



# leostream

Remote Desktop Access Platform

## **Leostream Quick Start for PCoIP Connections**

**Managing connections to workstations with PCoIP Remote Workstation Cards**

Version 202x

July 2023

## 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 2002-2023 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 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>
TERADICI PCoIP COMPONENTS .....	5
USING PCoIP CLIENTS WITH LEOSTREAM .....	6
ENSURING PROPER COMMUNICATION WITH LEOSTREAM AND PCoIP DEVICES .....	7
<b>CHAPTER 2: CONFIGURING THE CONNECTION BROKER .....</b>	<b>9</b>
STEP 1: ENABLING PCoIP DEVICE MANAGEMENT IN LEOSTREAM.....	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 Logins .....</i>	<i>14</i>
<i>Multi-Factor Authentication Options.....</i>	<i>16</i>
STEP 4: ADDING WORKSTATIONS 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 ON WORKSTATIONS.....	19
STEP 6: ASSOCIATING PCoIP REMOTE WORKSTATION CARDS AND DESKTOPS.....	20
<i>Automatic PCoIP Remote Workstation Card Matching for a Windows Desktop.....</i>	<i>20</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>26</i>
<i>Release Plans .....</i>	<i>27</i>
STEP 9: DEFINING USER POLICIES.....	30
STEP 10: CREATING LOCATIONS THAT REQUIRE PIV/CAC LOGINS .....	32
STEP 11: ASSIGNING POLICIES TO USERS .....	34
STEP 12: TESTING USER LOGIN.....	36
STEP 13: LOGGING INTO LEOSTREAM.....	38
<i>Using PCoIP Zero Clients .....</i>	<i>38</i>
<i>Using Leostream Connect.....</i>	<i>38</i>
<b>USING THE LEOSTREAM GATEWAY FOR REMOTE ACCESS.....</b>	<b>39</b>
REQUIREMENTS.....	39
THE LEOSTREAM NETWORK ARCHITECTURE .....	39
HOW THE LEOSTREAM GATEWAY WORKS .....	41

INTEGRATING WITH THE CONNECTION BROKER .....	42
<i>Forwarding Connection Broker Logins through the Gateway</i> .....	42
<i>Attach the Leostream Gateway to your Connection Broker</i> .....	43
<i>Building Protocol Plans for PCoIP Remote Workstation Card Connections</i> .....	44
<i>Logging into your Leostream Environment</i> .....	45
<b>APPENDIX A: WORKING WITH PCOIP ZERO CLIENTS .....</b>	<b>46</b>
DISPLAYING A DISCLAIMER BEFORE PCOIP CLIENT LOGINS.....	46
HARD ASSIGNING WORKSTATIONS TO PCOIP ZERO CLIENTS .....	47
UPLOADING PCOIP ZERO CLIENTS.....	49
RESETTING PCOIP ZERO CLIENTS .....	51
MANAGING ANOTHER USER’S RESOURCES VIA PCOIP ZERO CLIENT LOGINS .....	51
OCTAL SUPPORT WITH PCOIP CLIENT BINDING.....	52
<i>Configuring Desktops for Octal-Monitor Support</i> .....	52
<i>Creating a Bonded PCoIP Zero Client Pair</i> .....	53

## Chapter 1: Overview

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

Teradici® 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 are not using the HP Anyware for Remote Workstation Cards and that you do not have a PCoIP Connection Manager installed in your Leostream environment. If you do plan to build a hosted desktop environment that includes both Remote Workstation Cards and HP Anyware, please see the [Quick Start Guide for HP Anyware](#).*

---



Connection Broker 9.0.38 and higher no longer support the Connection Management Interface for PCoIP Remote Workstation Cards. Upgrade your PCoIP Zero client and Remote Workstation Card firmware to version 20.x.x or higher before upgrading to this Leostream release. If you cannot upgrade your PCoIP firmware, please contact [support@leostream.com](mailto:support@leostream.com) for instructions on how to enable the Connection Management Interface in Connection Broker version 9.0.36.

## Teradici PCoIP Components

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

- **Desktop operating systems:** Leostream manages connections to remote workstations running Microsoft® Windows®, Linux, and macOS operating systems. Desktops that support the PCoIP protocol appear in the > **Resources** > **Desktops** page of the Connection Broker.
- **PCoIP Remote Workstation Cards:** Leostream 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 in the > **Resources** > **PCoIP Host Devices** page of the Connection Broker.
- **PCoIP Zero 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. PCoIP client devices appear in the > **Resources** > **Clients** page of the Connection Broker.

## Using PCoIP Clients with Leostream

Typically, Leostream customers use a PCoIP Zero Client to log into their Leostream environment. Using a zero client, Leostream can connect users to workstations with a PCoIP Remote Workstation Card and virtual machines running the VMware Horizon Direct Connection Plug-In.

If your environment includes PCoIP software or mobile clients, you must install the PCoIP Cloud Access Software and PCoIP Connection Manager in your environment. When using the PCoIP Connection Manager as an intermediary between the client and the Leostream Connection Broker, you can connect users to workstations and virtual machines running the Cloud Access Software. See the [Quick Start Using Leostream with HP Anyware](#) for instructions on how to configure Leostream to support these environments.

The table below summarizes these connection options.

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 Cloud Access Software PCoIP 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 Cloud Access Software PCoIP Standard or Graphics Agent.
PCoIP Software Client PCoIP Mobile Client PCoIP Zero Client	PCoIP Connection Manager Security Gateway <i>Enabled</i>	Running the Cloud Access Software PCoIP Standard or Graphics Agent	Running the Cloud Access Software PCoIP Standard or Graphics Agent
PCoIP Zero Client	Leostream Connection Broker	Running the VMware Horizon View Direct Connection Plug-In	With an installed PCoIP Remote Workstation Cards (no PCoIP RWC Agent installed)

Client Type	Client Points To	The client can connect to: Virtual Machines	The client can connect to: Physical Machines
PCoIP Zero Client  PCoIP Software Client - Windows	Leostream Gateway, forwarding to the Connection Broker	Not currently supported	With an installed PCoIP Remote Workstation Cards (no PCoIP RWC Agent installed)
Leostream Connect  and  PCoIP Software Client (Windows only)	Leostream Connection Broker  Or  Leostream Gateway, forwarding to the Connection Broker	Not currently supported	With an installed PCoIP Remote Workstation Cards (no PCoIP RWC Agent installed)
Leostream Web Client  (PCoIP Software Client installed)	Leostream Connection Broker  Or  Leostream Gateway, forwarding to the Connection Broker	Running the Cloud Access Software PCoIP 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 Cloud Access Software PCoIP Standard or Graphics Agent.



This Quick Start assumes your Leostream environment does not include a PCoIP Connection Manager and that your workstations do not have an installed PCoIP RWC Agent. This guide indicates features that are not available when your architecture includes the PCoIP Connection Manager.

## Ensuring Proper Communication with Leostream and PCoIP Devices

Leostream 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 Leostream, you cannot use some of the Leostream features described in this guide. Chapter 2 covers how to ensure that Leostream 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 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
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 [Introduction to the Leostream Platform](#).

The following procedure steps you through a Connection Broker configuration specific to working with PCoIP Remote Workstation Cards. It 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 in Leostream

After applying a Leostream 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 Leostream, 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 Leostream.

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


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.

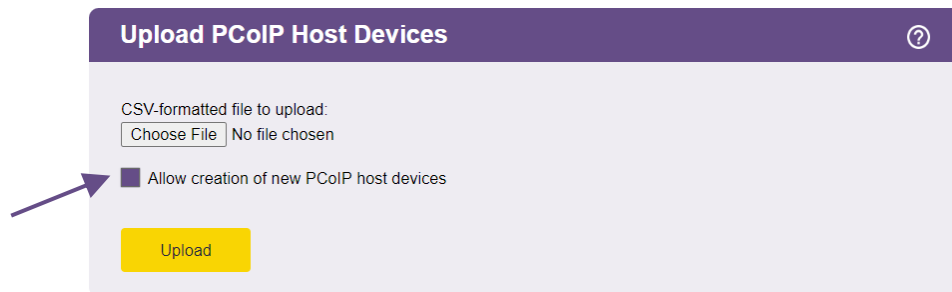
1. Go to the **> Resources > PCoIP Host Devices** page.
2. Click the **Add PCoIP Host Device** link.
3. In the **Add PCoIP Host Device** form that opens:
  - a. Enter a name for the PCoIP host device in the **Name** edit field.
  - b. If available, enter the device's DNS name in the **Hostname** edit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

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




If you do not select the **Allow creation of new PCoIP 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 PCoIP 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 PCoIP host devices, only)
  - `ip`
  - `hostname` (either `ip` or `hostname` must be specified, but do not enter both)

Specify new PCoIP host devices using either the `ip` or `hostname` field, but not using both fields. New host cards cannot be created using an `id` field.

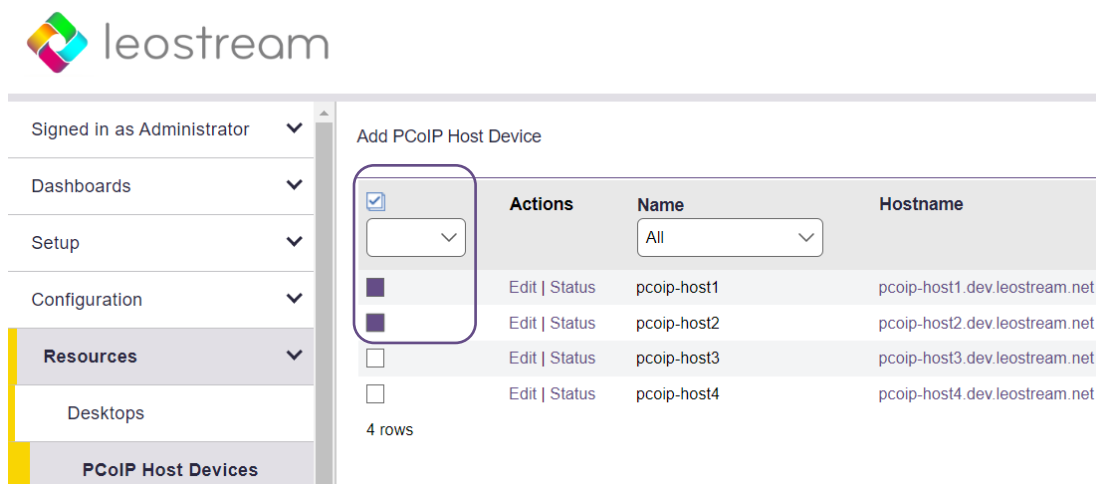
After uploading a CSV-file of PCoIP host devices, the Connection Broker performs a scan of the PCoIP Devices center and updates the PCoIP records with any additional information the Connection Broker can retrieve from the host card AWI.

 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

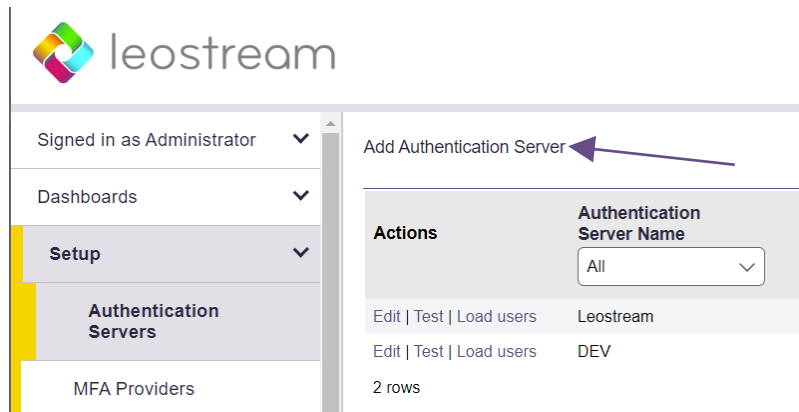
The Connection Broker uses your authentication server to authenticate users and assign policies. The Connection Broker can authenticate users against Microsoft Active Directory, OpenLDAP, and NIS authentication servers and can also act as a local authentication server in environments that do not have an external authentication system.

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

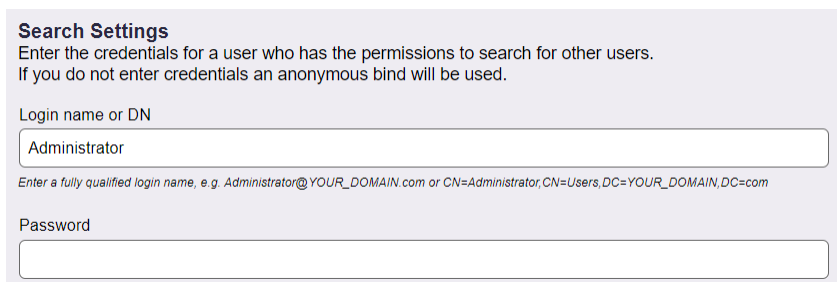
☐ Encrypt connection to the authentication server using SSL (LDAPS)

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. Leostream 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 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 Leostream 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 PCoIP connection is established.
3. 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:

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

4. 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.

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

6. 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
7. Click **Save**.

Leostream 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](#).



Leostream 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 Leostream 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 to your Connection Broker

After you import your PCoIP Remote Workstation Cards and connect Leostream 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.



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**.

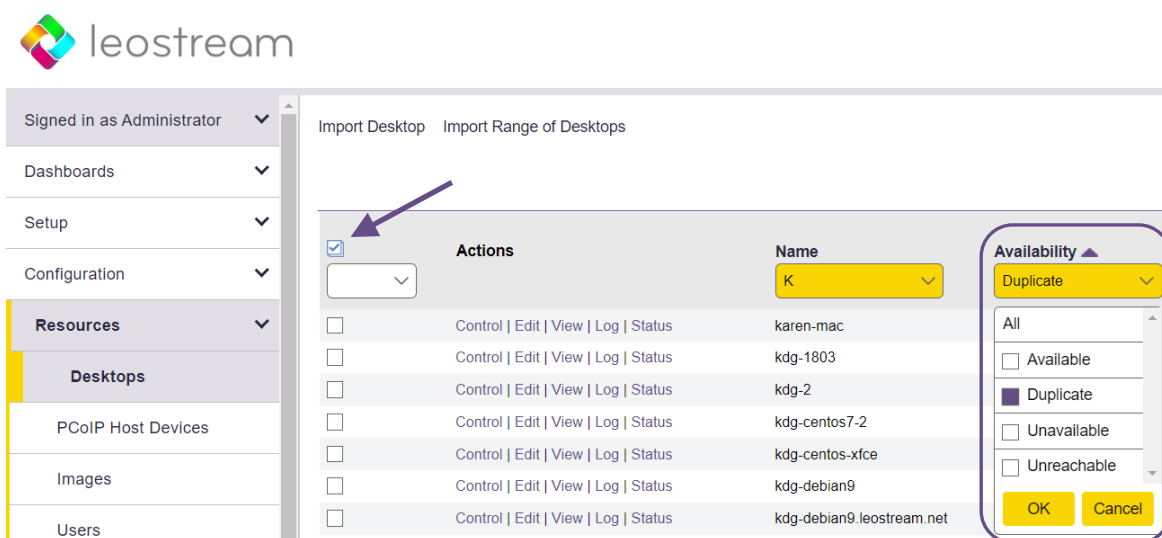
Workstations do not appear in the Uncategorized Desktops center until you install a Leostream Agent on the machine (see [Step 5: Installing the Leostream Agent on Workstations](#)).

## 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 on Workstations

The Leostream Agent performs the following crucial tasks when managing connections to workstations with installed PCoIP 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 Teradici 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 Teradici 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 workstations 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.

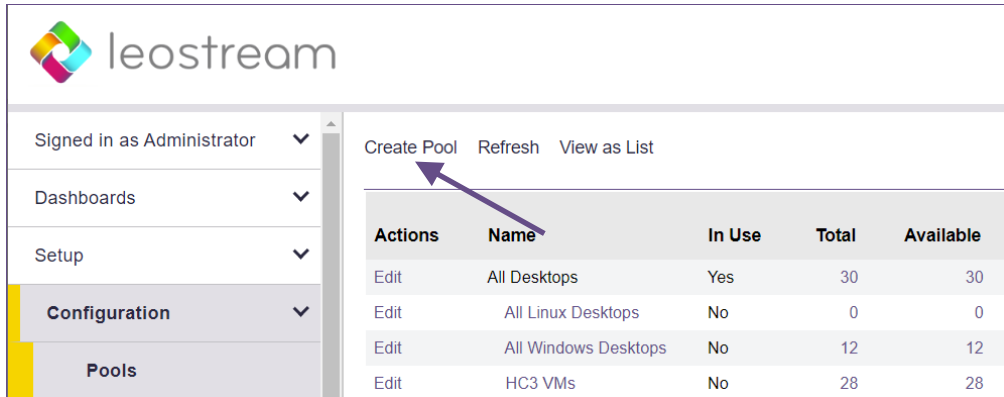
---

 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  
 All Desktops

Define pool using  
 Desktop attributes

Desktop attribute	Conditional	Value
Operating system	is equal to	Windows (any version)
[Add rows]		

☐ 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

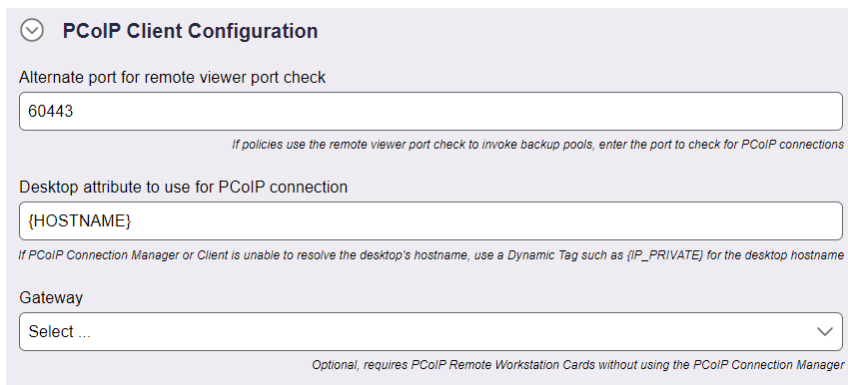
After you separate your desktops into pools, define plans that determine how the Connection Broker manages the user's session.

 *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 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.



**PCoIP Client Configuration**

Alternate port for remote viewer port check

60443

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

{HOSTNAME}

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

Gateway

Select ...

Optional, requires PCoIP Remote Workstation Cards without using the PCoIP Connection Manager

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 to the PCoIP Connection Manager when establishing connections using the Teradici Cloud Access Software. If the PCoIP Connection Manager is unable to resolve your desktop hostnames, use the **Desktop attribute to use for PCoIP connections** edit field to specify a different dynamic tag, such as {IP\_ADDRESS} or {IP\_PRIVATE}.
3. For remote users logging in using a PCoIP Zero client, you can send their PCoIP 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.

#### For Leostream Web Clients

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



**PCoIP Software Client** Priority: 1

Hostname or IP address of PCoIP Connection Manager

Send user domain as {DOMAIN}

Send user login name as {USER}

Desktop attribute to use for PCoIP connection {HOSTNAME}

Use an IP address-based Dynamic Tag if the PCoIP Connection Manager or Client is unable to resolve the desktop's hostname

1. The PCoIP connection must be initiated by a PCoIP Connection Manager, therefore, enter the appropriate address in the **Hostname or IP address of PCoIP Connection Manager** edit field.
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. Use the **Send user domain as** and **Send user login name as** edit fields to set these default values. The user must enter their password into the PCoIP software client to connect to their desktop.
3. By default, the Connection Broker sends the desktop's hostname to the PCoIP Connection Manager. If the PCoIP Connection Manager is unable to resolve your desktop hostnames, use the **Desktop attribute to use for PCoIP connections** edit field to specify a different dynamic tag, such as {IP\_ADDRESS} or {IP\_PRIVATE}.

### 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. Set the **Priority** of the **PCoIP Soft Client** to **1**, as shown in the following figure, and set the **Priority** of the remaining protocols to **Do not use**.

**PCoIP Software Client** Priority: 1

Command line parameters --hard-host {PCOIP\_HOST1} --quit-after-disconnect

Gateway Select ...

Optional

When establishing the connection, Leostream Connect launches the PCoIP software client using the parameters included in the **Command line parameters** field. The default value specifies the IP address of the Remote Workstation Card installed on the user's desktop, passed to the PCoIP software client using the `--hard-host` parameter.

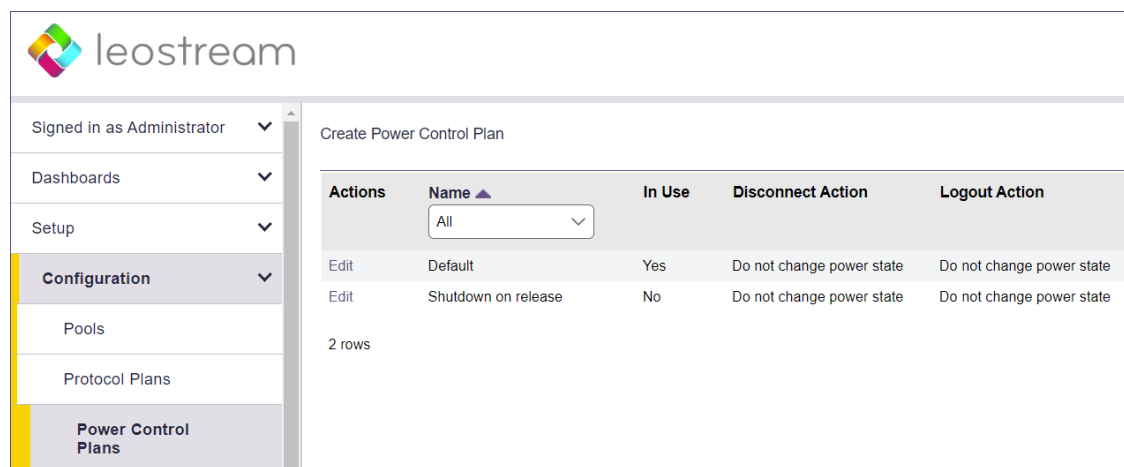
The PCoIP software client does not accept user credentials. Therefore, to provide single sign-on to the remote desktop, ensure that the user's policy selects the **Enable single sign-on to desktop console** option and the Leostream Agent was installed on the remote workstation with the single sign-on task selected.

**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.

Use the **Gateway** drop-down menu to send the PCoIP connection through a Leostream Gateway or Gateway Cluster.

### 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.



The screenshot shows the Leostream web interface. The left sidebar has a navigation menu with the following items: Signed in as Administrator, Dashboards, Setup, Configuration (selected), Pools, Protocol Plans, and Power Control Plans. The main content area is titled 'Create Power Control Plan' and contains a table with the following data:

Actions	Name	In Use	Disconnect Action	Logout Action
Edit	Default	Yes	Do not change power state	Do not change power state
Edit	Shutdown on release	No	Do not change power state	Do not change power state

Below the table, it says '2 rows'.

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.

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.

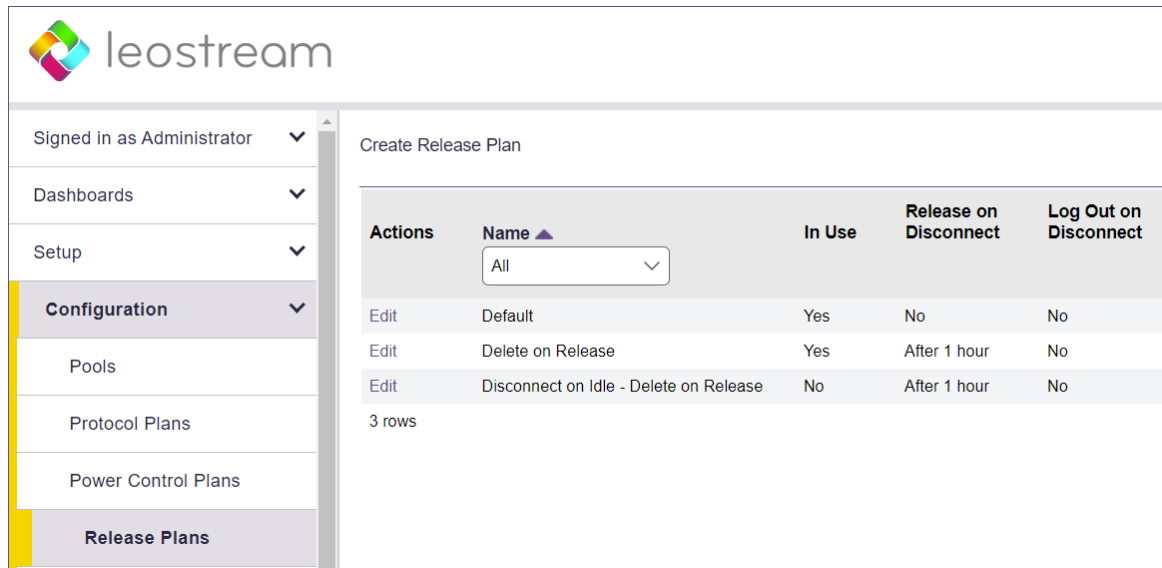
Select the power control action to take after the wait time elapses. For the Connection Broker to take actions based on disconnect or idle-time events, you must install the Leostream Agent on that desktop.

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.



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.

**Create Release Plan**

Plan name

When User Disconnects from Desktop

Release to pool: No

Log user out: After 1 hour

URL to call

When User Logs Out of Desktop

Release to pool: Immediately

URL to call

When Connection is Closed

Execute actions for: When User Logs Out of Desktop

This section of the plan executes when no Leostream Agent is installed or communicating on the remote desktop

When Desktop is Idle

Lock desktop: No

Disconnect: No

Log user out: No

When Desktop is First Assigned

Release to pool: No

Release if user does not log in: No

"When Desktop is Released" actions will not be invoked

When Desktop is Released

☒ Log user out of the desktop

Suspend logout and display warning message to user: No

Delete virtual machine from disk: No

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 to allow the Connection Broker to distinguish between user logout and disconnect and to perform actions based on idle time.**

## Step 9: Defining User Policies

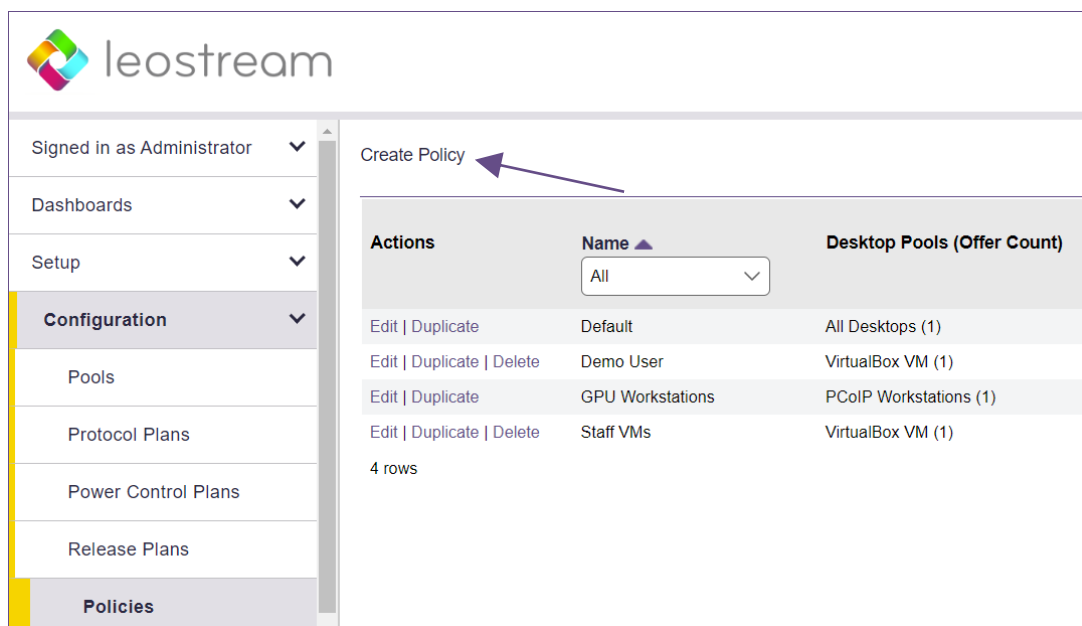
After you define pools and plans, build policies.

 *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)

When connecting to PCoIP Remote Workstation Cards, this option applies only when logging in using a PCoIP Zero Client. With this option selected:

- The user points the Zero 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. 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.

When User Connects to Desktop

Log user into remote desktop as:

☐ 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

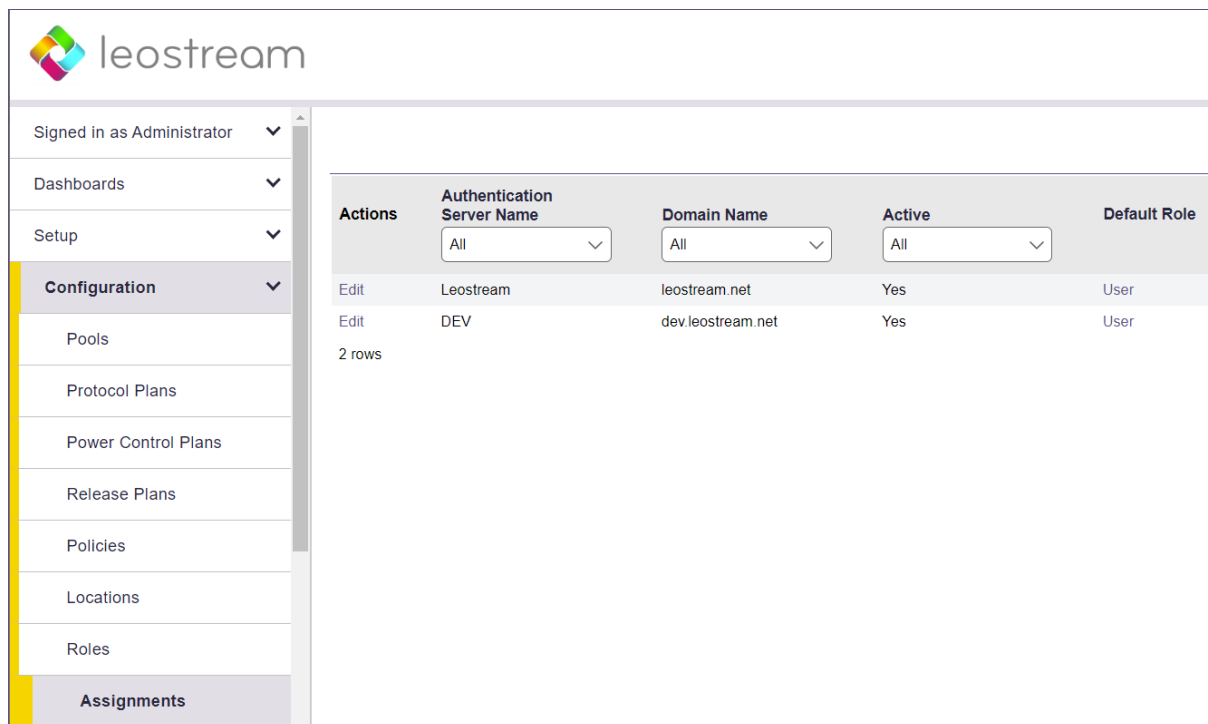
determine their policy.

- 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 PCoIP 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.



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

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.

**Edit Assignments for Authentication Server "Leostream"**

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:

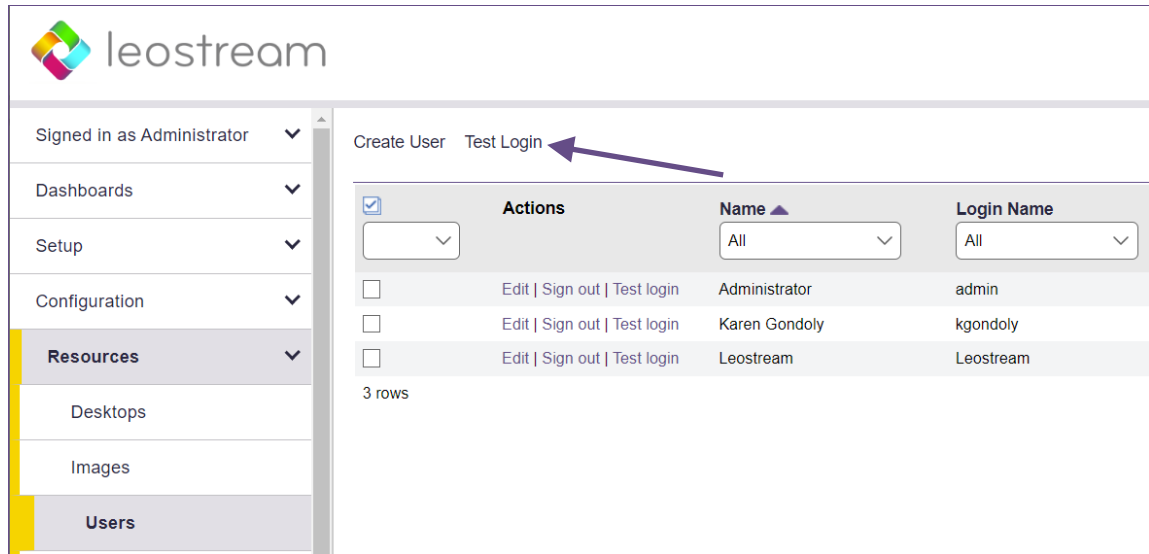
1. Select the group attribute from the **Group** drop-down menu
2. If you are using locations, select a location from the **Client Location** drop-down menu
3. Assign permissions to this group and client location pair by selecting an item from the **User Role** drop-down menu
4. Assign a policy to this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

### 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 Leostream

### Using PCoIP Zero Clients

Users can log into Leostream using any PCoIP Zero client.



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

---

To log into Leostream from a PCoIP Zero Client:

1. In the PCoIP 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 Connection Broker.
4. Save the changes.

You do not need to reboot the PCoIP 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 PCoIP zero client.

If you need to register multiple PCoIP 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 PCoIP Zero Clients](#) for more information.

### Using Leostream Connect

If users do not have a PCoIP Zero client, they can use Leostream Connect to launch a PCoIP Software client on Windows operating systems.

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

To use Leostream Connect, ensure that the **Options** dialog points the Leostream Connect client to your Connection Broker. 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. 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

## Requirements

- Users must be using PCoIP Zero Clients or the Windows version of Leostream Connect on a machine that also has an installed PCoIP Software client version 20.04.1 or later.
- The workstations must have an installed PCoIP Remote Workstation Card. This can be an internal or external card, but the card must be associated with the workstation record in the Leostream Connection Broker.
- The workstation must not be running the PCoIP Cloud Access Software.
- The Leostream Connection Broker must be version 9.0.36 or higher.
- The Leostream Gateway must be version 2.0 or higher.
- If single sign-on is required to the remote workstation, the Leostream Agent must be installed on the operating system with the single sign-on task selected. The Leostream Agent does not support single sign-on to macOS workstations.



Leostream can manage remote access to PCoIP Remote Workstation Cards without a Leostream Agent installed on the operating system. In this setup, some Leostream functionality is not available.

## The Leostream Network Architecture

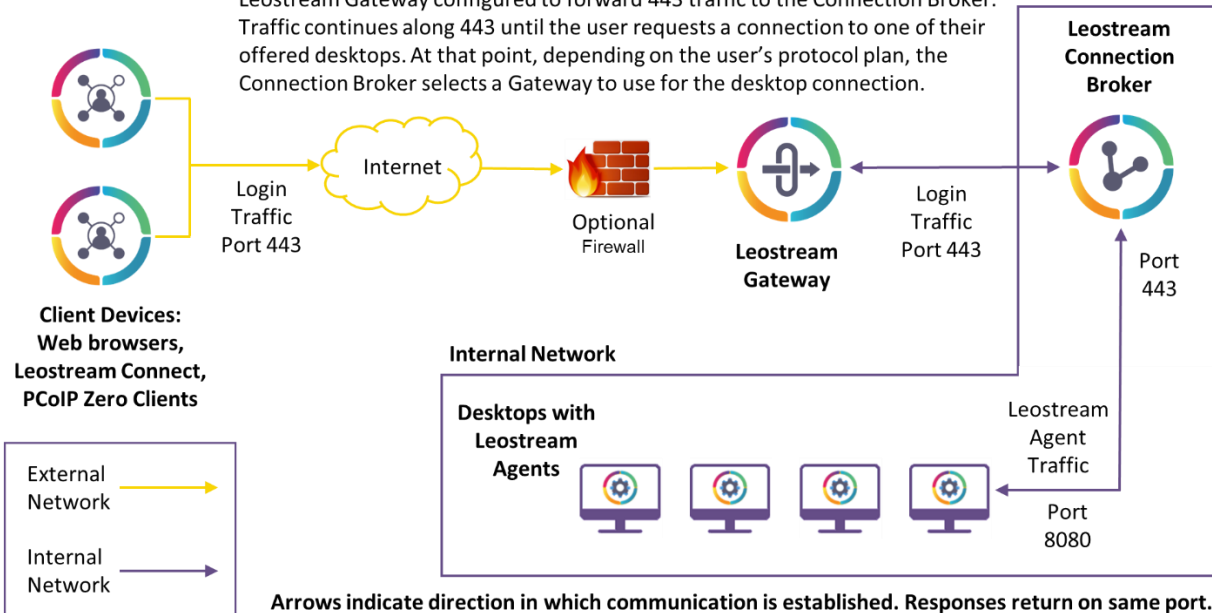
The Leostream Gateway serves two purposes when connecting remote users to your Leostream environment and their hosted workstations.

1. Forward login traffic from the PCoIP Zero Client to the Connection Broker
2. Forward PCoIP traffic from the PCoIP Zero Client to the PCoIP Remote Workstation Card

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

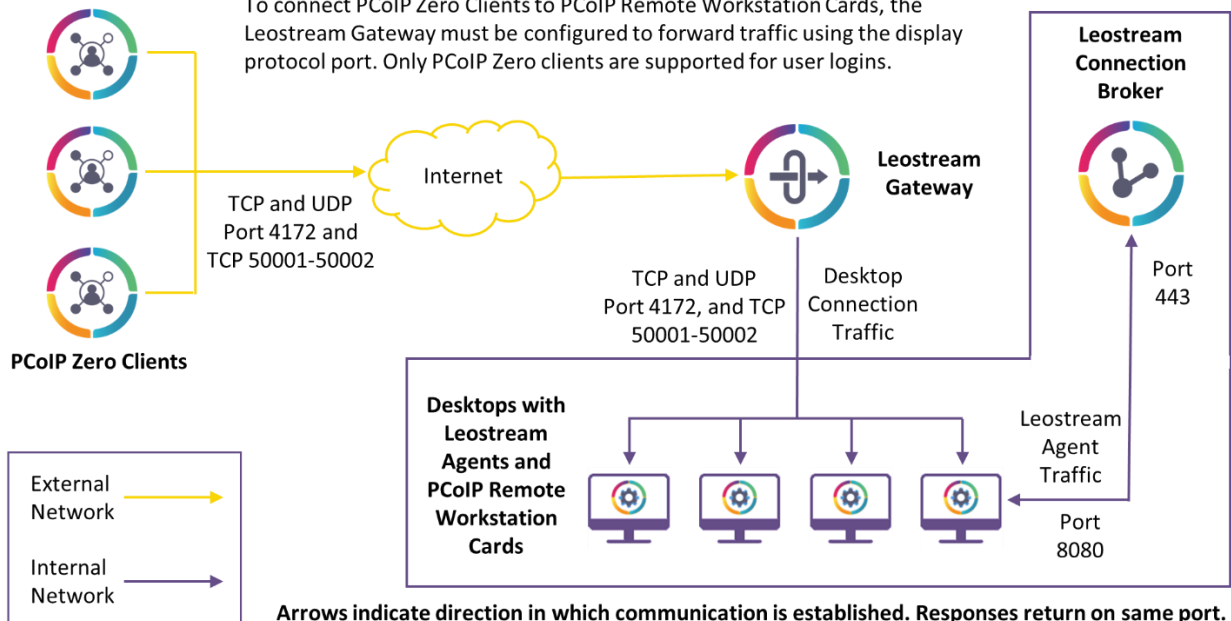
Leostream Gateway configured to forward 443 traffic to the Connection Broker. Traffic continues along 443 until the user requests a connection to one of their offered desktops. At that point, depending on the user's protocol plan, the Connection Broker selects a Gateway to use for the desktop connection.



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 for PCoIP Remote Workstation Cards

To connect PCoIP Zero Clients to PCoIP Remote Workstation Cards, the Leostream Gateway must be configured to forward traffic using the display protocol port. Only PCoIP Zero clients are supported for user logins.





## 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.

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](#).

## Integrating with the Connection Broker

After installing your Leostream Gateway, you use the Connection Broker Web interface to integrate it into your Leostream environment. The steps required to integration with PCoIP are, as follows.

1. [Forward Leostream logins through your Leostream Gateway](#) to the Connection Broker
2. [Attach the Leostream Gateway to your Connection Broker](#)
3. [Create protocol plans that use the Leostream Gateway](#)
4. Configure pools and policies that assign these protocol plans to desktops, and desktops to users (see [Step 8: Defining Pool-Based Plans](#) and [Step 9: Defining User Policies](#))
5. [Log in to Leostream using a PCoIP Zero Client](#)

## Forwarding Connection Broker Logins through the Gateway

The Leostream Gateway can be used to forward user login traffic from remote PCoIP Zero clients or Leostream Connect to the Leostream Connection Broker. With Connection Broker forwarding enabled on your Leostream Gateway, the Connection Broker does not need to be accessible from the user's network and, instead, can be isolated in the same network as your desktops.

To enable Connection Broker forwarding, log into your Leostream Gateway and execute the following command from a terminal.

```
sudo leostream-gateway --broker <your-broker-address>
```

After forwarding is enabled, all HTTPS calls to your Leostream Gateway are forwarded to the entered Connection Broker with the exception of the URL used to check the status of the gateway and access the Leostream Gateway API.



The Leostream Gateway does not forward traffic from port 80 to port 443. After enabling Connection Broker forwarding, you must enter the URL for your Leostream Gateway using HTTPS. Calls to HTTP result in a warning that the site cannot be reached.

To disable Connection Broker forwarding, run the following command:

```
sudo leostream-gateway --no-broker
```

## Attach the Leostream Gateway to your Connection Broker

Each Leostream Gateway can be attached to a single Connection Broker or Connection Broker cluster. You attach your Leostream Gateway to your Connection Broker, as follows.

1. Log into the Connection Broker Administrator's Web interface.
2. Go to the **> Setup > Gateways** page.
3. Click the **Add Gateway** link.
4. In the **Add Gateway** form, enter a name for the Leostream Gateway in the **Name** edit field.
5. In the **Address** edit field, enter the publicly accessible IP address or hostname for your Leostream Gateway. This address must be accessible by the end users' client devices, and is the address used to log into Leostream and to forward desktop connections.
6. In the **Private address** field, optionally enter the private address of your Leostream Gateway. If the Connection Broker can contact the Leostream Gateway on the gateway's public IP address, you may leave this field blank.
7. If applicable, indicate if this Leostream Gateway is part of a cluster behind a load balancer, using the **Gateway cluster** drop-down menu.
8. From the **Method for routing display protocol traffic through this Leostream Gateway** drop-down menu, select **Use protocol specific port on both gateway and desktop, filtered by client source IP address**.



PCoIP traffic can be forwarded only when the Leostream Gateway is configured to use the protocol specific port, filtered by client source IP address.

9. Click **Save**.

After saving the form, the Connection Broker registers with the Leostream Gateway and the gateway can now be used in protocol plans.

You cannot save the form if the Leostream Gateway is already attached to another Connection Broker. If you receive an error indicating the Leostream Gateway is already controlled by another Connection Broker, log into that Connection Broker and remove the Leostream Gateway.

If the previously associated Connection Broker is no longer in service, you can manually detach the Connection Broker from the Leostream Gateway, as described in the "Manually Detaching a Leostream Gateway from a Connection Broker" section of the main Leostream Gateway guide.

If the form displays a warning indicating the Connection Broker cannot contact the Leostream Gateway and the form fails to save, check that port 443 is open on the Leostream Gateway. You can test the Leostream Gateway connection by logging into the Connection Broker virtual machine console and executing one of

the following commands at the Linux shell.

```
curl -k https://GATEWAY_ADDRESS/app/system/ping
```

```
wget --no-check-certificate -q -S -O - https://GATEWAY_ADDRESS/app/system/ping
```

Where `GATEWAY_ADDRESS` is the IP address or fully qualified hostname of your Leostream Gateway.

You can register multiple Leostream Gateways with your Connection Broker. For example, if you have workstations in different networks, build unique Leostream Gateways for each network and create individual protocol plans, as described in the next section.

If you are sending a large number of connections to a particular network, consider installing multiple Leostream Gateways for that network and using a load balancer to distribute user connections. Load balancers and Leostream Gateway clusters are discussed in the main [Leostream Gateway Guide](#).

### Building Protocol Plans for PCoIP Remote Workstation Card Connections

After you install your Leostream Gateway, configure Connection Broker login forwarding, and register the gateway with your Connection Broker, configure a protocol plan to send the PCoIP traffic through the Leostream Gateway, as follows:

1. Go to the **> Configuration > Protocol Plans** page in your Connection Broker.
2. Either edit an existing protocol plan or click the **Create Protocol Plan** link to build a new plan.
3. For users logging in using Leostream Connect and the PCoIP Software client:
  - a. Select **1** for the **Priority** of the **Teradici PCoIP Software Client** in the **Leostream Connect** section of the protocol plan.
  - b. From the **Gateway** drop-down menu, select the Leostream Gateway to use for connections, for example:

PCoIP Software Client

Priority: 1

Command line parameters

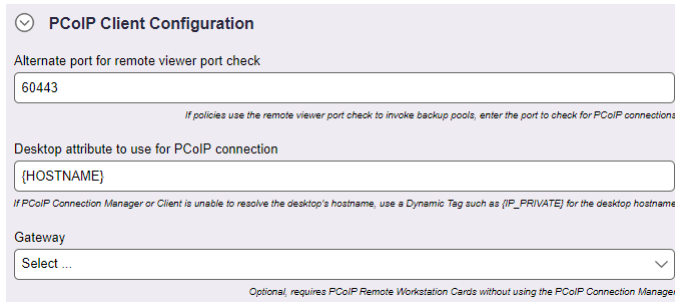
--hard-host {PCOIP\_HOST1} --quit-after-disconnect

Gateway

Select ...

Optional

4. For users logging in using a PCoIP Zero client:
  - a. Scroll down to the **PCoIP Client Configuration** section.
  - b. From the **Gateway** drop-down menu in this sub-section, select the Leostream Gateway to use for connections, for example:



**PCoIP Client Configuration**

Alternate port for remote viewer port check

60443

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

{HOSTNAME}

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

Gateway

Select ...

Optional, requires PCoIP Remote Workstation Cards without using the PCoIP Connection Manager

5. Click **Save**.

After you build your protocol plans, use policies to assign these protocol plans to pools or hard-assigned desktops. Users are then assigned to policies on the **> Configuration > Assignments** page. Refer to the main section of this quick start guide for complete instructions.

## Logging into your Leostream Environment

For users with a PCoIP Zero Client:

- On the **Options** dialog of the Zero client, go to the **Session** and select either **Auto Detect** mode or **PCoIP Connection Manager**
- Enter **https://<GATEWAY\_PUBLIC\_ADDRESS>** in the edit field. You must include `https://` before your Leostream Gateway hostname or IP address.

When using Leostream Connect:

- Enter the publicly accessible hostname or IP address of your Leostream Gateway on the **Broker** tab of the **Options** dialog. Do not include `https://` before your Leostream Gateway hostname or IP address.
- Ensure that the PCoIP Software client version 20.04.1 or later is installed on the same client device as Leostream Connect.

### Important restrictions:

- Note that every client must register a unique IP address. For remote users, that typically means each remote location can support only one client connection at a time
- Each user/client pair can be assigned to a single desktop at a time. If a user is currently assigned to a desktop that was connected via the Leostream Gateway, you must release that assignment before the user will be able to connect to another Remote Workstation Card.

## Appendix A: Working with PCoIP Zero Clients

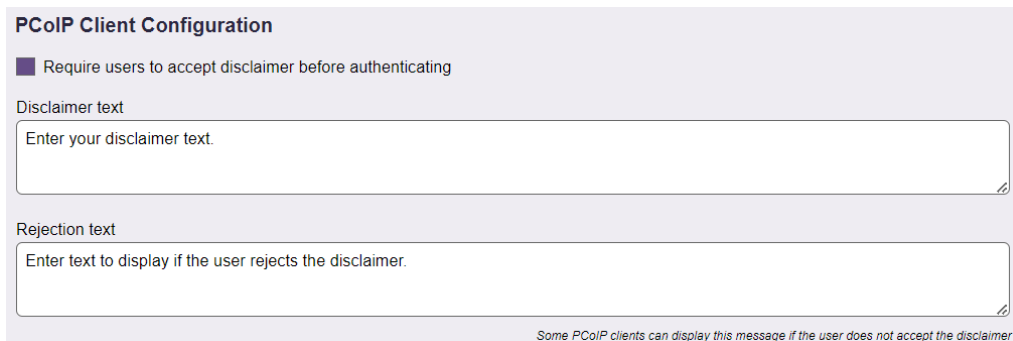
### Displaying a Disclaimer before PCoIP Client Logins

Teradici 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 **Teradici PCoIP 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:

The screenshot shows a web interface for connecting to a remote workstation. It has two input fields: "Host Address or Code:" with the value "10.110.37.35" and a "NEXT" button to its right; and "\*Connection Name:" with the value "e.g. My Work Windows 7 Machine". Below these fields are three buttons: a menu icon (three horizontal lines), "CANCEL", and "SAVE". A white "Disclaimer" dialog box is centered over the interface, containing the text "Enter your disclaimer text" and two buttons: "Accept" and "Decline".

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

This screenshot shows the same interface as the previous one, but with an "ERROR" dialog box displayed. The "Host Address or Code:" field now contains "10.110.37.35:443" and there is a gear icon to the right of the "NEXT" button. The "ERROR" dialog box is white and contains the text "This text is displayed if the user rejects the disclaimer" and a "Close" button.

## Hard Assigning Workstations to PCoIP Zero Clients

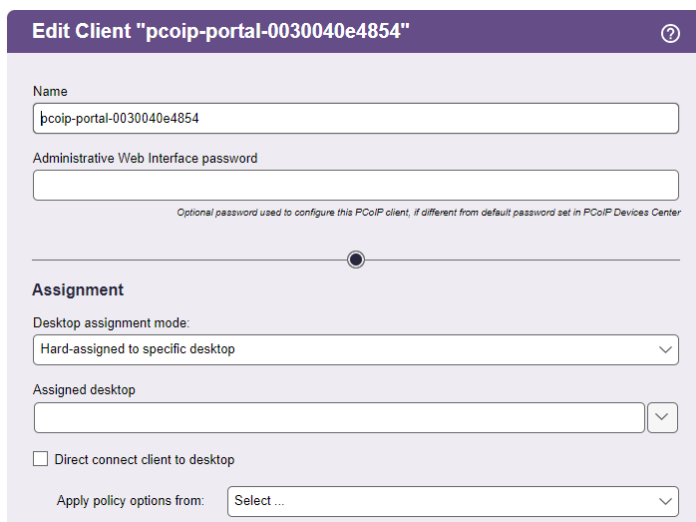
You can hard-assign a workstation to a single PCoIP Zero client to ensure that any user logging in at that client receives the same desktop.



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.



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.

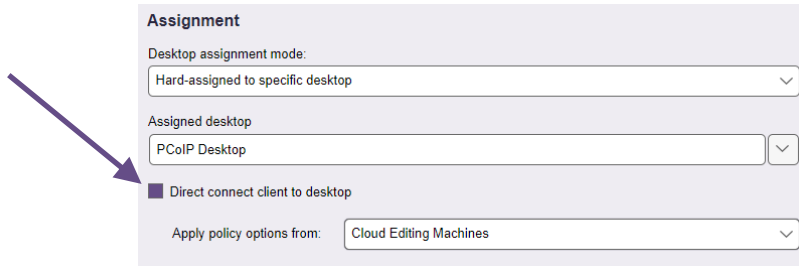
The user authenticates at the desktop operating system. Direct connections are useful if the desktop operating system requires the user to accept a legal disclaimer prior to logging into the desktop, for example.

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.

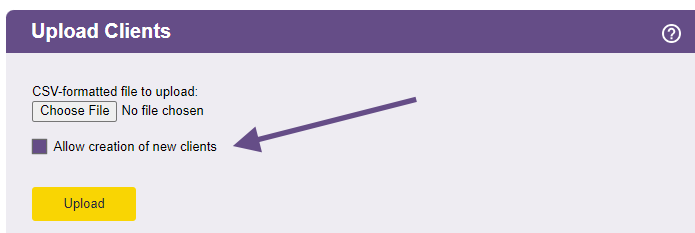
5. Click **Save** on the **Edit Client** form to save the changes.

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 PCoIP 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:

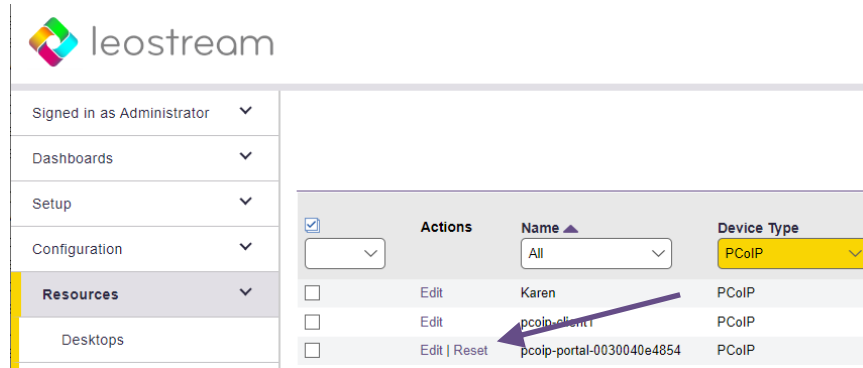
`https://cb-address/download/account\_db.html#client`

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.

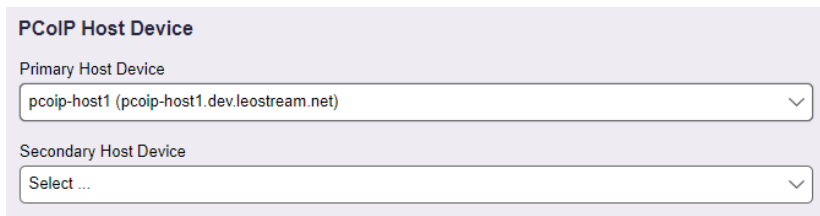
- The *primary* PCoIP client connects to the PCoIP host card listed as the primary card on the **Edit Desktop** page.
- The *secondary* PCoIP client connects to the PCoIP host card listed as the secondary card on the **Edit Desktop** page.

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.



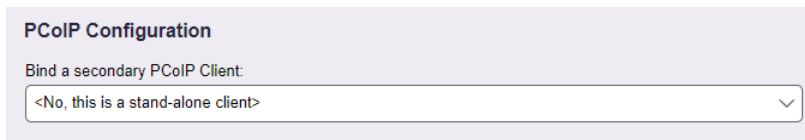
The screenshot shows a configuration section titled "PCoIP Host Device" with a light purple background. It contains two dropdown menus. The first is labeled "Primary Host Device" and has the text "pcoip-host1 (pcoip-host1.dev.leostream.net)" selected. The second is labeled "Secondary Host Device" and has "Select ..." selected. Both dropdowns have a downward arrow icon on the right.

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 arrow on the right side of the menu box.

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.