally not required as you can reset the PCoIP Remote Workstation Card parameters from the AWI (**Configuration > Reset Parameters**).

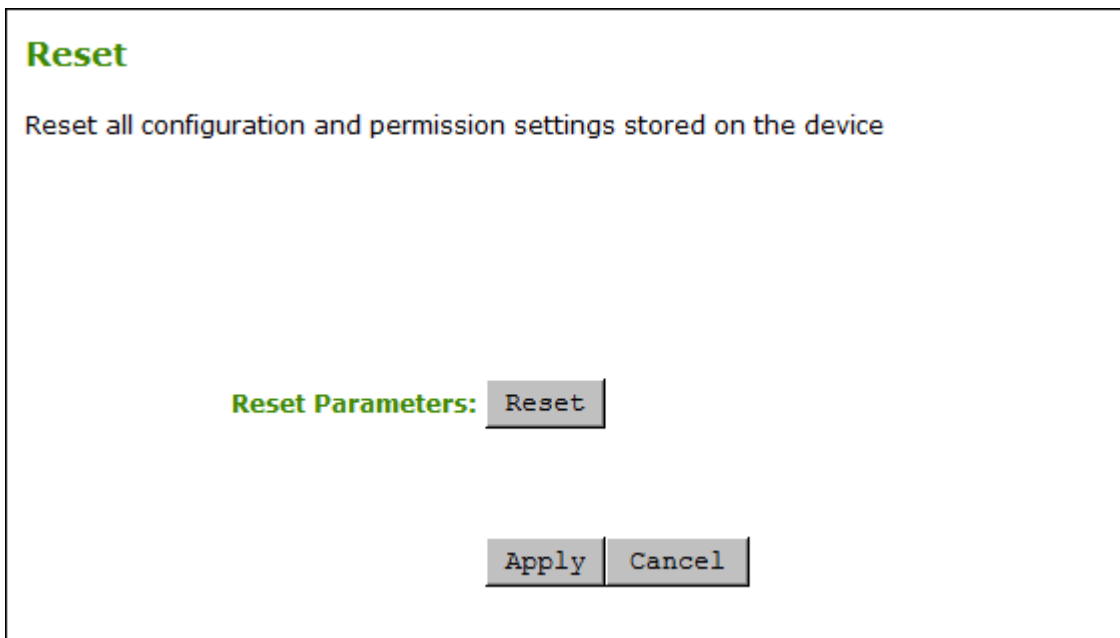## Software Reset Parameters

To reset the endpoint to factory default settings:

1. Browse to the AWI *Reset Parameters* page, and click the **Reset** button and select **OK** on the warning message that appears.

2. Then click the **Reset** button for the Reset PCoIP Processor setting.

3. Then select **OK** to acknowledge the next message that advises the changes will take affect on the next host system restart.

> ✏️ **Factory Default Values**
>
> Resetting parameters to factory default values does not revert the firmware.

AWI Reset Parameters page

Jumpers

All external connectors on Tera2 PCoIP Remote Workstation Cards are for diagnostic purposes. Jumpers J15 and J25 are configurable and their functions are described below.

The picture below shows the location of the jumpers on a Tera2 PCoIP Remote Workstation Card.

Jumper J15 Reset Parameters

This jumper will reset parameters on the host card back to factory default settings.

To reset:

1. Place the jumper on pins 2 and 3 on a PCoIP Remote Workstation Card. If installed into the host PC, ensure the host PC has no power supplied to it.

2. Power on the host PC and wait until the heartbeat pulse is visible on the PCoIP Remote Workstation Card. The PCoIP heartbeat LED flashes twice quickly followed by a slight pause.

3. Power down the host PC containing the PCoIP Remote Workstation Card.

4. Put jumper back to pin 1-2.

5. Power on the host PC.

Jumper J25 Isolated Ground

Adjustment of the ground jumper is not normally required. The power button output from the host card is isolated so that it can be connected to the motherboard in either polarity. Some motherboards do not work with an isolated input and thus require the ground jumper to be installed. This is done by shorting pins 2-3 which requires the power cable to match polarity with the motherboard pins. When left on the default settings (pins 1-2 shorted), the polarity of the power cable is ignored as the power button is now isolated.

LEDs

There are 4 LEDs on the back of the Tera2 PCoIP Remote Workstation Card that serve the same purpose on both the dual and quad cards. The 2 PCoIP LEDs show the health of the PCoIP Remote Workstation Card and the 2 NIC LEDs indicate the NIC status.
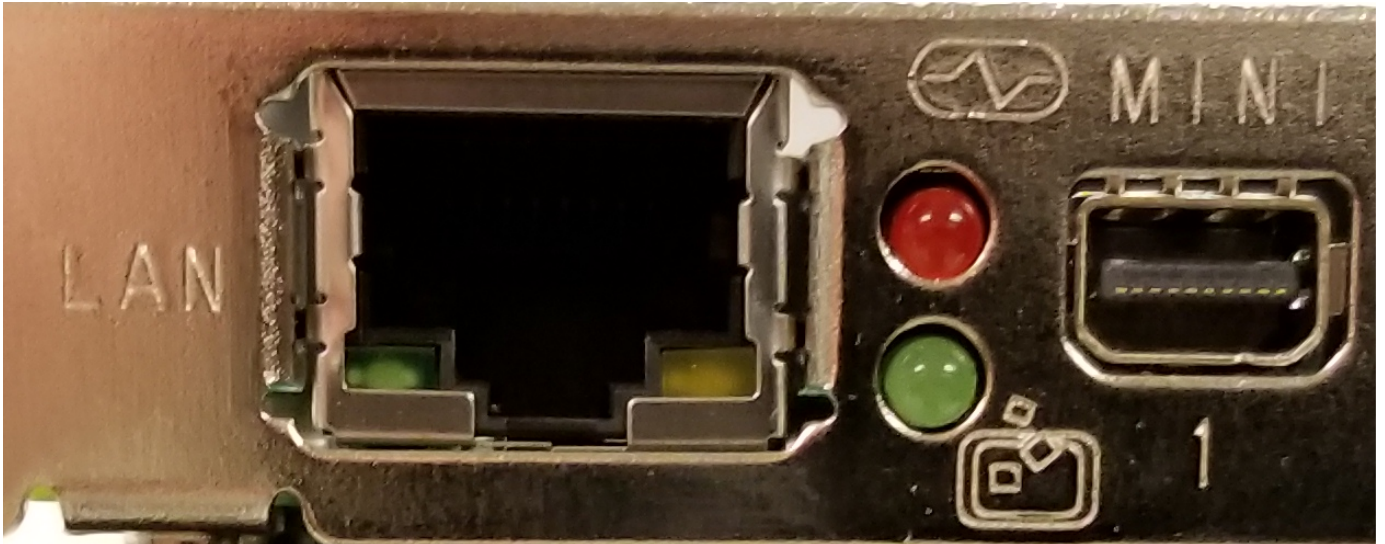
- PCoIP Heartbeat Red LED has a heartbeat icon above it. This LED will normally blink indicating normal operation

- PCoIP Status Green LED has a PCoIP icon below it. This LED will be solid green when in session.

- NIC RJ45 Green LED indicates network activity. This LED blinks during network activity indicating normal operation.

- NIC RJ45 Yellow LED indicates the connections state and is solid when a network connection is established.

PCoIP Remote Workstation Card Security Overview

PCoIP Remote Workstation Cards are easy to manage devices that offer a rich user experience and allow for ultra-secure data transfer. They are available in a variety of form factors from a number of trusted OEMs. With embedded hardware support for PCoIP from the TERA chipset by Teradici, PCoIP Remote Workstation Cards are a natural choice wherever security and performance are critical. The security section of this manual contains configuration options that affect the security of the PCoIP Remote Workstation Card.

Data Control

When control and lockdown of sensitive data are a primary objective, PCoIP Remote Workstation Cards enable an environment where no application data ever leaves the host PC. The host PC sends only encrypted PCoIP data to the PCoIP client where no sensitive application data is ever processed or stored. In a PCoIP session the data is separated into management channel and media (display data, USB data, and audio network traffic) stream, both encrypted.

Encryption

PCoIP Remote Workstation Cards support the following encryption types.

TLS Security Mode for session negotiation security.

- Maximum Compatibility: TLS 1.2 or higher with 112-bit or higher elliptic curve encryption
- Suite B: TLS 1.2 with Suite B compliant 192-bit elliptic curve encryption

PCoIP Data Encryption Ciphers for session security:

- AES-256-GCM

To establish a PCoIP session the PCoIP Remote Workstation Card exchanges information with several services while connecting to endpoint managers, connection managers, and PCoIP clients. These encryption methods are discussed in Security Cipher Suites.

802.1X Network Authentication

PCoIP Remote Workstation Cards support 802.1X network device authentication using EAP-TLS certificates. With 802.1X network authentication, all network end devices must be authenticated before they are granted access to the network. This is a typical method of device authentication for high security environments, providing an additional layer of security beyond username and password credentials.

See Configuring 802.1X Network Device Authentication in the "How To" section for instructions on how to configure PCoIP Remote Workstation Cards for this type of authentication.

Management Security Level

The PCoIP Remote Workstation Card is set to the most flexible management state by default settings. The lowest security setting enables the host be manually discovered by an endpoint management tool and verified by its certificate fingerprint. To further secure PCoIP Remote Workstation Card management, two additional security level options are available—Medium Security Environment and High Security Environment. See About PCoIP Remote Workstation Card Management Security Levels for further information.

Securing Your PCoIP Remote Workstation Card

The security needs of your deployment are driven by your specific environment. You can configure PCoIP Remote Workstation Cards to meet security requirements for a range of scenarios, from high-security environments to trusted environments.

Securing your PCoIP Remote Workstation Card involves some or all of these tasks, depending on your deployment needs:

- **Peering to your PCoIP Zero Client**: Adding a peer-to-peer certificate allows for a secure connection between dedicated Remote Workstation Cards and PCoIP Zero Clients. See Peering Remote Workstation Cards to PCoIP Zero Clients

> 🔥 **Best Security Practices**
>
> Teradici highly recommends using custom peer-to-peer certificates to create a more secure environment when connecting to your Remote Workstation Card. Contact your IT department to ensure your deployment is in accordance with your Company's security policy.

- **Uploading certificates to the PCoIP Remote Workstation Card**: Depending on the certificate checking mode you choose, you may have to upload server certificates to the PCoIP Remote Workstation Card's certificate store. See Uploading Certificates.

- **Configuring the PCoIP Remote Workstation Card with an endpoint manager**: Configure your PCoIP Remote Workstation Card for either automatic or manual discovery by an endpoint manager. See About PCoIP Remote Workstation Card Management Security Levels.

- **Configuring 802.1X Network Device Authentication**: Configure 802.1X network device authentication for enhanced security. See Configuring 802.1X Network Device Authentication.

- **Configuring Access to Management Tools**: Configure a PCoIP device management tool from managing the PCoIP Remote Workstation Card, disable administrative access to the PCoIP Remote Workstation Card's AWI, or force an administrative password change the next time someone accesses the AWI. See Configuring Access Settings.

> 🔥 **You can access additional security functionality from the PCoIP Management Console**
>
> You can configure security settings for multiple devices from the PCoIP Management Console, as well as access additional AWI security settings such as disabling the AWI. For more information, see the PCoIP Management Console Administrators' Guide.

Using an Endpoint Manager

An installed certificate is required to connect to an endpoint manager in medium or high security levels; however, out of the box, the PCoIP Remote Workstation Card's local certificate store is empty and it can only connect using the low security level.

To deploy a system using *medium* or *high* security settings, you must stage the device by connecting to an endpoint manager in low security mode and installing any required certificates or installing the certificate from the AWI.

Once the certificate has been installed, you can connect using any security level.

In some deployments, administrators choose to remove administration of the PCoIP Remote Workstation Card by the PCoIP Management Console or AWI which adds an additional layer of security.

Configuring Access Settings

The Access page lets you prevent the PCoIP device from being managed by the MC (or any other PCoIP device management tool), and lets you disable administrative access to the device's AWI. It also provides an option to force an administrative password change the next time the AWI is accessed.

You can access this page from the **Configuration > Access menu**.

AWI Access Page

These options can also be configured from the PCoIP Management Console 3.1 or newer.

> ⚠ **Enable at least one of the configuration interfaces**
>
> At least one of the device's management configuration interfaces (AWI or MC) must remain enabled at all times. If you disable both management interfaces you will lose the option to perform a software parameter reset should you want to reuse the PCoIP Remote Workstation Card in another deployment. You will be left having to do a hardware jumper parameter reset to regain administrative access to your PCoIP Remote Workstation Card

When the **Disable Management Console Interface** is checked, the management console interface on the PCoIP Remote Workstation Card cannot be accessed or managed by the MC (or any other PCoIP device management tool).

When checked, the **Disable Administrative Web Interface** on the PCoIP Remote Workstation Card cannot be accessed or managed using the AWI.

The **Force password change at next login** causes the administrative password on the AWI to be changed the next time the AWI is accessed. The new password may be blank.

About PCoIP Remote Workstation Card Management Security Levels

There are three available management security level settings in the PCoIP Remote Workstation Card: *low*, *medium*, and *high*. These settings determine whether the PCoIP Remote Workstation Card can be discovered by an endpoint manager, how an endpoint manager can be discovered by the PCoIP Remote Workstation Card, and also dictate whether a certificate must be installed in the PCoIP Remote Workstation Card for discovery to succeed.

The management security level is configured on the Management page of the AWI (see Configuring the Management State). Detailed instructions for allowing discovery under most scenarios, including security level settings, are described in Configuring Endpoint Management Discovery Methods.

The general implications of each security mode are summarized in the following table and described in detail next.

> ✏️ **Discovery Mode definition**
>
> The Discovery Mode setting on the Management page, described here, configures how endpoint managers are discovered by the PCoIP Remote Workstation Card.
>
> Discovery in this context does not refer to discovery of the PCoIP Remote Workstation Card by endpoint managers. For instructions on having an endpoint manager discover your PCoIP Remote Workstation Card, see Configuring Endpoint Management Discovery Methods.

The following table shows the Remote Workstation Card behavior in the three management security modes.

> ✏️ **No High Security Automatic Discovery**
>
> In high security mode, there is no automatic discovery of the management tool by the Remote Workstation Card.

Behaviour	Low Automatic	Low Manual	Medium Automatic	Medium Manual	High Manual
Can be discovered by endpoint managers	✔	✔	✖	✖	✖
Can automatically discover endpoint managers using DNS	✔	:fa-times	✔	:fa-times	:fa-times
Can trust endpoint managers using DNS or DHCP	✔	:fa-times	:fa-times	:fa-times	:fa-times
Can manually connect to endpoint managers	:fa-times	✔	:fa-times	✔	✔
Can trust endpoint managers using an installed certificate	✔	✔	✔	✔	✔

Low Security Mode

In low security mode, both automatic and manual discovery methods are available. Certificates are not required in automatic manager discovery mode if the DNS server is configured to provision the PCoIP Remote Workstation Card with the URI of the endpoint manager's bootstrap server and its certificate fingerprint.

In *automatic* discovery mode the PCoIP Remote Workstation Card:

- can use DNS or DHCP to automatically discover endpoint managers.

- is discoverable by endpoint managers.

- can use DNS to trust the endpoint manager. DNS must be configured to provision your endpoint with the URI and certificate fingerprint of the endpoint manager's bootstrap server.

> ✏ **DNS server configuration information**
>
> For details about how to configure your DNS server for automatic discovery, see the PCoIP® Management Console Administrators' Guide.

In *manual* discovery mode:

- the endpoint must be manually configured with the endpoint manager's bootstrap server URI.

- the endpoint is discoverable by endpoint managers.

- the endpoint does NOT require an installed certificate to trust the endpoint manager.

> ✏️ **Certificates installed on the endpoint**
>
> If a certificate for the endpoint manager has not previously been installed by an endpoint manager in the endpoints certificate store, one must be installed by the endpoint manager or AWI. See Using an Endpoint Manager.

Medium Security Mode

In *medium* security mode, the PCoIP Remote Workstation Card cannot be discovered by endpoint managers. The PCoIP Remote Workstation Card can discover endpoint managers automatically or manually. Certificates are required in medium security mode.

> ✏️ **Certificates installed on the endpoint**
>
> If a certificate for the endpoint manager has not previously been installed by an endpoint manager in the endpoints certificate store, one must be installed by the endpoint manager or AWI. See Using an Endpoint Manager.

In *automatic* discovery mode the PCoIP Remote Workstation Card:

- can use DNS or DHCP to automatically discover endpoint managers.

- is not discoverable by endpoint managers.

- must have an installed certificate to trust the endpoint manager.

In *manual* discovery mode the PCoIP Remote Workstation Card:

- is not discoverable by endpoint managers.

- must be manually configured with the endpoint manager's bootstrap server URI.

- must have an installed certificate to trust the endpoint manager.

High Security Mode

In *high* security mode, the discovery bootstrap phase is disabled.

All settings must be manually configured, and certificates are required.

- cannot use DNS or DHCP automatic discovery.

> ✏️ **Certificates installed on the endpoint**
>
> If a certificate for the endpoint manager has not previously been installed by an endpoint manager in the endpoints certificate store, one must be installed by the endpoint manager or AWI. See Using an Endpoint Manager.

In *manual* discovery mode the PCoIP Remote Workstation Card.

- is not discoverable by endpoint managers.

- must be manually configured with the endpoint managers' internal (and, optionally, external) URI.

- must have an installed certificate to trust the endpoint manager.

About Certificates

Certificates can be used to trust endpoint managers at all security levels, but are required when using medium or high security.

If a PCoIP Management Console certificate is required, you can use an issuer certificate—either the *root CA certificate*, or the *leaf certificate* used to issue the PCoIP Management Console's public key certificate—or the PCoIP Management Console's *public key certificate*.

> ✏️ **PCoIP Management Console certificates**
>
> For complete information about PCoIP Management Console components, including the Endpoint Bootstrap Manager and PCoIP Management Console certificates, see the PCoIP® Management Console Administrators' Guide.

Customer peer-to-peer certificates can also be used to secure PCoIP Zero Clients connecting to Remote Workstation Cards in your deployment. See Peering Remote Workstation Cards to PCoIP Zero Clients and Uploading Certificates for further details on how to upload and apply peer-to-peer certificates.

> 🔥 **OCSP (Online Certificate Status Protocol)**
>
> OCSP (Online Certificate Status Protocol) is currently not supported on PCoIP Remote Workstation Cards.

Uploading Certificates

You can upload and manage your CA root and client certificates for PCoIP Remote Workstation Cards from the AWI's Certificate Upload page, shown next.

AWI Certificate Upload Page

You can simplify the retrieval and installation of digital certificates by enabling devices to obtain certificates automatically from a Simple Certificate Enrollment Protocol (SCEP) server. To upload certificates automatically using SCEP, see Obtaining Certificates Automatically Using SCEP.

Certificates used in PCoIP firmware must be in PEM format with a maximum file size of 10,237 bytes, and maximum RSA key size of 4096 bits. You can upload up to 16 certificates providing you don't exceed the maximum storage size of 163,648 bytes. Each SCEP usage type takes up one of the total number of certificates for upload. As an example, if there are 4 different usage types for certificates obtained using SCEP, there will be room for 12 remaining certificate uploads. The **Available Storage** field lets you know how much space is left in the certificate store. The **Details**

button allows you to view information about the particular certificate such as SCEP usage and key type.

Certificate Details:

Issued To:	pcoip-host-128569·3ee12
Issued By:	CA-INT
Key Usage:	Server Authentication
Subject Alternative Name:	pcoip-host-128569·3ee12.teradici.local,128569·3ee12
Start Date:	11/29/2021 17:34:47 (UTC)
End Date:	11/29/2023 17:34:47 (UTC)
Contains Private Key:	true
Key Type:	RSA
Intended Purpose (SCEP Usage):	Administrative Web Interface

Back

Certificate Details Information

> ✏️ **Authentication issues**
>
> If you have authentication issues after uploading a Connection Server client certificate, see PCoIP TROUBLESHOOTING STEPS: View Connection Server Client Certificates (KB 1363) for further information.

> ✏️ **Include all security information in 802.1X client certificate**
>
> The PCoIP protocol reads just one 802.1X client certificate for 802.1X compliant networks. Make sure you include all the security information for your PCoIP devices in that client certificate. For more information about uploading certificates, see Certificate management for PCoIP Zero Clients and Remote Workstation Cards (KB 1561). For information on 802.1X certificate authentication, see Configuring 802.1X Network Device Authentication.

802.1X Authentication

Consider the following when you use 802.1X authentication:

- 802.1X authentication requires two certificates—an 802.1X client certificate and an 802.1X server CA root certificate.

- The 802.1X client certificate must be in .pem format and contain a private key that uses RSA encryption. If the certificate is in a different format, you must first convert the certificate, including the private key, to .pem format before uploading it.

- After uploading the 802.1X client certificate from the Certificate Upload page, you must configure 802.1X authentication from the Network. This entails enabling 802.1X authentication, entering an identity string for the device, selecting the correct 802.1X client certificate from the drop-down list, and applying your settings.

- The 802.1X server CA root certificate must be in .pem format, but should not need to contain a private key. If the certificate is in a different format, you must convert it to .pem format before uploading it. This certificate does not require configuration from the **Network** page.

- Both the 802.1X client certificate and the 802.1X server CA root certificate must be less than 10,238 bytes; otherwise, you will not be able to upload them. Some certificate files may contain multiple certificates. If your certificate file is too large and it has multiple certificates within, you can open the file in a text editor, copy and save each certificate to its own file.

The following settings display on the AWI Certificate Upload page.

Certificate Upload Parameters

Parameter	Description
Certificate filename	Used to select a certificate to upload. Upload up to a maximum of 16 root and client certificates.
Available Storage:	Amount of remaining storage space to add additional certificates.
Uploaded Certificates	This displays any uploaded certificates. • **Remove button**: Us this button to delete an uploaded certificate. The deletion process occurs after the device is rebooted. • **Details button**: Use this button to quickly view certificate information. See Certificate Details Information image.
Selected Peer-to-Peer Certificate	This is a read-only field. It is linked to the **Peer-to-Peer Certificate** field on the *Session* page.
802.1X Client Certificate	This is a read-only field. It is linked to the **Client Certificate** field on the *Network* page.

To upload a certificate to a PCoIP Remote Workstation Card:

1. From the AWI, select the **Upload > Certificate**.

2. Browse to the folder containing the certificate file. This file will have a `.pem` extension.

3. Double-click the correct * `.pem` certificate file.

4. Click **Upload**.

5. Click **OK** to confirm that you want to proceed with the upload.

6. Click **Continue**.

If the certificate uploads successfully, it will appear in the Uploaded Certificates list on this page.

Peering Remote Workstation Cards to PCoIP Zero Clients

PCoIP Remote Workstation Cards are the only PCoIP hosts that can be peered (paired) to PCoIP Zero Clients using custom certificates to establish a PCoIP peer-to-peer connection that is unique to your environment. This optional but recommended configuration allows for a more secure connection than the default connection.

The custom peer-to-peer certificate and the root certificate (Root CA) or issuing certificate (Issuing CA) must be present in both the Zero Client and Remote Workstation Card certificate store. The custom certificate must then be applied to the **Peer-to-Peer Certificate** field in the AWI **Configuration > Session** page and have the correct **TLS Security Mode** selected. Only certificates that match the selected *TLS Security Mode* option are displayed. Suite B is used in environments requiring Suite B-compliant cryptography. See Encrypting PCoIP Session Negotiation with PCoIP Hosts for further information on encryption suites.

✏️ **Matching PCoIP Zero Client configurations**

Ensure you follow the peer-to-peer procedure on your PCoIP Zero Client before attempting to connect to it. See the PCoIP Zero Client Administrators' Guide for details.

🔥 **Support for Peer-to-Peer Certificates**

- The peer-to-peer connection using certificates supports connections between PCoIP Zero Clients and Remote Workstation Cards only.
- Peer-to-peer certificates can also be requested via SCEP. If using SCEP, the certificate will automatically be selected in the Advanced Session Configuration page. See Obtaining Certificates Automatically Using SCEP.

🔥 **Important: OCSP (Online Certificate Status Protocol)**

OCSP (Online Certificate Status Protocol) is currently not supported for custom peer-to-peer certificates

---

To configure a peer-to-peer connection from a PCoIP Zero Client:

1. Upload both your custom peer-to-peer certificate and your root certificate to your Remote Workstation Card certificate store. See Uploading Certificates for details.

> 🔥 **PCoIP Zero Client Certificate**
>
> Ensure the desired trusted certificate is uploaded to the connecting PCoIP Zero Client certificate store.

2. From the AWI Session page select whether one client or multiple clients can connect to your Remote Workstation Card.

   - Select **Accept Any Peer** if you want any properly configured PCoIP Zero Client to be able to connect to your Remote Workstation Card.

   - De-select **Accept Any Peer** and enter the **Peer MAC Address** of the specific PCoIP Zero Client you want connecting to your Remote Workstation Card.

3. Select the TLS Security Mode you wish to use. (the Zero Client must match this mode)

4. Select the correct **Peer-to-Peer Certificate** from the drop down list. (If it is not displayed, you have not yet uploaded it to the certificate store)

5. Select **Apply** and then **Continue**.

✏️ **Notes**

- If a custom peer to peer certificate is applied and a connection is made, and the custom certificate is removed from the certificate store on either endpoint, a subsequent connection will not establish.
- A connection reset is required before changes take affect.

High Security Settings Checklist

The following table provides a list of PCoIP Remote Workstation Card security settings that are frequently used in high security deployments. Your network administrator or your security advisor must determine whether these settings are appropriate for your own network environment. The most secure options are shown and are presented in the order seen in the AWI.

PCoIP Remote Workstation Card Security Settings

Configuration Category	Setting Name	Setting
Initial Setup	Accept Any Client	False
Network	Enable 802.1X Security	True
Network	Enable 802.1X Authentication Identity	Enter the username configured for the 802.1X authentication
Management	Security Level	High Security Environment - Bootstrap phase disabled
Access	Disable Management Console Interface	False Warning: Disabling both the Management Console and AWI interfaces will make your Remote Workstation Card unmanageable unless a factory reset is performed on the card
Access	Disable Administrative Web Interface	True
Access	Force password change on next login	True
Discovery	Enable SLP Discovery	False
SNMP	Enable SNMP	False

Configuration Category	Setting Name	Setting
Session	Accept Any Peer	False
Session	TLS Security Mode	Suite B: TLS 1.2 with Suite B compliant 192-bit elliptic curve encryption
Session	Peer-to-Peer Certificate	If a custom certificate is uploaded then it will appear in the **Peer-to-Peer Certificate** field and you will be able to select it to be used for PCoIP Zero Client to Remote Workstation Card peer-to-peer connections
Session	PCoIP Data Encryption Ciphers	AES-256-GCM
Session	Enable DSCP	False
USB	Authorized Devices	Enter the USB rule, class, sub class and protocol of *authorized* USB devices bridged to the host PC to gain access to the USB device. Example: To allow USB access to HID devices only, click **Add New** and configure these settings: • Authorized: Rule Type: **Class** Device Class: **Human Interface Device** Sub Class: **Any** Protocol: **Any** • Unauthorized No unauthorization rules. Delete any existing rules. When there are no rules, the MC displays two radio buttons on the Manage Profiles page. Select **Erase the device's existing USB unauthorizations** and replace them with an empty set.

Configuration Category	Setting Name	Setting
USB	Unauthorized Devices	Enter the rule, class, sub class and protocol of *unauthorized* USB devices that are bridged to the host PC to prevent access to the USB device from the host PC. Example: To allow USB access to all devices except mass storage, click **Add New** and configure these settings. • Authorized: Rule Type: **Class** Device Class: **Any** Sub Class: **Any** Protocol: **Any** • Unauthorized: Rule Type: **Class** Device Class: **Mass Storage** Sub Class: **Any** Protocol: **Any**
Certificate Store	N/A	Stores certificates for 802.1X and certificates for secure connections using the management protocol allowing management of the Remote Workstation Card

Security Cipher Suites and Encryption Methods

Overview

The Remote Workstation Card exchanges information with several services while connecting to endpoint managers, and PCoIP clients. The various communication types are described followed by the set of supported TLS cipher suites, Elliptic Curve Cryptography (ECC) curves, or encryption methods available to each type.

> 🔥 **Tip regarding elliptic curve encryption**
>
> Security strength in bits of elliptic curve encryption is ½ of the key size.
>
> Examples:
>
> - If elliptic curve encryption uses the P-384 curve (which needs a 384-bit key), then the security strength is 384/2 = 192 bits.
> - If elliptic curve encryption uses the P-224 curve (which needs a 224-bit key), then the security strength is 224/2 = 112 bits.

Cipher suite and ECC curve order of preference for TLS client based connections are determined by the TLS server the client connects to—such as Management Console or an 802.1x RADIUS Server. TLS server based connections have a preferred order of cipher suites and ECC curves that are determined by the TLS server. The three TLS server based communication types described below are—**Encrypting Browser Connections**, **Encrypting Endpoint Discovery**, and **Encrypting PCoIP Session Negotiation with PCoIP Clients**.

TLS server based connections:

- Encrypting Browser Connections
- Encrypting Endpoint Discovery
- Encrypting PCoIP Session Negotiation with PCoIP Clients

TLS client based connections:

- Encrypting Endpoint Manager Administration

- Encrypting RADIUS Server Using EAP-TLS During 802.1X Authentication

Non-TLS based connections:

- In-Session Encryption

- Encryption in SCEP Requests

Encrypting Browser Connections

PCoIP Remote Workstation Cards allow a browser to connect to the Administrative Web Interface (AWI) over a secure connection. This connection is a TLS server controlled connection and listed in the order of preference. In this scenario, the Remote Workstation Card acts as the TLS server.

The cipher suite and ECC order of preference is listed in descending order where the first entry is the most preferred.

Supported cipher suites:

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

Supported Elliptic Curves:

- NIST P-256

- NIST P-384

- NIST P-521

- NIST P-224

> ✏️ **Recommended Web Browsers**
>
> Recommended web browsers are Firefox, Chrome, and Edge.

Encrypting Endpoint Discovery

PCoIP Remote Workstation Cards that are not managed by an endpoint manager, such as the PCoIP Management Console, listen for incoming discovery requests only when the Management Security Level is set to Low. When an endpoint discovery request from an endpoint manager is received by the PCoIP Remote Workstation Card, communications between the endpoint manager and the PCoIP Remote Workstation Card are established securely using one of the supported cipher suites and ECC curves. In this scenario, the Remote Workstation Card acts as the TLS server.

The cipher suite and ECC order of preference is listed in descending order where the first entry is the most preferred.

Supported cipher suites:

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

Supported Elliptic Curves:

- NIST P-256

- NIST P-384

- NIST P-521

- NIST P-224

Encrypting PCoIP Session Negotiation with PCoIP Clients

PCoIP sessions are negotiated between the PCoIP Remote Workstation Card and the PCoIP client. A client can be a PCoIP Zero Client or a compatible PCoIP Software Client and communications are secured using either **Maximum Compatibility** or **Suite B** cipher suites. In this scenario, the Remote Workstation Card acts as the TLS server.

The cipher suite and ECC order of preference is listed in descending order where the first entry is the most preferred.

- **Maximum Compatibility**: Connections to Zero Clients are limited to two of the common cipher suites and any compatible ECC curve.

  Supported cipher suites:

  - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

  - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

  Supported Elliptic Curves:

  - NIST P-256

  - NIST P-384

  - NIST P-521

  - NIST P-224

- **Suite B**: Suite B can only be used for connections from PCoIP Zero Clients.

  Supported cipher suite:

  - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

  Supported elliptic curve:

  - NIST P-384

Encrypting Endpoint Manager Administration

Once an endpoint manager discovers a PCoIP Remote Workstation Card, it uses the PCoIP Management Protocol to administer the endpoint. Communications between endpoint managers and PCoIP Remote Workstation Cards are secured using one of the supported cipher suites. This is a TLS client based connection.

Supported cipher suites:

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

Supported Elliptic Curves:

- NIST P-256
- NIST P-384
- NIST P-521
- NIST P-224

Encrypting RADIUS Server using EAP-TLS during 802.1X Authentication

In environments that have implemented an 802.1X RADIUS server, the RADIUS server uses the following secure communications to authenticate the endpoint. This is a TLS client based connection.

Supported cipher suites:

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA

Supported Elliptic Curves:

- NIST P-256
- NIST P-384
- NIST P-521
- NIST P-224

In-Session Encryption

Once a PCoIP session has been negotiated and the connection established, PCoIP Remote Workstation Cards encrypt the session data using the AES-256-GCM encryption algorithm. This algorithm secures all PCoIP communications during an active PCoIP session.

Supported Session Algorithm:

- AES-256-GCM

Encryption in SCEP Requests

- Endpoint SCEP requests do not use a TLS connection. The Tera2 endpoint generates its own 3072-bit SCEP RSA private key when certificates other than **Peer-to-peer Suite B** certificates are requested. For **Peer-to-peer Suite B** certificates, the endpoint generates its own ECC P-384 SCEP private key.
  The private key is used to construct parts of the PKCS#10-formatted certificate request which is then delivered to the SCEP server, and the SCEP server's Registration Authority (RA) RSA certificate's public key is used to encrypt the actual certificate request. The SCEP challenge password is encrypted as it is contained within the certificate request.
  The following cryptography algorithms are used to generate a SCEP request:

    - Content Key Encryption Algorithm: **RSAES-OAEP**

    - Hash Algorithm: **SHA384**

    - Content Encryption Algorithm: **AES-256-CBC**

Configuring 802.1X Network Device Authentication

This section describes the components you need to configure 802.1X authentication, and the detailed steps you need to follow to configure the authentication. The 802.1X configurable options are listed in table form and show the default settings and where the options can be managed from.

Preparing for 802.1X Configuration

This section describes the components you need to configure 802.1X authentication, and the detailed steps you need to follow to configure the authentication. The instructions provided in this topic were done on a Microsoft 2019 Datacenter. If you are performing these instructions from a different version of Microsoft Server you may have to consult your server documentation for any changes in procedures.

The supported 802.1X configuration has the Remote Workstation Card pre-populated with a proper certificate. It then connects and presents the certificate to the 802.1X switch and is authenticated. Remote Workstation Cards will also connect under a different configuration of the switch which has the MAC address of authorized endpoints stored in it's configuration.

> ✏️ **Using certificates to sign other certificates**
>
> If a certificate is used to sign another certificate, it must have the digitalSignature key usage field enabled.

Before you begin the configuration process, make sure you have these components:

- Remote Workstation Card with firmware 5.x or newer

- PCoIP Management Console 2.x or newer

- Windows Server 2019 with AD DS (Active Directory Domain Services)

- Windows Server 2019 with AD CS (Active Directory Certificate Services)

- Windows Server 2019 with NPS (Network Policy and Access Services)

- A switch with 802.1X support configured

Configuring Devices for 802.1X Authentication

To configure 802.1X device authentication, complete the following steps:

1. Create a 802.1X Client User.

2. Export the Root CA Certificate.

3. Create a Certificate Template for 802.1X Client Authentication.

4. Issue the 802.1X Client Certificate.

5. Export the 802.1X Client Certificate.

6. Convert the Certificate Format from .pfx to .pem.

7. Import the 802.1X Client Certificate into the Client User Account.

8. Import the Certificates to the 802.1X Client Device.

> ✏️ **The following sections assume you are using Windows Server 2019 Datacenter**
>
> The instructions in the following sections are based on Windows Server 2019 Datacenter. If you are using a newer version of Windows Server, the steps may vary slightly.

Create a 802.1X Client User

In the Windows server, create a 802.1X client user.

To create a client user:

1. Log in to the Windows server.

2. Click **Start > Windows Administrative Tools > Active Directory Users and Computers**.

3. Navigate to **Roles > Active Directory Domain Services > Active Directory Users and Computers > <your_domain.local> > Users**.

4. Right-click Users, select **New > User**, and follow the wizard.
   (Example: Create a user called pcoip_endpoint which would have a UPN name of pcoip_endpoint@<mydomain.local>)

Export the Root CA Certificate

In the Certificate Authority (CA) server, export the root CA certificate.

To export the root CA certificate:

1. Log in to the Certificate Authority (CA) server.

2. Open a Microsoft Management Console window (for example,enter **mmc.exe** in the **Start** menu search field).

3. From the console window, select **File > Add/Remove Snap-in**.

4. Add the **Certificates** snap-in, selecting **Computer account** and then **Local computer**.

5. Click **OK** to close the *Add or Remove Snap-ins* dialog.

6. From the console, select **Certificates (Local Computer) > Trusted Root Certification Authorities > Certificates**.

7. In the right panel, right-click the certificate, and select **All Tasks > Export**.

8. Follow the wizard to export the certificate:

    a. Select **Base-64 encoded X.509 (.CER)** and click **Next**.

    b. Click **Browse**, specify a name and location for the certificate, and then click **Save**.

    c. Click **Finish**, and then click **OK**.

Create a Certificate Template for 802.1X Client Authentication

In the CA server, create a certificate template for client authentication.

To create a certificate template for client authentication:

1. From the CA server, click **Start > Administrative Tools > Certification Authority**.

2. Expand the tree for your CA.

3. Right-click **Certificate Templates**, and then click **Manage**.

4. Right-click the *Computer* template, and then click **Duplicate Template**.

5. Configure the template as follows:

    a. From the *Compatibility* tab, select **Windows Server 2003**.

b. From the *Extensions* tab, ensure the **Digital signature** is included in the certificate **Key Usage**

c. From the *General* tab, enter a name for the template (for example, **PCoIP Endpoint 802.1X**) and change the validity period to match the organization's security policy.

d. From the *Request Handling* tab, select **Allow private key to be exported**.

e. From the *Subject Name* tab, select **Supply in the request** and then click **OK**.

f. From the *Security* tab, select the user who will be requesting the certificate, and give **Enroll** permission to this user.

g. Click **OK** and close the *Certificate Templates Console* window.

6. From the *Certification Authority* window, right-click **Certificate Templates**, select **New**, and then click **Certificate Template to Issue**.

7. Select the certificate you just created (that is, **PCoIP Endpoint 802.1X**), and then click **OK**. The template will now appear in the *Certificate Templates* list.

8. Close the window.

Issue the 802.1X Client Certificate

From the CA Web Enrollment interface for the certificate server, issue the client certificate.

To issue the client certificate:

> ✏ **Use Internet Explorer to log in to certificate server**
>
> Do not use any other browser except Internet Explorer to log into the certificate server or some options may not appear.

1. Using Internet Explorer on your local machine, go to your Certificate Authority URL using the format **https://<server&tgt/certsrv/** (for example, https://ca.domain.local/certsrv/).

2. Click **Request a certificate** and then click **advanced certificate request**.

3. Click **Create and submit a request to this CA**.

4. From the pop-up window, click **Yes**.

5. Fill out the *Advanced Certificate Request* form as follows:

   a. In the *Certificate Template* section, select the certificate for clients (for example, **PCoIP Endpoint 802.1X**).

   b. In the *Identifying Information for Offline Template* section, enter the account name in the *Name* field. The other fields are not required.
   The other fields are not required.

   > ⚠️ **Enter the same name as the universal principal name of the client user**
   >
   > The name you enter in the *Name* field must be the universal principal name (UPN) of the client user you created in Create a 802.1X Client User(for example, **pcoip_endpoint@mydomainlocal**)

   c. In the *Key Options* section, check **Mark keys as exportable**.

   d. In the *Additional Options* section, set the Request Format to **PKCS10**.

   e. If desired, enter a name in the *Friendly Name* field.

   f. Click **Submit**.

   g. From the *Certificate Issued* window, click the **Install this certificate** link.
   (This will save the certificate in the **Current User > Personal** store.)

Export the 802.1X Client Certificate

From the machine on which you issued the certificate, export the client certificate.

To export the client certificate:

1. From the machine on which you issued the certificate, open a Microsoft Management Console window (for example, enter `mmc.exe` in the **Start** menu search field).

2. From the console window, select **File > Add/Remove Snap-in**.

3. Add the **Certificates** snap-in, selecting **My user account**.

4. Click **Finish**, and then click **OK** to close the *Add or Remove Snap-ins* dialog.

5. Select **Certificates - Current User > Personal > Certificates**.

6. In the right panel, right-click the certificate, and select **All Tasks > Export**.

7. Follow the Certificate Export wizard to export the certificate by clicking **Next**:

    a. Click **Yes, export the private key**.

    b. Select **Personal Information Exchange - PKCS #12 (.PFX)**.

    c. Enter a password for the certificate.

    d. Click **Browse**, specify a name and location for the certificate, and then click **Save**.

    e. Click **Next**, **Finish**, and then click **OK**.

8. Repeat Steps 5 to 7 again to export the PCoIP endpoint certificate, but this time without the private key (**No, do not export the private key**), selecting the **DER encoded binary X.509 (.CER)** format instead of the PKCS format.

9. Save this `.cer` file to a location where it can be accessed by the Domain Controller and imported into Active Directory.

Convert the Certificate Format from .pfx to .pem

Using OpenSSL, convert the certificate format from .pfx to .pem.

To convert the certificate format from .pfx to .pem:

1. Download and install Windows OpenSSL from https://www.slproweb.com/products/Win32OpenSSL.html. (The light version is sufficient.)

2. Copy the **.pfx** client certificate file you saved above to the **C:\OpenSSL-Win32\bin** directory.

3. Open a command prompt window (C:\OpenSSL-Win32\bin), and enter the following command to convert the certificate format from **.pfx** to **.pem** where *<client_cert>* is the name of the **.pfx** certificate file you saved to your local machine.

```
openssl.exe pkcs12 -in <client_cert>.pfx -out <client_cert>.pem -nodes
```

4. When prompted, enter the password for the certificate file.

5. At the command prompt, enter the following command to create an RSA private key file where is the name of the .pem certificate file you created in the previous step.

```
openssl.exe rsa –in <client_cert>.pem –out < client_cert>_rsa.pem
```

6. In Notepad:

    a. Open both the original .pem file and the RSA .pem file you just created. The RSA **.pem** file contains only an RSA private key. Because the PCoIP Endpoint certificate requires its private key in RSA format, you need to replace its private key with this RSA private key.

    b. Copy the entire contents of the RSA .pem file (everything from `-----BEGIN RSA PRIVATE KEY -----` to `-----END RSA PRIVATE KEY-----`), and paste it into the original .pem file, replacing its private key with this RSA private key.

> ✏️ **RSA .pem file**
>
> In other words, make sure that all the text from `-----BEGIN PRIVATE KEY-----` to `-----END PRIVATE KEY` (including the dashes) in the *original .pem* file is replaced with the contents of `-----BEGIN RSA PRIVATE KEY -----` to `-----END RSA PRIVATE KEY-----` (including the dashes) from the RSA .pem file.

    c. Save the original **.pem** file and close it. The certificate is now ready to be uploaded to the PCoIP Endpoint.

Import the 802.1X Client Certificate into the Client User Account

In the Windows Domain Controller, import the client certificate into the client user account.

To import the client certificate into the client user account:

1. Log in to the Windows Domain Controller.

2. Click **Start > Administrative Tools > Active Directory Users and Computers**.

3. From the **View** menu, select **Advanced Features**.

4. Navigate to the user you created for the PCoIP Endpoint.

5. Right-click the user, and select **Name Mappings**.

6. In the *X.509 Certificates* section, click **Add**.

7. Locate and select the PCoIP Endpoint certificate you exported that does not contain the private key (This file was saved to a network location in step 9 of Export the 802.1X Client Certificate.)

8. Make sure both identity boxes are selected and click **OK**, and then click **OK** again.

Import the Certificates to the 802.1X Client Device

From the endpoint's AWI, import the certificates.

To import the certificates into a profile using the PCoIP Management Console, see the PCoIP® Management Console Administrators' Guide.

To import the certificates to a device using the AWI:

1. From a browser, log into the AWI for the PCoIP Endpoint.

2. From the AWI, select **Upload > Certificate**.

3. Upload both the Root CA certificate and the certificate with the private key, using the Browse button to locate each certificate and the Upload button to upload them.

4. From the AWI, select **Configuration > Network**.

5. Select **Enable 802.1X Security**.

6. Click **Choose** beside the *Client Certificate* field.

7. Select the certificate with the private key, and then click **Select**.

8. Enter the identity name of the certificate. Typically, this is the universal principal name (UPN) that appears after Subject: (for example, pcoip_endpoint@mydomain.local).

   > ✏️ **Windows server may be configured to use the certificate's Subject, the Subject Alternative Name, or another field**
   >
   > For the identity name, your Windows server may be configured to use the certificate's *Subject*, the *Subject Alternative Name*, or another field. Check with your administrator.

9. To enable greater 802.1X compatibility for older switches on the network, select **Enable 802.1X Support for Legacy Switches**. This setting is only available from the PCoIP endpoints AWI *Network* page.

10. Click **Apply**, and then click **Reset**.

> ✏️ **Getting more information about 802.1X**
>
> For more information about 802.1X, see the following Knowledge Base articles, available from the Teradici Support Center:
>
> - Do PCoIP Zero Clients and PCoIP Remote Workstation Cards support network authentication or 802.1X? (KB 1357)
> - How to set up Windows Server 2008 R2 as an 802.1X Authentication Server (KB 1336)
> - PCoIP Troubleshooting Steps: IEEE 802.1X Network Authentication (KB 1088)

To disable 802.1X authentication on your endpoint:

Disabling 802.1X requires the deselection of the **Enable 802.1X Security** option in the AWI **Configuration > Network** page. It is also recommended that you remove all 802.1X certificates from the endpoint certificate store.

1. Using the AWI browse to **Configuration > Network**.

2. De-select **Enable 802.1X Security**.

3. Browse to **Upload > Certificate**.

4. Select the **Remove** button beside all 802.1X certificates.

5. Click on the **Apply** button.

About USB Settings

USB Overview

From the AWI and Management Console, you can configure access to the host PC operating system for USB devices plugged into PCoIP Zero Client USB ports. For PCoIP Management Console configurations, see the managing profiles topic in the PCoIP Management Console Administrators' Guide.

> ✏️ **Software Client USB support**
>
> USB devices connected to Teradici Software Client hosts are not supported when connecting to Remote Workstation Cards or Remote Workstation Card Agents.

USB plug events are blocked in the Tera2 PCoIP Zero Client firmware by configuring the Unauthorized Devices in its AWI. The PCoIP Remote Workstation Card can also be configured to block USB device access to the host PC for an additional layer of security.

The PCoIP Remote Workstation Card USB permissions has a higher priority than the PCoIP Zero Client and thus overrides the client USB permissions. The authorized and unauthorized tables found in the AWI USB permissions page can each have up to 10 USB devices added. It is strongly recommended you only set the USB permissions on the host when connecting to a PCoIP Remote Workstation Card from a PCoIP Zero Client.

> ✏️ **Endpoint Default Permissions**
>
> The factory defaults have no USB permissions configured on the host. The factory defaults for the client USB permissions are 'any, any, any' for the Authorized devices tables.

The following rules apply when configuring USB permissions.

- If the host has permissions configured, the permissions are sent to the client. If the client has unauthorized devices, they are added to the host's unauthorized devices and the consolidated list is used.
- If the host does not have permissions programmed, the client's permissions are used.

- The host USB permissions are updated at the start of a PCoIP session. They are authorized in the following order of priority (from highest to lowest):

  ◦ Unauthorized Vendor ID/Product ID

  ◦ Authorized Vendor ID/Product ID

  ◦ Unauthorized Device Class/Sub Class/Protocol

  ◦ Authorized Device Class/Sub Class/Protocol

From the AWI you can configure USB permissions to authorize or unauthorize USB devices bridged to the host PC to access the host operating system.

Authorized Table: In this table, you can use the **Add new** button to create up to 10 USB rules that *allow* USB devices to connect to your endpoint based on the USB Vendor ID(VID) and Product ID(PID), or by USB device Class.

Unauthorized Table: In this table, you can use the **Add new** button to create up to 10 USB rules that *prevent* USB devices to connect to your endpoint based on USB ID or USB device Class. You can use wildcards (or specify any) to reduce the number of entries needed to define all devices.

The Class rules include categories Device Class, Sub Class, and Protocol. You can use wildcards (or select **any**) to reduce the number of entries needed to define all devices.
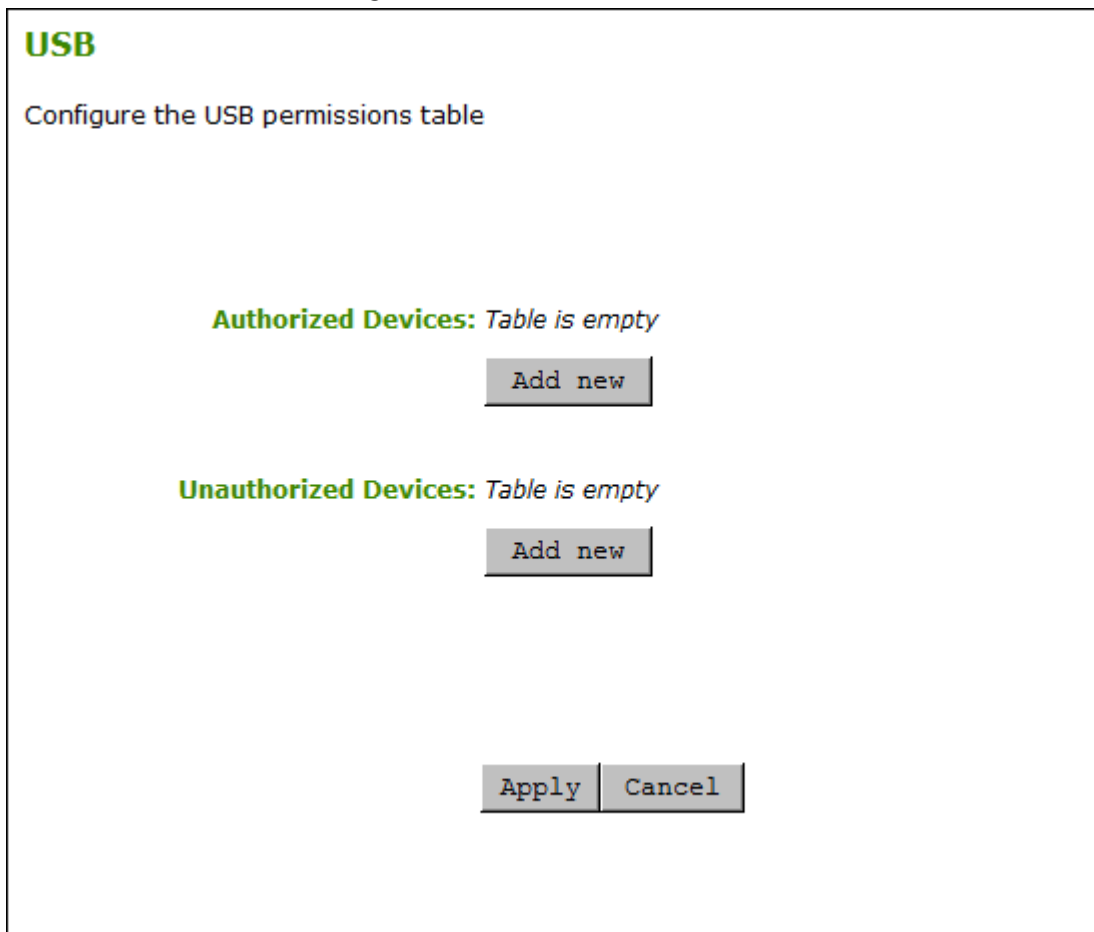
USB Permissions Page

The following categories display on the AWI Permissions > USB page:

Category	Description
Authorized Devices	Lists up to 10 rules that authorize USB devices to connect to your endpoint.
	Add New: This adds a new rule to the authorized table using the USB device's ID, or Class:
	• **ID:** The USB device is authorized by its Vendor ID(VID) and Product ID(PID).
	• **Class:** A group of USB devices are added to the authorized table by creating a rule using USB Device Class, Sub Class, and Protocol.
	Remove: Delete a rule from the table.

Category	Description
Unauthorized Devices	Lists up to 10 rules that prevent USB devices from connecting to your endpoint. **Add New:** This adds a new rule to the unauthorization table using the USB device's ID, or Class: • **ID:** The USB device is unauthorized by its VID and PID. • **Class:** A group of USB devices are added to the unauthorized table by creating a rule using USB Device Class, Sub Class, and Protocol. **Remove:** Delete a rule from the table.

To configure USB settings:

1. From the AWI, select **Configuration > USB**.

AWI USB permissions page

2. From the AWI USB page, update the USB settings by selecting **Add new** and configure the required parameters. The parameters that display depend on whether you describe the device by **Class** or **ID**.

Device Class parameters

Device ID parameters

3. Click **Add**.

4. Click **Apply**.

USB Configuration Parameters

The following parameters display when you authorize or unauthorize USB device parameters:

Parameter	Description
Add new	When adding a new USB authorization or unauthorization entry, select one of the following: • **Class:** The USB device is authorized by its device class, sub-class, and protocol information. • **ID:** The USB device is authorized by its vendor ID and product ID information.
Device Class	This field is enabled when **Class** is selected. Select a supported device class from the drop-down menu, or select **Any** to authorize or unauthorize (disable) any device class.

Parameter	Description
Sub Class	This field is enabled when **Class** is selected.
	Select a supported device sub class from the drop-down menu, or select **Any** to authorize or unauthorize (disable) any sub-class.
	Note: If **Any** is selected as the device class, this will be the only selection available.
Protocol	This field is enabled when **Class** is selected.
	Select a supported protocol from the drop-down menu, or select **Any**.
	Note: If **Any** is selected as the device class or sub-class, this will be the only selection available.
Vendor ID	This field is enabled when **ID** is selected.
	Enter the vendor ID of the authorized (or unauthorized) device. The valid range is hexadecimal 0-FFFF.
Protocol ID	This field is enabled when **ID** is selected.
	Enter the product ID of the (authorized or unauthorized) device. The valid range is hexadecimal 0-FFFF.

Establishing a PCoIP Session to a Remote Workstation Card Overview

After successfully completing the installation steps, the PCoIP Remote Workstation Card will connect to the network when the workstation is powered on. By default, DHCP is enabled on the Remote Workstation Card to allow your DHCP server to assign an IP address to the Remote Workstation Card. If your network does not support DHCP, the card's default IP address will be 192.168.1.100. The PCoIP Remote Workstation Card is by default configured to accept connections from any peer which will allow you to initiate a PCoIP session from any PCoIP Zero Client. TLS Security Mode is set to **Maximum Compatibility: TLS 1.2 or higher with 112-bit or higher elliptic curve encryption** by default to allow for easy setup but can be changed to a more secure setting of **Suite B: TLS 1.2 with Suite B compliant 192-bit elliptic curve encryption** if using a PCoIP Zero Client.

> 🔥 **Session Security Setting**
>
> Ensure your PCoIP Zero Client has a matching session configuration if you are having issues connecting to the PCoIP Remote Workstation Card.

If using a PCoIP Zero Client without a known IP address, you have the option of using SLP discovery. Service Location Protocol (SLP) can dynamically discover devices without requiring prior knowledge of their whereabouts on the network. SLP host discovery requires the PCoIP Zero Client and host PC to reside on the same subnet. You also need to know the IP address and/or MAC address of the Remote Workstation Card so you can select it from the list of available hosts. In addition, the Remote Workstation Card must be configured to accept any peer or to accept the specific MAC address of the PCoIP Zero Client. You can configure this setting from the PCoIP Remote Workstation Card AWI. See Configuring a Session page. To use SLP discovery, it must be configured for use on both the PCoIP Zero Client and Remote Workstation Card. This setting on the Remote Workstation Card is found on the AWI *Discovery* page.

> 🔥 **Using SLP**
>
> A PCoIP Zero Client configured to use SLP reports the first 10 responding PCoIP Remote Workstation Cards. If you do not see the MAC or IP address of your card, you can try reconnecting the PCoIP Zero Client to the network after powering down some or all of the host PCs that you do not want to connect to and see if your IP/MAC address is displayed.

Connections from a Teradici Software Client to Remote Workstation Card require the use of the command line or the installation and licensing of the Remote Workstation Card Agent. Once the Remote Workstation Card Agent is installed and activated on the host computer, clients are required to use the IP address of the host computer NIC or the FQDN of the host computer to connect.

For information on how to configure a connection to a PCoIP Remote Workstation Card using a Teradici PCoIP® Software Client or PCoIP® PCoIP Zero Client, see the Administrators' Guide for the client your are using, available from the Teradici support site or see PCoIP Software Client to Remote Workstation Card or PCoIP Zero Client to Remote Workstation Card

Connecting Remotely Across a Wide Area Network (WAN)
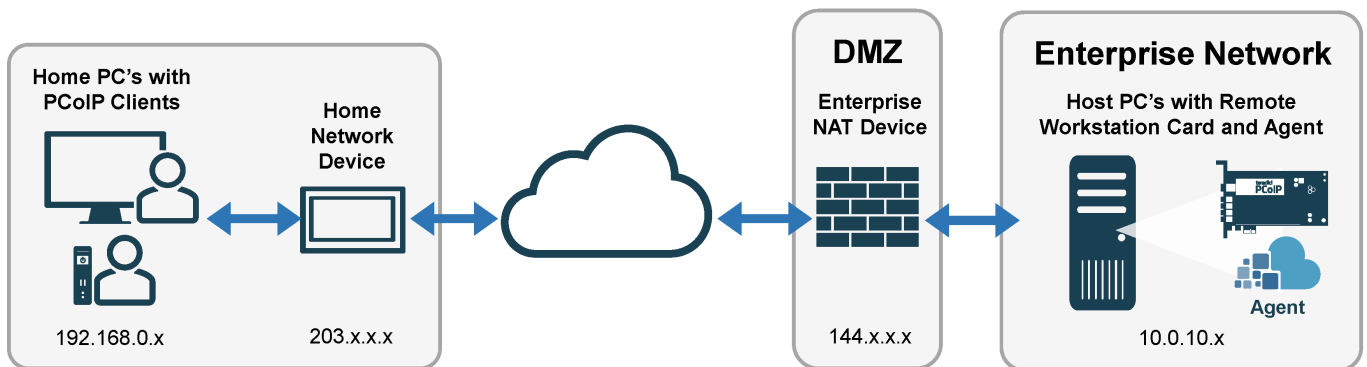
PCoIP sessions between clients and Remote Workstation Cards can operate in a wide area network (WAN) that traverses the Internet with the proper infrastructure. Using a PCoIP Zero Client, you can connect to Remote Workstations Card remotely across the WAN using Network Address Translation (NAT) or a Virtual Private Network (VPN). PCoIP Zero Clients and Remote Workstation Cards use UDP-encapsulated IPsec format. Because this encapsulation type supports IP address and port number translation, it is not necessary to set up a VPN when PCoIP Zero

Clients connect remotely to Remote Workstations Cards and NAT with Suite B certificates can be an option.

You can also connect to PCoIP Remote Workstation Cards remotely with a Teradici Software Client when the Remote Workstation Card Agent is installed.

> **ⓘ Remote Workstation Card Software Assumption**
>
> All Remote Workstation Card scenarios assume you have the PCoIP Remote Workstation Card Software installed on the host PC. For details, please see PCoIP Remote Workstation Card Software for Windows or Linux for further information.

For information connecting from PCoIP Clients see the following articles:

- PCoIP Zero Client Connections

- PCoIP Zero Client Connections Using NAT

- PCoIP Zero Client Connections Using VPN

- Teradici Software Client Connections
  Connections using a Teradici Software Client provides the quickest configuration and requires the installation and licensing of the Remote Workstation Card Agent.

Remote Management

Management of Remote Workstation Cards not on premises can be done from a single management tool such as PCoIP Manamgent Console. See PCoIP Management Console Remote Endpoint Management (Enterprise) for further details.

Connecting from a PCoIP Zero Client

Before connecting a Zero Client to a Remote Workstation Card on a LAN, ensure you have reviewed the following requirements:

- The Remote Workstation Card and host computer NIC are plugged into the same network.

- The PCoIP Zero Client and Remote Workstation Card are using compatible security encryption. See Configuring a Session.

- For high security environments, peer the PCoIP Zero Client and Remote Workstation Card using a Peer-to-Peer certificate configuration. See Peering Remote Workstation Cards to PCoIP Zero Clients for details.

- Ensure the Remote Workstation Card and PCoIP Zero Client have compatible firmware versions identified in the release notes.

  - For information on how to assign a firmware file to a profile using the Management Console, see Management Console Administators' Guide

  - For information on how to upload firmware to a single host or client using the AWI, see Uploading Firmware.

For the best user experience with all the latest features, ensure the following prerequisites are met:

- The networks between the Remote Workstation Card and PCoIP Zero Client are properly configured and optionally have a 1 Gb connection between them for a better experience.

- The PCoIP Remote Workstation Card Software for Windows or Linux is installed on the host PC.

  - The Remote Workstation Card Software requires the Host Firmware Function be enabled. You can enable this setting by logging in to the Remote Workstation Card from the AWI page—**Configuration > Host Driver Function**

- The host PC power cable is connected if you are wanting to power off the host computer via the Zero Client.

- For 4K Zero Client Configurations

To establish a LAN connection:

1. On the PCoIP Zero Client select Connecting direct to host or Connecting using SLP host discovery

2. From the Remote Workstation Card's AWI configure the Session connection type to accept a connection from any peer or enter the MAC IP address of the connecting PCoIP Zero Client.

3. If required for high security environments, peer the PCoIP Zero Client and Remote Workstation Card using a Peer-to-Peer certificate configuration. See Peering Remote Workstation Cards to PCoIP Zero Clients for details.

   • See Creating and Applying Custom Certificates

4. Start a PCoIP session.

Connect Remotely Using Virtual Private Network (Recommended)

The decision to deploy a VPN should be weighed against alternative approaches such as using NAT devices.

The figure below shows a PCoIP session between a PCoIP Zero Client and Remote Workstation Card over a hardware VPN.
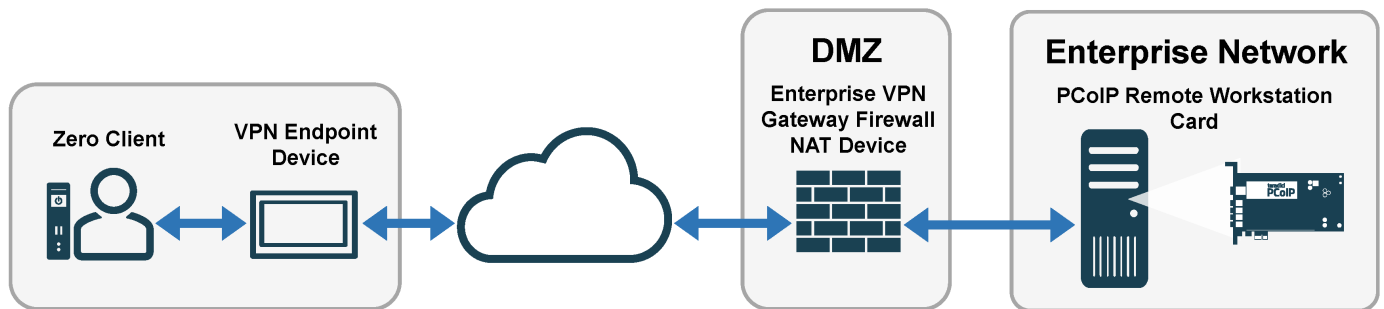
PCoIP Zero Client to Remote Workstation Card over WAN

A VPN is necessary when connecting the following PCoIP endpoints over the Internet.

• PCoIP Zero Client to a Tera2 Remote Workstation Card when the installed firmware in these devices is prior to release 4.1.0

• PCoIP Zero Client or Software Client to a Tera2 Remote Workstation Card when the enterprise NAT device/gateway cannot implement the required IP address and port translation

- Teradici Software Client to a Remote Workstation Card when the Remote Workstation Card Agent is not installed

- Teradici Software Client to a Remote Workstation Card when the client software host PC has no VPN software installed.

To establish the connection:

1. At the home network, install a VPN endpoint device (e.g., a router) and establish a VPN session between the endpoint device and the enterprise VPN gateway. For information on how to set up the VPN, please see the documentation for your device.

2. Configure the enterprise VPN gateway/firewall/NAT device to allow IPsec ESP traffic, and also traffic on UDP port 4172 for the PCoIP data stream and on TCP port 4172 for the TCP handshake.

3. From the PCoIP Zero Client's AWI:

    - Configure the Direct to Host session connection type, and enter the IP address of the Remote Workstation Card.

    - Configure the address of the home VPN endpoint device as the default gateway.

    - Set the packet MTU to be less than or equal to the largest size supported by the VPN tunnel.

    - Peer the Zero Client to the Remote Workstation Card. See Peering Zero Clients to Remote Workstation Cards

4. From the Remote Workstation Card's AWI:

    - Configure the Session connection type.

    - Set the packet MTU to be less than or equal to the largest size supported by the VPN tunnel.

5. Start a PCoIP session.

6. If necessary, adjust bandwidth and image parameters on both the host and client to optimize performance.

For information on optimizing networks for WAN connections, please log in to the Teradici Support Site and see the following Knowledge Base topics:

- Packet size (MTU) settings: KB 1685

- Bandwidth settings: KB 1422

- Image settings: KB 1107

- Windows desktop experience optimization: KB 1359

Connect Remotely Using Network Address Translation with Custom Peer-to-Peer Suite B Certificates

You can have single or multiple PCoIP Zero Clients and Remote Workstation Cards connected behind NAT devices when using custom Peer-to-Peer Suite B certificates. This method applies only to Tera2 devices that employ UDP-encapsulated IPsec ESP encryption.

> ⚠ **Custom Peer-to-Peer Certificates**
>
> Custom Suite B Peer-to-Peer certificates are required to ensure the most secure connections available and is the recommended method when using a NAT configuration. For certificate information see Creating and Applying Custom Certificates

> ✏ **Example IP addresses**
>
> The IP addresses used in the following figures are intended as example addresses only.

Scenario 1: Connecting a PCoIP Zero Client to a Remote Workstation Card (WAN).

This scenario requires you to configure network address translation (NAT) devices with the necessary IP address and port translation at both ends of your network. This scenario describes a single connection from a PCoIP Zero Client to a dedicated Remote Workstation Card located in a different area across the WAN.
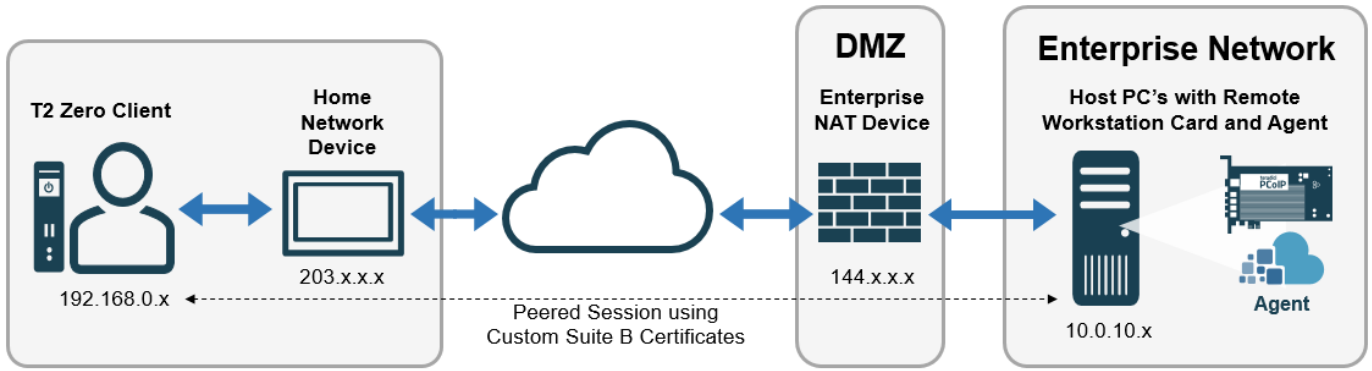
PCoIP Zero Client to Remote Workstation Card over WAN

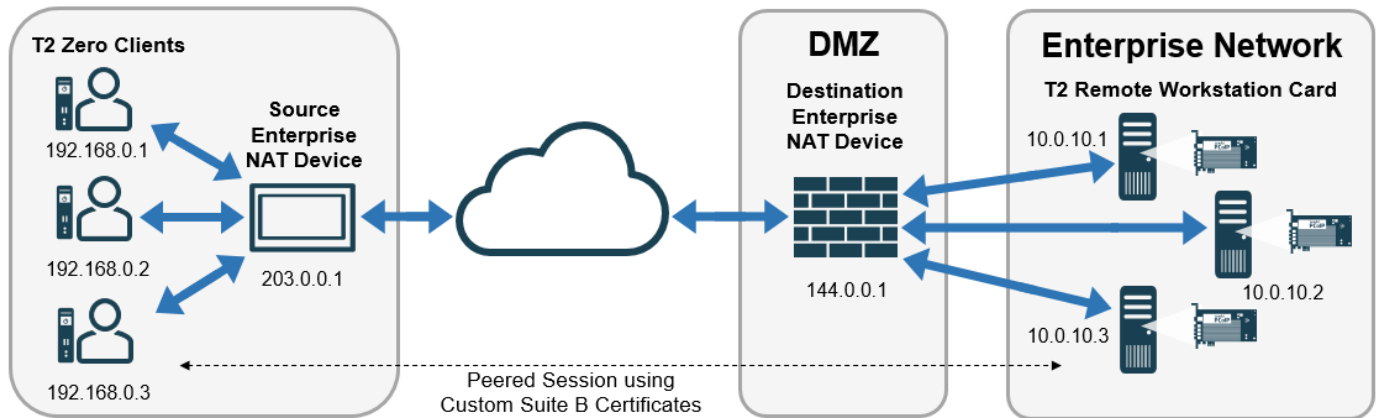To establish the connection perform the following steps:

1. Configure the client side NAT device to redirect TCP/UDP port 4172 to the PCoIP Zero Client.

2. Configure the host side NAT device to redirect TCP/UDP port 4172 to the Remote Workstation Card.

3. Ensure you have a custom Suite B certificate to peer your PCoIP Zero Client to Remote Workstation Card. See Creating and Applying Custom Certificates.

4. From the PCoIP Zero Client's AWI, configure the Peering Zero Clients to Remote Workstation Cards, and enter the IP address of the destination enterprise NAT device.

5. From the Remote Workstation Card's AWI configure Peering Remote Workstation Cards to PCoIP Zero Clients.

6. Start a PCoIP session.

Scenario 2: Multiple PCoIP Zero Client Sessions over WAN

This scenario requires you to configure network address translation (NAT) devices with the necessary IP address and port translation at both ends of your network.

> ℹ️ **NAT**
>
> In this scenario, an **enterprise-level NAT device** is required in both the source and destination networks.

Multiple PCoIP Zero Client Sessions over WAN

To establish the connection perform the following steps:

1. Configure the source enterprise NAT device (203.0.0.1) to translate IP address and ports as follows:

   192.168.0.1:4172 to 203.0.0.1:4172
   192.168.0.2:4172 to 203.0.0.1:4173
   192.168.0.3:4172 to 203.0.0.1:4174

2. Configure the destination enterprise NAT device (144.0.0.1) to translate IP addresses and ports as follows:

   144.0.0.1:4172 to 10.0.10.1:4172
   144.0.0.1:4173 to 10.0.10.2:4172
   144.0.0.1:4174 to 10.0.10.3:4172

3. Ensure you have a custom peer-to-peer Suite B certificate ready to use to peer your PCoIP Zero Client to Remote Workstation Card. See Creating and Applying Custom Certificates.

4. From the PCoIP Zero Client's AWI configure the Peering Zero Clients to Remote Workstation Cards, and enter the IP address of the destination enterprise NAT device.

5. From the Remote Workstation Card's AWI configure Peering Remote Workstation Cards to PCoIP Zero Clients.

6. On your firewall or router, allow both TCP and UDP traffic on the ports you have configured in your NAT devices (4172+).

7. Start a PCoIP session.

8. If necessary, adjust bandwidth and image parameters on both the host and client to optimize performance.

For more information on how NAT applications work with PCoIP, please log in to the Teradici support site and view KB 1623.

Connections from Software Clients

Connections from a Teradici Software Client to Remote Workstation Card require the use of the command line or the installation and licensing of the Remote Workstation Card Agent. Once the Remote Workstation Card Agent is installed and activated on the host computer, clients are required to use the IP address of the host computer NIC or the FQDN of the host computer to connect. Optional host computer changes can improve performance of software client connections. If configuration changes on the host computer are needed, you will need administrator permissions and access to the host computer.

> ✏️ **Software Client USB support**
>
> USB devices connected to Teradici Software Client hosts are not supported when connecting to Remote Workstation Cards or Remote Workstation Card Agents.

The following optional configurations are recommended for the best experience when accessing the Remote Workstation Card.

- Enable monitor emulation on Remote Workstation Card to avoid blank grey screens when you connect. To enable monitor emulation using the AWI, see Configuring Monitor Emulation.

- Disable temporal dithering as it may cause blurriness, heavy packet loss, and high CPU usage on the PCoIP Software Client machine.See KB 1087 for more information.

Prerequisites

- You are using the same release of Teradici Software client as PCoIP Remote Workstation Card firmware or one release prior. Other software client releases may work but are not supported.

- The network the Remote Workstation Card and Teradici Software Client are installed are properly configured and optionally have a 1 Gb connection between them for a better experience.

- The PCoIP Remote Workstation Card is using **Maximum Compatibility** encryption. See Configuring a Session

- For details about PCoIP software client requirements, and instructions on how to configure the client to connect to a Remote Workstation Card, see your Windows, Linux, or macOS software client administrators guide.

Requirements

- The host computer NIC and the Remote Workstation Card is plugged into the same network.
- The PCoIP Remote Workstation Card Agent for Windows or Linux is installed and licensed on the host computer.
- Known IP address:
  - The NIC IP address of the host computer is known for connections via the Remote Workstation Card Agent.
  - The Remote Workstation Card IP address is known for direct connections without the agent.
- The PCoIP Remote Workstation Card Software for Windows or Linux is installed on the host computer.
  - This requires the **Host Firmware Function** is enabled. You can enable this setting by logging into Remote Workstation Card from the AWI page—**Configuration > Host Driver Function**.

> ⚠ **What IP address to connect to**
>
> When the Remote Workstation Card Agent is installed, the IP address of the Remote Workstation Card is not used. Clients must connect to the IP address of the host computer NIC card.

Connecting Remotely using VPN

The same principles that apply for Zero Clients using a VPN apply to Software Clients when connecting to multiple hosts through a WAN. Connections from a Teradici Software Client to a Remote Workstation Card across a WAN will require a VPN with enterprise level NATing devices.

The following directions show how to connect a Windows Software Client to Remote Workstation Card installed in a Windows host computer.

To connect from your Software Client using the Remote Workstation Card Agent:

1. Install the Remote Workstation Card Agent on the host computer that has the Remote Workstation Card installed.

2. Ensure the Remote Workstation Card Software is installed on the host computer.

3. License your Remote Workstation Card Agent.

4. From your Software Client interface enter the IP address or FQDN of the *host computer* in the **Host Address or Code:** field connect.

5. Connect to your Remote Workstation Card host computer.

To connect from your Software Client using the command line without the Remote Workstation Card Agent installed:

1. Confirm the Remote Workstation Card Software is installed on your host computer.

2. Open the command prompt on your client host computer.

3. Enter the following command:

   - **Linux Client**: `pcoip-client.exe --hard-host <RWC_FQDN or RWC_IP_Address>`

   - **Windows Client**: `"pcoip_client.exe --hard-host <RWC_FQDN or RWC_IP_Address>`

🔥 **Create a shortcut**

If you have multiple Remote Workstation Cards to connect to on Windows hosts, create shortcuts to each one using the following:

```
"C:\Program Files (x86)\Teradici\PCoIP Client\bin\pcoip_client.exe" quit-after-disconnect -h
<RWC_IP or RWC_FQDN>
```

Upload a Firmware Release to a Remote Workstation Card

To upload a firmware release to a PCoIP Remote Workstation Card:

1. Ensure the host PC is in an idle state (i.e., that all applications are closed).

2. Log into the host's AWI.

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 correct "*.all" firmware file.

5. Click **Upload**.

6. 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**.

7. Click **Reset**.

8. Click **OK**.

9. Power off and then power on the host PC. It is necessary to power off (not just restart) the PC or workstation in order for the changes to take effect on the Remote Workstation Card.

> ✏️ **Large deployments**
>
> Administrators wanting to apply new firmware to a large number of PCoIP Remote Workstation Cards should consult the managing profiles section of the PCoIP Management Console Administrators' Guide.

Displaying Processor Information

The **Processor** field on the AWI Home page for a host or client displays the name of the device's processor, or chipset.

Processor Information on AWI Home Page

The processor family name and other information displays on the AWI Version page (Info > Version) for a host or client.

Processor Family Information on AWI Version Page

Syslog

Syslog Overview

The syslog protocol is a standard for logging program messages to a database. It is commonly used to monitor devices that do not have a large amount of storage capacity, such as networking devices, ESX servers, PCoIP Zero Clients, and PCoIP Remote Workstation Cards. Using syslog for logging allows you to centralize the storage of log messages and to capture and maintain a longer history of log data. It also provides a set of tools to filter and report on syslog data.

Syslog messages include a facility level (from decimal 0 to 23) that indicates the application or operating system component that is generating the log message. For example, a facility level of "0" indicates a kernel message, a facility level of "1" indicates a user-level message, and a facility level of "2" indicates a message from a mail system. Processes and daemons that have not been explicitly assigned a facility may use any of the eight "local use" facilities ("16 – local use 0" to "23 – local use 7") or they may use the "1 – user-level" facility. Facilities allow for easy filtering of messages generated by a device.

Syslog messages are also assigned a severity level from 0 to 7, where a severity level of "0" indicates an emergency panic condition and a severity level of "7" indicates a debug-level message useful to developers but not for operations.

Configuring Syslog Settings

You can configure syslog settings for a host or PCoIP Zero Client from the device's AWI, or you can use the Management Console to configure settings for a device profile. Both methods are shown below. Configuration involves entering the IP address or fully qualified domain name (FQDN) for the syslog server, and then specifying the port number and facility to use when sending messages to the syslog server.

Teradici uses UDP to send syslog messages to a centralized syslog server. Because most servers use port 514 for incoming messages, Teradici recommends you configure port 514 (the default) as the syslog port to use. However, you can use a different port as long as the syslog server is set to receive syslog messages on the same port as the device is set to send them.

Teradici also uses "19 – local use 3" as the default facility under the assumption that this facility is not commonly used. If it is being used, you can select a different facility.

> ✏️ **Additional Devices**
>
> Cisco IOS devices, CatOS switches, and VPN 3000 concentrators use the "23 – local use 7" facility. Cisco PIX firewalls use the "20 – local use 4" facility.

> 🔥 **Log Messages**
>
> Ensure that your syslog server can handle the volume of messages sent by a PCoIP Zero Client. With some free syslog servers, messages can become lost if the volume is too great.

Setting up Syslog from the AWI

Syslog settings in the AWI are located in the Event Log page. To configure syslog settings from the AWI for a single device:

1. From an Internet browser, enter the IP address of the PCoIP Zero Client or host.

2. Select the **Diagnostics > Event Log** menu to display the **Event Log** page.

3. Check **Enable Syslog**, and then select whether you want to identify the syslog server by its IP address or fully qualified domain name (FQDN).

4. Enter the IP address or FQDN of the syslog server.

5. If the syslog server is configured to receive data on a port other than 514, enter this port number.

6. If you wish the device to use a facility other than the default, select it from the **Syslog Facility** drop-down list.

7. Click **Apply**.

8. At the **Success** page, click **Continue**.

Setting up Syslog from the Management Console

Syslog settings in the Management Console are located in the Management Console's Profiles page. To configure syslog settings from the Management Console for a device profile:

1. From an Internet browser, enter the IP address of the Management Console.

2. Select **PROFILE**.

3. Add or edit the appropriate host/client profile.

4. Select the LOGGING link on the left.

5. Enter the required syslog settings.

6. Click **Save**.

> ✏️ **Entered Values**
>
> You must enter a value in both the Syslog Server Port and Syslog Facility Number fields.

Local Cursor and Keyboard

Local cursor and keyboard is a feature of the PCoIP Remote Workstation Card Software that improves usability for PCoIP sessions operating over WAN connections (latency > 40 ms). When enabled, it allows the PCoIP Zero Client to terminate input from the mouse and keyboard, and to draw the cursor on the attached display(s).

For more information about this feature and instructions on how to enable it, please see the PCoIP® Remote Workstation Card Software for Windows Administrators' Guide Using the Remote Workstation Card Software User Interface WAN Experience - Enable Local Cursor and Keyboard topic.

Monitor Emulation

Teradici's monitor emulation feature for PCoIP Remote Workstation Cards presents a generic display to ensure the boot process completes. It is intended to alleviate issues related to graphics cards that do not enable Display Port or DVI ports when no monitor is detected and/or do not honor hot plug events. These issues can occur during initial BIOS/OS boot or at some time after a full OS boot.

Enabling monitor emulation will provide the motherboard/GPU BIOS, OS, and GPU software driver a valid EDID. In general, the firmware will respond with the last connected monitor EDID when monitor emulation is enabled. If no display has been connected to a port since the device was factory programmed, a default EDID is used. The default monitor definitions shown below.

Monitor Name	TERA DEFAULT
Manufacturer ID	XXX
Monitor Serial Number	000000000000
Established Timing Supported	640x480 @ 60Hz (IBM,VGA) 800x600 @ 60Hz (VESA) 1024x768 @ 60Hz (VESA)
Standard Timing Supported	1280x1024 @60Hz
Native Resolution	1024x768 @60Hz Min Vertical Freq − 50 Hz Max Vertical Freq − 75 Hz
Monitor Range Limits Description	Min. Horiz. Freq − 30 KHz Max Horiz. Freq − 82 KHz Pixel Clock − 140 MHz
EDID Revision	1.4

> ✏️ **Disable monitor emulation**

This feature can be disabled to prevent GPUs from driving unwanted display outputs. When in session, the true hotplug/display state is only bridged from the client if the Teradici Remote Workstation Card Software is installed. This implies that a GPU may drive emulated ports with a video signal, even if the port on the client does not have an attached display.

PCoIP Software Session Variables

The PCoIP software session variables in Microsoft's Group Policy Object (GPO) editor let you configure users' desktops with a collection of parameters that affect PCoIP sessions with soft hosts. These variables are defined in a GPO administrative template file called **pcoip.adm**, which is located on the View Connection Server installation directory (**\\<servername>\c$\Program Files\VMware\VMware View\Server\extras\GroupPolicyFiles\pcoip.adm**).

You can enable and configure PCoIP software session variables in either the Group Policy Object editor's **PCoIP Session Variables > Overridable Administrator Defaults** list to allow users to override settings or the **PCoIP Session Variables > Overridable Administrator Defaults** list to prevent users from overriding settings.

> ✏️ **PCoIP GPO Template**
>
> For large environments, you can apply **pcoip.adm** to a Windows Active Directory organizational unit (OU) or to a machine that you are configuring as a template for a desktop pool. For further details, see "VMware View 5 with PCoIP Network Optimization Guide" from the VMware Documentation website.

For instructions on how to load the PCoIP session variables template to a virtual machine's GPO editor, please see KB 1085 in the Teradici Support Site.

PCoIP Packet Format

PCoIP is a real-time technology that uses UDP as the transport-layer protocol. PCoIP supports two encryption types—UDP-encapsulated ESP and native IPsec ESP. An unencrypted PCoIP transport header field is also present for devices with firmware 4.1.0+ installed and/or for scenarios using View 5.1+. The PCoIP transport header allows network devices to make better QoS decisions for PCoIP traffic.
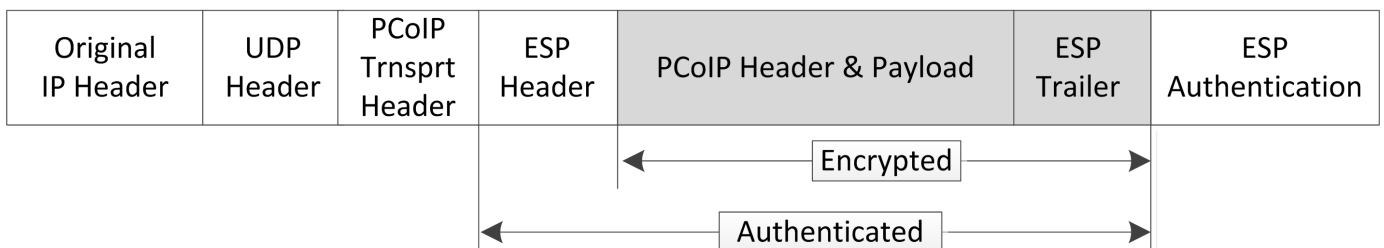
> ✎ **Port 4172**
>
> TCP/UDP port 4172 is the Internet Assigned Numbers Authority (IANA) port assigned to the PCoIP protocol. UDP port 4172 is used for the session data, and TCP port 4172 is used for the session handshake. For more information about TCP/UDP ports that are used for PCoIP technology, see ,KB 1351 on the Teradici Support Site.

UDP-encapsulated ESP Packet Format

UDP-encapsulated ESP is the default packet format for Tera2 devices with firmware 4.1.0 installed. It is also used for Tera1 devices with firmware 3.x+ installed that connect remotely via a View Security Gateway.

The UDP-encapsulated ESP packet format is illustrated in the figure below. This figure also shows the location of the PCoIP transport header in a UDP-encapsulated ESP packet.

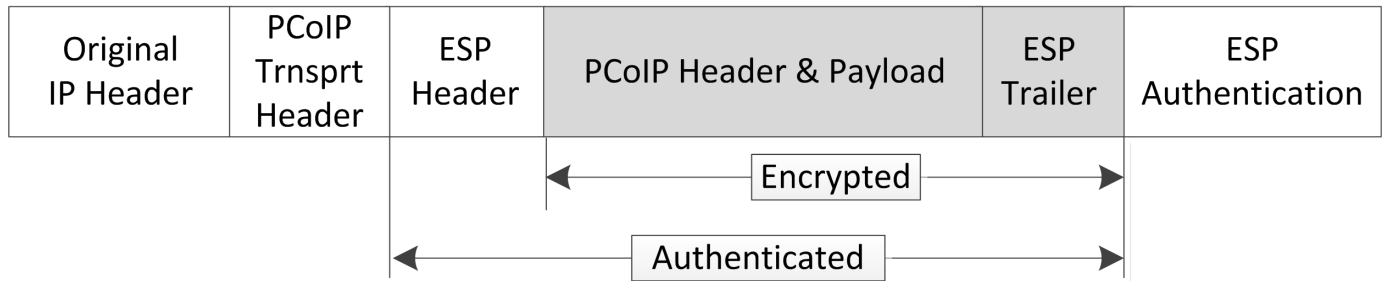| Original IP Header	UDP Header	PCoIP Trnsprt Header	ESP Header	PCoIP Header & Payload	ESP Trailer	ESP Authentication

UDP-encapsulated ESP Packet Format

IPsec ESP Packet Format

IPsec ESP encapsulation is the default packet format for direct connections that involve a Tera1 PCoIP Zero Client and/or Tera1 Remote Workstation Card.

The IPsec ESP packet format is illustrated in the figure below. This figure also shows the location of the PCoIP transport header in an IPsec ESP packet.

Original IP Header	PCoIP Trnsprt Header	ESP Header	PCoIP Header & Payload	ESP Trailer	ESP Authentication

Encrypted

Authenticated

IPsec ESP Packet Format

Creating and Applying Custom Certificates

In order to securely connect your PCoIP Zero Client to a Remote Workstation Card, the certificates must meet PCoIP Zero Client and PCoIP Remote Workstation Card Suite B requirements and both devices must be configured correctly.

This reference provides the Suite B certificate requirements so that you can create your own custom certificate to securely connect your PCoIP Zero Client to a Remote Workstation Card. It also provides the configuration steps to connect your endpoints using the **Suite B: TLS 1.2 with Suite B compliant 192-bit elliptic curve encryption** TLS Security Mode parameter.

Required Certificate Parameters

All Certificate Requirements (Root/Client/Server)

- **Subject** and **Issuer** name must be valid (both the CN and O and cannot be empty).

- **Signature algorithm** must be SHA-384ECDSA.

- **Signature hash algorithm** must be SHA-384.

- **Public key** needs to be an 384 bit elliptic curve key that was generated from the secp384r1 curve (commonly known as the P-384 curve).

- Must be generated as unencrypted .pem files.

Client Certificate Specific Requirements

- **Key Usage** must be Digital Signature or omitted.

- Self signed certificates are not allowed.

Server Certificate Specific Requirements

- **Key Usage** must be Key Agreement, Key Encipherment or omitted.

- Self signed certificates are not allowed.

> ✏️ **Notes**
>
> - The validity period is optional.
> - The Certificate Revocation List (CRL) lookup and Online Certificate Status Protocol (OCSP) is not used.
> - If certificate key usage has both Digital Signature and Key Agreement (or if certificate has no Key Usage), then it is possible to use the same certificate on both host and client.
> - See Samples_v2 for PCoIP Zero Client (client), Remote Workstation Card (server), and Root CA certificates. The **example_suite_b_client_server_combo_cert** sample certificates provided can be used as either a client or server certificate.
> - The Generate_Certificate_Script package has been provided to demonstrate how to generate custom certificates. Unzip and run the **example_suiteb_all_gen.sh** script (certificates will be created in the **certificates** folder).

Perform the following configuration steps on the Remote Workstation Card and PCoIP Zero Client to establish a secure connection with your custom certificates.

Remote Workstation Card Configuration

1. Login to the Remote Workstation Card AWI.

2. Browse to **Upload > Certificate** and **Upload** both the issuer (example_suite_b_root_ca_cert.pem) and server (example_suite_b_client_server_combo_cert.pem) certificates.

3. Browse to **Configuration > Session**.

4. Select **Suite B: TLS 1.2 with Suite B compliant 192-bit elliptic curve encryption** for TLS Security Mode parameter.

5. Select the correct Server certificate for the **Peer-to-Peer Certificate** parameter.

6. Click on **Apply** and then **Continue**.

PCoIP Zero Client Configuration

1. Login to the PCoIP Zero Client AWI.

2. Browse to **Upload > Certificate** and **Upload** both the issuer (example_suite_b_root_ca_cert.pem) and client (example_suite_b_client_server_combo_cert.pem) certificates.

3. Browse to **Configuration > Session**.

4. Select **Direct to Host** for the Session Connection Type and enter the IP address of the Remote Workstation Card that you are connecting to for the **DNS Name** or **IP Address** parameter.

5. Select **Show Advanced Options** and select **Suite B: TLS 1.2 with Suite B compliant 192-bit elliptic curve encryption** for the TLS Security Mode parameter.

6. Select the correct Client certificate for the **Peer-to-Peer Certificate** parameter.

7. From the OSD connect to your Remote Workstation Card.

> ✏️ **Notes**
>
> - If a custom peer to peer certificate is applied and a connection is made, and the custom certificates are removed from the certificate store on either device, a subsequent connection will not establish.
> - A connection reset is required before changes will take affect.