



# leostream<sup>®</sup>

Remote Desktop Access Platform

## Quick Start for PCoIP Connections

Managing connections to workstations and VMs using PCoIP

## Contacting Leostream

Leostream Corporation  
77 Sleeper St.  
PMB 02-123  
Boston, MA 02210  
USA

<http://www.leostream.com>  
Telephone: +1 781 890 2019

To submit an enhancement request, email [features@leostream.com](mailto:features@leostream.com).

To request product information or inquire about our future directions, email [sales@leostream.com](mailto:sales@leostream.com).

## Copyright

© Copyright 2002-2025 by Leostream Corporation

This software program and documentation are copyrighted by Leostream. The software described in this document is provided under a license agreement and may be used or copied only under the terms of this agreement. No part of this manual may be copied or reproduced in any form without prior written consent from Leostream.

## Trademarks

The following are trademarks or registered trademarks of Leostream Corporation.

Leostream®

The Leostream graphical logo™

The absence of a product name or logo from this list does not constitute a waiver of the trademark or other intellectual property rights concerning that product, name, or logo by Leostream.

The OpenStack Word Mark and OpenStack Logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. Leostream is not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community. Linux is the registered trademark of Linus Torvalds in the U.S. and other countries. OpenLDAP is a trademark of The OpenLDAP Foundation. Microsoft, Active Directory and Windows are trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Other brand and product names are trademarks or registered trademarks of their respective holders. Leostream claims no right to use of these marks.

## Patents

Leostream software is protected by U.S. Patent 8,417,796.

# Contents

<b>CONTENTS .....</b>	<b>3</b>
<b>CHAPTER 1: OVERVIEW .....</b>	<b>5</b>
PCoIP Remote Workstation Components .....	5
Using HP Anyware (PCoIP) Clients with the Leostream Platform .....	5
Ensuring Proper Communication with PCoIP Devices .....	7
<b>CHAPTER 2: CONFIGURING THE CONNECTION BROKER .....</b>	<b>9</b>
STEP 1: Enabling PCoIP Device Management .....	9
STEP 2: Registering PCoIP Devices with the Connection Broker.....	10
<i>Adding PCoIP Remote Workstation Cards to the Connection Broker .....</i>	<i>10</i>
<i>Uploading Multiple PCoIP Remote Workstation Cards.....</i>	<i>11</i>
<i>Removing PCoIP Remote Workstation Cards from your Connection Broker.....</i>	<i>12</i>
STEP 3: Specifying Authentication Servers and Methods .....	12
<i>Defining an Authentication Server .....</i>	<i>13</i>
<i>Enabling PIV/CAC Cards for Leostream Platform Logins .....</i>	<i>14</i>
<i>Multi-Factor Authentication Options.....</i>	<i>16</i>
STEP 4: Adding Workstations and VMs to your Connection Broker .....	16
<i>Creating an Active Directory Center .....</i>	<i>16</i>
<i>Creating an Uncategorized Desktops Center .....</i>	<i>18</i>
<i>Removing Duplicate Desktop Records .....</i>	<i>18</i>
<i>Troubleshooting Missing Workstations .....</i>	<i>19</i>
STEP 5: Installing the Leostream Agent .....	19
STEP 6: Associating PCoIP Remote Workstation Cards and Desktops.....	20
<i>Automatic PCoIP Remote Workstation Card Matching for a Windows Desktop.....</i>	<i>21</i>
<i>Automatic PCoIP Remote Workstation Card Mapping for a Linux Desktop .....</i>	<i>21</i>
<i>Confirming and Editing PCoIP Remote Workstation Card Mappings .....</i>	<i>22</i>
STEP 7: Defining Pools of Desktops.....	22
STEP 8: Defining Pool-Based Plans .....	24
<i>Protocol Plans.....</i>	<i>24</i>
<i>Power Control Plans.....</i>	<i>28</i>
<i>Release Plans .....</i>	<i>29</i>
STEP 9: Defining User Policies.....	31
STEP 10: Creating Locations that Require PIV/CAC Logins .....	33
STEP 11: Assigning Policies to Users .....	35
STEP 12: Testing User Login .....	37
STEP 13: Logging into the Leostream Platform .....	39
<i>Using PCoIP Zero Clients .....</i>	<i>39</i>
<i>Using an HP Anyware Software Client.....</i>	<i>39</i>
<i>Using Leostream Connect.....</i>	<i>40</i>
<b>USING THE LEOSTREAM GATEWAY FOR REMOTE ACCESS.....</b>	<b>41</b>
OVERVIEW .....	41
THE LEOSTREAM NETWORK ARCHITECTURE .....	41

HOW THE LEOSTREAM GATEWAY WORKS .....	42
<b>APPENDIX A: WORKING WITH PCOIP CLIENTS .....</b>	<b>44</b>
DISPLAYING A DISCLAIMER BEFORE PCOIP CLIENT LOGINS.....	44
HARD ASSIGNING WORKSTATIONS TO PCOIP ZERO CLIENTS .....	45
UPLOADING PCOIP ZERO CLIENTS .....	47
RESETTING PCOIP ZERO CLIENTS .....	49
MANAGING ANOTHER USER’S RESOURCES VIA PCOIP ZERO CLIENT LOGINS .....	49
OCTAL SUPPORT WITH PCOIP CLIENT BINDING.....	50
<i>Configuring Desktops for Octal-Monitor Support.....</i>	<i>50</i>
<i>Creating a Bonded PCoIP Zero Client Pair.....</i>	<i>51</i>

## Chapter 1: Overview

The Leostream® Connection Broker makes it possible to manage connections to pools of workstations and virtual machines with installed [PCoIP Remote Workstation cards](#) and HP Anyware agents. PCoIP Remote Workstation Cards provide the full frame-rate rendering capabilities necessary to create complex designs and images.

PCoIP® technology provides an optimal end-user experience when connecting users to hosted desktops by delivering a true PC experience over standard IP networks. For more information on the PCoIP protocol, please visit <https://www.teradici.com/what-is-pcoip>.

---

*This Quick Start assumes that you do not have a PCoIP Connection Manager and Security Gateway installed in your Leostream environment. If you plan to use a PCoIP Connection Manager and Security Gateway in your Leostream Environment, please see the [Quick Start Guide for HP Anyware](#).*

---

## PCoIP Remote Workstation Components

The Leostream Connection Broker manages three distinct components in environments that include workstations with PCoIP Remote Workstation cards.

- **Desktop operating systems:** The Leostream platform manages connections to remote workstations running Microsoft® Windows®, Linux, and macOS operating systems. Desktops that support the PCoIP protocol appear on the > **Resources** > **Desktops** page of the Connection Broker.
- **PCoIP Remote Workstation Cards:** The Leostream platform automatically pairs the PCoIP Remote Workstation card, the PCoIP hardware technology used to transfer information from the desktop to the client, to the desktop operating system running in the workstation. PCoIP Remote Workstation cards appear on the > **Resources** > **PCoIP Host Devices** page of the Connection Broker.
- **PCoIP Clients:** A number of client vendors, such as Amulet Hotkey and Dell Wyse®, have embedded PCoIP firmware in their zero-client hardware. With the single purpose of image decompression and decoding, PCoIP eliminates endpoint hard drives, graphic processors, operating systems, applications and security software. Users can also log into your Leostream environment using Leostream Connect or the Leostream Web client, which then launches an HP Anyware software client to establish a PCoIP connection. All client devices appear on the > **Resources** > **Clients** page of the Connection Broker.

## Using HP Anyware (PCoIP) Clients with the Leostream Platform

Leostream customers use an HP Anyware client, PCoIP Zero Client, Leostream Web client, or Leostream Connect client to log into their Leostream environment. The Leostream Connect client and Leostream Web client then launch an HP Anyware software client to establish a PCoIP connection. The Leostream Platform can connect users to workstations with a PCoIP Remote Workstation Card and virtual machines running the

HP Anyware Agent, either directly or through the Leostream Gateway.



If you plan to use a PCoIP Connection Manager and Security Gateway (CMSG) as an intermediary between the HP Anyware clients and the Leostream Connection Broker, please refer to the [Quick Start Using Leostream with HP Anyware](#) for further instructions.

The table below summarizes the desktop connection options for different client types and architectures.

Client Type	Client Points To	The client can connect to: Virtual Machines	The client can connect to: Physical Machines
PCoIP Software Client PCoIP Mobile Client PCoIP Zero Client	PCoIP Connection Manager Security Gateway <i>Disabled</i>	Running the HP Anyware Standard or Graphics Agent	With installed PCoIP Remote Workstation cards if the operating system has an installed HP Anyware Agent for Remote Workstation Cards  <b>And</b> Running the HP Anyware Standard or Graphics Agent.
PCoIP Software Client PCoIP Mobile Client PCoIP Zero Client	PCoIP Connection Manager Security Gateway <i>Enabled</i>	Running the HP Anyware Standard or Graphics Agent	Running the HP Anyware Standard or Graphics Agent
PCoIP Zero Client	Leostream Connection Broker (No CMSG required)	Running the HP Anyware Standard or Graphics Agent	With an installed PCoIP Remote Workstation Cards (no HP Anyware Agent installed)
PCoIP Zero Client PCoIP Software Client	Leostream Gateway, forwarding to the Connection Broker (No CMSG required)	Running the HP Anyware Standard or Graphics Agent	With an installed PCoIP Remote Workstation Cards  <b>And</b> Running the HP Anyware Standard or Graphics Agent.

Client Type	Client Points To	The client can connect to: Virtual Machines	The client can connect to: Physical Machines
Leostream Connect  and  PCoIP Software Client (Windows only)	Leostream Connection Broker  Or  Leostream Gateway, forwarding to the Connection Broker  (No CMSG required)	Running the HP Anyware Standard or Graphics Agent	With an installed PCoIP Remote Workstation Cards (no HP Anyware Agent installed)
Leostream Web Client  (PCoIP Software Client installed)	Leostream Connection Broker  Or  Leostream Gateway, forwarding to the Connection Broker  (No CMSG required)	Running the HP Anyware Standard or Graphics Agent	With installed PCoIP Remote Workstation cards if the operating system has an installed PCoIP Agent for Remote Workstation Cards  <b>And</b>  Running the HP Anyware Standard or Graphics Agent.



This Quick Start assumes your Leostream environment does not include a PCoIP Connection Manager.

## Ensuring Proper Communication with PCoIP Devices

The Leostream platform uses the PCoIP Administrator Web Interface (AWI) and syslog events to control and monitor PCoIP devices, including PCoIP Zero clients and Remote Workstation Cards.



If either the AWI or syslog events are unavailable to your Connection Broker, you cannot use some of the Leostream features described in this guide. Chapter 2 covers how to ensure that your Connection Broker has adequate access to your PCoIP AWI and receives the necessary syslog notifications so your Leostream environment is fully functional.

The following table describes the Leostream platform functionality that is dependent on the AWI and syslog messages. When calling the AWI to disconnect PCoIP sessions, the Connection Broker first attempts to contact the PCoIP Zero Client. If the client is unreachable or the user logged in using a PCoIP software client, the Connection Broker uses the AWI of the Remote Workstation Card.

Feature	AWI Required?	Syslog Required?
Follow-me mode	Yes	No
Disconnect PCoIP session after user logs out of OS	Yes	No

Feature	AWI Required?	Syslog Required?
Reconnect to disconnected session	No	No
Reset PCoIP client	Yes, required on Zero client	No
Force logout from > Desktops page	Yes	Not required
Force disconnects based on idle notifications from Leostream Agent	Yes	Not required
Receive notice when user disconnects session (to use in Release plans)	Not required	Required
Host card information discovery	Yes, required on Remote Workstation Card	Not required
Single sign-on	Not required	Not required
Direct Connect hard-assigned client to its desktop	Yes, required on Zero client	Not required
Role option to <a href="#">manage another user's desktop</a>	Not required	Not required
<a href="#">Client binding</a> (Amulet Hotkey octal support)	Yes, required on Zero client	Not required

## Chapter 2: Configuring the Connection Broker

You use the Leostream Connection Broker Administrator Web Interface to configure the concepts that define your Leostream environment. For more information on Leostream concepts, see the [Getting Started with Leostream Concepts](#).

The following procedure assumes you have installed and licensed your Leostream Connection Broker. For information on installing and licensing the Leostream components, see the [Leostream Installation Guide](#).

### Step 1: Enabling PCoIP Device Management



This step applies only if your environment includes PCoIP Remote Workstation Cards or Zero clients. If you are using HP Anyware software clients and agents, skip to step 3.

After applying a Leostream platform license key that enables PCoIP Remote Workstation Cards, the **> Setup > Centers** page includes a **PCoIP Devices** center. The Connection Broker uses this center as a repository for the PCoIP Remote Workstation Cards and PCoIP Zero Clients in your environment.

Before beginning to add PCoIP devices to your Connection Broker, configure the **PCoIP Devices** center to allow access to the PCoIP AWI and enable syslog event tracking, as follows:

1. Go to the **> Setup > Centers** page in your Connection Broker.
2. Click the **Edit** action for the **PCoIP Devices** center.
3. If the Administrator Web Interface for your PCoIP devices is password protected, enter that default password in the **Default password** field. Leave this field blank if the AWI does not require a password to log in.



The Connection Broker requires access to the AWI in order to perform connects and disconnects of the user's PCoIP session, for example, when implementing follow-me mode. If you do not enable AWI access for your Connection Broker, you cannot use Leostream Release Plan options to disconnect the user's session. The AWI is also required for client binding, described in [Multi-Monitor Support with PCoIP Client Binding](#).

If any Remote Workstation Card or PCoIP Zero client uses a password that is different from the default, you can edit that object's record on either the **> Resources > PCoIP Host Devices** or **> Resources > Clients** page to enter the new password.



You do not need to enter information for an SSH user to utilize any of the functionality described in this document.

4. From the **Inventory scan interval** drop-down menu, select an interval to indicate how often the Connection Broker scans the remote workstation cards and zero clients inventoried in this center

5. Check the **Configure PCoIP endpoints to send events to this Connection Broker via syslog** option.



You should allow all PCoIP Zero Clients and Remote Workstation Cards to send syslog events to your Leostream Connection Broker. The Connection Broker uses the syslog events to invoke Release Plan options related to disconnect notices. If you are already sending syslog events to a different syslog server, use the AWI of your PCoIP devices to remove the external syslog server from the PCoIP device and set up your PCoIP Devices center as follows.

- a. Select the **Relay syslog events to another syslog server** option.
- b. Enter the external syslog server into the **Hostname or IP address of syslog server** edit field.

When you save the PCoIP Devices center, the Connection Broker attempts to connect to the AWI for any PCoIP Zero Clients and PCoIP Remote Workstation Cards registered with your Connection Broker. If the PCoIP device does not already send syslog events to a server, the Connection Broker configures the PCoIP device to send events to the Connection Broker.

## Step 2: Registering PCoIP Devices with the Connection Broker



This step applies only if your environment includes PCoIP Remote Workstation Cards or Zero clients. If you are using HP Anyware software clients and agents, skip to step 3.

You register your PCoIP Remote Workstation Cards with your Connection Broker using one of the techniques described in the following sections. In order for the Connection Broker to associate PCoIP host cards with the desktops they are installed in, the host cards must be present in the Connection Broker before the Leostream Agent on the desktop registers with the broker.


### Adding PCoIP Remote Workstation Cards to the Connection Broker

To inventory individual PCoIP Remote Workstation cards in your Connection Broker.

1. Go to the **> Resources > PCoIP Host Devices** page.
2. Click the **Add PCoIP Host Device** link.
3. In the **Add PCoIP Host Device** form that opens:
  - a. Enter a name for the PCoIP host device in the **Name** edit field.
  - b. If available, enter the device's DNS name in the **Hostname** edit field.
  - c. Enter the device's IP address in the **IP Address** edit field.
  - d. Click **Save**.


After you save the form, the Connection Broker attempts to contact the AWI of the Remote Workstation

Card to gather additional information about the card, such as its MAC address.

 If the Connection Broker cannot obtain the card's MAC address, the Leostream Agent cannot automatically associate the card with the guest operating system of the remote host. In this case, ensure that you manually enter the MAC address or manually associate your Remote Workstation Cards with the appropriate desktop.

## Uploading Multiple PColP Remote Workstation Cards

You can use the **Upload PColP host devices** option on the **> System > Maintenance** page to upload a group of PColP host devices into the Connection Broker. By default, the uploaded CSV-file modifies existing PColP host cards and does not create new host cards. To create new host cards, select the **Allow creation of new PColP host devices** option, shown in the following figure.



If you do not select the **Allow creation of new PColP host devices** option, the Connection Broker indicates if it cannot find an existing host device and skips that row in the CSV-file.


When uploading PColP host devices data, the CSV-file must have the following format.

- The CSV-file must be comma delimited
- Quotes must be double quotes
- The first row must contain the field names, separated by commas with no additional blank spaces, and the data must be in the remaining rows
- The field names must match the field names in the `terahost` table in the data dictionary
- The only modifiable fields are:
  - `name`
  - `serial_number`
  - `mac`
  - `ip`
  - `hostname`
  - `notes`
- One of the following fields is required and must uniquely identify the host card
  - `id` (for updating existing PColP host devices, only)
  - `ip`
  - `hostname` (either `ip` or `hostname` must be specified, but do not enter both)

Specify new PColP host devices using either the `ip` or `hostname` field, but not using both fields. New host

cards cannot be created using an `id` field.

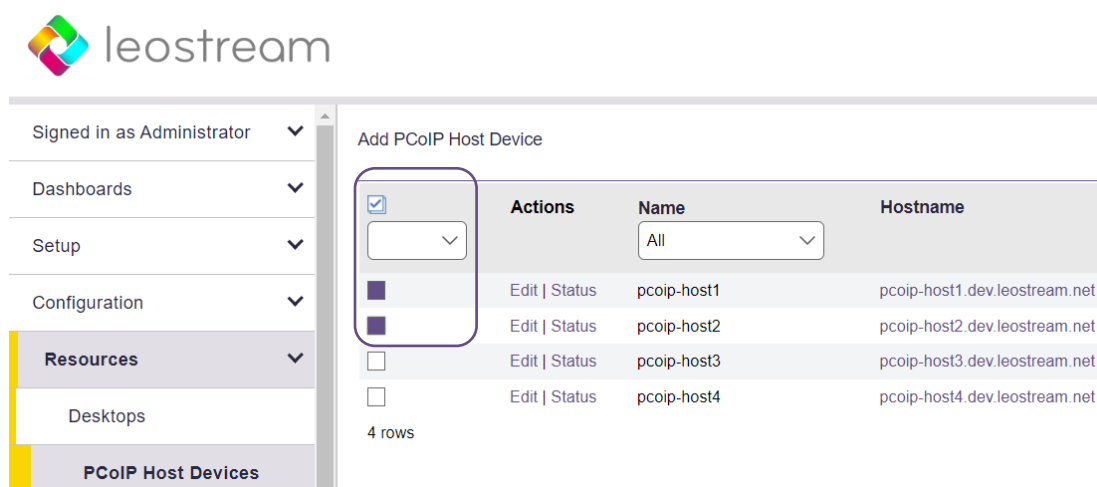
After uploading a CSV-file of PCoIP host devices, the Connection Broker performs a scan of the PCoIP Devices center and updates the PCoIP records with any additional information the Connection Broker can retrieve from the host card AWI.

 When uploading information for Remote Workstation Cards that do not have the AWI enabled, specify as much information as possible, most importantly the devices' MAC addresses.

### Removing PCoIP Remote Workstation Cards from your Connection Broker

You can remove PCoIP Remote Workstation cards from the **> Resources > PCoIP Host Devices** page using any of the following methods.

1. Click the **Delete** action associated with a PCoIP Remote Workstation card on the **> Resources > PCoIP Host Devices** page.
2. Select the **Bulk action** check box for multiple PCoIP Remote Workstation cards, as shown in the following figure, then select **Delete** from the bulk action drop-down menu at the top of the column of check boxes.



If bulk action check boxes are not included on your **> Resources > PCoIP Host Devices** table, use the **Customize columns** link at the top-right of the page to add the **Bulk action** column.

### Step 3: Specifying Authentication Servers and Methods

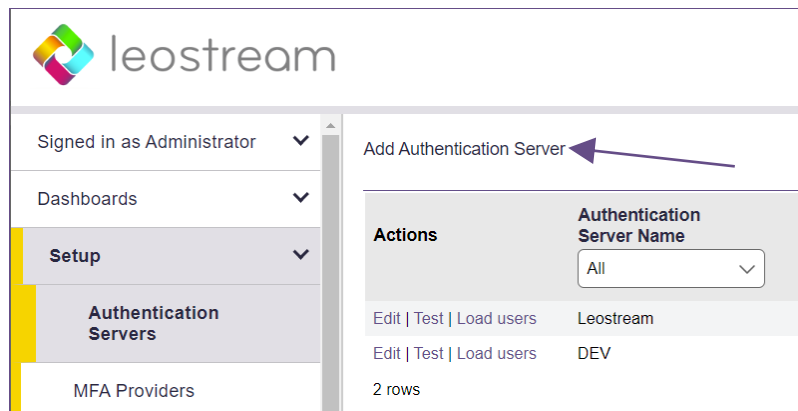
The Connection Broker uses your authentication server to authenticate users and assign policies. The Connection Broker can authenticate users against Microsoft Active Directory and OpenLDAP authentication servers and can also act as a local authentication server in environments that do not have an external authentication system. You can also leverage any SAML-based Identity Provider along with your Leostream environment.

When using Active Directory for authentication, the Connection Broker can also inventory physical desktops and workstations using the Computer records found in your Active Directory tree.

## Defining an Authentication Server

**Note:** For this example, any options not covered in the following procedure remain at their default values.

1. Navigate to the **> Setup > Authentication Servers** menu.
2. Click the **Add Authentication Server** link, shown in the following figure.



3. The **Add Authentication Server** form opens. In the **Authentication Server name** edit field, enter a name for this server in the Connection Broker.
4. In the **Domain** edit field, enter the domain name associated with this Active Directory server.
5. In the **Connection Settings** section, shown in the following figure, use the following procedure to integrate with your Active Directory authentication server.

**Connection Settings**

Specify address using  
 Hostnames or IP addresses

Hostname or IP address Port  
 389

If using multiple addresses, separate each entry with spaces

Algorithm for selecting from multiple addresses  
 Random

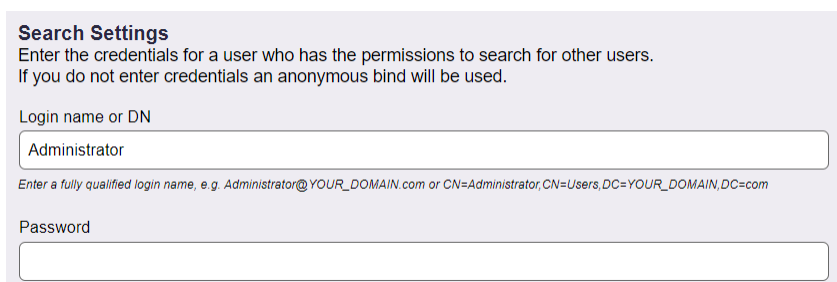
The sequential algorithm uses the first working address in the list

☐ Encrypt connection to the authentication server using SSL (LDAPS)

AWS Directory ID

Enter the Directory ID if this is an AWS directory that will be used for a Amazon Workspaces

- a. Select **Active Directory** from the **Type** drop-down list.
  - b. From the **Specify address using** drop-down menu, select **Hostname or IP address**.
  - c. Enter the authentication server **Hostname or IP address**.
  - d. Enter the port number in the **Port** edit field.
  - e. Check on the **Encrypt connection to authentication server using SSL (LDAPS)** checkbox if you need a secure connection to the authentication server. The port number automatically changes to 636. Re-edit the **Port** edit field if you are not using port 636 for secure connections.
6. In the **Search Settings** section, shown in the following figure, enter the username and password for an account that has read access to the user records. The Connection Broker does not need full administrator rights to your Active Directory authentication server.



**Search Settings**  
Enter the credentials for a user who has the permissions to search for other users.  
If you do not enter credentials an anonymous bind will be used.

Login name or DN  
  
Enter a fully qualified login name, e.g. Administrator@YOUR\_DOMAIN.com or CN=Administrator,CN=Users,DC=YOUR\_DOMAIN,DC=com

Password

7. In the **User Login Search** section, ensure that the **Match Login name against this field** edit field is set to **sAMAccountName**. This is the attribute that the Connection Broker uses to locate the user in the authentication server, based on the information the user enters when logging into Leostream.
8. Click **Save**.

For more detailed instructions, see the chapter “Authenticating Users” in the [Connection Broker Administrator’s Guide](#).

## Enabling PIV/CAC Cards for Leostream Platform Logins

For users logging in from a PCoIP Zero Client, you can specify that they must log into your Leostream environment using their smart cards instead of their usernames and passwords.

### IMPORTANT NOTES:

1. Smart card logins are not supported when using a PCoIP Software or Mobile Client.
2. When logging into the Leostream platform with a CAC or PIV card, you may need to enable the policy option to **Prompt user for alternate credentials before connecting to selected desktop (PCoIP only)**. The Leostream Agent on the remote desktop requires the username/password to perform single sign-on to the remote operating system. If you do not prompt for alternate credentials, the user must enter their username and password into the remote operating system

after the PColP connection is established.

- Before you begin the following procedure, obtain the Intermediate Certificate or CA Bundle file used to sign the certificates stored on the smart cards.

To enable PIV/CAC card logins:

- Go to the **> Setup > Authentication Servers** page
- Edit the Active Directory server used to issue the certificates on the smart card.
- Scroll down to the new **Smart/PIV Card Authentication** section shown in the following figure.

- Use the **Choose File** button to upload the CA certificate or CA bundle file used to generate and sign the certificates on your smart cards.



You must upload the entire certificate chain, not just the root CA.

- If you want to use OCSP to check for revoked certificates, select the **Check for certificate revocation using OSCP** option.



When checking certificate revocation, the issuing CA must appear first in the uploaded CA bundle. Also, the user's certificate on the PIV card must contain the OCSP URI.

- In the **Account linking** drop-down menu, indicate which AD attribute the Connection Broker uses to link the certificate on the smartcard to the appropriate AD user record
- Click **Save**.

The Connection Broker validates the certificate when saving the form so you will know, at that time, if there is a problem with your certificate. If the certificate is valid, the Connection Broker displays the certificates subject and issuer.

You use Leostream Locations to indicate which users require smart card authentication, as described in [Step 10: Creating Locations that Require PIV Logins](#).



The Connection Broker validates the certificate and identifies the user with the smart card, however to

perform single sign-on to the operating system, the Leostream Agent on the remote host requires a username and password. If you plan to enable smart card logins and require SSO, ensure you configure your policy as described in Step 11 to obtain a username and password to send to the Leostream Agent on the remote host.

### Multi-Factor Authentication Options

PCoIP clients support multi-factor authentication for any Identity Provider that supports the RADIUS protocol. See the Leostream guide for [Using RADIUS Servers for MFA](#) for more information.

In addition, you can leverage SAML-based Identity Providers (IdP) to provide single sign-on to the Leostream web client with multi-factor authentication, and launch the PCoIP connection from the Leostream Web client. You can integrate the Leostream platform with any authentication service, such as Azure AD, Okta, Duo, and Ping Identity, that acts as a SAML 2.0 Identity Provider. See the Leostream guide for [Using SAML-based Identity Providers with Leostream](#).

## Step 4: Adding Workstations and VMs to your Connection Broker

After you import your PCoIP Remote Workstation Cards and connect the Leostream platform to your authentication servers, inventory your workstations using either an Uncategorized Desktops center or Active Directory center. If all your Workstations have Computer records in Active Directory, create an Active Directory center. Otherwise, use the Leostream Agent to register your workstations with the Uncategorized Desktops center.

You can inventory virtual machines running the HP Anyware Agent using the Active Directory or Uncategorized Desktops centers, as well, or create a native center for your virtualization or cloud environment. See the [Connection Broker Administrator's Guide](#) for instructions on connecting to virtual or cloud host providers.



To simplify your Connection Broker configuration, use either an Active Directory center or an Uncategorized Desktops center. Simultaneously using both types of center can lead to duplicate desktop records in your Connection Broker.

### Creating an Active Directory Center

To add an Active Directory center:

1. Go to the **> Setup > Centers** page.
2. Click **Add Center**.
3. Select **Active Directory** from the **Type** drop-down menu. The form updates, as shown in the following figure.

Add Center
?

Type
Active Directory

Name

Authentication Server
Dev

Sub-tree

The sub-tree that will be searched to find the computers  
e.g., DC=QA\_MACHINES,DC=YOUR\_DOMAIN,DC=com

Advanced filter expression (optional)

The default filter expression is "(objectClass=Computer)". You can override this by entering a filter expression here. For example:  
"(&(objectCategory=Computer)(objectClass=Computer)(!(CN=a\*)(CN=b\*)))",  
which would find all computer objects that start with either "a" or "b".

Inventory scan interval
Manual only

Power state scan interval
Manual only

Power state is determined by scanning ports used by remote viewers

☒ Offer desktops from this center

☐ Assign rogue users to desktops from this center (requires Leostream Agent)

☐ Initialize newly-discovered desktops as "unavailable"

☐ Continuously apply any Auto-Tags

☐ Resolve addresses in this center using short hostnames

4. Enter a name for the center in the **Name** edit field.
5. Select the associated Active Directory authentication server from the **Authentication Server** drop-down menu. The list contains only the Active Directory server you entered into your Connection Broker in step 3.
6. In the **Sub-tree** edit field, specify the sub-tree within the Active Directory system that contains the machines. If you do not specify a sub-tree, the Connection Broker assumes the same start point as the Active Directory search start point.
7. Leave the remaining fields at their default values and click **Save**.

After you create your Active Directory center, go to the **> Resources > Desktops** page. This page lists the workstations the Connection Broker imported from the Active Directory tree.

## Creating an Uncategorized Desktops Center

If your desktops are not part of your Active Directory structure, you can inventory your desktops using an **Uncategorized Desktops** center. To add the **Uncategorized Desktops** center:

1. Go to the **> Setup > Centers** page.
2. Click **Add Center**.
3. Select **Uncategorized Desktops** from the **Type** drop-down menu.
4. Click **Save**.

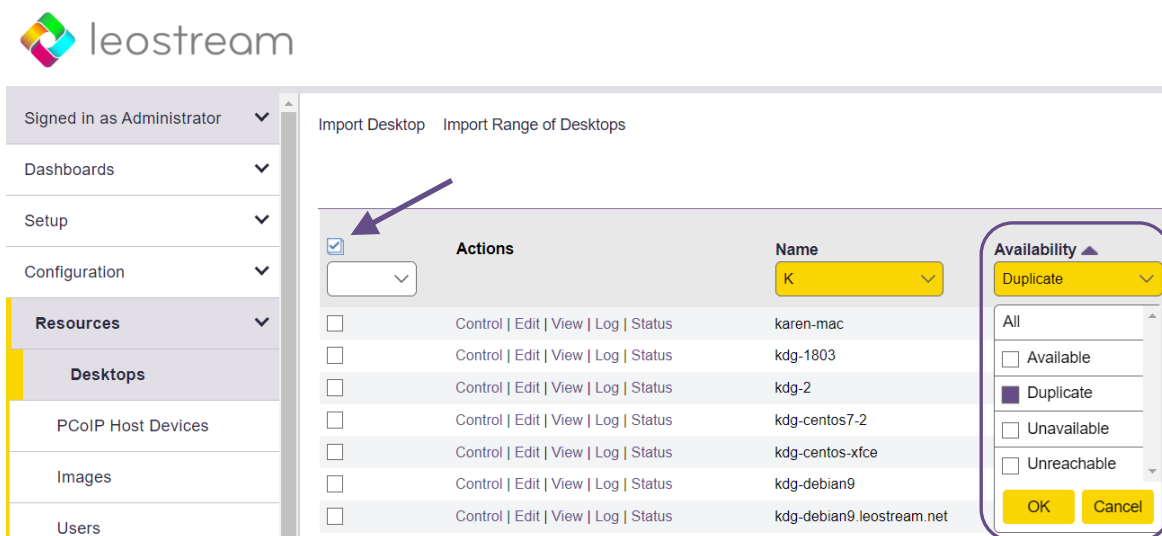
Workstations do not appear in the Uncategorized Desktops center until you install a Leostream Agent on the machine (see [Step 5: Installing the Leostream Agent on Workstations](#)).

## Removing Duplicate Desktop Records

If you add an **Active Directory** center and an **Uncategorized Desktops** center, you may have desktops that are inventoried twice on the **> Resources > Desktops** page. The Connection Broker uses information provided by the Leostream Agent to determine which desktop records represent the same desktop and marks the entry in the **Uncategorized Desktops** center as a duplicate.

To remove duplicate desktop records, you can remove the desktop records, as follows.

1. Go to the **> Resources > Desktops** page.
2. From the drop-down menu at the top of the **Availability** column, select **Duplicate**, as shown in the following figure.



3. Click the checkbox at the top of the column of check boxes, pointed out in the previous figure.

4. From the drop-down menu at the top of the row of checkboxes, select **Remove**.



Do not select **Delete**. The **Delete** option is intended for deleting virtual machines from disk.

5. Click **OK** in the **Remove Desktop** confirmation dialog that opens.

## Troubleshooting Missing Workstations

If some workstations are not appearing in your **> Resources > Desktops** list, check for the following conditions.

- Is the workstation powered on?
- Is the Leostream Agent installed and running on the blade? If the workstation is imported using the **Uncategorized Desktops** center, the Leostream Agent must be installed, running, and able to communicate with the Connection Broker. Stopping and restarting the agent forces the agent to register with the Connection Broker.

To stop and start the agent on Windows:

1. Open the Leostream Agent control panel
  2. Go to the **Status** tab
  3. Click the **Stop** and/or **Start** button.
- Is the DNS SRV record for your Connection Broker configured correctly? If this record is not correct and your Leostream Agents are configured to discover the broker using that record, the agents cannot find the Connection Broker.

If you do not want to use a DNS SRV record for the Connection Broker, you can hard-code the Connection Broker IP address into the Leostream Agent, as follows (for Microsoft Windows).

1. Open the Leostream Agent dialog from your machine's Control Panel.
2. Go to the **Options** tab.
3. In the **Leostream Connection Broker** section, uncheck the **Obtain Connection Broker address automatically** check box.
4. Enter the Connection Broker address and port into the **Address** and **Port** edit fields.
5. Click **OK**.

## Step 5: Installing the Leostream Agent


For physical workstations and for virtual or cloud machines running the HP Anyware agent, the Leostream Agent notifies the Connection Broker when users log in, disconnect, reconnect, logout, and are idle. You can use those events in your Leostream Power Control and Release Plans. In addition, the Leostream Agent performs the following crucial tasks when managing connections to physical workstations with installed PColP Remote Workstation Cards.

- The Leostream Agent registers with the Connection Broker, resulting in a desktop record in the Uncategorized Desktops center
- The Leostream Agent provides information about the installed PCoIP Remote Workstation Card, allowing the Connection Broker to map the PCoIP Remote Workstation Card record in the Connection Broker to the underlying operating system on the workstation.
- The Leostream Agent provides single-sign on to the underlying operating system (Windows and Linux, only).

When installing the Leostream Agent, ensure that you enter a valid Connection Broker address. The Leostream Agent can locate the Connection Broker through the `_connection_broker` DNS SRV record. If you do not have a DNS SRV record for the Connection Broker, enter the broker IP address or hostname.

Also, ensure the appropriate single sign-on tasks are selected.

- On a Windows operating system, install the Windows version of the Leostream Agent with the **Install Credential Provider** task selected.
- On a Linux workstation, install the Java version of the Leostream Agent with both the **Enable SSO** option and **Desktop Experience** option selected.


 The Java version of the Leostream Agent can be installed on macOS to monitor user logins and logouts. However, when installed on macOS, the Leostream Agent does not support USB device passthrough or single sign-on. These tasks are not available when installing on macOS.

See the [Leostream Installation Guide](#) for instructions on installing the Leostream Agent. For more information on the Leostream Agent, see the [Leostream Agent Administrator's Guide](#).

## Step 6: Associating PCoIP Remote Workstation Cards and Desktops

The Connection Broker automatically attempts to match PCoIP Remote Workstation Cards to the desktop operating system running on the workstation, using information provided by the Leostream Agent.

For Remote Workstation Cards associated with a Windows operating system, you must install the PCoIP Agent on the Windows desktop in order for the Leostream Agent to obtain the information needed to perform the automatic host card mapping.

 The following procedure is not support for the Amulet Hotkey DXT-H4 device. Please see [Confirming and Editing PCoIP Remote Workstation Card Mappings](#) if you are using these devices.

## Automatic PCoIP Remote Workstation Card Matching for a Windows Desktop

The Connection Broker uses the following procedure to match PCoIP cards to the correct Windows desktops.

1. Load the PCoIP Devices into the **PCoIP Devices** center. You can accomplish this step using various methods, as described in [Step 2: Registering PCoIP Devices with the Connection Broker](#). After you load a PCoIP Remote Workstation card into the Connection Broker, the Connection Broker calls the card using either its IP address or hostname, in order to obtain additional host card information, such as MAC address.
2. Install the Leostream Agent on the desktop, or restart the Leostream Agent if it was previously installed. When the Leostream Agent starts, it searches the registry for entries in the following key:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\PCI\
```

The Leostream Agent selects entries that contain 6549, 1200, and 2200, the PCoIP vendor codes. The Leostream Agent relies on the PCoIP Agent to return information about the PCoIP host card.

3. The Leostream Agent sends the Connection Broker all PCoIP information that can be identified from the registry key or PCoIP Agent, including MAC address. The Leostream Agent cannot retrieve the PCoIP host card name or IP address from the registry.
4. In addition, the Leostream Agent sends desktop information to the Connection Broker, including the desktop hostname and IP address.
5. The Connection Broker matches the PCoIP Remote Workstation card MAC address provided by the Leostream Agent to the MAC address of a card inventoried on the **> Resources > PCoIP Host Devices** page. Based on the desktop information provided by the Leostream Agent, the Broker maps the identified host card record to the desktop record on the **> Resources > Desktops** page.

## Automatic PCoIP Remote Workstation Card Mapping for a Linux Desktop

The Connection Broker uses the following procedure to match PCoIP Remote Workstation cards to the correct Linux desktops.

1. Load the PCoIP Devices into the **PCoIP Devices** center. You can accomplish this step using various methods, as described in [Step 2: Registering PCoIP Devices with the Connection Broker](#). After you load a PCoIP Remote Workstation card into the Connection Broker, the Connection Broker calls the card using either its IP address or hostname, in order to obtain additional host card information, such as MAC address.
2. Install the Leostream Agent onto the desktop, or restart the Leostream Agent if it was previously installed. When the Leostream Agent starts, it issues the following command to search for PCoIP PCI information:

```
lspci -xxxx -d6549:*
```

3. The Leostream Agent sends the Connection Broker all PCoIP information that can be identified from

the PCI, including MAC address. The Leostream Agent cannot retrieve the PCoIP host card name or IP address from the PCI.


4. In addition, the Leostream Agent sends desktop information to the Connection Broker, including the desktop hostname and IP address.
5. The Connection Broker matches the PCoIP Remote Workstation card's MAC address provided by the Leostream Agent to the MAC address of a host card inventoried on the **> Resources > PCoIP Host Devices** page. Based on the desktop information provided by the Leostream Agent, the Connection Broker maps the identified host card record to the desktop record on the **> Resources > Desktops** page.

### Confirming and Editing PCoIP Remote Workstation Card Mappings

To confirm or edit the desktop-to-PCoIP Remote Workstation card mapping:

1. Go to the **> Resources > Desktops** page.
2. Select the **Edit** action associated with the appropriate desktop.
3. Use the drop-down menus in the **PCoIP Host Device** section to assign PCoIP host card associated with this desktop.
  - a. If the desktop contains a single PCoIP host card, select that card from the **Primary Host Device** drop-down menu.
  - b. For desktops with two PCoIP host cards, select the second card from the **Secondary Host Device** drop-down menu. Desktops with two PCoIP cards can simultaneously attach to two PCoIP client devices, providing support for octal-monitor configurations.
4. Click **Save**.

---


 *If the PCoIP Remote Workstation cards are not correctly associated with the appropriate desktops, the Connection Broker cannot use PCoIP to connect a PCoIP client to the desktop.*

---

## Step 7: Defining Pools of Desktops

To share machines with a group of users, you combine the desktops into logical groups, or **pools**. Use pools to create sets of desktops that have similar attributes, or come from the same center.

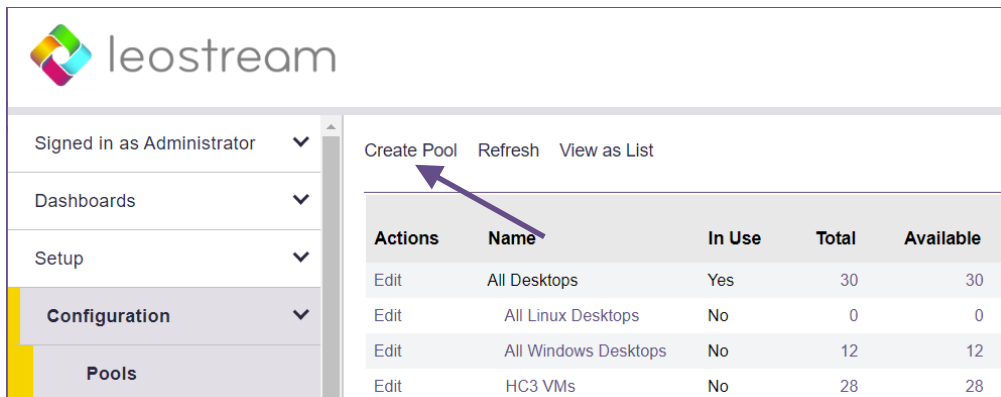
---

 The Leostream Connection Broker defines a **pool** as any group of desktops or applications.

---

To create a pool:

1. Go to the **> Configuration > Pools** page.
2. Click **Create Pool**, as shown in the following figure.



3. Enter the basic pool characteristics, as follows:
  - a. **Name:** a unique identifier for this pool
  - b. **Subset of pool:** The parent pool from which to draw desktops for this pool
  - c. **Define pool using:** The information to use when selecting desktops for this pool
4. Based on your selection in part c of step 3, enter the characteristics that define the pool. For example, if you select **Desktop attributes** from the **Define pool using** drop-down menu, the following figure shows the **Pool Definition** configured to create a pool defined as a subset of the **All Desktops** pool and including all desktops running a Windows operating system.

**Pool Definition**

Subset of pool

Define pool using

Desktop attribute	Conditional	Value
<input type="text" value="Operating system"/>	<input type="text" value="is equal to"/>	<input type="text" value="Windows (any version)"/>
<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>
<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>

☐ The desktops must match any of the attribute rules (OR)  
☒ The desktops must match all of the attribute rules (AND)


☐ Associate initial user login with assigned user  
*Executes assigned user's Power Control and Release Plans for the first user who logs into desktops in this pool*

5. Click **Save**.

After you finish entering your pools, the **Pools** page displays a hierarchy of all available pools. For a complete description of pools, see “Chapter 8: Creating Desktop Pools” chapter in the [Connection Broker Administrator’s Guide](#).

## Step 8: Defining Pool-Based Plans

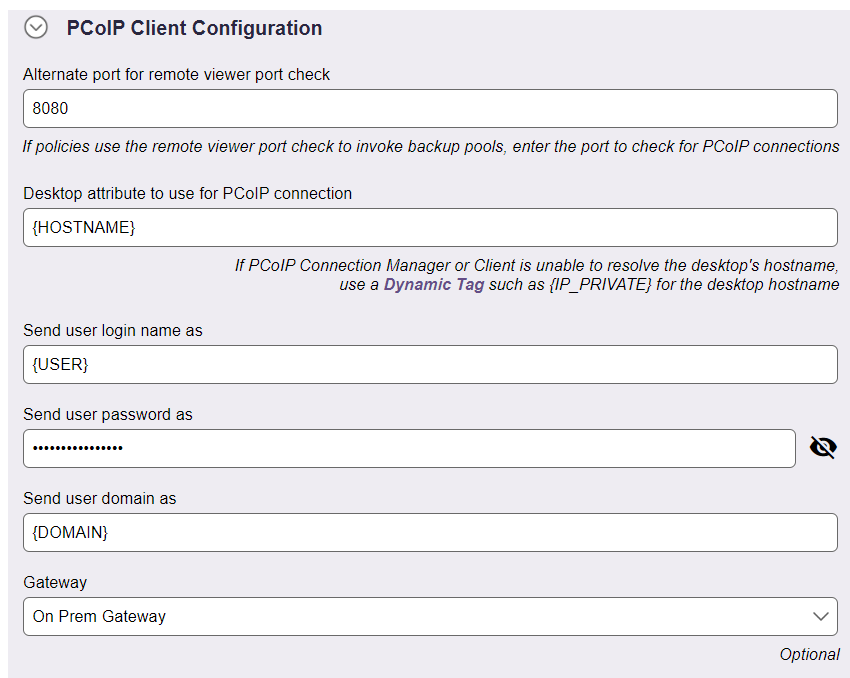
After you separate your desktops into pools, define plans that determine how the Connection Broker manages the user’s session.

 *The Leostream Connection Broker defines a **plan** as a set of behaviors that can be applied to any number of pools. This step describes three types of plans: 1) Power Control, 2) Release, and 3) Protocol.*

### Protocol Plans

#### *For PCoIP Zero Clients and HP Anyware Software Clients*

The Connection Broker always establishes a PCoIP connection when a user logs in using a PCoIP client. Use the **PCoIP Client Configuration** section of the Protocol Plan, shown in the following figure, to configure aspects of the connection.



The screenshot shows the 'PCoIP Client Configuration' section of a web interface. It contains several input fields and a dropdown menu, with some fields being optional. The fields are:

- Alternate port for remote viewer port check:** A text input field containing '8080'. Below it is a note: 'If policies use the remote viewer port check to invoke backup pools, enter the port to check for PCoIP connections'.
- Desktop attribute to use for PCoIP connection:** A text input field containing '{HOSTNAME}'. Below it is a note: 'If PCoIP Connection Manager or Client is unable to resolve the desktop's hostname, use a **Dynamic Tag** such as {IP\_PRIVATE} for the desktop hostname'.
- Send user login name as:** A text input field containing '{USER}'.
- Send user password as:** A text input field with masked characters (dots) and a toggle icon (an eye with a slash) to the right.
- Send user domain as:** A text input field containing '{DOMAIN}'.
- Gateway:** A dropdown menu with 'On Prem Gateway' selected.


The word 'Optional' is written in a smaller font at the bottom right of the configuration area.

1. In the **Alternate port for remote viewer port check** edit field, specify the port the Connection Broker should use when checking if the desktop is running and able to accept PCoIP connections.

2. By default, the Connection Broker sends the desktop's hostname when establishing connections using PColP. Use the **Desktop attribute to use for PColP connections** edit field to specify a different dynamic tag, such as {IP\_ADDRESS} or {IP\_PRIVATE}.
3. By default, the Connection Broker sends the user credentials used to log into your Leostream environment. To log the user into their remote desktop operating system as a different user, update the values in the **Set user login name as**, **Send user password as**, and **Send user domain as** fields.

If users share a set of fixed desktop operating system credentials, see "Using Fixed Desktop Credentials in the [Connection Broker Administrator's Guide](#) for instructions on how to configure the protocol plan to use those credentials.

4. For remote users logging in using a PColP Zero client or HP Anyware software client, you can send their PColP connections through the Leostream Gateway. Select the Leostream Gateway to use for connections from the **Gateway** drop-down menu. See [Using the Leostream Gateway for Remote Access](#) for more information.

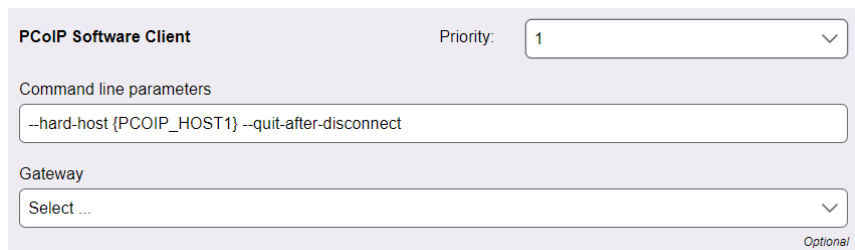
 Do not specify a Leostream Gateway if you are using the PColP Connection Manager and Security Gateway.

### For Leostream Connect Clients

Use the **Leostream Connect and Thin Clients Writing to Leostream API** section of the form to build a protocol plan for Leostream Connect logins. When establishing the connection, Leostream Connect launches the PColP software client using the parameters included in the **Command line parameters** field.

To configure the protocol plan:

1. Set the **Priority** of the **PColP Soft Client** to **1**, as shown in the following figure.



2. The value in the **Command line parameters** depends on if you are connection to a Remote Workstation Card or the HP Anyware software.
  - The default value is adequate for connection to workstations with an installed Remote Workstation Card. It specifies the IP address of the Remote Workstation Card installed on the user's desktop, passed to the PColP software client using the `--hard-host` parameter.

To provide single sign-on to the remote desktop, ensure that the user's policy selects the **Enable single sign-on to desktop console** option and the Leostream Agent was installed on the remote workstation with the single sign-on task selected.

- To connect to desktops running an HP Anyware agent, update the default command line parameters to send the user credentials and desktop IP, for example:  
`-b {IP_ADDRESS} -u {USER} -d {DOMAIN} -p {PLAIN_PASSWORD}`
- 3. Optionally, use the **Gateway** drop-down menu to send the PCoIP connection through a Leostream Gateway or Gateway Cluster.
- 4. Set the **Priority** of the remaining protocols to **Do not use**.

**NOTE:** The `--quit-after-disconnect` parameter forces the PCoIP software client to close after the PCoIP connection disconnects. This parameter does not close the PCoIP software client when the user logs out of the desktop. Therefore, when the Connection Broker receives a log out notification from the Leostream Agent, the Connection Broker attempts to manually disconnect the PCoIP connection at the Remote Workstation Card, which closes the client.

### For Leostream Web Clients

For users logging in from the Leostream Web client, select **1** for the **Priority** of the **PCoIP Soft Client** in the **Web Browser** section of the protocol plan, as shown in the following figure.

The screenshot shows the 'PCoIP Software Client' configuration form. At the top, there is a 'Priority' dropdown menu set to '1'. Below this is a text field for 'Hostname or IP address of PCoIP Connection Manager' containing 'gateway\_external\_ip.mydomain.com'. A checkbox labeled 'Send username in Azure AD format to log into Entra ID-joined desktop' is unchecked. Below this are two text fields: 'Send user domain as' containing '{DOMAIN}' and 'Send user login name as' containing '{USER}'. Another text field 'Desktop attribute to use for PCoIP connection' contains '{IP\_PRIVATE}'. A note below this field states: 'If PCoIP Connection Manager or Client is unable to resolve the desktop's hostname, use a Dynamic Tag such as {IP\_PRIVATE} for the desktop hostname'. At the bottom, there is a 'Gateway' dropdown menu set to 'Leostream Gateway' and an 'Optional' label.

1. In the **Hostname or IP address of PCoIP Connection Manager** edit field, enter in the appropriate address depending on your use case and architecture, as follows.
  - a. If the user's HP Anyware client can communicate with your Leostream Connection Broker to initiate the PCoIP session, leave this field blank.
  - b. If users are remote and the HP Anyware client communication need to traverse a Leostream Gateway, enter the Leostream Gateway address.
2. The Leostream Web client uses a URI to launch the PCoIP software client. In the URI, you can set default values to enter for the username and domain.
  - a. If the remote desktop is joined to an Entra ID domain and requires the username in

AzureAD format, check the **Send username in Azure AD format to log into an Entra ID-joined desktop** option. After checking this option, ensure that the **Send user login name as** edit field contains a dynamic tag that resolves to the user's UserPrincipalName. The initial value in this field is a default Entra ID attribute returned in the SAML assertion that logged the user into your Leostream environment, however ensure that you check or modify that attribute, as required by your environment.

With this option selected, the Connection Broker always sends the user login name to the remote operating system in the following format:

AzureAD\UserPrincipalName

- b. If the remote desktop is not joined to an Entra ID domain, use the **Send user domain as** and **Send user login name as** edit fields to set these default values.

In either case, the user is prompted for their password by PCoIP software client to connect to their desktop.

3. By default, the Connection Broker sends the desktop's hostname when establishing connections using PCoIP. Use the **Desktop attribute to use for PCoIP connections** edit field to specify a different dynamic tag, such as {IP\_ADDRESS} or {IP\_PRIVATE}.
4. If needed, select a Leostream Gateway from the **Gateway** drop-down menu to send the PCoIP connection from the HP Anyware client to the desktop through a Leostream Gateway or Gateway Cluster.

### ***Logging into Entra ID-Joined Desktops***

If the remote operating systems requires users to log in with their Azure AD credentials, ensure that you select the **Send username in Azure AD format to log into Entra ID-joined desktops** option in the protocol plan.

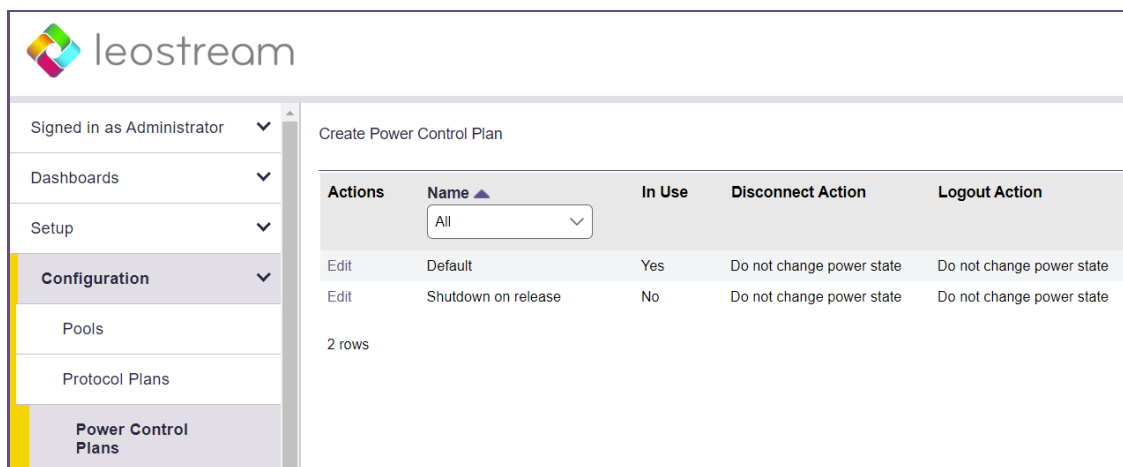
With this option selected, the Connection Broker ignores the user's domain and always sends the username in the following format,

AzureAD\UserPrincipalName

See [For Leostream Web Clients](#) for complete instructions on building protocol plans for launching PCoIP connections.

## Power Control Plans

Power control plans define what power control action is taken on a desktop when the user disconnects or logs out of the desktop or when the desktop is released to its pool. Available power control plans are shown on the **> Configuration > Power Control Plans** page, shown in the following figure.



New Connection Broker installations contain one default power control plan, called **Default**. You can create as many additional power control plans as needed for your deployment. To build a new power control plan:

1. Click the **Create Power Control Plan** link on the **> Configuration > Power Control Plans** page. The **Create Power Control Plan** form, shown in the following figure, opens.

**Create Power Control Plan**

Plan name:

When User Disconnects from Desktop  
Wait: 0 minutes then Do not change power state

When User Logs Out of Desktop  
Wait: 0 minutes then Do not change power state

When Desktop is Released  
Wait: 0 minutes then Do not change power state

When Desktop is Idle  
Wait: 0 minutes then Do not change power state


Enter a descriptive name. You'll refer to this name when assigning the plan to a pool.

Select the amount of time to wait before changing the desktop's power state. A wait time of zero tells the Connection Broker to immediately execute the selected power control action.

Select the power control action to take after the wait time elapses. For the Connection Broker to take actions based on disconnect or idle-time events, you must install the Leostream Agent on that desktop.

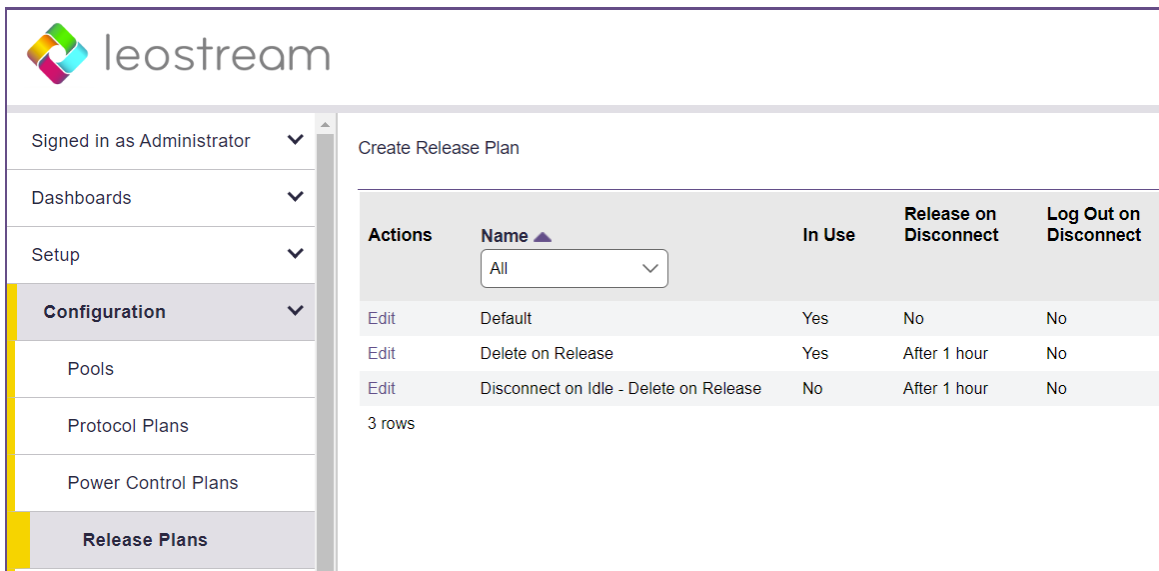
2. Enter a unique name for the plan in the **Plan name** edit field.
3. For each of the remaining sections:

- a. From the **Wait** drop-down menu, select the time to wait before applying the power action.
  - b. From the **then** drop-down menu, select the power control action to apply. Selecting **Do not change power state** renders the setting in the **Wait** drop-down menu irrelevant, as no action is ever taken.
4. Click **Save** to store the changes or **Cancel** to return to the **> Configuration > Power Control Plans** page without creating the plan.

 *The desktop must have an installed and running Leostream Agent to allow the Connection Broker to distinguish between user logout and disconnect and to perform actions based on idle time.*

## Release Plans

Release plans determine how long a desktop remains assigned to a user. When the assignment is broken, the Connection Broker releases the desktop back to its pool, making it available for other users. Available release plans are shown on the **> Configuration > Release Plans** page, shown in the following figure.



Actions	Name ▲	In Use	Release on Disconnect	Log Out on Disconnect
	<input type="text" value="All"/>			
<a href="#">Edit</a>	Default	Yes	No	No
<a href="#">Edit</a>	Delete on Release	Yes	After 1 hour	No
<a href="#">Edit</a>	Disconnect on Idle - Delete on Release	No	After 1 hour	No
3 rows				

New Connection Broker installations contain one default release plan. The default release plan is designed to keep the user assigned to their desktop until they log out. When the user logs out, the Connection Broker releases the desktop back to its pool. You can create as many additional release plans as needed for your deployment.

For example, the following procedure shows how to build a release plan that forcefully logs the user out an hour after they disconnect from their desktop. The logout event then triggers the **When User Logs Out of Desktop** section of the release plan, which releases the desktop back to its pool and removes the user's assignment to the desktop

1. Click the **Create Release Plan** link on the **> Configuration > Release Plans** page. The **Create Release Plan** form, shown in the following figure, opens. The figure describes additional use cases you can model using Release Plans.

The screenshot shows the 'Create Release Plan' form with several sections and fields. Annotations with arrows point to specific fields and sections:

- Plan name:** A text input field at the top.
- When User Disconnects from Desktop:** A section containing:
  - Release to pool:** A dropdown menu with 'No' selected.
  - Log user out:** A dropdown menu with 'After 1 hour' selected.
  - URL to call:** A text input field.
- When User Logs Out of Desktop:** A section containing:
  - Release to pool:** A dropdown menu with 'Immediately' selected.
  - URL to call:** A text input field.
- When Connection is Closed:** A section containing:
  - Execute actions for:** A dropdown menu with 'When User Logs Out of Desktop' selected.
- When Desktop is Idle:** A section containing:
  - Lock desktop:** A dropdown menu with 'No' selected.
  - Disconnect:** A dropdown menu with 'No' selected.
  - Log user out:** A dropdown menu with 'No' selected.
- When Desktop is First Assigned:** A section containing:
  - Release to pool:** A dropdown menu with 'No' selected.
  - Release if user does not log in:** A dropdown menu with 'No' selected.
- When Desktop is Released:** A section containing:
  - Log user out of the desktop:** A checkbox that is checked.
  - Suspend logout and display warning message to user:** A dropdown menu with 'No' selected.
  - Delete virtual machine from disk:** A dropdown menu with 'No' selected.

Small text annotations include: 'This section of the plan executes when no Leostream Agent is installed or communicating on the remote desktop' and '\*When Desktops Released' actions will not be invoked'.

Enter a descriptive name. Refer to this name when assigning this plan to pools.

To model a persistent desktop, ensure that the desktop is not released when the user disconnects or logs out.

If a Leostream Agent is not installed on the remote desktop, the Connection Broker cannot distinguish when the user disconnects or logs out of their desktop. If the user logs in using Leostream Connect, the client sends a Connection Close event, and you can determine if the Disconnect or Log out portion of the release plan should be executed.


You can perform actions on the desktop after the user's session is idle for the selected elapsed time. In addition, you can monitor the desktop's CPU levels to ensure that any processes the user is running come to completion before you forcefully log them out.

You can release a desktop back to its pool after a specified elapsed time since the desktop was initially assigned to the user. After the desktop is released, if the user remains logged in, the Connection Broker considers them to be **rogue**.

To avoid rogue users, forcefully log out the user when the desktop is released to its pool.


Use this option to have the Connection Broker completely delete the VM from disk as soon as the desktop is released to its pool. The Connection Broker deletes the VM only if the "Edit Desktop" page for that VM selects the "Allow this desktop to be deleted from disk" option.

2. Enter a unique name for the plan in the **Plan name** edit field.
3. In the **When User Disconnects from Desktop** section, select **after 1 hour** from the **Forced Logout** drop-down menu.
4. Click **Save**.

 **The desktop must have an installed and running Leostream Agent for the Connection Broker to distinguish between user logout and disconnect and to perform actions based on idle time.**

## Step 9: Defining User Policies

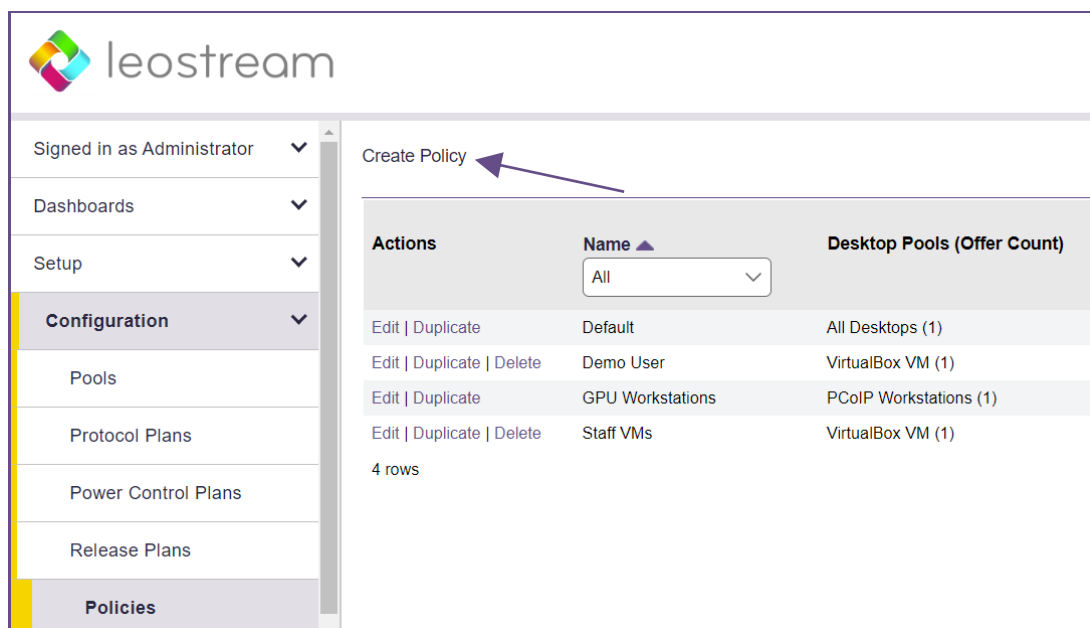
After you define pools and plans, build policies.

 *The Leostream Connection Broker defines a **policy** as a set of rules that determine how desktops are offered, connected, and managed for a user, including what specific desktops are offered, which Power Control and Release plans are applied to those desktops, what USB devices the user can access in their remote desktop, and more.*

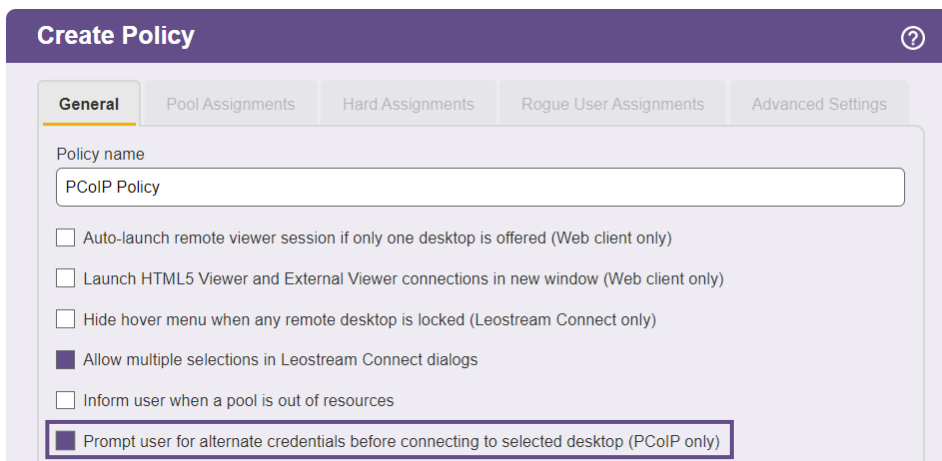
The Connection Broker provides a Default policy that applies if no other policy exists or is applicable. The Default policy assigns one desktop from the All Desktops pool. You can create additional policies, as follows:

You can create additional policies, as follows:

1. Go to the **> Configuration > Policies** page.
2. Click **Create Policy**, shown in the following figure.



3. In the **Create Policy** form, enter a name for the policy in the **Policy name** edit field. For a discussion of the remaining general policy properties, see the [Connection Broker Administrator's Guide](#).
4. If you are using PIV/CAC cards for Leostream login or if you need to use different user credentials to log into the remote operating system than used to log into Leostream, select the **Prompt user for alternate credentials before connecting to selected desktop** option in user's policy, as shown in the following figure.



**Create Policy**

**General** | Pool Assignments | Hard Assignments | Rogue User Assignments | Advanced Settings

Policy name  
PCoIP Policy

☐ Auto-launch remote viewer session if only one desktop is offered (Web client only)

☐ Launch HTML5 Viewer and External Viewer connections in new window (Web client only)

☐ Hide hover menu when any remote desktop is locked (Leostream Connect only)

☒ Allow multiple selections in Leostream Connect dialogs

☐ Inform user when a pool is out of resources

☒ Prompt user for alternate credentials before connecting to selected desktop (PCoIP only)

This option applies only when logging in using a PCoIP Zero client or HP Anyware client. With this option selected:

- The user points the PCoIP client at the Connection Broker and clicks **Connect**.
  - The Connection Broker determines the initial mode of authentication, either username/password or smart card.
  - If the initial authentication succeeds, the Connection Broker returns the user's list of offered desktop.
  - The Zero client displays this list and instructs the user to select the desktop to connect to and to enter the username and password to send to that desktop.
  - The PCoIP connection then start, using the alternate credentials entered when the desktop was selected.
5. Click **Save** to initialize the policy.
  6. Go to the **Pool Assignments** tab.
  7. Click the **Add Pool Assignments** link. The **Edit Pool Assignment** form opens.
  8. In the **When User Logs into Connection Broker** section use the **Number of desktops to offer** drop-down menu to indicate the number of desktops to offer to a user of this policy.
  9. Also, in this section, use the **Pool** menu to select the pool to offer desktops from. When a user is offered this policy, the Connection Broker sorts the desktops in the selected pool based on the other Pool Assignment settings, then offers the user the top  $n$  desktops from the pool, where  $n$  is the number selected in the **Number of desktops to offer** drop-down menu
  10. If this pool offers workstations with an installed Remote Workstation Card and you are using the Leostream Agent for single sign-on in the **When User Connects to Desktop** section, shown in the

following figure, select the **Enable single sign-on to desktop console** option to have the Connection Broker pass the user's credentials to the Leostream Agent for single sign-on. You do not need to select this option when connecting to machines running an HP Anyware agent.

When User Connects to Desktop

Log user into remote desktop as: <Determined by user's role>

☐ Log out any rogue users (also applies when reconnecting to assigned desktop)

☒ Enable single sign-on to desktop console (PCoIP only)



In a simple proof-of-concept environment, many of the remaining Pool Assignment settings can be left at their default values. Note that, by default, the Connection Broker does not offer a desktop to the user if the desktop does not have an installed Leostream Agent. If you want to offer desktops that do not have a Leostream Agent, select the **Yes, regardless of Leostream Agent status** option from the **Offer running desktops** drop-down menu.

11. In the **Plans** section, select the protocol, power control, and release plans we created in this example. When the user requests a connection to one of the offered desktops in the pool, the Connection Broker associate these plans with that desktop.

12. Click **Save**.



*A policy can offer desktops from multiple pools. Click the **Add Pool Assignment** link to add a new pool, or use the kebab menu to clone an existing Pool Assignment to simplify initializing the options for an additional pool.*

See the “Configuring User Experience by Policy” chapter of the [Connection Broker Administrator's Guide](#) for information on using the additional options in the **Create Policy** form.

## Step 10: Creating Locations that Require PIV/CAC Logins

Leostream supports PIV/CAC card logins only for users logging in using PCoIP Zero clients. You indicate which Zero clients require PIV/CAC card logins using Leostream Locations.

1. Go to the **> Configuration > Locations** page.
2. Create a new location.
3. Select the **Require PIV smart card for login** option, as shown in the following figure.

PCoIP software or mobile clients that fall into this location will not require PIV card logins.

Create Location

Name

PCoIP

Subset of location

All

Attribute Selection

Client attribute	Conditional	Value
Device type	is equal to	PCoIP

[Add rows]

☐ The Clients must match any of the attribute rules (OR)
 ☒ The Clients must match all of the attribute rules (AND)

Plans

Protocol:

<Determined by policy>

PCoIP Zero Client Authentication

NOTE: A CA certificate or bundle file must also be uploaded to the Authentication Server(s)

☒ Require PIV smart card for login

When using smart card authentication, if you require single sign-on, the user's policy must select the **Prompt user for alternate credentials before connecting to selected desktop** option. In this case, the workflow of a user login is as follows.

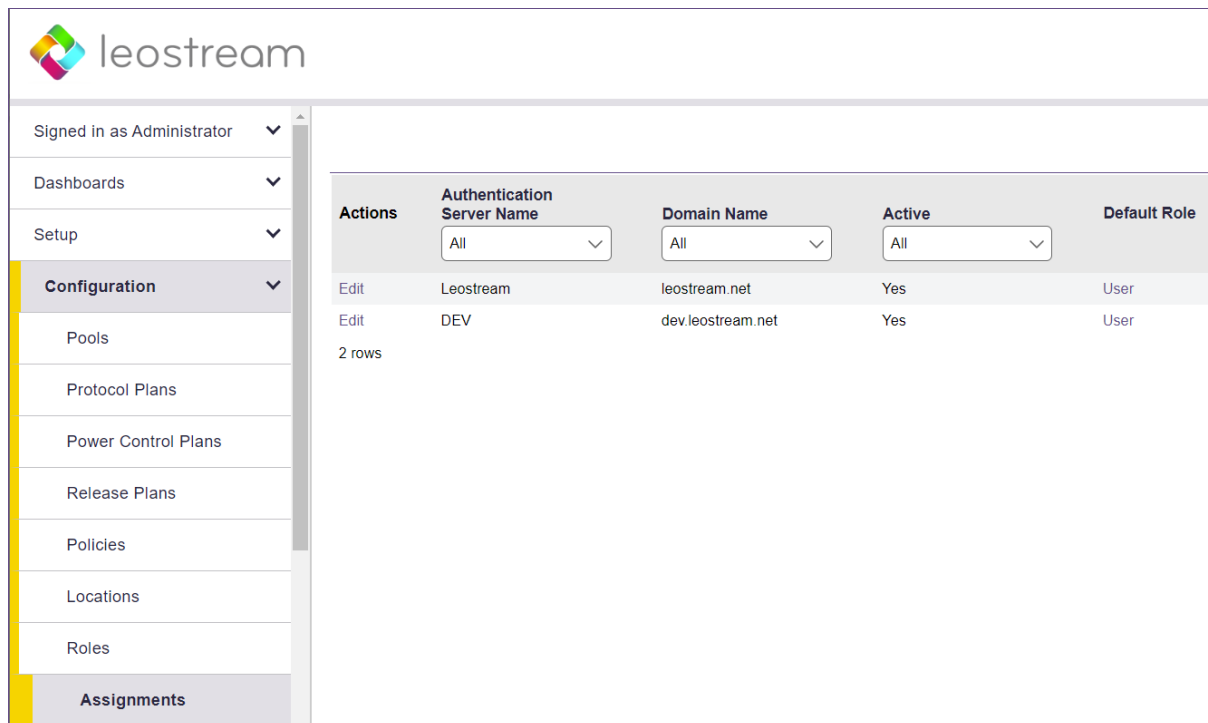
- The user points the Zero client at the Connection Broker and clicks **Connect**.
- Leostream checks if that PCoIP clients fall into a location that requires smart card logins.
- If the Zero Client is in a location that requires a smart card, it displays a prompt for the user's smart card or, if it's already inserted, asks for the PIN.
- The zero client uses the PIN to unlock the smart card. A validation process then takes place between the Zero client, Connection Broker, and Active Directory to ensure that the smart card contains a valid certificate.
- The Connection Broker then uses the `userPrincipalName`, or email address if the `userPrincipalName` is not available, from the certificate to identify the user and determine their policy.

- The Connection Broker returns the user's list of offered desktop and the Zero client displays this list. At this point:
  - a. If the user's policy selects the **Prompt user for alternate credentials before connecting to selected desktop** option, the Zero client prompts the user to select the desktop to connect to and enter the username and password for that desktop. The alternate credentials are passed to the Leostream Agent on the remote workstation to use for single sign-on.
  - b. If the user's policy does not require alternate, the user selects the desktop to connect to and Leostream establishes the PColP connection from the Zero client to the Remote Workstation Card. At this point, the user must manually log into the remote operating system.

## Step 11: Assigning Policies to Users

When a user logs in to the Connection Broker, the Connection Broker searches the authentication servers on the **> Setup > Authentication Servers** page for a user that matches the credentials provided by the user.

The Connection Broker then looks on the **> Configuration > Assignments** page, shown in the following figure, for the assignment rules associated with the user's authentication server. For example, if the Connection Broker authenticated the user in the `LEOSTREAM` domain defined on the **> Setup > Authentication Servers** page, the Connection Broker would look in the `LEOSTREAM` assignment rules in the following figure.



The screenshot shows the Leostream web interface. The top navigation bar includes the Leostream logo and a user profile dropdown showing 'Signed in as Administrator'. The left sidebar contains a menu with 'Configuration' expanded, showing sub-items like 'Pools', 'Protocol Plans', 'Power Control Plans', 'Release Plans', 'Policies', 'Locations', 'Roles', and 'Assignments'. The main content area displays a table of assignment rules.

Actions	Authentication Server Name	Domain Name	Active	Default Role
Edit	Leostream	leostream.net	Yes	User
Edit	DEV	dev.leostream.net	Yes	User

Below the table, it indicates '2 rows'.

To assign policies to users in a particular authentication server, click the **Edit** link associated with that authentication server on the **> Configuration > Assignments** tab, shown in the previous figure. The **Edit**

**Assignment** form for this authentication server appears, shown in the following figure.

Domain name  
leostream.net

**Assigning User Role and Policy**  
In this section, you can set up rules to assign Users to Roles and Policies based on their group membership. Optionally, use the Order column to re-order the rows.

Order	Group	Client Location	MFA Provider	User Role	User Policy
1	[any group]	Leostream	<Not required>	User	GPU Workstations
2		All	<Not required>	User	Default
3		All	<Not required>	User	Default
4		All	<Not required>	User	Default

[Add rows]

Default MFA Provider  
<Not required>

Default Role  
User

Default Policy  
Default

☐ Assign policies using explicit LDAP expressions (This cannot be undone without removing all assignment rules)

Users will be assigned the default role and policy if they don't match an assignment rule

You must save this form for this setting to take effect

By default, the Connection Broker matches the selection in the **Group** drop-down menu to the user's `memberOf` attribute in Active Directory.



*If you modified your groups since you last signed into your Connection Broker, you must sign out and sign back in to have your Connection Broker reflect the authentication server changes.*

To assign rules based on the user's group attribute:

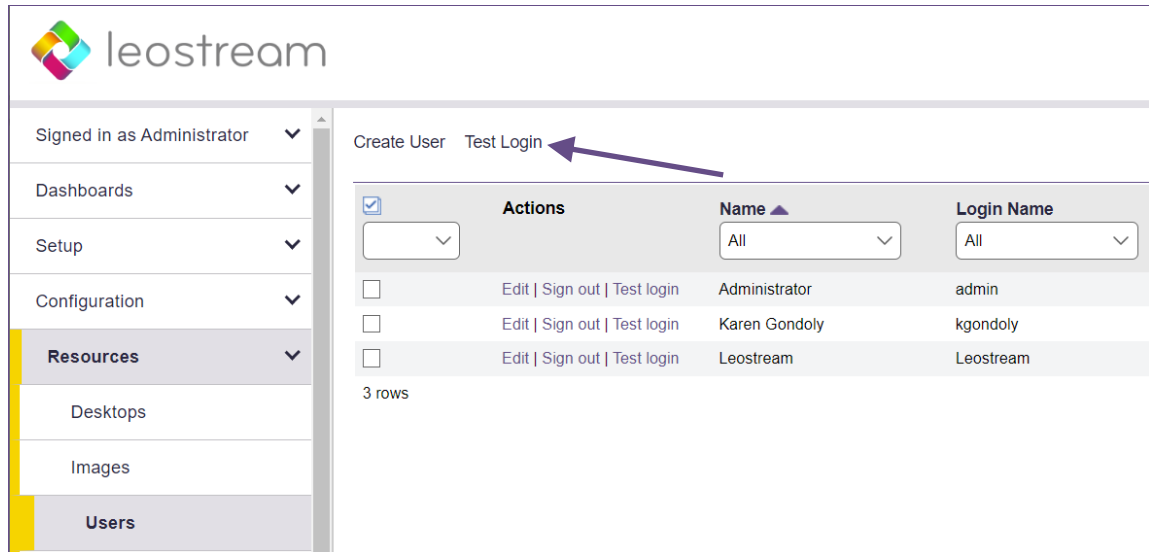
1. Select the group attribute from the **Group** drop-down menu
2. If you are using locations, select a location from the **Client Location** drop-down menu
3. Assign permissions to this group and client location pair by selecting an item from the **User Role** drop-down menu
4. Assign a policy by selecting an item from the **User Policy** drop-down menu

If you need to assign roles and policies based on a different user attributes, see "Assigning Roles and Policies Based on any Attribute" in Chapter 14 of the [Connection Broker Administrator's Guide](#).

## Step 12: Testing User Login

To test your Connection Broker, ensure that users are being correctly assigned to their desktops, as follows:

1. Navigate to the **> Resources > Users** page. As users log into your Leostream environment, their user information is added to this page. You do not need to load users before they can log in.
2. Click **Test Login**, as shown in the following figure:



3. In the **Login Test** form that opens, enter the name of the user to test in the **User Name** edit field.
4. If you are allowing the user to specify their domain, select a domain from the **Domain** drop-down menu.
5. Use the **Filter client list by location** drop-down menu to restrict the clients shown in the **Clients** drop-down menu. You create these locations on the **> Configuration > Locations** page. If you are not using locations, select **All**.
6. If you have any clients loaded into your Connection Broker, use the **Client** menu to select the client you want to test this user logging in from.
7. Click **Run Test**. The Connection Broker searches the authentication server for your user, and then presents a report, for example:

## Chapter 2: Configuring the Connection Broker

---

### Test Results

User name: Maybel  
Authentication server: Leostream  
Domain: leostream.net  
Client: Chrome/91.0 (Web Browser) at 10.110.3.40  
(This client is in these locations: Web browsers, All)

Looking up user "Maybel":  
in authentication server "Leostream" ← **found user** ([show Active Directory attributes](#))

Trying to match with Authentication Server Assignment rules: ([edit](#))

- 1: "memberOf" exactly matches "CN=Karen Test Sub Group,OU=Karen Test,OU=Karen Groups,DC=leostream,DC=net", location "All" ← no attribute match
- 2: "memberOf" exactly matches "CN=Students,OU=Security Groups,DC=leostream,DC=net", location "All" ← **matched**

**User will have Role "User" and Policy "Default"**

User must first successfully authenticate with RADIUS server "Okta RADIUS Agent" ← **PIN+token not provided**

User's role provides access to Web Client, only.

**Policy: Default** ([edit](#))

No hard-assigned desktops found

**Pool "All Desktops"** ([edit](#))

Including pool for all users

Looking for two desktops

Policy settings for this pool:

- follow-me mode
- do not allow users to change power state of offered desktops
- offer powered-on desktops without a running Leostream Agent
- do not offer stopped/suspended desktops
- favor previously-assigned desktops
- may offer desktops with pending reboot job
- do not confirm desktop power state
- do not power on stopped desktops
- do not log out rogue users
- do not attempt single sign-on into desktop console session
- allow manual release (but Maybel's role prevents it)
- Power control plan: Default
  - when user disconnects, do not change power state
  - when user logs out, do not change power state
  - when desktop is released, do not change power state
  - when desktop is idle, do not change power state
- Release plan: Default
  - handle unverified user state as disconnect
  - do not release on disconnect
  - do not log user out on disconnect
  - when user logs out, release immediately
  - do not lock desktop if idle
  - do not disconnect user if desktop is idle
  - do not log user out if desktop is idle
  - do not release after initial assignment
  - if user does not log in, release

(389 total, 383 in service, 18 policy filtered, 18 pool filtered, 18 available, 8 running, 8 with an IP address)

kdg-debian9 ← **available**, running, Leostream Agent v5.1.22.0, will offer as: "kdg-debian9", will connect via RDP ([show](#)) ← will use protocol plan "Default" associated with policy [Default](#)  
kdg-1803 ← **available**, running, Leostream Agent v7.3.13.0, will offer as: "kdg-1803", will connect via RDP ([show](#)) ← will use protocol plan "Default" associated with policy [Default](#)

Offering two desktops with this policy.

See "Testing User Role and Policy Assignment" in the [Connection Broker Administrator's Guide](#) for information on interpreting test login results.



*Please complete a login test before contacting Leostream Support.*

---

## Step 13: Logging into the Leostream Platform

### Using PColP Zero Clients

Users can log into Leostream using any PColP Zero client.



*If you previously used the PColP zero client in a VMware Horizon View environment, you must reset the PColP processor to its factory defaults before you can manage the PColP zero client with the Leostream Connection Broker.*

To log into Leostream from a PColP Zero Client:

1. In the PColP client's **Configuration** dialog or Web interface, go to **> Configuration > Session**
2. Set the **Connection Type** to **PCoIP Connection Manager**.
3. In the **Server URI** field, enter the address of your Leostream environment.
4. Save the changes.

You do not need to reboot the PColP zero client for the changes to take effect. However, the client does not appear on the **> Resources > Clients** page until you click **Connect** on the PColP zero client.

If you need to register multiple PColP zero clients with the Connection Broker in order to hard-assign clients to desktops, you can bulk upload clients listed in a CSV-file. See [Uploading PColP Zero Clients](#) for more information.

### Using an HP Anyware Software Client

End users can log into your Leostream environment using any HP Anyware software or mobile client. First, create a saved connection for your Leostream environment, as follows:

1. Launch the HP Anyware client.
2. If this is the first time connecting to the Leostream environment, click the **Add connection** button.
3. In the **Host Address or Registration Code** edit field, enter the FQDN of your Leostream environment.

You must have a valid certificate installed on your Leostream Connection Brokers and/or Leostream Gateways to continue.

4. Enter a descriptive name in the **Connection Name** field.
5. Click **Save**.

After you have a saved connection, to log into Leostream:

1. Click on the saved connection for your Leostream environment.
2. Select the domain to log into from the top drop-down menu.

If you defined any authentication servers in your Leostream Connection Broker, local users are unable to log in using an HP Anyware client.

3. Enter your username and password in the **Username** and **Password** edit fields, respectively.
4. Click **Connect**.
5. Your list of offered desktops is displayed on the **Desktop selection** screen. Click on the desktop you wish to connect to and the PCoIP connection launches.

### Using Leostream Connect

If you need to support local users in addition to domain users, or have users that launch connections using other display protocols in addition to PCoIP, they can use Leostream Connect to launch the HP Anyware software client.

The users must install version 20.04.1 or later of the HP Anyware client on the client device running Leostream Connect.

To use Leostream Connect, ensure that the **Options** dialog points the Leostream Connect client to your Leostream environment. Users log in using their username and password, with multi-factor authentication supported using a RADIUS server.

Leostream Connect does not currently support PIV/CAC smart card logins, nor does it support the policy option to enter alternate credentials for the remote workstation. When connecting to machines running the HP Anyware agent, the user credentials on the remote desktop must be the as those used to log into your Leostream environment. For physical workstations with an installed Remote Workstation Card, if the workstation requires different credentials than are used to log into Leostream, disable the user's policy option to perform single sign-on and require the user enter the alternate credentials directly on the remote operating system.

# Using the Leostream Gateway for Remote Access

## Overview

The Leostream Gateway supports PCoIP connections to workstations with an installed Remote Workstation Card and to machines (virtual, cloud, or physical) running the HP Anyware agent. No PCoIP Connection Manager or Security Gateway is required.

Users can connect from any PCoIP Zero client, HP Anyware client, Leostream Web client, or Leostream Connect client.

## The Leostream Network Architecture

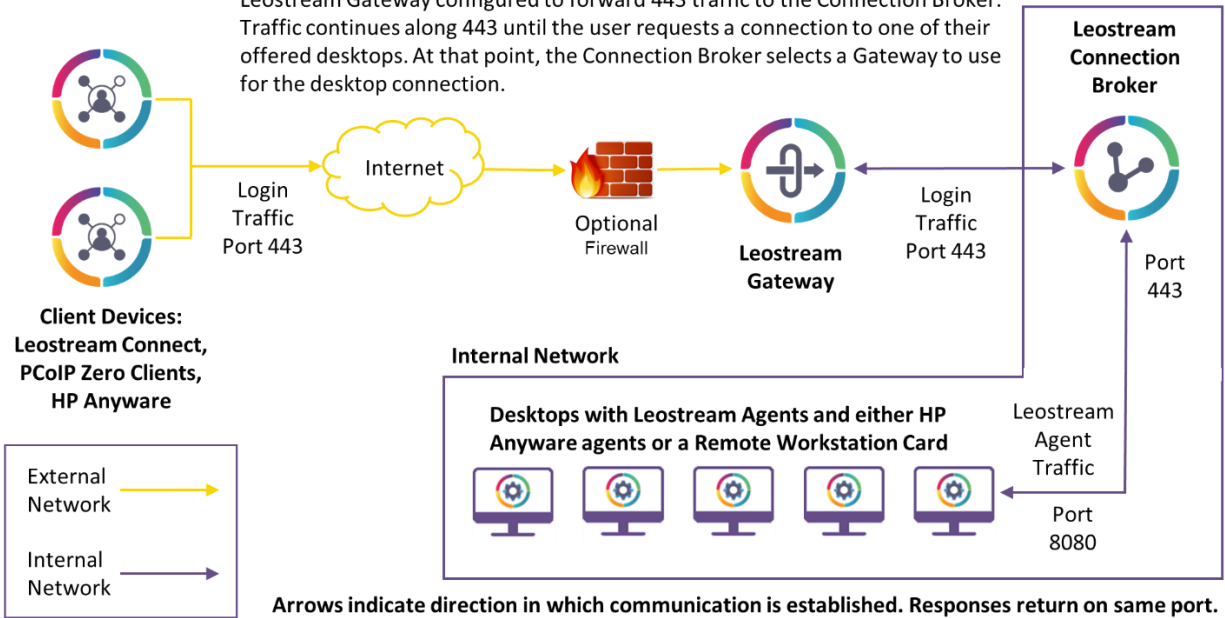
The Leostream Gateway serves two purposes when connecting remote users to your Leostream environment and their hosted workstations.

1. Forwarding login traffic to the Connection Broker
2. Initiating the HP Anyware client session when launching the client from a Leostream Web client login
3. Forwarding PCoIP traffic from the PCoIP Zero client or HP Anyware software client to the remote desktop

When building a Leostream environment, you must configure your network to open all ports required for communication between the different components. The following diagrams illustrate the simple network topology required for the two steps in the remote access workflow.

### Leostream Remote Access Workflow – Step 1: Login

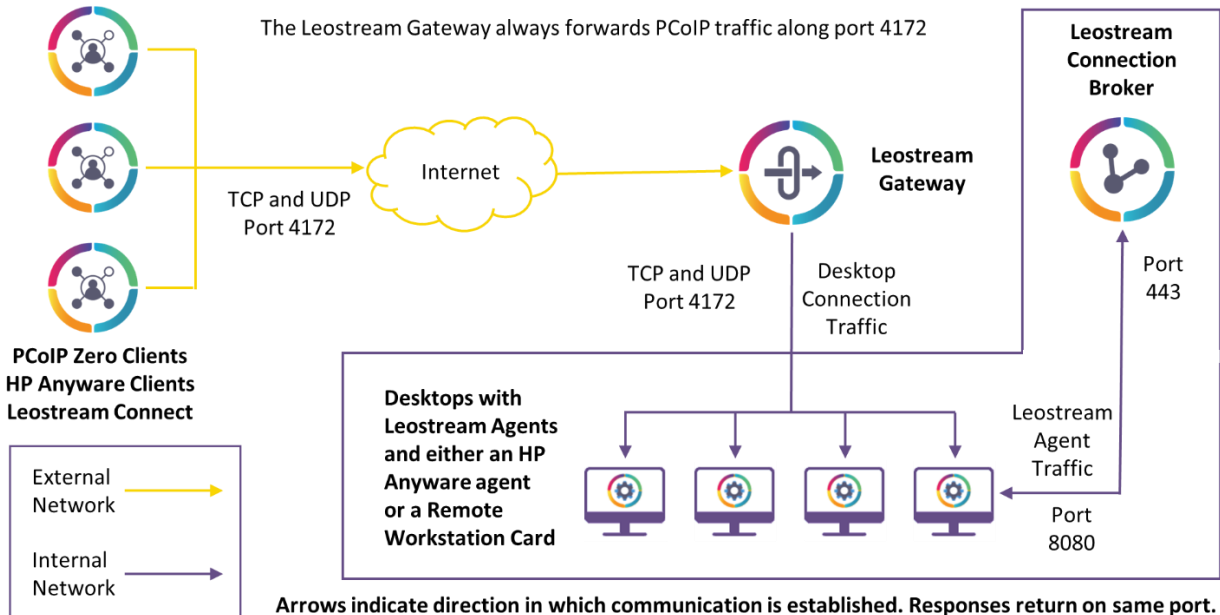
Leostream Gateway configured to forward 443 traffic to the Connection Broker. Traffic continues along 443 until the user requests a connection to one of their offered desktops. At that point, the Connection Broker selects a Gateway to use for the desktop connection.



Port 8080 is the default Leostream Agent port. If you change the port during or after installation, ensure that your network opens the corresponding port.

### Step 2: PCoIP Connections through the Leostream Gateway

The Leostream Gateway always forwards PCoIP traffic along port 4172



## How the Leostream Gateway Works

In the network diagrams included in the previous section, your users are located outside of the network that hosts your desktops. Your Leostream Connection Broker is co-located in the desktops' network. Sitting

in between the two networks, with access to both, is the Leostream Gateway, which provides an access point for the Connection Broker to initiate user logins.

For example, for a user to log into their Leostream environment, the user points their PCoIP Zero client at the public-facing address of the Leostream Gateway.

The user provides their login credentials, the Leostream Gateway sends those credentials to the Connection Broker, and the Connection Broker uses those credentials to authenticate and identify the user and assign them to a Leostream policy, which determines which desktops the user may connect to.

When the user requests a connection to one of their offered desktops, the Connection Broker informs the Leostream Gateway about the desktop's address. All communication between the Leostream Gateway and Leostream Connection Broker is on port 443.

At that point, the Leostream Gateway configures firewall rules to open the ports required to redirect the PCoIP traffic from the user's client device to the Remote Workstation Card or remote desktop.

The Leostream Gateway receives display protocol traffic from the remote desktop on the default display protocol port, in this case, 4172. You do not need to configure your remote desktops for use with the Leostream Gateway. From the remote desktop's perspective, it's transmitting the display protocol data to the Leostream Gateway along the default display protocol port. The Gateway then redirects the traffic to the client IP and display protocol port on the user's client.

When the user logs out or disconnects from their remote desktop, the Leostream Gateway closes the port in its firewall, blocking access to that VM.

For a complete description of all Leostream Gateway functionality, see the [Leostream Gateway Guide](#).

## Appendix A: Working with PCoIP Clients

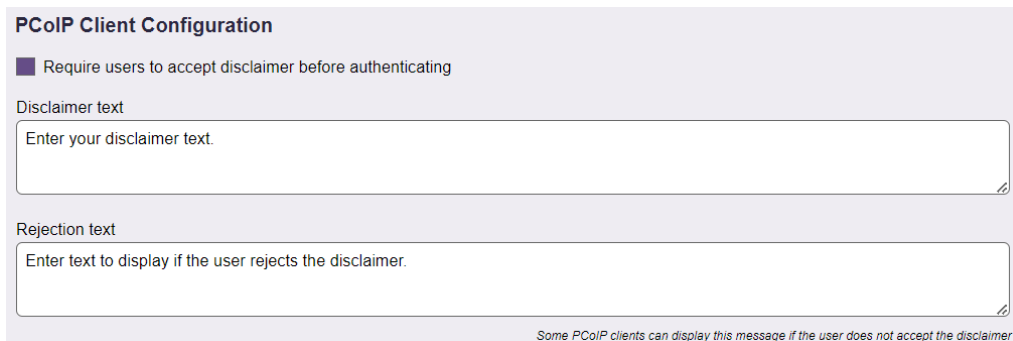
### Displaying a Disclaimer before PCoIP Client Logins

PCoIP connections typically result in single sign-on to the remote operating system. This may be incompatible with Microsoft GPOs used to display a disclaimer prior to the remote operating system login.

For these cases, you can use Leostream to display a disclaimer to the user before they log into your Leostream environment and connect to their desktops. Disclaimers display on PCoIP Zero clients, software clients, and mobile clients.

You enable disclaimers, as follows.

1. Scroll down to the **PCoIP Client Configuration** section on the **> System > Settings** page in your Connection Broker, shown in the following figure.



**PCoIP Client Configuration**

☒ Require users to accept disclaimer before authenticating

Disclaimer text

Enter your disclaimer text.

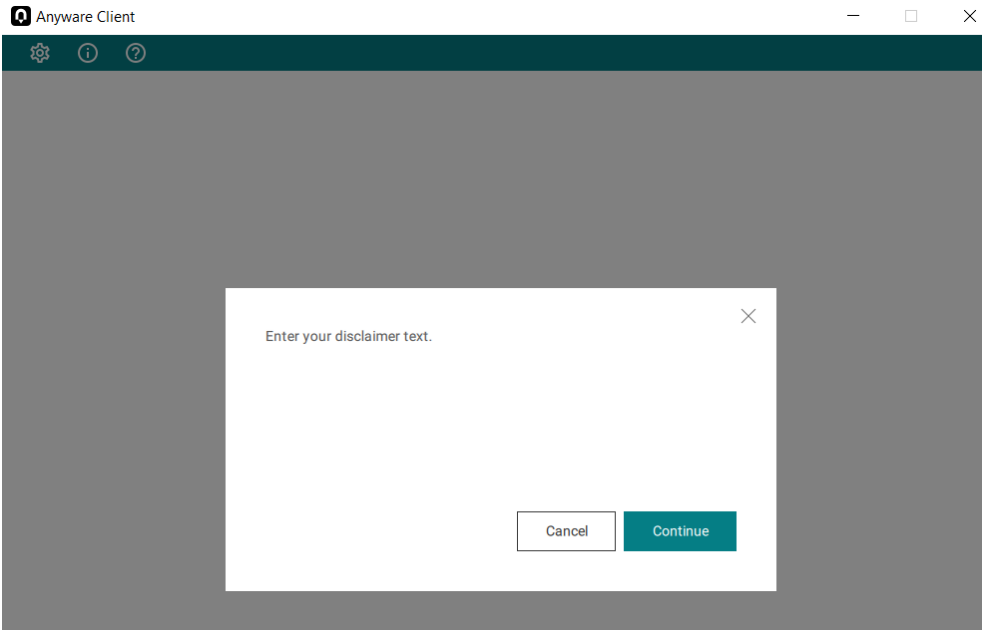
Rejection text

Enter text to display if the user rejects the disclaimer.

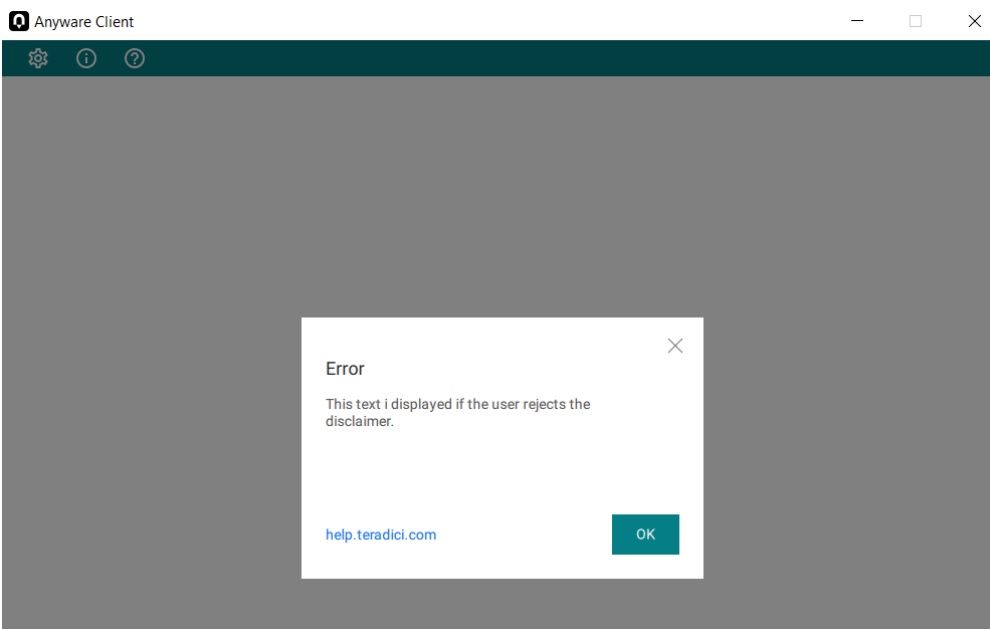
Some PCoIP clients can display this message if the user does not accept the disclaimer

2. Select the **Require users to accept disclaimer before authenticating** option.
3. In the **Disclaimer text** edit field, enter your full disclaimer text. HTML formatting is not currently supported.
4. In the **Rejection text** edit field, enter the text to display if the user rejects the disclaimer. Note that not all PCoIP clients display this reply.

When the disclaimer is enabled, after the user enters the Connection Broker address into their PCoIP Client, the disclaimer displays, for example:



If the user clicks **Continue**, they are prompted for their credentials to log into the environment. If they click **Cancel**, if possible, the rejection text displays, for example:



## Hard Assigning Workstations to PCoIP Zero Clients

You can hard-assign a workstation to a single PCoIP Zero client to ensure that any user logging in at that client receives the same desktop.



A user who logs in at a client that is hard-assigned to a desktop is *not* offered their hard-assigned or policy-assigned desktops.

To hard-assign a desktop to a client:

1. Go to the **> Resources > Clients** page.
2. Select the **Edit** action for the appropriate client. The **Edit Client** form opens.
3. Select the **Hard-assigned to a specific desktop** option from the **Desktop assignment mode** drop-down menu. The **Assigned desktop** drop-down menu appears, as shown in the following figure.

The screenshot shows the 'Edit Client' form for a client named 'pcoip-portal-0030040e4854'. The form is divided into sections. The 'Assignment' section is highlighted, showing 'Desktop assignment mode' set to 'Hard-assigned to specific desktop'. Below this, the 'Assigned desktop' drop-down menu is visible, and a purple arrow points to it. Other fields include 'Name', 'Administrative Web Interface password', and 'Apply policy options from'.

4. Select the desktop you want to assign to this client from the **Assigned desktop** drop-down menu.
5. Click **Save**. All users that log in at this client receive same hard-assigned desktop.

For PCoIP Zero clients, you can configure the client to establish the PCoIP connection to that desktop without requiring a preliminary login to the Connection Broker. In this configuration, when the client boots and registers with the Connection Broker, the broker returns the hard-assigned desktop information and the client immediately connects to the desktop.

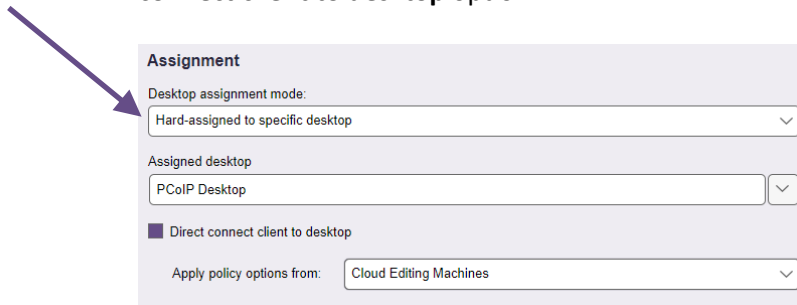
The user authenticates at the desktop operating system. Direct connections are useful if the desktop operating system requires the user to accept a legal disclaimer prior to logging into the desktop, for example.

To retain the PCoIP connection when the user logs out of the remote operating system select the **Retain console connection (VNC and PCoIP, only)** option in the **Desktop Hard Assignments** section of the user's policy. With this option selected, the user is returned to the operating system login page, not the client login page.

You configure a client to perform a direct connection, as follows.

1. Go to the **> Resources > Clients** page.
2. Click the **Edit** link associated with the client you want to direct connect to its hard-assigned desktop.

3. In the **Assignment** section of the **Edit Client** form, shown in the following figure, click the **Direct connect client to desktop** option.



**Assignment**

Desktop assignment mode:  
 Hard-assigned to specific desktop

Assigned desktop:  
 PCoIP Desktop

☐ Direct connect client to desktop

Apply policy options from:  
 Cloud Editing Machines

This option does not appear until you switch the **Desktop assignment mode** drop-down menu to **Hard-assigned to specific desktop**. For information on hard-assigning a client to a desktop.

4. The Connection Broker requires a policy to define how the hard-assigned desktop is managed. Typically, this policy is determined by the identity of the user who logs into the Connection Broker.

In direct-connection mode, no user logs into the Connection Broker prior to the desktop connection. Therefore, you must specify the policy to apply in the **Apply policy options from** drop-down menu.

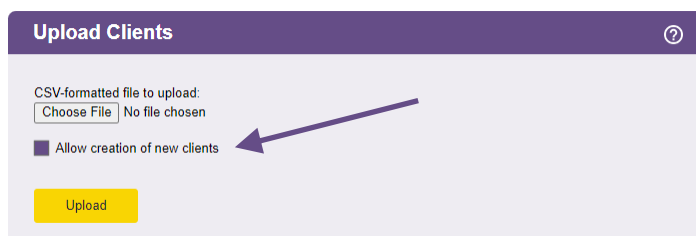
5. Click **Save** on the **Edit Client** form to save the changes.

Use the **Bulk Edit** option to enable direct-connection mode on multiple clients, simultaneously. If the clients are not inventoried in the Connection Broker, upload a CSV-file of client information to create the clients and enable the direct-connection flag, as described in the following section.

## Uploading PColP Zero Clients

You can upload a group of clients into your Connection Broker by uploading a CSV-file of client attributes. Uploading clients is useful if you need to hard-assign clients to particular workstations.

By default, the uploaded CSV-file modifies existing clients, but does not create new clients. To create new clients, select the **Allow creation of new clients** option, shown in the following figure. Specify new clients using the `name`, `mac`, or `serial_number` field. New clients cannot be created using an `id` field.



**Upload Clients**

CSV-formatted file to upload:  
 Choose File No file chosen

☐ Allow creation of new clients

Upload

If you do not select the **Allow creation of new clients** option, the Connection Broker provides a message indicating it cannot find the client, and skips that row in the CSV-file.

When uploading client data, the CSV-file must have the following format.

- The CSV-file must be comma delimited
- Quotes must be double quotes
- The first row must contain the field names, separated by commas with no additional blank spaces, and the data must be in the remaining rows
- The field names must match the field names in the `client` table in the data dictionary
- One of the following fields is required to uniquely identify the client
  - o `id` (for updating existing clients, only)
  - o `ip` (for PCoIP clients, only)
  - o `name`
  - o `mac`
  - o `serial_number`
- Additional modifiable fields are:
  - o `client_assignment_mode` – set to H to hard-assign the client to a desktop
  - o `client_type` – must be set to blade
  - o `direct_to_host_policy_id` – Set to a policy name or policy ID to enable direct-connect to the hard-assigned desktop
  - o `vm_id` – indicates the hard-assigned desktop
- The `vm_id` and `direct_to_host_policy_id` fields can contain either the numeric ID of the associated record or the name of the associated record

For a list of field names and values in the client table, go to:

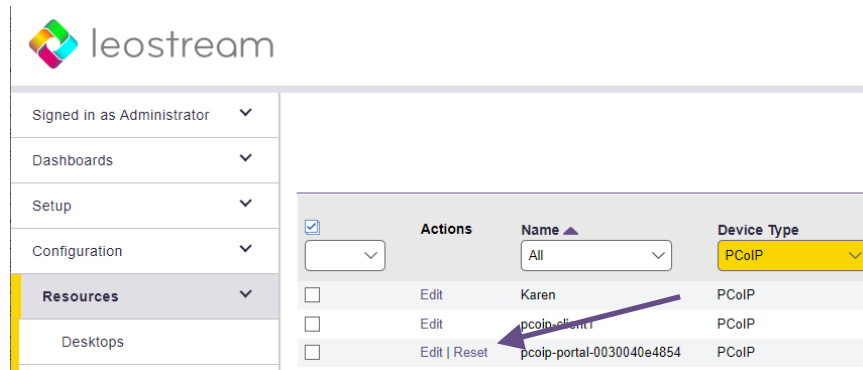
```
https://cb-address/download/account_db.html#client
```

Where *cb-address* is your Connection Broker address.

After the clients are uploaded, the Connection Broker performs a scan of the PCoIP Devices center. If the AWI is enabled on the PCoIP Zero clients, the Connection Broker populates the **> Resources > Clients** page with additional information about the Zero clients.

## Resetting PCoIP Zero Clients

You can use the **Reset** action on the > **Resources** > **Clients** page, shown in the following figure, to reset a PCoIP Zero client.



Clicking **Reset** instructs the Connection Broker to reboot the PCoIP Zero client, disconnecting any user with an active PCoIP connection at that client. When the user is disconnected, the Connection Broker invokes the **When User Disconnects from Desktop** section of the user's release plan.

## Managing another User's Resources via PCoIP Zero Client Logins

If you log into the Connection Broker with a role that has the **Allow user to manage another user's resources** option selected, PCoIP Zero clients allow you to log in to Leostream as another Leostream user and see their offered desktops. For a description of setting up the feature for managing another user's desktops, see the "Managing Resources" section in the [Leostream Connect Administrator's Guide and End User's Manual](#).

To use a PCoIP Zero client to manage another user's resources:

1. Log into the PCoIP Zero client using your usual credentials.
2. If your role allows you to manage another user's desktops, you are taken to an intermediate dialog where you can enter the domain and username for that user. In this dialog:
  - a. Click **Cancel** to return to the login page.
  - b. Click **No** to see your offered desktops.
  - c. Enter the other user's domain and username and click **Yes** to see their offered list of desktops
3. The Connection Broker launches a PCoIP connection to the desktop and prompts you for the username and password to use to log into that desktop.

## Octal Support with PCoIP Client Binding

To support octal monitor layout, a workstation contains two PCoIP Remote Workstation Cards. Amulet Hotkey devices can connect to both of these cards to provide octal monitor support. Each Amulet Hotkey device appears as two independent clients on the **> Resources > Clients** page in the Leostream Connection Broker. Therefore, to provide a seamless user experience while supporting octal-monitor configurations, you create a bonded pair from the two PCoIP Zero clients.

- The *primary* PCoIP client connects to the PCoIP host card listed as the primary card on the **Edit Desktop** page.
- The *secondary* PCoIP client connects to the PCoIP host card listed as the secondary card on the **Edit Desktop** page.

After the two clients are bonded, when a user logs into the either of the clients, the Connection Broker automatically connects both clients to the two PCoIP host cards, providing single sign-on with octal-monitor support. The following sections describe how to set up your Connection Broker to create bonded client pairs.

### Configuring Desktops for Octal-Monitor Support

The first step in configuring any PCoIP deployment is associating the PCoIP host cards with the desktops that contain them. The Connection Broker displays the host cards in the **> Resources > PCoIP Host Devices** page. In some cases, when the desktop has two host cards, you must manually associate the PCoIP host cards with the desktop, as follows.

1. Go to the **Edit Desktop** page for the desktop that contains two PCoIP host cards.
2. Scroll down to the **PCoIP Host Device** section, shown in the following figure.



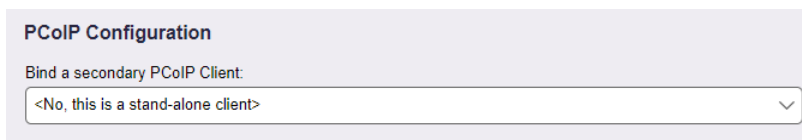
The screenshot shows a configuration section titled "PCoIP Host Device". It contains two dropdown menus. The first is labeled "Primary Host Device" and has the value "pcoip-host1 (pcoip-host1.dev.leostream.net)" selected. The second is labeled "Secondary Host Device" and has the value "Select ..." selected.

3. From the **Primary Host Device**, select the PCoIP host card to connect to the primary PCoIP Zero client.
4. From the **Secondary Host Device**, select the PCoIP host card to connect to the secondary PCoIP Zero client.
5. Click **Save**.

## Creating a Bonded PCoIP Zero Client Pair

The **> Resources > Clients** page contains separate entries for every PCoIP Tera2 card contained in a PCoIP Zero client. Client devices, such as those from Amulet Hotkey, containing two PCoIP cards result in two entries on the **> Resources > Clients** list. To provide octal monitor support, you must bond these two client records together, as described below.

Go to the **Edit Client** page for the primary client. Use the **Bind secondary client for octal-monitor support** drop-down menu in the **PCoIP Configuration** section, shown in the following figure, to select a second client to bind to this client.



The screenshot shows a light purple rectangular box titled "PCoIP Configuration". Inside the box, the text "Bind a secondary PCoIP Client:" is followed by a dropdown menu. The dropdown menu is currently open, showing the option "<No, this is a stand-alone client>" with a downward-pointing arrow on the right side of the menu.

If you display the **Client Binding** column on the **Clients** page, the Connection Broker displays information about which clients are bonded.



The **Edit** Client form for the secondary client becomes read-only. To remove the bond, you must edit the primary client.