

PCoIP Software Client for Linux Administrators' Guide

24.03

Table of Contents

Anywhere Software Client for Linux	7
Who Should Read This Guide?	7
Additional Documentation	7
What's New in This Release	9
Simplified Update Experience Ensures that Clients Are Always Up to date	9
Alternative Approach Ensures Added Security While Launching Anyware Client	9
Smart Cards Authentication for Enhanced Security	10
System Requirements	11
Hardware System Requirements	11
Feature Support	12
Audio Support	12
Client Modes	13
High Performance Mode	13
Standard Mode	13
High Performance (Legacy) Mode	13
Selecting a Client Mode	14
Collaboration	15
Collaboration Requirements	15
Enabling Collaboration	16
Sharing Your Session With Collaborators	16
Joining a Collaboration Session	29
Anywhere Connection Health	31
Connection Health Status	32
Network Connection Indicator	32
Measured Statistics	33
Displays	34

Language Support	35
Changing the Software Client for Linux Display Language	35
PCoIP Ultra	37
PCoIP Ultra Modes	37
Setting PCoIP Ultra	38
Printing Support	40
Relative Mouse Support	42
Enabling Relative Mouse	43
USB	44
USB Support	44
Bloomberg Keyboard Support	45
Tangent Panel Support	49
Wacom Tablet Support	50
Webcam Support	56
Console Game Controller Support	58
Smart Cards	59
Supported Smart Cards	59
Installation	63
Prerequisites for Installing the Software Client for Linux	63
Installing the Anyware Software Client for Linux	64
Installing the Software Client in Silent Mode	64
Kernel Network Configuration	65
Downloading the Anyware Client Update	66
Upgrading the Anyware Software Client	67
Upgrading the Anyware Software Client in Silent Mode	67
Uninstalling the Anyware Software Client	68
Uninstallation Steps	68
Removing Deprecated Repos	68

Connecting	70
Connecting to an Agent Machine	70
Creating Your First Connection	70
Connecting to a Session	73
Managing Connections	76
Managing Desktops	77
Using Smart Card Authentication to Connect to a Session	82
Preparing for Remote Workstation Card Connections	88
Initial Workstation Configuration	88
Disconnecting a Session	91
In-session actions	92
Using Displays	92
Display Modes	92
Adding or Removing Displays	94
Detecting Monitors	94
Connecting USB Devices	96
Important considerations	96
Connect a USB Device	97
Disconnect a USB Device	98
Automatically Forward All USB Devices	99
Automatically Forward Devices by Vendor ID/Product ID	100
Connect USB Webcams	102
Configuring Wacom Tablets	103
Wacom Tablet Monitor	103
Enhanced Audio and Video Synchronization	107
PCoIP Ultra AV-Lock	107
Sending a Ctrl-Alt-Del Command	108

Configuration Guide	109
Configuring the Anyware Software Client for Linux	109
Setting Configuration Values on the Command Line	109
Setting Configuration Values via a URI	110
Setting Configuration Values via Config files	111
Config File Syntax	111
Config File Location	111
Configurable Settings	112
Securely Passing Parameters via the Command Line	126
JSON String Format	126
HID Local Termination Blacklist	128
H.264 Hardware Decode	129
Enabling Hardware Decoding	129
Security Guide	130
Anyware Software Client Security Modes	130
Setting the Security Mode	130
System Libraries	132
Installing the Internal Root CA Certificate on an Anyware Client for Linux	133
Installing a Root Certificate on Ubuntu and Debian	133
Reference	134
Azure Virtual Desktop Keyboard Shortcuts	134
Disabling the Virtual Terminal Functionality	135
Disabling the Super Key	136
Linux Keyboard Shortcuts	137
Troubleshooting and Support	140
Support and Troubleshooting	140
Creating a Support Bundle	140
Finding Your Client Version	141
Finding Your Client Version	141

Anyware Client Logging	143
Log Location	143
Log Levels	143
Setting the Log Level in the Pre-session Interface	144
Setting the Log Level Programmatically	144

Anyware Software Client for Linux

Welcome to the Software Client for Linux Administrators' Guide.

Anyware Software Clients are applications that establish PCoIP sessions with remote Windows, Linux, or macOS desktops. Connections can be made to Anyware 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 Linux. 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 Linux.

Additional Documentation

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

For more information about HP Anyware, including detailed information on included Anyware components as well as HP Anyware plans, see the Cloud Access Architecture Guide.

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

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

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

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

What's New in This Release

Release 24.03 of the Software Client for Linux includes:

Simplified Update Experience Ensures that Clients Are Always Up to date

Version 24.03 introduces a simplified experience for updating Anyware clients. Clients are now equipped to check for new updates and send notifications that appear as banners if an update is available. Clicking the banner redirects to the product download page, from where users can download the client installer.

This allows users to access the newest client version with new features and improvements with minimal intervention. For more information, see [Downloading the Linux Update](#).

Alternative Approach Ensures Added Security While Launching Anyware Client

When invoking the Anyware Client via the Command Line, the command line parameters can be viewed in the shell history or process list. To prevent this, the ability to protect sensitive parameter values while launching has been introduced in Anyware Client 24.03.

This is accomplished with the new `--ask-extra-args-as-json` parameter, which enables the user to pass parameter values to the `pcoip-client` process via Standard Input. With this new approach, sensitive parameter values are not stored in the shell history or process list, thereby ensuring enhanced security while launching the client. For more information, see [Securely Passing Parameters via the Command Line](#).

Smart Cards Authentication for Enhanced Security

Version 24.03 of the Linux Client introduces support smart card authentication. Linux client machines can now connect to Windows agents using smart cards for authentication and SSO (single sign-on). Additionally, Linux clients can read and process smart card information for in-session tasks such as document signing.

Smart card authentication not only adds a layer of security, but also ensures simplified identity management while accessing PCoIP deployments. For information on supported smart cards and readers, see [Supported Smart Cards & Readers](#). To know how to connect to Windows agents using smart card authentication, see "Using Smart Card Authentication to Connect to a Session" in the [Using a Smart Card to Authenticate a Connection](#) topic.

Note: Supported Deployments

Smart card authentication is only supported in deployments where Linux clients connect to Windows Standard agents or Windows Graphics agents.

System Requirements

The following table outlines the system requirements for the Anyware Software Client for Linux:

System	Version Required
Anyware Software Client Operating System	<ul style="list-style-type: none">• Ubuntu 20.04• Ubuntu 22.04
Compatible Anyware Agents	<p>The Software Client for Linux can connect to any Anyware agent. Some features require specific agent versions; see the <i>Feature Support</i> section of this guide for details.</p> <p>We recommend always using the same version of Anyware agent and Anyware client.</p>
Compatible Remote Workstation Cards ¹	TERA22x0 with firmware 20.04+ and Remote Workstation Card Software for Windows or Linux 20.04+.
Supported IP versions	IPv4 and IPV6.

Note: h264 Hardware Decode

The Software Client for Linux supports h264 hardware decode under limited conditions; see [H.264 Hardware Decode](#) for more information.

Hardware System Requirements

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

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

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

Feature Support

Audio Support

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

The Anyware 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 Linux supports multiple performance modes to suit different types of workloads. Performance modes are described next. To change the client mode, see [Selecting a Client Mode](#) below.

High Performance Mode

High Performance (recommended) mode delivers high frame rates and synchronized audio, resulting in smoother images and video streaming. This mode is suitable for demanding applications such as 3D modelling and visual effects software.

This mode is enabled by default and is recommended for most users.

Standard Mode

Standard performance provides consistent performance at moderate framerates. This mode is suitable for task workers using low-demand applications such as browsers and Microsoft Office applications.

High Performance (Legacy) Mode

 **Caution: High performance (legacy) mode is deprecated**

This mode is deprecated, and will be removed in a future release. New users should use the **High Performance** mode instead.

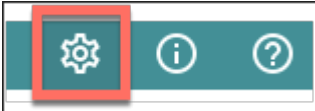
High performance (legacy) mode is an earlier implementation of the high performance client. Unless your workflow specifically requires this mode, you should switch to *High Performance* mode.

Selecting a Client Mode

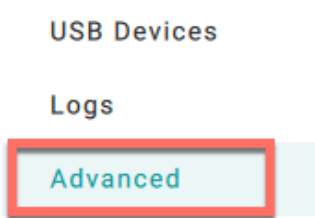
Changes to the client mode take effect when the next session starts, and persist until changed again.

To change client modes:

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



3. In the side navigation panel, click **Advanced**, then choose your preferred mode in the **Performance mode** section.



- Security mode - Medium
If the certificate cannot be verified, you will get a warning, but can still connect.
- Security mode - Low
No certificate verification required to connect.

Performance mode

Select a preferred performance mode for your PCoIP Client.

- Standard performance
Provides consistent performance at moderate frame rates. Suitable for software with low performance requirements, such as task workers, web browsers, or Microsoft Office applications.
- High performance (Recommended)
Provides high frame rates and audio synchronization, resulting in smoother images and videos. Suitable for software such as 3D modelling and visual effects.
- High performance (Legacy)
This mode will be deprecated in the future and replaced by high performance mode.

4. Close the settings window.

Collaboration

PCoIP Ultra Collaboration enables a PCoIP session user to share their session with multiple remote collaborators using Anyware Software Clients.

Note: Collaboration terminology

When discussing this feature, we'll refer to the first user as the *session owner*, and subsequent users who join the session as *collaborators*. The session owner's screens, audio, and input devices (if allowed) are shared with the collaborators when they join the session.

Up to 5 collaborators can join an ongoing PCoIP session using the same invitation.

While connected, all collaborators can view and hear the session owner's screens and audio, and see the controlling collaborator's mouse movements. If permitted by the session owner, they can also share control of the session owner's keyboard and mouse using [input control](#).

During a collaboration session, *all* of the session owner's desktop screens may be shared depending on the session owner's Anyware software client display settings. See [Understanding Display Behavior](#) for more information.

Collaboration Requirements

PCoIP Ultra Collaboration is supported by all Anyware agents. Anyware software clients that support PCoIP Ultra can participate in collaboration sessions (all Anyware software clients 23.04 and higher meet this requirement).

Some collaboration features have specific version requirements for Anyware agents and Anyware software clients; [these are noted below](#).

Note: Only Anyware Software Clients are supported

Anyware Tera2 Zero Clients and mobile clients do not support PCoIP Ultra and cannot join collaboration sessions.

Feature Version Requirements

PCoIP Ultra Collaboration features depend on coordinated updates in Anyware agents and Anyware clients, so review these requirements carefully to ensure the features you need are supported by your system. **We strongly recommend using the latest versions of both Anyware agent and Anyware client.**

Feature	Required versions	Notes
Collaborate menu	Anyware agent 23.06+ Anyware client 23.06+	Both client and agent must be 23.06 or higher, with Collaboration and PCoIP Ultra enabled.
Multiple collaborators	Anyware agent 23.04+ Anyware client 23.04+	HP Anyware versions 22.07–23.01 supported single collaborators only.
Input control	Anyware agent 23.01+ Anyware client 23.01+	See Input Control for more information.
Mouse visibility	Anyware agent 22.07+ Anyware client 22.07+	Session owner and collaborator software clients must be in <i>standard client mode</i> for mouse visibility to work.

Enabling Collaboration

PCoIP Ultra Collaboration is enabled and configured on the Session Owner's desktop. Refer to the following documentation, depending on the Anyware agent you are connecting to:

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

Collaboration is disabled by default. The following instructions will not work until Collaboration is enabled on the session owner's Anyware agent as described in the guides above.

Sharing Your Session With Collaborators

You can invite up to 5 collaborators to participate in your session, and optionally allow them to control your desktop.

 **Important: Anyware Client steps**

Collaboration sessions are shared from Anyware clients in established PCoIP sessions. Make sure the software client version you are using supports the collaboration features you expect. For details, see [Feature Version Requirements](#).

Collaboration sessions are managed using the **Collaboration manager**. The collaboration manager shows you who is connected to your session, whether each collaborators can view or control the session, and allows you to invite new collaborators or stop collaborating.

 **Note: New Collaboration Manager menu option**

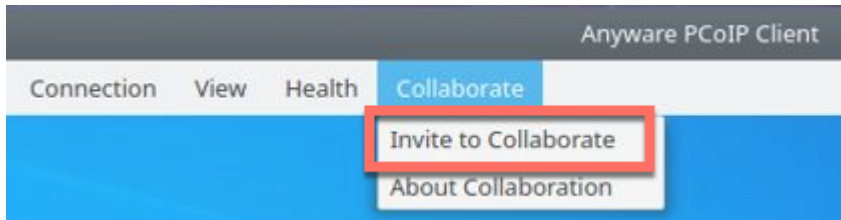
The Collaboration manager can now be launched by using the client's in-session menu, in addition to the system menu bar.

To launch the Collaboration Manager:

1. Connect to a PCoIP session with PCoIP Ultra and Collaboration enabled.

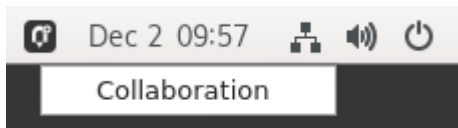
2. From the remote session, open the **Collaboration Manager** using either of these methods:

- **From the in-session menu:** From the in-session menu, select **Collaborate > Invite to Collaborate**.



The Collaborate menu appears if both the Anyware agent and Anyware client are version 23.06 and higher, and if both support Collaboration. If the Collaborate menu does not appear, open the Collaboration Manager using the menu bar instead.

- **From the menu bar:** by clicking the **Anyware Collaboration** icon in the menu bar:



This example shows a Linux desktop; yours may vary depending on which operating system you are connecting to.

To invite collaborators, the session owner generates a *collaboration invitation* using the collaboration manager, and distributes the invitation to all collaborators.

About Collaboration Invitations

Collaboration invitations are created by the session owner and distributed to collaborators, who use them to join an established collaboration session.

Note: About collaboration invitations

A single collaboration invitation can be used by multiple collaborators (up to the maximum number configured). You do not need to generate a new invitation for each collaborator.

Collaboration invitations behave as follows:

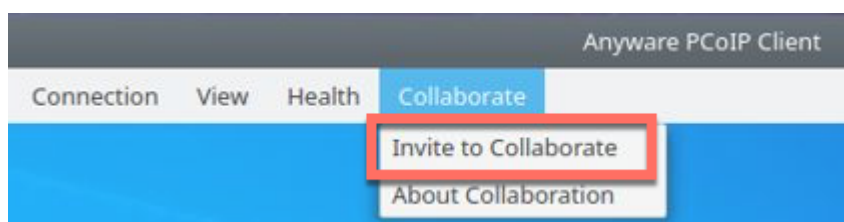
- If an invitation is generated but no collaborators connect within one hour, it expires and can no longer be used. If this happens, generate a new invitation.
- If *any* collaborators connect using an invitation, the invitation is activated and its time limit is removed. Once activated, an invitation can be re-used until the session owner stops collaborating or ends the session.
- Collaborators can disconnect from a collaboration session and then rejoin it later using the same invitation.
- Collaboration sessions persist even if all collaborators leave and only the session owner remains. Until the session owner disconnects or stops the collaboration session, collaborators can rejoin the session using the same invitation.
- The collaboration invitation remains valid until the session owner disconnects or stops the collaboration session.

Inviting the First Collaborator

To begin a collaboration session, generate an invitation using the Collaboration Manager.

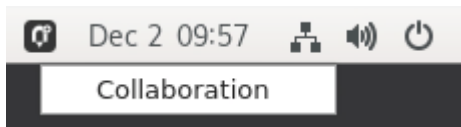
To generate a collaboration invitation:

1. Connect to a PCoIP session with PCoIP Ultra and Collaboration enabled.
2. From the remote session, open the **Collaboration Manager** using either of these methods:
 - **From the in-session menu:** From the in-session menu, select **Collaborate** > **Invite to Collaborate**.



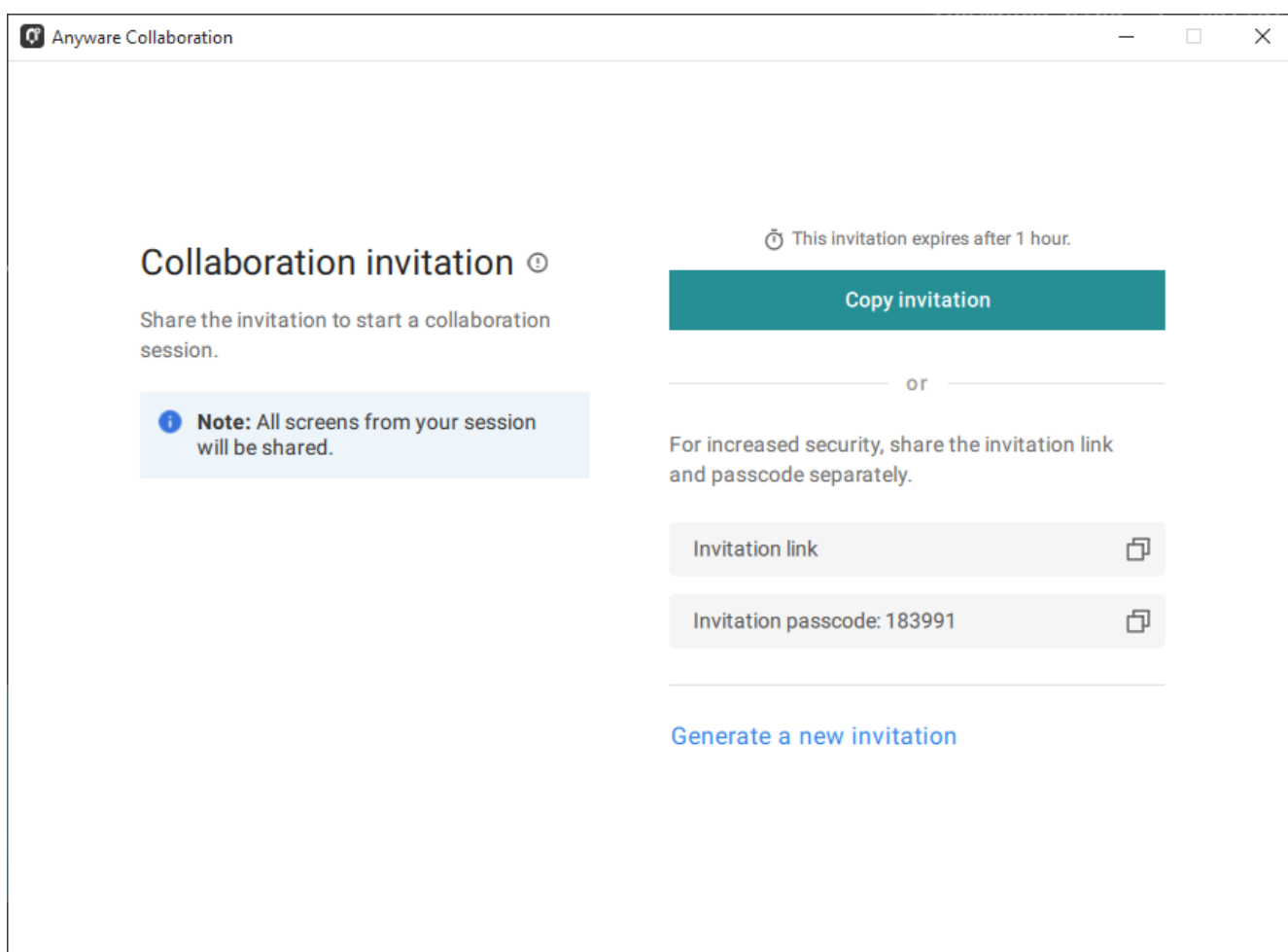
The Collaborate menu appears if both the Anyware agent and Anyware client are version 23.06 and higher, and if both support Collaboration. If the Collaborate menu does not appear, open the Collaboration Manager using the menu bar instead.

- **From the menu bar:** by clicking the **Anyware Collaboration** icon in the menu bar:



This example shows a Linux desktop; yours may vary depending on which operating system you are connecting to.

3. The Collaboration manager generates and displays an invitation:



The invitation contains two pieces of information that are used to invite the collaborator:

- **Invitation Link:** The collaborator will use this link to join your session. The link may be opened on any Mac, Windows or Linux machine with a Anyware Client 21.07 or newer.
- **Invitation passcode:** This is a 6-digit code that confirms the identity of the individual connecting to the collaboration session. A new code is generated along with each new token.

4. Share the *invitation link* and the *invitation passcode* with the collaborator.

- To share both the link and the code at once, click the **Copy invitation** button. This will create a single message containing both the link and the code and place it on your clipboard. Share this with your collaborators using any acceptable method.
- To share the link and code *separately*, click the *copy* button beside each item and share them using separate communications. Sharing the invitation this way reduces risk in the event that a message is inadvertently sent, forwarded, or intercepted by a third party.

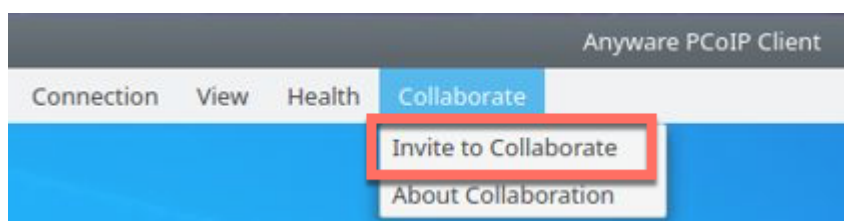
Inviting Additional Collaborators

Once the collaboration session has been created, you can invite additional collaborators by sharing the same invitation link and passcode with them. You can also view the invitation, and copy its link and passcode for sharing, using the Collaboration Manager.

To view and copy the invitation link and passcode:

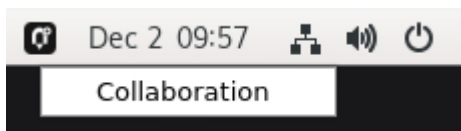
1. From the remote session, open the **Collaboration Manager** using either of these methods:

- **From the in-session menu:** From the in-session menu, select **Collaborate > Invite to Collaborate**.



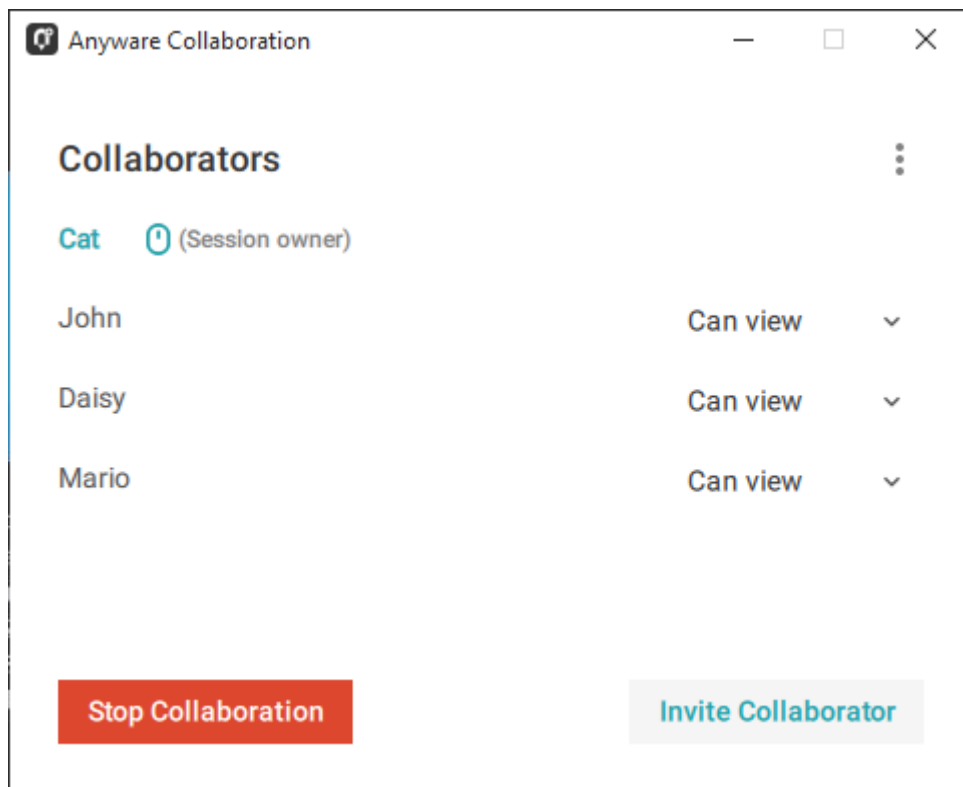
The Collaborate menu appears if both the Anyware agent and Anyware client are version 23.06 and higher, and if both support Collaboration. If the Collaborate menu does not appear, open the Collaboration Manager using the menu bar instead.

- **From the menu bar:** by clicking the **Anyware Collaboration** icon in the menu bar:

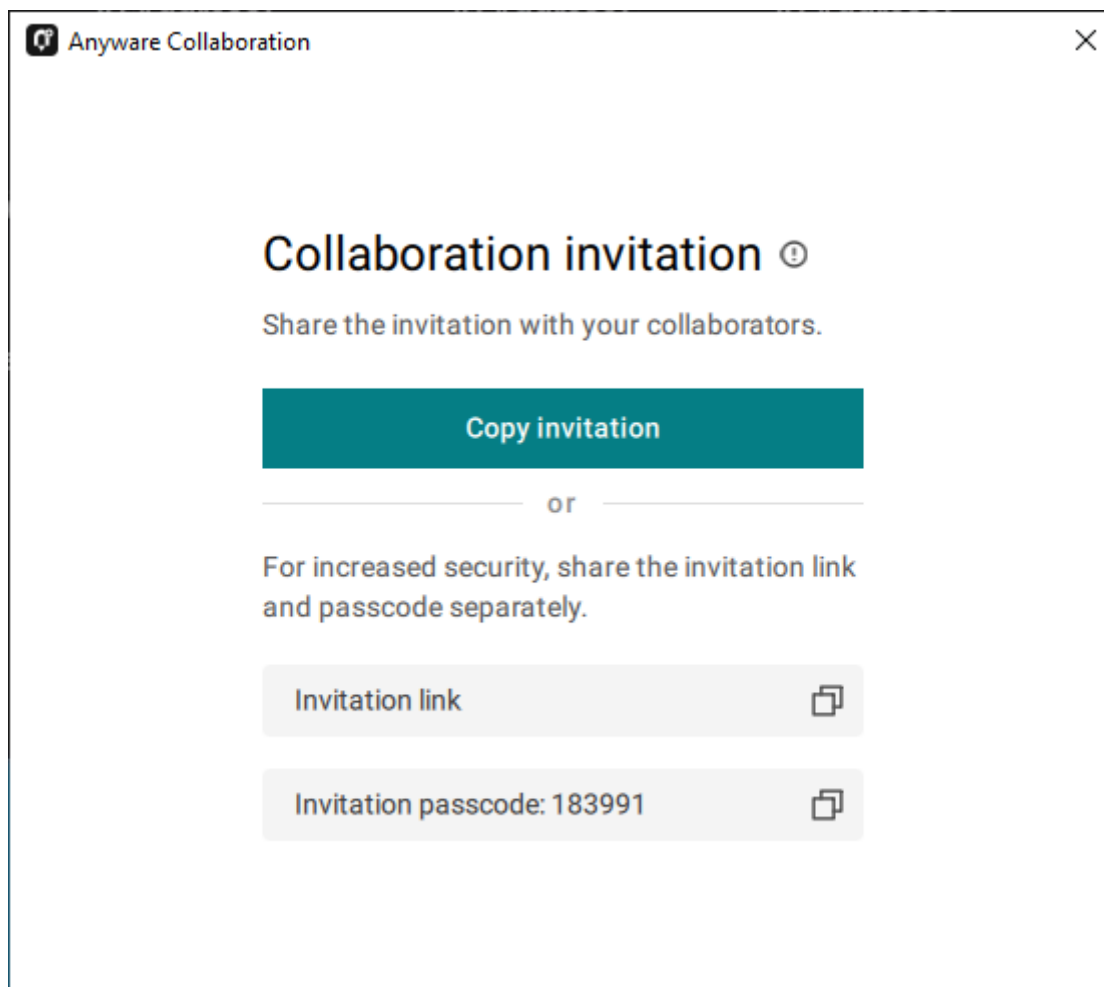


The collaboration manager shows a list of your active collaborators (if any).

2. In the Collaboration manager, below the list of active collaborators, click **Invite Collaborator**:



3. The Collaboration manager displays the generated invitation. Note that this is the *same* invitation link and passcode you used previously. It is not a new invitation:



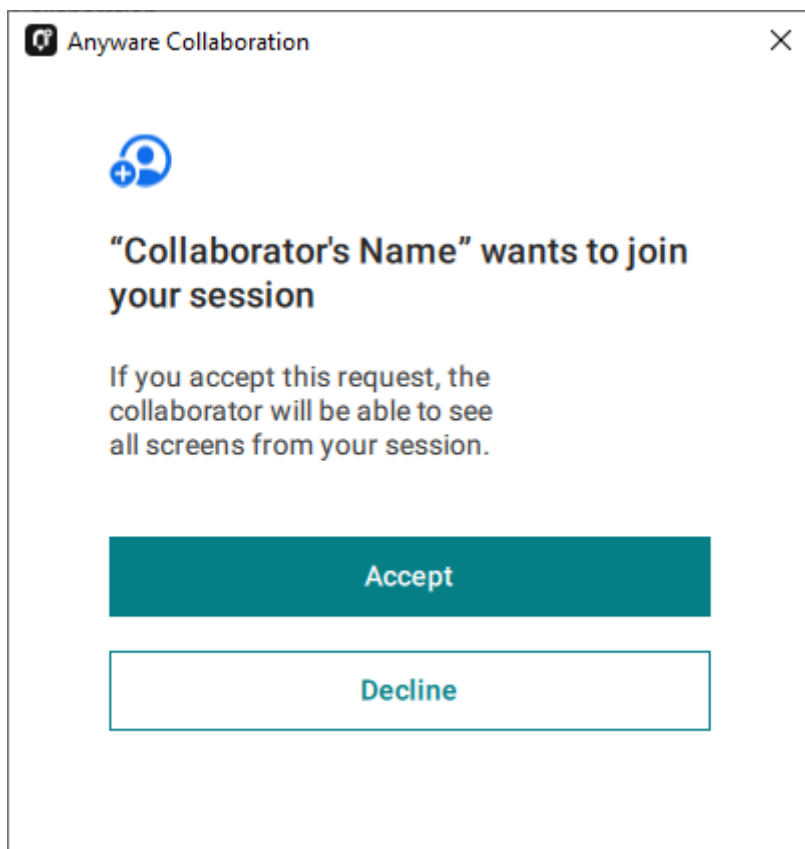
4. Share the *invitation link* and the *invitation passcode* with the additional collaborators.

Accepting or Declining Collaborators

Once distributed, the session owner's collaborators can [join the collaboration session](#). As collaborators use the invitation, the session owner is notified and can accept or reject each connection attempt.

To respond to a collaborator:

1. When the collaborator attempts to join the session, the Collaboration manager will display options to accept or reject the connection.



2. Click **Accept** to start the collaboration session. Click **Decline** to deny the request. Whether you accept the request or not, the invitation has been used and is now disabled. Subsequent attempts will require a new invitation.

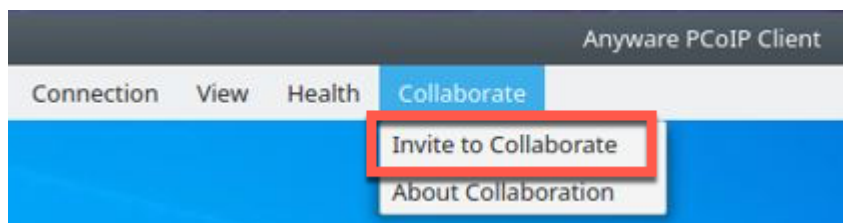
Ending a Collaboration Session

The collaboration session will end when the session owner disconnects their PCoIP session, or if they stop collaborating using the collaboration manager.

Ending the collaboration session invalidates the invitation. To start a new session, generate a new invitation by inviting another collaborator.

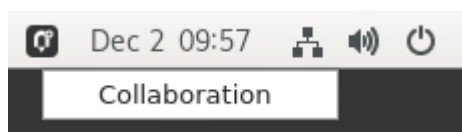
To stop collaborating:

1. From the remote session, open the **Collaboration Manager** using either of these methods:
 - **From the in-session menu:** From the in-session menu, select **Collaborate > Invite to Collaborate**.



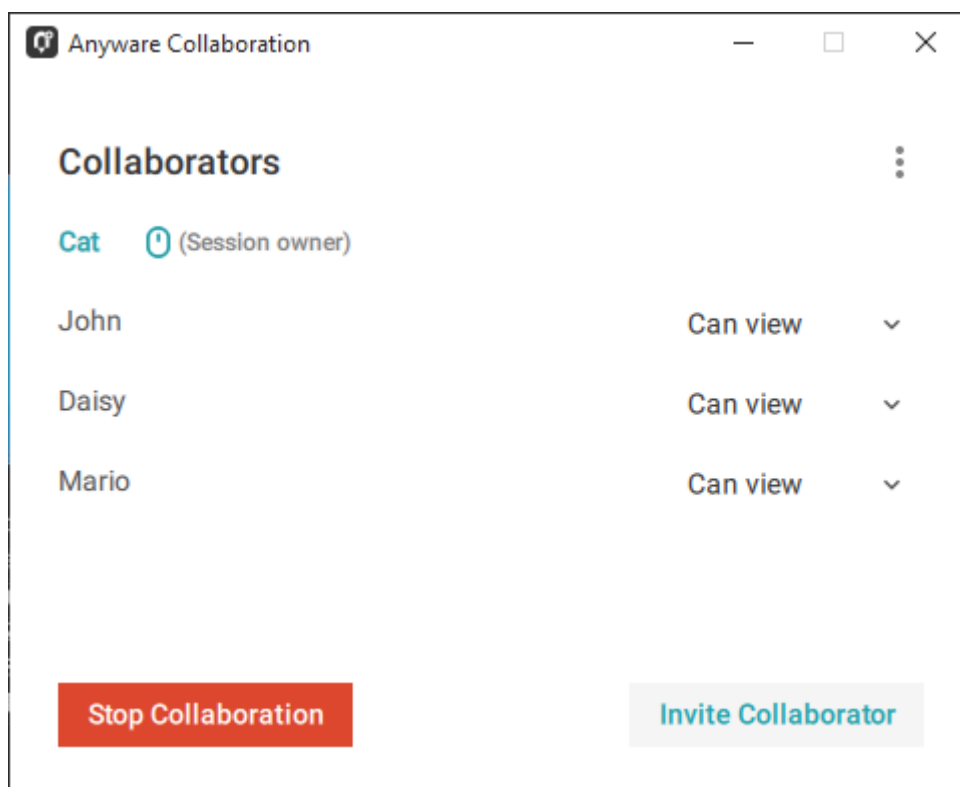
The Collaborate menu appears if both the Anyware agent and Anyware client are version 23.06 and higher, and if both support Collaboration. If the Collaborate menu does not appear, open the Collaboration Manager using the menu bar instead.

- **From the menu bar:** by clicking the **Anyware Collaboration** icon in the menu bar:



This example shows a Linux desktop; yours may vary depending on which operating system you are connecting to.

2. Click the **Stop Collaboration** button.



Allowing Collaborators to Control the Session

Collaborator input control allows collaborators to use their own mice and keyboards to control the session owner's desktop. **This feature is disabled by default**, and must be enabled on the Anyware agent before it is available.

Once enabled, input control options are available from the collaboration manager. Input control can be granted (or retracted) for each user separately or for all users at once.

Note: Disabling input control globally

You can disable Input Control on the Anyware agent, which turns the feature off entirely. When disabled this way, session owners will not be able to allow collaborators to take control, and all sessions will be view-only. For more information, see [Disabling Input Control](#).

Important: The session owner always has control of their Anyware client's in-session menu

The session owner always has control of their Anyware client's in-session menu. If the owner is unable to reclaim session input control for any reason, they can disconnect the PCoIP session using the in-session menu option. When the owner disconnects from the session, the collaborator is immediately disconnected.

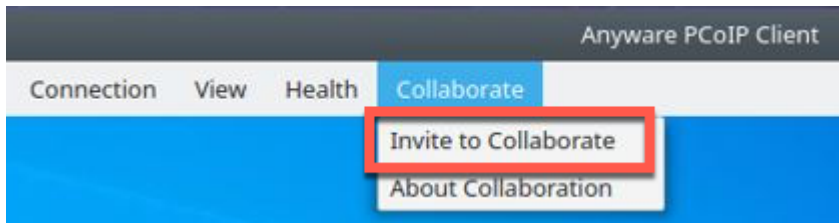
ENABLING INPUT CONTROL FOR COLLABORATORS

The following steps will allow one or more collaborators to take control of the session desktop. The collaborators will not immediately have control when this is granted; they must still take control using the [process described above](#).

This option will not be available if Input Control has been disabled on the Anyware agent.

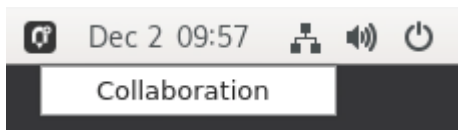
To allow collaborators to control the session desktop:

1. From the remote session, open the **Collaboration Manager** using either of these methods:
 - **From the in-session menu:** From the in-session menu, select **Collaborate > Invite to Collaborate**.



The Collaborate menu appears if both the Anyware agent and Anyware client are version 23.06 and higher, and if both support Collaboration. If the Collaborate menu does not appear, open the Collaboration Manager using the menu bar instead.

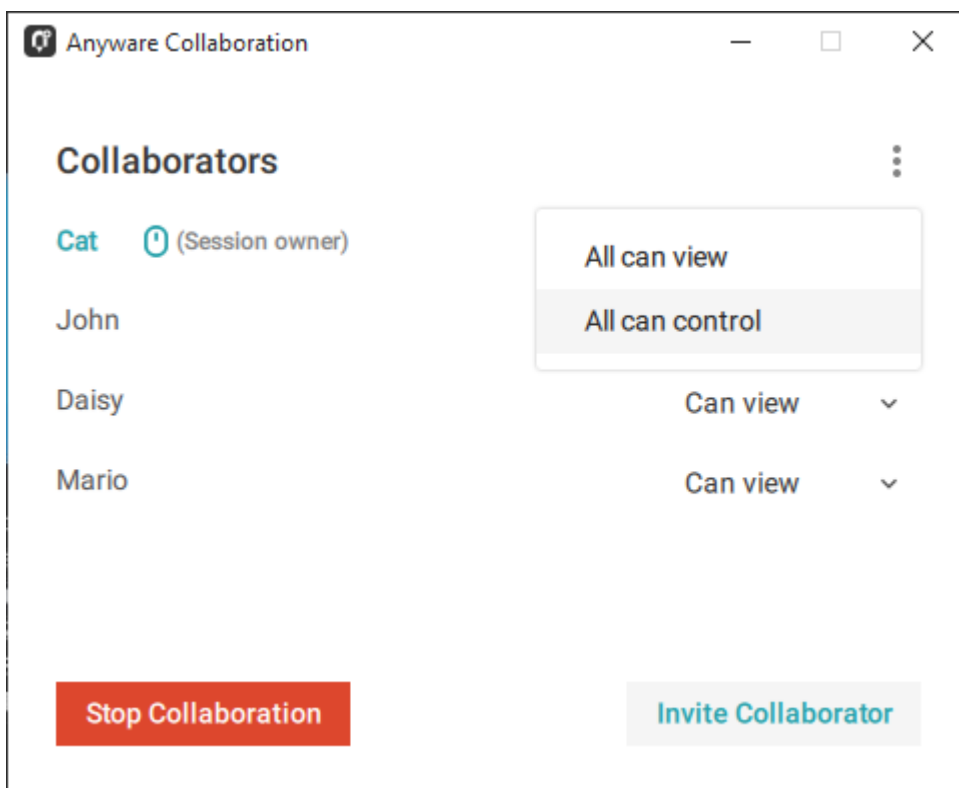
- **From the menu bar:** by clicking the **Anyware Collaboration** icon in the menu bar:



This example shows a Linux desktop; yours may vary depending on which operating system you are connecting to.

2. Grant input control using one of these methods:

- To allow input control for *all collaborators*, click the dropdown menu at the top right and select **All can control**.



- To allow input for *one collaborator*, click the dropdown menu beside the collaborator's name and select **Can control**.

STOPPING INPUT CONTROL

To return a user (or all users) to view-only mode:

1. From an active collaboration session, open the collaboration manager.
2. Beside the collaborator's name, click the dropdown menu and select **Can View**.

Understanding Display Behavior

Collaboration sessions support sharing of multiple monitors, which varies by session owner's client setting as follows:

- **Windowed mode:** The session in the owner's client window will be shared.

- **Fullscreen One Monitor:** The single fullscreen session will be shared. The session owner should set their Anyware Client to *Fullscreen One Monitor* mode prior to starting the collaboration session.
- **Fullscreen All Monitors:** All monitors will be shared, beginning with the Session Owner's monitor 1 and continuing up to the number of displays in the collaborator's system. The monitors that are shared cannot be configured, and are shared in system order.

*When using this mode, the session owner should assume that collaborators can see **all** displays unless a specific configuration has been tested and verified.*

For example, if the session owner has four monitors and a collaborator only has two, the collaborator will see the session owner's first and second monitors. If different collaborators have a different number of screens, each will see as many displays their system supports; in this scenario, you may have some displays that are visible to certain collaborators but not others.

The session owner should set their Anyware Client to *Fullscreen All Monitors* mode prior to starting the collaboration session.

If the session owner's and collaborator's screen resolutions are different, the collaborator's screen will use scrollbars and letterboxing to display the shared content.

If *high performance client* mode is enabled, and if the session owner's resolution is greater than the collaborator's, the collaborator's screen will be clipped instead.

Joining a Collaboration Session

Collaborators receive the invitations generated by session owners, and use the invitation URI and passcode to connect to the session.

Important: Anyware Client steps

Collaborators join sessions using Anyware clients. Make sure the software client version you are using supports the collaboration features you require. For details, see [Feature Version Requirements](#).

Each collaborator can join the session with the collaboration link and the Collaboration Invitation passcode. The same URI and passcode are used for all collaborators on the same session.

To join a collaboration session as a collaborator:

1. Open a web browser and go to the collaboration 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 *Anyware Client* application. Allow the browser to open the Anyware client.
3. When the Anyware client opens, it will prompt you for your name and the Collaboration Invitation passcode. The name you provide here will identify you in the collaboration session. The collaboration invitation passcode is the six digit number provided by the session owner. Enter both values and click **Submit**.
4. Once the session owner accepts your connection request, the Collaboration screen share will start.
5. To leave the collaboration session, select **Connection > Disconnect** from the Anyware Client menu.

Collaborator Input Control

If the session owner has enabled input control for a collaborator, the collaborator can take control of the session owner's desktop including mouse, keyboard, and pointer activity. The session owner retains the ability to stop input control at any time.

USING INPUT CONTROL AS A COLLABORATOR

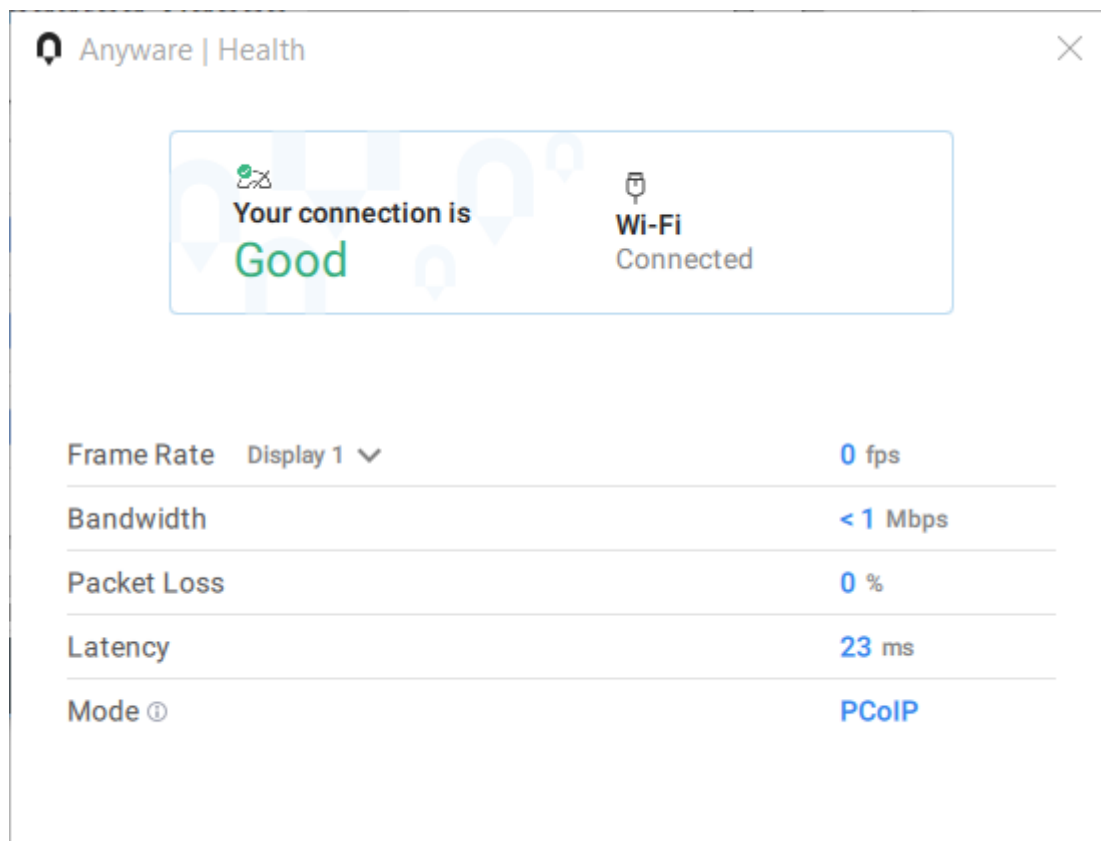
A collaborator who has input control can release it by idling—stopping all keyboard, mouse, and pointer activity—for a short time. Once the control timeout has elapsed, the floor is open, and whichever collaborator provides input next takes control.

By default, the control timeout is 3 seconds. The timeout value can be configured when enabling the input control feature.

For example: the session owner has initial control of the session. In order to give control to the collaborator, the owner takes their hands off the keyboard and mouse for three seconds, allowing the control timeout to pass. A collaborator then moves their mouse, which gives them control. To give control back to the session owner, the collaborator takes their hands off their keyboard and mouse for three seconds. This exchange continues as long as needed.

Anyware Connection Health

The **Connection Health Indicator** gives you quick feedback on the quality of your active PCoIP session, including a general status indicator and several specific metrics that you can use to troubleshoot connection problems.



The screenshot shows a window titled "Anyware | Health" with a close button in the top right corner. Inside the window, there is a status box that says "Your connection is Good" in green text, accompanied by a Wi-Fi icon and the text "Wi-Fi Connected". Below this, there is a table of connection metrics:

Frame Rate	Display 1 ▾	0 fps
Bandwidth		< 1 Mbps
Packet Loss		0 %
Latency		23 ms
Mode ⓘ		PCoIP

Note: Not available in the legacy high performance mode

The Connection Health Indicator is only available in the client's *standard* mode and *High Performance (Preview)* mode. It is not available in the *High Performance (Legacy)* mode.

To open the Connection Health Indicator:

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

The Anyware Health opens as a separate window on top of the current session. You can move the window as needed, including to a different monitor, but it will remain on top of the current session displays until it is closed.

The Anyware Health monitor shows the [general network health status](#), identifies the [type of network connection](#) being used, and displays several [real-time metrics](#).

Connection Health Status

The general connection health is described as *good*, *fair*, or *poor* depending on a combination of packet loss and latency statistics.

Connection Health Status	
Good	The network connection is healthy and should provide excellent PCoIP performance.
Fair	The network is experiencing packet loss greater than 0.25%, or latency greater than 50ms. PCoIP sessions may be degraded, and you may experience moderate dropped frames, image stutter, and sluggish responsiveness.
Poor	The network is experiencing packet loss greater than 0.5%, or latency greater than 100ms. PCoIP sessions will be significantly degraded and will suffer from dropped frames, stutter, poor responsiveness, and loss of image quality.

Network Connection Indicator

This identifies the type of connection your client is using for the current session. It will indicate if your connection is wired (LAN) or wireless (WIFI), and show the name of the connected network and its state.

Note that PCoIP over WIFI is not as robust as connections on a wired LAN; if you are experiencing degraded performance on a WIFI connection, switch to a wired LAN connection if possible.

Measured Statistics

The following real-time statistics are reported in the Anyware Health indicator:

Metric	Description	Notes
Frame rate	Displays the current frame rate for the PCoIP session.	<p>If you have multiple displays, you can check the frame rate for each display by selecting it from the provided dropdown.</p> <p>Frame rates are dynamic in PCoIP sessions, varying by the amount of dynamic content shown on screen as well as network and hardware capacity. It is normal for PCoIP frame rates to drop as low as zero if the screen content is perfectly static.</p>
Bandwidth	The total network bandwidth being used by the current PCoIP session.	Bandwidth utilization fluctuates based on many factors, including frequency and range of dynamic screen changes and audio output.
Packet loss	The percentage of PCoIP packets that are being lost to network quality.	Packet loss greater than 0.25% will negatively affect PCoIP performance; a loss of greater than 0.50% will result in severely degraded performance.
Latency	The total end-to-end network latency between the Anyware client and Anyware agent.	Latency greater than 50ms will negatively affect PCoIP performance; latency greater than 100ms will result in severely degraded performance.
PCoIP mode	The active PCoIP protocol mode.	Note that PCoIP Ultra Auto-Offload mode can employ different protocols on different screens simultaneously; you can select a specific display from the dropdown here to inspect them individually.

Displays

The Anyware 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

Anyware 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 Linux's interface will automatically use the operating system's language setting, if it is supported.

The interface language can be changed to any of the following supported languages:

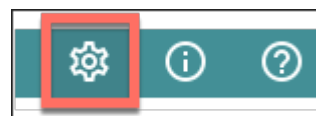
- Chinese Simplified
- English
- French
- German
- Italian
- Japanese
- Korean
- Portuguese (Iberian)
- Spanish

Changing the Software Client for Linux Display Language

To set the client's display language:

1. If you are connected to a PCoIP session, disconnect.
- 2.

Click the **Settings** icon at the top of the Software Client for Linux window.



3. Click the **Language** tab in the left sidebar.
4. Select the language you would like to set from the dropdown menu.

This setting is persistent, and will remain active until changed.

This setting only affects the Software Client for Linux's pre-session interface. It does not change language settings on remote desktops.

 Note: In-session menus are not localized

This feature sets the language for the client's pre-session display *only*. The in-session menu bar is not affected by this change. Support for localization of the in-session menu bar will be added in a future release.

 Important: Broker-generated screens are not localized

Multi-factor authentication screens displayed during a login sequence use content provided by an external connection broker. These screens are not localized.

Setting the Language via Command Line

You can also set the Software Client for Linux language by invoking it on the command line and passing a language code as an argument. For details and instructions about this method, see [Configuring the Anyware Client: Language](#)

PCoIP Ultra

The Software Client for Linux provides support for PCoIP Ultra, the latest protocol enhancements from HP.

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

Important: PCoIP Ultra is Enabled by Default

PCoIP Ultra is enabled by default. To configure Ultra, carefully review the recommended use cases in the next section to determine the PCoIP Ultra value most suited for your needs.

Requirement: AVX2 Support

All client machines *and* remote Windows and Linux agent machines must support the AVX2 instruction set. The Anyware Agent for macOS requires AVX2 support when running on Intel hardware. PCoIP Ultra is supported on Apple Silicon with Anyware Agent for macOS 22.09 or higher.

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:** When using a Anyware 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 Anyware Graphics agent and the Anyware software client are capable of both CPU and GPU 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.

Setting PCoIP Ultra

PCoIP Ultra defaults to **Auto Offload** on agent machines, provided that it has not been set to Auto Offload (in a prior deployment), and the agent and client machines are capable of both CPU and GPU Offload.

The PCoIP Ultra offload mode is set on the Anyware agent. Refer to the appropriate documentation for instructions:

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

- Linux Standard Agent
 - [PCoIP Ultra](#)

Note: Setting the PCoIP Ultra Values

PCoIP Ultra now defaults to "Auto Offload" on agent machines. When [the H.264 Hardware Decoding setting is disabled](#) on client machines, it results in PCoIP Ultra not defaulting to "Auto Offload".

PCoIP Codec Indicator

When enabling PCoIP Ultra, an onscreen indicator is observed at the bottom-left corner of the screen. CPU optimization is indicated by a dark blue dot, while GPU optimization is indicated by a magenta dot.

To disable this codec, update the `pcoip.codec_indicator` parameter:

```
~/pcoip.rc pcoip.codec_indicator = 0
```

Ensure that you maintain the space before and after the `=` sign.

H.264 Hardware Decode

The Anyware Software Client for Linux supports H.264 hardware decode for selected hardware configurations by using the Anyware Client to enable the decode. For information on this, see [H.264 Hardware Decode](#).

Printing Support

Anywhere Clients support the following printing options:

- **Printing from the Local Machine:** This option permits jobs created on host machines to be printed using printers connected to the client machines. Documents can also be printed on printers in the Anyware client's local area network.

This method is suitable for printing when the host and the client are not on the same network, such as in multi-site organizations.

- **Printing from a USB Printer:** This option permits jobs to be printed on USB printers that are connected by means of the USB Bridging feature. USB printers are typically attached to Anyware clients, but are redirected to the remote host.

The following options are also available for printing:

Note: Default Printing Options

The printing options described below are default options, independent of the client software.

- **Printing from the Agent Machine:** This option permits jobs to be printed on printers that are connected to the agent machines.
- **Printing Using a Cloud Service:** This option permits the use of an external cloud service, such as Google Print, for processing print jobs created on host machines. The use of an external cloud service allows for the use of shared printers on the client's network without the need for installing device drivers. Prior to using, the external cloud service must be correctly configured.

Support for these methods depends on the Anyware agent and the Software Client for Linux it connects to. The Software Client for Linux printing support is as follows:

	Windows agents	Linux agents	macOS agents
Printing from the Local Machine	✓	–	–
Printing from a USB Printer	✓	–	–
Printing from the Agent Machine	✓	✓	✓
Printing Using a Cloud Service	✓	✓	✓

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 Anyware clients. Note that Anyware Zero Clients must be configured to enable it.

Relative mouse mode is supported by the following agents:

- Anyware Standard Agent for Windows
- Anyware Graphics Agent for Windows
- Anyware Standard Agent for Linux
- Anyware Graphics Agent for Linux

Relative mouse mode is not supported by the Anyware 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 Linux.

Enabling from the Menu Tab

The following steps outline how to enable relative mouse from the menu tab, while connected to a supported Anyware Agent with a supported Anyware 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 Anyware 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 Anyware Agent with a supported Anyware Client, press `ctrl + alt + r`. This will toggle the feature on and off. This will only work if you are connected to a Anyware Agent version that supports relative mouse.

USB

USB Support

Anyware 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 Anyware Agent.

USB Redirection

USB redirection is only intended to be used with a single instance of the Anyware Software Client. Launching a second instance of the Anyware 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 Anyware Agent for Linux.

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

Bloomberg Keyboard Support

 **Note: Certain keys are not sent to the remote session**

The "Pause/Break/Log Off" and "Application" keys found on Bloomberg Keyboards are not forwarded to the remote session and will have no effect.

The following Bloomberg Keyboards are supported when connecting from a Windows or Linux software client to a Windows agent (both 23.06 or higher).

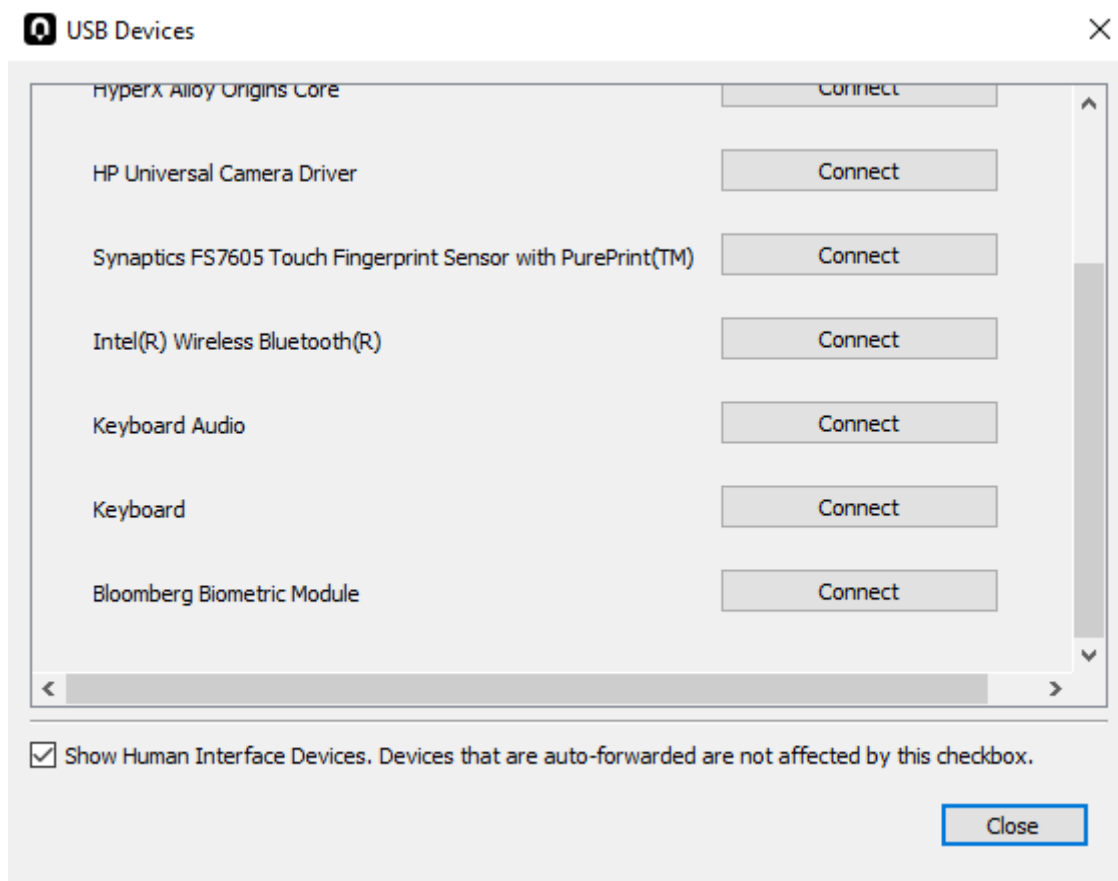
- Bloomberg Keyboard 4
- Bloomberg Keyboard 5

Using The Bloomberg Biometric Module

To use the Bloomberg Biometric Module (Fingerprint Scanner) in an remote Session, *Bloomberg Professional software* must be installed on the remote host, and the biometric module device must be connected.

To connect the biometric module:

1. Connect to the PCoIP session.
2. If you are in a full-screen mode, reveal the client's in-session menu bar by hovering the cursor at the top of any display.
3. From the client's in-session menu bar, click **Connection > USB Devices...**
4. In the *USB Devices* window, find "Bloomberg Biometric Module" and click Connect:



Note: The device name shown may be different

On some systems, the Biometric Module is named *HID-compliant Device*. If *Bloomberg Biometric Module* is not shown in the list of devices, connect *HID-compliant Device* instead.

Important: Only connect the biometric module using this method

Do not connect "Keyboard" or "Keyboard Audio" using this method; those devices must remain locally connected to function properly. See [Using Bloomberg Keyboard Audio](#) below for instructions on using Bloomberg Keyboard as an audio device.

Once connected, the Biometric Module will be available for the Bloomberg Professional software installed on the remote host. See Bloomberg Keyboard documentation for instructions on installing and configuring Bloomberg Professional software.

Using Bloomberg Keyboard Audio

The Bloomberg Keyboard has both audio input and audio output capabilities. To use these features in your remote session, you must set the Bloomberg Keyboard's input and output devices as the default audio device on your local machine.

Important: Multiple audio streams are not supported

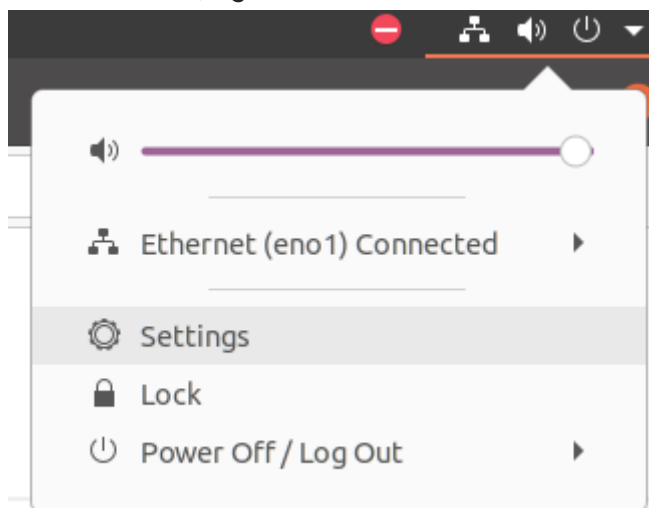
Remoting multiple, simultaneous audio streams between Anyware clients and remote agents is not currently supported. Connecting the keyboard audio device over USB remoting is not recommended as it will result in poor audio quality.

To set the keyboard as your default audio device:

Note: GNOME desktop examples

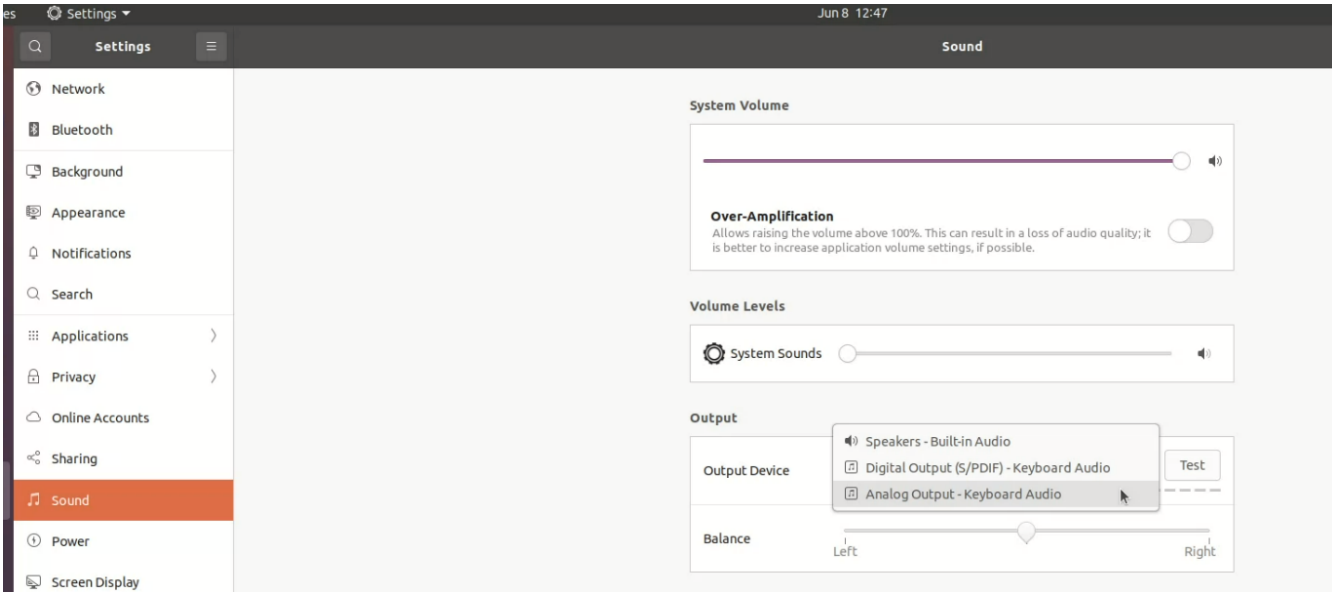
The instructions and screenshots in this section are from the GNOME desktop environment. Your interface may be different.

1. In the task bar, right click on the *Audio* icon and click Settings:

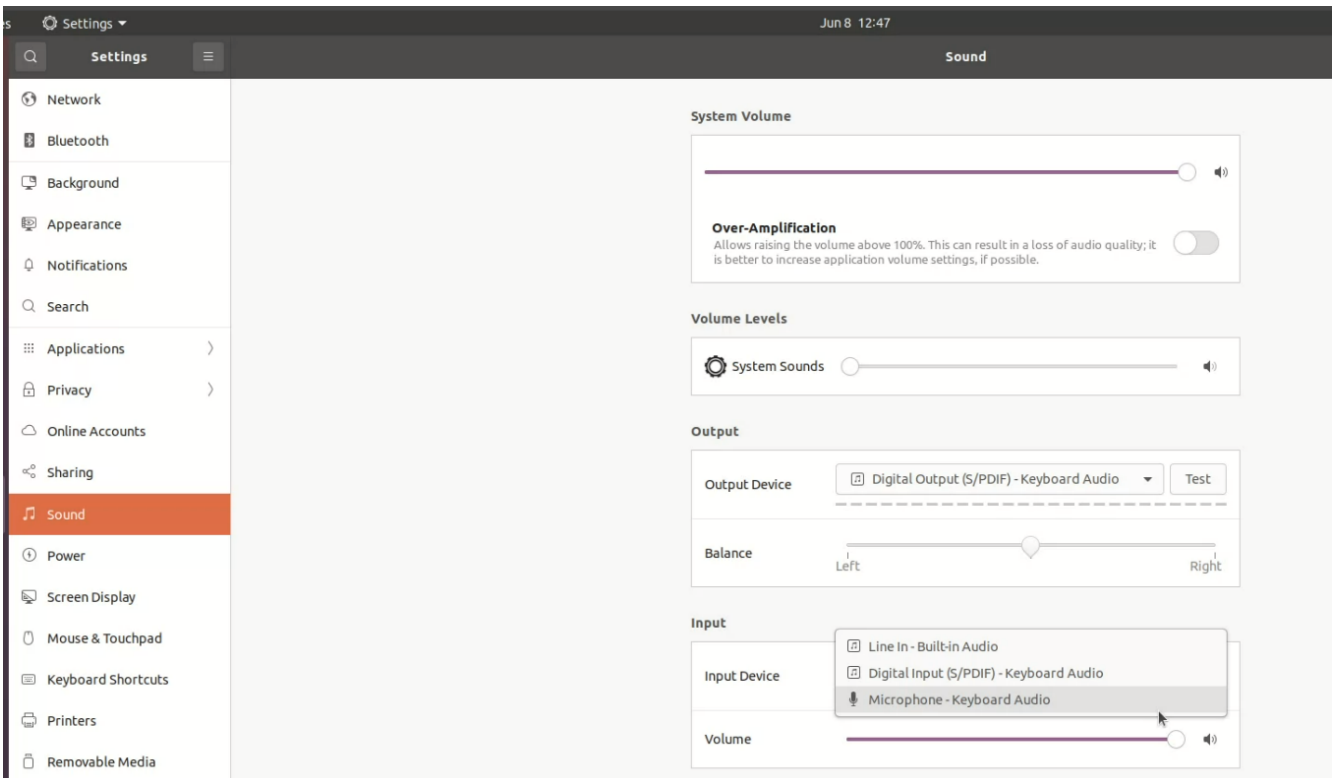


2. Navigate to Sound settings.

3. Configure your output device to be **Digital Output (S/PDIF) - Keyboard Audio** or **Analog Output - Keyboard Audio** - **Keyboard Audio**:



4. Configure Input Device to **Digital Input (S/PDIF) - Keyboard Audio** or **Microphone - Keyboard Audio** - **Keyboard Audio**:



Tangent Panel Support

The following Tangent panels are supported when connecting from a Windows or Linux software client to a Windows or Linux agent (both 23.04 or higher).

- Tangent Ripple
- Tangent Wave
- Tangent Element BT
- Tangent Element MF
- Tangent Element KB
- Tangent Element TK
- Tangent Arc (Navigation)
- Tangent Arc (Grading)
- Tangent Arc (Function)

The Graphics Agent for macOS and the Software Client for macOS do not support Tangent panels.

Wacom Tablet Support

The Software Client for Linux 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 Anyware agent (any type), and a supported Software Client for Linux.

Anyware client support for *locally terminated* Wacom tablets and the Software Client for Linux

	Anyware agents (Windows)	Anyware agents (Linux)	Anyware Graphics Agent for macOS	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 Pro 16 <i>DTH-167</i>	✓	✓	–	–
Cintiq Pro 16 <i>DTH-1621</i>	✓	✓	–	–
Cintiq 22 <i>DTK-2260</i>	✓	✓	–	–
Cintiq 22HD <i>DTK-2200</i>	✓	✓	–	–
Cintiq 22HDT - Pen & Touch <i>DTH-2200</i>	–	–	–	–
Cintiq Pro 24 <i>DTK-2420</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>	✓	✓	–	–

Important: Touch is not supported

Touch features of Wacom devices are not supported with local termination.

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 Linux 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 Linux:

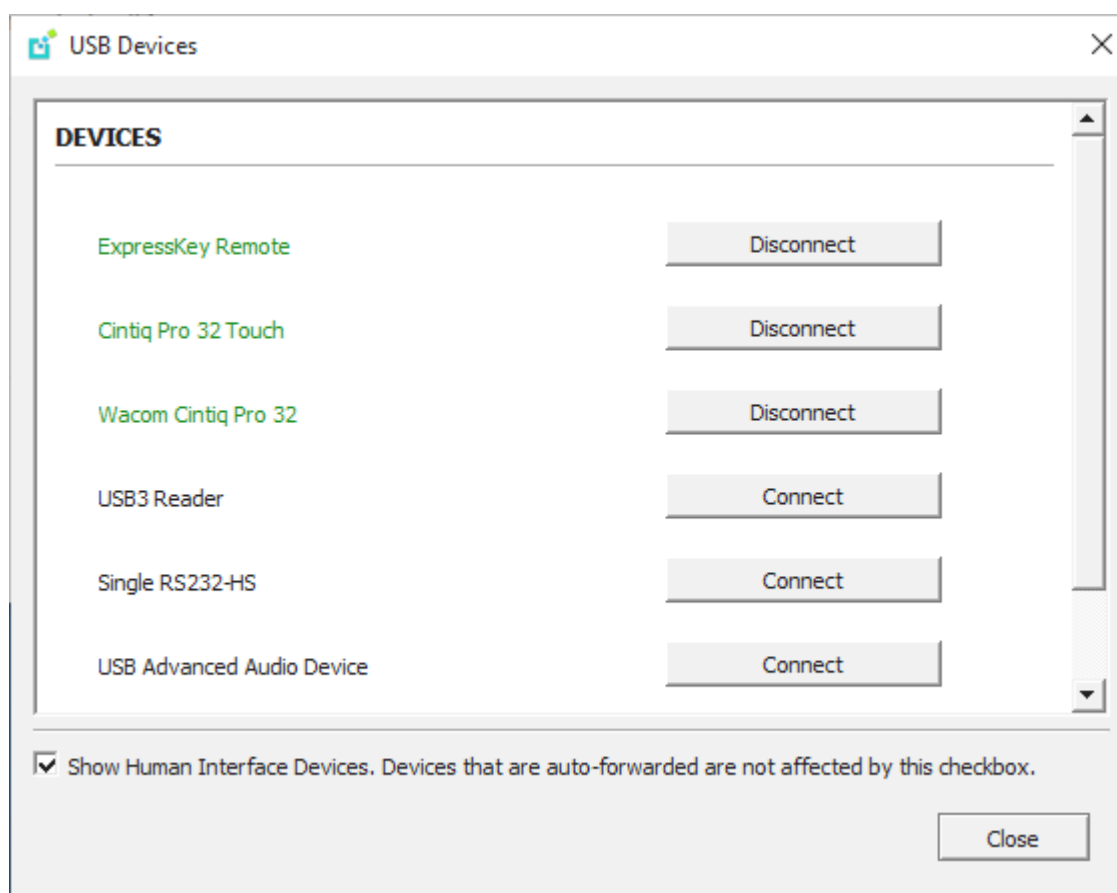
Anyware client support for *bridged* Wacom tablets and the Software Client for Linux

	Anyware agents (Windows)	Anyware agents (Linux)	Anyware Graphics Agent for macOS	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 Pro 16 <i>DTH-167</i>	✓	✓	—	—
Cintiq Pro 16 <i>DTH-1621</i>	✓	✓	—	—
Cintiq 22 <i>DTK-2260</i>	✓	✓	—	✓
Cintiq 22HD <i>DTK-2200</i>	✓	✓	—	✓
Cintiq 22HDT - Pen & Touch <i>DTH-2200</i>	✓	✓ <i>Ubuntu only</i>	—	✓
Cintiq Pro 24 <i>DTK-2420</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>	✓	✓	—	✓

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



Tablet Force Proportions

You can enable the **Tablet Force Proportions** feature of your Wacom tablet in a PCoIP session. This feature constrains the device to match the horizontal and vertical proportions of your display, ensuring that there is no undesired stretching of your drawing.

For example: if you draw a perfect circle on the device, with *tablet force proportions* enabled the display will show a perfect circle; when it is disabled, the circle could appear as an ellipse depending on the screen proportions.

When this mode is enabled, the entire active surface of the device may not be usable; only the portion of the device that matches the proportion of the screen will be active.

 **Note: Wacom driver setting must match**

The Wacom driver must also be configured to use force proportions, or this setting will have no effect.

To enable or disable *Tablet Force Proportions*:

From the Software Client for Linux in-session menu, select **View > Tablet Force Proportions** to toggle the setting.

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.
- Anyware 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 Linux'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 Linux now supports USB webcams when connecting to a Anyware 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 Linux, 21.07+
- Anyware Standard Agent for Windows or Anyware 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.
- Anyware 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 Anyware Software Client, connect the webcam as described in [USB Bridging of Webcams](#).

Console Game Controller Support

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

- PS4
- PS5
- Logitech F310 gamepad

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

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

Smart Cards

Supported Smart Cards

Anyware Linux Clients support pre-session smart card authentication when connecting to Windows Graphics agents and Windows Standard agents, provided that the following system requirements are met. For deployments that meet these requirements, Linux Clients can also read and process smart card information and allow SSO (single sign-on) authentication of the user prior to session establishment.

This topic describes the requirements to support pre-session smart card authentication when connecting to Windows Graphics agents or Windows Standard agents.

Smart Card Dependencies

It is important to test your smart card in your deployment. Changes to smart card vendor applets and middleware software may cause smart cards to become ineffective in your deployment.

Anyware Agent

Smart Card Authentication is supported while connecting to the following agents: - Windows Graphics agent 24.03 or later - Windows Standard agent 24.03 or later

Anyware Client

At this time, smart Card Authentication is only supported while connecting from **Linux Client version 24.03 or later**.

SMART CARD CERTIFICATE REQUIREMENTS

The smart card certificate prerequisites are as follows:

- Key usage is set to digital signature
- Subject common name and/or subject alternative name (other name) are set

- Enhanced key usage must include client authentication and/or smart card logon
- Key length must not be larger than 2048 bit

Smart Card Readers

The following smart card readers have been tested:

- Belkin USB Smart Card Reader (F1DN008U)
- Identiv SCR3310 USB Contact Smart Card Reader

Tested Smart Card Models

This version of Linux Clients supports both pre-session authentication and in-session use of smart cards. The following smart card models have been tested:

Product Name	Type of Card	Notes
Gemalto TOP DL V2.1 144K FIPS	CAC	
IDEMIA Cosmo v8.0	Alternate token	
IDEMIA ID-one 125 V8.0D	CAC	
G+D Sm@rtCafe Expert v7.0	CAC	
G+D Sm@rtCafe Expert v7.0 144K DI	CAC	
PIVkey C910	PIV	
PIVkey C980	PIV	
PIVkey C990	PIV	
Yubikey 5C		Using PIV interface.
Yubikey 5 NFC		Using PIV interface.

Note: Testing Smart Card Solutions

Solutions must be validated in user environments before selecting a solution, as environmental differences including network conditions or other components may impact support.

Notes

- Smart Card Authentication works only with the Anyware Standard Agent for Windows and the Anyware Graphics Agent for Windows.
- Smart Card authentication can only be enabled or disabled during installation. If the Anyware agent has already been installed, re-install the software using the instructions below.
- The interface-driven installer for the Software Client for Linux cannot enable this functionality. You must use the scripted (silent) installer.
- At present, only a single card and single reader configuration is supported.
- We have tested ActivClient 7.4.3.13; other versions may work but have not been tested.
- While in a PCoIP session, the remote desktop's Device Manager will show two identical smart cards. This is expected and does not affect the session.

Known Limitations

- The [Interactive logon: Smart card removal behavior](#) is not supported during smart card sessions.
- When authenticated using smart cards, Anyware Clients cannot recognize HP Digital Badges.
- Concurrent users cannot log on to agent machines using the same smart card for authentication. Smart cards having multiple certificates allow only one user to log on at a time. To be able to log in, other users must wait until the current user logs off.

Client Setup

Note: Agent Setup is Required

To enable authentication using smartcards, configuration is required on agent machines. For more information, see "Enabling Smart Card Authentication Using Linux Clients" in the agent guide.

1. Make sure that you downloaded Anyware Linux Client version 24.03 or later on the client machine.
2. Configure the client machine to connect to the agent machine. Follow the instructions in the topic "Connecting to an Agent Machine" in the Anyware Linux Client guide.
3. Plug the smart card reader into the Client machine, and use your smart card for authenticating the PCoIP session. For instructions on using the smart card to authenticate PCoIP sessions, consult

"Using Smart Card Authentication to Connect to a Session" in the topic "Connecting to an Agent Machine" of the Anyware Linux Client guide.

Installation

Prerequisites for Installing the Software Client for Linux

There are a few prerequisites to complete before Anyware Software Client for Linux installation will work. The prerequisites are listed as follows:

- A desktop environment of your choice is required. Kubuntu distributions are bundled with KDE; you can install KDE from other distributions by using this command:

```
sudo apt install kubuntu-desktop
```

To install Mate Desktop, use this command:

```
sudo apt install ubuntu-mate-desktop
```

These commands are provided as a convenience; there is no requirement for KDE or Mate Desktop. Any desktop environment will work.

- The desktop machine meets the client's requirements.
- You have super user (root) privileges and are able to issue `sudo` commands.
- A graphical environment has been installed/configured on the Software Client system by running the following command:

```
sudo systemctl get-default  
graphical.target
```

Installing the Anyware Software Client for Linux

1. Install the Software Client for Linux repository, using the script on our [download site](#).

teradici-repo Package

If you do not install the teradici-repo package then you will not be able to successfully install the Anyware Software Client. You may be experiencing this issue if you see an error message stating **Unable to locate Anyware-client**. Please ensure you download and install the repo.

2. Install the Anyware Software Client for Linux by running the following command:

```
sudo apt install pcoip-client
```

3. Launch the *pcoip-client* to create default configuration files and then quit the client.

Refer to the reference section for additional information, such as [Disabling the Virtual Terminal Functionality](#) and configuring [Linux Keyboard Shortcuts](#).

Installing the Software Client in Silent Mode

To install the Software Client for Linux in silent mode, use the following command:

```
sudo apt install -y <pcoip-client deb package>
```

Important: Post Installation Configuration

After the installation completes, [tune the kernel networking configuration](#).

Kernel Network Configuration

The `pcoip-configure-kernel-networking.sh` script is installed with the Anyware Software Client for Linux. This script tunes the kernel networking configuration to facilitate the network performance required by the Client. You need to run this script after installing the Anyware Software Client for Linux.

- To do that run the following command:

```
sudo pcoip-configure-kernel-networking --persistent
```

The script contains the following parameters:

- `rmem_max`: A kernel parameter that controls the maximum size of receive buffers used by sockets.
- `rmem_default`: A kernel parameter that controls the default size of receive buffers used by sockets.
- `ipv4_udp_mem`: A kernel parameter that controls the maximum total buffer-space to allocate.
- `netdev_max_backlog`: A kernel parameter that controls the maximum size of the receive queue.

`rmem_max` size

This parameter must be at least as large as `rmem_default` /

The values of these parameters can be viewed on the command line when the script is run, as outlined in the example below:

```
# cat /etc/sysctl.d/01-pcoip-client.conf
net.core.rmem_max = 32000000
net.core.rmem_default = 32000000
net.ipv4.udp_mem = 1000000 2000000 4000000
net.core.netdev_max_backlog = 2000
```

Downloading the Anyware Client Update

Anyware Clients are equipped to check for new updates and send notifications that appear as banners if an update is available. Clicking the banner redirects to the product download page, from where you can download the client installer.

1. Open Anyware Client, and click the Info icon in the top-left corner.
2. On **Anyware Client | About** pop-up, check if an update is available.
3. If an update is available, the **Update now** link will appear. Click this link to go to the product download page.
4. Proceed with installation of the client as described in the **installation topic**.

Note: More About the Update

If the client is up to date, the **Release notes** link becomes available on the **Anyware Client | About** pop-up dialog. If the client is unable to access an update, the **Try again** link will appear on the **Anyware Client | About** pop-up dialog.

Upgrading the Anyware Software Client

Updates to the Anyware Software Client for Linux are published on a regular basis.

To upgrade to the latest version, use the following two commands:

```
sudo apt update
sudo apt install pcoip-client
```

Upgrading the Anyware Software Client in Silent Mode

1. [Uninstall the current version.](#)
2. Install the client by using the following command:

```
sudo apt install -y <pcoip-client deb package>
```

Uninstalling the Anyware Software Client

This section contains instructions for uninstalling the Linux client as well as removing the repo configuration. You might need to remove the repo completely if you are switching from one channel to another (for example, from beta to stable), before reconfiguring with the new repo.

Uninstallation Steps

1. Run the following command:

```
sudo apt remove pcoip-client
```

2. Remove the Software Client for Linux from your system, or [remove the repo config entirely](#).

Removing Deprecated Repos

Software Client for Linux repositories were formerly hosted at `downloads.teradici.com`. This server is deprecated, and requests to it will fail with a certificate error.

If your repo config is pointing at this deprecated server, you must remove references to it and then configure your system with the new server.

1. Search for `downloads.teradici.com` in `/etc/apt/sources.list.d/` and delete them.

```
grep downloads.teradici.com /etc/apt/sources.list.d/*
```

The response will contain the files that need to be removed.

2. Remove the outdated files. The following example will remove the `pcoip.list` file at `/etc/apt/sources.list.d/pcoip.list`; the value you use here will be found in the response to the previous step:

```
sudo rm /etc/apt/sources.list.d/pcoip.list
```

3. Remove any references to `downloads.teradici.com`. Search for `downloads.teradici.com` in any files in `/etc/apt/sources.list.d/` and delete these files. Run the following command:

```
$ grep downloads.teradici.com /etc/apt/sources.list.d/*  
/etc/apt/sources.list.d/pcoip.list:deb [arch=amd64] https://  
downloads.teradici.com/artifactory/pcoip-agent-deb-stable-local bionic  
stable  
username@ABCDEF1:~$ sudo rm /etc/apt/sources.list.d/pcoip.list
```

pcoip.list is an example filename that may be captured with the `$ grep` command.

4. Once the legacy file is removed refresh the repository cache.

```
$ sudo apt-get update
```

Connecting

Connecting to an Agent Machine

The Software Client for Linux can connect to any remote host with a Anyware agent installed and configured, or a Remote Workstation Card. Remote hosts can be Windows, macOS, or Linux, and connections can be made directly (client direct to host) or brokered through Anyware Manager or a Connection Manager.

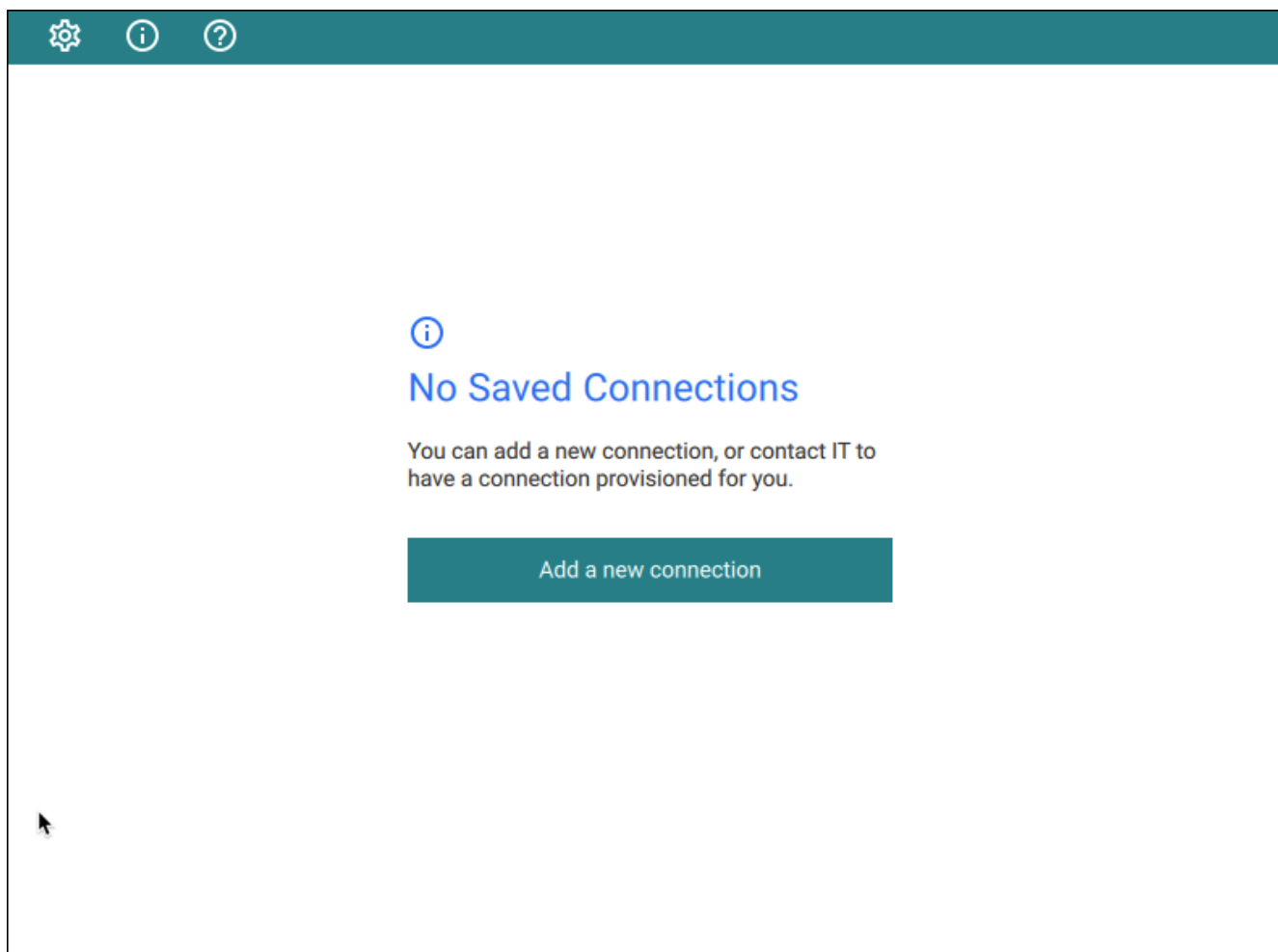
 **Note: Remote Workstation Card connections**

Connections to 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

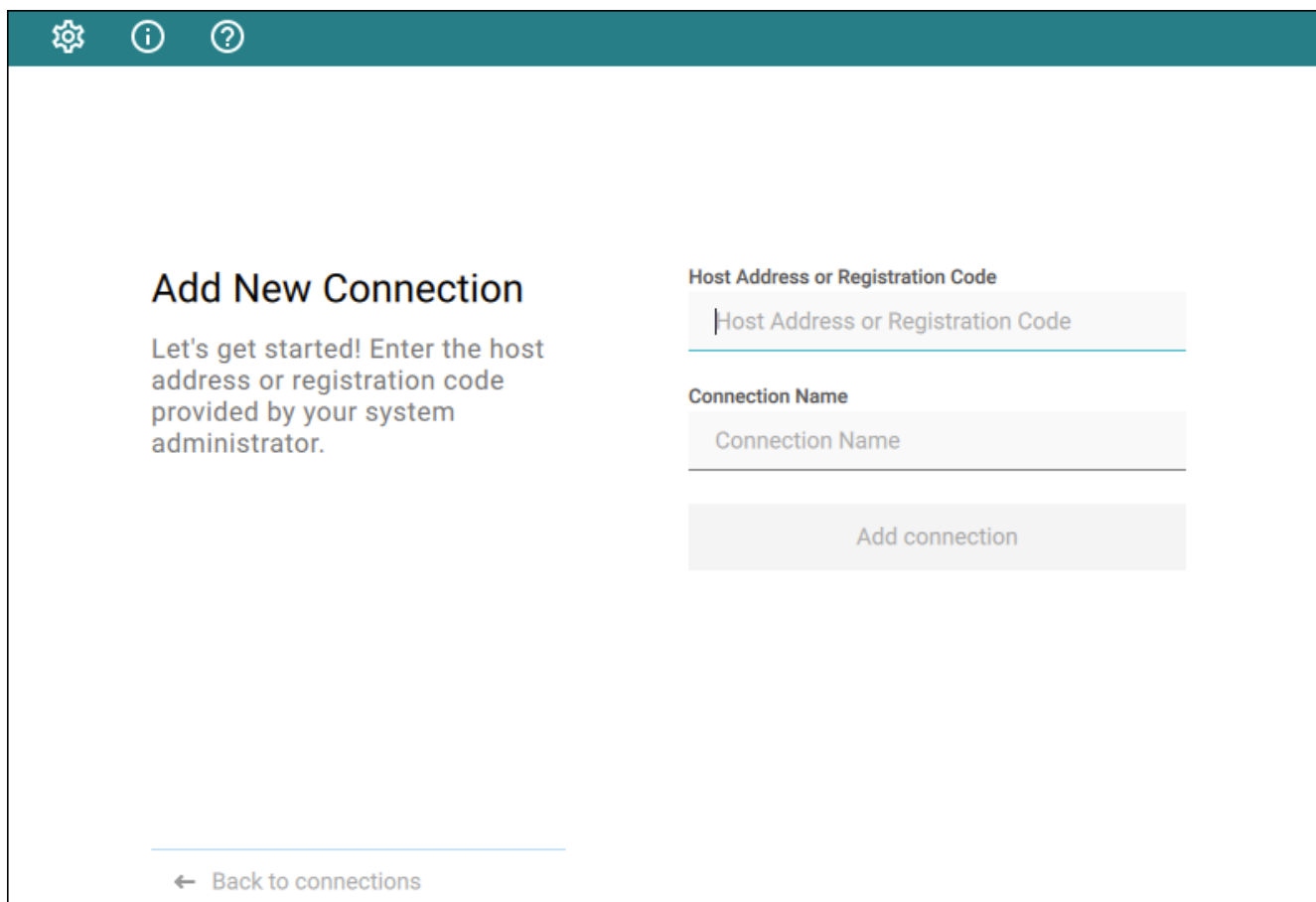
The first step is to create a *connection* to either your agent (for direct connections) or to your connection manager (for managed deployments).

1. Launch the Software Client for Linux.
2. If this is your first connection, the Software Client for Linux 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

Host Address or Registration Code

Connection Name

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.

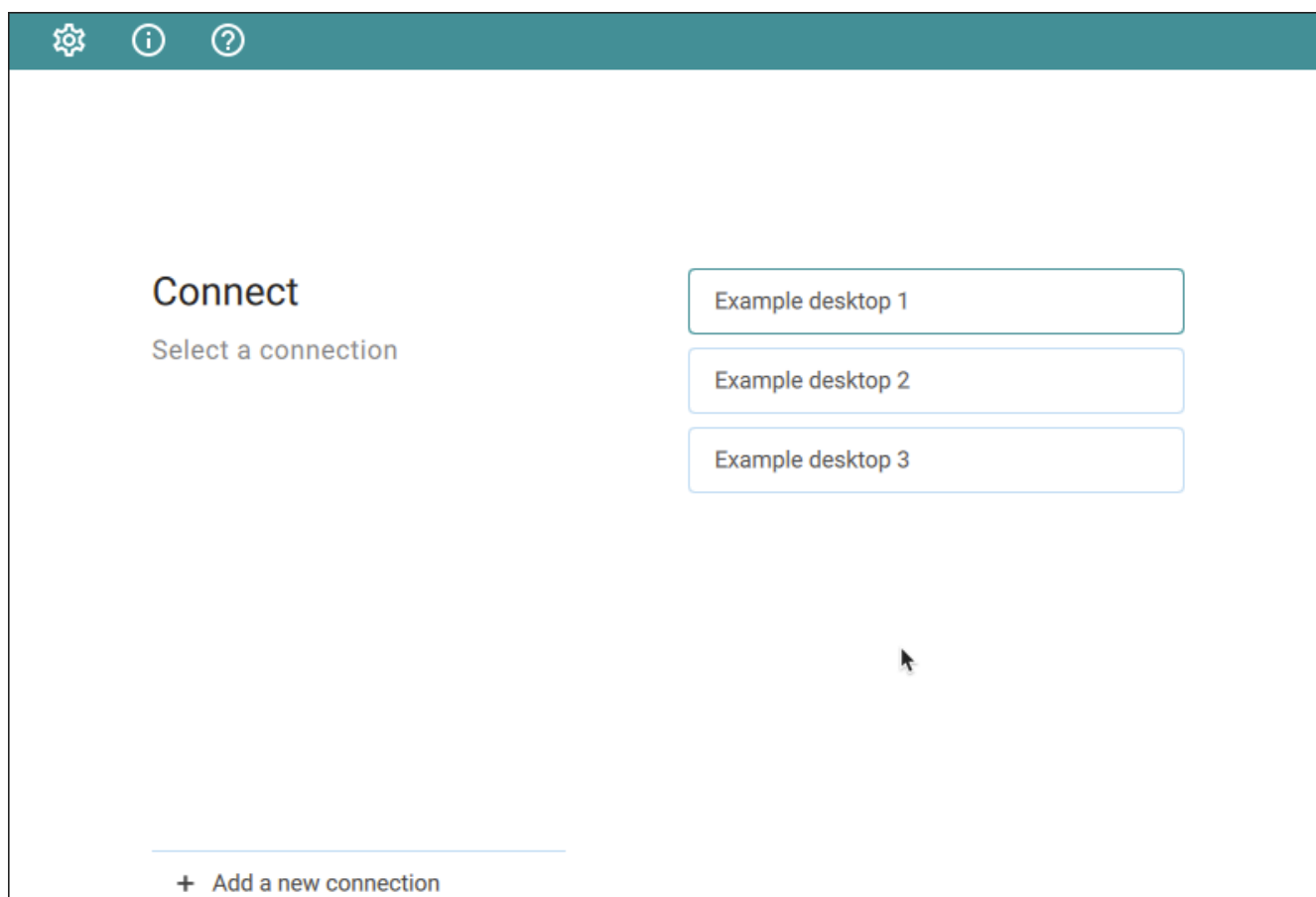
Tip: Difference from previous workflows

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.

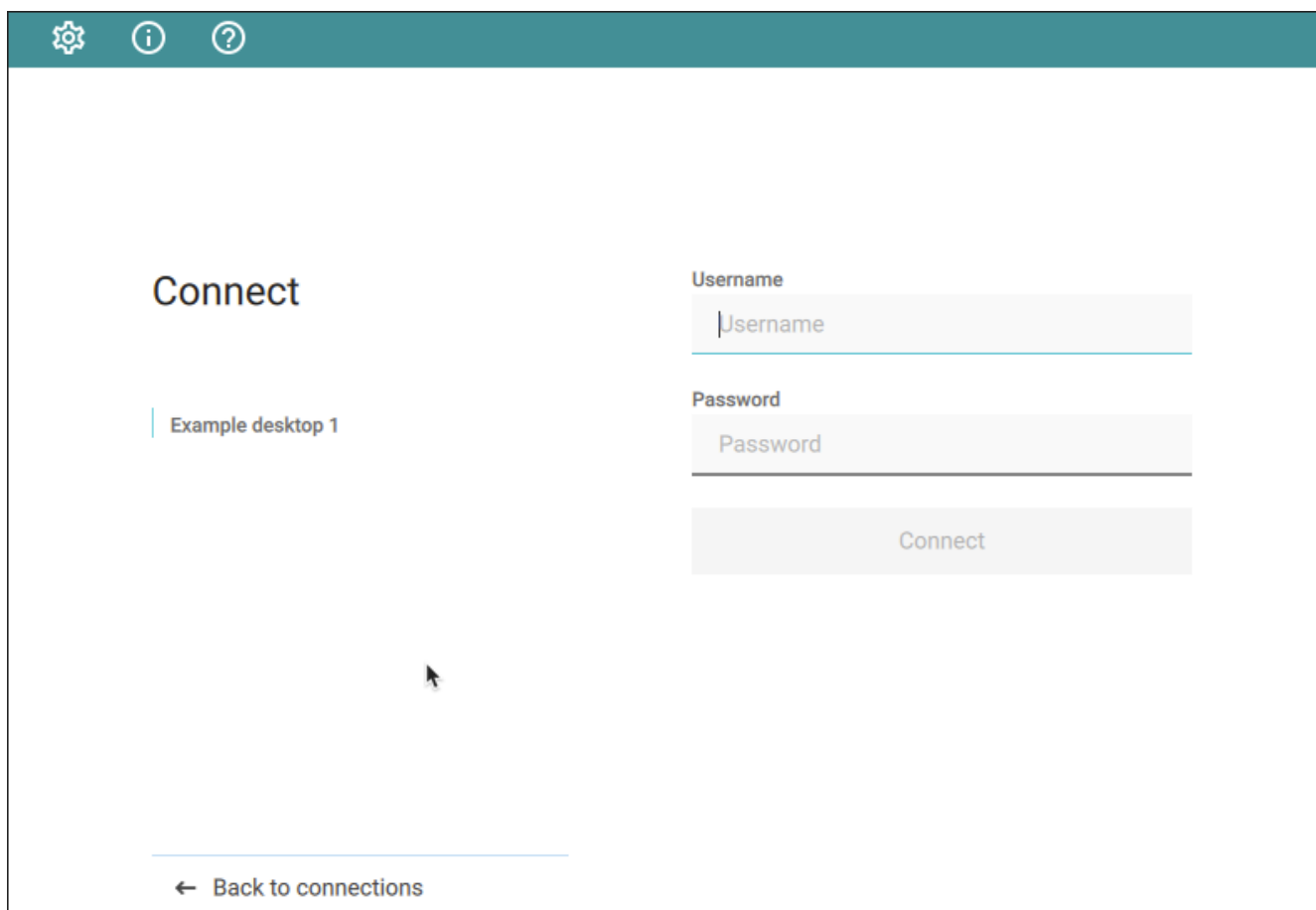
If you have existing saved connections from previous releases, they will continue to work when you upgrade to this client version. However, if they are deleted, they cannot be re-created.

Connecting to a Session

1. Assuming you have created at least one connection, the Software Client for Linux 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 user interface for connecting to a session. At the top, there is a teal header bar containing three icons: a gear for settings, an 'i' for information, and a question mark for help. Below the header, the main content area is titled "Connect". On the left side, there is a list of connections, with "Example desktop 1" selected. On the right side, there are two input fields: "Username" and "Password". Below these fields is a "Connect" button. At the bottom left, there is a link that says "← Back to connections".

 **Note: About authentication credentials**

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

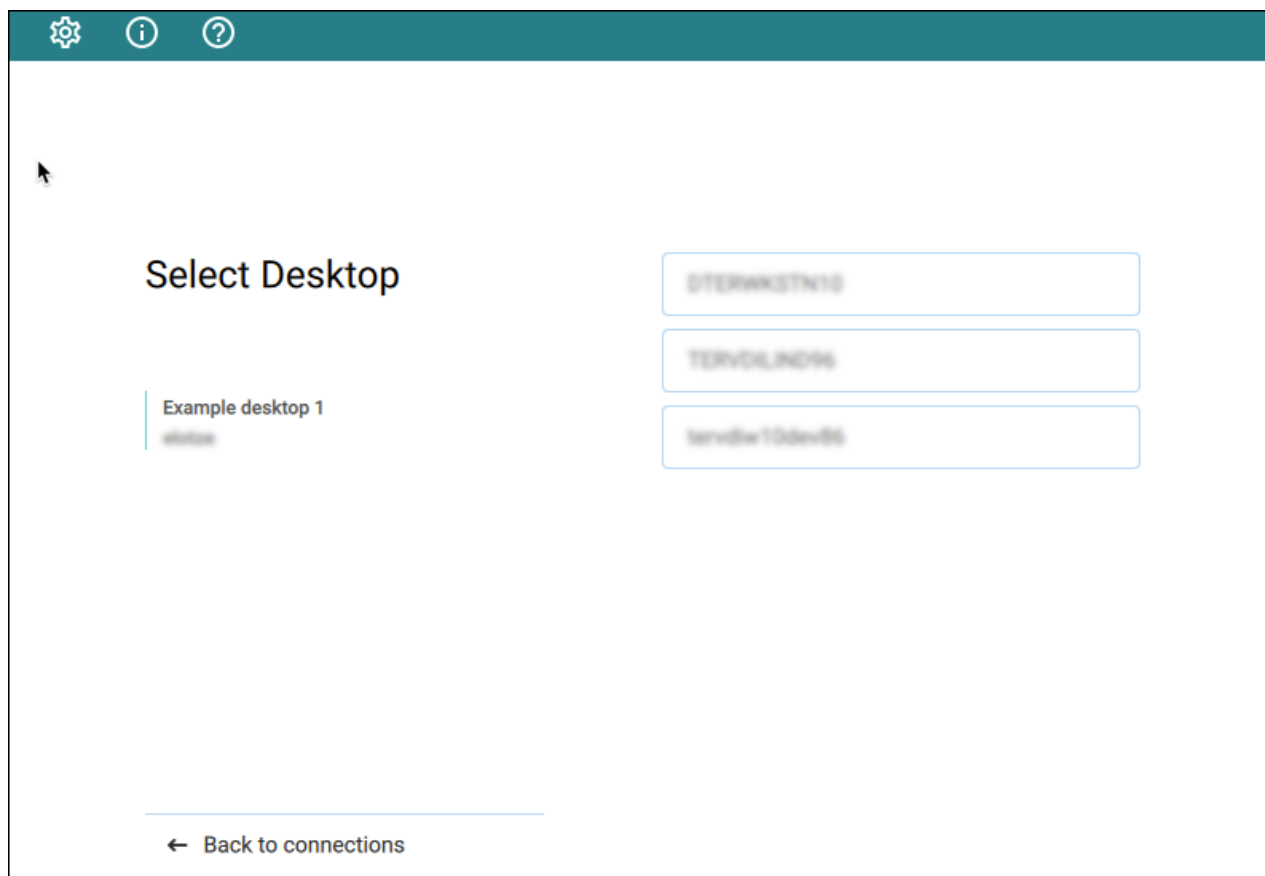
For **direct connections** where no broker is present, use the credentials for your user account on the remote machine.

3. If your system is configured for multi-factor authentication, you will see a *Multi-Factor Authentication* screen next. The actual view shown here depends on your MFA implementation; in this example, the MFA screen accepts a passcode or sends a push:

The screenshot shows a web interface for Multi-Factor Authentication. At the top, there is a teal header bar with three icons: a gear (settings), an 'i' (information), and a question mark. Below the header, the main content area is white. On the left, the text 'Multi-Factor Authentication' is displayed in a large, bold font. Below this, there is a list of desktops, with 'Example desktop 1' visible. On the right, there is a 'Passcode' input field with a light gray background and a teal border. Below the input field is a 'Submit Passcode' button. Underneath the button is the text 'or' flanked by horizontal lines. Below that is a teal button labeled 'Send Me a Push'. At the bottom left, there is a link with a left-pointing arrow and the text 'Back to connections'.

4. Once your credentials are accepted:

- **If you have a single desktop** available, your connection credentials will be used to automatically log into it and your session starts immediately.
- **If you have multiple desktops** available, the Software Client for Linux shows you a list of desktops. Click the desktop you want to connect to.



Once you are connected, 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.

Managing Connections

1. On the **Saved connections** window, click the vertical ellipsis next to the connection to reveal the context menu.
2. To rename the connection, select **Edit**.
3. Update the **Host Address or Registration Code** or the **Connection Name** as necessary.
4. Click **Save**.
5. To delete the connection, from the context menu, click **Delete**.

Note: More About the Manage desktops option

The **Manage desktops** option in the context menu is used to rename desktop labels and restart desktops in scenarios where **a single desktop** is associated with a connection. For more information, see [Changing remote desktop labels](#) and [Restarting remote desktops](#).

Managing Desktops

You can manage the desktops belonging to each of your defined connections. The following actions are available, when supported by the desktop:

- [Rename](#) the desktop's label in the client.
- [Restart](#) the remote desktop (if supported).
- [Display information](#) about the desktop, including its resource name and protocol.

To use these features, first display the list of desktops belonging to the connection, then select the action you want from the available desktops. These procedures are described next.


Display the List of Desktops

Desktop management options require you to authenticate with the connection that owns them.

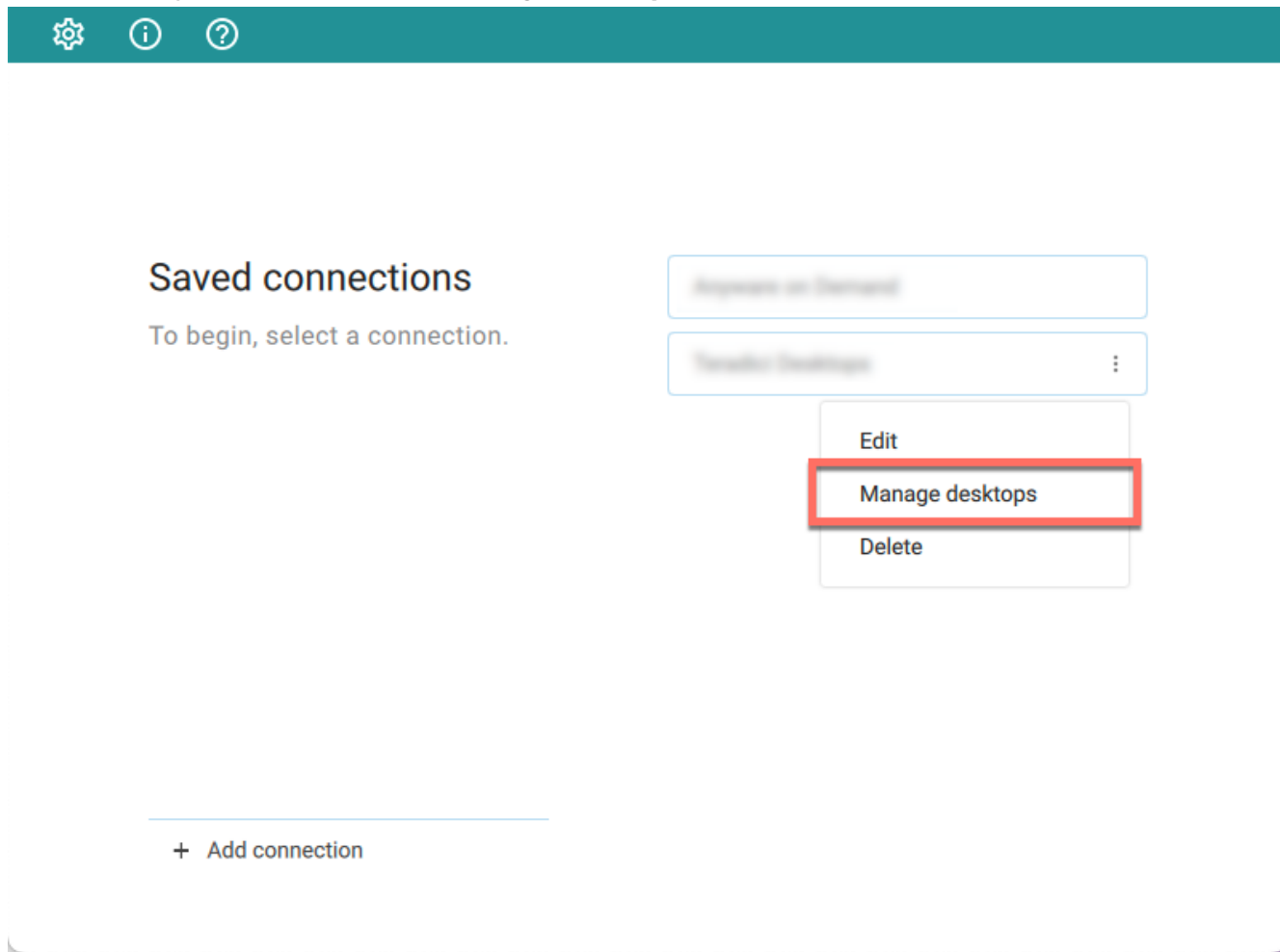
Tip: Connections with multiple desktops

If you have multiple desktops, you can also click on a connection directly instead of following the procedure shown here. Single-desktop users are not shown a desktop list after authenticating, and must follow this procedure to manage their desktop.


To access the desktop management options:

1. From the list of connections, click the vertical expansion icon  beside the connection you want to work with.

2. From the dropdown menu, click **Manage Desktops**:



You will be asked to authenticate with the connection.

Once authenticated, you will see the list of desktops belonging to the connection. To manage one of the desktops, click the vertical expansion icon  beside the *desktop* you want to work with, and choose one of the following options.

Rename a Desktop

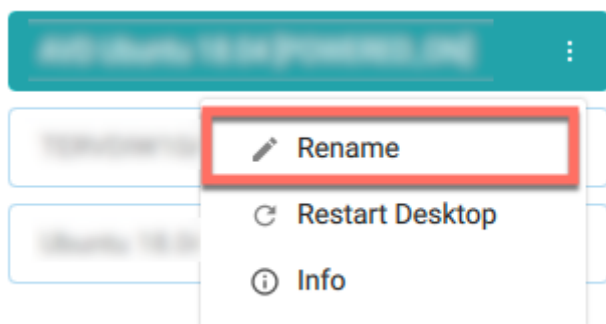
By default, the Software Client for Linux displays the *machine names* of your remote desktops. These names can often be automatically-generated strings that are difficult to identify or differentiate. You can modify the name shown in the desktop list to give them human-friendly names that are easier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

Note: Only labels are changed

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

To change a desktop label:

1. Display the desktop list as described [above](#).
2. Click **Rename**:



3. Provide a new name to use in the desktop list. Note that once this is done, the default machine name will no longer be visible; if you need to see it later, see [View Desktop Information](#).

Restart a Desktop

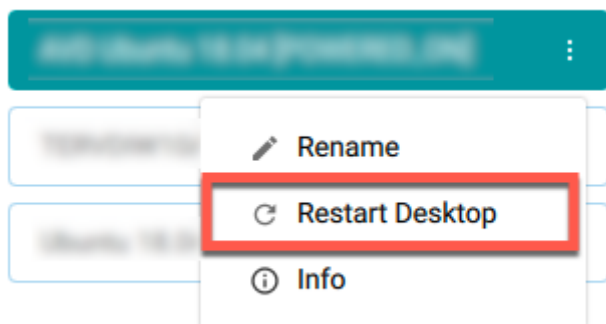
You can send a restart command to a remote desktop from the client interface, if supported by your remote system.

Note: Not all deployments support this feature

The restart option is only be available if your remote system supports it. If it does not, the option will be disabled.

To restart a remote desktop:

1. Display the desktop list as described [above](#).
2. Click **Restart Desktop**:



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

View Desktop Information

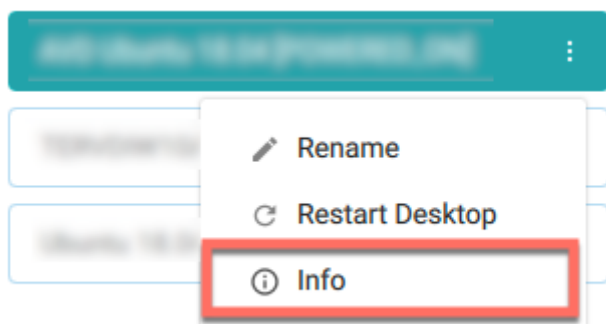
You can view detailed information about each of your available remote desktops, including resource names, IDs, and protocols.

Tip: Desktop machine names

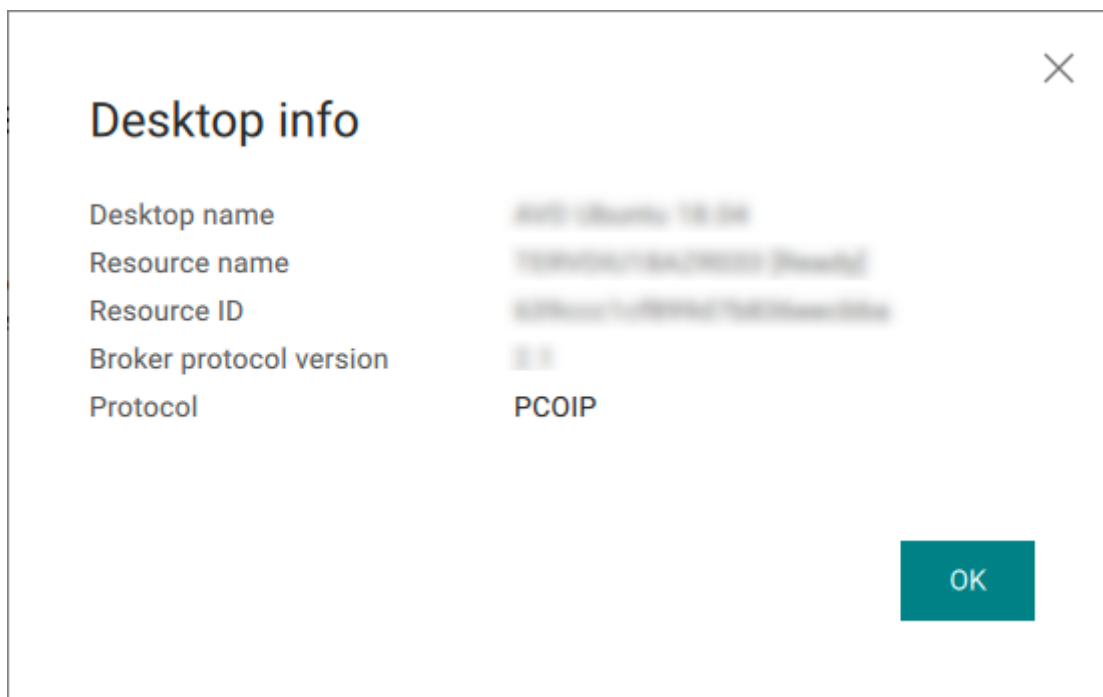
If you have [renamed a desktop](#), the original machine name is the *resource name* shown here.

To view desktop info:

1. Display the desktop list as described [above](#).
2. Click **Info**:



3. Review the displayed information.



4. To dismiss the info window, click **OK** or click the close button in the top corner.

Some Keystrokes Will not Be Interpreted Correctly

Keystrokes of special keys sent by clients might not be interpreted correctly by agents. This happens when the clients and the agents are running different operating systems, and the special keys are unique to the operating system of the clients. For example, the Numlock keystroke sent by a Windows client does not work on a macOS agent. This is by design.

Note: Troubleshooting PCoIP Session Connection Issues

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

Using Smart Card Authentication to Connect to a Session

Anyware Linux Client supports smart card authentication, provided that:

- The client connects to a Windows Graphics Agent or a Windows Standard Agent, and
- The client machine as well as the agent machine are running version 24.03 or later.

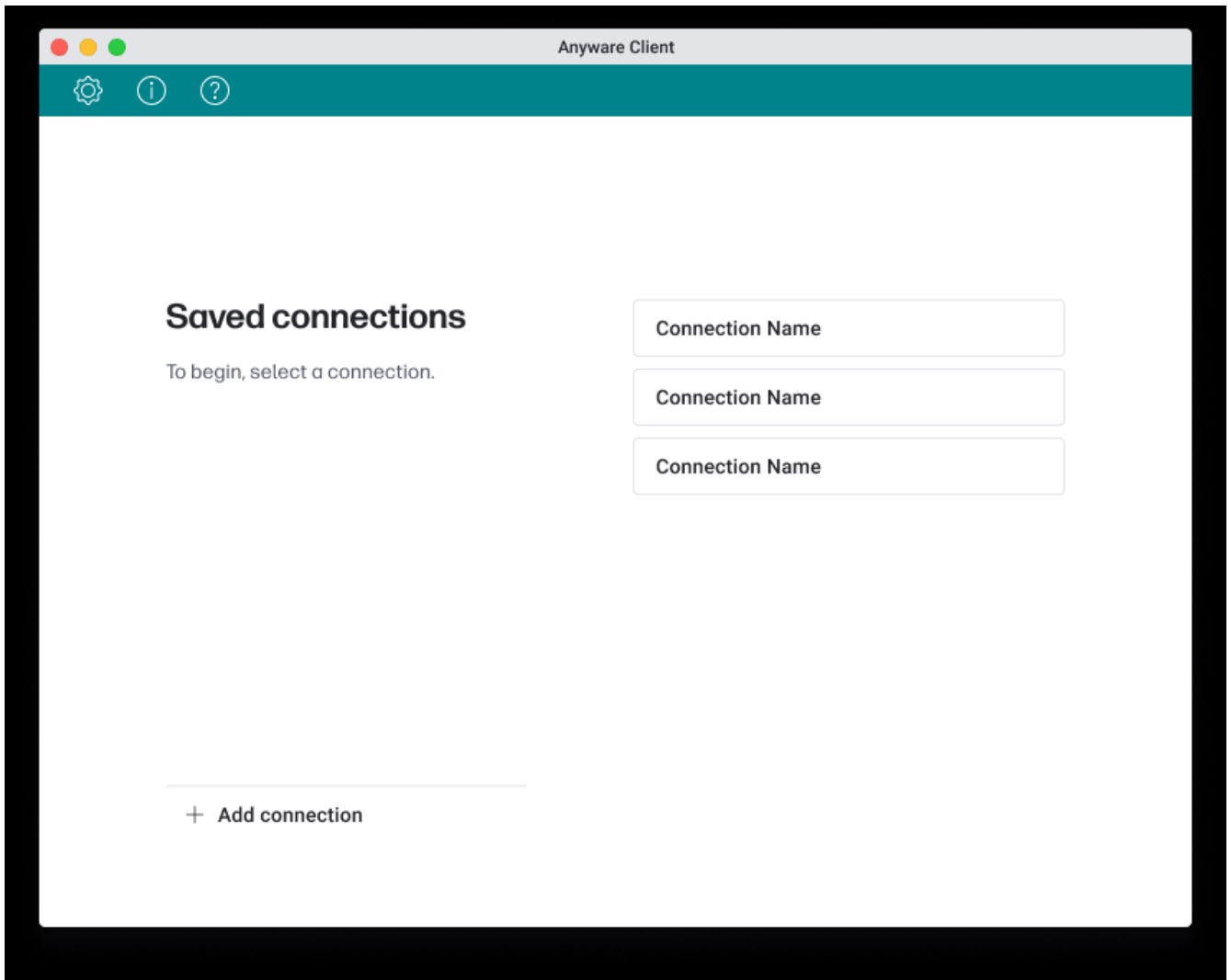
Additionally, you must use a combination of [supported smart cards and readers](#) in your deployment.

Note: Concurrent Users Cannot Logon

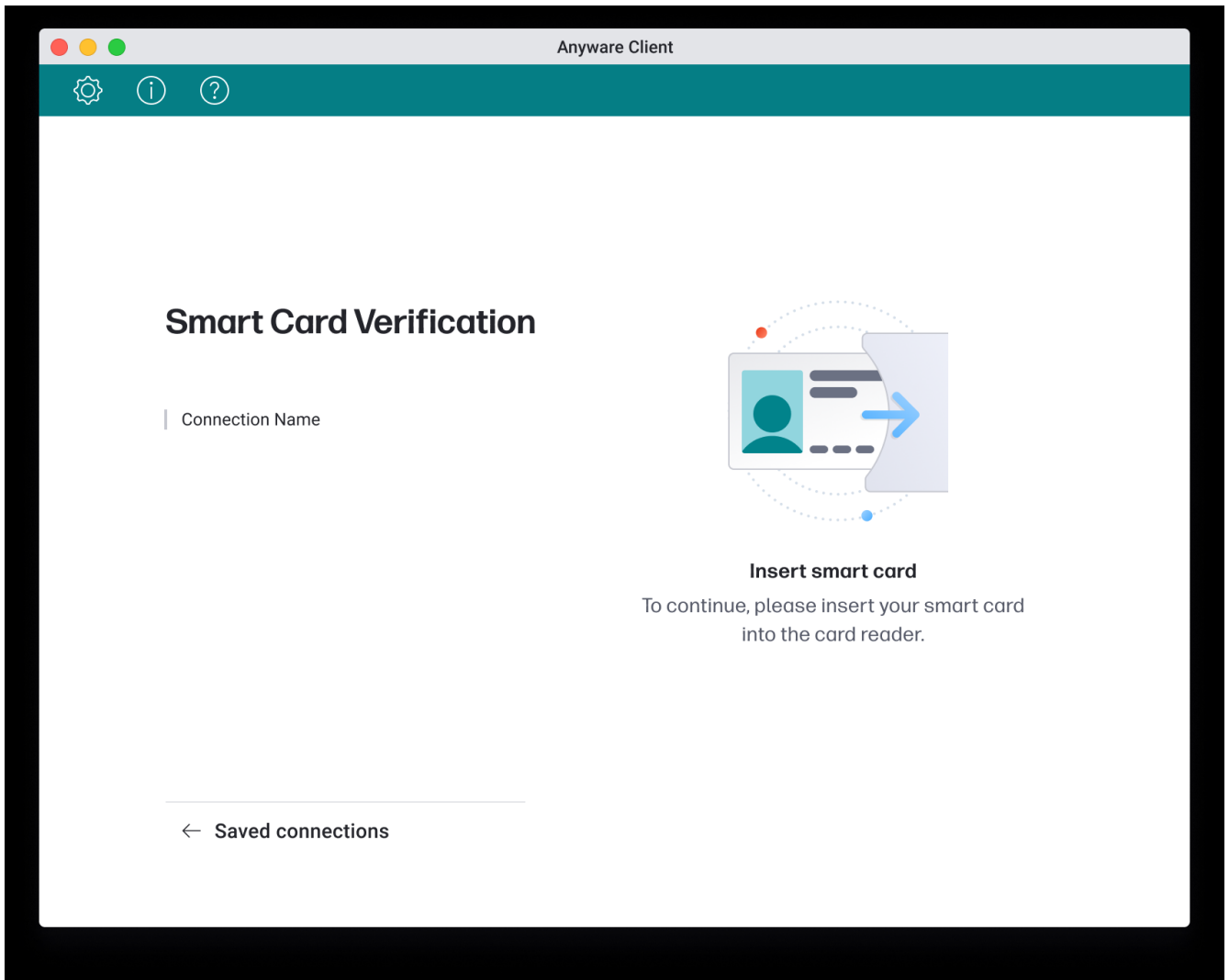
Concurrent users cannot log on to agent machines using the same smart card for authentication. Smart cards having multiple certificates allow only one user to log on at a time. To be able to log in, other users must wait until the current user logs off.

To use a smart card for authentication:

1. Attach the smart card reader to the Anyware Linux Client.
2. Launch the Software Client for Linux.
3. On the **Saved Connections** window, select a connection.

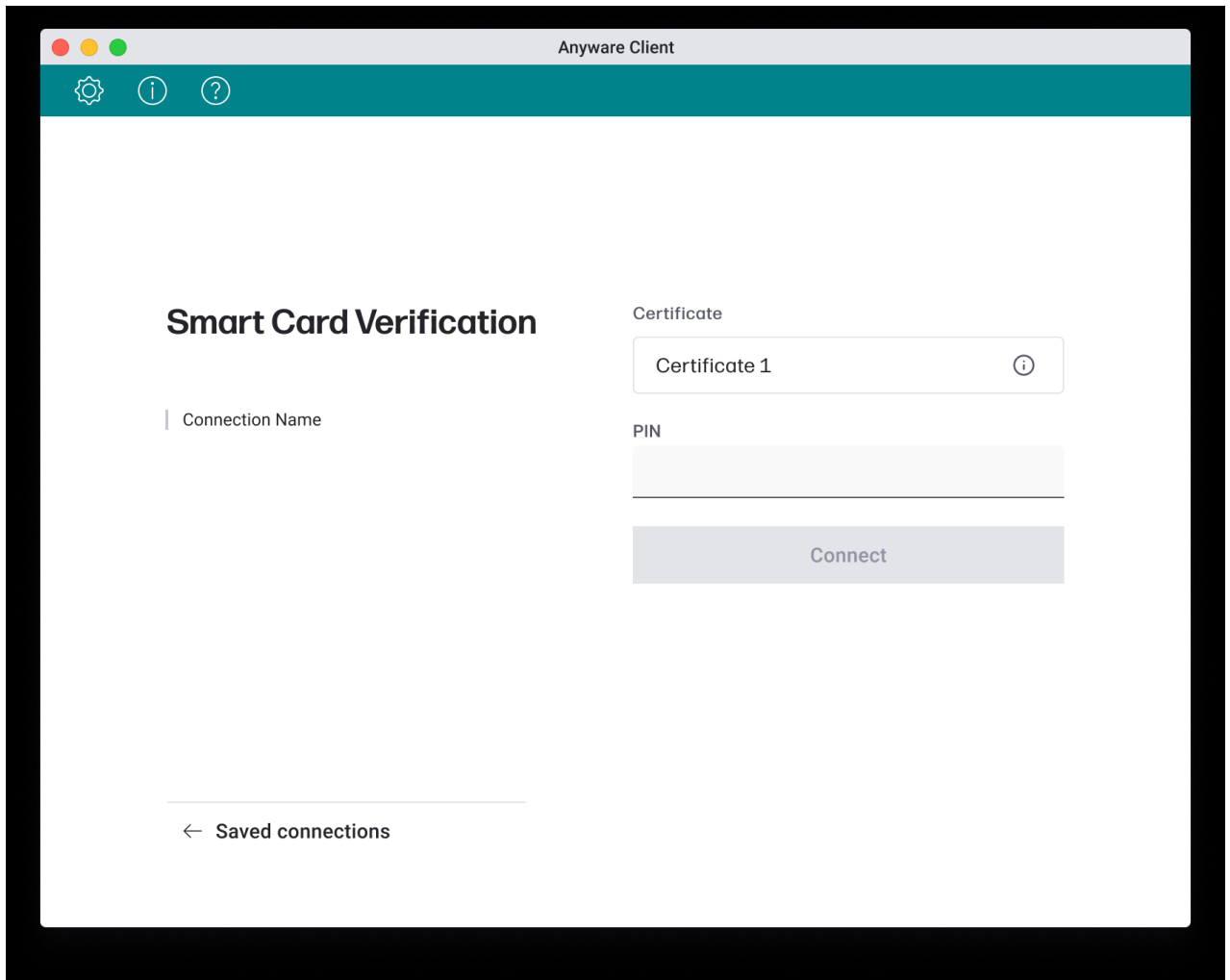


4. When the **Smart Card Verification** window appears, insert your smart card and wait until it is verified.

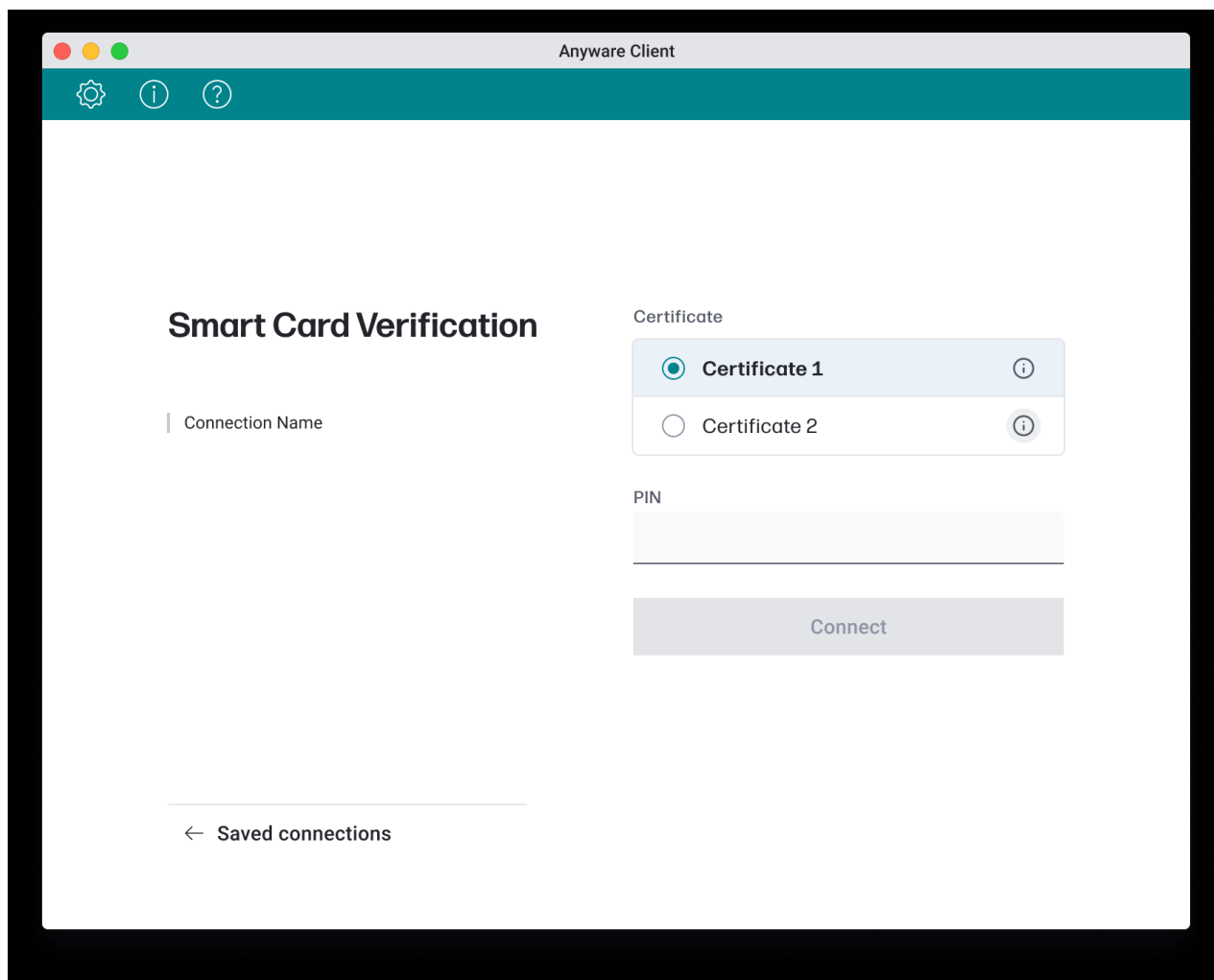


5. Do one of the following:

- If the client detects **only one certificate**, provide the smart card PIN and click **Connect** on the **Smart Card Verification** window.



- If the client detects **multiple certificates**, on the **Smart Card Verification** window, select a certificate, provide the smart card PIN, and click **Connect**.



6. On the **Desktop Selection** window, select a desktop and connect to this session.

Note: Removing the Smart Card During Session

Removing the smart card while in session will end the session. However, the smart card will continue to be available on the client machine.

Viewing Certificate Information

You can view detailed information about each of the certificates detected by the client, such as certificate authority, certificate recipient, certification path, and certificate properties.

To view certificate information:

1. Launch the client, select a connection, and insert your smart card. Wait until it is verified.

2. From the [available certificates](#), select one for which you want to view details.

Information related to the certificate is displayed on the **Certificate details** window under the following tabs:

- **General:** Contains general information such as certifying authority, validity, and certificate recipient.
- **Details:** Contains details about the properties of the certificate such as key usage, thumbprint, and subject alternative name.
- **Certification Path:** Contains information about the certification path of the certificate.

Preparing for Remote Workstation Card Connections

You can connect to remote workstations equipped with a Remote Workstation Card, and with 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 Remote Workstation Card**

Before you install the Remote Workstation Card, **record the MAC address of the 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 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 Remote Workstation Card, such as the MAC address. The MAC address enables you to connect to the 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 Remote Workstation Card, see [How do I find the IP address of my newly installed Anyware Zero Client or Remote Workstation card?](#) in the knowledge base.

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

- **Disable temporal dithering:** Temporal dithering causes blurriness, heavy packet loss, and high CPU usage on the Anyware Software Client machine.
- **Linux workstations: configure Remote Workstation Card Software to Start Automatically:** To configure the Remote Workstation Card Software to start automatically, log into the workstation using a Anyware Zero Client or directly from a local mouse and keyboard, and modify the workstation startup script to launch the Remote Workstation Card Software. For details, see Installing 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 Linux to connect to it.

Connecting to a Remote Workstation Card through the command line

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

Remote Workstation Card Limitations

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

Audio: 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 Remote Workstation Card does not support the display configuration on the client.

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

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

Connecting Remotely using NAT or VPN

The same principles that apply for Anyware Zero Clients apply to Anyware Software Clients when connecting to multiple hosts through a WAN. Connections from a Anyware 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 Anyware Software Client to a Remote Workstation Card installed in a Windows host computer, see [Connections from Software Clients](#) in the 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 Linux menu bar by moving the mouse cursor to the top of a display.
2. From the Software Client for Linux menu bar, select **Connection > Disconnect**.

To quickly disconnect from a session, press **Ctrl + Alt + F12**. On Mac machines, press **Ctrl + Option + F12**.

Tip: Mac Laptops Might Require Additional Key Press

On Mac laptops, you might need to press the **Fn** key, along with **Ctrl + Option + F12**.

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

In-session actions

Using Displays

When you connect to a PCoIP session, the Software Client for Linux 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 Linux 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 Linux, 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 Linux 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 Linux menu bar by moving the mouse cursor to the top of a display.
2. From the Software Client for Linux menu bar, select **View > Leave Fullscreen**.

Full Screen Modes

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

In both full-screen modes, the Software Client for Linux 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 Linux menu bar by moving the mouse cursor to the top of a display.
2. From the Software Client for Linux 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 Linux menu bar by moving the mouse cursor to the top of a display.
2. From the Software Client for Linux 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 Linux menu bar by moving the mouse cursor to the top of a display.
2. From the Software Client for Linux 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 Anyware Agent configuration:** The remote Anyware 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 Linux 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:** Anyware 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 Anyware 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.

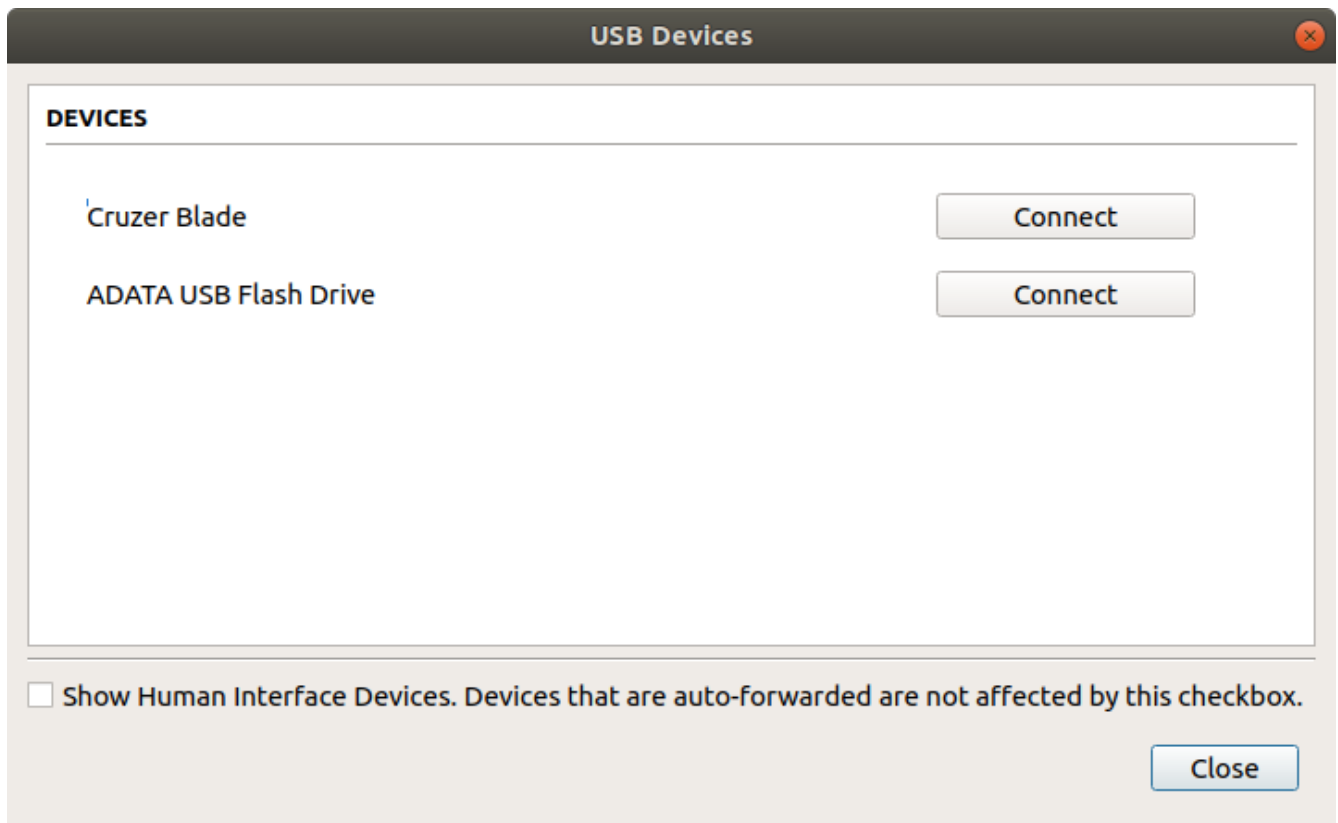
The name shown in the list is self-reported by the device; some devices will identify themselves only as *USB Device*.

Important: Connecting special HID devices

Because most Human Interface Devices (HIDs) are automatically processed by the Software Client for Linux, 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.

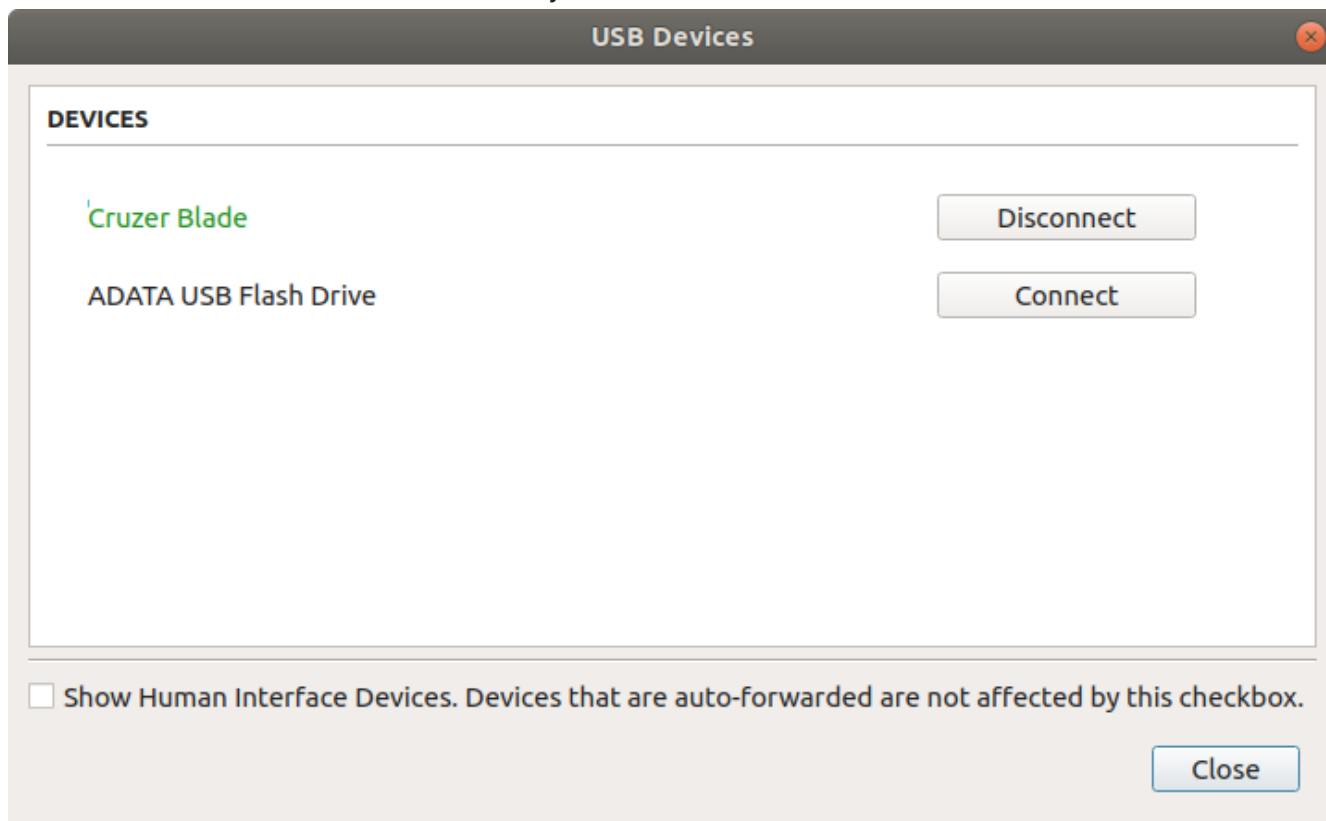
3. Click **Connect** beside the USB device you want to use.



Disconnect a USB Device

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

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



Automatically Forward All USB Devices

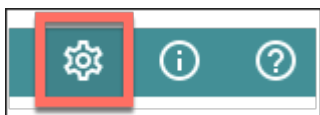
Automatic forwarding allows you to bridge all non-HID USB devices without requiring a manual connection step.

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

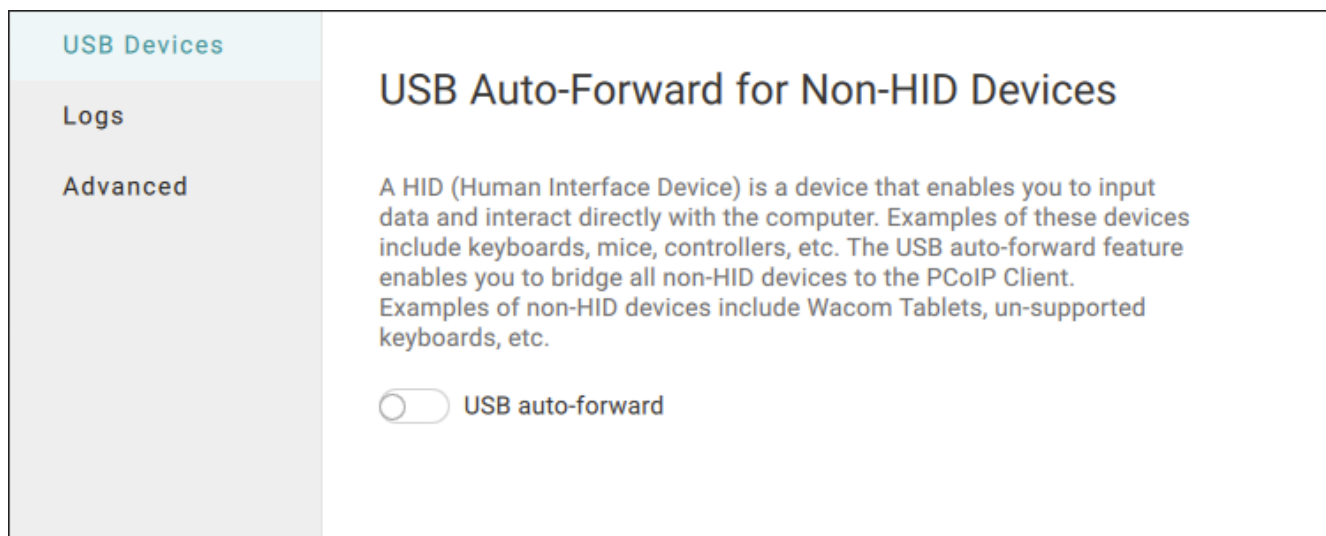
Devices that are automatically forwarded can still be disconnected and reconnected via the Software Client for Linux interface.

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 Linux 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 Linux.
3. Plug in the device.
4. Close the Software Client for Linux.
5. [Find the most recent Anyware 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.

Configuring Wacom Tablets

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

USB Connection Instructions

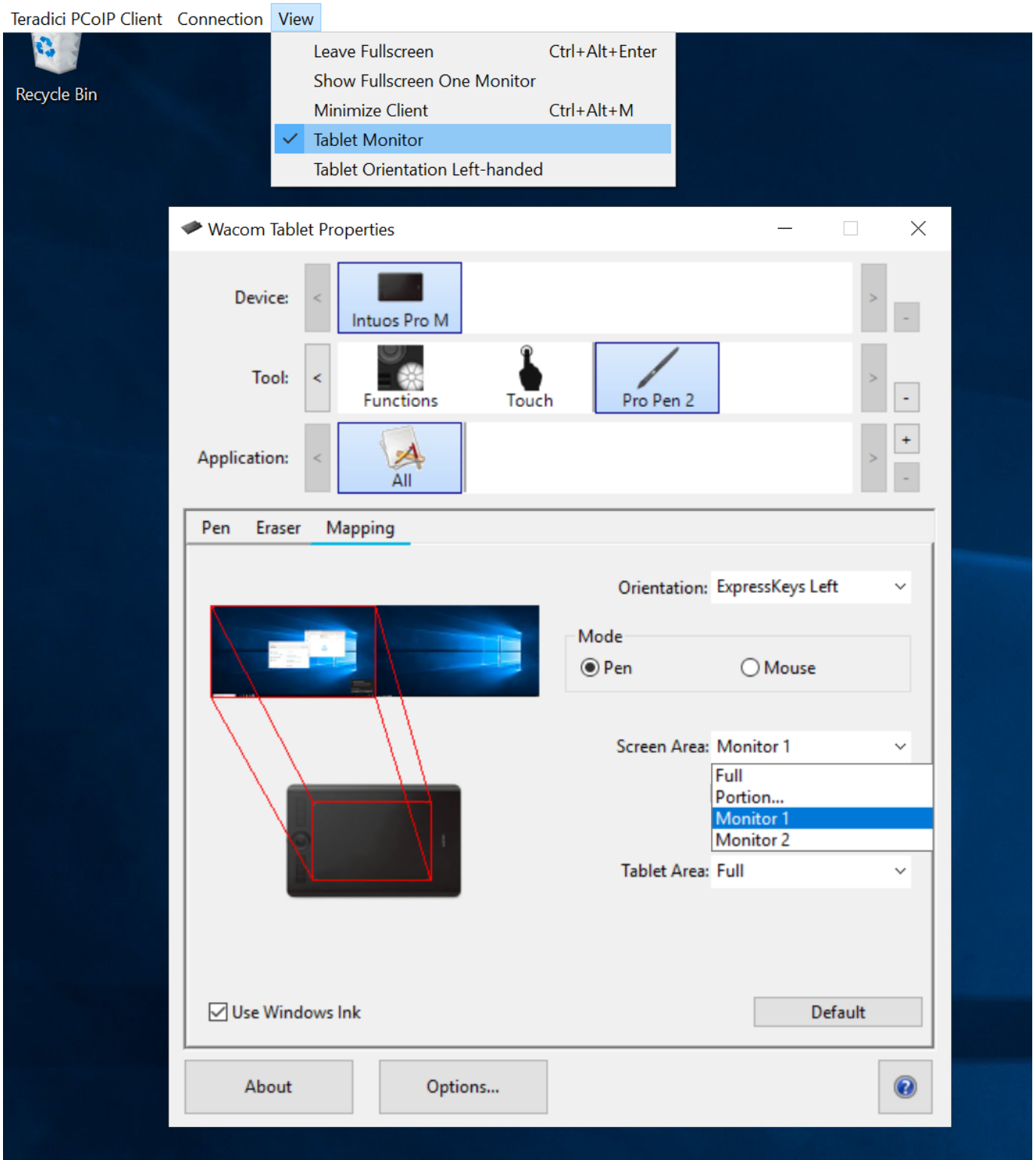
Before you carry out the Wacom tablet monitor configurations below, you must connect to the device by following the instructions outlined in the [Connecting to USB Devices](#) section.

Wacom Tablet Monitor

The 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.



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

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

Wacom Tablet Properties

Device: Intuos Pro M

Tool: Functions Touch Pro Pen 2

Application: All

Pen Eraser Mapping

Orientation: ExpressKeys Right

Mode: Pen

Screen Area: Monitor 1

Force Proportions

Tablet Area: Full

Use Windows Ink

Default

About Options...

Enhanced Audio and Video Synchronization

Enhanced Audio and Video Synchronization 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.

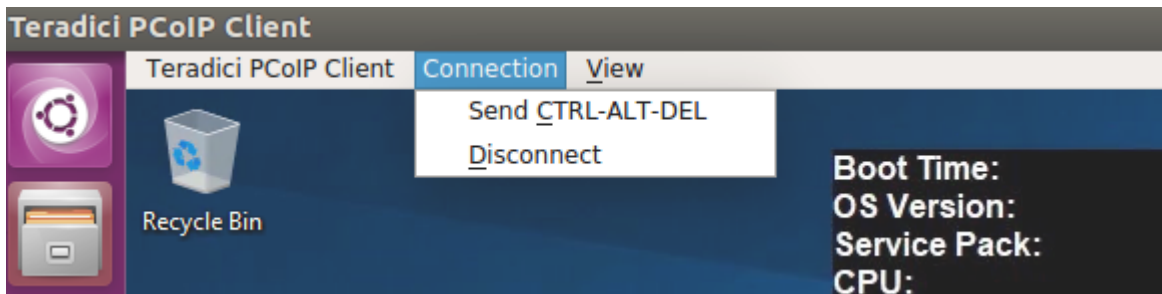
PCoIP Ultra AV-Lock

PCoIP Ultra AV-Lock enables regulated synchronization of audio and video frames. When audio is playing the video frames will be delayed to align with the audio sound track. When there is no audio playing the video frames will be presented to the user without delay. For some use cases, such as video editorial, audio video synchronization is critical and must be tolerant of variable network conditions that may be present with remote work.

PCoIP Ultra AV-Lock enables more regulated synchronization of audio and video frames compared to Enhanced AV Sync described above. PCoIP Ultra AV-Lock is available with PCoIP Ultra CPU Offload, GPU Offload or Auto Offload. You must enable the High Performance Client mode for this feature to function correctly, for information on this, see [High Performance Client](#).

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.



Configuration Guide

Configuring the Anyware Software Client for Linux

The Software Client for Linux 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
- [Via a URI](#), providing your configuration values in an encoded JWT string
- [via Config files](#), where advanced configuration values are set via configuration files

Note: Configuration Methods

Not all options available via the configuration methods are the same. Some might also have different names.

Setting Configuration Values on the Command Line

To set configuration values this way, launch the Software Client for Linux 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):

```
/usr/bin/pcoip_client --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 Linux 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 Linux.
<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.eyJmdWxsc2NyZWVuIjp0cnVlLCJsb2ctbGV2ZV
```

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

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 Linux when it launches.

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 Location

The `.ini` file is located in the `~/config/Teradici/Teradici PCoIP Client.ini` folder.

The configuration file does not exist until a user changes a persistent setting via the user interface. If that has not occurred, you must create the file.

Configurable Settings

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

General Settings

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

LANGUAGE

Sets the user interface language.

Options	Default	Type
Interface language	English	string (short code or ISO code; see next table for options)

Supported language options:

Language	Short code	ISO code
Chinese Simplified	cn	zh_CN
English	en	en_US
French	fr	fr_FR
German	de	de_DE
Italian	it	it_IT
Japanese	ja	ja_JP
Korean	ko	ko_KR
Portuguese (Iberian)	pt	pt_PT
Spanish	es	es_ES

Usage

Method	Valid	Full	Alias	Example
Command Line	✓	<code>--locale</code>	—	<code>--locale zh_CN</code>
URI	—	—	—	—

If the `locale` parameter is present but the argument is invalid or missing, the Software Client for Linux displays a *Parameter parsing error* and lists the valid settings, then exits (the client will not start).

Connection Settings

These settings control how the Software Client for Linux 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>--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.	—	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 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.	—	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	–	–	–	–

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	false (USB enabled)	boolean
<code>false</code> : enabled		

Usage

Method	Valid	Full	Alias	Example
Command Line	✓	<code>--disable-usb</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	False (do not auto-forward)	boolean
<code>False</code> : Do not auto-forward USB devices		

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>vbl</code>	<code>{vbl: "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>
URI	✓	<code>windowed</code>	<code>win</code>	<code>{win: true}</code>

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	✓	<code>--log-folder</code>	–	<code>--log-folder path/to/folder</code>
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	Not set	integer
1 : Error		
2 : Info		
3 : Debug		
4 : Verbose		

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 Linux. 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 Anyware 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 Anyware 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 Software Client for Linux. 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>	qad	<code>{qad: true}</code>

Note: Quit After Disconnect is Automatically Set

`Quit After Disconnect` is automatically selected when the following parameters are specified:

- Username
- Password
- Domain
- Connection Broker
- Desktop

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>

Securely Passing Parameters via the Command Line

In addition to passing arguments via the Command Line, you can also provide parameters via the standard input stream using the `--ask-extra-args-as-json` parameter. This approach is preferred when you want to pass sensitive data, such as user credentials, to the `pcoip-client` process. The `--ask-extra-args-as-json` parameter accepts arguments as JSON strings, thereby ensuring that user data is prevented from being recorded in the shell history.

To launch the client, using the `--ask-extra-args-as-json` parameter:

1. From the CLI, run the following command:

```
pcoip-client --ask-extra-args-as-json
```

2. When the following prompt appears, provide the required arguments as a JSON string:

```
Arguments should be specified with '-' prefixes and flags specified under a 'flags' section.  
For example: {"--username": "alice", "flags": ["--use-egl"]}  
For a more detailed description of the format, please see the help by using flag --help.  
Please enter extra arguments (as JSON):
```

These arguments are passed through the standard input of the `pcoip-client` process, and are not recorded in the command history or process list.

JSON String Format

The JSON string should consist of key value pairs, such that the keys are the names of the command line parameters and the associated values are the values of the parameters.

- The keys in the JSON object must be strings enclosed within quotes.
- The parameters may be specified in long form, for example, `--username`. They can also be specified as short form. For example, `-u`.

- Parameters can be of the following types: string, boolean, or numeric.
- The JSON object cannot contain new lines. It can contain spaces and tabs.
- Flags such as `--help` and `--use-egl` that have no associated values can be included as values in the special "flags" array.

Here are some examples of valid JSON strings, which can be passed to the client from standard input of the `pcoip-client` process:

```
{ "-u": "<username>", "-p": "<password>", "--connection-broker":  
"<connectionManager>", "--domain": "<domain>", "--log-level": 3 }
```

```
{ "--connect-tag": "<encodedConnectTag>", "--session-id":  
"<encodedSessionId>" }
```

```
{ "flags" : ["--use-egl"] }
```

HID Local Termination Blacklist

Local Termination of Wacom tablets provides the best user experience in networks with high latency, however some features of the tablet may not be fully supported with local termination. A HID local termination blacklist has been added to override the preferred local termination mode.

Devices on the blacklist would be bridged to the remote desktop. To enable the HID local termination blacklist, add the following setting to `~/.config/Teradici/Teradici\ PCoIP\ Client.ini`. The vendor and product IDs are separated by a comma and multiple devices are separated by a space.

```
localtermination_black_list "vid,pid vid2,pid2"
```

For more information on USB Vendor ID/Product ID Auto-Forward, see [USB Vendor ID/Product ID Auto-Forward](#).

Troubleshooting HID Local Termination Blacklist

The following lines should appear in the Anyware Agent log if a device is using HID local termination:

```
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'
```


H.264 Hardware Decode

The Anyware Software Client for Linux supports H.264 hardware decode for selected hardware configurations on supported hardware platforms. This enables improved frame rate performance when using PCoIP Ultra GPU-Offload or Auto-Offload, especially in conjunction with high resolution content. This feature must be used in combination with the [High Performance Client](#) and invoked with `--use-egl`.

Note: Support for Hardware Decoding

Hardware decoding is only supported for Chroma subsampled H.264 encoded data. This is a Anyware Agent configuration setting, which is only supported on Graphics agents for Windows and Linux.

Enabling Hardware Decoding

1. On the Anyware Client, open the file `~/.pcoip.rc` in a text editor.
2. Add the following line:

```
pcoip.enable_hw_h264 = 1
```

3. Save your changes.

Note: Disabling Hardware Decoding

PCoIP Ultra does not default to "Auto Offload" when H.264 Hardware Decoding is disabled.

Intel Integrated Graphics Recommended

Currently the Anyware Client does not support H.264 hardware decoding functions on NVIDIA graphics cards. HP recommends endpoint devices configured with integrated Intel UHD graphics. Hardware decoding will only work if the graphics driver on the client computer supports the VA-API.

Security Guide

Anyware Software Client Security Modes

The Anyware 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 **Anyware 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.

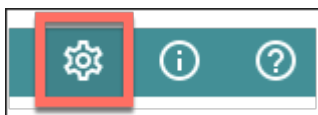
PCoIP sessions are always encrypted

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.

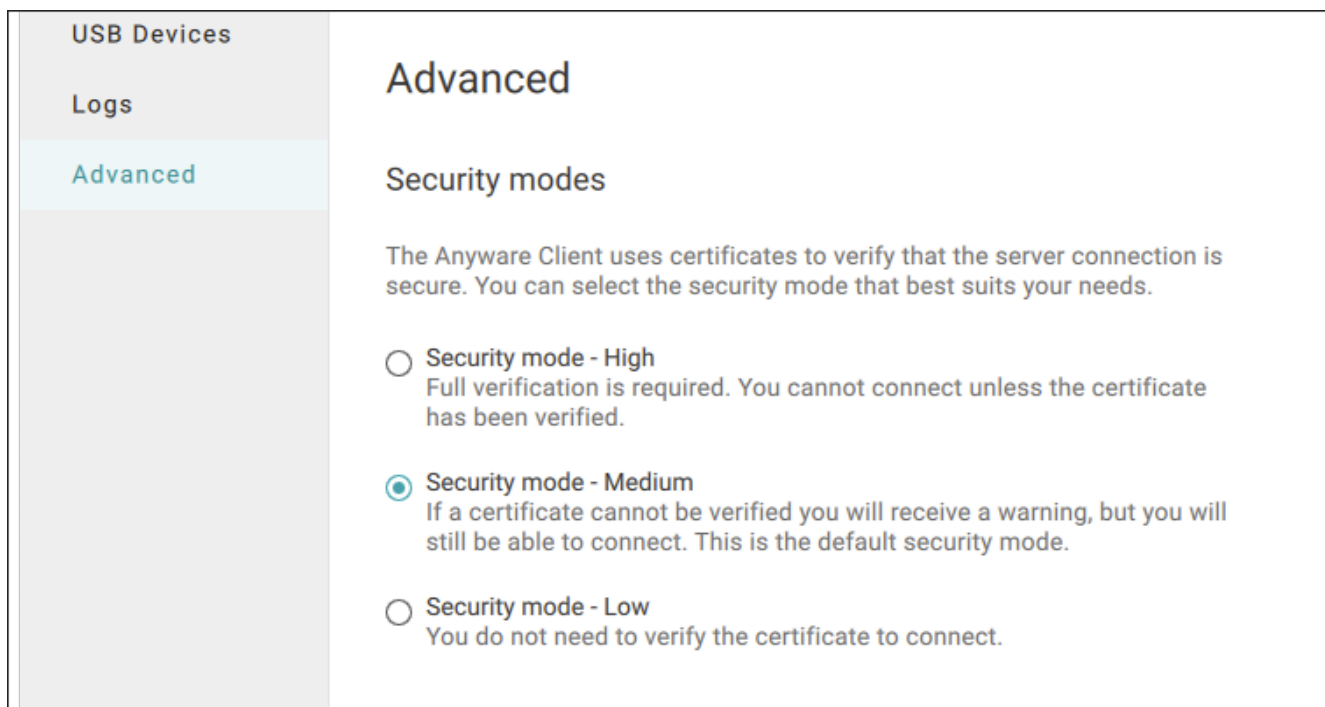
Setting the Security Mode

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 `~/.config/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.

System Libraries

The following system libraries are used by the Software Client for Linux:

- libcap2
- libbz2
- libc6
- libegl1
- libgcc
- libgl1
- libharfbuzz0b
- libpng16
- libprotobuf10
- libpulse0
- libqt5
- libssl1.1
- libstdc++6
- libudev1
- libva-drm2

Previously these libraries had been distributed along with the client application. Security updates to these packages are available via system updates.

Installing the Internal Root CA Certificate on an Anyware Client for Linux

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

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>.

Important: Root CA Certificate must have a .crt extension

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

Installing a Root Certificate on Ubuntu and Debian

1. Copy the certificate to the folder `/usr/local/share/ca-certificates/extra`. You may need to create the `/extra` folder.
2. Update the certificate store with the following command:

```
update-ca-certificates
```

3. Remove the certificate from the folder.
4. Update the certificate store with the following command:

```
update-ca-certificates --fresh
```

Reference

Azure Virtual Desktop Keyboard Shortcuts

The following keyboard shortcuts apply when using the Software Client for Linux for Linux to access a Azure Virtual Desktop (AVD) using RDP:

- **CTRL** + **ALT** + **END** = **CTRL** + **ALT** + **DEL** (inside the remote desktop)
- **ALT** + **Pg-Up** = **ALT** + **TAB** (task switcher inside the remote desktop)
- **ALT** + **Home** = Windows button (inside the remote desktop)
- **SHIFT** + **ALT** + **Enter** = Toggle full-screen mode on/off

Disabling the Virtual Terminal Functionality

On the Anyware Software Client for Linux using either `Ctrl + Alt + SHIFT + F12` or `Ctrl + Alt + F12` will switch to virtual terminal 12, which typically does not exist. This can result in a blank screen. To avoid this you can disable virtual terminal functionality by creating a file `/usr/share/X11/xorg.conf.d/60-pcoip.conf` with the following contents:

```
Section "Serverflags"
    Option "DontVTSwitch" "yes"
EndSection
```

This file needs to be created with root permissions.

Disabling the Super Key

On Linux Clients that connect to Windows agents, sometimes, hotkeys do not work as expected. Specifically, the clients inconsistently receive Super key press events if the Super key is mapped to the local system. This issue can be resolved by disabling the Super key on the client machine.

To do this, run the following command:

```
sudo apt-get install gnome-tweaks  
gsettings set org.gnome.mutter overlay-key ''
```


Linux Keyboard Shortcuts

There are a number of system level keyboard shortcuts on Ubuntu 18.04 that can affect your remote desktop experience. If you are using some of these keys then it is recommended that you re-map or disable them.

There are separate keyboard shortcuts if you are connecting to a Azure Virtual Desktop (AVD) using RDP, as outlined [below](#).

To re-map a keyboard shortcut go to the **Keyboard** tab within your system settings, select the keyboard shortcut and enter the keys you wish to use to re-map with. You can also click backspace to disable the shortcut.

The following keyboard shortcuts may be of interest:

Navigation Shortcut: 

Ubuntu 18.04: Switch applications (on local client).

Windows 10: Switch applications (on remote desktop).

Navigation Shortcut: 

Ubuntu 18.04: Switch applications (on local client)

Windows 10: Open task view (on remote desktop)

Navigation Shortcut: 

Ubuntu 18.04: Move window one monitor up.

Windows 10: Stretch the desktop window to fill the entire screen.

Navigation Shortcut: 

Ubuntu 18.04: Hides all normal windows.

Windows 10: Adds a virtual desktop.

Navigation Shortcut: 

Ubuntu 18.04: Switch System Controls Windows.

Windows 10: View open applications.

Navigation Shortcut: Super + Home

Ubuntu 18.04: Switch to workspace 1.

Windows 10: Minimize all but the active desktop window(Restores all windows on second stroke).

Navigation Shortcut: Super + Lock

Ubuntu 18.04: Lock screen.

Windows 10: Lock screen.

Navigation Shortcut: Super + A

Ubuntu 18.04: Show all applications.

Windows 10: Open action center.

Navigation Shortcut: Super + S

Ubuntu 18.04: Show the overview.

Windows 10: Open search.

Navigation Shortcut: Super + H

Ubuntu 18.04: Hide window.

Windows 10: Open the share charm.

Navigation Shortcut: Super + Up arrow

Ubuntu 18.04: Maximize window.

Windows 10: Maximize app window.

Navigation Shortcut: Super + Down arrow

Ubuntu 18.04: Restore window.

Windows 10: Minimize app window.

Navigation Shortcut: Super + Left arrow

Ubuntu 18.04: View split window from the left side.

Windows 10: Snap app window left.

Navigation Shortcut:  + 

Ubuntu 18.04: View split window from the right side.

Windows 10: Snap app window right.

Troubleshooting and Support

Support and Troubleshooting

If you encounter a problem installing or using the Software Client for Linux, 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 bundle:

1. Open a terminal window.
2. Launch the support bundler utility:

```
pcoip-client-support-bundler
```

The support bundler will collect diagnostic information and logs, and bundle them into a .tar.gz archive in your /tmp/ directory. Support bundle files look like this: supportbundle-client-2021-04-21T21212112Z.tar.gz.

Troubleshooting Client Crashes

When troubleshooting issues involving a client crash, system crash dumps are extremely helpful. Some systems may not have crash dumps enabled; if this is the case, you must enable it in order to capture the crash data.

Crash dumps are disabled by setting the size limit to `0`. To check if there is a limit on the size of core dumps use the `ulimit` command:

```
ulimit -c
```

The response will indicate the limit on core dumps. If the response is `0`, it indicates that core dumps are disabled (limited to a size of zero blocks), and you must enable core dumps.

If required, enable crash dumps by setting the limit to `unlimited`:

```
ulimit -S -c unlimited pcoip-client
```

Then, reproduce your issue and collect the support bundle. After completing this sequence, reset the crash dump setting to its previous level (this example will set it to zero, or disabled):

```
ulimit -S -c 0
```

Finding Your Client Version

Finding Your Client Version

You can find your Software Client for Linux 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:
 - a. Click the Info icon in the top left of the client interface. The **Anyware Client | About** pop-up dialog appears displaying version information.
- **In-session:** If you *are* in a session:
 - a. Find or reveal the client menu bar
 - b. Select **Anyware Anyware Client > About Anyware Anyware Client**.

c. Find the version number in the information window that appears.

Anyware Client Logging

The Software Client for Linux 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 `/tmp/Teradici/<USERNAME>/PCoIPClient/logs/` by default, where,

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

Log locations can be overridden via [launch configuration](#) if required.

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 (<i>default setting</i>)
3	Debug messages and higher

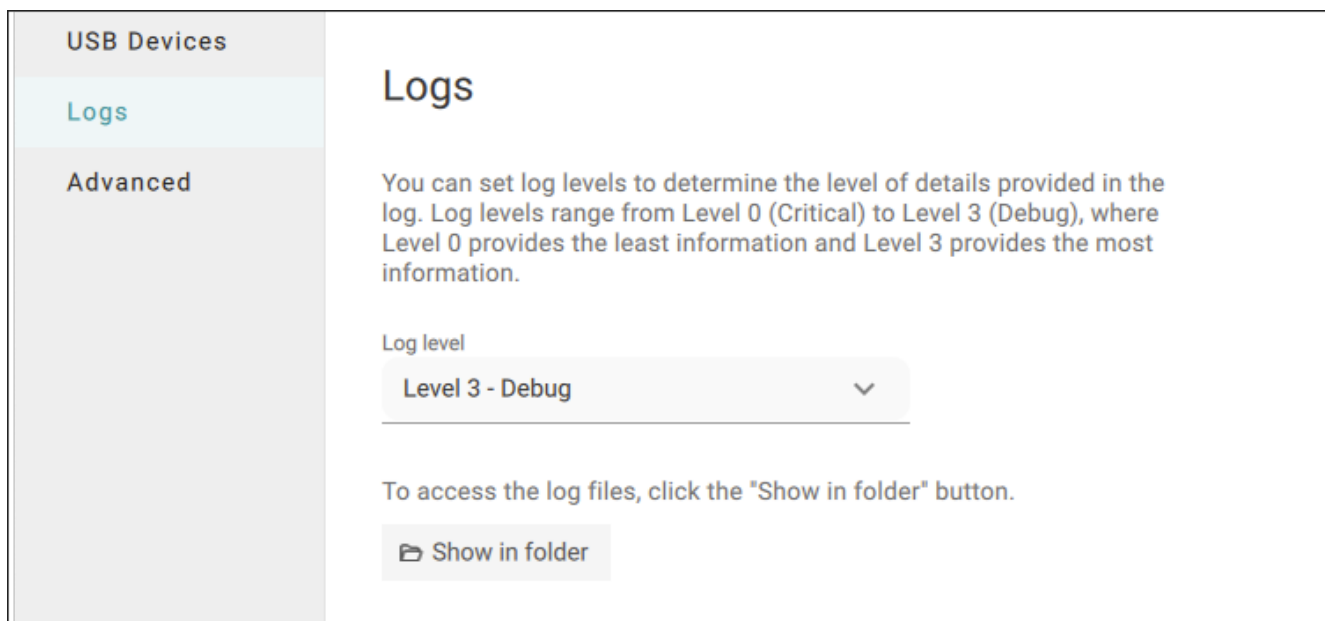
The log level can be changed either from the pre-session interface, or programmatically from the Command Prompt.

Tip: Reporting Issues to Support

When reporting an issue to support, set the log level to 3 (debug), reproduce the issue, and then create a support bundle. This ensures that the required details are captured, making diagnostics more effective.

Setting the Log Level in the Pre-session Interface

1. Disconnect active PCoIP sessions and return to the pre-session interface.
2. Click the gear icon in the top-left corner to open the **Anyware | Settings** window.
3. Click **Logs** in the left pane.
4. Under **Log level**, specify the desired log level.



Setting the Log Level Programmatically

1. Launch the Software Client for Linux from the Command Prompt. Include the `log-level` flag as a part of the command.

The following example launches the client in full-screen mode, sets the log level to `3`, and points to a connection broker at `broker.domain.com`.

```
/usr/bin/pcoip_client --connection-broker broker.domain.com --log-level 3 --fullscreen
```