Remote Workstation Card Agent for Windows Administrators' Guide

23.08

Table of Contents

PCoIP Remote Workstation Card Agent for Windows Documentation

This guide is intended for administrators who require brokering of PCoIP clients to computers using Remote Workstation Cards. It assumes administrators have thorough knowledge of conventions and networking concepts, including firewall configuration.

> **Command-line tools are required**
>
> Although many agent features and settings can be configured using the Windows user interface, some administrative tasks require use of Windows command line tools. Users should be familiar with both *cmd* and *PowerShell*.

About the PCoIP Remote Workstation Card Agent for Windows

Remote Workstation Card Agent for Windows introduces brokering to a Remote Workstation Card deployment, allowing the desktop to be managed by HP Anyware Manager, PCoIP Connection Broker or third-party brokers that support the PCoIP Broker protocol.

A complete PCoIP Remote Workstation Card deployment includes these components:

- **A physical host machine**, which provides the desktop to remote clients. See System Requirements for more information.
- **A PCoIP Remote Workstation Card** installed on the host machine.
- **The PCoIP Remote Workstation Card software for Windows** installed on the host machine.
- **The Remote Workstation Card Agent for Windows** installed on the host machine.

About PCoIP Licensing

When the Remote Workstation Card Agent for Windows is installed, the Remote Workstation Card can be licensed using a HP Anyware license. With this flexibility, you can conveniently move to HP Anyware and virtual solutions when you are ready, and without changing licenses.

What's New in This Release

Release 23.08 of the Remote Workstation Card Agent for Windows includes:

- This release maintains version parity with other products.

System Requirements

The Remote Workstation Card Agent for Windows depends on the following system capacities and capabilities:

Supported Instance Types

The Remote Workstation Card Agent for Windows requires a physical machine with a Remote Workstation Card installed.

Host Instance Requirements

Global instance requirements	
Operating Systems	Windows 10 21H2, 22H2 (64-bit Professional and Enterprise)
	Windows 11 21H2, 22H2
	Windows Server 2019, 2022 (single-user only)
Remote Host Memory	At least *2GB* of RAM is required on the host desktop. The agent should have at least *512MB* of available memory.
Remote Host CPUs	At least 2 CPUs are required on the host desktop. Processors must support Streaming SIMD Extensions (SSE) 4.2.
Network Ports	The following ports must be open on the host desktop: • TCP 443 • TCP 4172 • UDP 4172 • TCP 60443
Storage	At least 100MB for installation and 100MB for logging are recommended.

Installation Guide

Anyware Remote Workstation Card Agent for Windows Installation Guide

Before you proceed with installation, a few prerequisites must be met.

Prerequisites

These instructions assume you have already built the remote desktop machine, and that the machine meets the agent's requirements.

A few other things to confirm before proceeding:

- You should have already installed the Remote Workstation Card Software for Windows on the desktop machine.
- The desktop machine requires the following ports to be open: TCP 443, TCP 60443, TCP 4172, and UDP 4172.
- You should be able to run applications as an administrator.
- The Remote Workstation Card Agent for Windows must be able to execute PowerShell scripts. If your PowerShell execution policy set to *Restricted*, the execution policy will be automatically changed so installation can proceed. *If the agent cannot execute PowerShell scripts or change the execution policy, the installation will fail*.
- If you are using a Local License Server, you'll need to know it's URL and port numbers.

Installation Overview

Once your prerequisites are in place, you can proceed with installation. Here's a brief overview of the process:

1. Temporarily connect a physical display, mouse, and keyboard to the machine for installation.

2. Download or transfer the Anyware Remote Workstation Card Agent for Windows installer to the system.
3. Install the Anyware Agent using one of these methods:
    - Using the installer's setup wizard for a guided, interface-driven process, or
    - Silently using a script
4. If required, configure the agent software.
5. Disconnect physical display, mouse, and keyboard.
6. Connect to the desktop using a Anyware client.

If you're ready to start, proceed to installation.

Installing the Anyware Remote Workstation Card Agent for Windows

Download the Remote Workstation Card Agent for Windows Installer

The Remote Workstation Card Agent for Windows installs at the system level and is available to all users. You must have administrator privileges to install it. You can download the installer directly onto the machine, or download it separately and transfer it yourself.

The installer can be downloaded here.

Install or Update the Remote Workstation Card Agent for Windows

Once the installer is present on the desktop, you can run the setup wizard or install it silently using a script. The procedure is the same for new installations and system upgrades.

Installing the Remote Workstation Card Agent for Windows using the Wizard

If you're installing the Remote Workstation Card Agent for Windows via the Windows interface and would prefer to use a graphical interface and guided setup, use the Remote Workstation Card Agent for Windows setup wizard.

Important: Required ports will be automatically opened

The Remote Workstation Card Agent for Windows installer will add firewall exceptions for the following required PCoIP ports during installation: TCP 443, TCP 4172, UDP 4172, and TCP 60443.

To install the Remote Workstation Card Agent for Windows using the setup wizard:

1. Temporarily connect a physical display, mouse, and keyboard to the machine for installation.
2. Navigate to the Remote Workstation Card Agent for Windows installer file and launch it. The setup wizard will appear.

3. Select an installer language and click **OK**.
4. Click **Next** at the welcome screen.
5. Review and accept the license agreement by clicking **I agree**.
6. Specify an installation directory and click **Install**.

   By default, the software will be installed in the `C:\Program Files (x86)\Teradici\Remote Workstation Card Agent for Windows` directory.
7. Provide your licensing information on the License Registration screen.

   Type or paste a registration code in the *Registration code* field and click **Next** for the proxy settings screen.

   > **Important: Local license server users**
   >
   > If you are using a local License Server, do not enter a registration code here. Select **Not now** and then click **Next** instead. You will configure your license server information later.

   - If you use a proxy server to access the internet, select **Use a proxy server for Internet connection** and specify the address and port numbers of the proxy server, then click **Next** to register the license.
   - If your system does *not* use a proxy server, leave this screen unchanged and click **Next** to register the license.
8. The Windows desktop must be rebooted to complete installation; you can choose to do that now, or do it yourself later. Some features may not work until the system is restarted.
9. Click **Finish** to exit the installer.
10. If you skipped license registration, complete registration by following one of the procedures listed here.
11. Disconnect the monitor, keyboard, and mouse.

Scripted Installations

The Remote Workstation Card Agent for Windows can be installed on the desktop programmatically, without using a graphical interface. The installation will proceed silently and the system will reboot when finished.

Scripted installation requires access to the Windows Command Prompt or PowerShell.

Important: Required ports will be automatically opened

The Remote Workstation Card Agent for Windows installer will add firewall exceptions for the following required PCoIP ports during installation: TCP 443, TCP 4172, UDP 4172, and TCP 60443.

To install the Remote Workstation Card Agent for Windows via a script:

1. Temporarily connect a physical display, mouse, and keyboard to the machine for installation.
2. Copy the agent installer file to the desktop.
3. Run the agent installer using one of the following methods:

- **Windows BAT**: Open a Windows command line tool and enter the following:

```
    start /WAIT <path_to_installer> /S /NoPostReboot
    echo %ERRORLEVEL%
```

...where `<path_to_installer>` is the system filepath of the installer file.

- **Windows PowerShell**: Open a PowerShell window and enter the following:

```
    $process = Start-Process -FilePath <path_to_installer> -ArgumentList
"/S /NoPostReboot _?<path_to_installer>" -Wait -PassThru
$process.ExitCode
```

...where `<path_to_installer>` is the system filepath of the installer file. Note that this argument is used twice!

Both methods will return one of these process return codes:

code	description
0	success
1	installation aborted by user (user cancel)
2	installation aborted due to error
1641	success, reboot required

4. If you are using Cloud Licensing, register the Remote Workstation Card Agent for Windows's license by running the `pcoip-register-host.ps1` script:

```
C:\Program Files (x86)\Teradici\Remote Workstation Card Agent for
Windows\pcoip-register-host.ps1 [-ProxyServer <String>] [-ProxyPort
<String>] -RegistrationCode <String> [<CommonParameters>]
```

Where:

- `-RegistrationCode` sets the registration code to use.
- `-ProxyServer` sets the address of your proxy server, if you have one.
- `-ProxyPort` sets the port number of your proxy server, if you have one.

Important: PowerShell execution policy

PowerShell scripts must be permitted to run on your machine. If your execution policy prevents pcoip-register-host.ps1 from running, you can temporarily enable PowerShell script execution with the following command:

```
    powershell.exe -InputFormat None -ExecutionPolicy Bypass -Command .
\pcoip-register-host.ps1
```

Register a License After Installation

In most cases, a PCoIP license is registered during installation. If you are using a local license server, or if you skipped registration during installation, you can register your agent using the methods described next.

- **Registering with Cloud Licensing**: If you are using HP's Cloud Licensing service (most systems use this method), you can register the agent using the PCoIP control panel or via a PowerShell script.
- **Registering with a Local License Server**: If you are serving licenses with your own license server, your registration method depends on your brokering environment. For complete information and instructions, see Licensing Remote Workstation Card Agent for Windowss with a Local License Server.

Licensing The Remote Workstation Card Agent for Windows

The Remote Workstation Card Agent for Windows must be assigned a valid PCoIP session license before it will work. Until you've registered it, you can't connect to the desktop using a Anyware client.

You receive a registration code when you purchase a pool of licenses from HP. Each registration code can be used multiple times; each use consumes one license in its pool.

> ✎ **Note: Registration code format**
>
> Registration codes look like this: `ABCDEFGH12@AB12-C345-D67E-89FG`

PCoIP agent license registrations are managed automatically by HP Anyware's Cloud Licensing Service. If necessary, you can manage them yourself, using your own locally-installed PCoIP License Server instead.

If you need to purchase licenses, contact HP.

Troubleshooting Licensing Issues

If you're encountering problems with HP licensing, refer to Troubleshooting License Issues.

Using HP Anyware Cloud Licensing

To use Cloud Licensing, all you need to do is provide a registration code for each PCoIP agent in your deployment (the same registration code can be used multiple times).

Important: Allowlist network blocks for Anyware Cloud Licensing

If you are using Anyware Cloud Licensing, you will need to add the following to your allowlist:

- `teradici.flexnetoperations.com`
- `teradici.compliance.flexnetoperations.com`

If you use an IP-based allowlist, we recommend your IT team add the following network blocks to your allowlist:

- `IPv4: 185.146.155.64/27`
- `IPv6: 2620:122:f005::/56`

Important: Migrating from the previous specification

Previously, our allowlist specification looked like this:

- **Production**: `64.14.29.0/24`
- **Disaster Recovery**: `64.27.162.0/24`

If you have an existing implementation using an IP-based allowlist like this, we recommend you leave it in place until the new allowlist is active and tested.

The Windows setup wizard collects this registration code during installation. If you're already registered your Anyware agents, there's nothing more to do here. If you've already installed the Anyware agent software but *have not* registered it yet, you can register post-installation using the PCoIP Control panel or via a PowerShell Script.

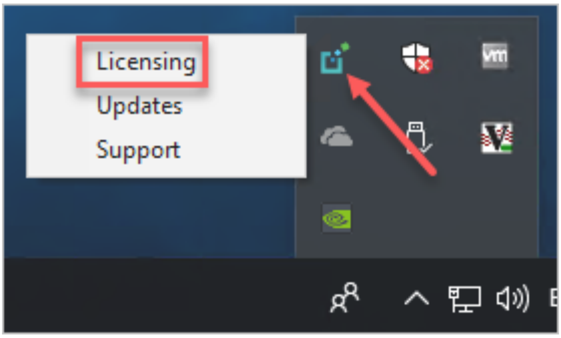
Register or Renew a PCoIP License With the PCoIP Control Panel

Use this method to register or renew an installed Anyware agent using the Windows user interface.

To provide the registration code via the PCoIP Control Panel:

1. Connect to the desktop using RDP (if you're renewing a license that is still active, you can use a PCoIP session to do this instead).

2. Open the *PCoIP control panel* by clicking in the system tray and select **Licensing** from the pop-up menu:



The PCoIP Control panel appears with the licensing tab enabled.

3. Provide the registration code in the registration code field.

Register or Renew a PCoIP License With PowerShell

Use this method to register a Anyware agent using Windows PowerShell. You can do this during a scripted installation, or at any time after installation.

To provide the registration code via the Windows PowerShell script:

1. Connect to your dekstop using RDP.
2. Run the `pcoip-register-host.ps1` script:

```
    "C:\Program Files\Teradici\PCoIP Agent\pcoip-register-host.ps1"
[-ProxyServer <String>] [-ProxyPort <String>] -RegistrationCode <String>
[<CommonParameters>]
```

Where:

- `-RegistrationCode` sets the registration code to use.
- `-ProxyServer` sets the address of your proxy server, if you have one.
- `-ProxyPort` sets the port number of your proxy server, if you have one.

Important: PowerShell execution policy

PowerShell scripts must be permitted to run on your machine. If your execution policy prevents pcoip-register-host.ps1 from running, you can temporarily enable PowerShell script execution with the following command:

```
    powershell.exe -InputFormat None -ExecutionPolicy Bypass -Command .
\pcoip-register-host.ps1
```

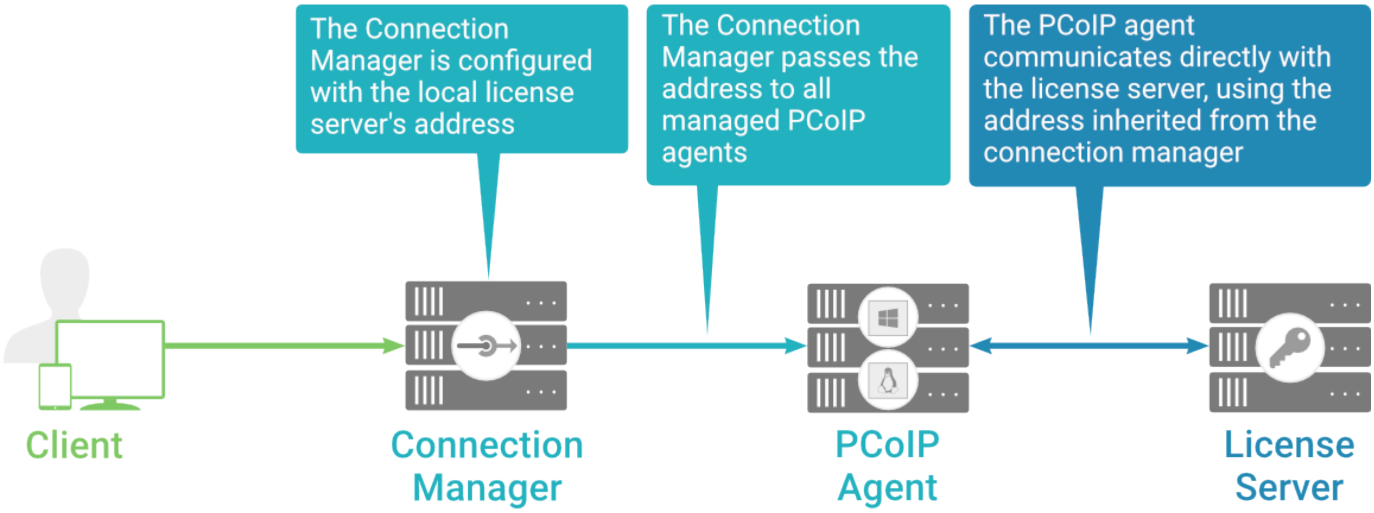
Licensing PCoIP Agents With a Local License Server

In deployments where PCoIP agents cannot access the internet, or where cloud-based licensing is not permitted or desired, a local PCoIP License Server can be used instead. The PCoIP License Server manages PCoIP session licenses within your private environment.

Configuring PCoIP agents to use a local license server is done in one of two ways, depending on whether your deployment uses a PCoIP Connection Manager, or whether your PCoIP clients connect directly to PCoIP agents.

Brokered Environment Licensing

In *brokered* deployments, the license server address is configured in the Connection Manager, which passes it through to its managed PCoIP agents.


The Connection Manager is configured with the local license server's address
The Connection Manager passes the address to all managed PCoIP agents
The PCoIP agent communicates directly with the license server, using the address inherited from the connection manager
Client
Connection Manager
PCoIP Agent
License Server

When using a Connection Manager, the license server address is only configured once no matter how many PCoIP agents are behind the Connection Manager.

To set the License Server URL in the Connection Manager:

1. On the Connection Manager machine, use a text editor to open /etc/ConnectionManager.conf.
2. Set the `LicenseServerAddress` parameter with the address of your local license server:
    - `http://{license-server-address}:{port}/request`
3. Save and close the configuration file.
4. Restart the Connection Manager.

VERIFYING YOUR BROKERED LICENSING CONFIGURATION

To verify your system's licensing configuration, run the `pcoip-validate-license.ps1` PowerShell script on the Anyware Agent machine. The script will ping the license server and attempt to retrieve information on an available license:

```
C:\ProgramFiles\Teradici\PCoIPAgent\pcoip-validate-license.ps1
-LicenseServerUrl <license-server-address> [-ThroughProxyServer <proxy-server-
address>] [-ProxyPort <proxy port>]
```

Where `<license-server-address>` is the address of the license server to ping, formatted as `http://{license-server-address}:{port}/request`

If the license server is behind a proxy server, provide the proxy information via the `-ThroughProxyServer` and `-ProxyPort` parameters.

If successful, the response will show that a valid license was found on the license server, and its expiration date.

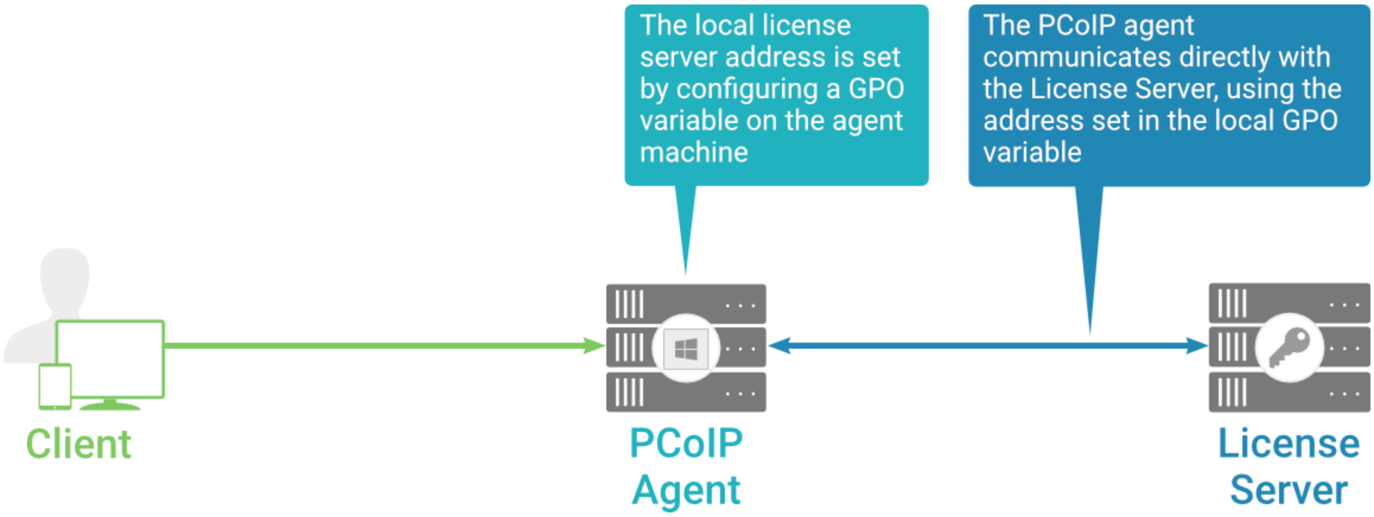
If the connection is unsuccessful, investigate the following possibilities:

- The license server address is incorrect, or formatted incorrectly.
- The license server is inaccessible.
- There are no available licenses on the license server. `pcoip-validate-license.ps1` will only return a positive response if there is at least one available session license.

- If you have only one license on the license server and run `pcoip-validate-license.ps1` from a PCoIP session, the command will fail because you are currently using the single license. In this scenario, disconnect your PCoIP session and try again from an RDP session instead.

Unbrokered Environment Licensing

In direct, or unbrokered, deployments, each PCoIP agent is configured with the license server address via a GPO variable. When a client initiates a new PCoIP session, the PCoIP agent uses its local configuration to communicate with the license server.


The local license server address is set by configuring a GPO variable on the agent machine
The PCoIP agent communicates directly with the License Server, using the address set in the local GPO variable
Client
PCoIP Agent
License Server

Local license validation using a PCoIP Windows agent and a direct (unbrokered) connection

Each PCoIP agent in your environment must be individually configured with the license server's URL.

To configure the License Server URL on the Anyware Agent machine:

1. Open the Local Group Policy Editor on the agent machine:
    a. Press ⊞ + `r` to open the run dialog
    b. type `gpedit.msc` and press `Enter`.
2. Navigate to *Computer Configuration > Administrative Templates > PCoIP Session Variables > Overridable Administrative Defaults*.

    The list of configurable PCoIP settings will appear in the right panel.
3. Open the **Configure the license server URL** variable.
4. Select the **Enabled** option.
5. Enter the License Server URL in the option field and click **OK**. The URL format is `http://{license-server-address}:{port}/request`.

VERIFYING YOUR UNBROKERED LICENSING CONFIGURATION

To verify your system's licensing configuration, run the `pcoip-validate-license.ps1` PowerShell script. The script will ping the license server using the local GPO configuration and attempt to retrieve information on an available license:

```
C:\ProgramFiles\Teradici\PCoIPAgent\pcoip-validate-license.ps1
```

If successful, the response will show that a valid license was found on the license server, and its expiration date.

If the connection is unsuccessful, investigate the following possibilities:

- The license server address is incorrect, or formatted incorrectly.
- The license server is inaccessible.
- There are no available licenses on the license server. `pcoip-validate-license.ps1` will only return a positive response if there is at least one available session license.
- If you have only one license on the license server and run `pcoip-validate-license.ps1` from a PCoIP session, the command will fail because you are currently using the single license. In this scenario, disconnect your PCoIP session and try again from an RDP session instead.

Updating the Remote Workstation Card Agent for Windows

To install an update:

To update the Remote Workstation Card Agent for Windows, copy the new installer file onto the host machine and run it in place, either via the installation wizard or silently via command line.

Unisntalling the Remote Workstation Card Agent for Windows

The Remote Workstation Card Agent for Windows can be uninstalled using the Windows Control panel, or by running the uninstall utility provided in the agent's installation directory.

In either case, you should disconnect any active PCoIP sessions and then connect to the machine *as an administrator* with a physical keyboard, mouse, and display.

- **To uninstall using the Windows Control Panel**: Open the Windows Control Panel, navigate to *Programs > Uninstall a program*, select the Remote Workstation Card Agent for Windows from the list, and click **uninstall**.
- **To uninstall using the provided utility**: Run the executable found at `C:\Program Files (x86)\Teradici\PCoIP Agent\uninst.exe`,

Configuration Guide

You can configure the Remote Workstation Card Agent for Windows, and optimize the PCoIP broker protocol for security, licensing and control panel behavior by adjusting the Windows GPO settings found in the **admx** template files.

Import GPO Template Files

GPO template files are automatically imported by the Remote Workstation Card Agent for Windows installer, *except* on domain controllers. You must manually import the files into the domain controller's Group Policy Editor.

To import the template on a domain controller:

1. Copy the **admx** file from

   ```
   bash
   C:\Program Files\Teradici\PCoIP Agent\configuration\policyDefinitions\PCoIP.admx
   ```

   to

   ```
   bash
   C:\Windows\PolicyDefinitions
   ```

2. Copy the **adml** file from

   ```
   bash
   C:\Program Files\Teradici\PCoIP Agent\configuration\policyDefinitions\en-US\PCoIP.adml
   ```

   to

   ```
   bash
   C:\Windows\PolicyDefinitions\en-US
   ```

Modifying PCoIP GPO Variables

The PCoIP broker protocol settings can be configured using this procedure. The configurable settings are described in the following section.

To modify a PCoIP session variable:

1. Open the Local Group Policy Editor on the agent machine:
    a. Press ⊞ + `r` to open the run dialog
    b. type `gpedit.msc` and press `Enter`.
2. In the left pane, navigate to *Administrative Templates* and then to *PCoIP Session Variables*.

    The variables you can configure appear in the right pane.
3. Double-click the GPO you want to configure to open the variable's configuration window, then:
    a. Select *Enabled* to enable the PCoIP setting.
    b. Configure any parameters that are available for the setting.
    c. Click **OK** to close the GPO's configuration window.
4. Repeat step 3 until all policies have been set.
5. Close the Local Group Policy Editor.

Note: Changes require a new PCoIP connection

Changes take effect on the next PCoIP connection to the desktop.

Only the settings documented here apply to the Remote Workstation Card Agent for Windows

The Remote Workstation Card Agent for Windows man pages document additional configuration settings, beyond those described here. These additional settings apply to virtual machine instances and have no effect on Remote Workstation Card systems. Only the settings described here apply to the Remote Workstation Card.

Configurable Settings

The following settings can be configured on the Remote Workstation Card Agent for Windows. Initially, all settings are **not configured**.

Enable Disclaimer Authentication

Directive	Options	Default
`Enable disclaimer auth`	Enabled (on), Disabled (off), Not configured	Not configured

This setting takes effect when you start the next session. When this setting is enabled, users connecting via direct connect will be presented a disclaimer prior to password based authentication. If the disclaimer is rejected, the user will not be able to connect.

Disclaimer files must be placed in %PROGRAMDATA%\Teradici\PCoIPAgent\disclaimers. Files must be named according to the locale, e.g. **en_US.txt** for en_US, **ko_KR.txt** for ko_KR, etc. If a file matching the negotiated locale is not present, en_US will be used as a fallback. If disclaimer text cannot be found, a blank disclaimer will be presented.

Enable the PCoIP control panel

Directive	Options	Default
`Control panel`	Enabled (on), Disabled (off), Not configured	Not configured

This setting takes effect when the system is restarted. This policy enables or disables the PCoIP control panel. When enabled, the PCoIP control panel will be running, and when disabled the control panel will not be running. When not configured, will run by default.

License server URL

Directive	Options	Default
`License server path`	string *(up to **511* characters)**	Not configured

This setting takes effect when you start the next session. This policy sets the license server path. Enter the license server path in `https://address:port/request` or `http://address:port/request` format.

PCoIP Security Certificate Settings

Directive	Options	Default
`SSL cert type`	From certificate storage Generate a unique self-signed certificate From certificate storage if possible, otherwise generate	Not configured
`Cert store name`	string *(up to **255* characters)*	MY
`SSL cert min key length`	1024 bits 2048 bits 3072 bits 4096 bits	Not configured

This setting takes effect when you start the next session. This policy dictates the handling of certificates.

A certificate is used to secure PCoIP related communications. The way PCoIP components choose a certificate is based on the certificate type, the name of the Certificate Store (referred to as "certificate storage") and the key length. Without a certificate being generated or selected, a PCoIP Session cannot be established.

Depending on the value chosen for the option, 'How the PCoIP agent chooses the certificate...' and the availability of appropriate certificates, PCoIP components may acquire a CA signed certificate from the Windows Certificate Store or generate an in-memory self-signed certificate.

Name the Windows Certificate Store where the CA signed certificate is stored. The default is the "MY" store (shown as "Personal" in Management Console). Set the friendly name of the CA signed certificate to be PCoIP, in the Windows Certificate Store.

CA certificate(s) must be stored in the "Trusted Root Certification Authorities" store (sometimes referred to as "ROOT").

Select a minimum key length (in bits) for choosing a CA signed certificate from the Windows Certificate Store. Longer length certificates will require more computing resources and may reduce performance, but will increase security. Shorter length certificates will provide better performance at the cost of lower security.

Note: Please refer to HP documentation for instructions on creating and deploying certificates.

PCoIP Security Settings

Directive	Options	Default
`TLS security mode`	Maximum Compatibility	Not configured
`TLS cipher blacklist`	string *(up to **1023* characters)*	Not configured
`Data encryption ciphers`	AES-256-GCM, AES-128-GCM (default, AES-256-GCM preferred) AES-256-GCM only AES-128-GCM only	Not configured

This setting takes effect when you start the next session. Controls the cryptographic cipher suites and encryption ciphers used by PCoIP endpoints.

The endpoints negotiate the actual cryptographic cipher suites and encryption ciphers based on the settings configured here. Newer versions of TLS and stronger cipher suites will be preferred during negotiation between endpoints.

If this setting is not configured or disabled, the TLS Security Mode will be set to Maximum Compatibility, and the PCoIP Data Encryption Ciphers will be set to AES-256-GCM, AES-128-GCM.

TLS Security Mode

Maximum Compatibility offers TLS 1.1, 1.2 and a range of cipher suites including those that support Perfect Forward Security (PFS) and SHA-1. Supported cipher suites:

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_AES_256_GCM_SHA384

Blacklisted Cipher Suites

Provides the ability to block specific cipher suites from being offered during negotiation. Must be entered as a semi-colon separated list of cipher suites.

PCoIP Data Encryption Ciphers

Encryption ciphers used for PCoIP UDP data encryption. "AES-256-GCM, AES-128-GCM" is the default setting. AES-256-GCM will get negotiated if the client supports it, otherwise, AES-128-GCM will get negotiated.

PCoIP event log verbosity

Directive	Range	Increment	Default
`Event filter mode`	0 – 3	1	2

This setting takes effect immediately. This policy enables the configuration of the PCoIP event log verbosity ranging from 0 (least verbose) to 3 (most verbose).

When this policy is Disabled or Not Configured, the default event log verbosity setting is 2. When this policy is Configured, the setting controls the verbosity level as described above.

PCoIP log retention

Directive	Range	Increment	Default
`Max log retention days`	7 – 100	1	30

This setting takes effect immediately. This policy sets the retention period (in days) for PCoIP logs that have been archived. PCoIP log files are periodically archived to %PROGRAMDATA%\Teradici\logs\ROTATE. When this policy is Disabled or Not Configured, archived logs that have not been modified in 30 days are removed. When this policy is Configured, the setting controls the retention period as described above.

When configuring a retention period PowerShell 4.0 or newer is required. If an older PowerShell version is installed then the default retention period will be used, regardless of the configured setting.

Proxy Access to a remote License Server

Directive	Options	Range	Increment	Default
`License proxy server`	string *(up to **511** characters)*			Not configured
`License proxy port`		0 – 65535	1	Not configured

This setting takes effect when you start the next session. If a proxy is required to access a local License Server or the Cloud License Server, enter those parameters here. These parameters are loaded only during agent startup.

Making a Connection from a Anyware Client

Anyware clients are remote endpoint devices available as software or firmware devices that make secure PCoIP connections to remote desktops. Once you've installed your Remote Workstation Card Agent, you will have the ability to create brokered connections from *Anyware Clients* to computers with a *Remote Workstation Card*.

For more information about Anyware client connectivity requirements and usage instructions, see the following documentation:

- Software Clients:
  - Anyware Software Client for Windows
  - Anyware Software Client for macOS
  - Anyware Software Client for Linux
- Zero Clients:
  - Anyware Tera2 Anyware Zero Client

Managing Client Connections

All a Anyware client requires is the IP address of the remote computer where the Remote Workstation Card Agent is installed. Simply enter the IP address in the appropriate field of the Anyware client or broker. The broker is responsible for matching users to their available desktops, and then establishing the PCoIP session with their selected resource.

Remote Workstation Card Agent does not need to be configured to use brokering services since all relevant configuration is done at the broker which then communicates with the Remote Workstation Card Agent.

Brokering Options

There are several ways you can manage client connections to remote desktops.

Direct Connections

In this scenario, the Remote Workstation Card Agent acts as its own broker. You only require the IP address of the remote computer NIC to establish a PCoIP session on a properly equipped host computer and client. If using a Tera2 Zero Client, you need to use its session connection type of **Anyware Connection Manager** or **Auto Detect**.

> ✎ **Alternative connections**
>
> Direct connect scenarios where Remote Workstation Card Agent is not installed are not discussed in this guide.

Anyware Manager

Anyware Manager is a service, available as a cloud-based service or as an installable instance, that centrally manages PCoIP deployments. It enables highly scalable and cost-effective HP Anyware deployments by managing cloud compute costs and brokering PCoIP connections to remote Windows or Linux workstations.

Connection Manager

The **Connection Manager** is provided in a bundle with the **Security Gateway**, and allows self-managed brokering services. For information about the Connection Manager, including installation and configuration instructions, see the Connection Manager and Security Gateway documentation.

Third-party Connection Brokers

Anyware agents also support third-party connection brokers. For a current list of brokering partners, see Technology Partners on the website.

Security Guide

Security in PCoIP Agents

PCoIP requires a certificate to establish a session. By default, Anyware agents generate a self-signed certificate that secures the PCoIP session. Each component in the PCoIP system can generate these self-signed certificates, which will automatically work together without requiring any configuration.

You can, if needed, create and deploy your own custom certificates instead of relying on HP's self-signed certificates. This section explains how to create and implement custom certificates.

Using Custom Security Certificates

You can use OpenSSL, Microsoft Certification Authority, or a public certificate authority (CA) of your choice to create your certificates. If you are not using OpenSSL, consult your certificate authority's documentation for instructions on creating certificates in a Windows Certificate Store-compatible format.

The procedures is this section use OpenSSL to generate certificates that will satisfy most security scanner tools when the root signing certificate is known to them.

> ⚠ **Caution: Certificates are stored in the Windows Certificate Store**
>
> Certificates are stored in the Windows certificate store. If you have old certificates that are stored on the host, they should be deleted to avoid conflicts or confusion.

Custom Certificate Guidelines

If you choose to use your own certificates, follow these general guidelines:

- Save your root CA signing certificate in a safe place for deployment to clients.
- Back up private and public keys to secure locations.

- Never store files created when generating keys or certificates on network drives without password protection.
- Once certificates have been deployed to the Windows certificate store, the files they came from are no longer needed and can be deleted.
- Standard automatic tools, such as Automatic Certificate Enrollment and Group Policy, can be used for deploying automatically generated certificates. Both Automatic Certificate Enrollment and Group Policies are implemented through Active Directory. See MSDN Active Directory documentation for more information.

Pre-session Encryption Algorithms

Connections are negotiated using the following supported RSA cipher suites:

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_AES_256_GCM_SHA384

> **Note: Minimum SSL version**
>
> These Max Compatibility security level cipher suites have a minimum required SSL version of TLS 1.2.

Creating And Installing Custom Certificates

This section describes how to replace HP's default certificates with your own custom certificates.

Note: These procedures use OpenSSL

The procedures in this section use OpenSSL to create private keys, certificate signing requests, and certificates. To use OpenSSL, install Visual C++ 2008 Restributables and Win32 OpenSSL Light v1.0.2g+.

For detailed information about OpenSSL, refer to OpenSSL documentation.

To replace HP's default certificates with custom certificates:

1. Install required OpenSSL components on your system.
2. Create the internal root CA certificate.
3. Create a private key and certificate pair for the Anyware agent.
4. Configure the certificate mode for each desktop.
5. Install the internal root CA in your Anyware clients.

Installing OpenSSL Requirements

Install the following components on your Windows machine:

- Visual C++ 2008 Redistributables
- Win32 OpenSSL v1.0.2g Light (or later).

  When prompted during OpenSSL installation, copy the OpenSSL DLLs to the OpenSSL binaries directory; for example, C:\OpenSSL-Win32\bin.

Note: Examples use the default installation directory

The following examples assume the default OpenSSL installation directory: `C:\OpenSSL-Win32`.

Creating the Internal Root CA Certificate

This section shows how to create a root CA private key, how to use this key to self-sign and generate an internal root CA certificate, and how to add X.509 v3 extensions to a certificate that restrict how the certificate can be used.

Creating a Root CA Private Key

To create a root CA private key in RSA format:

1. Open a command prompt and navigate to the OpenSSL binaries directory (`c:\OpenSSL-Win32\bin`).
2. Type `openssl` and press `Enter` to launch OpenSSL.

> **Note: OpenSSL may need help finding the .cfg file**
>
> If you see the following error, you will need to set the OPENSSL_CONF variable before proceeding.
>
> ```
> WARNING: can’t open config file: /usr/local/ssl/openssl.cnf
> ```

3. To create 3072-bit root RSA key named *rootCA.key*, use one of the following commands:

    - For an *unsecured* key, type:

      ```
      genrsa -out rootCA.key 3072
      ```

    - For a *password-protected* key, add the -des3 argument:

      ```
      genrsa -out rootCA.key -des3 3072
      ```

   Password-protected keys require the password to be entered each time they are used.

> **Caution: Store your private root key in a safe location**
>
> Anyone with access to your private root key can use it to generate certificates that your PCoIP clients will accept.

Setting the OPENSSL_CONF variable

If OpenSSL is unable to find its configuration file, you may need to set the OPENSSL_CONF variable.

To set the OPENSSL_CONF variable:

1. Exit OpenSSL.
2. Type the following command:

```
set OPENSSL_CONF=C:\OpenSSL-Win32\bin\openssl.cfg
```

3. Type `ssl` and press `Enter` to continue with the step you were performing when you saw the error.

Self-signing and Creating the Internal Root CA Certificate

Now that we have our private key, we will use it to generate a self-signed X.509 root CA certificate called **rootCA.pem** that is valid for 1095 days (1095 days is three years, ignoring leap days).

To create the root CA certificate:

1. Type the following command. This example creates a certificate that is valid for 3 years (1095 days). Change the `-days` parameter to customize the certificate lifetime:

```
req -x509 -new -nodes -key rootCA.key -days 1095 -out rootCA.pem
```

An interactive script will run, which prompts you to enter values for several fields.

2. Follow the prompts to enter field values:

Field	Notes
Country Name	Optional. Use one of the ISO 3166-1 alpha-2 country codes.
State or Province Name	Optional
Locality name	Optional
Organization Name	Optional
Common name	**Required**. Enter a name for your root CA (for example, certificates.mycompany.com)
Email address	Optional. Enter an administrative alias email if you use this field.

Note: Field values can be templatized

If you will be creating a lot of certificates, consider using a configuration file that contains global field values. See http://www.openssl.org/docs for more information.

Creating a Private Key and Certificate for the Anyware Agent

For each Anyware Agent instance, you will create three items:

- A private key file
- A certificate signing request (CSR)
- A certificate

You will also need an X.509 v3 extension file, which is used as an input when generating the workstation certificate.

Note: There are two different private keys

The private key you create here is used by the Anyware Agent to decrypt data. It is different from the internal root CA private key.

Creating an X.509 Version 3 Extension File

X.509 Version 3 extensions restrict how certificates can be used.

To create the X.509 v3 extension file:

1. Using a text editor, open a new file and paste the following text into it:

```
authorityKeyIdentifier=keyid,issuer
basicConstraints=CA:TRUE
keyUsage=digitalSignature, nonRepudiation, keyEncipherment,
dataEncipherment
subjectAltName=email:test@mycompany.com
```

2. Save the file with an **.ext** extension (for example, `v3.ext`).
3. Store the file in the `C:\OpenSSL-Win32\bin directory`.

> **Note: More about X.509 v3 extensions**
>
> For more information about X.509 v3 certificate extensions, see https://www.openssl.org/docs/apps/x509v3_config.html.

Creating the Private Key and Certificate

To create the Anyware Agent's private key, certificate signing request, and certificate:

1. Launch **openssl** from the `C:\OpenSSL-Win32\bin` directory.
2. Create a *3072-bit private key* in RSA format:

   ```
   genrsa -out pcoipprivate.pem 3072
   ```

   This command creates a pcoipprivate.pem file in the current directory.
3. Create a *certificate signing request*:

   ```
   req -new -key pcoipprivate.pem -out pcoip_req.csr
   ```

   This command initiates an interactive script that prompts you to enter certificate metadata.

   You may be prompted for a challenge password and company name.

   The **Common Name** field must be the fully-qualified domain name (FQDN) of the desktop where the Anyware Agent is installed for example, `mypcname.mydomain.local`. If you want to use the same certificate on multiple machines in the same domain, use a wild card for all but the last two segments of the FQDN: `*.mydomain.local`.

   When finished, this command creates a `pcoip_req.csr` file in the current directory.
4. Sign and create an *X.509 v3 certificate*. This example creates a certificate valid for one year (365 days). To customize the certificate lifetime, change the `-days` parameter:

   ```
   x509 -req -outform PEM -in pcoip_req.csr -extfile v3.ext -CA rootCA.pem -
   CAkey rootCA.key -CAcreateserial -sha256 -out pcoipcert.pem -days 365
   ```

   This command creates a *poipcert.pem* file in the current directory.

⚠ Caution: Use Secure Hash Algorithms

Windows Certificate Manager has deprecated the use some older hash algorithms such as MD4, MD5, and SHA1. Use SHA-384 or SHA-256 when creating your certificates.

5. Create a *PKCS#12 file* to import into a Windows certificate store. Replace `<password>` with your password:

   ```
   pkcs12 -export -in pcoipcert.pem -inkey pcoipprivate.pem -name PCoIP -out
   pcoipagent.p12 -password pass:<password>
   ```

   This command creates a `pcoipagent.p12` file in the current directory.

   Note: The -name parameter must be 'PCoIP'

   You must specify `PCoIP` as the `-name` parameter value. This value sets the certificate's friendly name.

6. Place the `pcoipagent.p12` and `rootCA.pem` files where administrative users of the Anyware agent can access them, such as on network storage or on a USB key.

Installing the Private Key and Certificate on the Anyware agent Desktop

The agent certificate and signing certificate must be installed on each desktop running a Anyware agent.

To install the agent certificate and signing certificate:

1. Open the Microsoft Management Console on the agent machine:
    a. Press ⊞ + `r` to open the run dialog
    b. type `mmc` and press `Enter`.
2. Add the Certificates snap-in:
    a. Select **File** > **Add/Remove Snap-in**.
    b. Select **Certificates** from the Available snap-ins list and click **Add**.
    c. Select **Computer account** and click **Next**.
    d. Select **Local computer** and click **Finish**.
    e. Click **OK**.
3. Add `rootCA.pem` to the 's Trusted Root Certification Authorities list:
    a. Expand **Certificates (Local Computer)**.
    b. Right-click **Trusted Root Certification Authorities**, select **All Tasks** > **Import from the context menu**, and click **Next**.
    c. Use the Browse button to navigate to the directory where the `rootCA.pem` file is located.
    d. Select **All Files (*.*)** from the File name drop-down list, and select the `rootCA.pem` file.
    e. Click **Open**, **Next** (twice), and **Finish**.
    f. Click **OK** to close the *The import was successful* message.
4. Add `pcoipagent.p12` to the Personal store of the agent's computer account:
    a. Expand **Certificates (Local Computer)**.
    b. Right-click **Personal**, select **All Tasks** > **Import** from the context menu, and click **Next**.

c. Select **Personal Information Exchange (*.pfx;*.p12)** from the File name drop-down list, and select the `pcoipagent.p12` file.

d. Click **Open** and **Next**.

e. Type the certificate password.

f. Ensure these settings are correct:

- **Mark this key as exportable...** is enabled
- **Include all extended properties** is enabled

g. Click **Next** twice and **Finish**.

h. Click **OK** to close the The import was successful message.

5. Restart the Anyware agent service on the workstation:

a. Open Control Panel and select **Administrative Tools**.

b. Double-click **Services**.

c. Select your Anyware agent service in the Services list.

d. Click **Restart the service**.

Installing the Internal Root CA Certificate in a Anyware client

Your root CA certificate must be installed in any Anyware client that will be used to connect to the Anyware agent.

Installing Root CA Certificates on a Zero Client

Zero clients are managed via an Administrative Web Interface (AWI) and accessed using a web browser. Supported browsers are:

- Firefox 86
- Chrome 60
- Internet Explorer 11
- Microsoft Edge 25

> **Note: Browser must support TLS**
>
> Web browsers must support TLS 1.2 or later to connect to the zero client's Administrative Web Interface.

To upload the root CA certificate to a zero client:

1. From a supported browser, enter the IP address of the zero client and log in to its Administrative Web Interface.
2. Select the **Upload** > **Certificate** menu to display the *Certificate Upload* page.
3. In the *Certificate filename* field, click **Browse**, and then navigate to the directory that contains your root CA certificate.
4. Select your root CA certificate (`.pem`) and then click **Open*.
5. Click **Upload** and then **OK**.
6. Click **Continue**.

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

Installing Root CA Certificates on a Mobile Client

Before you can install the root CA certificate in an Anyware Mobile Client, you must change the file extension from `.pem` to `.crt`.

The `.pem` extension is used for different types of X509 v3 files that contain ASCII Armor (Base64) data prefixed with a "-----BEGIN" line. The `.crt` extension is used for certificates that may be encoded either in binary DER format or ASCII PEM format.

Installing Root CA Certificates in the Anyware Software Client for macOS

Important: Root CA Certificate must have a .crt extension

You must change the root CA certificate's extension from `.pem` to `.crt` before installing it on a Anyware Software Client.

In macOS, certificates are stored in the Keychain Access application.

To import your root CA certificate in the Anyware Software Client for macOS:

1. Copy your root CA certificate file (*.crt) to the Mac client desktop.
2. Double-click **Applications** > **Utilities Keychain Access.app** to open Keychain Access.
3. Select **File** > **Import Items**.
4. Navigate to the desktop and then select your root CA certificate.
5. In the Destination Keychain drop-down menu, select **System**, and then click **Open**.
6. If prompted, enter your Keychain Access password and then click **Modify Keychain**.
7. At the next screen, click **Always Trust** when asked whether you want your computer to trust certificates signed by this certificate.
8. If prompted, enter your Keychain Access password and then click **Update Settings**.

After the certificate installs successfully, it appears in the *System* > *Certificates* list.

Installing Root CA Certificates in the Anyware Software Client for Windows

Important: Root CA Certificate must have a .crt extension

You must change the root CA certificate's extension from `.pem` to `.crt` before installing it on a Anyware Software Client.

Note: Windows must trust your root certification authority

When you use your own private key and certificate, you must add your internal root CA certificate to the Windows Trusted Root Certification Authorities certificate store on the client computer.

Users without a trusted root CA will receive an Unable to get local issuer certificate error and fail to connect.

The following instructions explain how to add a root CA certificate to the Trusted Root Certification Authorities store on a client PC using Microsoft Management Console.

Note: Active Directory group policies

For information on using Active Directory Group Policy to distribute certificates to client computers, see http://technet.microsoft.com/en-us/library/cc772491.aspx.

To import the root CA certificate for the Anyware Software Client for Windows:

1. Copy your root CA certificate file (*.crt) to a directory reachable by your Windows client.
2. Open the Microsoft Management Console on the agent machine:
    a. Press ⊞ + `r` to open the run dialog
    b. type `mmc` and press `Enter`.
3. Add the Certificates snap-in:
    a. Select **File** > **Add/Remove Snap-in**.
    b. Select **Certificates** from the Available snap-ins list and then click **Add**.
    c. Select **My user account** and then click **Finish**.
    d. Click **OK**.

4. Import the root CA certificate:
    a. Expand **Certificates - Current User**.
    b. Right-click on **Trusted Root Certification Authorities**, select **All Tasks** > **Import** from the context menu, and then click **Next**.
    c. Use the Browse button to navigate to the directory where your root CA certificate is located and select your root CA certificate.
    d. Click **Open** and then **Next**.
    e. Select the option to place all certificates in the Trusted Root Certification Authorities certificate store.
    f. Click **Next** and then **Finish**.
    g. At the security warning, click **Yes**.

After the certificate installs successfully, it appears in the Trusted Root Certification Authorities > Certificates list.

Installing in a Anyware Mobile Client

To install your internal root CA certificate on an iOS, Android, or ChromeOS device, consult the documentation for your device. The Anyware Mobile Client software does not implement certificate installation.

Verifying Certificate Formats

If you have OpenSSL installed on your system, you can use it to verify that your root CA certificate is in ASCII PEM format.

To verify that the root CA certificate is in ASCII PEM format:

1. Launch **openssl** from the `C:\OpenSSL-Win32\bin` directory.
2. Type the following command:

```
x509 -in rootCA.pem -text -noout
```

If your certificate contents successfully display on the screen, it is encoded correctly as a PEM file.

Configuring the Agent Certificate Mode

The Anyware Agent chooses a certificate based on the parameters set in the *Configure PCoIP Security Certificate Settings* GPO variable.

Since Anyware agents automatically generate and use self-signed certificates by default, you only need to configure the Configure PCoIP Security Certificate Settings GPO variable if you are deploying your own custom certificates.

You can configure Anyware Agents to handle certificates in the following ways:

- Always use self-signed certificates (default)
- Always use local custom certificates
- Attempt to use a local certificate, and revert to self-signed if not found

> ✎ **Note: Import the administrative template file before configuring**
>
> The Configure License Server Path GPO variable only appears in the GPO editor after you import the administrative template file.

The example in this section configures the agent to look for the certificate only in the remote workstation's Windows certificate store. The example also gives the store the friendly name of "PCoIP". These settings are mandatory when you deploy your own custom certificates.

To configure the Configure PCoIP Security Certificate Settings GPO variable with a custom certificate:

1. Open the Local Group Policy Editor on the agent machine:
    a. Press ⊞ + `r` to open the run dialog
    b. type `gpedit.msc` and press `Enter`.
2. Navigate to *Local Computer Policy > Computer Configuration > Administrative Templates > PCoIP Session Variables > Not Overridable Administrator Defaults*
3. Double-click **Configure PCoIP Security Certificate Settings** to open the variable's dialog.
4. Select **Enabled** to enable the setting.

5. In the *How the Anyware agent chooses the certificate...* drop-down list, select **From the Certificate Store**. A search field will appear next, labelled *Name of the Certificate Store to search for CA-signed certificates*.
6. In the search field, enter the name for the certificate in the Windows Cert store. This should be the *friendly name* of the CA signed cert which appears in the store.
7. In *The minimum key length...* drop-down list, select the desired minimum key length (in bits). If you're unsure, specify the actual length of the cert you're using.
8. Click **OK**.
9. Close the Local Group Policy Editor and reboot the desktop to apply your settings.
10. After the Anyware agent restarts, you can verify that it is using your custom certificate by checking the agent's level 2 log files.

Reference

Supported Installer Languages

The Remote Workstation Card Agent for Windows installer supports the following languages:

- French
- German
- Spanish
- Simplified Chinese
- Traditional Chinese
- Japanese
- Portuguese
- Italian
- Korean
- Russian
- Turkish

Troubleshooting

Support

Contacting Support

If you encounter any problems installing, configuring, or running the agent, you can create a support ticket with HP.

Before creating a ticket, be prepared with the following:

- A detailed description of the problem
- Your agent version number (how do I find my version number?)
- A prepared support file

The HP Community Forum

The Community Forum enables users to have conversations with other IT professionals to learn how they resolved issues, find answers to common questions, have peer group discussions on various topics, and access the Technical Support Service team. The HP staff are heavily involved in the forums.

To visit the HP community, go to https://communities.teradici.com.

Finding the Agent Version Number

You can find your Anyware Agent's version number using the PCoIP Control Panel or the Windows Control Panel.

To find your version number using the PCoIP Control panel:

1. Click in the Windows system tray and select **Updates** from the context menu.

   The control panel appears with the Updates tab selected.

2. The installed software version appears in the *Status* box of the Updates tab.

To find your agent's version number using the Windows control panel:

1. Open the Windows Control Panel, and navigate to Uninstall a program.
2. Find the Anyware agent type and version number in the program list.

Creating a Technical Support File

We may request a support file from your system in order to troubleshoot and diagnose issues. The support file is an archive containing Anyware Remote Workstation Card Agent for Windows logs and other diagnostic data that can help support diagnose your problem.

You can create a support file using the PCoIP control panel. If the PCoIP control panel is disabled, you can also run the bundling application directly using Windows Explorer or from the command line.

Both methods place a support bundle in the Support folder, located at `C:\ProgramData\Teradici\Support`.

To create a support file with the PCoIP Control Panel:

1. Open the PCoIP Control Panel in the system tray.
2. Select the *Support* tab and then click the **Create Support File** button.
3. When the zipped support file is ready, an Explorer window opens and displays your Support folder. The generated file is selected.

To create a support file with the bundling application:

1. Using Windows Explorer or a command line tool, navigate to `C:\Program Files\Teradici\Anyware Agent`.
2. Run `SupportBundler.exe`.
3. When the zipped support file is ready, an Explorer window opens and displays your Support folder. The generated file is selected.

Performing Diagnostics

Each Anyware component creates and updates a log file which records its activity as the system is used. Most troubleshooting within a Anyware system begins by examining these log files and looking for error conditions or other indications that may explain why the system is not operating as expected.

Log files for the Remote Workstation Card Agent for Windows and other Anyware components are saved to log directories.

The Windows Event Viewer also contains event logs for high-level events.

Note: Bundling log files for support

When investigating issues with HP support, you may need to provide a support file which includes system log files. Instructions are provided here.

Logs

Locating Agent Log Files

Log files for the Anyware agent are located in the following directories by default. If you changed your agent's location during installation, the log files will be in your custom location instead.

Component	Log file location
Remote Workstation Card Agent for Windows	`%programdata%\Teradici\PCoIPAgent\logs`
PCoIP Server	`%programdata%\Teradici\PCoIPAgent\logs`

Note: Bundling log files for support

When investigating issues with HP support, you may need to provide a support file which includes system log files. Instructions are provided here.

Setting the Remote Workstation Card Agent Log Level

Each Anyware component is configured to log events. The amount of information captured can be configured by setting the log verbosity on a scale from 0 (least verbose) to 3 (most verbose). **By default, the Remote Workstation Card Agent for Windows records log events at level 2**.

When troubleshooting a particular problem, HP Support Services may recommend adjusting the log level for specific components to obtain more information from certain parts of the system.

To change the agent's log level:

1. Navigate to the *HKEY_LOCAL_MACHINE > SOFTWARE > Teradici > PCoIP > pcoip_admin* directory. The configured DWORDs are shown in the right pane.
2. If the `pcoip.event_filter_mode` DWORD does not exist, create it: Right-click the *pcoip_admin* folder and select **New > DWORD (32-bit) Value**. Name the new entry `pcoip.event_filter_mode`.
3. Right-click *pcoip.event_filter_mode* and select **Modify**.
4. In the *Edit DWORD Value* dialog box, revise the number in the **Value data** field:
    - Valid values are `0`, `1`, `2`, and `3`, ranging from least to most verbose.
    - For normal operation, `2` is recommended (and is the default setting).
    - For debugging and support, `3` should be used.
5. Click **OK**.

Session Log IDs

At the start of each PCoIP session, a unique session ID is generated by the Anyware Client and passed to all connected Anyware components (including the agent). Log messages generated by the agent are prefixed with this session ID, making it easy to identify All log messages generated during a single session, by any Anyware component, will be prefixed with the same session log ID in RFC-4122 format:

```
yyyy-mm-ddThh:mm:ss.ffffffZ xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx > …
```

For example:

```
2015-11-06T08:01:18.688879Z 4208fb66-e22a-11d1-a7d7-00a0c982c00d > …
```

Log messages that do not pertain to a specific session will show a string of zeroes in place of the session log ID number.

If a Anyware component does not receive a session log ID from the Anyware client, or receives an invalid value, it will generate a new session log ID and distribute it to the other components in the system.

Viewing Windows Event Viewer Anyware Agent Logs

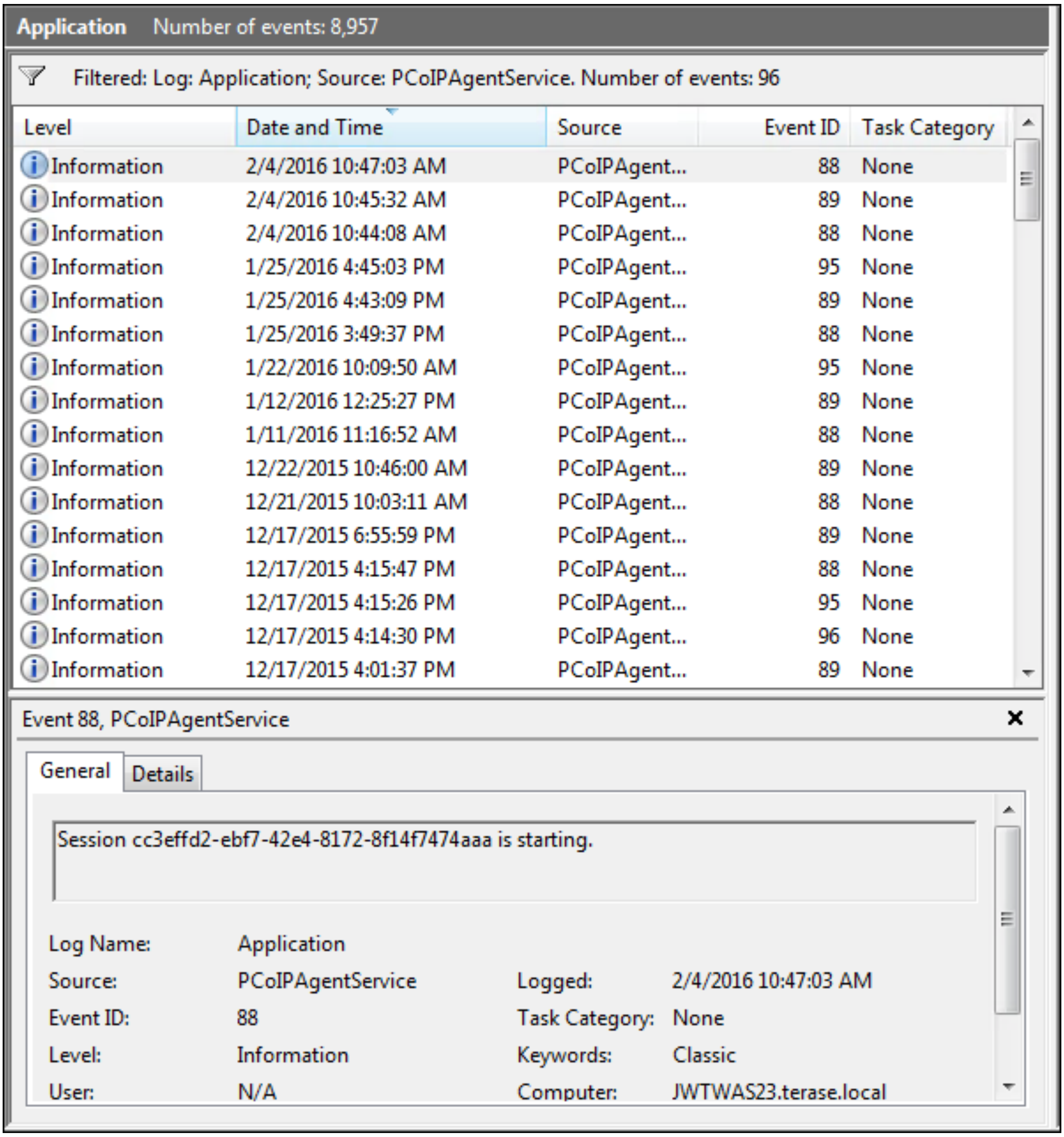
You can view high-level session and connection events generated by the Anyware agent and Anyware Manager in the Windows Event Viewer.

Anyware Agent Events

To view events using the Windows Event Viewer:

1. Navigate to *Start* > *Control Panel* > *System and Security* > *Administrative Tools* and double-click **Event Viewer**.
2. Navigate to *Event Viewer (Local)* > *Windows Logs*, right-click **Application**, and select **Filter Current Log**.
3. In the *Event sources* drop-down list, select **PCoIPAgentService** and click **OK**.
4. Select an event to view its details.

The next example shows typical Anyware agent session and connection events that you can view in the Windows Event Viewer.



Application Number of events: 8,957

Filtered: Log: Application; Source: PCoIPAgentService. Number of events: 96

Level	Date and Time	Source	Event ID	Task Category
Information	2/4/2016 10:47:03 AM	PCoIPAgent...	88	None
Information	2/4/2016 10:45:32 AM	PCoIPAgent...	89	None
Information	2/4/2016 10:44:08 AM	PCoIPAgent...	88	None
Information	1/25/2016 4:45:03 PM	PCoIPAgent...	95	None
Information	1/25/2016 4:43:09 PM	PCoIPAgent...	89	None
Information	1/25/2016 3:49:37 PM	PCoIPAgent...	88	None
Information	1/22/2016 10:09:50 AM	PCoIPAgent...	95	None
Information	1/12/2016 12:25:27 PM	PCoIPAgent...	89	None
Information	1/11/2016 11:16:52 AM	PCoIPAgent...	88	None
Information	12/22/2015 10:46:00 AM	PCoIPAgent...	89	None
Information	12/21/2015 10:03:11 AM	PCoIPAgent...	88	None
Information	12/17/2015 6:55:59 PM	PCoIPAgent...	89	None
Information	12/17/2015 4:15:47 PM	PCoIPAgent...	88	None
Information	12/17/2015 4:15:26 PM	PCoIPAgent...	95	None
Information	12/17/2015 4:14:30 PM	PCoIPAgent...	96	None
Information	12/17/2015 4:01:37 PM	PCoIPAgent...	89	None

Event 88, PCoIPAgentService

Session cc3effd2-ebf7-42e4-8172-8f14f7474aaa is starting.

Log Name:	Application		
Source:	PCoIPAgentService	Logged:	2/4/2016 10:47:03 AM
Event ID:	88	Task Category:	None
Level:	Information	Keywords:	Classic
User:	N/A	Computer:	JWTWAS23.terase.local

Key events to watch for in the event viewer logs:

Event ID	Key	Notes
88	SESSION_START	
89	SESSION_END	
90	LAUNCHER_EXIT	
91	CONNECTION_TIMEOUT	
92	CONNECTION_FAILURE	
93	SESSION_REDIRECTION	
94	SESSION_INTERRUPTION	
95	SERVICE_STARTING PCoIP	Agent service starting.
96	SERVICE_STOPPING PCoIP	Agent service stopping.
97	SESSION_RESUMING	
98	VIDEO_DRIVER_REPAIR_ERROR	
99	FLEXERA_SERVICE_ERROR	
100	VCHAN_LOADER_EXCEPTION	An exception was thrown in a PCoIP virtual channel plugin.
101	NO_AGENT_ERROR	The Anyware agent process could not be detected.
102	VCHAN_LOADER_INTERNAL_ERROR	An internal error has occured.
103	VCHAN_LOADER_BAD_INVOCATION_ERROR	The PCoIP virtual channel loader utility was invoked incorrectly.
104	AGENT_PROCESS_TERMINATED_ERROR	The Anyware Agent process was terminated.
105	SSO_PIPE_CREATION_ERROR	The Single Sign On framework was unable to establish a secure connection with the Teradici Agent.
106	MANUAL_DISCONNECT	The PCoIP session was disconnected by the user.
107	USER_SIGNOUT_SWITCH	The PCoIP session was disconnected by a user logout or user switch.
108	SHUTDOWN_RESTART_SLEEP	The PCoIP session was disconnected by a machine shutdown, restart, or sleep event.
112	SERVICE_START_ERROR PCoIP	Agent service cannot be started.
113	SERVICE_INTERNAL_ERROR	
114	SERVICE_ADMINISTRATIVE_MESSAGE	
115	SERVICE_SHUTDOWN	A shutdown of the server machine was initiated.

Anyware Manager Events

If you are using Anyware Manager to start and stop your host machines, the CAMIdleShutdown process will log events as well. Follow the same procedure

Event ID	Description
95	CAM Idle Machine Shutdown service starting
96	CAM Idle Machine Shutdown service stopping
114	Machine will be checked for idle state.
115	Shutting down idle machine.

Troubleshooting Licenses

Troubleshooting License Issues

The license troubleshooting utilities are included with the Remote Workstation Card Agent for Windows. These utilities allow you to validate your licenses and list license entitlements.

Validate Licenses

`pcoip-validate-license` scans your local system and any connected physical or cloud-based license servers for active licenses, and lets you know when your license subscription expires. For more information, see Welcome to Cloud Licensing.

To run the license validation tool, open a PowerShell window, navigate to the PCoIP Agent directory, and type:

```
./pcoip-validate-license.ps1
```

For more detailed instructions, open a PowerShell window and type:

```
get-help ./pcoip-validate-license.ps1
```

List License

`pcoip-list-licenses` retrieves and displays all license entitlements on a connected physical or cloud-based license server.

To run the license list tool, open a PowerShell window, navigate to the Anyware agent directory, and type:

```
./pcoip-list-licenses.ps1
```

For more detailed instructions, open a PowerShell window and type:

```
get-help ./pcoip-list-licenses.ps1
```

Tracking Usage Over Time

HP Local License Server users can use our open-source script, which displays the maximum HP Anyware license concurrent usage for a license server over time. For more information, refer to our Github page.

HP Cloud Licensing users can write a short script that runs `pcoip-list-licenses` periodically (for example, every 60 minutes) on any Anyware agent machine to track license usage.

Managing Session Licenses Using the PCoIP Control Panel

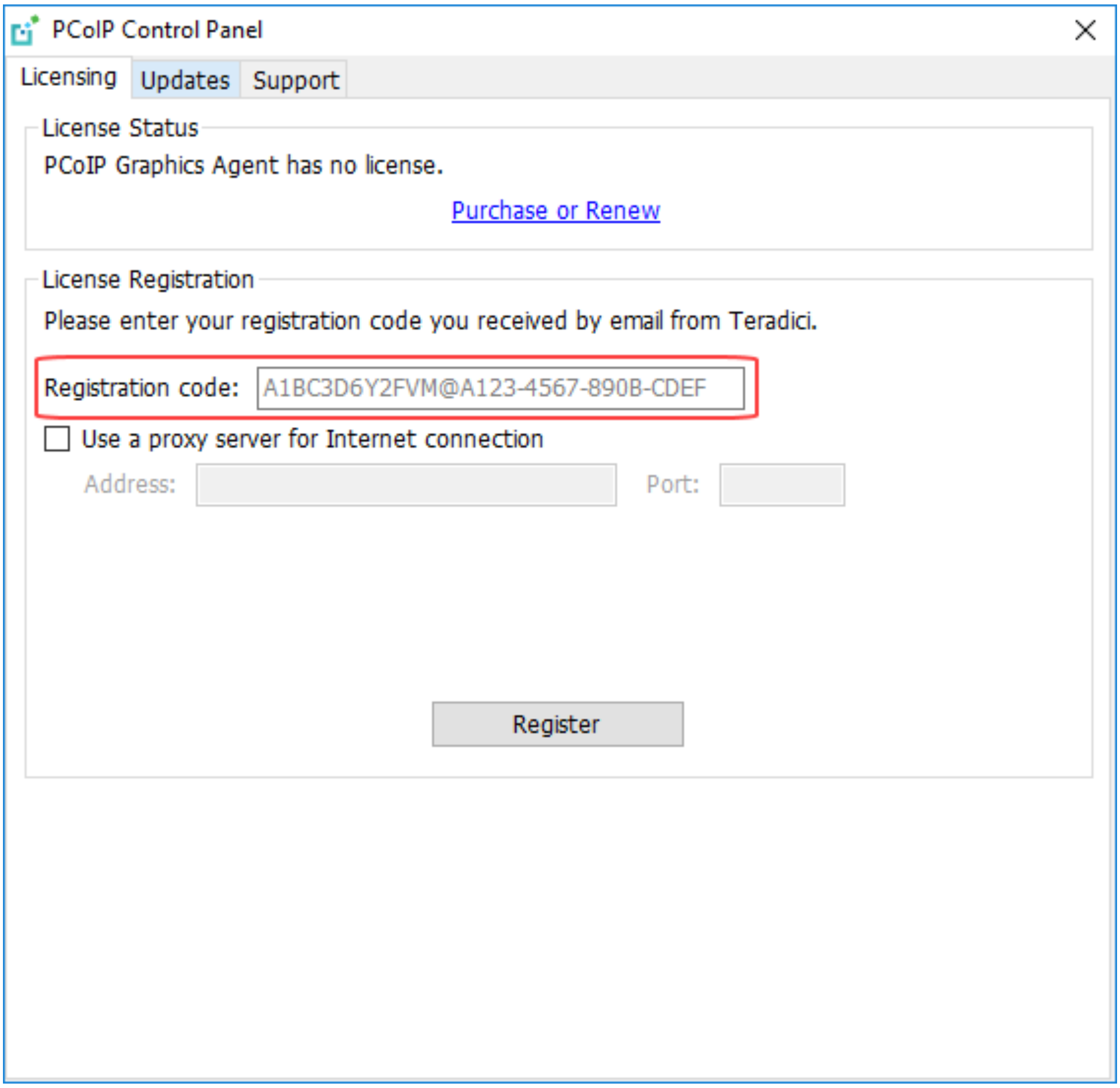
You can use the PCoIP Control Panel to register a license, check the status of a license, and renew a license.

The PCoIP Control Panel can be opened using either of these methods:

- Click in the Windows system tray
- Open a command line tool and run

```
"C:\Program Files\Teradici\PCoIP Agent\bin\pcoip_control_panel.exe"
```

If you have not registered your license already, select the **Licensing** tab and enter your registration code, as shown next.



PCoIP Graphics Agent has no license.

Please enter your registration code you received by email from Teradici.

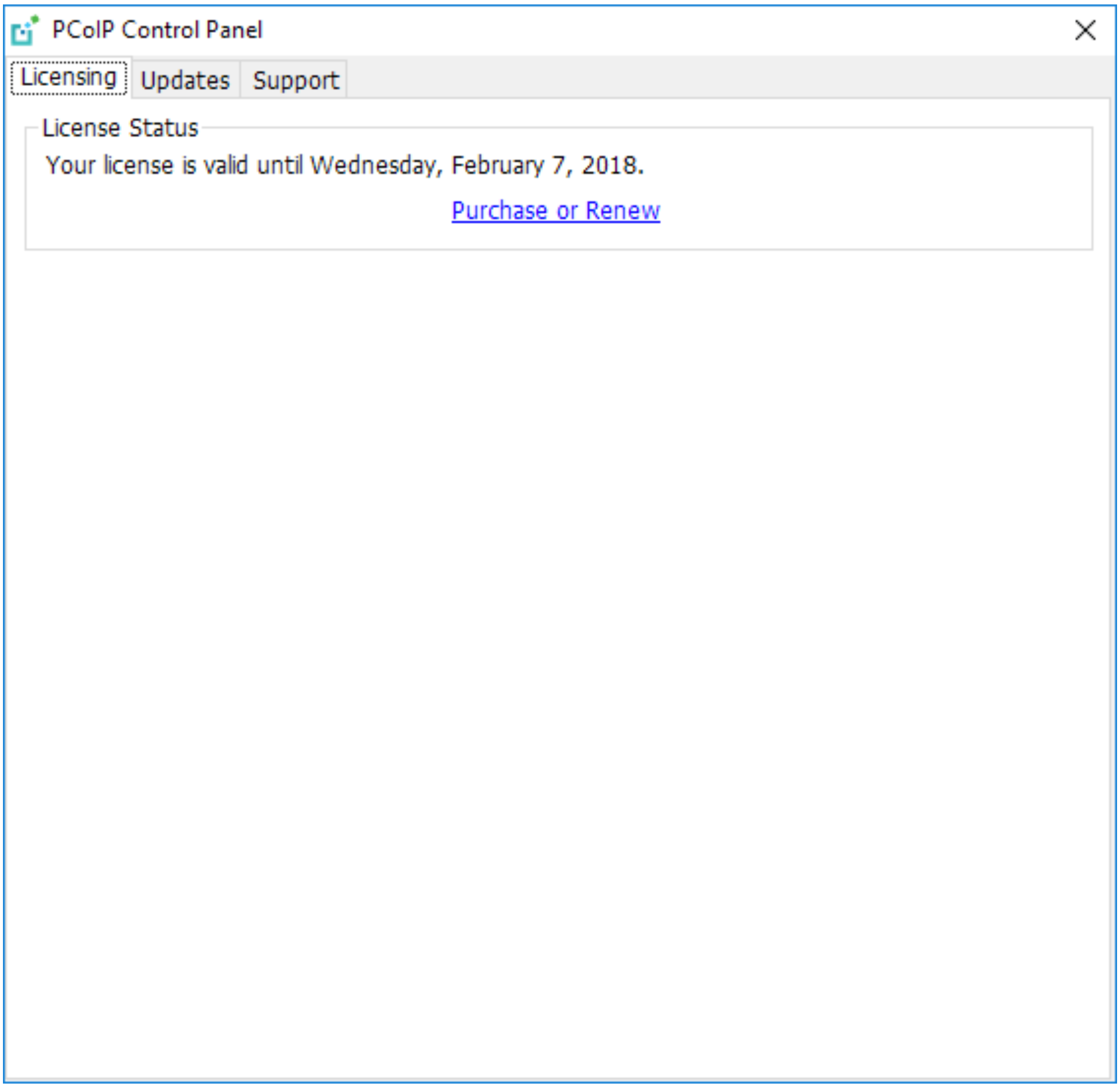
Registration code: A1BC3D6Y2FVM@A123-4567-890B-CDEF

□ Use a proxy server for Internet connection

Address:

Port:

Once you are licensed, the tab will show your license subscription expiry information, and enables you to renew the license.



Your license is valid until Wednesday, February 7, 2018.

Frequently Asked Questions

Can I use a screensaver?

Yes. However, a blank, static screensaver will provide the most efficient CPU and network bandwidth usage.

How quickly does a Anyware agent complete a connection?

Anyware agents can usually achieve a connection in 15 to 30 seconds. We use the statistical value Top Percentile (TP) to measure the time to establish a session:

- TP99: Ninety-nine percent of connections complete in under 30 seconds.
- TP50: Fifty percent of connections complete in under 15 seconds.

What do I need to know about power management?

Hosts with Windows power management enabled may drop PCoIP connections when turning off displays or going to sleep. If this behavior is undesirable, these Windows power management features should be turned off.

To disable Windows power management features:

1. From the Windows Control Panel, open **Power Options**.
2. Click **Change plan settings** next to the enabled power plan.
3. Select **Never** from the drop-down list for *Turn off the display*
4. Select **Never** in the drop-down list for *Put the computer to sleep*.
5. Click **Save changes**.

Why is my application not sending audio?

The Anyware agent delivers audio over PCoIP connections by reassigning the system's default audio device. Only applications that use the system default audio device will send or receive audio over

PCoIP; applications that are configured to use non-default devices will not work. If you don't hear audio from your application, make sure it is configured to use the system default audio device.

I'm using Anyware Cloud Licensing. What network blocks should I leave open?

If you are using Anyware Cloud Licensing, you will need to add the following to your allowlist:

- `teradici.flexnetoperations.com`
- `teradici.compliance.flexnetoperations.com`

If you use an IP-based allowlist, we recommend your IT team add the following network blocks to your allowlist:

- `IPv4: 185.146.155.64/27`
- `IPv6: 2620:122:f005::/56`

Important: Migrating from the previous specification

Previously, our allowlist specification looked like this:

- **Production**: `64.14.29.0/24`
- **Disaster Recovery**: `64.27.162.0/24`

If you have an existing implementation using an IP-based allowlist like this, we recommend you leave it in place until the new allowlist is active and tested.