

Welcome to PCoIP Software Client for Windows

Welcome to the Software Client for Windows Administrators' Guide.

PCoIP Software Clients are applications that establish PCoIP sessions with remote Windows, Linux, or macOS desktops. Connections can be made to PCoIP agents installed on virtual or physical machines, or to Remote Workstation Cards in physical workstations.

This guide explains how to install, configure, and use the Software Client for Windows. It includes client system requirements and information on host dependencies.

Who Should Read This Guide?

This guide is intended for administrators and users who install, configure, or use the Software Client for Windows.

Additional Documentation

The following guides contain additional information relevant to PCoIP systems and PCoIP Software Clients:

For more information about HP Anyware, including detailed information on included PCoIP components as well as HP Anyware plans, see the [Teradici Cloud Access Architecture Guide](#).

For more information about Teradici PCoIP agents, which are required on remote virtual machines, see the following pages:

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

For information about Teradici PCoIP Remote Workstation Card Software, which is required on remote workstations using a Teradici PCoIP Remote Workstation Card, see the following pages:

- [PCoIP Remote Workstation Card Software for Windows](#)
- [PCoIP Remote Workstation Card Software for Linux](#)

What's New in This Release

The PCoIP Software Client for Windows 22.09 introduces the following features and enhancements:

- **Adds support for Windows 10 IoT.** Windows 10 IoT 64 21H2 Enterprise LTSC is now supported.
- **HP Anyware Client User Interface Refresh:** This release introduces our newly-redesigned user interface, with a clean, modern feel and greatly simplified connection management. For more information, see [Connecting to Remote Desktops](#).

As part of the interface update, the following settings are now available via the pre-session UI (previously, these were only available programmatically). See the following topics for more information:

- [PCoIP Log Level](#)
- [PCoIP Client Security Mode](#)
- [USB Auto-Forwarding](#)
- **Collaboration Input Control:** This release introduces *input control* for PCoIP Ultra Collaboration sessions, allowing session hosts to yield mouse and keyboard control to their guest collaborators. This feature is off by default and is enabled on the PCoIP Agent. For more information, see the guide for the PCoIP agent you are connecting to:
 - [Graphics Agent for Windows](#)
 - [Graphics Agent for macOS](#)
 - [Graphics Agent for Linux](#)
 - [Standard Agent for Windows](#)
 - [Standard Agent for Linux](#)
- **Introduces the next-generation High Performance Client mode [TECHNOLOGY PREVIEW].** The next-generation *high performance client* mode is now available as a technology preview for testing and feedback. This new high-performance mode combines the audio and video performance gains of the legacy high-performance client with the full functionality of the standard client. See [Next-Generation High Performance Client](#) more information.

- Bug fixes and stability enhancements.

System Requirements

The following table outlines the system requirements for the PCoIP Software Client for Windows:

System	Version Required
PCoIP Software Client Operating Systems	<ul style="list-style-type: none"> • Windows 10 (64-bit) • Windows 10 IoT 64 21H2 Enterprise LTSC • Windows 11
Compatible PCoIP Agents	<p>The Software Client for Windows can connect to any PCoIP agent. Some features require specific agent versions; see the Feature Support section of this guide for details.</p> <p>We recommend always using the same version of PCoIP agent and PCoIP client.</p>
Compatible PCoIP Remote Workstation Cards ¹	TERA22x0 with firmware 20.04+ and PCoIP Remote Workstation Card Software for Windows or Linux 20.04+.
Supported IP versions	IPv4 and IPV6.

Hardware System Requirements

For different display configurations Teradici recommends certain processor and RAM combinations:

- For up to dual 1920 x 1080 display configuration Teradici recommends 1.6 GHz dual core processor or higher with at least 4 GB RAM.
- For up to dual 4K/UHD Teradici recommends a 3.0 Ghz quad core processor or higher with at least 8GB Dual Channel RAM.

1. For details on feature limitations between PCoIP Software Clients and PCoIP Remote Workstation Cards, see [Connecting to PCoIP Remote Workstation Cards](#).

Audio Support

Stereo audio output and mono audio input are supported and enabled by default.

The PCoIP Client provides an enhanced audio and video synchronization (AV Lock) feature that provides improved full-screen video playback, reducing the difference in delays between the audio and video channels and smoothing frame playback on the client. This improves lip sync and reduces video frame drops for movie playback. This feature introduces a small lag in user interaction responsiveness when enabled. Using enhanced audio and video synchronization will reduce the maximum frame rate.

Audio input devices should not be bridged to the remote session. Audio input devices are locally terminated and utilize local OS audio drivers. A bluetooth headset can be supported locally, but cannot be bridged.

For more information on the AV Lock feature, see [Enhanced Audio and Video Synchronization](#).

Client Modes

The Software Client for Windows supports the following operational modes:

Standard Client Mode

This mode is the default, and is recommended for most environments. The standard mode provides a good balance of performance features, and has the full complement of in-session menu features.

If you require high framerate support or need PCoIP Ultra AV Lock, you can switch to the [High Performance Client](#) mode, described next.

Note: Standard mode does not support PCoIP Ultra AV Lock

PCoIP Ultra AV Lock is supported by the [High Performance Client](#) and the [Next-Generation High Performance Client Mode](#). It is not available in the standard client mode.

Tip: Next-generation High Performance Client Preview

The next-generation High Performance Client mode is now available for testing and feedback. See [Next-Generation High Performance Client Mode](#) for details.

High Performance Client Mode

High performance client mode is a special mode which provides higher frame rates, with fewer dropped frames, than the default client, and supports PCoIP Ultra AV Lock. This mode is especially beneficial for 4K video workloads.

The High Performance Client has limited in-session client feature support. The High Performance Client does not support the full suite of in-session menu features available on the standard client. For this reason, we recommend the high performance client *only* for scenarios which require high frame rates and reduced dropped frames, or where support for PCoIP Ultra AV Lock is required.

 **Note: Auto-forwarding by device ID is supported**

The high performance client supports auto-forwarding USB devices, such as Wacom tablets, by providing their device IDs in a configuration call; see [Vidpid Auto-Forward](#) for details.

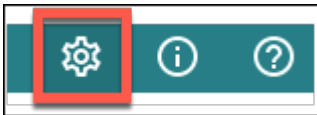
High Performance Client Limitations

The high performance client has the following major limitations:

- Only *Fullscreen all monitors* display mode is supported.
- The following limited in-session menu options are available:
 - **Teradici PCoIP Client** menu
 - Quit Teradici PCoIP Client
 - **Connection** menu
 - Send `Ctrl+Alt+Del`
 - Disconnect (To disconnect use `ctrl+alt+~`)
 - **View** menu
 - Minimize Client (You can minimize the client by using `ctrl+alt+m`)
 - Tablet Monitor
 - Tablet Orientation Left-handed
 - PCoIP Ultra AVLock

To Enable High Performance Client (Legacy) mode:

1. If you are in a PCoIP session, disconnect from it.
2. In the Software Client for Windows, click the gear icon to open the client settings window.



3. In the side navigation panel, click **Advanced**.
4. In the advanced settings, find the *Client Mode* section, and select **High Performance (Legacy)**.
5. Close the settings window.

Subsequent PCoIP sessions will use the preview version of the High Performance Mode.

To Disable High Performance Client (Legacy) mode:

1. If you are in a PCoIP session, disconnect from it.
2. In the Software Client for Windows, click the gear icon to open the client settings window.
3. In the side navigation panel, click **Advanced**.
4. In the advanced settings, find *Client Mode*, and select **Standard Mode** or **High Performance (Preview)**.
5. Close the settings window.

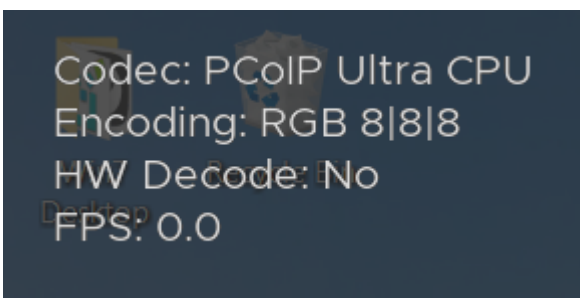
Subsequent PCoIP sessions will use the mode selected.

Tip: Next-generation High Performance Client Preview

The next-generation High Performance Client mode is now available for testing and feedback. See [Next-Generation High Performance Client Mode](#) for details.

Statistics Overlay

The statistics overlay is an additional feature provided by the High Performance Client, which displays performance and configuration data for your connection.



The overlay shows the following information:

Value	Description
Codec	Reports the current PCoIP encoding that is in use. Possible values are <i>PCoIP Ultra CPU</i> , <i>PCoIP Ultra GPU</i> and <i>PCoIP</i> .

Value	Description
Encoding	Reports the color space that is being used to encode the information. PCoIP and PCoIP Ultra CPU offload will report RGB 8:8:8 which means full 8 bit RGB pixels are being used. For PCoIP Ultra GPU optimization, either YUV 4:4:4 or YUV 4:2:0 will be used, depending on the system configuration.
HW Decode	Reports whether or not the PCoIP Client is decoding the frames using built-in GPU hardware decoding.
FPS	Reports the current frames per second that are presented on the PCoIP Client.

Once enabled, the overlay can be toggled on and off by pressing **Ctrl+Win**.

To enable the statistics overlay:

1. Open the Software Client for Windows configuration file in a text editor. For instructions and file locations, see [Configuration Files](#).
2. Add the following line:

```
enable_high_perf_client_stats_overlay=1
```

3. Save the file.

Next-Generation High Performance Client Mode

The next-generation High Performance Client is now available as a technology preview. This new high performance client combines the best of the current Standard and High Performance Client modes, providing all of the features available to the standard PCoIP client while delivering improved video and PCoIP Ultra AV Lock features.

In a future release, this mode will replace both the standard and High Performance Client (legacy) modes.

Caution: Preview feature

This release of the next-generation High Performance Client may have stability or performance issues in certain situations. We recommend using either the standard mode or legacy high performance mode for production work.

To Enable High Performance Client Preview:

1. If you are in a PCoIP session, disconnect from it.
2. In the Software Client for Windows, click the gear icon to open the client settings window.



3. In the side navigation panel, click **Advanced**.
4. In the advanced settings, find the *Client Mode* section, and select **High Performance (Preview)**.

USB Devices	<input checked="" type="radio"/> Security mode - Medium If a certificate cannot be verified you will receive a warning, but you will still be able to connect. This is the default security mode.
Logs	<input type="radio"/> Security mode - Low You do not need to verify the certificate to connect.
Advanced	<p>Client Mode</p> <p>It is possible to enable different performance modes for the HP Anyware client depending on your use case.</p> <input type="radio"/> Standard client Recommended for the majority of use cases. Preferred by users requiring the most consistent experience at moderate framerates.
	<div style="border: 2px solid red; padding: 5px;"> <input checked="" type="radio"/> High Performance (Preview) Recommended for high framerate and audio synchronization. Preview of the next generation client mode that is designed to replace both legacy modes for all users. This is still being refined for performance and consistency. </div> <input type="radio"/> High performance client Only recommended for users with high performance audio synchronization requirements, is missing features offered in the other modes. This mode will be deprecated in future releases, replaced by the next generation High Performance Client currently in preview.

5. Close the settings window.

Subsequent PCoIP sessions will use the preview version of the High Performance Mode.

To Disable High Performance Client Preview mode:

1. If you are in a PCoIP session, disconnect from it.

2. In the Software Client for Windows, click the gear icon to open the client settings window.
3. In the side navigation panel, click **Advanced**.
4. In the advanced settings, find **Client Mode**, and select **Standard Mode** or **High Performance (Legacy)**.
5. Close the settings window.

Subsequent PCoIP sessions will use the mode selected.

Collaboration

The PCoIP Ultra Collaboration feature enables a user to share their PCoIP session with a remote guest collaborator using a PCoIP Software Client. While connected, the guest collaborator can view the screen output and hear the audio output of the shared PCoIP session.

When discussing this feature, we'll refer to the first user as the *host collaborator*, and the second user who joins the session as the *guest collaborator*.

Feature Support, Requirements and Limitations

- The PCoIP Ultra Collaboration feature is supported when connecting from any PCoIP software client to any PCoIP agent.
- When connecting to a PCoIP standard agent, PCoIP Ultra CPU Offload is *required*.
- When connecting to a PCoIP graphics agent 22.07 or later, PCoIP Ultra CPU Offload, GPU Offload, and Auto Offload are supported.
- *Collaboration Mouse Visibility* only works when the host collaborator and all guest collaborators are using a PCoIP Client in **Standard Client** mode, or in the next-generation high performance client mode (technical preview). The *high performance client* mode does not support mouse visibility.

The features described on this page are only supported when both PCoIP Clients and PCoIP Agents are running on version 22.07 or later.

Enabling and Hosting a Collaboration Session

For information and steps on how to enable collaboration, and how to host a collaboration session, see the PCoIP Agent documentation linked below. The instructions for enabling and hosting collaboration will vary based on the PCoIP Agent you use. You should select the instructions that apply to the PCoIP Agent that you are connecting to:

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

- [PCoIP Standard Agent for Windows - Collaboration](#)

Important: User input control

PCoIP Collaboration sessions support user input control, which allows the session host to transfer control of keyboard and mouse input to the guest collaborator. This feature is disabled by default. Instructions for enabling input control, and guidance on usage, are also available in the PCoIP agent documents linked above.

Joining a Collaboration Session

The guest collaborator can join the PCoIP session once they have received the invite link and invite code from the host collaborator. Invite links and codes are generated on the remote PCoIP agent machine; for instructions, refer to the agent administrators' guides linked above.

1. Open a web browser and go to the invite link shared with you (you may be able to click this link directly, depending on how it was shared with you).
2. The web browser will warn you that the link is attempting to open the *PCoIP Client* application. Allow the browser to open the PCoIP Client.
3. When the PCoIP Client opens, it will prompt you for your name and the Collaboration Invitation Code. The value you enter for your name is used to tell the host who is joining; the Collaboration Invitation Code is the six digit number provided by the host. Enter both values and click **Submit**.
4. Once the host collaborator accepts your connection request, the Collaboration screen share will start.
5. To leave the collaboration session, select **Connection > Disconnect** from the PCoIP Client menu.

Mouse Visibility

Collaboration Mouse Visibility allows the guest collaborator to see the host's mouse cursor movements within a collaboration session. This feature is only available when both collaborators are using a PCoIP client 22.07 or newer, and the PCoIP agent is also version 22.07 or later.

Currently, mouse visibility only works in the default *standard client* mode. *High performance client* mode does not support mouse visibility. See [High Performance Client](#) for instructions to enable or disable high performance client mode.

Future releases will add the ability for the Guest Collaborator to take control of the session mouse and keyboard.

Displays

The PCoIP Client supports a maximum of four displays and a maximum resolution of 4K UHD (3840×2160).

Monitors can be arranged in a vertical line, a horizontal line, or as a 2×2 box display. They can be used in any standard rotation (0°, 90°, 180°, or 270°), with any monitor as the primary display.

Note: Using multiple high-resolution displays

Systems with multiple high-resolution displays, such as quad 4K UHD topologies, require powerful system infrastructure. Be sure to use a system with sufficient bandwidth and client capability to support your required display topology.

Important: Attaching monitors to the host machine is not supported

PCoIP client supports a maximum of four displays. Attaching extra monitors to the host machine will conflict with client display topologies.

Language Support

The Software Client for Windows is not currently localized, and is offered only in English. Localization will be added in a future release.

If you require language support in non-English languages, we recommend using the Software Client for Windows 22.07, which is localized.

PCoIP Ultra

The Software Client for Windows provides support for PCoIP Ultra, the latest protocol enhancements from Teradici.

PCoIP Ultra enhancements are controlled on the PCoIP agent. There is no configuration required on the PCoIP Client.

Important: PCoIP Ultra is appropriate for specific use cases

For most users, the default PCoIP protocol will provide the best possible experience. Carefully review the recommended use cases in the next section to determine whether you should enable it.

Requirement: AVX2 Support

On Windows or Linux machines, both the client and agent CPUs must support the AVX2 instruction set. This requirement does not apply to macOS machines.

For additional detail on PCoIP Ultra technical requirements for various use cases and troubleshooting steps, refer to [KB 2109: PCoIP Ultra Troubleshooting](#).

PCoIP Ultra Modes

PCoIP Ultra has three acceleration modes, which leverage CPU and GPU offloading to optimize content delivery.

- **Auto Offload:** Dynamically switches between CPU and GPU offload modes depending on the workload being processed. This setting is appropriate for work-from-home or WAN content creators who require optimized delivery of high resolution content, including video playback, while still achieving build-to-lossless color accuracy. This mode requires a GPU and a graphics agent.
- **CPU Offload:** Provides efficient scaling across multicore CPUs, leveraging AVX2 instruction sets. Appropriate for users that require CPU-optimized delivery of 4K UHD, high-framerate

video playback and build-to-lossless color accuracy. It is also useful when GPU encoding resources must be reserved for video encoding applications, typically in LAN environments.

- **GPU Offload:** PCoIP encoding is always offloaded to a GPU. Appropriate for users who demand the highest possible CPU efficiency. This mode requires a GPU and a graphics agent.

Enabling PCoIP Ultra

PCoIP Ultra is disabled by default, and must be enabled on the PCoIP agent. The method used to do this varies by agent type; consult the following documentation for instructions:

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

Auto-Offload with PCoIP Ultra

When using a PCoIP graphics agent, PCoIP Ultra can automatically select and switch between CPU-offload and GPU-offload modes based on the amount of pixel change in the displays. When displays are rendering highly dynamic content, PCoIP Ultra will enable GPU Offload to provide improved frame rates and bandwidth optimization. When displays are less dynamic, PCoIP Ultra defaults to CPU offload to provide the best image fidelity.

PCoIP Ultra Offload only takes effect if the remote PCoIP graphics agent and the PCoIP software client are capable of both CPU and GPU offload.

The PCoIP Ultra offload mode is set on the PCoIP agent; PCoIP Ultra Auto Offload requires a PCoIP Graphics Agent. Refer to the appropriate documentation for instructions:

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

PCoIP Codec Indicator

When enabling PCoIP Ultra there will be an onscreen indicator at the bottom left corner of the screen. PCoIP Ultra CPU optimization is indicated with a dark blue dot. PCoIP Ultra GPU optimization is indicated by a magenta dot.

To disable this codec indicator, create the following registry key and set it to 0:

**Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Teradici\PCoIP\pcoip_admin_def:
pcoip.codec_indicator (DWORD)**

Printing Support

The following are the printing options available with the PCoIP Client:

- **Local USB Printing:** Printing to a USB printer locally attached to the Client device.
- **Remote Network Printing:** Enables printing to a network printer on the host machine's network. Not suitable in situations where the PCoIP Software Client device is not on the same network as the host device.
- **Cloud Printing:** This is access to external Cloud Services that are set-up on your local workstation and network. Once these services have been correctly configured they can be used by the PCoIP Software Client.
- **Local Network Printing:** Enables printing from the host machine to a printer in the PCoIP Client machine's local area network. This method is suitable for printing when host and client are not on the same network or for identifying and printing to local printers that exist in multi-site organizations.

Support for each of these methods varies depending on which PCoIP agent the Software Client for Windows connects to. The Software Client for Windows printing support is as follows:

	Windows agents	Linux agents	macOS agents
Local USB Printing	—	—	—
Remote Network Printing	✓	—	—
Local Network Printing	✓	—	—
Cloud Printing	✓	—	—

Relative Mouse Support

Relative Mouse is a method of translating mouse movements as a delta from the last mouse position rather than a move to an absolute position on the screen. This type of mouse control is used in many CAD/CAM, Visual Effects and First-Person Gaming software. In a CAD program you may want to control an objects orientation in 3-D with mouse movements. Moving the mouse to the left or right rotates the object around the Z-axis, and moving the mouse up or down rotates the object around the X-axis. As you continue to move the mouse left the object continues to rotate about the axis, and the rotation is not bounded by the mouse stopping at the borders of the screen.

While in relative mouse mode, **the mouse cursor is not visible** since it the mouse is controlling directional movement and is not pointing to a location on the screen.

Applications that use relative mouse movements generally provide methods for entering or exiting relative mouse mode, for instance clicking on an object with the middle button. While the middle button is held down the object may be controlled using relative mouse movements.

Relative mouse mode is supported by all PCoIP clients. Note that PCoIP Zero Clients must be configured to enable it.

Relative mouse mode is supported by the following agents:

- PCoIP Standard Agent for Windows
- PCoIP Graphics Agent for Windows
- PCoIP Standard Agent for Linux
- PCoIP Graphics Agent for Linux

Relative mouse mode is not supported by the PCoIP Graphics Agent for macOS.

 **Note: Only supported on standard mode**

Relative Mouse is not supported when a client is running in High Performance Mode. It is only supported in standard mode.

Enabling Relative Mouse

The following sections outline how to enable relative mouse support on the Software Client for Windows.

Enabling from the Menu Tab

The following steps outline how to enable relative mouse from the menu tab, while connected to a supported PCoIP Agent with a supported PCoIP Client:

1. Click **Connection** from the menu tab.
2. Select the **Relative Mouse** option and click it to enable it. Once the check-mark is visible beside the Relative Mouse option it is enabled.

If you are connected to a PCoIP Agent version that does not support relative mouse then you will not be able to select this option.

Enabling with a Hot-Key

To enable relative mouse using a hot-key, while connected to a supported PCoIP Agent with a supported PCoIP Client, press `ctrl+alt+r`. This will toggle the feature on and off. This will only work if you are connected to a PCoIP Agent version that supports relative mouse.

USB Support

PCoIP Clients supports redirecting USB devices to a remote session. Administrators can set rules governing allowed and disallowed devices, device classes, or device protocols.

Important: USB support is enabled by default

USB bridging is enabled by default. If you want to restrict or disable USB support, you can globally disable or set rules governing USB behavior via GPO settings on the PCoIP Agent.

USB Redirection

USB redirection is only intended to be used with a single instance of the PCoIP Software Client. Launching a second instance of the PCoIP Software Client while USB devices are redirected from another client may not work as expected.

Isochronous USB device support

Some USB devices with time-sensitive information, such as webcams, are supported when connecting to the PCoIP Agent for Windows.

Additionally, Teradici's technology partners provide solutions to expand peripheral support. For more information, look for partners listed under Peripherals on the [Teradici Technology Partners](#) page.

Console Game Controller Support

PCoIP Software Clients are compatible with the following console game controllers:

- PS4
- PS5
- Logitech F310 gamepad

The following console game controllers are supported with the PCoIP Zero Client:

- Xbox One 2015
- Xbox One
- Xbox One S
- Xbox One Bt
- Xbox One Elite

SpeechMike Support

SpeechMike is supported between the PCoIP software client for Windows and a PCoIP agent for Windows.

SpeechMike is an isochronous USB device, and requires USB ISO device support to be enabled. The HID checkmark needs to be selected for the feature to work.

On the Windows VM agents set **pcoip.enable_unsupported_iso_devices=1**, using the command line below:

```
REG ADD HKLM\Software\Policies\Teradici\PCoIP\pcoip_admin_defaults /v  
pcoip.enable_unsupported_iso_devices /t REG_DWORD /d 1
```

On the PCoIP Client machine, set **pcoip.usb_allow_unsupported_device=1** using the command line below:

```
REG ADD HKLM\Software\Policies\Teradici\PCoIP\pcoip_admin_defaults /v  
pcoip.usb_allow_unsupported_device /t REG_DWORD /d 1
```

Wacom Tablet Support

The Software Client for Windows supports Wacom tablets in two configurations: *bridged*, where peripheral data is sent to the desktop for processing, and *locally terminated*, where peripheral data is processed locally at the Software Client.





Locally-Terminated Wacom Tablets





Locally terminated Wacom tablets are much more responsive, and tolerate high-latency connections better than bridged.

Local Termination is automatically used whenever it is supported for a device. If you prefer to use bridged mode—if, for example, you must use sophisticated tablet features like touch, which is not supported by local termination—you can override this behavior by [blacklisting a device for local termination](#).

Local termination requires a supported PCoIP agent (any type), and a supported Software Client for Windows.

PCoIP client support for *locally terminated* Wacom tablets and the Software Client for Windows


	PCoIP agents (Windows) 	PCoIP agents (Linux) 	PCoIP Graphics Agent for macOS 	PCoIP Remote Workstation Card 
Intuos Pro Small <i>PTH-460</i>	✓	✓	—	—
Intuos Pro Medium <i>PTH-660</i>	✓	✓	✓	—
Intuos Pro Large <i>PTH-860</i>	✓	✓	✓	—
Cintiq 22HD <i>DTK-2200</i>	✓	✓	—	—

	PCoIP agents (Windows) 	PCoIP agents (Linux) 	PCoIP Graphics Agent for macOS 	PCoIP Remote Workstation Card 
Cintiq 22 <i>DTK-2260</i>	✓	✓	—	—
Cintiq Pro 24 <i>DTK-2420</i>	✓	✓	—	—
Cintiq 22HDT - Pen & Touch <i>DTH-2200</i>	—	—	—	—
Cintiq Pro 24 - Pen & Touch <i>DTH-2420</i>	✓	✓	—	—
Cintiq Pro 27 <i>DTH-271</i>	✓	✓	—	—
Cintiq 32 Pro - Pen & Touch <i>DTH-3220</i>	✓	✓	—	—

Bridged Wacom Tablets

Bridged Wacom tablets should be used only in low-latency environments. Tablets that are bridged in network environments with high latency (greater than 25ms) will appear sluggish and difficult to use for artists, and are not recommended.





When connecting a Wacom tablet, bridged mode is used only if local termination is not available. To override this behavior, causing the Software Client for Windows to use bridged mode instead, add the device to the [Local Termination Blacklist](#).

 **Note: Graphics Agent for macOS does not support bridged Wacom tablets**

The Graphics Agent for macOS only supports local termination of Wacom devices.

The following Wacom tablet models have been tested and are supported on the Software Client for Windows:

PCoIP client support for *bridged* Wacom tablets and the Software Client for Windows

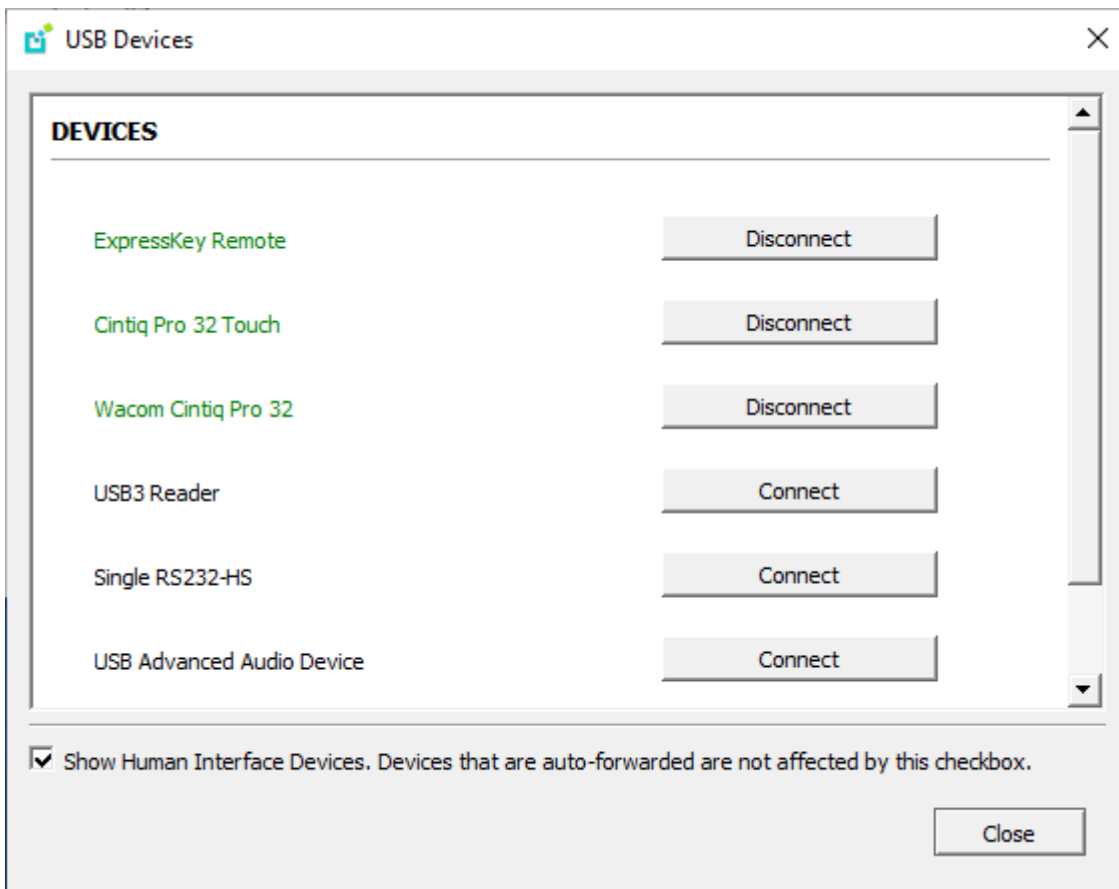
	PCoIP agents (Windows) 	PCoIP agents (Linux) 	PCoIP Graphics Agent for macOS 	PCoIP Remote Workstation Card 
Intuos Pro Small <i>PTH-460</i>	✓	✓	—	✓
Intuos Pro Medium <i>PTH-660</i>	✓	✓	—	✓
Intuos Pro Large <i>PTH-860</i>	✓	✓	—	✓
Cintiq 22HD <i>DTK-2200</i>	✓	✓	—	✓
Cintiq 22 <i>DTK-2260</i>	✓	✓	—	✓
Cintiq Pro 24 <i>DTK-2420</i>	✓	✓	—	✓
Cintiq 22HDT - Pen & Touch <i>DTH-2200</i>	✓	✓ <i>Ubuntu only</i>	—	✓
Cintiq Pro 24 - Pen & Touch <i>DTH-2420</i>	✓	✓	—	✓
Cintiq Pro 27 <i>DTH-271</i>	✓	✓	—	—

	PCoIP agents (Windows) ☐	PCoIP agents (Linux) 🔒	PCoIP Graphics Agent for macOS 🍏	PCoIP Remote Workstation Card 🖨️
Cintiq 32 Pro - Pen & Touch DTH-3220	✓	✓	—	✓

Connecting Cintiq Pro 32 Tablets

The Wacom Cintiq Pro 32 appears as *three* separate devices in the USB menu. You should connect the following USB devices to use this tablet:

- ExpressKey Remote
- Cintiq Pro 32 Touch
- Wacom Cintiq Pro 32



Known Issues

The following limitations apply to Wacom tablet support:

- Touch only works on the Cintiq Pro 32 Pen & Touch (DTH-2420). Touch functionality is not supported for any other Wacom tablet.
- ExpressKey Remote does not work on the Wacom Cintiq Pro 32 (DTH-3220). You should still connect this device when connecting the Wacom tablet.
- There are cursor limitations when working with the Wacom Cintiq 22HD (DTK-2200) and Wacom Cintiq Pro 24 (DTK-2420) for both bridged and locally terminated devices.
- Control buttons on the Wacom Cintiq Pro 32 (DTH-3220) do not function when locally terminated.
- PCoIP Clients are not compatible with NoMachine and No Machine USB drivers. For information on how to uninstall NoMachine USB drivers, see [No Machine's knowledge base](#).



Important: Wacom devices must be connected to the session for full feature support

Locally-terminated Wacom tablets must be connected to the PCoIP session using the Software Client for Windows's in-session menu in order to use pressure sensitivity and other supported features. If a device is plugged into a USB port but is **not** connected to the session, it will behave as a simple pointer device; this creates a confusing situation where the device initially appears to work, but expected features do not function.

Webcam Support

The Software Client for Windows now supports USB webcams when connecting to a PCoIP Agent for Windows. USB webcams can now be used while in the remote desktop, including with applications such as Microsoft Teams or Zoom.

For detailed information which models have been tested and the performance metrics associated with these models see [here](#). This knowledge base article also deals steps on how to test and verify other webcam models.

This feature is enabled by default.

Requirements

Webcam support requires the following:

- Software Client for Windows, 21.07+
- PCoIP Standard Agent for Windows or PCoIP Graphics Agent for Windows, 21.03+
- USB-attached webcam.

Notes and Limitations

- Webcams must be connected via USB. Webcams that are not USB, such as embedded laptop webcams, are not supported.
- Linux agents are not supported.
- PCoIP Software Client for macOS is not supported.
- If the browser on the remote desktop terminates when a webcam is connected, you must disable the webUSB setting in Chrome by running the following command in the search bar of the Chrome browser:

```
chrome://flags/#enable-webusb-device-detection
```

Open the Chrome menu and disable the webUSB flag.

Setup

On the PCoIP Software Client, connect the webcam as described in [USB Bridging of Webcams](#).

Installing the Software Client for Windows

In this section, you will learn how to install and uninstall the Software Client for Windows for Windows.

Before You Begin

Before installing the Software Client for Windows:

- You must be logged in as an administrator to the client machine.
- Close any existing Software Client for Windows applications.

Installing the Software Client

You can install the Software Client for Windows with the provided Windows installation wizard or from the command line.

To install the Software Client for Windows using the wizard:

1. Double-click the Software Client for Windows installer executable (pcoip-client.exe) to begin installation.
2. Follow the prompts to specify installation locations, and to agree to any licenses.



Microsoft Visual C++ Redistributable package

The libraries in this package are required by the Software Client for Windows. If they aren't already installed, a wizard will launch and install them for you.

3. Click **Finish** to complete installation and close the installer.

To install the Software Client for Windows silently from the command line:

- Install the Software Client for Windows silently by running the installer executable from the command line:

```
<path-to-installer>\pcoip-client.exe /S`
```

where `<path-to-installer>` is the full path to the folder containing the `pcoip-client.exe` executable.

Silent installation uses default options

The silent installer uses default settings and options. For example, a silent installation won't create a desktop shortcut.

Updating the Software Client

To upgrade to a newer version of the Software Client for Windows, download and install the new version in place. You do not need to uninstall your current version; your settings will be preserved.

Uninstalling the Software Client

To uninstall the Software Client for Windows:

1. Click **Start** (or **Search Windows** for Windows 10).
2. In the search box, type **Add or remove programs** and press **Enter**.
3. Select **Teradici PCoIP Client** from the list of programs.
4. Click the **Uninstall/Change** button above the list.

Troubleshooting PCoIP Session Connection Issues

If you encounter issues with your PCoIP Session, please see the following KB article: <https://help.teradici.com/s/article/1027>. This article details some potential causes and fixes for common connection issues.

Installing the Software Client in Silent Mode

The following section outlines how to install the PCoIP Software Client in silent mode. Please note that you must authorize the application to run in silent mode. To install the PCoIP Software Client

on Windows use the `/S` switch on the command line when launching the installer in the Windows CMD Prompt as outlined in the following example:

```
C:\Downloads\pcoip-client_21.03.0.exe /S
```

Connecting to Remote Desktops

Important: Welcome to our new user interface!

In release 22.09, the Software Client for Windows user interface has been redesigned from the ground up. If you're a new user, you should find the new interface easy to follow; for existing users, note that some behavior has changed. Notes appear throughout this page when a task has changed from previous releases.

The Software Client for Windows can connect to any remote host with a PCoIP agent installed and configured, or a PCoIP Remote Workstation Card. Remote hosts can be Windows, macOS, or Linux, and can be made directly (client to host) or through a connection manager in enterprise deployments.

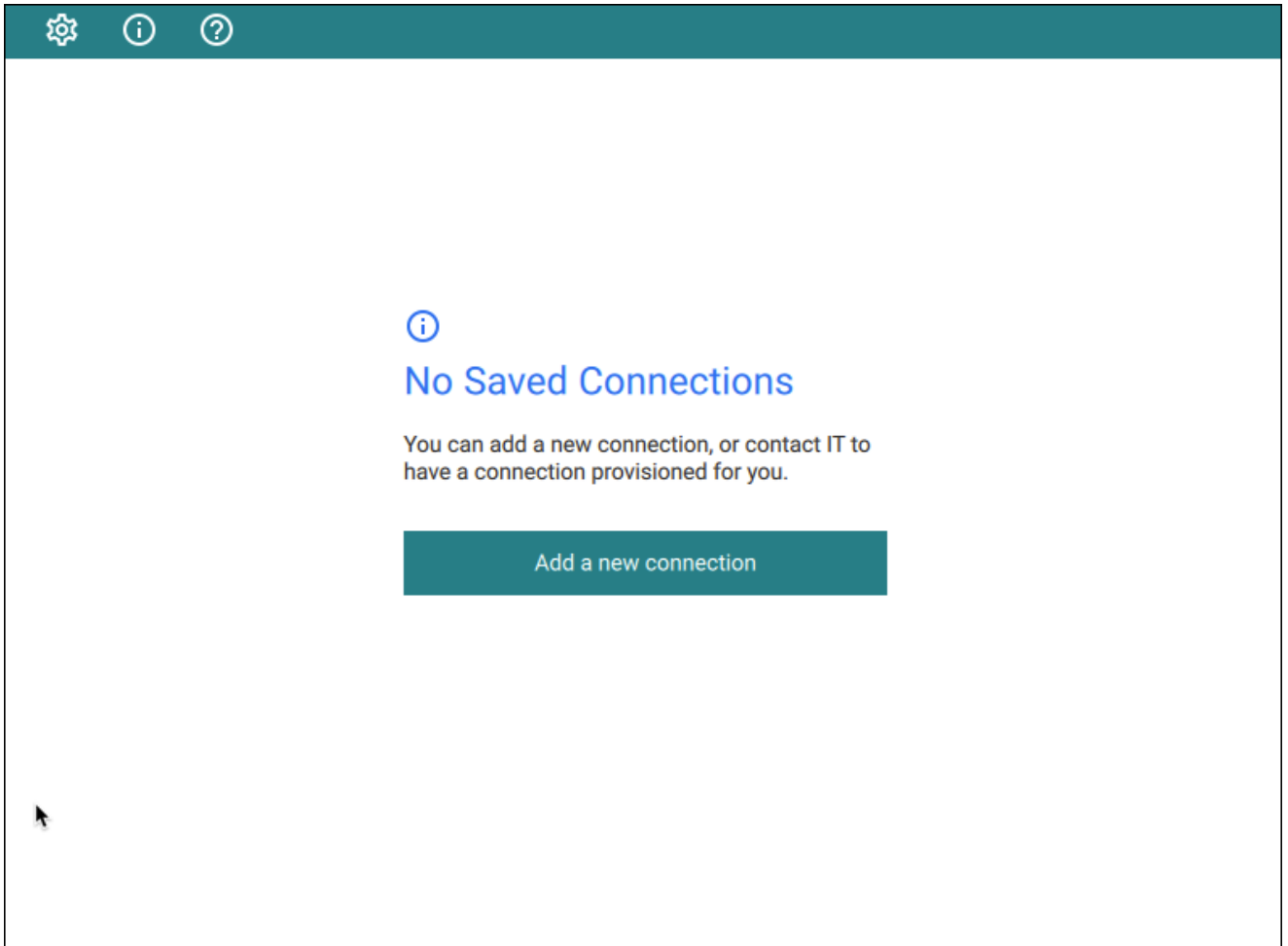
Note: PCoIP Remote Workstation Card connections

Connections to PCoIP Remote Workstation Cards require preparation on the remote machine before they will work. For details, see [Preparing for PCoIP Remote Workstation Card Connections](#).

Creating Your First Connection

The first step is to create a **connection** to either your agent (for direct connections) or to your connection manager (for managed deployments).

1. Launch the Software Client for Windows.
2. If this is your first connection, the Software Client for Windows will prompt you to create one:



Click **Add a new connection** to proceed.

3. In the **Add New Connection** pane, there are two fields to provide:

Add New Connection

Let's get started! Enter the host address or registration code provided by your system administrator.

Host Address or Registration Code

Connection Name

Add connection

[← Back to connections](#)

- **Host Address or Registration Code:** Enter the address of the remote system you want to reach (you should have this information from your system administrator). This field accepts IP addresses, domain names, and registration codes, as in these examples:
 - *An IP address:* `123.456.789.012`
 - *A domain name:* `remote-desktops.example.com`
 - *A registration code:* `a1b2c3!@#`

 **Note: Amazon WorkSpaces registration codes**

If you are connecting to an Amazon WorkSpaces desktop, provide your WorkSpaces registration code in this field.

- **Connection Name:** Provide a name for this connection. This can be anything; you will use this name to select this connection in future sessions. You can always change it later.

4. Click **Add connection**.

Once this is done, you'll see the connection you created shown as a clickable button. You can add as many connections as you like, by clicking **+ Add a new connection** at the bottom of the **Connect** pane.

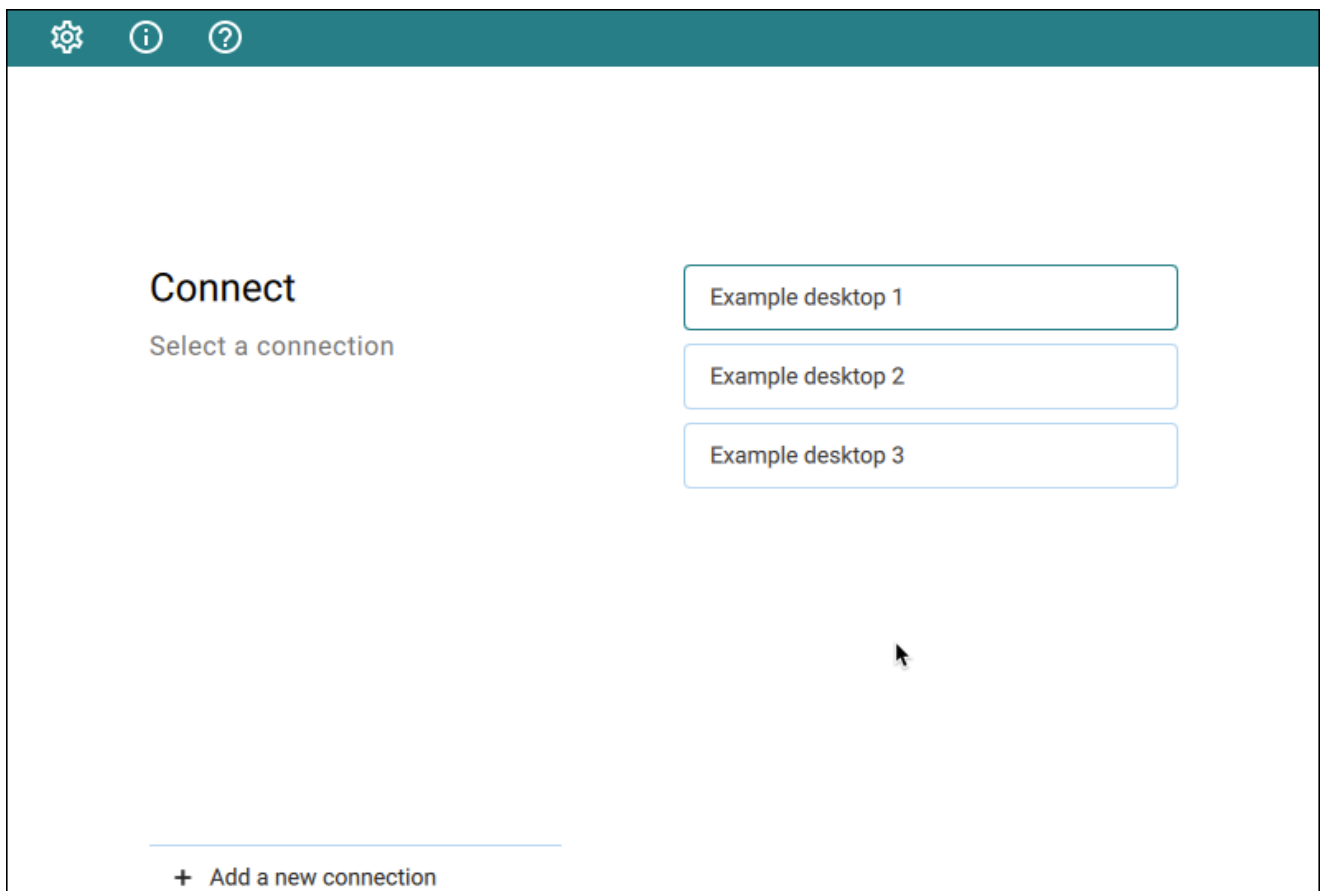
Tip: Difference from previous workflows

The connections you save here are to *brokers*, or to *direct desktop connections*. If you have multiple desktops behind a single broker, you will still have to choose your desired desktop after authenticating with the broker. In the previous interface, you could save connections at any stage of the process, including to individual desktops.

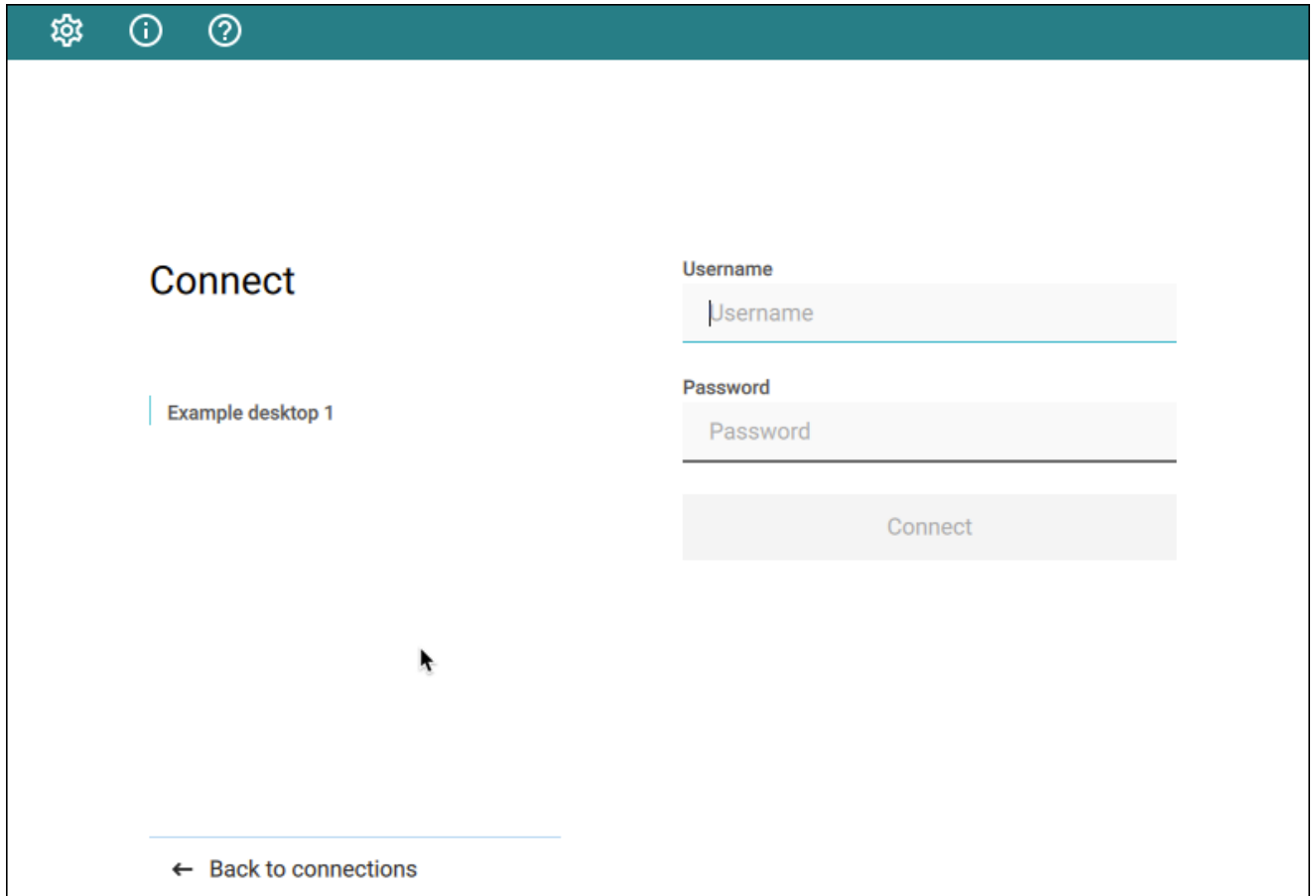
If you have existing saved connections from previous releases, they will continue to work when you upgrade to this client version. However, if they are deleted, they cannot be re-created.

Connecting to a Session

1. Assuming you have created at least one connection, the Software Client for Windows will now look something like this:



2. Click the name of the connection you want. Next, provide your username and password:



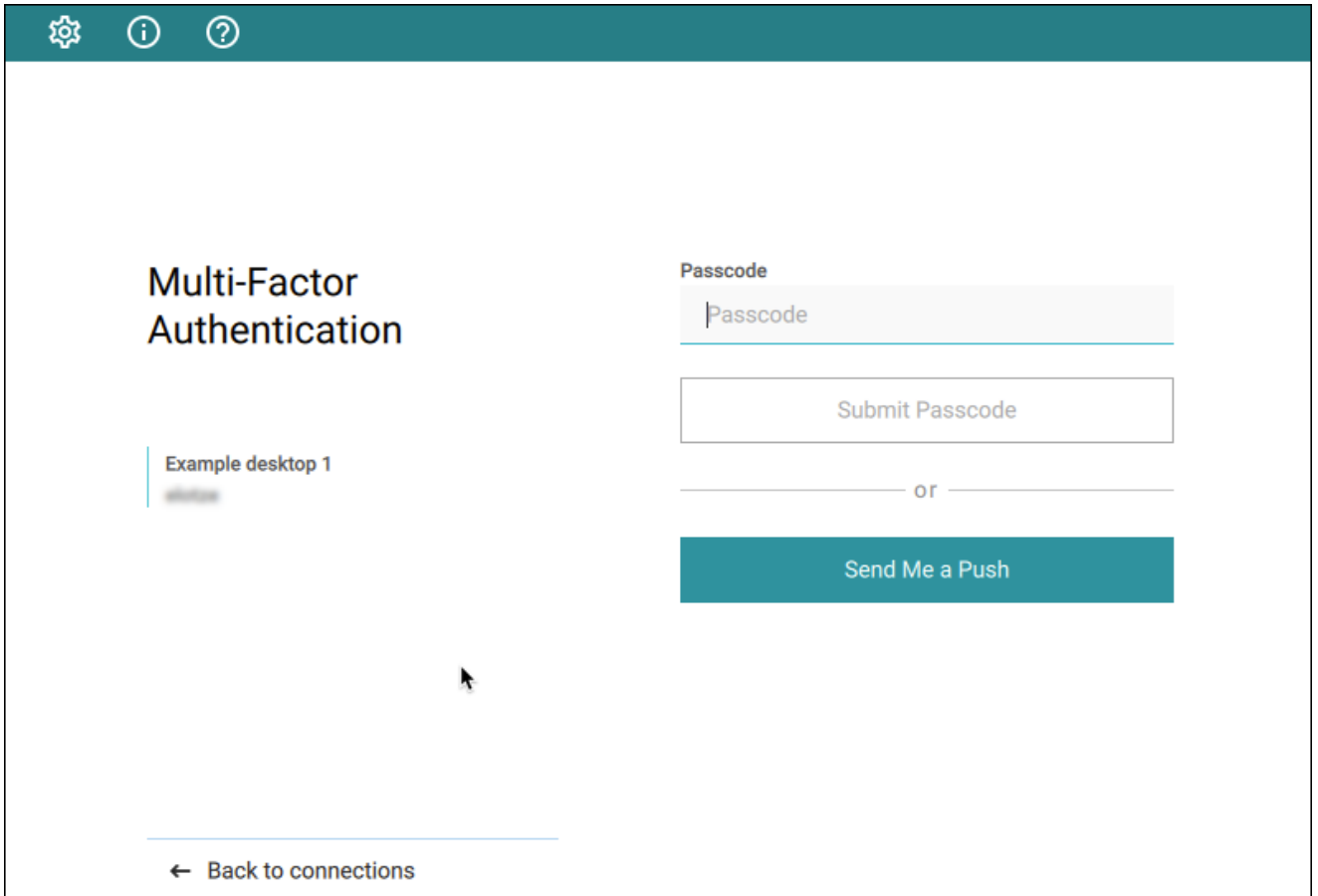
The screenshot shows a web interface for connecting to a session. At the top, there is a teal header bar with three icons: a gear (settings), an 'i' (info), and a '?' (help). Below the header, the main content area is white. On the left, the word 'Connect' is displayed in a large, bold font. Below it, there is a vertical line followed by the text 'Example desktop 1'. On the right side, there is a form with two input fields: 'Username' and 'Password'. The 'Username' field contains the text 'Username' and the 'Password' field contains the text 'Password'. Below these fields is a large, light gray button labeled 'Connect'. At the bottom left of the form area, there is a blue horizontal line followed by a left-pointing arrow and the text 'Back to connections'.

 **Note: About authentication credentials**


For **managed connections**, the authentication screen and validation that happens here is managed by your connection broker. The credentials are supplied to you by your system administrators, and are usually your corporate credentials.

For **direct connections** where no broker is present, use the credentials for your user account on the remote machine.

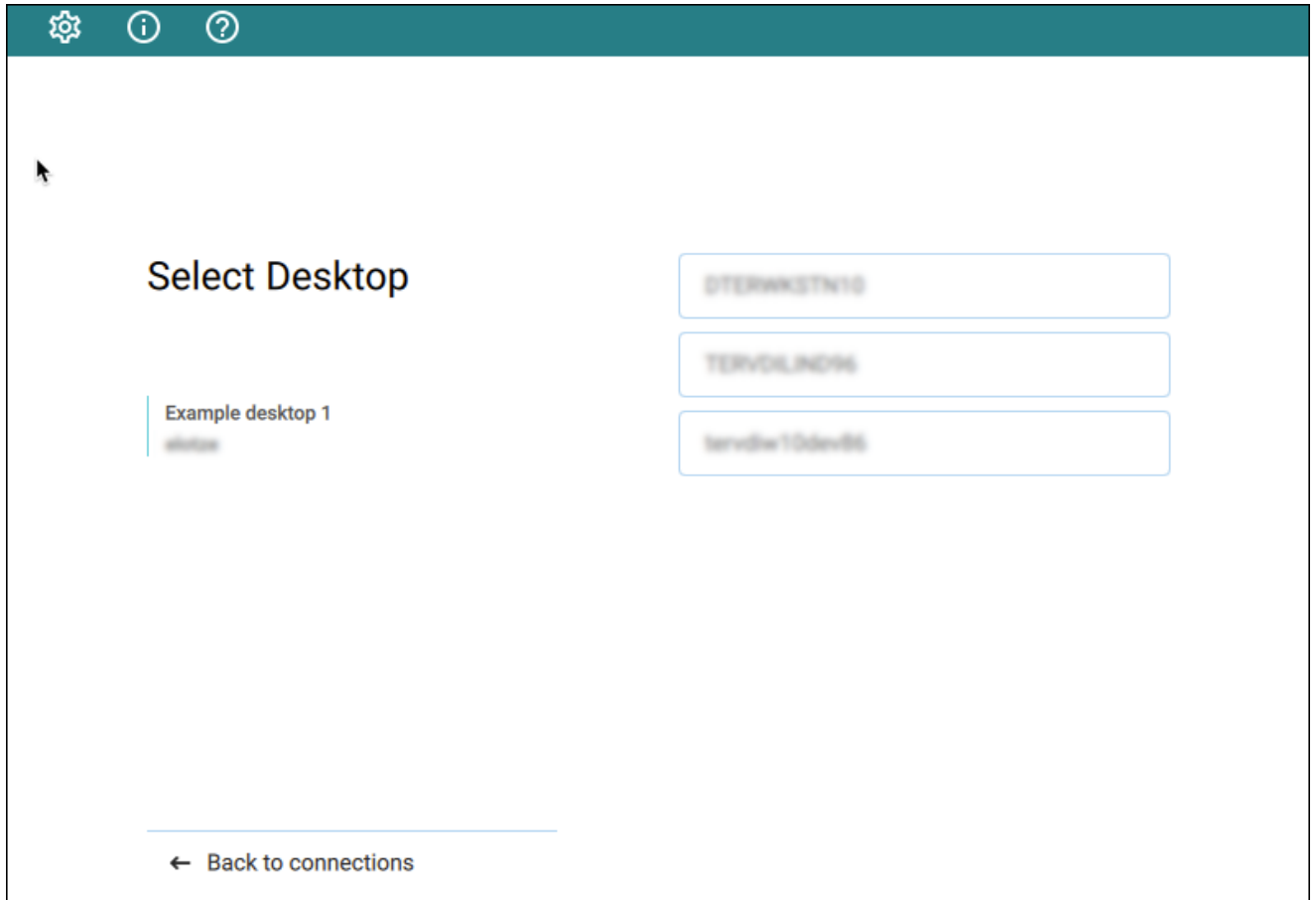
3. If your system is configured for multi-factor authentication, you will see a **Multi-Factor Authentication** screen next; either provide your passcode if you have one, or click **Send Me a Push** to have an authentication request sent to your registered device.



4. Once your credentials are accepted, the Software Client for Windows shows you a list of your authorized desktops.

 **Tip: Customizing desktop labels**

You can change the labels that appear in this list to make them easier to identify. See [Changing the Remote Desktop labels](#) for instructions.



Click the desktop you want to connect to.

Once you have selected your desktop, you will be connected to it and your PCoIP session will begin. The connection will use the display mode you last used (windowed, fullscreen one monitor, or fullscreen all monitors), unless altered by a launch-time [configuration](#).

There may be a delay of a few seconds before you have control of your mouse and keyboard; this is normal.

Changing Remote Desktop Labels

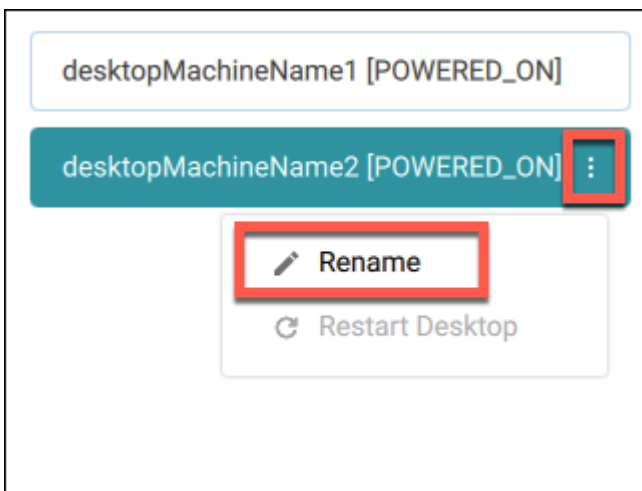
By default, the Software Client for Windows displays the *machine names* of your remote desktops. These names can often be obscure strings that are difficult to identify or differentiate. You can modify the name shown in the desktop list to give them human-friendly names that are easier to understand.

Note: Only labels are changed

This procedure changes the desktop's label, shown in the client interface. It does not change the desktop's machine name.

To change the label for a desktop:

1. Select a connection in the Software Client for Windows and provide your credentials.
2. From the list of displayed desktops, find one you want to change and click its expansion icon to reveal the context menu:



3. Click **Rename**.
4. Provide the new, human-friendly name you'd like to see instead of the machine name.
5. When finished, your desktops will appear using the name you specified:



Restarting Remote Desktops

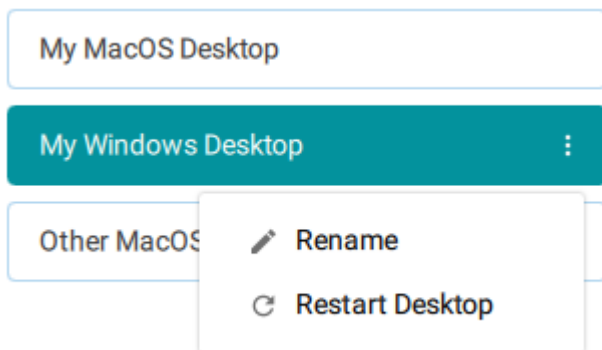
If your deployment supports remote restarts, you can command a desktop to restart from the Software Client for Windows pre-session interface (before you have connected to a PCoIP session).

 **Note: Not all deployments support this feature**

The restart option will only be available if your system supports it. If it does not, the restart option will appear in the menu but will be disabled.

To restart a remote desktop:

1. Select a connection in the Software Client for Windows and provide your credentials.
2. From the list of displayed desktops, find one you want to restart and click its expansion icon to reveal the context menu:



3. Click **Restart**.

The remote desktop will be restarted. Note that it will be unavailable for connections until the restart is complete, which may take several minutes depending on the system.

Connecting to PCoIP Remote Workstation Cards

You can connect to remote workstations equipped with a PCoIP Remote Workstation Card, and with PCoIP Remote Workstation Card Software (for Windows or Linux) installed.

Refer to [System Requirements](#) for supported versions.

Initial Workstation Configuration

Before you can connect to your remote workstation for the first time, you must install software and make some configuration changes. These actions only need to be taken once for each remote workstation in your system:

- **Record the MAC address of the PCoIP Remote Workstation Card**

Before you install the PCoIP Remote Workstation Card, **record the MAC address of the PCoIP Remote Workstation Card**; this will allow you to log into the card to configure its settings. Type `https://pcoip-host-<MAC_ADDRESS>.mydomain` where `<MAC_ADDRESS>` is the MAC address of your PCoIP Remote Workstation Card and `mydomain` is the local domain of your network. This step is important as the host driver function is disabled by default, so the Remote Workstation Card Software will not pick up information about the PCoIP Remote Workstation Card, such as the MAC address. The MAC address enables you to connect to the PCoIP Remote Workstation Card to view the IP address and enable the host driver function.

For more information on IP and MAC information relating to the PCoIP Remote Workstation Card, see [How do I find the IP address of my newly installed PCoIP Zero Client or PCoIP Remote Workstation card?](#) in the knowledge base.

- **Install the PCoIP Remote Workstation Card Agent:** To connect to a PCoIP Remote Workstation Card machine with a PCoIP Software Client, the ***Remote Workstation Card Agent*** software must be installed.
- **Verify accessibility:** Both the NIC of the workstation and the NIC of the PCoIP Remote Workstation card need to be accessible by the PCoIP Software Client. They can be on different local networks as long as both are accessible by the PCoIP Software Client. If they are both behind a NAT and accessed by the PCoIP Software Client then the PCoIP Remote Workstation Card Agent must send the NAT'ed address to the PCoIP Software Client when connecting.

- **Enable monitor emulation for the video ports on your remote workstation:** If monitor emulation is not enabled, you may see blank gray screens when you connect from the PCoIP Software Client.

To enable monitor emulation, log in to the card's Administrator Web Interface (AWI) and select **Enable Monitor Emulation on Video Port n** from the *Configuration > Monitor Emulation* menu. For more information, see the [PCoIP Remote Workstation Card Administrators' Guide](#).

- **Disable temporal dithering:** Temporal dithering causes blurriness, heavy packet loss, and high CPU usage on the PCoIP Software Client machine.
- **Linux workstations: configure PCoIP Remote Workstation Card Software to Start Automatically:** To configure the PCoIP Remote Workstation Card Software to start automatically, log into the workstation using a PCoIP Zero Client or directly from a local mouse and keyboard, and modify the workstation startup script to launch the PCoIP Remote Workstation Card Software. For details, see [Installing PCoIP Remote Workstation Card Software Binary RPM in the PCoIP® Remote Workstation Card Software for Linux User Guide](#).

Once the remote workstation is properly configured, you can use the Software Client for Windows to connect to it.

Connecting to a PCoIP Remote Workstation Card through the command line

You can connect directly to a PCoIP Remote Workstation card from a PCoIP Software Client by launching the client from the command line. For details, see [hard host](#) in client configuration.

PCoIP Remote Workstation Card Limitations

Not all features with the Software Client are fully supported when connecting to a PCoIP Remote Workstation Card. The following section outlines these limitations against certain features.

Audio: PCoIP Remote Workstation Card uses a hardware based audio protocol which is not fully supported on the Software Client.

Topology: Single display configurations will work. There may be disruptions in the forms of black bars or scroll bars on the client if the PCoIP Remote Workstation Card does not support the display configuration on the client.

USB: Connecting USB devices to the PCoIP Remote Workstation Card is not supported.

Performance: The PCoIP Remote Workstation Card does not support PCoIP Ultra enhancements.


Connecting Remotely using NAT or VPN

The same principles that apply for PCoIP Zero Clients apply to PCoIP Software Clients when connecting to multiple hosts through a WAN. Connections from a PCoIP Software Client to a Remote Workstation Card across a WAN will require a VPN or NAT setup with enterprise level NATing devices. For information on how to connect a PCoIP Software Client to a Remote Workstation Card installed in a Windows host computer, see [Connections from Software Clients](#) in the PCoIP Remote Workstation Card Administrators' Guide.

Disconnecting a Session

To disconnect a PCoIP session:

1. If you are in a full-screen mode, reveal the Software Client for Windows menu bar by moving the mouse cursor to the top of a display.
2. From the Software Client for Windows menu bar, select **Connection > Disconnect**.

 **Tip: Quickly disconnect from a session**

To quickly disconnect from a session, press `Ctrl+Alt+F12`.

Quitting the PCoIP Client application will also disconnect the current session.

Using Displays

When you connect to a PCoIP session, the Software Client for Windows shows your remote desktop as one or more displays. The number of displays it shows is constrained by your local system's available monitors (and the PCoIP protocol itself, which supports up to four monitors).

You can choose whether the Software Client for Windows shows your remote session as a single display in a resizable [window](#), or as [one](#) or [many](#) full-screen displays.

You can also [add or remove local displays](#) during a session.

Display Modes

Using the Software Client for Windows, you can switch between three display modes. Note that some of these modes are system-dependent; for example, if your local system has only one monitor, you will not see options for multiple displays.

- [Windowed mode](#): A single display shown in a window.
- [Full Screen All Monitors](#): All available local monitors are used in full-screen mode to show the remote desktop.
- [Full Screen One Monitor](#): A single display shown full-screen on the local system.

Windowed Mode

In Windowed mode, the Software Client for Windows provides a single window, resizable and movable, which contains the remote desktop. The remote desktop will rescale to fit your window dimensions if you change them.

To use windowed mode:

1. Reveal the Software Client for Windows menu bar by moving the mouse cursor to the top of a display.
2. From the Software Client for Windows menu bar, select **View > Leave Fullscreen**.

Full Screen Modes

In *full-screen* modes, the Software Client for Windows expands to fill either [one local display](#) or [all of your local displays](#).

In both full-screen modes, the Software Client for Windows menu bar is hidden. To reveal it, move your mouse cursor to the top of the display and hover for a moment.

Tip: Quickly switch to full-screen mode

You can quickly switch from windowed mode to whichever full-screen mode you used last by pressing

`ctrl+alt+Enter`.

Full Screen All Monitors

In *full screen all monitors* mode, the application expands to present full-screen remote displays on *all* of your local monitors. The remote desktop will map a remote display to each of your local displays.

You will only see this option if your local system has multiple displays.

To use Full Screen All Monitors mode:

1. If you are in *full-screen one monitor* mode, reveal the Software Client for Windows menu bar by moving the mouse cursor to the top of a display.
2. From the Software Client for Windows menu bar, select **View > Fullscreen All Monitors**.

Full Screen One Monitor

In *full screen one monitor* mode, the presents a single full-screen remote display on one of your monitors.

If you switch from *Full Screen All Monitors* to *Full Screen One Monitor*, all open windows and applications will be moved onto the single display.

Tip: Monitor selection

The local monitor chosen for full-screen display depends on the mode you are switching from:

- If switching from *windowed* mode, the client's current display becomes full-screen.
- If switching from *full screen all monitors* mode, the display used to select *fullscreen one monitor* mode becomes full-screen.

To use Full Screen One Monitor mode:

1. If you are in a full-screen mode already, reveal the Software Client for Windows menu bar by moving the mouse cursor to the top of a display.
2. From the Software Client for Windows menu bar, select **View > Fullscreen One Monitor**.

Note: Systems with only one display

If your local machine has only one display, the menu option will say **Show Fullscreen**.

Adding or Removing Displays

You can add or remove local displays during a PCoIP session. If you are using [full screen all monitors](#) mode, you must [detect](#) the changes before they will be effective. Note that in the case of removing monitors, this could mean that some applications or information is inaccessible until the *detect monitors* command is issued.

Detecting Monitors

If the local display configuration changes during a session—for example, if you attach a new local monitor, or disconnect an old one—the display mapping between the local and remote topographies is no longer accurate, leading to unpredictable display behavior. You must refresh the display mapping to accurately show the new configuration.

To synchronize local display changes:

1. If you are in a full-screen mode already, reveal the Software Client for Windows menu bar by moving the mouse cursor to the top of a display.

2. From the Software Client for Windows menu bar, select **View > Detect Monitors**.

The local display configuration will be synchronized with the remote. The local displays may flicker or go black momentarily while the remote system updates its display topography.

Connecting USB Devices

Remote desktops can use USB devices that are attached to the client, using a process called *redirection*. USB devices are not automatically redirected to the remote desktop; they must be specifically connected to the session.

Note: Excludes Mice and Keyboards

Normal Human Interface Devices (HID), such as keyboards and mice, are always connected and used by the remote desktop. This page describes using non-HID USB devices such as tablets or cameras.

Important considerations

- **USB functionality depends on PCoIP Agent configuration:** The remote PCoIP agent must be configured to allow USB redirection. If it is not, only HID devices like keyboards and mice will be used, and the *Connection > USB Devices* option will not be visible in the Software Client for Windows menu bar.
- **Local Termination and Bridging:** Most USB devices are *bridged* to the host, which means their input is sent directly to the host machine for processing. Certain devices, including ePadLink Signature Pads and some Wacom tablets, connect using a different method called *local termination*. This mode does some pre-processing of device information locally at the client before forwarding to the host, resulting in increased responsiveness and better tolerance of high-latency networks.

The mode chosen is automatic, unless overridden. See [Wacom Tablets](#) for information about which Wacom tablets are supported.

- **Persistence:** USB device connections do not persist across multiple PCoIP sessions. You must connect your USB device each time you connect.
- **NoMachine USB Drivers:** PCoIP Clients are not compatible with NoMachine and No Machine USB drivers. For information on how to uninstall NoMachine USB drivers, see [NoMachine's knowledge base](#).

Connect a USB Device

To Connect a USB device:

1. Attach the USB device you want to connect to your local machine.
2. Select **Connection > USB Devices** from the PCoIP Software Client menu.

A list of all USB devices connected to your client machine appears. The list includes both external devices you plug in and integrated devices such as laptop cameras.

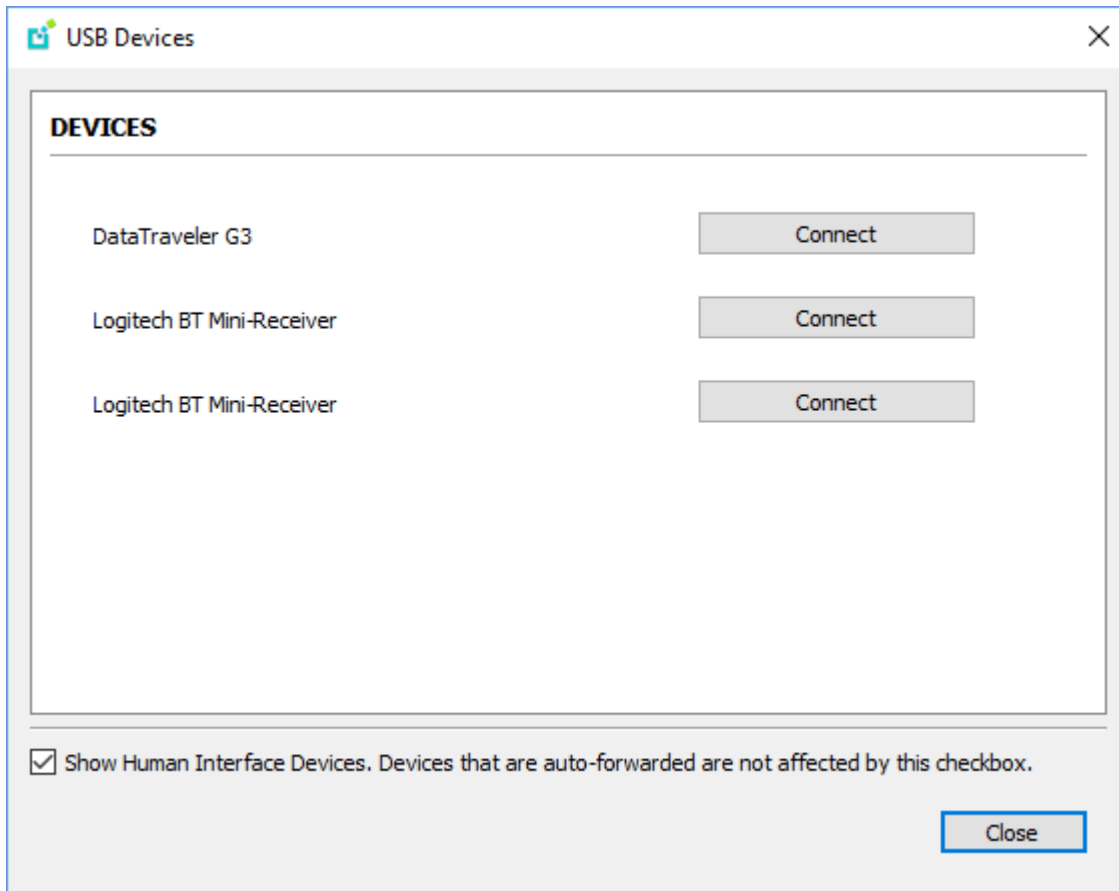
The name shown in the list is self-reported by the device; some devices will identify themselves only as *USB Device*.

Important: Connecting special HID devices

Because most Human Interface Devices (HIDs) are automatically processed by the Software Client for Windows, they do not appear on this list even if they use a USB connection. However, certain HID devices—like 3D mice and Wacom tablets—actually do require processing on the remote host, and will not work as expected unless connected to the session.

To show these hidden HID devices and allow them to be connected, enable the **Show Human Interface Devices** checkbox. You may also need to perform additional configuration steps or install drivers on the remote machine.

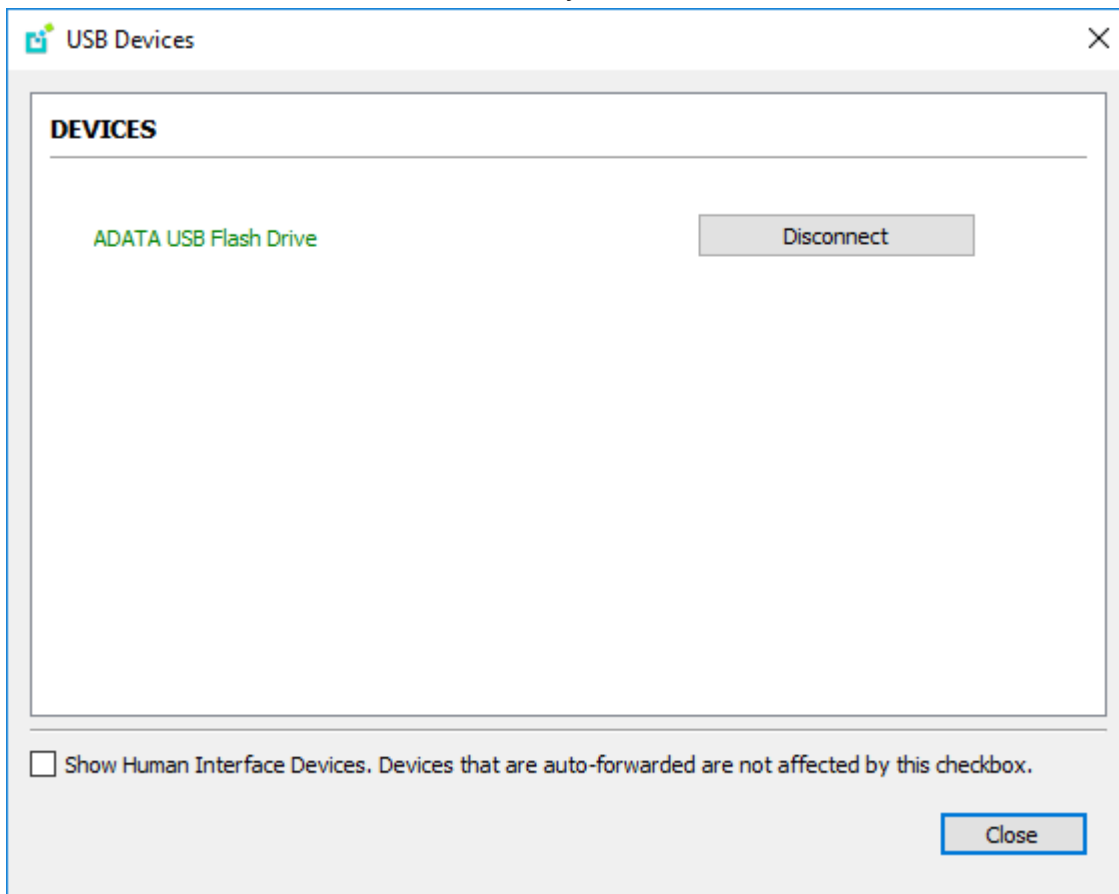
3. Click **Connect** beside the USB device you want to use.



Disconnect a USB Device

1. Select **Connection > USB Devices** from the PCoIP Software Client menu.

2. Click **Disconnect** beside the USB device you want to disconnect.



Automatically Forward All USB Devices

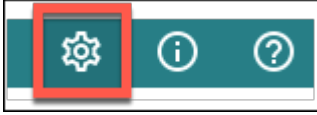
Automatic forwarding allows you to bridge all non-HID USB devices without requiring a manual connection step.

Note: Auto-forwarded devices can be disconnected from the client

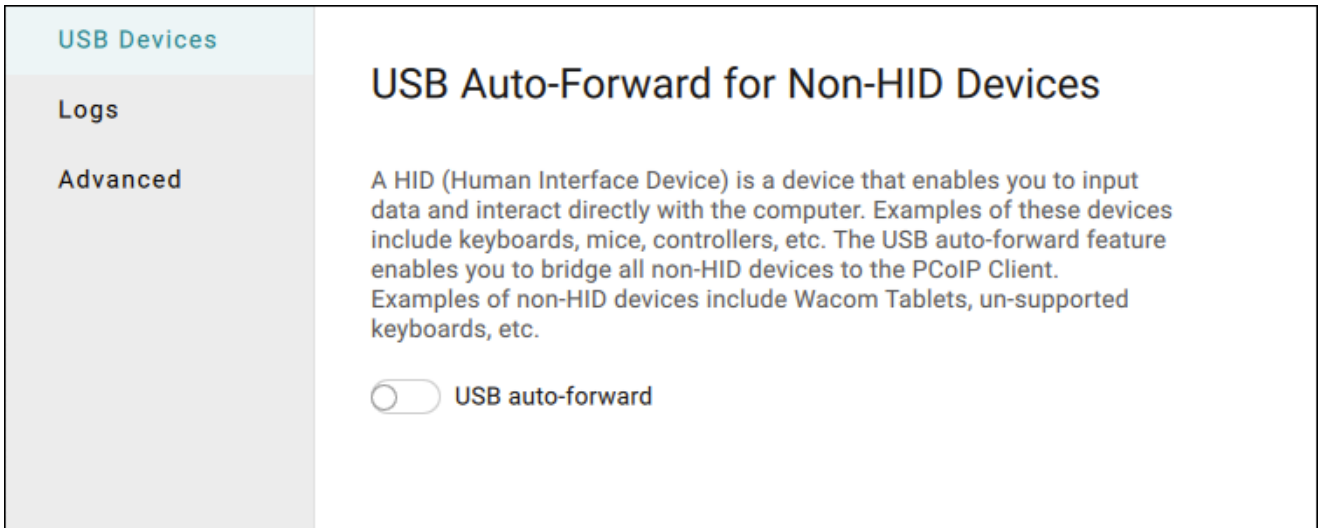
Devices that are automatically forwarded can still be disconnected and reconnected via the Software Client for Windows interface.

To enable automatic USB forwarding in the pre-session interface:

1. Disconnect any active PCoIP sessions and return to the pre-session interface.
2. Click the gear icon to open the settings window:



3. Click **USB Devices** in the left side menu, then enable **USB auto-forward** in the *USB Auto-Forward for Non-HID Devices* panel.



To enable automatic USB forwarding programmatically:

To enable automatic forwarding programmatically, launch the client using either the command-line or URI methods and use the `usb-auto-forward` flag. For more information, see [USB Auto-Forward](#) in the Configuration section.

Automatically Forward Devices by Vendor ID/Product ID

You can automatically forward specific devices to the remote host without requiring a manual connection step (devices not specified can still be connected manually, as shown [above](#)).

Note: Auto-forwarded devices can be disconnected from the client

Devices that are automatically forwarded can still be disconnected and reconnected via the Software Client for Windows interface.

Devices are identified by their Vendor ID and Product ID (VID and PID, respectively) which together make a unique identifier. You can specify up to 20 devices to automatically connect using this

method. If more than 20 devices are provided, only the first 20 will be accepted. The rest will be ignored, and noted in logs.

Invalid VID/PID pairs are discarded, and noted in logs.

To enable automatic forwarding by Vendor ID and Product ID, launch the client using either the command-line or URI methods and use the `vidpid-auto-forward` setting, providing the VID/PID pairs for the devices you want to connect. For more information, usage, and examples, see [Vidpid Auto-Forward](#) in the Configuration section.

Identifying Vendor and Product IDs

If you do not know the Vendor ID and Product ID of the device you want to automatically forward, you can discover them using the client logs.

To discover the Vendor and Product IDs:

1. Unplug all USB devices.
2. Launch the Software Client for Windows.
3. Plug in the device.
4. Close the Software Client for Windows.
5. [Find the most recent PCoIP Client log file.](#)
6. In a log viewer or text editor, look for lines containing `MGMT_USB :Device` , **and** `VID=` . In this example, there are two entries with `MGMT_USB :Device` ; we want the first line, which also contains the `VID` and `PID` assignments:

```
2040-12-12T20:36:46.117Z e0f9e9e9e-866f-1038-test-ac87a3007abc LVL:2 RC:
0      MGMT_USB :Device 0x00010001 VID=0x18a5PID=0x0302
2040-12-12T20:36:46.117Z e0f9e9e9e-866f-1038-test-ac87a3007abc LVL:2 RC:
0      MGMT_USB :Device 0x00010001 Name=TEST Serial=012345ABCDE
pp=000222222
```

7. VID and PID assignments appear like this: `VID=0x<VID_VALUE>PID=0x<PID_VALUE>` . *The VID and PID values we need are the strings after `0x` .*

Continuing the example, `VID=0x18a5PID=0x0302` means the VID we want is `18a5` , and the PID is `0302` .

8. The VID/PID pair is expressed as `<VID>, <PID>` . Following our example, this device would be specified as `18a5, 0302` .
9. Provide this (and others, if applicable) VID/PID pair to [Vidpid Auto-Forward](#) when launching via command line or URI, as indicated above.

Connect USB Webcams

USB Webcams may be used in remote sessions by connecting them to a Windows remote session as USB devices. This feature has been tested with a limited number of popular webcams, including the Logitech C920. See [PCoIP Cloud Access Software Webcam Support](#) for a current list of tested webcams.

This feature is only supported by the Graphics Agent for Windows and the Standard Agent for Windows, and is limited to resolutions of 480p or lower.

Configure Wacom Devices

This section outlines how to configure your Wacom tablet through the PCoIP Client session. There are two available features within the PCoIP Client that can be used to configure the monitor display and orientation. This only applies to locally terminated Wacom Tablets.

USB Connection Instructions

Before you carry out the Wacom tablet monitor configurations below, you must connect to the device by following the instructions outlined in the [Connecting to USB Devices](#) section.

Wacom Tablet Monitor

The Wacom Tablet Monitor feature enables you to select the monitor you want to use with your Wacom tablet. You can change between using a pen or mouse and select the orientation position.

To configure Tablet Monitor settings:

1. Select **View** from the in-session options bar.
2. Check the **Tablet Monitor** option.
3. Open **Wacom Tablet Properties** from the Wacom Desktop Center.
4. Select your device, tool and application.
5. Select your screen area from the dropdown menu.

Teradici PCoIP Client Connection View

- Leave Fullscreen Ctrl+Alt+Enter
- Show Fullscreen One Monitor
- Minimize Client Ctrl+Alt+M
- ✓ Tablet Monitor
- Tablet Orientation Left-handed

The screenshot shows the 'Wacom Tablet Properties' window with the 'Mapping' tab selected. The 'Device' is 'Intuos Pro M', the 'Tool' is 'Pro Pen 2', and the 'Application' is 'All'. The 'Mapping' section shows a red trapezoid representing the tablet area mapped to a red rectangle on the monitor. The 'Orientation' is set to 'ExpressKeys Left', 'Mode' is 'Pen', 'Screen Area' is 'Monitor 1', and 'Tablet Area' is 'Full'. The 'Use Windows Ink' checkbox is checked. Buttons for 'About', 'Options...', and 'Default' are visible at the bottom.

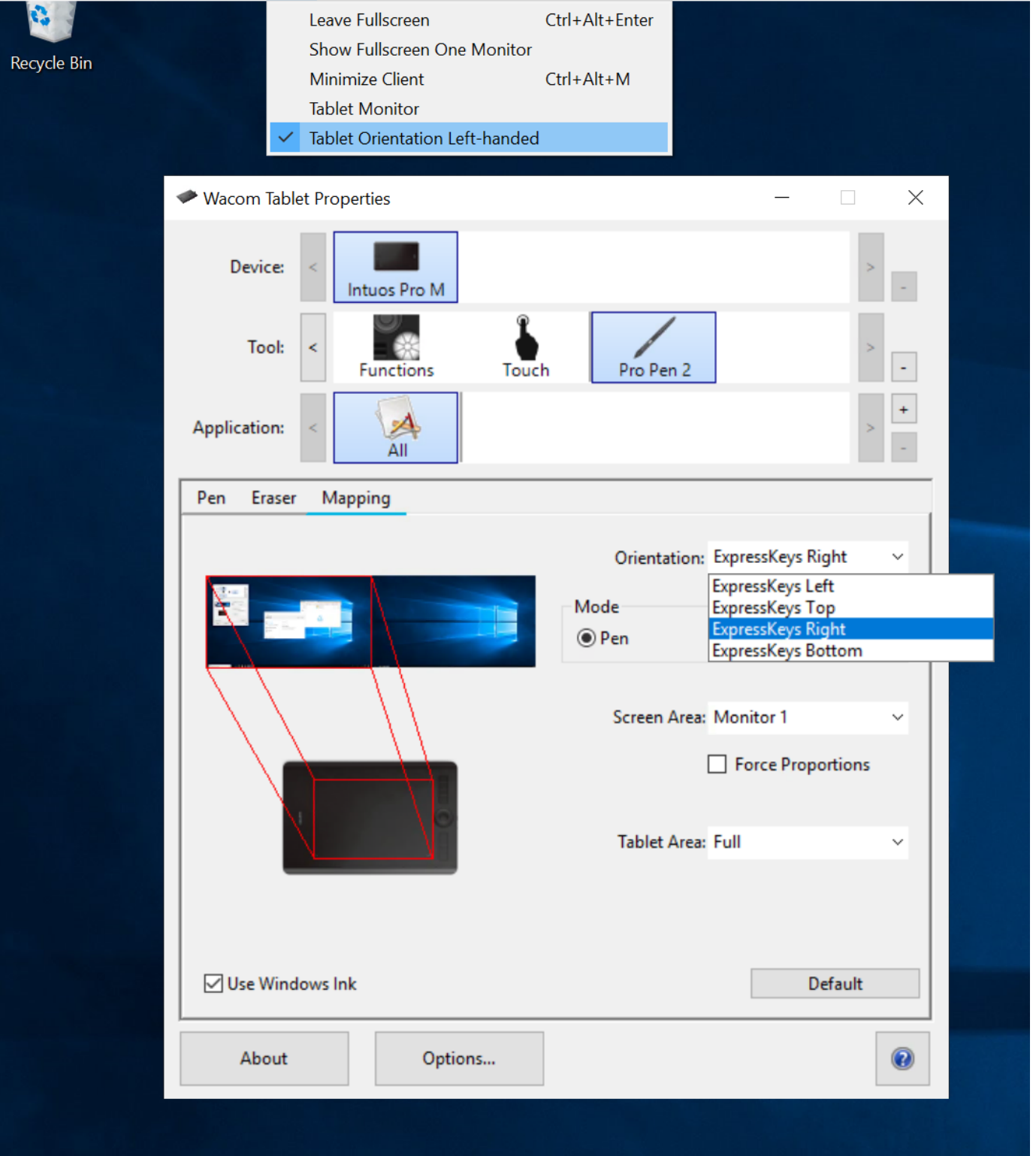
Tablet Orientation Left-handed

The left-handed orientation configures the tablet for a left-handed orientation. Select **ExpressKeys Right** for a left-handed orientation, and **ExpressKeys Left** for a right-handed orientation. Rotate the tablet to the desired orientation.

To configure Tablet Orientation:

1. Select **View** from the in-session options bar.
2. Check the **Tablet Orientation Left-handed** option.
3. Open **Wacom Tablet Properties** from the Wacom Desktop Center.
4. Select your device, tool and application.
5. Select your orientation from the dropdown menu.

Teradici PCoIP Client Connection View



Reset Virtual Desktop

The following section outlines how to reset a saved desktop in the PCoIP Client. You can reset to a virtual desktop by following the steps outlined below:

1. Click the configure button and select **Edit** from the popup menu. Alt Text
2. Click **NEXT** on the initial saved connection screen. Alt Text
3. Enter your access credentials and click **SAVE**. Alt Text
4. Click the configure button and select **Reset**. If the **Reset** option is not available, then this feature is not supported by the Connection Manager. Alt Text

Enhanced Audio and Video Synchronization

Enhanced Audio and Video Synchronization (AV Lock) provides improved full-screen video playback, reducing the difference in delays between the audio and video channels and smoothing frame playback on the client. This improves lip sync and reduces video frame drops for video playback.

This feature introduces a small lag in user interaction responsiveness when enabled. Using enhanced audio and video synchronization will reduce the maximum frame rate.

AV Lock is enabled on a per-display basis, so you can dedicate individual displays to playback without impacting responsiveness on the others.

To use AV Lock:

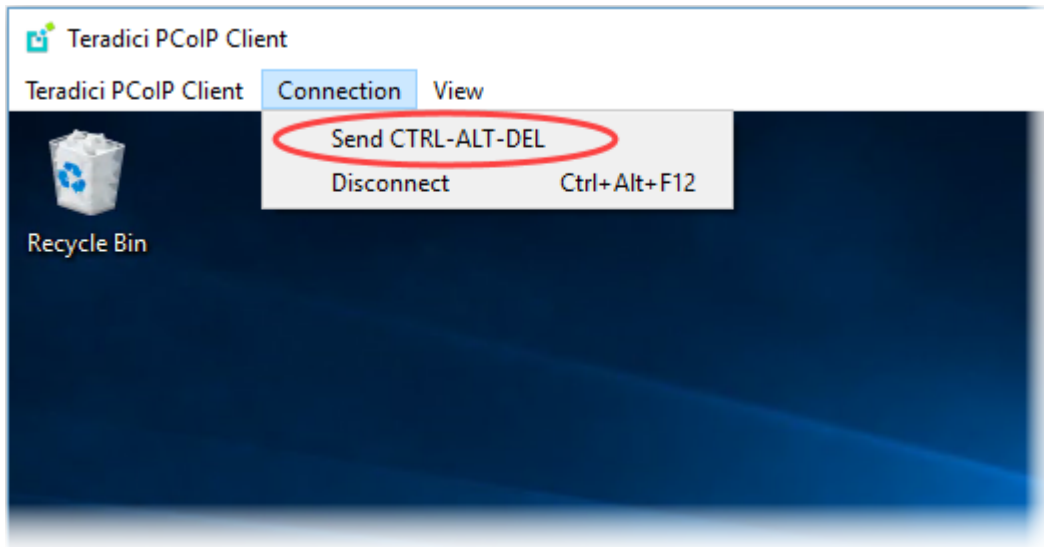
1. If you are in full-screen mode, reveal the menu bar on the display you want to enhance by moving the mouse cursor to the top of the screen.
2. On the display you want to enhance select **View>AV Lock** to toggle the enhanced sync mode.

Persistent Display Topology

The Enhanced Audio and Video Synchronization feature is persistent across sessions from the same client, provided that the display topology has not changed.

Sending a Ctrl-Alt-Del Command

To send the Ctrl-Alt-Del keyboard command to a remote workstation, select the **Connection > Send CTRL-ALT-DEL** menu option.



Configuring the PCoIP Software Client for Windows

The Software Client for Windows provides a number of configurable settings and behaviors, which allow the setting of user options, performance modes, and triggering actions like automated connections. These settings are not persistent and cannot be set via the user interface; they are set by launching the application using one of the methods described next.

To configure a client instance, you must launch it using one of these methods:

- [On the command line](#), with configuration values passed inline as flags, or
- [Via a URI](#), providing your configuration values in an encoded JWT string.

Setting Configuration Values on the Command Line

To set configuration values this way, launch the Software Client for Windows from a command prompt, and include the required options as flags. Multiple flags can be included in the same line. Use the following conventions when setting these parameters:

Type	Format
Boolean	No value is required; the flag implies "True"
Numeric	Provide the parameter and then the numeric value, separated by a space.
String	Provide the parameter and then the string value, separated by a space. Values can be wrapped in double quotation marks if they contain spaces.

The following example launches the client in full-screen mode, sets log level 3, and points to a connection broker at `broker.domain.com` (if your application is installed somewhere else, use your own path instead):

```
"c:\Program Files (x86)\Teradici\PCoIP Client\bin\pcoip_client.exe" --
connection-broker broker.domain.com --log-level 3 --full-screen
```

The available settings are shown [below](#).

Setting Configuration Values via a URI

Using this method, the Software Client for Windows is launched using a URI with configuration options (and, optionally, connection credentials) encoded in a [JWT token string](#).

To use this method, create a URI with the following structure:

```
pcoip://[broker]/connect[?data={jwt}]
```

Where each segment shown above is:

Segment	Description
<code>pcoip://</code>	Required. This scheme is registered with the operating system and will launch the Software Client for Windows.
<code>broker</code>	Optional. FQDN of the connection broker to use. If the connection is not brokered, this can be omitted.
<code>/connect</code>	Required. Requests a connection with the parameters defined in "?data"
<code>?data={jwt}</code>	Optional. The string indicated by {jwt} here is a JWT payload, containing any required configuration settings and connection credentials. If all you want to do is launch the client with no options set, this can be omitted.

The JWT payload can contain both credential information and client configuration. To create the JWT payload:

1. Create your configuration and credentials as a JSON object, using available [configuration parameters](#) and [authentication credentials](#).
2. Encode the object as a JWT token.
3. Pass the token through the URI as the `data` parameter.

For example, the following JSON object would launch the client in full-screen mode, with log level 3:

```
{
  "fullscreen": true,
  "log-level": 3
}
```

Encoded, and pointing to a connection broker at `broker.domain.com`, this would result in a URI similar to the following:

```
pcoip://broker.domain.com/connect?
data=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJmdWxsc2NyZWVuIjp0cnV1LCJsb2ctbGV2ZWwiC
```

The available settings are shown [below](#).

Configurable Settings

The following settings can be configured on the Software Client for Windows.

General Settings

These settings affect the client's behavior both in and out of PCoIP sessions.

Language

Sets the user interface language.

Caution: Localization is not available in this release

Localization has not been implemented in this version of the user interface, and will always display English text. This parameter is ignored.

Localization support will be implemented in a future release.

Options	Default	Type
English only in this release	Not set	string

Usage

Method	Valid	Full	Alias	Example
Command Line	✓	<code>--locale</code>	—	<code>--locale zh_CN</code>
URI	✓	<code>locale</code>	<code>loc</code>	<code>{loc: "zh_CN"}</code>

Connection Settings

These settings control how the Software Client for Windows connects to PCoIP sessions.

Connection Broker

The connection broker's URL.

Note that this parameter is used by the command line only; when using the URI method, the connection broker URL is part of the URI (not part of the configuration JWT payload).

Values	Default	Type
The URL for the connection broker, if present	—	string

Usage

Method	Valid	Full	Alias	Example
Command Line	✓	<code>--connection-broker</code>	<code>-b</code>	<code>-b broker.domain.com</code>
URI	—	—	—	—

Desktop

The name of the desktop to connect to.

Values	Default	Type
The name of a desktop to connect to	—	string

Usage

Method	Valid	Full	Alias	Example
Command Line	✓	<code>--desktop</code>	<code>-</code>	<code>--desktop myDesktop</code>
URI	✓	<code>desktop</code>	<code>vm</code>	<code>{vm: "myDesktop"}</code>

Domain

The domain to send to the connection broker.

Options	Default	Type
The name of the domain to provide to the connection broker.	<code>-</code>	string

Usage

Method	Valid	Full	Alias	Example
Command Line	✓	<code>--domain</code>	<code>-d</code>	<code>--domain domain.example.com</code>
URI	✓	<code>domain</code>	<code>dom</code>	<code>{dom: "domain.example.com"}</code>

Hard Host

If connecting to a PCoIP Remote Workstation Card (also known as a *hard host*), provide its URL using this parameter.

This option is ignored if the `connection-broker` url is provided.

Options	Default	Type
The URL for the Remote Workstation Card.	<code>-</code>	string

Usage

Method	Valid	Full	Alias	Example
Command Line	✓	<code>--hard-host</code>	<code>-h</code>	<code>-h rwc.example.com</code>
URI	—	—	—	—

Password

The password sent to the Connection Broker, for logging into a desktop. **Transmitting passwords this way is not recommended.**

 **Note: Command-line only**

Passwords can only be sent via the command line. You cannot send a password in a JWT payload.


Options	Default	Type
A string password.	Not set	string

Usage

Method	Valid	Full	Alias	Example
Command Line	✓	<code>--password</code>	<code>-p</code>	<code>-p mypassword</code>
URI	—	—	—	—

Security Mode

The security mode used for validating connections.

 **Note: This setting can be provided in the user interface**

This setting is available from the user interface, in addition to the methods described here. For details, see [PCoIP Software Client Security Modes](#).

Options	Default	Type
0 : Verification not required 1 : Warn, but allow 2 : Full verification required	1 : Warn, but allow	integer

Usage

Method	Valid	Full	Alias	Example
Command Line	✓	<code>--security-mode</code>	<code>-s</code>	<code>-s 2</code>
URI	✓	<code>security-mode</code>	<code>sec</code>	<code>{sec:2}</code>

Session ID

This setting launches the JSESSIONID. This parameter is only available via JWT; it cannot be used on the command line.

Options	Default	Type
The session ID to launch.	Not set	boolean

Usage

Method	Valid	Full	Alias	Example
Command Line	–	–	–	–
URI	✓	<code>sessionid</code>	<code>sid</code>	<code>{sid: exampleSessionID}</code>

Username

The username sent to the Connection Broker.

Options	Default	Type
The username to pass to the connection broker	Not set	string

Usage

Method	Valid	Full	Alias	Example
Command Line	✓	<code>--username</code>	<code>-u</code>	<code>-u myUsername</code>
URI	✓	<code>username</code>	<code>usr</code>	<code>{usr: "myUsername"}</code>

USB Settings

These settings control how USB devices connect to PCoIP sessions, including rules for which devices are allowed to be forwarded.

Disable USB

USB devices are available by default. Use this flag to disable USB connections. This will not prevent simple human input devices like mice or keyboards from connecting.

Options	Default	Type
<code>true</code> : disabled <code>false</code> : enabled	false (USB enabled)	boolean

Usage

Method	Valid	Full	Alias	Example
Command Line	✓	<code>--disable-usb</code>	<code>-</code>	<code>--disable-usb</code>
URI	✓	<code>disable-usb</code>	<code>nousb</code>	<code>{nousb: true}</code>

USB Auto-Forward

This setting auto-forwards all non-HID devices to the host.

Options	Default	Type
<code>True</code> : Auto-forward USB devices <code>False</code> : Do not auto-forward USB devices	False (do not auto-forward)	boolean

Usage

Method	Valid	Full	Alias	Example
Command Line	✓	<code>--usb-auto-forward</code>	—	<code>--usb-auto-forward</code>
URI	✓	<code>usb-auto-forward</code>	<code>uaf</code>	<code>{uaf: true}</code>

 **Note: This setting is available in the user interface**

This setting is also available in the client's pre-session user interface, by clicking the gear icon and selecting **USB Devices**.

Vidpid Auto-Forward

To auto-forward specific devices, provide their VID and PID values separated by a comma (,). Multiple values can be provided, separated by spaces. Enclose the list in quotation marks.

Options	Default	Type
The list of VID,PID values to auto-forward	Not set	string

Usage

Method	Valid	Full	Alias	Example
Command Line	✓	<code>--vidpid-auto-forward</code>	—	<code>--vidpid-auto-forward "aa11,bb22 cc33,dd44"</code>
URI	✓	<code>vidpid-auto-forward</code>	<code>vaf</code>	<code>{vaf: "aa11,bb22 cc33,dd44"}</code>

If you are not sure of the device's ID values, see [Identifying Vendor and Product IDs](#) for instructions.

Vidpid Black List

To block specific devices from auto-forwarding at all, provide their VID,PID values as a space-separated list using this parameter.

This setting overrides `usb-auto-forward` and the USB dialog in the client interface.

Options	Default	Type
The list of VID,PID values to block	Not set	string

Usage

Method	Valid	Full	Alias	Example
Command Line	✓	<code>--vidpid-black-list</code>	—	<code>--vidpid-black-list "aa11,bb22 cc33,dd44"</code>
URI	✓	<code>vidpid-black-list</code>	<code>vb1</code>	<code>{vb1: "aa11,bb22 cc33,dd44"}</code>

If you are not sure of the device's ID values, see [Identifying Vendor and Product IDs](#) for instructions.

Session Behavior Settings

These settings control the client's behavior once a session is connected.

Fullscreen Mode

Fullscreen mode enables the display topology to support multiple monitors as an extended desktop.

If both `fullscreen` and `windowed` parameters are sent, the client will launch in Windowed mode.

Options	Default	Type
<code>true</code> : full screen <code>false</code> : windowed	Not set (uses client's last-set mode)	boolean

Usage

Method	Valid	Full	Alias	Example
Command Line	✓	<code>--fullscreen</code>	<code>-f</code>	<code>-f</code>
URI	✓	<code>fullscreen</code>	<code>full</code>	<code>{full: true}</code>

Windowed Mode

Launches the client in windowed mode.

If both `fullscreen` and `windowed` parameters are sent, the client will launch in Windowed mode.

Options	Default	Type
<code>True</code> : Launch in windowed mode <code>False</code> : Do not request windowed mode	<code>False</code> (does not request windowed mode)	boolean

Usage

Method	Valid	Full	Alias	Example
Command Line	✓	<code>--windowed</code>	<code>-w</code>	<code>-w</code>

Method	Valid	Full	Alias	Example
URI	✓	windowed	win	{win: true}

Log Settings

These settings control logging functionality, including verbosity and file location.

Log Folder

A custom location for client log files.

Options	Default	Type
A valid system path to a folder	Not set	string

Usage

Method	Valid	Full	Alias	Example
Command Line	✓	--log-folder	—	--log-folder path/to/folder
URI	—	—	—	—

Log ID

A unique ID that will identify sessions in all PCoIP log files (including those created by other components like agents and a connection manager).

Options	Default	Type
A unique session identifier	Not set	string

Usage

Method	Valid	Full	Alias	Example
Command Line	✓	<code>--log-id</code>	—	<code>--log-id abcde1234</code>
URI	—	—	—	—

Log Level

Sets the log level. This parameter will override any existing configuration values.

Options	Default	Type
0 : Critical 1 : Error 2 : Info 3 : Debug 4 : Verbose	Not set	integer

Usage

Method	Valid	Full	Alias	Example
Command Line	✓	<code>--log-level</code>	<code>-l</code>	<code>-l 2</code>
URI	✓	<code>log-level</code>	<code>logl</code>	<code>{logl:2}</code>

 **Note: This setting is available in the user interface**

This setting is also available in the client's pre-session user interface, by clicking the gear icon and selecting **Logs**.

Log Prefix

A user-defined prefix for log files. This value will be prepended to the timestamp in the log file name, like this:

```
<log-prefix value><timestamp>
```

Log files are saved in the location provided by `log-folder`.

Options	Default	Type
A prefix to use in generated log file names	Not set	string

Usage

Method	Valid	Full	Alias	Example
Command Line	✓	<code>--log-prefix</code>	—	<code>--log-prefix example-prefix</code>
URI	—	—	—	—

Advanced Settings

Caution: General use of these settings is not recommended

These settings are intended for specific use cases, and can drastically alter the behavior of the Software Client for Windows. Unless you understand what these settings do, and have a clear need to use them, they should be avoided.

Disable Hotkeys

Session convenience hot keys, such as `Ctrl + Delete + F12` (which disconnects a PCoIP session) are available to users by default. Use this flag to disable all hotkeys.

Options	Default	Type
<code>true</code> : disabled <code>false</code> : enabled	false (hotkeys enabled)	boolean

Usage

Method	Valid	Full	Alias	Example
Command Line	✓	<code>--disable-hotkeys</code>	—	<code>--disable-hotkeys</code>
URI	✓	<code>disable-hotkeys</code>	<code>nohot</code>	<code>{nohot: true}</code>

Disable Menu Bar

The PCoIP client menu bar is available to users by default. Use this flag to disable the menu bar, preventing users from accessing it or executing any of its functionality.

Options	Default	Type
<code>true</code> : disabled <code>false</code> : enabled	false (menu bar enabled)	boolean

Usage

Method	Valid	Full	Alias	Example
Command Line	✓	<code>--disable-menubar</code>	—	<code>--disable-menubar</code>
URI	✓	<code>disable-menubar</code>	<code>nomenu</code>	<code>{nomenu: true}</code>

Enable Scaling

This setting enables scaling on the PCoIP Client without having to specify the desktop resolution. This can only be configured on a single display. This is off by default.

Options	Default	Type
<code>true</code> : scaling enabled <code>false</code> : scaling disabled	false (scaling disabled)	boolean

Usage

Method	Valid	Full	Alias	Example
Command Line	✓	<code>--enable-scaling</code>	—	<code>--enable-scaling</code>
URI	✓	<code>enable-scaling</code>	<code>scale</code>	<code>{scale: true}</code>

Force Native Resolution

This setting sets the resolution of the Client monitor to the native resolution when the session client is launched. This can only be configured on a single display.

 **Note: Windows client only**

This parameter is only available on Windows clients. It will have no effect if provided to a Linux or macOS client.

Options	Default	Type
<code>true</code> : force enabled <code>false</code> : force disabled	false (Resolution force disabled)	boolean

Usage

Method	Valid	Full	Alias	Example
Command Line	✓	<code>--force-native-resolution</code>	—	<code>--force-native-resolution</code>
URI	✓	<code>force-native-resolution</code>	<code>native</code>	<code>{native: true}</code>

Maintain Aspect Ratio

This setting maintains the display aspect ratio between the host and the Client. Maintaining the aspect ratio in this way can result in letterboxing if the two devices are naturally different.

This can only be configured on a single display.

Options	Default	Type
<code>true</code> : Maintain aspect ratio <code>false</code> : Do not maintain aspect ratio	False (does not maintain aspect ratio)	boolean

Usage

Method	Valid	Full	Alias	Example
Command Line	✓	<code>--maintan-aspect-ratio</code>	—	<code>--maintain-aspect-ratio</code>
URI	✓	<code>maintain-aspect-ratio</code>	<code>aspect</code>	<code>{aspect: true}</code>

Quit After Disconnect

If this is enabled, disconnecting from the PCoIP session will immediately quit the `{! ./_common/name.md! }`. The pre-session interface will not be available after disconnecting.

Options	Default	Type
<code>True</code> : Quit on disconnect	False (does not quit on disconnect)	string
<code>False</code> : Do not quit, show pre-session UI on disconnect		

Usage

Method	Valid	Full	Alias	Example
Command Line	✓	<code>--quit-after-disconnect</code>	—	<code>--quit-after-disconnect</code>
URI	✓	<code>quit-after-disconnect</code>	<code>qad</code>	<code>{qad: true}</code>

Set Host Resolution

This setting locks the resolution of your host application display.

Provide the value as a string, made up of the *horizontal resolution*, the letter "x", and the *vertical resolution*. For example, "1024x768".

This can only be configured on a single display.

Options	Default	Type
A fixed resolution the host must use.	Not set	string

Usage

Method	Valid	Full	Alias	Example
Command Line	✓	<code>--set-host-resolution</code>	—	<code>--set-host-resolution 1024x768</code>
URI	✓	<code>set-host-resolution</code>	<code>res</code>	<code>{res: "1024x768"}</code>

Preventing Devices From Using Local Termination

By default, supported Wacom devices use **local termination** automatically to provide improved responsiveness and tolerance of high-latency networks. Local Termination does not support all advanced Wacom features; if you depend on one of these unsupported features, you can fall back to **bridged** mode by adding your device to a blacklist. This will pass all tablet data to the remote host for processing, which will make the full suite of functionality available at the cost of decreased performance and sensitivity to latency.

To add a device to the local termination blacklist, open `%APPDATA%\Teradici\Teradici PCoIP Client.ini` in a text editor, then add the `localtermination_black_list` setting and the VID/PID pairs for the devices you want to limit:

```
localtermination_black_list "<vid1>,<pid1> <vid2>,<pid2> ..."
```

...where `<vid1>,<pid1> <vid2>,<pid2>` are VID/PID pairs of the devices you are blacklisting.

If you do not know the Vendor ID and Product ID for the device you want to blacklist, use the method shown in [Identifying Vendor and Product IDs](#).

Troubleshooting HID Local Termination Blacklist

There is no user-facing indication of which mode a device is using to connect. If you are troubleshooting a connection and need to understand which mode is being used, inspect the PCoIP agent logs for a session. If the device is using local termination, you will see lines similar to these:

```
pcoip server log: `LVL:2 RC: 0 MGMT_KMP :Client added HoIP device (id:0x000a0005)
with vendor id=0x056a, product id=0x0391`
pcoip client log: `LVL:2 RC: 0 MGMT_USB :HoIP supported device detected (Vid:
0x056a, Pid: 0x0391), using HoIP protocol for local termination'
```

PCoIP Software Client Security Modes

The PCoIP Software Client uses certificates to verify the identity of the host to which it connects. The security mode is configured by the `security_mode` setting in the **Teradici PCoIP Client** configuration file *or* by setting its value in the pre-session user interface.

Three security mode options are available:

Level	Setting value	Description
High	2	Full verification is required; users cannot connect unless a certificate can be verified.
Medium	1	Warn but allow (default). If the certificate cannot be verified, warn the user, but allow them to connect.
Low	0	Always allow; verification is not required.

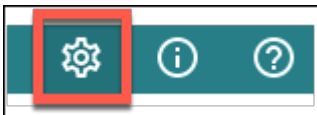
PCoIP sessions are always encrypted

Your PCoIP session is still encrypted and secure if you connect with security mode 0 or 1. The red padlock icon indicates that the certificate presented by the host is not signed by a trusted certificate authority in the client's certificate store, not that the session is insecure.

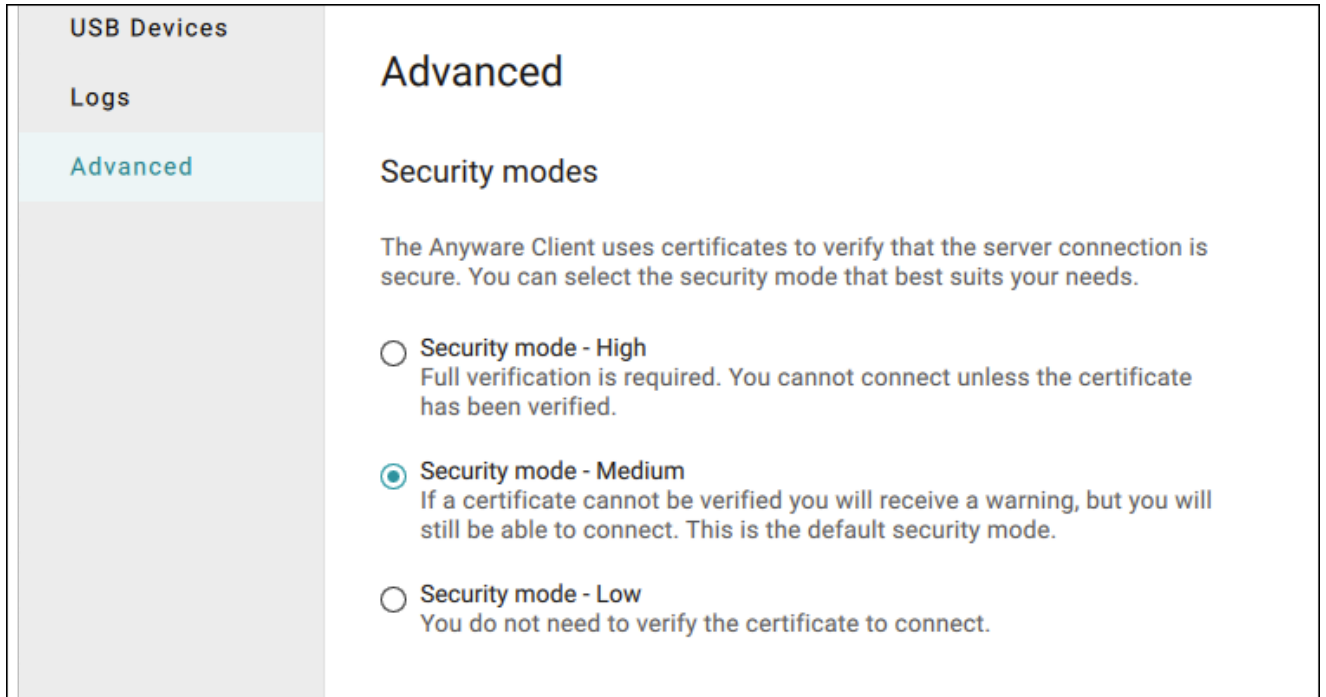
Setting the Security Mode

To set the security mode using the pre-session interface:

1. Disconnect any active PCoIP sessions and return to the pre-session interface.
2. Click the gear icon to open the settings window:



3. Click **Advanced** in the left side menu, and find **Security Modes** in the right panel.
4. Select the desired security mode.



To set the security mode programmatically:

1. Open `%appdata%\Teradici\Teradici PCoIP Client.ini` in a text editor.
2. Add a line that specifies the `security_mode` and sets the level:

```
security_mode = <value>
```

...where `<value>` is the integer corresponding to the desired security level (0, 1, or 2).

3. Save the file and close the editor.

Installing the Internal Root CA Certificate in a PCoIP Client

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

Installing Root CA Certificates in the PCoIP Software Client for Windows

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 PCoIP Software Client.

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.

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 PCoIP Software Client for Windows:

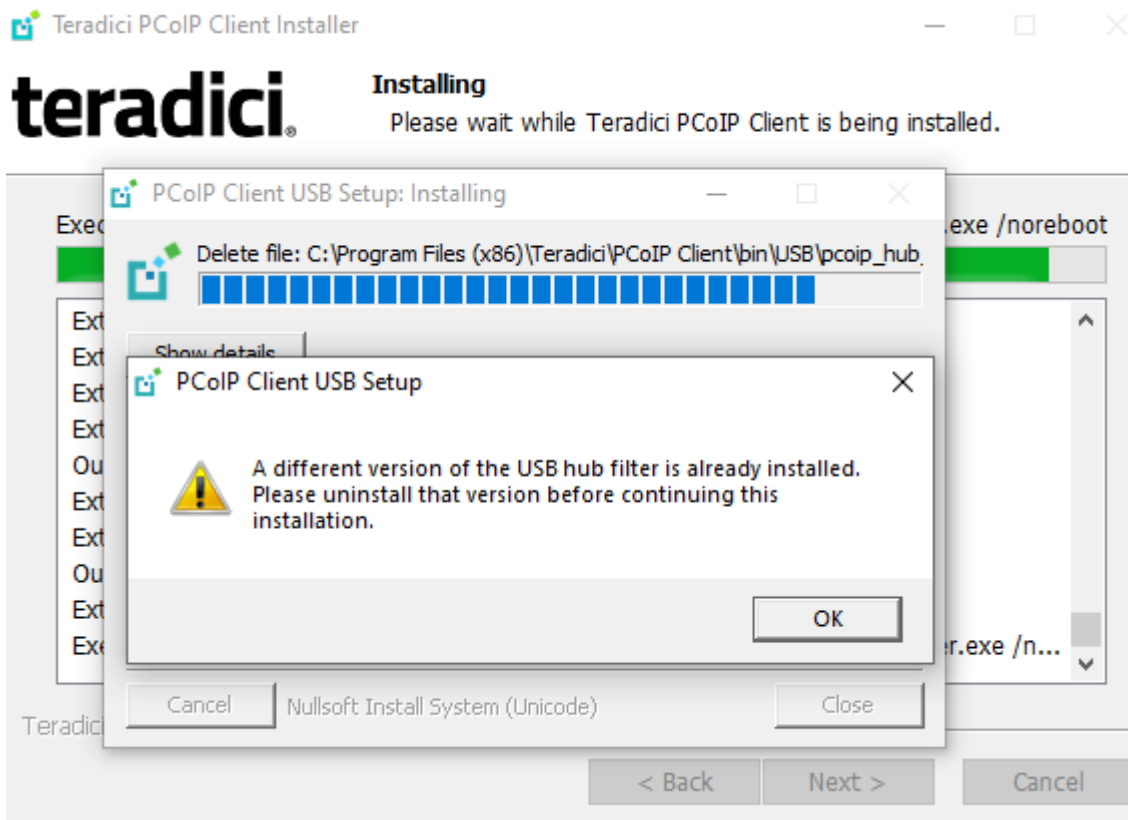
1. Copy your root CA certificate file (*.crt) to a directory reachable by your Windows client.
2. Open the Microsoft Management Console on the agent machine:
 - a. Press **Win+R** to open the run dialog
 - b. type **mmc** and press **Enter**.

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.

Recovering a USB Driver with the PCoIP Software Client

When using USB drivers on the PCoIP Software Client for Windows you can sometimes encounter issues around versioning of the USB hub filter, as displayed in the error message below:

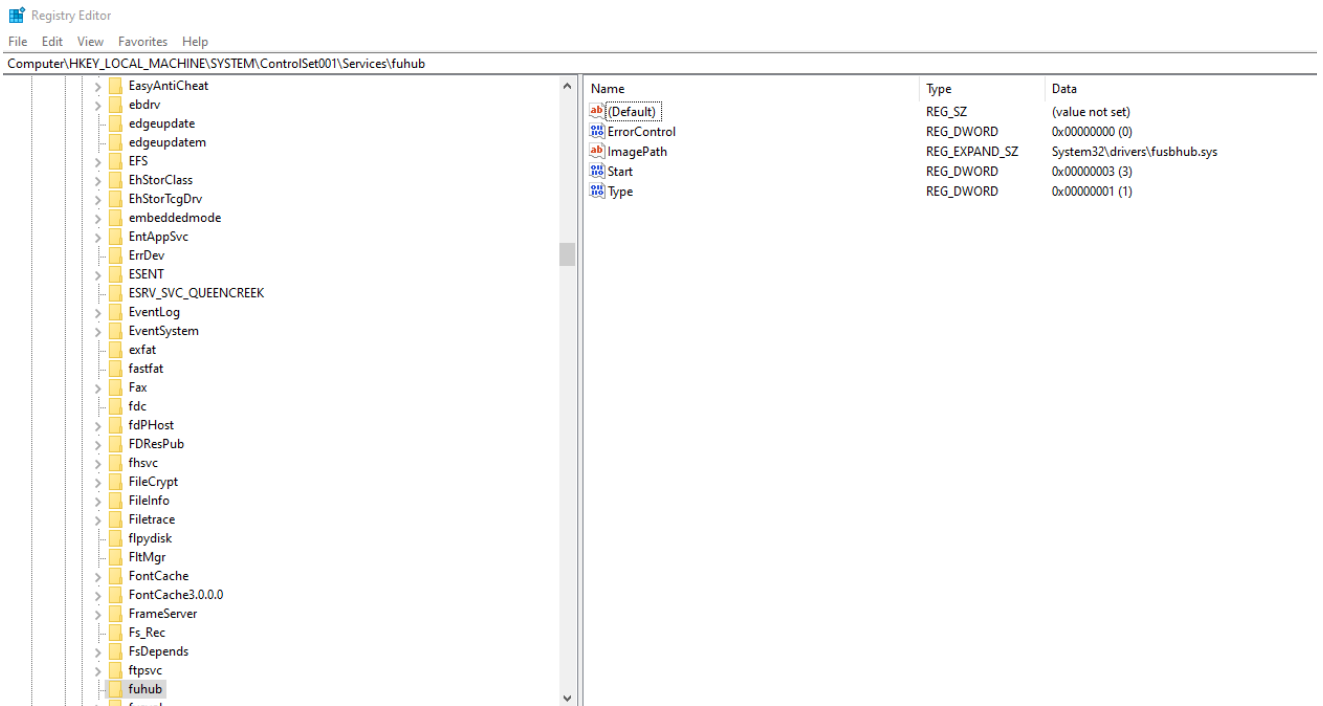


If you encounter this issue or another issue relating to your USB driver, Teradici recommends carrying out the following steps:

1. Uninstall the PCoIP Client.
2. Reboot your machine.
3. Open the **Registry Editor** editor.

4. Search for **fuhub** under HKLM. The file path is

Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\fuhub.



5. Remove the registry key which is the item in the left pane with the folder icon, in this case it is the **fuhub** key, containing **fusbhub**. If you cannot remove this registry key note the .inf file name associated with the registry entry. The .inf file name usually starts with oem, for example ***oem9.inf***. Open the commandline and run the following prompt:

```
pnputil -f -d oem9.inf
```

- Keep repeating step 5 until **fusbhub** is completely removed from the registry editor.
- Reboot your machine.
- Install the PCoIP Client.

Setting Configuration Values via Config files

Certain advanced configuration values are set via configuration files, rather than via the user interface, command line, or URI methods. These files are read and implemented by the Software Client for Windows when it launches.

Configuration files can be saved in a **system-scoped** location, for settings that should apply to any PCoIP client launched on a device, or a **user-scoped** location, for settings that should apply to specific users. **If a setting is found at both levels, the system scope takes precedence.**

Configuration files do not exist until a user changes a persistent setting via the user interface. If that has not occurred, you must create the file, either manually or using a deployment script.

Config File Syntax

The .ini file starts with a `[General]` group followed by a series of `<key>=<value>` pairs, each on its own line. For example, the following file would add the USB device identified by the VID/PID pair `18a5,0302` to the local termination blacklist, causing it to revert to **bridged** connections:

```
[General]
localtermination_black_list="18a5,0302"
```

Config File Locations

Depending on the desired scope, save the `.ini` file in one (or both) of these locations. Remember that the system-scoped file takes precedence over the user-scoped file:

Scope	Location
System	%PROGRAMDATA%\Teradici\Teradici PCoIP Client.ini
User	%APPDATA%\Teradici\Teradici PCoIP Client.ini

Support and Troubleshooting

If you encounter a problem installing or using the Software Client for Windows, there are a number of troubleshooting and support resources you can access.

- We maintain an extensive **knowledge base** which answers many questions and documents solutions to common problems. The knowledge base is part of the [Knowledge Center](#); click on the **Articles** tab to access it, or enter a search query in the search field at the top of the page.
- We host a **community forum**, allowing you to ask questions and get answers from other IT professionals and our support team, which monitors this channel. The forum is part of the [Knowledge Center](#); click on the **Discussions** tab to access it.
- If you need more help, open a [support ticket](#) and our support team will engage with you directly.

Creating a Support Bundle

Our support team may request a support bundle from you. The support file is an archive containing logs, diagnostic data, and system information that helps the team diagnose problems.

To create a support file using Windows:

1. From the Windows start menu, select **PCoIP Client Support Bundler**.
2. Run the bundler as an administrator.
3. Click **Yes** if the User Account Control panel appears.

To create a support file using PowerShell:

1. Open a PowerShell command prompt.
2. Set the PowerShell execution policy to enable the script to run:

```
Set-ExecutionPolicy -Scope Process -ExecutionPolicy Bypass
```

3. Launch the support bundler:

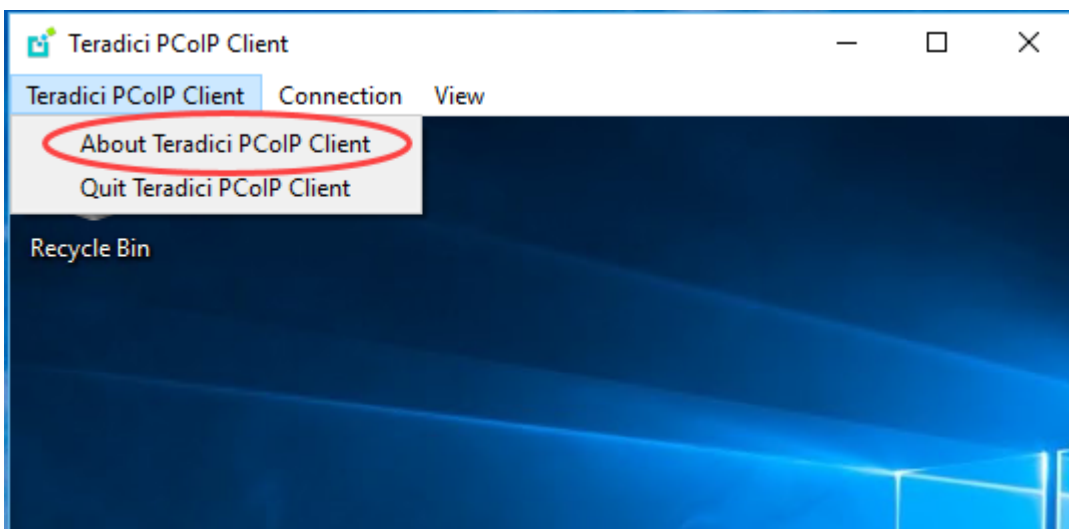
```
& 'C:\Program Files (x86)\Teradici\PCoIP Client\bin\pcoip-client-support-bundler.ps1'
```

The support file will be created and placed in `$env:ProgramData\Teradici\Support\`. A new File Explorer window will open with the generated support file selected.

Finding Your Client Version

You can find your Software Client for Windows version number from the pre-session interface, or, if you're already in a session, from the client menu bar.

- **Pre-session:** If you are not in a session:
 - Click on the hamburger icon, found at the bottom left of the screen beside the *Cancel* button.
 - Alt Text
 - From the context menu that appears, select **About**.
 - Find the version number in the information window that appears.
- **In-session:** If you *are* in a session:
 - Find or reveal the client menu bar
 - Select **Anyware PCoIP Client > About Anyware PCoIP Client**.
 - Find the version number in the information window that appears.



PCoIP Client Logging

The Software Client for Windows writes log files that document its processes and interactions with other services such as brokers and agents. These files are invaluable in diagnosing problems. This page describes how logs are handled and where they can be found.

Log Location

Client logs are placed in `%localappdata%\Teradici\PCoIPClient\logs` by default. Log locations can be overridden via [launch configuration](#) if required.

`<Username>` is the name of the user that launched the client.

Log Levels

Log verbosity is defined by a level, represented by an integer from 0 to 3:

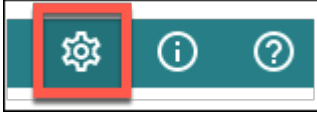
Level	Description
0	Critical messages only
1	Error messages and higher
2	Info messages and higher (default)
3	Debug messages and higher

The default setting is `2`, recording informational messages and higher.

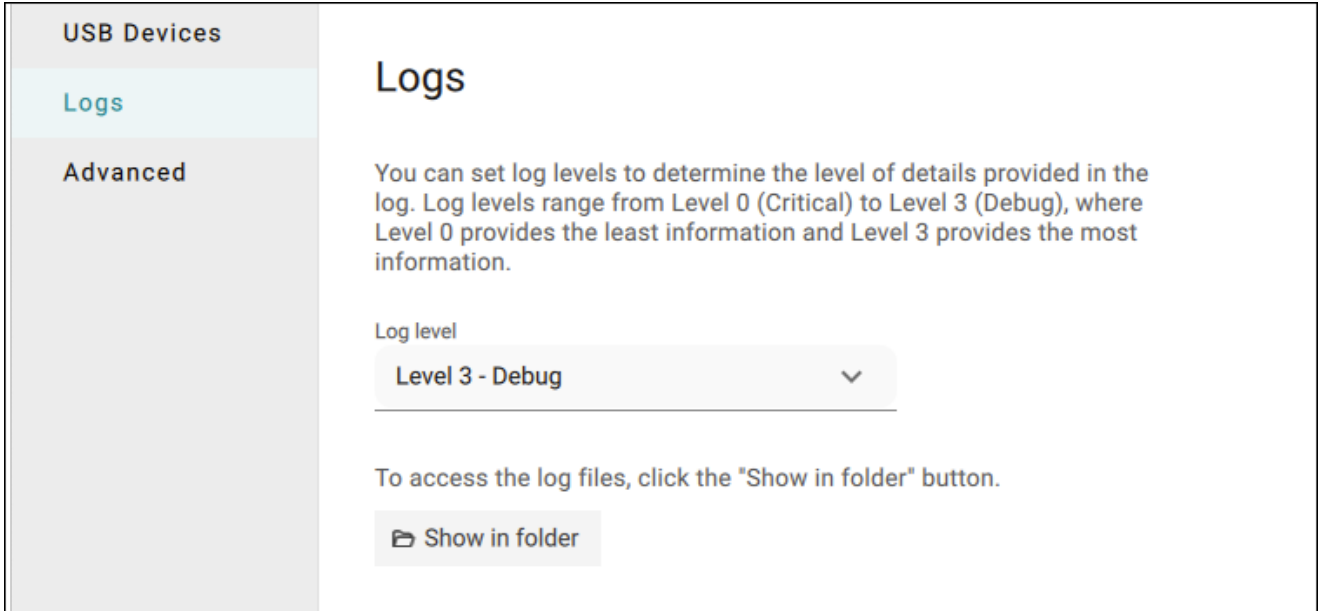
The log level can be changed in any of the following ways:

To set the log level in the pre-session interface:

1. Disconnect any active PCoIP sessions and return to the pre-session interface.
2. Click the gear icon to open the settings window:



3. Click **Logs** in the left side menu, and specify the desired log level in the panel.



To set the log level programmatically:

This method provides the log level inline during a command line launch; see [Log Level](#) in the configuration section for details.

Tip: Reporting issues to support

When you are reporting an issue to support, set the log level to 3 (debug) first, and then reproduce the issue and create a support bundle. This will capture much more detail than the default setting, making diagnostics more effective.

Log Session IDs

The Software Client for Windows creates a unique session ID when a new session is established, and distributes that ID to all components in the system. When PCoIP components generate log messages, they are prefixed by this unique session ID, allowing administrators and support to easily group events by session across multiple components:

```
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.

This session ID can be overridden by providing a custom string during a command line launch; see [Log ID](#) in the configuration section for details.