leostream

Remote Desktop Access Platform

Using Leostream with VMware Horizon Direct Connection Plug-In

High-Performance Connections to VMware Virtual Machines

Version 2023
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.
To request product information or inquire about our future directions, email sales@leostream.com.

Copyright

Trademarks

Patents

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

Contents

Overview

This document describes how to use Leostream to manage PCoIP connections to virtual machines with an installed VMware Horizon View Direct-Connection Plug-in. When using PCoIP zero-clients, you can configure Leostream to provide PCoIP connections to workstations with a PCoIP Remote Workstation Card and virtual machines with a Direct-Connection Plug-in from a single login.

- Read the Introduction to the Leostream Platform for a general overview of Leostream concepts and terminology.
- See the Installation Guide for information on downloading and installing the Connection Broker virtual appliance and related components.
- See the Leostream Quick Start Guide for managing Remote Workstations with a PCoIP Remote Workstation Card for information on how to set up Leostream to manage physical machines.
- See the Leostream Quick Start Guide for Using Leostream with HP Anyware Software if you want to use Leostream and Teradici to build a virtual workspaces solution.

Leostream™ Components

The Leostream Connection Broker consists of the following four components.

- **Connection Broker**: The Connection Broker is the central management layer for your environment. The Connection Broker inventories, provisions, and terminates desktops, assigns desktops to users, and defines the end-user experience.
- **Leostream Agent**: When installed on the remote desktop, the Leostream Agent provides the Connection Broker with insight into the connection status of the remote users. On Windows operating systems, the Leostream Agent also performs functions related to the Leostream printing and USB management features. The Leostream Agent is a critical component when scaling out deployments to a large number of end users.
- **Leostream Connect:** A software client provided by Leostream that allows users to log into Windows and Linux remote desktops from any Windows or Linux fat or thin clients.
- **Database:** When building a proof-of-concept, the Connection Broker stores all information in an internal database. Production deployments should configure a Connection Broker cluster attached to an external Microsoft SQL Server® 2012 or 2014 database, or PostgreSQL database.

Using PCoIP Clients with Leostream

You can use any supported PCoIP software, mobile, or zero client to log into Leostream. The type of client you use and whether the client communicates with Leostream or the PCoIP Connection Manager, determines what types of PCoIP resources can be connected. The following table describes the types of resources users can connect to when using different PCoIP client devices.

To connect to virtual machines running the VMware Horizon View Direct Connection Plug-In, you must configure use a PCoIP Zero Client and configure the zero client to communicate with the Leostream Connection Broker.

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 *Disabled*	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 **And** Running the Cloud Access Software PCoIP Standard or Graphics Agent.
PCoIP Software Client PCoIP Mobile Client PCoIP Zero Client	PCoIP Connection Manager Security Gateway *Enabled*	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 **And** Running the Cloud Access Software PCoIP Standard or Graphics Agent.

Installing the Leostream Connection Broker

The Connection Broker can be installed on any virtual or physical machine running the latest Red Hat® Enterprise Linux® 8.x operating system and its derivatives such as Rocky Linux and AlmaLinux OS.

⚠ The Connection Broker does not install on CentOS 8, on any operating system based on Fedora, or any other Linux distribution.

When creating a virtual machine for the Connection Broker installation, ensure that the VM has, at least, the following resources.

- 2 CPU or vCPU
- 8.0 Gbytes of RAM

- At least 20 Gbytes of hard drive space
- One NIC, ideally with Internet connectivity

Prior to installing your Connection Broker, install the latest updates to the operating system. See the Leostream Installation Guide for information on obtaining and applying your license key, using the Leostream serial number you obtained from Leostream sales.

Configuring the Microsoft® Windows® Virtual Machines

When using Leostream to manage PCoIP connections to VMware virtual machines, you must ensure that each virtual machine has an installed VMware View Direct-Connection Plug-in. You do not need to configure the View Connection Server to handle entitlements. All desktop assignments are controlled by Leostream.

Install the Leostream Agent on each virtual machine, as well. During the installation, specify the Connection Broker address from Step 1.

⚠ When installing the Leostream Agent, ensure that you *do not* select the task to install the Credential Provider when performing the installation. The Leostream Agent credential provider may conflict with the Direct-Connection Plug-in.

Ensure that the PCoIP connection can be established from the VMware Horizon View Client to the virtual machine, before attempting to use with Leostream. You must configure the **View Agent Direct-Connection Users** on the virtual machine before Leostream can establish the PCoIP connection.

Consult the VMware documentation for complete instructions on configuring the VMware Horizon View Direct Connection Plug-in.

Installing the VMware Horizon View Direct-Connection Plug-In automatically creates a new local group on the operating system, named **View Agent Direct-Connection Users**. Users must be a member of this group to connect to the desktop. Leostream does not automatically add users to this group. Therefore, ensure that you configure members of this group before proceeding with the Leostream setup.

Integrating with Your Existing Infrastructure

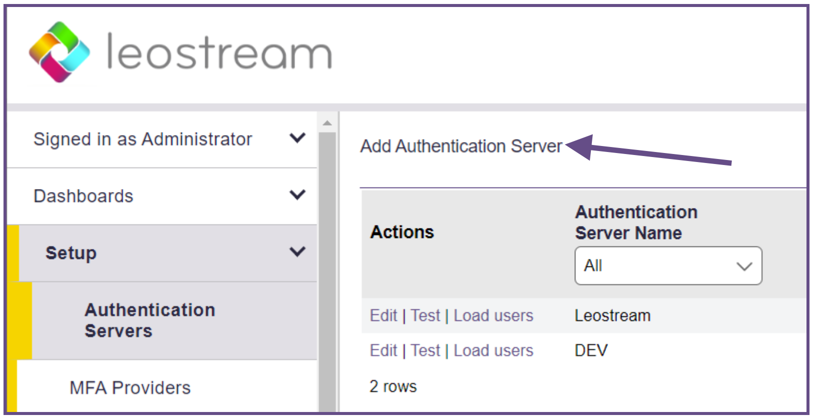
The Connection Broker is configured using the Administrator Web interface. In the **Setup** section of the Connection Broker Administrator Web interface, you integrate Leostream with the other components of your hosted desktop environment, such as your Microsoft Active Directory authentication servers and the virtualization or cloud platforms that host your desktops.

Adding Authentication Servers

The Connection Broker can authenticate users in standard LDAP systems, such as Active Directory, or OpenLDAP™, and with NIS authentication servers. In this example, we add an Active Directory authentication server, as follows.

Note: Any options not covered in the following procedure remain at their default values.

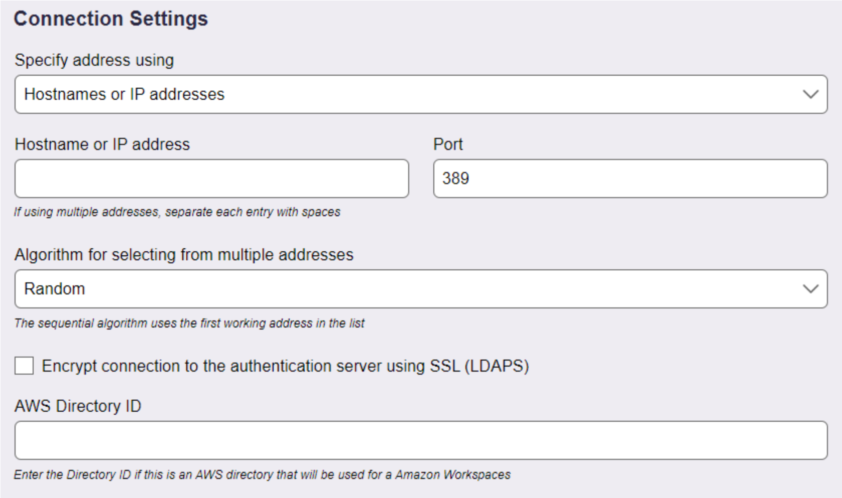
1. Navigate to the **> Setup > Authentication Servers** menu.
2. Click the **Add Authentication Server** link, shown in the following figure.



Actions	Authentication Server Name All
Edit | Test | Load users	Leostream
Edit | Test | Load users	DEV

2 rows

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.

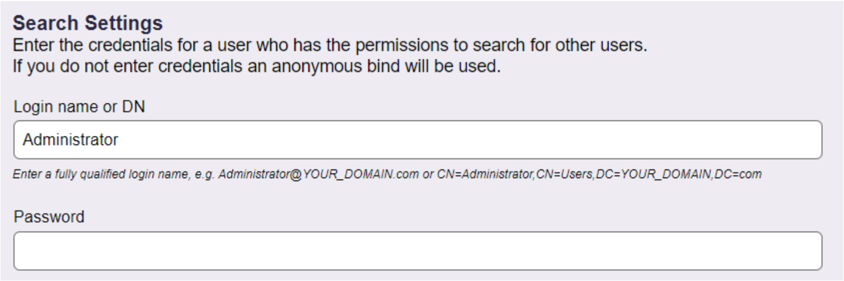
b. From the **Specify address using** drop-down menu, select **Hostname or IP address**.

c. Enter the server's hostname or IP address in the **Hostname or IP address** edit field.

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

Administrator

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.

Defining Centers to Communicate with Hosting Platforms

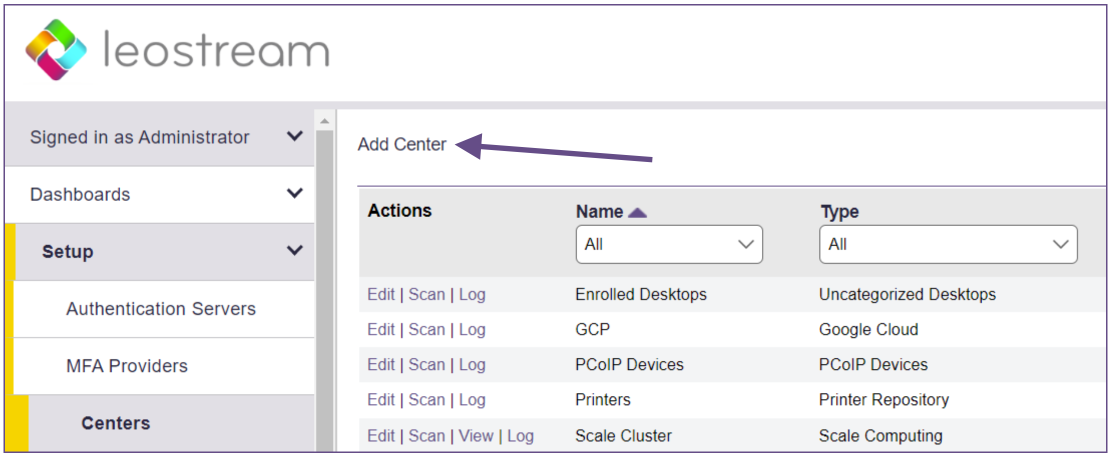
The Connection Broker interfaces with a number of virtualization and cloud platforms, allowing you to build a hybrid-cloud environment for your hosted desktops and applications.

*Leostream defines **centers** as the external, third-party platforms that host your desktops. The Connection Broker interacts with these centers to inventory desktops available for assignment to end users, as well as to provision and delete desktops based on demand.*

In this example, virtual machines are hosted in VMware vSphere, and vSphere is managed by VMware vCenter Server. For the Connection Broker to manage these machines, define a ***center*** for vCenter Server, as follows. For details on defining centers when not using VMware, see the “Creating Centers” section of the Connection Broker Administrator’s Guide.

1. Navigate to the **> Setup > Centers** menu.

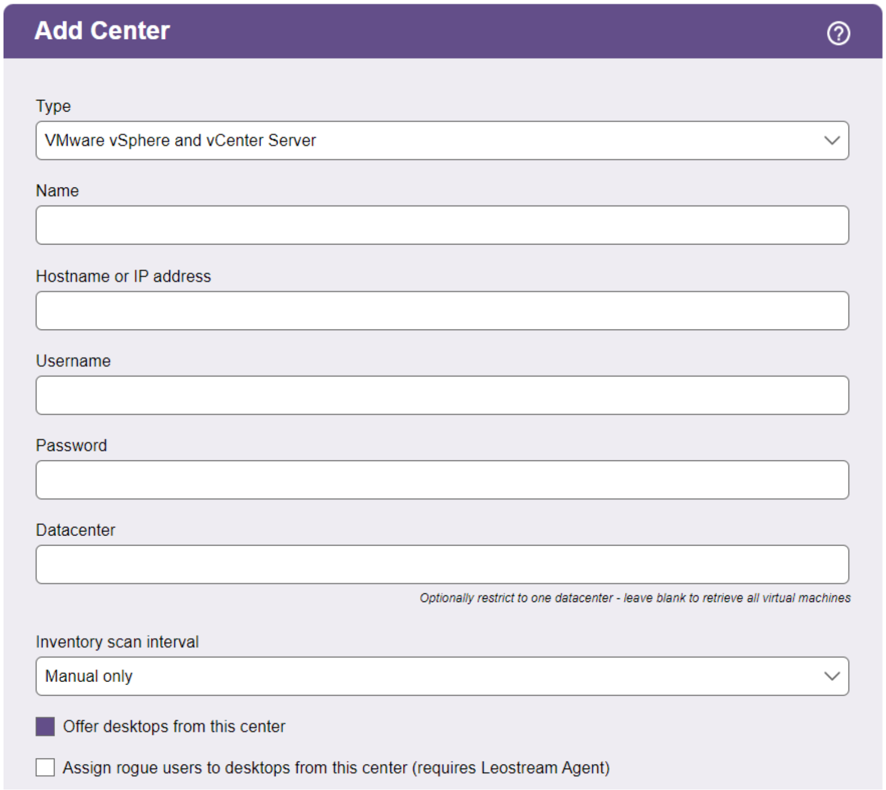
2. Click the **Add Center** link, as shown in the following figure.



Actions	Name	Type
	All	All
Edit | Scan | Log	Enrolled Desktops	Uncategorized Desktops
Edit | Scan | Log	GCP	Google Cloud
Edit | Scan | Log	PCoIP Devices	PCoIP Devices
Edit | Scan | Log	Printers	Printer Repository
Edit | Scan | View | Log	Scale Cluster	Scale Computing

3. Configure the **Add Center** form, as follows:

   a. Select VMware vSphere and vCenter Server from the **Type** drop-down, as shown in the following figure.



Add Center

Type

VMware vSphere and vCenter Server

Name

Hostname or IP address

Username

Password

Datacenter

Optionally restrict to one datacenter - leave blank to retrieve all virtual machines

Inventory scan interval

Manual only

☑ Offer desktops from this center

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

Your Connection Broker license determines which hosting platforms you can integrate with your Connection Broker. If the hosting platform you want to use is not listed in the ***Type*** *drop-down menu, please contact sales@leostream.com to obtain an updated license key.*

b. Enter a name for the center in the **Name** edit field.

c. Enter the vCenter Server's address in the **Hostname or IP address** edit field.

d. In the **Username** edit field, enter the name of a user with the necessary privileges.

e. Enter this user's password into the **Password** edit field.

f. Click **Save**.

For full instructions, see the "VMware vSphere and vCenter Server" section in Chapter 6 of the Connection Broker Administrator's Guide.

If your vCenter Server manages a large number of machines, refreshing the center can place a substantial load on vCenter Server. If you are experiencing responsiveness issues, try increasing the refresh interval.

Leostream requires specific VMware vCenter Server privileges in order to perform various actions, such as starting and stopping VMs, or provisioning new virtual machines. If your Connection Broker is unable to perform any of these actions, ensure that you create your center with an account that has all the required privileges. You can use the **Test** action associated with your saved VMware center to see what privileges are assigned to the user associated with this center.

To see the virtual machines inventoried from this center, navigate to the **> Resources** > **Desktops** page. See the "Working with Desktops" section of the Connection Broker Administrator's Guide for information on viewing, editing, and controlling desktops from within the Connection Broker.

Configuring the Connection Broker

In the **Configuration** section of the Connection Broker Administrator Web interface, you define the pools, plans, and policies that determine which users have access to which desktops, how they are connected, and how the Connection Broker manages the user's session.

Step 1: Creating Pools

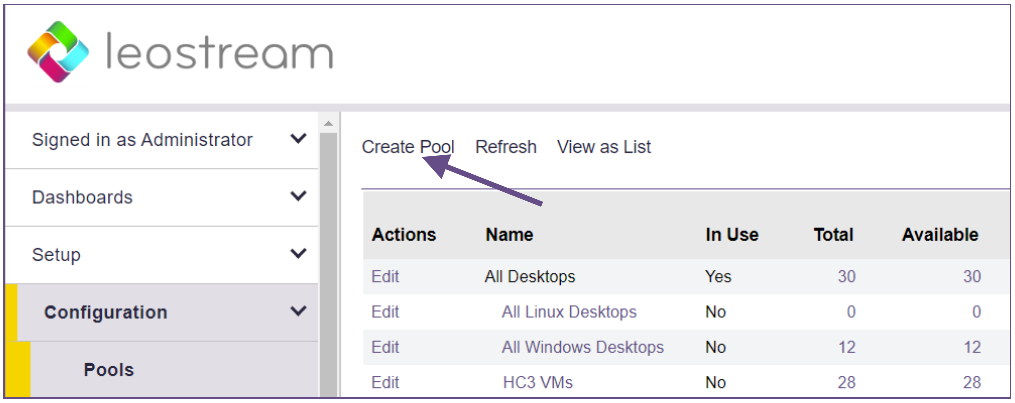
After you create your centers and the Connection Broker inventories your desktops, you logically group the desktops into ***pools***. Use pools to create sets of desktops that you want to offer to particular groups of users, or to group desktops that are administrated by particular individuals.

*The Leostream Connection Broker defines a **pool** as a group of desktops. Desktops can be members of multiple pools. How the Connection Broker manages the user's connection to a desktop is determined by the pool it is offered from.*

Leostream provides a number of flexible methods for creating pools. For a complete description, see the "Creating Desktop Pools" chapter in the Connection Broker Administrator's Guide. In this example, we'll create a pool of all of the Microsoft Windows virtual machines in the vSphere center created in the previous chapter.

1. Navigate to **> Configuration > Pools** menu.

2. Click the **Create Pool** link, shown in the following figure.



Actions	Name	In Use	Total	Available
Edit	All Desktops	Yes	30	30
Edit	All Linux Desktops	No	0	0
Edit	All Windows Desktops	No	12	12
Edit	HC3 VMs	No	28	28

3. In the **Create Pool** form that open, enter a unique name for this pool in the **Name** edit field.

4. From the **Subset of pool** drop-down menu, select **All Windows Desktops**.

5. Select **Centers** from the **Define pool using** drop-down menu.

6. From the **Available centers** list, select your vCenter Server center.

7. Click the **Add items** link to the right of the **Available centers** list. The VMware center should now be listed in the **Selected centers** list.

8. Click **Save**.

Step 2: Defining Pool-Based Plans

After you separate your desktops into pools, define the rules that control how the Connection Broker manages the user’s connection to desktops in those pools. To perform this step, ask yourself the following questions.

- What display protocols do I want the user to use to connect to their desktops?
- How do I want to manage the power state of each desktop, for example, should it be turned off when the user logs out?
- How long can users remain assigned to a particular desktop? For example, if the user logs out, should they remain assigned to that desktop, or should another user be able to log in?

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

Protocol Plans

The Connection Broker always establishes a PCoIP connection when a user logs in at a PCoIP client and connects to a virtual machine with a VMware View Direct-Connection Plug-In. Users can also log in using Leostream Connect, which launches the connection to the virtual machine using the VMware Horizon client.

Your Connection Broker license determines which display protocols your Connection Broker can use. If the display protocol you want to use is not shown on the ***Create Protocol Plan****, please contact sales@leostream.com to obtain an updated license key.*

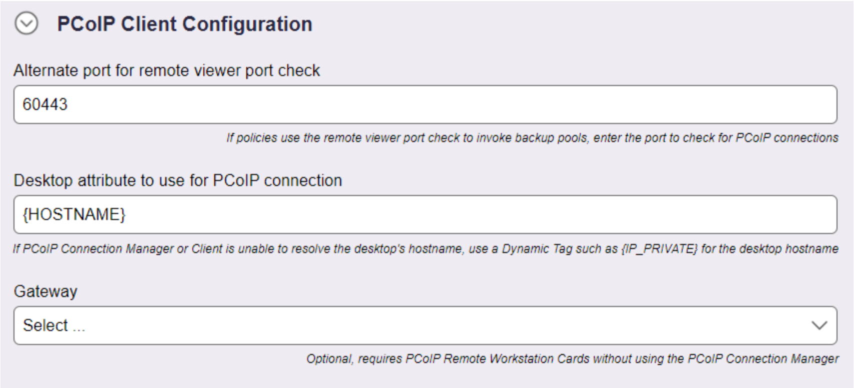
Establishing Connections from a PCoIP Zero Client

When logging in from a PCoIP zero client, the protocol plan is used only to configure the port to check when using backup pools. By default, the Connection Broker checks port 4172. If you want to change the default port:

1. Go to the **> Configuration > Protocol Plans** page.

2. Click the **Create Protocol Plan** at the top of the page. The **Create Protocol Plan** form opens.

3. Scroll down to the **Teradici PCoIP Client Configuration** section, shown in the following figure.



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

4. Enter the new port in the **Alternate port for remote viewer port check** edit field.

5. Click **Save** to save the form.

Establishing Connections using Leostream Connect

When using Leostream Connect, the user's client device must have an installed VMware Horizon View client. You can then use Leostream protocol plans to launch the VMware client and establish a PCoIP connection to a Windows virtual machine running the VMware View Direct-Connection Plugin.

To configure the protocol plan for software-based PCoIP connections:

1. Go to the **> Configuration > Protocol Plans** page.
2. Create a new protocol plan or edit an existing plan.
3. In the **Leostream Connection and Thin Clients Writing to Leostream API** section, select **1** from the **Priority** menu associated with **VMware View**.
4. Also in the **Leostream Connection and Thin Clients Writing to Leostream API** section, select **Do not use** or set lower priority to all other protocols.
5. In the **Command line parameters** edit field, enter the command line parameters needed to connect the user with single sign-on.
   The default parameters, shown below, launch the Windows version of the VMware View client.

   ```
   -nonInteractive -serverURL {IP} -userName {USER} -password
   {PLAIN_PASSWORD} -domainName {DOMAIN} -desktopName {VM:NAME} -
   desktopProtocol PCOIP
   ```

   The Linux version of the VMware View client requires different parameter. If your users are logging in from a Linux client device, modify the command line parameters, as follows;

   ```
   --nonInteractive --serverURL {IP} --userName {USER} --password
   {PLAIN_PASSWORD} --domainName {DOMAIN} --desktopName {VM:NAME} --protocol
   PCOIP
   ```

   If you have users logging in from Windows and Linux devices, create two protocol plans and assign the appropriate plan based on the user's location. See "Assigning Plans to Locations" in Chapter 13 of the Connection Broker Administrator's Guide for more information.

6. In the **Port for remote viewer check** specify the port number that the Connection Broker pings to determine if the desktop is available for PCoIP connections.
7. Click **Save**.

When creating a policy, ensure that you associate the protocol plan that uses the VMware View client with the pool of virtual machines with a VMware View Direct-Connection Plug-in.

Establishing Connections using the Leostream Web Client

The Leostream Web client uses the VMware Horizon View client URI to launch a PCoIP connection to the desktop. To configure the Connection Broker to support PCoIP connections to virtual machines:

1. Create a pool of virtual machines with a running VMware Horizon View Agent Direct-Connection Plug-In.

2. Create a protocol plan to assign to these virtual machines. In the **Web Browser** section of the protocol plan:

   a. Set the **Priority** of the **External viewer** to **1**.

   b. Set the **Priority** of all other protocols to **Do not use**.

   c. In the **Configuration file** for the external viewer, enter:

   ```
   vmware-view://{HOSTNAME}/{VM:NAME}?desktopProtocol=PCOIP
   ```

3. Build a policy that assigns the protocol plan from step 2 to the pool of virtual machines created in step 1.

4. Assign the policy to the user.

When a user who is assigned this policy logs into the Connection Broker, the broker offers the user a virtual machine from the pool. When the user requests a connection to the virtual machine, the Connection Broker launches the VMware Horizon View client, which establishes the PCoIP connection to the desktop.

The VMware Horizon View client URI does not support single sign-on.

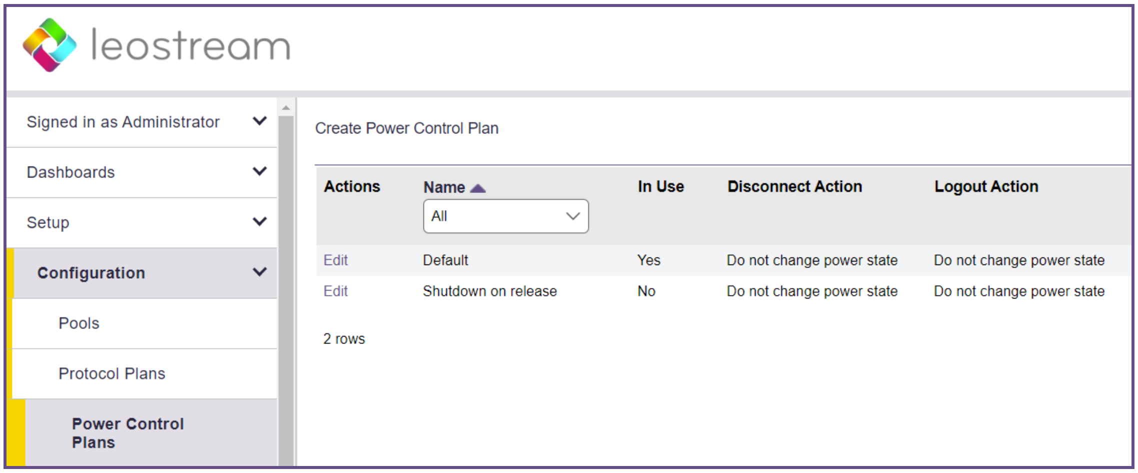
Power Control Plans

Power control and release plans allow you to take actions on the user’s remote desktop based on different events, such as:

- When the user disconnects from their desktop
- When the user logs out of their desktop
- When the desktop is released to its pool
- When the user’s session has been idle for a specified length of time

⚠ The remote 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. Not all display protocols allow the Connection Broker to perform actions at these times.

Power control plans define what power control action is taken on a desktop. Available power control plans are shown on the **> Configuration > Power Control Plans** page, shown in the following figure.



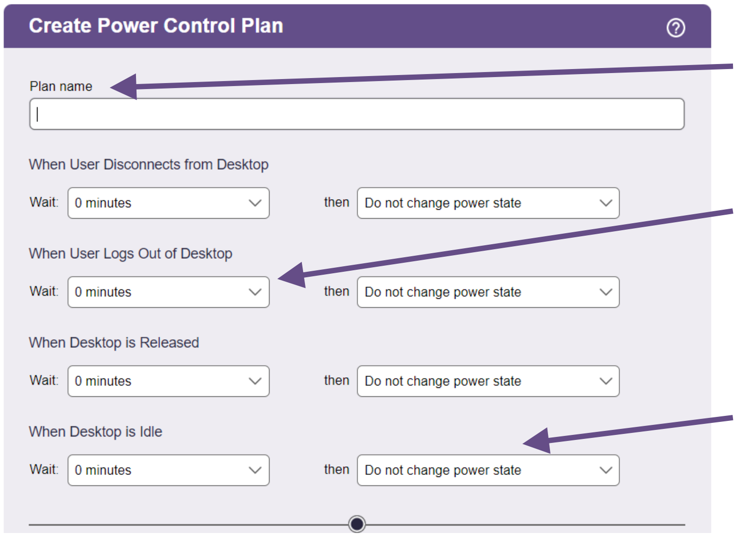
Create Power Control Plan

Actions	Name All	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

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



Create Power Control Plan

Plan name

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

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

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

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

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

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

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

2. Enter a unique name for the plan in the **Plan name** edit field.

3. For each of the remaining sections:

   a. From the **Wait** drop-down menu, select the time to wait before applying the power action.

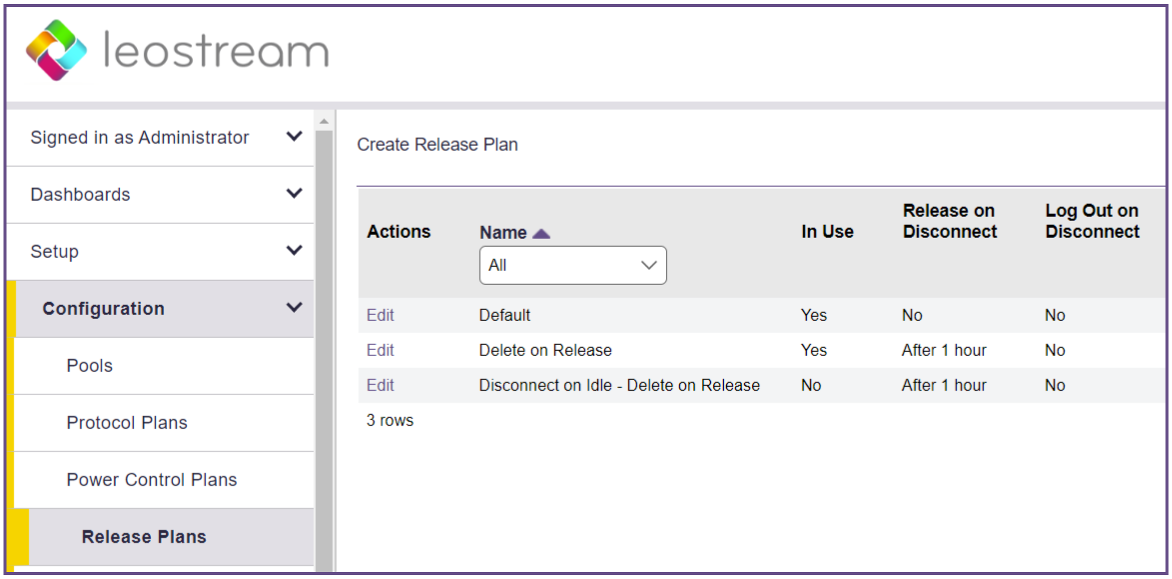
   b. From the **then** drop-down menu, select the power control action to apply. Selecting **Do not change power state** renders the setting in the **Wait** drop-down menu irrelevant, as no action is ever taken.

4. Enter any optional **Notes**.

5. Click **Save** to store the changes or **Cancel** to return to the **> Configuration > Power Control Plans** page without creating the plan.

Release Plans

Release plans define how long a desktop remains assigned to a user and when it is released to its pool, as well as if a user should be forcefully logged out of their desktop. Available release plans are shown on the **> Configuration > Release Plans** page, shown in the following figure.

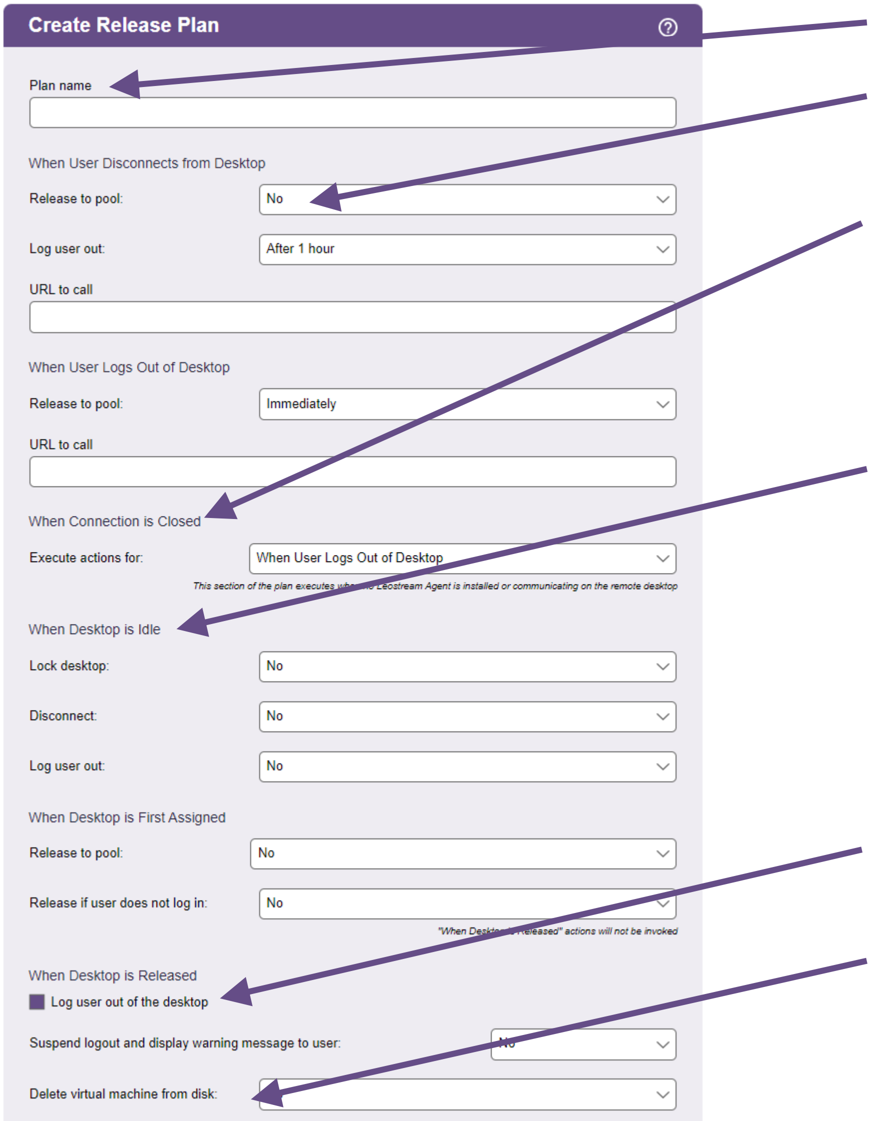


Actions	Name ▲ All	In Use	Release on Disconnect	Log Out on Disconnect
Edit	Default	Yes	No	No
Edit	Delete on Release	Yes	After 1 hour	No
Edit	Disconnect on Idle - Delete on Release	No	After 1 hour	No

3 rows

New Connection Broker installations contain one default release plan. However, you can create as many additional release plans as needed for your deployment. For example, to build a release plan that schedules a logout after the user disconnects from their desktop:

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



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:

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.

Select 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**.

When using this release plan, the Connection Broker 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.

Step 3: Building Policies

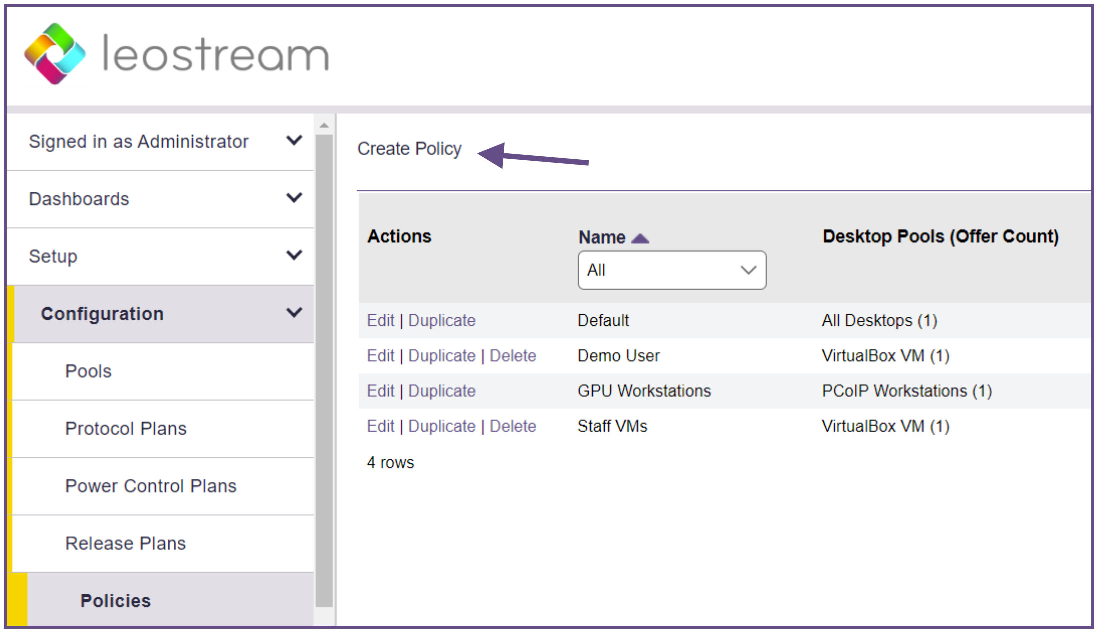
After you define your pools and plans, build policies that assign the plans to desktops.

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: the pools to offer desktops from; what display protocol is used to connect to those desktops, 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:

1. Navigate to the **> Configuration > Policies** menu.

2. Click the **Create Policy** link, shown in the following figure.



Actions	Name	Desktop Pools (Offer Count)
Edit | Duplicate	Default	All Desktops (1)
Edit | Duplicate | Delete	Demo User	VirtualBox VM (1)
Edit | Duplicate	GPU Workstations	PCoIP Workstations (1)
Edit | Duplicate | Delete	Staff VMs	VirtualBox VM (1)

4 rows

3. In the **Create Policy** form, enter a name for the policy in the **Policy name** edit field. For a discussion on the remaining general policy properties, see the Connection Broker Administrator’s Guide.

4. Click **Save** to initialize the policy.

5. Go to the **Pool Assignments** tab.

6. Click the **Add Pool Assignments** link. The **Edit Pool Assignment** form opens.

7. 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.

8. 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.

9. 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.

   In a simple proof-of-concept environment, many of these settings can be left at their default values. Note that, by default, the Connection Broker does not offer a desktop to a user if the desktop does not have an installed Leostream Agent. If you want to assign 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.

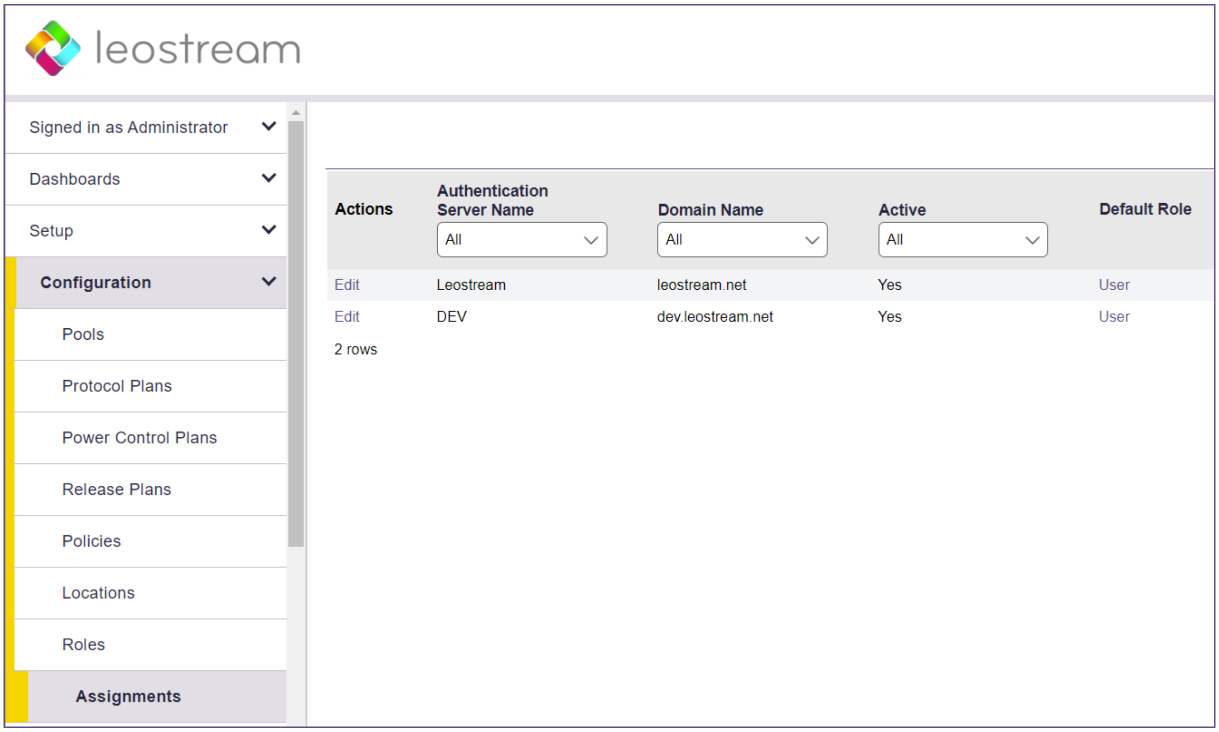
10. Click **Save**.

See the “Configuring User Experience by Policy” chapter in the Connection Broker Administrator’s Guide for a complete description on Connection Broker policies.

Step 4: 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.

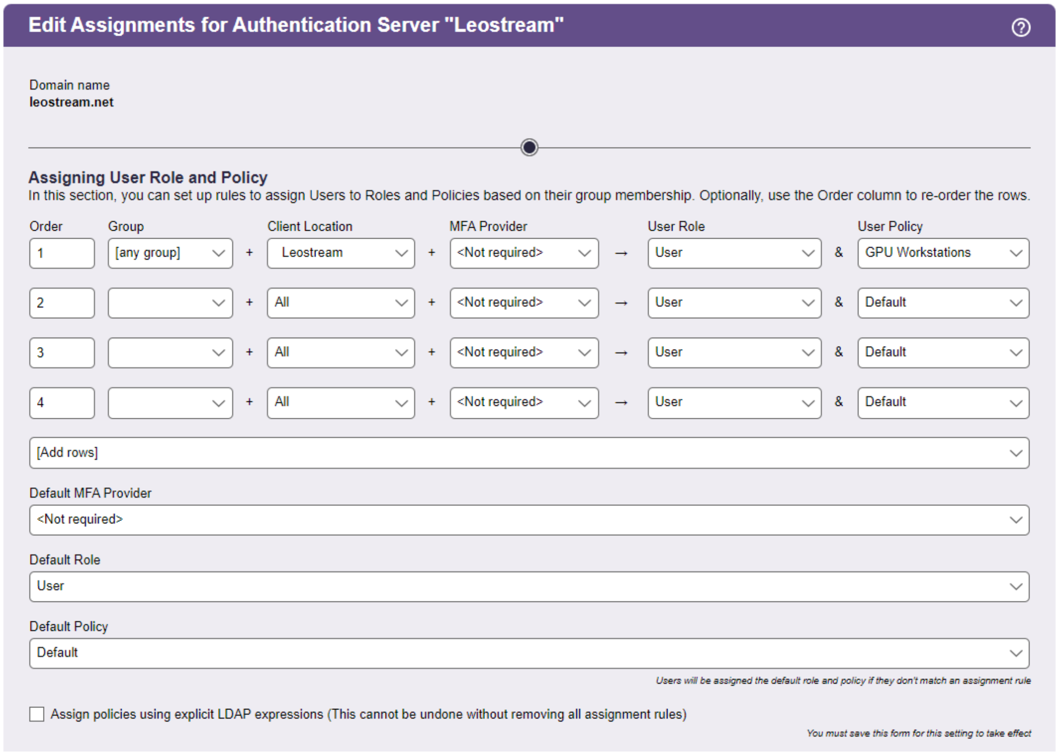
The Connection Broker then looks on the **> Configuration > Assignments** page, shown in the following figure, for the assignment rules associated with the user’s authentication server. For example, if the Connection Broker authenticated the user in the `Leostream` domain defined on the **> Setup > Authentication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

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

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

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 in Active Directory after 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 a role 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

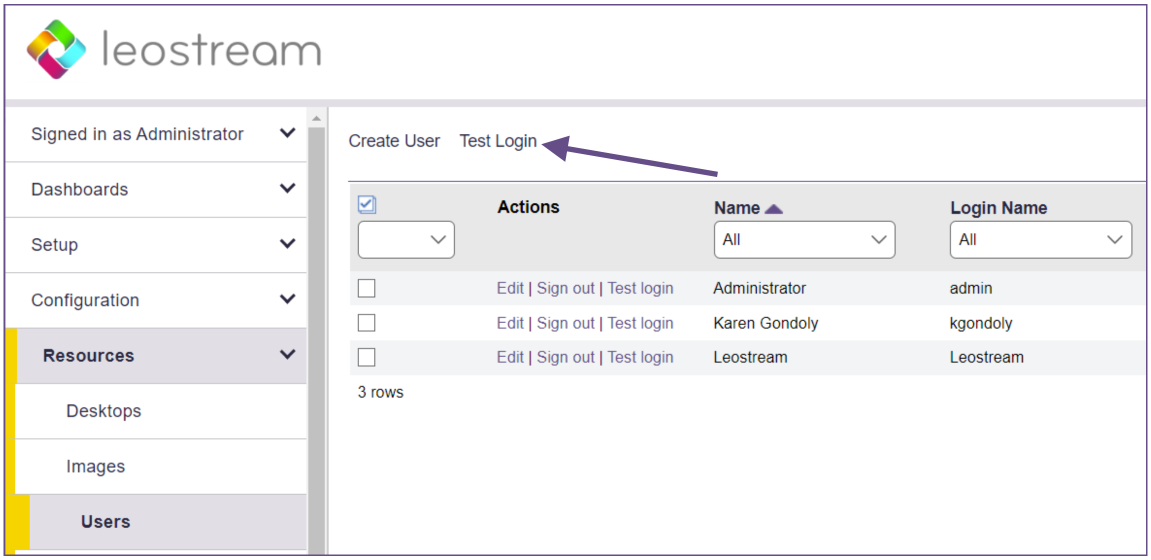
If you need to assign roles and policies based on a different authentication server attribute, uncheck the **Query for group information** option at the bottom of the **Edit Assignments** form. After you save the form, the format of the **Assigning User Role and Policy** section changes.

For information on locations and roles, see the Connection Broker Administrator's Guide.

Step 5: Testing User Login

To test your Connection Broker, ensure that users are being assigned to the correct policy, and offered the correct desktops. You can test user logins before the user has ever logged into, and been loaded into, Leostream.

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 the **Test Login** link at the top of the page, shown in the following figure.



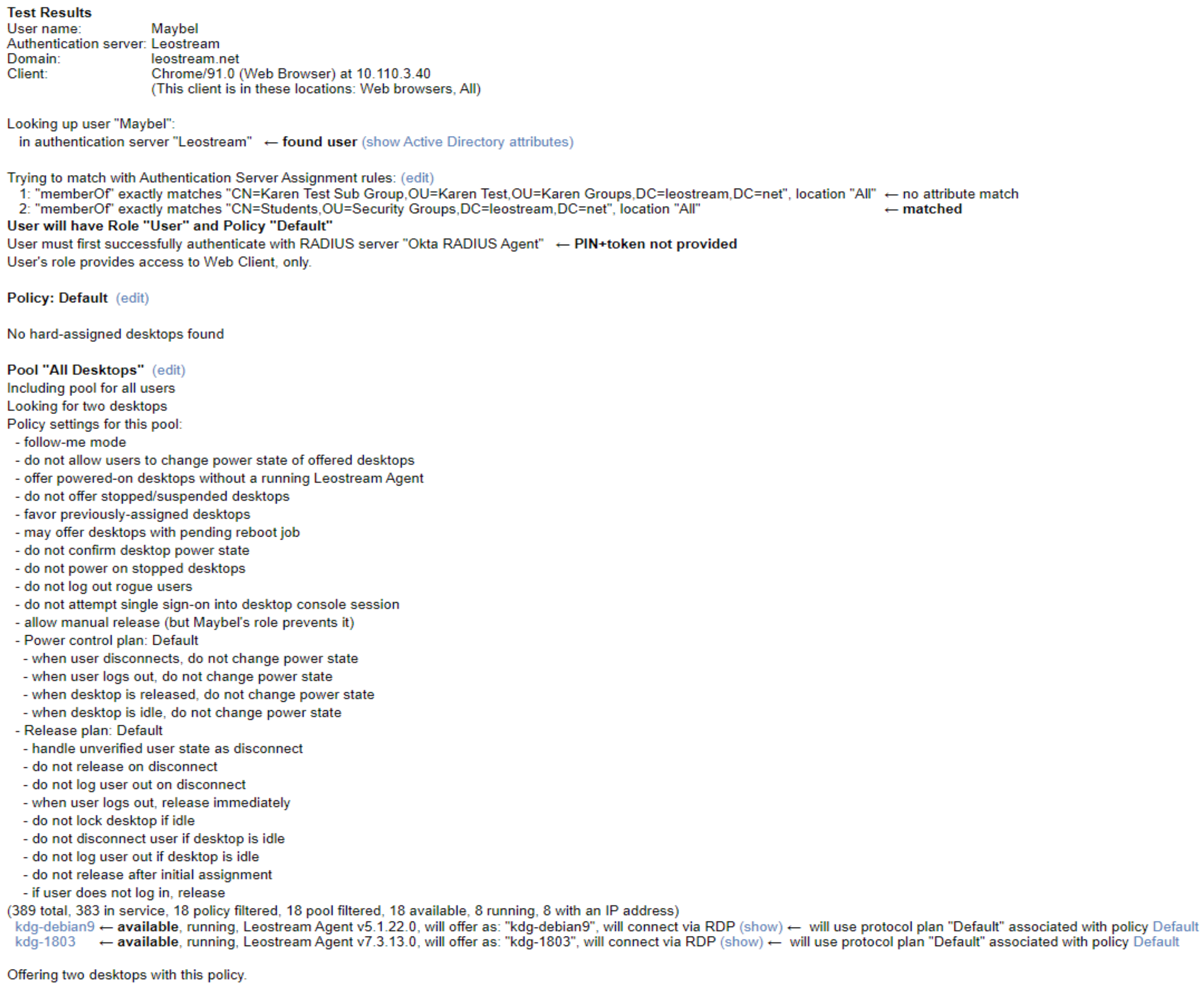
☑	Actions	Name ▲	Login Name
		All	All
□	Edit | Sign out | Test login	Administrator	admin
□	Edit | Sign out | Test login	Karen Gondoly	kgondoly
□	Edit | Sign out | Test login	Leostream	Leostream

3 rows

3. In the **Test Login** 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.

5. 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 6: Configuring PCoIP Zero Clients

You can use any PCoIP Zero client to manage PCoIP connections to a virtual machine running the VMware Horizon View Direct-Connection Plug-in. To configure a PCoIP zero client for Leostream logins:

1. Go to the zero client’s **Configuration** dialog or the **Configuration** menu in the client’s Web interface
2. Select **Session**.
3. In the **Session** page:
   a. Select **PCoIP Connection Manager** from the **Session Connection Type** drop-down menu
   b. Enter your Leostream Connection Broker address in the **Server URI** edit field.
4. Click **Apply**.

PCoIP zero clients that use the **PCoIP Connection Manager** connection type can offer the user workstations with a PCoIP Remote Workstation card or virtual machines with the Direct-Connection Plug-in. Leostream establishes the PCoIP connection to the user’s selected resource.