leostream®

Remote Desktop Access Platform

Configuring the Leostream® Connection Broker

Connecting People – Connecting Business

Version 2024
August 2025

Contacting Leostream

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

http://www.leostream.com
Telephone: +1 781 890 2019
Fax: +1 781 688 9338

To submit an enhancement request, email features@leostream.com.
To request product information or inquire about our future direction, email sales@leostream.com.

Copyright

Trademarks

Patents

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

Contents

Chapter 1: Using this Documentation

Overview

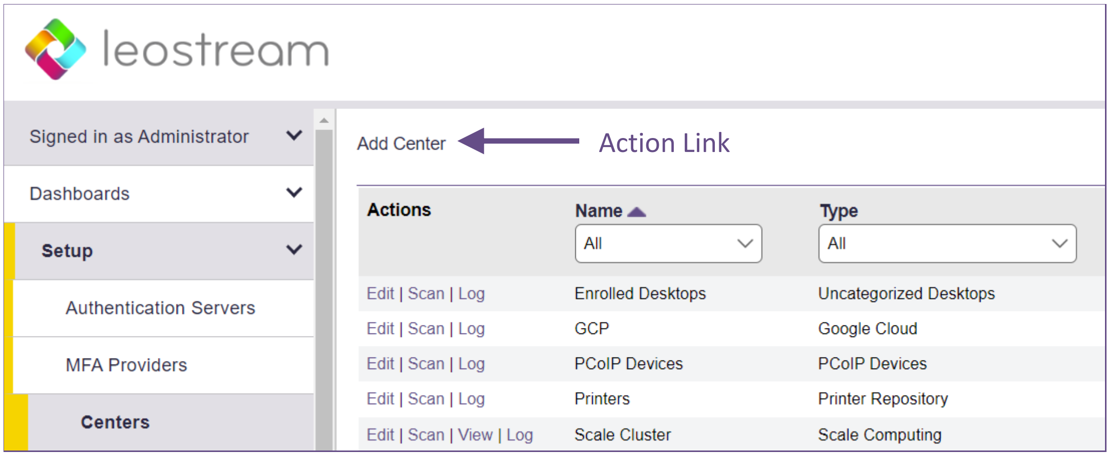
The Connection Broker Administrator’s Guide is intended for system administrators who are configuring and administering the Connection Broker via the Administrator Web interface.

- The term *you* in this document represents the administrator installing and configuring the Connection Broker.

- The term *user* or *end user* represents an end user that logs into the Connection Broker to access their assigned resources.

Navigational Conventions

The Connection Broker Administrator Web interface contains a two-level navigation tree along the left side. Your selection in the navigation tree determines the contents of the management panel, which includes links for actions that can be taken in that panel, for example:



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

This document uses the following convention when referencing items in the navigation tree and on the management panel:

- **> Setup** indicates a top-level selection

- **> Setup > Centers** indicates a secondary level selection

- **Add Center** indicates clicking a link or action in the management panel

Formatting Conventions

Format	Indicates
Bold	The name of a menu item, button, or link to be clicked, or a selection from a drop-down menu.
`Courier New`	Example code, commands, or directory/file name, or text to be entered into an edit field
Italics	Part of a command to be replaced by information specific to your configuration

Related Documentation

- Introduction to Leostream Concepts: Describes Leostream components and terminology. Please, consult this document before beginning to work with your Leostream Connection Broker.

- Installation Guide: Instructions on installing the Connection Broker, Leostream Connect, and Leostream Agent.

- Quick Start Guides: Step-by-step instructions on setting up common Connection Broker configurations.

- Guide to Working with Display Protocols: Information on how to integrate the Leostream Connection Broker with a variety of third-party display protocols.

- Connection Broker Virtual Appliance Guide: Instructions for managing and configuring the Leostream Connection Broker virtual appliance.

- Leostream Scaling Guide: Information on building production Leostream environments that supports high availability, resiliency, and scale.

- Security Review: Pieces of the Connection Broker relevant to a security audit.

Chapter 2: Getting Started

Installing the 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 or any other Linux distribution.

The Connection Broker can be installed on a minimal operating system or, if you prefer, on a system running a desktop environment. The Connection Broker utilizes the time zone and networking configuration of the underlying operating system, so ensure that you configure all time and networking information prior to installing the Connection Broker.

⚠ Ensure that the machine where you are installing the Connection Broker has at least 8GB of RAM.

For complete installation instructions, please consult the **Leostream Installation Guide**.

Entering Your License

Your Leostream license is derived from the serial number you received from Leostream Sales. Install your Connection Broker before trying to obtain your Leostream license, as you require the installation code associated with your broker. If you are adding new Connection Brokers to a Leostream cluster, consult the **Leostream Scalability Guide** for information on how to apply your existing Leostream license to all Connection Brokers in the cluster.

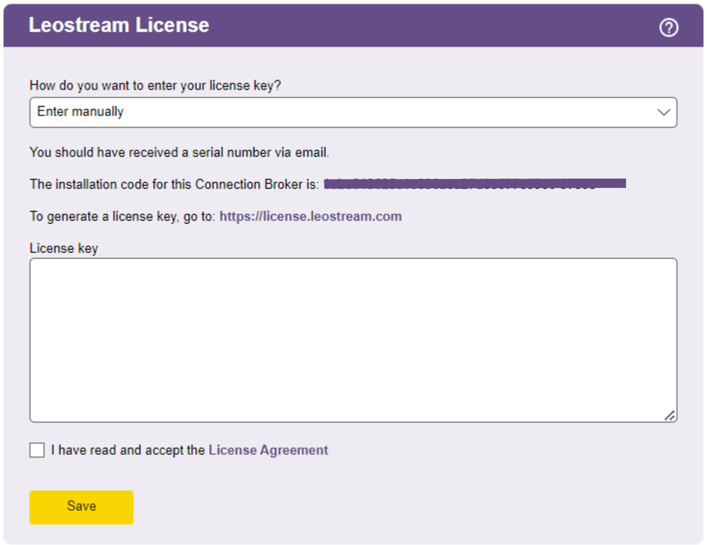
If you have not obtained a Leostream serial number, please contact **sales@leostream.com**.

To apply your license key:

1. Log into your Connection Broker from a Web browser that has internet access.

   The default administrator credentials are:
   - Username = `admin`
   - Password = `leo`

2. On the **Leostream License** page, shown in the following figure, select **Enter manually** from the **How do you want to enter your license** key drop-down menu.



Leostream License

How do you want to enter your license key?

Enter manually

You should have received a serial number via email.

The installation code for this Connection Broker is: [redacted]

To generate a license key, go to: https://license.leostream.com

License key

□ I have read and accept the License Agreement

3. In the text below the installation code for your Leostream Connection Broker, click the link to go to **https://license.leostream.com**. The installation code for your Connection Broker is automatically populated.

4. Enter the serial number you obtained from Leostream sales.

5. Enter the email address associated with that serial number.

6. Click **Generate a license**.

7. Click the **Apply to the broker** button above the generated license key. The browser returns to the **Leostream License** page.

8. Select the **I have read and accept the License Agreement** check box.

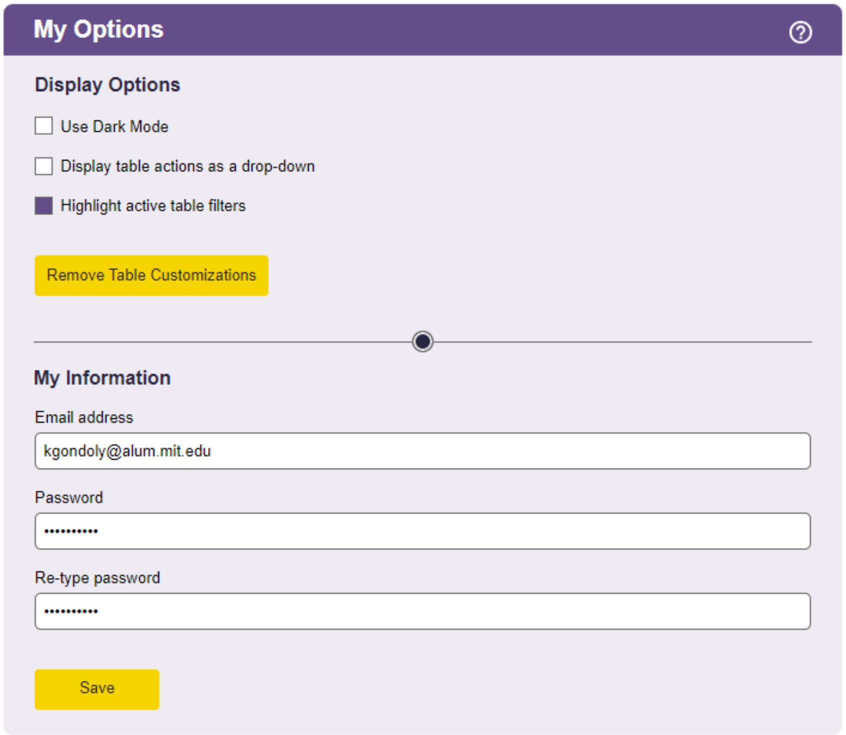
9. Click **Save**.

If you cannot access the Leostream license server from your Connection Broker Web portal, navigate to **https://license.leostream.com** on a different device. Manually enter your serial number and installation code, then copy your Leostream license to enter into your Connection Broker.

Because you entered your Connection Broker installation code with your serial number, the generated license key is tied to this Connection Broker installation.

Changing Your Password

For security reasons, change the default administrator password the first time you use your Connection Broker. To change the administrator password, log in to the Connection Broker as the default administrator and go to the **> Signed in as > My Options** page, shown in the following figure.



My Options

Display Options

□ Use Dark Mode

□ Display table actions as a drop-down

☑ Highlight active table filters

My Information

Email address: kgondoly@alum.mit.edu

Password: ••••••••••

Re-type password: ••••••••••

1. Enter a new password in the **Password** edit field.

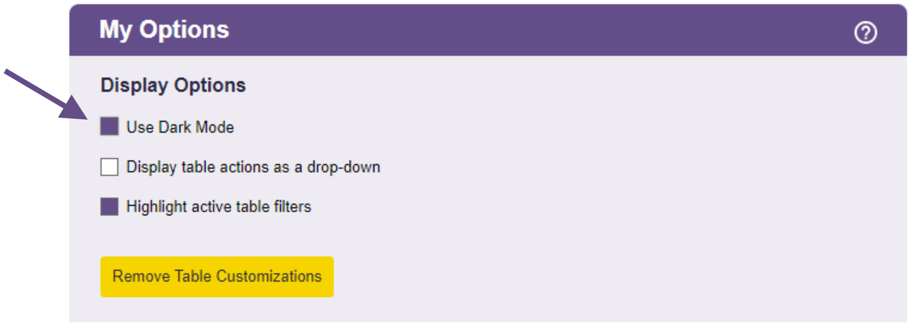
2. Reenter the new password in the **Re-type password** edit field.

3. Click **Save**.

⚠ The Connection Broker cannot remind you of your password. If you forget your administrator password, reset it using the Connection Broker virtual machine console. See “The Local Connection Broker Administrator” in the **Connection Broker Security Review** document for complete instructions.

Entering and Exiting Dark Mode

Connection Broker 2023.2 introduces Dark Mode to the Administrator and User Web Client. Each individual with a Role that gives them access to the Administrator Web interface may individually elect to display the portal in Dark Mode. To enter Dark Mode, select the **User Dark Mode** checkbox, shown in the following figure, and save the **My Options** form. To return to Light Mode, uncheck this option and save the form.



My Options

Display Options

☑ Use Dark Mode

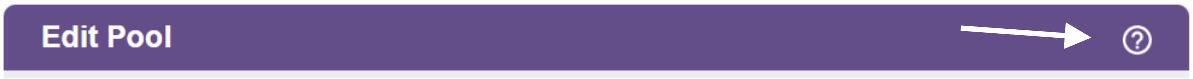
□ Display table actions as a drop-down

☑ Highlight active table filters

Using Standard Connection Broker Web Interface Controls

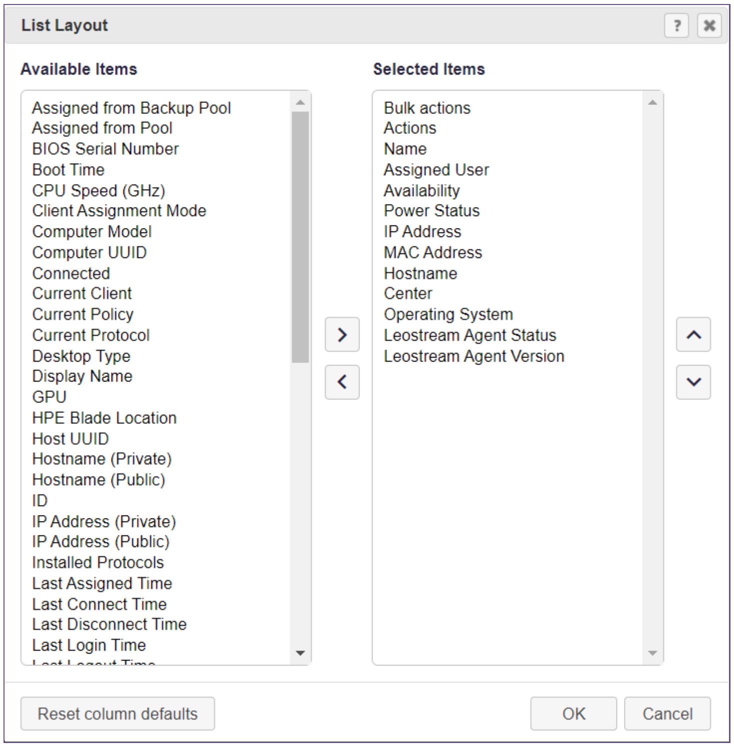
Getting Context Sensitive Help

You can access context sensitive help for Connection Broker forms by clicking on the question mark icon at the top-right of each form, as shown in the following figure. Clicking the help button opens a reference page that describes the options available on that form.



Customizing Tables

Clicking the **Customize columns** link at the top-right of any table in the Connection Broker management panel opens the **List Layout** dialog. This dialog, shown in the following figure, allows you to change the content and order of the columns in the associated table.


List Layout

Available Items

Assigned from Backup Pool
Assigned from Pool
BIOS Serial Number
Boot Time
CPU Speed (GHz)
Client Assignment Mode
Computer Model
Computer UUID
Connected
Current Client
Current Policy
Current Protocol
Desktop Type
Display Name
GPU
HPE Blade Location
Host UUID
Hostname (Private)
Hostname (Public)
ID
IP Address (Private)
IP Address (Public)
Installed Protocols
Last Assigned Time
Last Connect Time
Last Disconnect Time
Last Login Time
Last Logout Time

Selected Items

Bulk actions
Actions
Name
Assigned User
Availability
Power Status
IP Address
MAC Address
Hostname
Center
Operating System
Leostream Agent Status
Leostream Agent Version

- To add columns to the table, select the desired item or items in the **Available Items** list and click the **>** button.

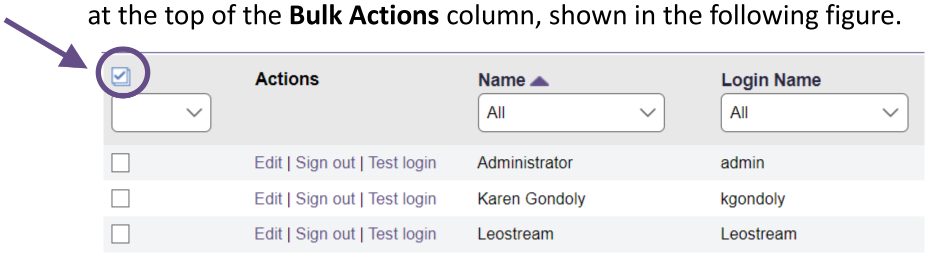
- To remove columns from the table, select the item or items in the **Selected Items** list click the **<** button

Click **OK** to save the changes or **Cancel** to discard your changes.

At any time, you can click **Reset column defaults** to return to the out-of-the-box list of selected items.

Performing Bulk Actions

You can quickly select or deselect all items in any of the Connection Broker tables by clicking the checkbox at the top of the **Bulk Actions** column, shown in the following figure.



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

Select an action from the drop-down menu below the checkbox to apply an action to all selected items.

If the **Bulk Actions** column does not appear on one of the Connection Broker tables, use the **customize** link at the bottom of the table to add this column (see **Customizing Tables**)

Saving and Deleting Records

All Connection Broker forms provide some or all of the following command buttons.

Button	Description
Save	Stores the information on the screen in the Connection Broker database. To exit from a form without saving changes to the data, click a menu link or the Web browser’s **Back** button. The Connection Broker discards all changes.
Delete	Removes the record from the Connection Broker database. In all cases, the Connection Broker asks you to confirm your choice. The **Delete** button may not appear if the record is in use. For example, in the **Edit Role** dialog, the **Delete** button does not appear if the role is assigned to one or more users. To delete the role, you must first ensure that all users are assigned to another role.
Cancel	Discards any changes made in the form. • For forms that are accessed from a link, the **Cancel** button closes the form without saving changes and navigates back to the page containing the original link. • For forms accessed directly from a secondary menu, the **Cancel** button reverts any changes made since the form was last saved. • For forms that open in a separate Web browser, the **Cancel** button closes the browser without saving changes.

Sorting, Searching, and Filtering Lists

You can sort, search, and filter the contents of all lists using the headers and drop-down menus at the top of each column.

- Click on the column headers to sort the table using the entries in that column.
- Use the drop-down menus filter the table to show only entries that match the selected characteristic

Task	How to
Sort a list of records	Click the column heading. An arrow next to the header indicates the current sorted order, either ascending or descending. For example, on the **> Resources > Desktops** page, to sort by name, click the **Name** link. Until you specifically sort a table, the rows in the table are presented in the order in which the table was filled.
Filter a list by a selected field value or an alphabetic character	Open the drop-down list below the column heading and check one or more items to include in the list. For example, on the **> Resources > Desktops** page, to display only desktop with names starting with the letter T, check the **T** from the drop-down list under the **Name** link. To display desktops with names starting with T and U, check both **T** and **U** from the drop-down list under the **Name** link. To clear the filter restriction for a specific field, choose **All** from the drop-down list for that field.
Search a list specific items	Open the drop-down list below the column heading and select the **Search** option. For example, on the **> Resources > Desktops** page, to display only desktop with names starting with the text **QA**, open the drop-down menu for the **Name** column, enter **QA** in the box that appears and click **Search**. The next time you open the drop-down menu, the value you entered is displayed as a selected option, allowing you to remove or add additional items to the filtered list. See **Per-Page Search** for more detailed instructions.

To keep track of which filters are in use, you can highlight active filters on all Connection Broker tables (see **Highlighting Active Filters**.)

Entering Search Strings in Edit Fields

Certain Connection Broker edit fields allow you to search for items in a long list, for example, when selecting a user or client to hard-assign to a desktop. Begin entering text into the field to display the first 20 items that begin with that string.

You must enter or select a valid user or desktop in the edit field. The edit field will not accept a string that does not match a current user or desktop in the Connection Broker

You can use the following wildcards to modify the search.

The percent (`%`) wildcard matches any character string. For example:

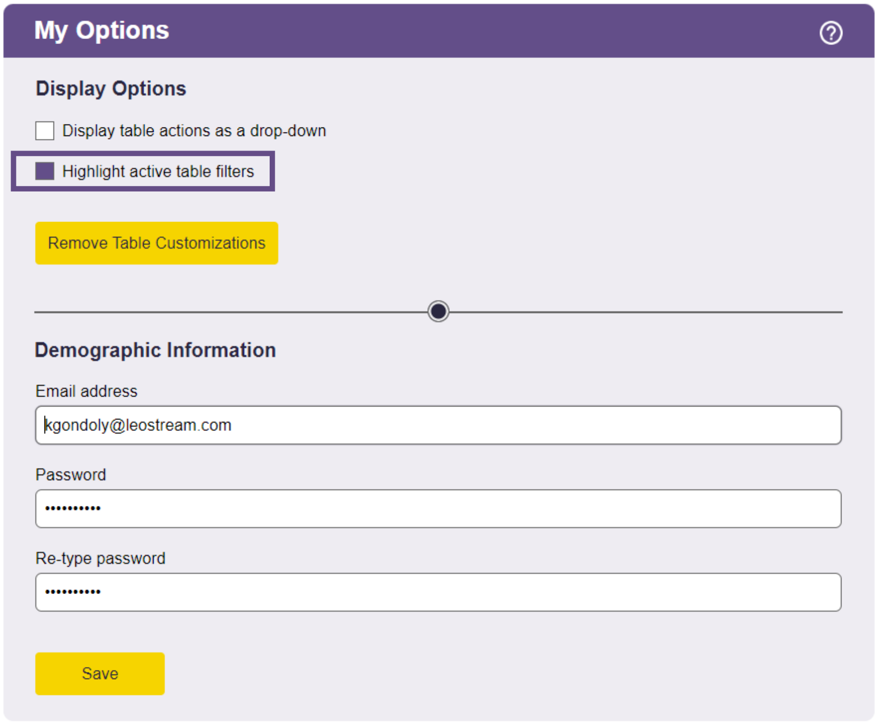
`%DEV` searches for any string that contains `DEV`

The underscore wildcard (_) matches any one character in a fixed position. For example:

`_EE_` searches for any string whose second and third character are `EE`

Highlighting Active Filters

You can use the **Highlight active table filters** option on the **> Signed in as > My Options** page, shown in the following figure, to call attention to all active filters on any Connection Broker management panel that displays a table.



My Options

Display Options

□ Display table actions as a drop-down

☑ Highlight active table filters

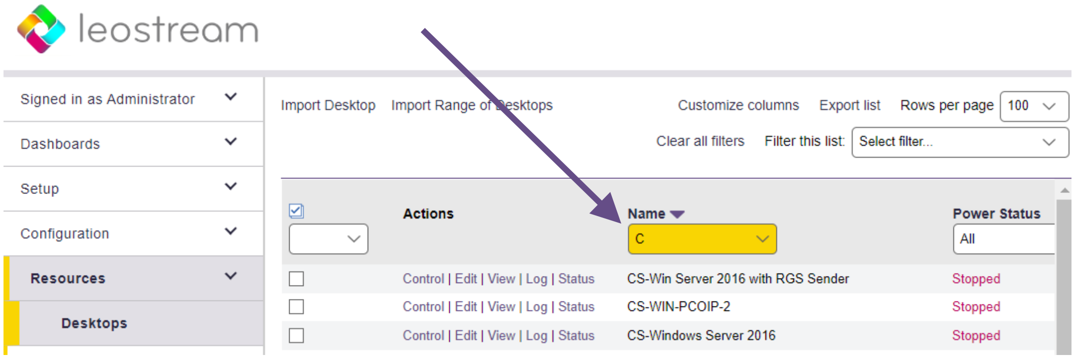
Demographic Information

Email address: kgondoly@leostream.com

Password: ••••••••••

Re-type password: ••••••••••

The Connection Broker highlights filters using Leostream yellow. Filters can be used to limit the amount of data shown in any table (see **Sorting, Searching, and Filtering Lists**). When highlighting filters, as shown in the following figure, you can ensure that you understand what data is shown, and what data may be missing, in a table.



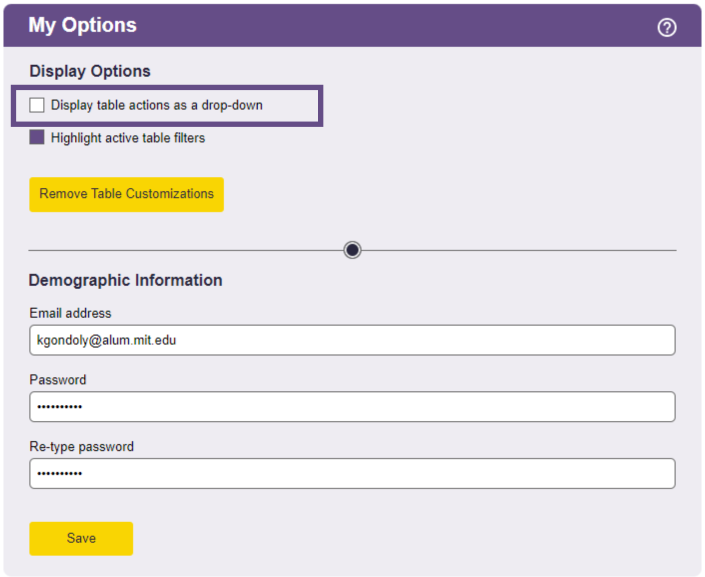
Rows per page: 100

Filter this list: Select filter...

☑	Actions	Name	Power Status
		C	All
☐	Control | Edit | View | Log | Status	CS-Win Server 2016 with RGS Sender	Stopped
☐	Control | Edit | View | Log | Status	CS-WIN-PCOIP-2	Stopped
☐	Control | Edit | View | Log | Status	CS-Windows Server 2016	Stopped

Formatting the Display of Actions in Tables

On pages that display tables, such as the **> Resources > Desktops** page, you can display the contents of the **Actions** column as a series of links or combined into a drop-down menu. Use the **Display table actions as a drop-down** option on the **> Signed in as > My Options** page, shown in the following figure, to switch between formats.



☐ Display table actions as a drop-down

☑ Highlight active table filters

Email address: kgondoly@alum.mit.edu

Password: ••••••••••

Re-type password: ••••••••••

When this option is selected, actions appear in the web page as drop-down menus. If this option is not selected, actions appear as a series of links.

Restoring Connection Broker Default Views

The Connection Broker stores page configurations for all users with access to the Connection Broker Administrator Web interface, including how columns are arranged in tables, which filters are applied, etc. This information is stored in the user’s session state file. The session file grows as you customize more display settings, which may result in degraded response times in the Administrator web interface.

If the load time for pages in the Connection Broker becomes slow, you can remove your stored configurations from the session file to improve performance, as follows.

1. Go to the **> Signed in as > My Options** page.

2. Click the **Remove Table Customizations** button.

3. Click **OK** in the confirmation dialog to continue.

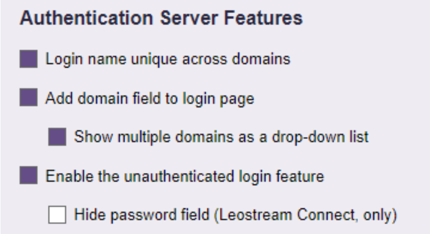
The Connection Broker removes stored customizations from the session file, but you must log out and log back in to see the changes reflected on the Connection Broker lists.

Chapter 3: Configuring Connection Broker Settings

Leostream configuration options that apply globally to your Leostream environment are set on the **> System > Settings** page.

Enabling Authentication Server Features

The following figure shows the options available for configuring user authentication.



Authentication Server Features

■ Login name unique across domains

■ Add domain field to login page

■ Show multiple domains as a drop-down list

■ Enable the unauthenticated login feature

□ Hide password field (Leostream Connect, only)

The following features can be toggled on or off.

- **Login name unique across domains**: Determines if a specific login name applies to the same physical user across multiple domains.
    - If the **Login name unique across domains** option is *not* selected, the Connection Broker assumes that a username that is repeated in multiple domains belongs to a different physical user and creates a new user record for each instance of the username. In this case, the **Domain** drop-down menu contains a **<None>** option. Selecting **<None>** instructs the Connection Broker to authenticate users only if they are defined locally in the Connection Broker.

      If your user names are not unique across domains, ensure that you select the **Add domain field to login page** option to display the **Domain** field on all client login pages, to ensure that users can select their correct domain.

    - If the **Login name unique across domains** option *is* selected, the Connection Broker assumes that a username that is repeated in multiple domains belongs to the same physical user, and creates a single user record for that username. In this case, the **Domain** drop-down menu contains an **<Any>** option. Selecting **<Any>** instructs the Connection Broker to search through all the authentication servers in the order of their priority
- **Add domain field to login page**: When selected, the **Domain** field is shown on the **Sign in** page of the Leostream Web client and the **Login** dialog of Leostream Connect. This option automatically selects when you uncheck the **Login name unique across domains** option, and Leostream recommends leaving this option on in this configuration.
- **Show multiple domains as a drop-down list:** When selected, the **Domain** field on Leostream Web clients and Leostream Connect clients appears as a drop-down menu. Otherwise, the **Domain** field

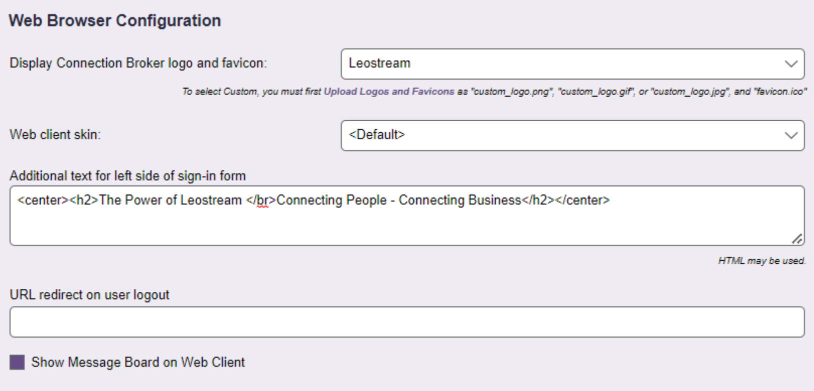
appears as an edit field. The **Domain** field is always an edit field if the Connection Broker contains a single authentication server, regardless of if this option is selected.

When using a drop-down menu, the **Include domain in drop-down** option on the individual **Edit Authentication Server** pages determines if a particular domain is included in the list.

- **Enable the unauthenticated login feature**: Displays the **Allow unauthenticated logins** option on the **Create/Edit Authentication Server** forms. Selecting this option in an authentication server allows users to log in through that authentication server without entering a password.
  - **Hide password field (Leostream Connect, only)**: Select this option to hide the password field on the Leostream Connect **Login** page.

Web Interface Look-and-Feel

The **Web Browser Configuration** section, shown in the following figure, allows you to define aspects of the end-user experience and brand identity for the Leostream Web client and Connection Broker Administrator Web interface.



Web Browser Configuration

Display Connection Broker logo and favicon: Leostream

To select Custom, you must first Upload Logos and Favicons as "custom_logo.png", "custom_logo.gif", or "custom_logo.jpg", and "favicon.ico"

Web client skin: <Default>

Additional text for left side of sign-in form

```
<center><h2>The Power of Leostream </br>Connecting People - Connecting Business</h2></center>
```

HTML may be used.

URL redirect on user logout

☑ Show Message Board on Web Client

The following sections describe the options shown in the previous figure.

Internationalizing the Web Login Page

You can customize the text on the Connection Broker **Sign in** page by defining a new set of sign-in terminology. To define the text displayed on the **Sign in** page, go to **> System > Skins**.

After you define new terminology, apply it to your Connection Broker using the **Web client skin** drop-down menu in the **Web Browser Configuration** section of the **> System > Settings** page. All Connection Brokers in a cluster use the same terminology.

Displaying a Custom Logo and Favicon

Use the **Display Connection Broker logo and favicon** drop-down menu in the **Web Browser Configuration** section of the **> System > Settings** page to show or hide the Leostream branding on all Connection Broker Web pages.

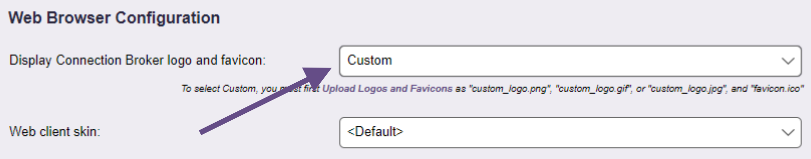
- Select **Leostream** to display the default Leostream logo and favicon.
- Select **Custom** to display a logo and favicon you load into the Connection Broker, as described in the following procedure.
- Select **None** to hide the Leostream logo and favicon. If the Leostream favicon continues to appear, close all instances of the Connection Broker Web interface and clear your Web browser's cache.

To display a custom logo and favicon.

1. Create your custom logo and favicon, using the following constraints
   a. The logo must be saved to a file named `custom_logo`.
   b. The logo must be saved in one of the following formats:
      - `gif`
      - `png`
      - `jpg`

      If you load multiple logos, the Connection Broker displays the first file, as determined by the ordered shown in the previous list.
   c. The filename must be all lower case, for example, `custom_logo.jpg`.
   d. The logo can be any size. If you plan to display message text along with the logo, limit the logo height to allow room for the text.
   e. The favicon must be stored in a file named `favicon.ico`.
   f. The favicon must be 16x16 pixels.
2. After you create your files, go to the **> System > Maintenance** page to upload them into the Connection Broker.
3. Select the **Upload** option in the **Logos and Favicons** section of the **Maintenance** page.
4. Click **Next**.
5. In the **Upload Logos and Favicons** form that opens, enter or browse for the `custom_logo` file.
6. Click **Upload** to upload the file.
7. Repeat steps 3 through 6 to install the `favicon.ico` file.
8. If you have a cluster of Connection Brokers, repeat steps 2 through 7 to upload the image into each Connection Broker in the cluster.
9. After all image files are installed, go to the **> System > Settings** page.

10. In the **Web Browser Configuration** section, select **Custom** from the **Display Connection Broker logo and favicon** drop-down menu, as shown in the following figure.



Web Browser Configuration

Display Connection Broker logo and favicon: Custom

To select Custom, you must first Upload Logos and Favicons as "custom_logo.png", "custom_logo.gif", or "custom_logo.jpg", and "favicon.ico"

Web client skin: <Default>

11. Click **Save** on the **> System > Settings** page.

In many web browsers, you must close all instances of the Connection Broker Web interface and clear the browser’s cache before the new favicon displays.

Use the **Remove** option in the **Logos and Favicons** section of the **Maintenance** page to list and remove logos that were previously uploaded into your Connection Broker.

Setting Message Board Text

Select the **Show Message Board on Web Client** option to display the information on the **> Dashboards > Message Board** page to end users who log into the Leostream Web client.

To edit the message board:

1. Log in to the Connection Broker Administrator Web interface.

2. Go to the **> Dashboards > Message Board** page.

3. Click the **Edit the message board** link at the bottom of the page.

4. Enter the new message board text in HTML format. See **Adding Customized Text, Links, and Images to the Login Page** for instructions on adding images and links to documents in the message text.

5. Click **Save**.

Adding Customized Text, Links, and Images to the Sign In Page

Use the **Additional text for the left side of sign-in form** field in the **Web Browser Configuration** section of the **> System > Settings** page to place customized text and images on the **Sign In** page. You can enter any text in HTML format. The text appears in the Web page to the right of the **Sign In** form.

To add images or links to documents, first upload the file into the Connection Broker using your preferred secure file transfer application. For organizational purposes, Leostream suggests placing the files in the `/var/lib/leo/app/tpc` directory. After the images are located in that directory, you can use the following HTML code in the **Additional text for left side of sign in form** field to display the uploaded image in your **Sign In** form.

```
<IMG SRC=https://cb-address/tpc/filename WIDTH=w HEIGHT=h>
```

Where:

- *cb-address* is your Connection Broker IP address
- *filename* is the name of your image file you uploaded into the Connection Broker
- *w* is the image width
- *h* is the image height

Use the following HTML code in the **Additional text for left side of sign-in form** field to display a link to an uploaded document.

```
<A HREF=https:// cb-address /tpc/filename>Text to display here</A>
```

Where:

- *cb-address* is your Connection Broker IP address
- *filename* is the name of your file you uploaded into the Connection Broker
- *Text to display here* is text you want displayed on the login page

URL Redirect on User Logout

When a user logs out of the Connection Broker Web client, by default, they are redirected back to the Connection Broker **Sign In** page. You can redirect users to a different web page by entering the web address into the **URL redirect on user logout** edit field in the **Web Browser Configuration** section of the **> System > Settings** page.

Communicating with Leostream Agents

The Leostream Agents accepts communications only from Connection Brokers or clusters that are registered with the agents.

To ensure proper Leostream Agent communications, first inventory your desktops in your Connection Broker (see **Chapter 6: Connecting to your Hosting Platforms**) and then install the Leostream Agent on your desktops. When installing Leostream Agents, ensure that you specify your Connection Broker address

When the Leostream Agent starts, it contacts the registered Connection Broker and obtains the public key required to communicate with those brokers. If the Leostream Agent contacts the Connection Broker on a port that is different from the default Leostream Agent port, the Connection Broker updates the desktop record, accordingly.

Setting the Connection Broker VIP for Leostream Agent Responses

Leostream Agents respond to the Connection Broker using the Connection Broker virtual IP (VIP).

The Connection Broker is accessed at the IP address of the operating system on which it is installed. Leostream recommends using a static IP address or DNS SRV record, and configuring DNS with your primary search domain. Otherwise, if your DHCP has a short lease time, your Connection Broker IP address may time-out and your end users will not be able to log in to their desktops.

You can use DNS A records instead of DNS SRV records. However, the Leostream Agents and Leostream Connect clients will not automatically discover the Connection Broker address in a DNS A record. If using DNS A records, you must manually configure the Connection Broker address in every Leostream Agent and Leostream Connect client. In addition, to have the Connection Broker send the name in the A record instead of the Connection Broker IP address, you must enter the A record name into the **Connection Broker Virtual IP (VIP) address or hostname** field.

The Connection Broker VIP address serves the same purpose as a DNS SRV record, and can be used in cases where you do not have or cannot create a DNS SRV record. The information you enter in this setting depends on your Connection Broker configuration, as follows.

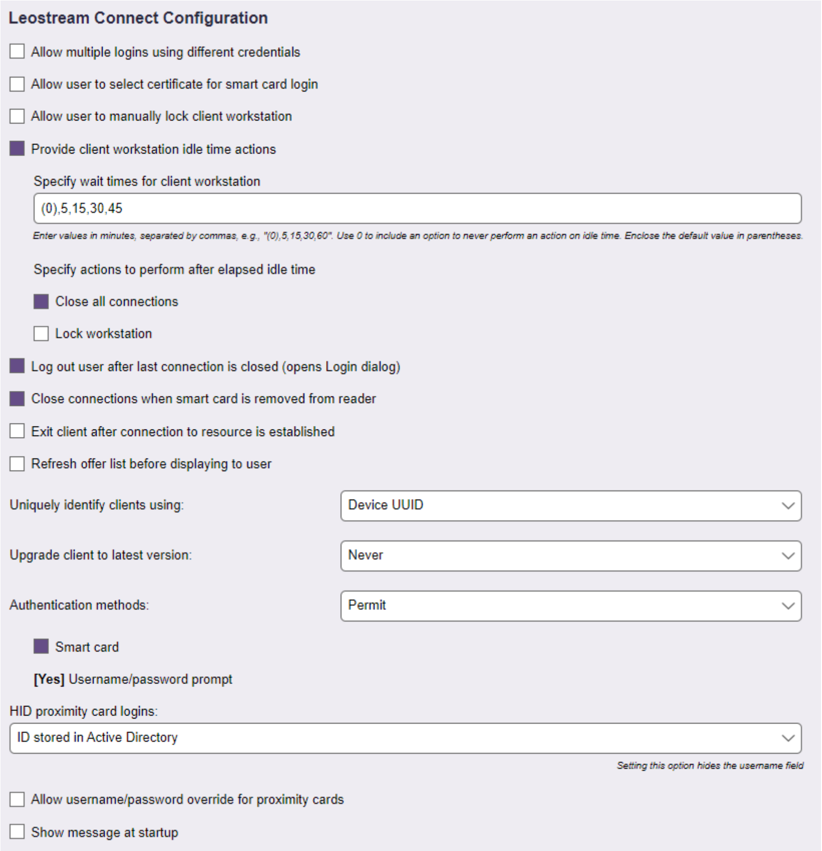
- If you have a single Connection Broker, in most cases, leave this field empty. Specify the VIP only if you have a DNS SRV record pointing to a different Connection Broker. For example, you may have a production Connection Broker that uses the DNS SRV record and want to set up a second test environment Connection Broker. In this example, enter the test environment's Connection Broker IP address into its **Connection Broker Virtual IP (VIP) address or hostname** edit field.

- If you have a cluster of Connection Brokers and you configured a DNS SRV record with either the Connection Broker addresses or the VIP address of a load balancer, leave the **Connection Broker Virtual IP (VIP) address or hostname** edit field empty.

- If you have a cluster of Connection Brokers that are load balanced through a third-party load balancer and do not have a DNS SRV record with the VIP address of a load balancer, enter the IP address of the load balancer in the **Connection Broker Virtual IP (VIP) address or hostname** edit.

Configuring Leostream Connect

The Leostream Connect client allows users to connect to their hosted resources from any Microsoft Windows®, Linux® or Apple macOS device. Use the options in the **Leostream Connect Configuration** section of the **> System > Settings** page, shown in the following figure, to control the function and appearance of Leostream Connect.



Leostream Connect Configuration

☐ Allow multiple logins using different credentials

☐ Allow user to select certificate for smart card login

☐ Allow user to manually lock client workstation

■ Provide client workstation idle time actions

Specify wait times for client workstation

(0),5,15,30,45

Enter values in minutes, separated by commas, e.g., "(0),5,15,30,60". Use 0 to include an option to never perform an action on idle time. Enclose the default value in parentheses.

Specify actions to perform after elapsed idle time

■ Close all connections

☐ Lock workstation

■ Log out user after last connection is closed (opens Login dialog)

■ Close connections when smart card is removed from reader

☐ Exit client after connection to resource is established

☐ Refresh offer list before displaying to user

Uniquely identify clients using: Device UUID

Upgrade client to latest version: Never

Authentication methods: Permit

■ Smart card

[Yes] Username/password prompt

HID proximity card logins: ID stored in Active Directory

Setting this option hides the username field

☐ Allow username/password override for proximity cards

☐ Show message at startup

Except where specified, the options apply to the Windows and Java version of Leostream Connect.
`

- **Allow multiple logins using different credentials:** (*Applies to the Windows version of Leostream Connect, only.)* Select this option to allow a user to log into Leostream Connect with multiple sets of credentials, simultaneously. Leostream Connect displays the desktops offered to all logged in users in the same resource dialog.

- **Allow user to select certificate for smart card login**: (*Applies to the Windows version of Leostream Connect, only.)* Select this option if users have smart cards containing multiple certificates, and must be able to select which certificate to use during login. With this option unchecked, the Connection Broker always uses the first valid certificate on the smart card.

- **Allow user to manually lock client workstation**: (*Applies to the Windows version of Leostream Connect, only.)* Select this option if users need to use Leostream Connect to lock their client workstation session. See "Locking the Client Session" in the Leostream Connect Administrator's Guide and End User's Manual for more information.

- **Provide client workstation idle time actions**: (*Applies to the Windows version of Leostream Connect, only.)* Select this option to allow the user to automatically lock their client workstation or close all open desktop connections when the client device running Leostream Connect is idle for a specified length of time. See the "Using Client-Side Idle Actions" section in the **Leostream Connect Administrator's Guide** for more information.

- **Log out user after last connection is closed (opens Login dialog)**: Select this option to specify that Leostream Connect should automatically log out the user after the user closes, either by disconnecting or logging out, their last resource connection. After the user is logged out, the Leostream Connect **Login** dialog automatically opens.

  Use this option in conjunction with the **Close connections when smart card is removed from reader** option to automatically prompt the next user to log in after the previous user removes their smart card or taps their proximity card to log out. With both of these options selected, after the initial users removes their smart card or taps their proximity card, all of their open resources are disconnected, they are logged out of Leostream Connect, and the **Login** dialog opens.

- **Close connections when smart card is removed from reader**: (*Applies to the Windows version of Leostream Connect, only.)* Select this option to automatically disconnect all the user's desktops and applications when they remove their smart card from the reader or when they tap their proximity card to log out of the client.

- **Exit client after connection to resource is established**: Select this option to automatically exit the user's Leostream Connect session after the connection to their resources is established.

  If the user is launching a connection to a resource they are managing for another user, Leostream Connect will not automatically exit after the connection is established. This option applies only when the user launches their assigned resource.

- **Refresh offer list before displaying to user:** Select this option to instruct Leostream Connect to perform an automatic refresh of the user's offered desktops when the user opens their offer list, ensuring that any desktops that are no longer available are removed from the list.

- **Uniquely identify clients using**: Select the primary client characteristic to use when identifying unique clients on the **> Resources > Clients** page.

  Client devices that register with the Connection Broker have the option to provide one or more of the following attributes.

  - Device UUID – An ID unique to the client hardware
  - Client UUID – An ID unique to the software client that handles the user login
  - MAC address – The client device MAC address
  - Serial number – The client device serial number

  When a client device registers with the Connection Broker and, for example, **Device UUID** is selected, the Connection Broker searches the **Device UUID** column on the **> Resources > Clients** page for a client with the provided device UUID. If the Connection Broker finds the device UUID, the Connection Broker assumes a record for the registering client already exists. If the Connection Broker does not find the device UUID, the Connection Broker creates a new client record for the registering client.

  If clients register without providing the selected characteristic, the Connection Broker searches the **Device UUID**, **Client UUID**, **MAC Address**, and **Serial Number** columns on the **> Resources > Clients** page, in order. When a client registers, if the Connection Broker finds a client on the **> Resources >**

Clients page that matches the value for any of these attributes of the registering client, the Connection Broker assumes a record for the registering client already exists. If the Connection Broker does not find a match for any of these attributes, the Connection Broker creates a new client record for the registering client.

- **Upgrade client to latest version**: When the version of Leostream Connect shown on the **> Dashboards > Downloads** page is newer than the version currently installed on your clients, use this option to push updates of Leostream Connect to the user's client device. Choose one of the following three options:

    - **Never**: Do not update Leostream Connect. In this case, you must manually update end users' clients.

    - **Always**: Always update Leostream Connect. In this case, when an end user runs Leostream Connect, the Connection Broker warns them that an update is in process. Leostream Connect restarts when the update is finished.

    - **Prompt user**: Let the user decide if they want to update Leostream Connect. In this case, when the user runs Leostream Connect, the client prompts the user to install the update.

  If users do not have administrator privileges on their Windows client device and Leostream Connect was originally installed with a task that required administrator privileges, such as USB redirection, you must install the Leostream Update service on the client device.

- **Authentication Methods**: (*Applies to the Windows version of Leostream Connect, only.)* Use this option to restrict or permit various authentication methods. To allow users to log in using any of the different types of authentication methods:

    - Select **Permit** from the drop-down menu in the **Authentication Methods** section
    - Check each of the allowed authentication method. You must permit user name and password authentication.

  To require the user to use certain authentication methods:

    - Select **Require** from the drop-down menu in the **Authentication Methods** section
    - Check each of the authentication method the user is required to use.

- **HID proximity card logins**: (*Applies to the Windows version of Leostream Connect, only.)* Use this option to allow users to log into the Connection Broker using an RF IDeas proximity card reader and HID proximity card. For complete instructions on using proximity cards for user logins, see "HID Proximity Card Authentication with RF IDeas pcProx© Readers" in the Leostream Connect Administrator's Guide and End User's Manual.

- **Allow username/password override for proximity cards**: Provide a link on the Leostream Connect proximity card Login dialog that allows users to enter a username and password instead of tapping their proximity card.

- **Show message at startup**: Indicate if a message should be displayed to the user directly after they launch Leostream Connect. Selecting this option displays the following two fields.

- **Dialog title**: Enter a string to include in the title bar of the message dialog.
- **Message text**: Specify the message to display. You can enter text formatted as plain text or HTML.

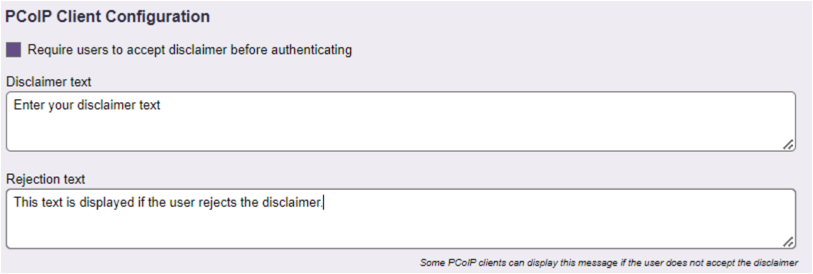
Displaying a Disclaimer before PCoIP Client Logins

PCoIP (HP Anyware) 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.

To enable disclaimers:

1. Scroll down to the **PCoIP Client Configuration** section on the **> System > Settings** page in your Connection Broker.
2. Select the **Require users to accept disclaimer before authenticating** option. The form updates as shown in the following figure.



PCoIP Client Configuration

☑ Require users to accept disclaimer before authenticating

Disclaimer text

Enter your disclaimer text

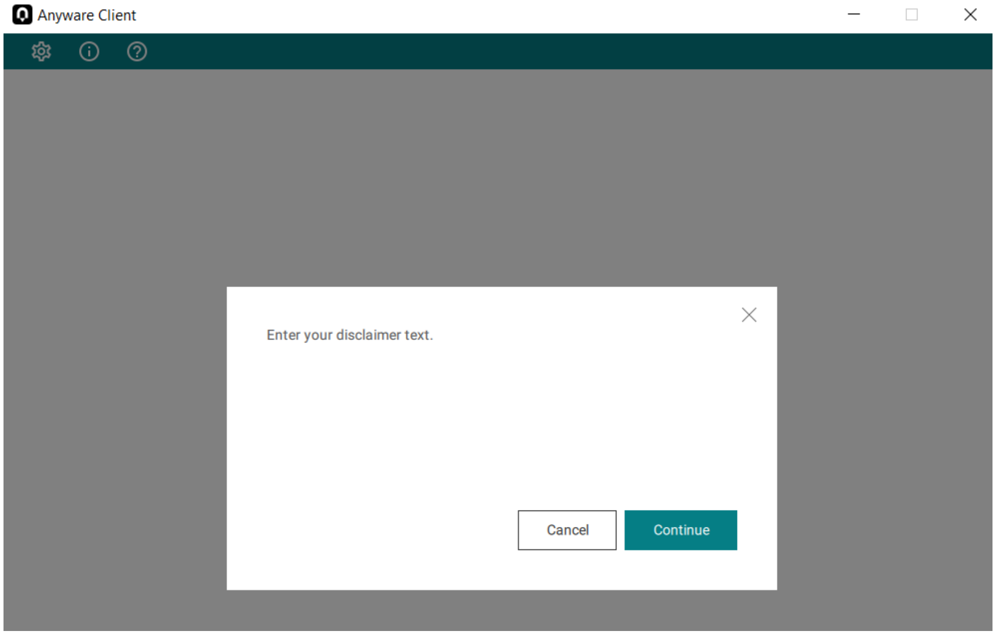
Rejection text

This text is displayed if the user rejects the disclaimer.

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

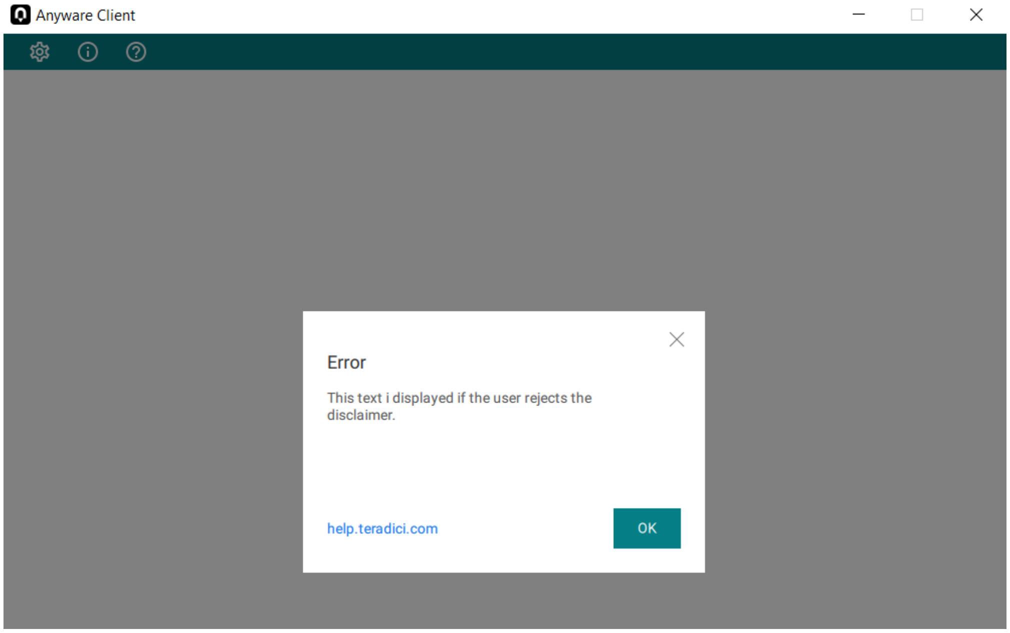
3. In the **Disclaimer text** edit field, enter your full disclaimer text. HTML formatting is not currently supported.
4. In the **Rejection text** edit field, enter the text to display if the user rejects the disclaimer. Note that not all PCoIP clients display this reply.

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



Enter your disclaimer text.

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

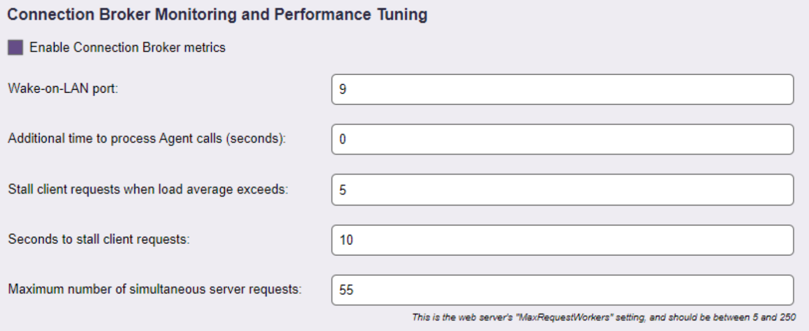


Error

This text i displayed if the user rejects the disclaimer.

Setting and Monitoring Connection Broker Performance Thresholds

If you have applications, for example, thin clients, that communicate with the Connection Broker, you can change the default load average threshold on the **> System > Settings** page. Scroll down to the bottom of the form to the **Connection Broker Performance Tuning** section, shown in the following figure.



Connection Broker Monitoring and Performance Tuning

■ Enable Connection Broker metrics

Wake-on-LAN port: 9

Additional time to process Agent calls (seconds): 0

Stall client requests when load average exceeds: 5

Seconds to stall client requests: 10

Maximum number of simultaneous server requests: 55

This is the web server's "MaxRequestWorkers" setting, and should be between 5 and 250

To use this section:

- By default, Connection Broker calls to the Leostream Agent time out after 30 seconds. If the agent cannot be contacted before the time out, the Leostream Agent may be marked as Unreachable or users may experience long wait times before their remote desktop connection occurs. To resolve these cases, you can instruct the Connection Broker to extend the timeout by entering a value up to 120 seconds in the **Additional time to process Agent calls** edit field.

- The setting in the **Stall client requests when load average exceeds** edit field sets the threshold on the load averaged number of client calls the Connection Broker processes. The default value allows the Connection Broker to process client calls without sacrificing performance. You can increase this number if your clients are receiving too many “Server Busy” warnings. Be aware that, if you set this number too high, your Connection Broker may become clogged with client calls, and cease to function properly.

  This setting applies to stalling client requests, only, and does not apply to stalling the job queue.

- The setting in the **Seconds to stall client requests** edit field indicates how long the Connection Broker will wait before returning the “Server Busy” warnings to a client. If you typically experience a login storm at some point in your business week, stalling the “Server Busy” warning may prevent the user from instantly trying to log in again, giving the Connection Broker time to process client calls and fall below its load average limit.

- The setting in the **Maximum number of simultaneous server requests** edit field sets the maximum number of client connections the Connection Broker accepts. After a client has connected, the **Stall client requests when load average exceeds** option determines the conditions for which requests from that client are accepted.

To collect metrics that indicate the load average and disk usage of your Connection Broker and cluster select the **Enable Connection Broker metrics** option. With this option selected, monitor jobs in the Connection Broker job queue collect load average information that can be displayed on the **> Dashboards > Reports** page. See **Reporting Connection Broker Metrics** for more information.

Configuring Connection Broker Security Options

The **Connection Broker Security Options** section of the **> System > Settings** page contains a set of options that allow you to tune the security settings for Connection Broker communications.

Restricting HTTP Access

The Connection Broker includes a default Leostream certificate used to encrypt traffic between the Connection Broker, Leostream Agent, and Leostream Connect clients. By default, HTTP access is also available to the Connection Broker Web interfaces, including the Administrator Web interface and Web client.

If your security guidelines require to you restrict all communications to port 443, including access to the Connection Broker Administrator Web interface, select the **Block all traffic on port 80** option available in the **Connection Broker Security Options** section of the **> System > Settings** page.

After selecting this option, click **Save** on the **> System > Settings** page to store the change. You must then reboot the Connection Broker to finalize the change to port 80 access (see **Restarting the Connection Broker**).

When port 80 is blocked, you cannot access the Connection Broker Administrator Web interface or Leostream Web client using HTTP. You must enter an HTTPS address to sign into the Connection Broker.

If port 80 is open, you can use the **Redirect http traffic to https** option to redirect the **Sign in** page from HTTP to HTTPS.

⚠ If you block all traffic to port 80 and try to use an HTTP address to access the Connection Broker, the Web browser cannot contact the Connection Broker. In this case, selecting the **Redirect http traffic to https** has no effect.

Configuring TLS Versions and SSL Cipher Suites

When negotiating secure communications between the Connection Broker and Leostream Agents or Leostream Connect clients, the Connection Broker tries any of the protocol options selected on the **> System > Settings** page.

📝 The Leostream Agent require the TSLv1.2 SSL protocol. Therefore, you cannot disable TLS v1.3 or TLSv1.2 in your Connection Broker.

The **Enable Strict-Transport-Security header (HSTS)** option on the **> System > Settings** page allows you to instruct the Connection Broker to enforce strict transport security and sets the expiration time for when the Connection Broker can be accessed using only HTTPS. Enter the expiration time in seconds. The default value is one year.

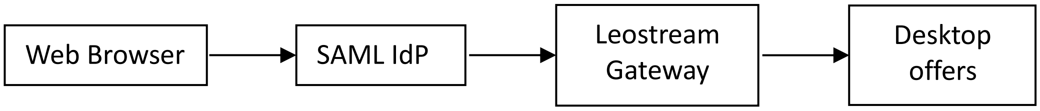
The **Connection Broker Security Options** section of the **> System > Settings** page includes an additional option that allows you to configure the Cipher Suite used for SSL. In the **Web server “SSLCipherSuite” directive** edit field, enter a colon-separated cipher-spec string consisting of OpenSSL cipher specifications to configure the Cipher Suite. For more information on the syntax entered in this field, see the **Apache Module mod_ssl** documentation.

The TLS versions accepted by the Connection Broker and the SSLCipherSuite settings are not changed when you upgrade your Connection Broker. If you use the default SSLCipherSuite and want to upgrade to the latest default settings after upgrading your Connection Broker, go to the **> Sytem > Settings** page, choose the TLS versions you want to allow, and delete all text in the **Web server “SSLCipherSuite” directive** edit field. Save the **> System > Settings** form, check that the new default Cipher Suites are shown in the the **Web server “SSLCipherSuite” directive** edit field, and restart your Connection Broker.

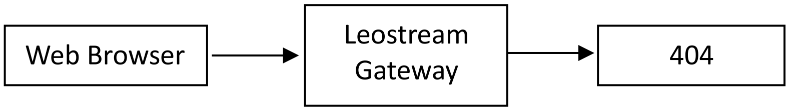
Blocking External Access to the Login Page

If your Leostream environment includes Leostream Gateways that forward login traffic to your Connection Broker *and* you leverage a SAML-based Identity Provider (IdP) for authentication, you can block access to the Leostream Login page by selecting the **Block web browser login dialog when accessing Connection Broker via a Leostream Gateway** option on the **> System > Settings** page. Enabling this option keeps bad actors from accessing the Login form for your Leostream environment.

Regardless of if the **Block web browser login dialog when accessing Connection Broker via a Leostream Gateway** option is selected or not, the following workflow is always supported.



With this option selected, however, pointing a web browser directly at the Leostream Gateway displays a 404 Not Found page.



Setting the Content Security Policy

The **Content Security Policy** (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. You can view and edit the Connection Broker Content Security Policy HTTP header using the **Web server "Content-Security-Policy" HTTP header** field on the **> System > Settings** page.

By default, the Connection Broker CSP uses the `frame-ancestors` directive to block the Connection Broker **Sign in** page from being embedded in an iframe. If you want to include the Leostream Sign in page in an iframe in your corporate portal, ensure that you add the appropriate site to the list of `frame-ancestors`.

Because the `frame-ancestors` directive obsoletes the `X-Frame-Options` header, the Connection Broker no longer includes the `X-Frame-Options` HTTP response header. Some security scanning software may flag the missing `X-Frame-Options` header.

Setting HTTP Security Headers

- Use the **Web server "Cross-Origin-Embedder-Policy" HTTP header** to prevent a document from loading any cross-origin resources that don't explicitly grant the document permission.
- Use the **Web server "Cross-Origin-Opener-Policy" HTTP header** to ensure a top-level document does not share a browsing context group with cross-origin documents.
- Use the **Web server "Cross-Origin-Resource-Policy" HTTP header** to convey a desire that the browser blocks no-cors cross-origin/cross-site requests to the given resource.

Closing Leostream Gateway Ports for Disconnected Desktop Sessions

In many circumstances, for optimal security, the Connection Broker should instruct the Leostream Gateway to close forwarded ports as soon as the user disconnects or logs out from their remote desktop. However, the Connection Broker may receive disconnect notices from the Leostream Agent when desktop connections are dropped due to temporary network outages.

Some display protocols, such as Mechdyne TGX and HP ZCentral Remote Boost, attempt to re-establish the desktop connection after a loss of network. If the Leostream Gateway forwarded port is dropped, however, the desktop connection is unavailable even after the network is restored.

If you are using a display protocol that automatically attempts to re-establish lost desktop connections, you can use the **Delay closing gateway forwarding ports on disconnect** option to hold the forwarded port open for the specified length of time, to allow the display protocol client to reconnect to the desktop when the network is restored using the original forwarded port.

If the **Delay closing gateway forwarding ports on disconnect** option is set to zero or to a value shorter than the length of time the display protocol client attempts to reconnect to the desktop, the user must return to their Leostream session to request the desktop connection and open a new Leostream Gateway port.

Throttling User Login Attempts

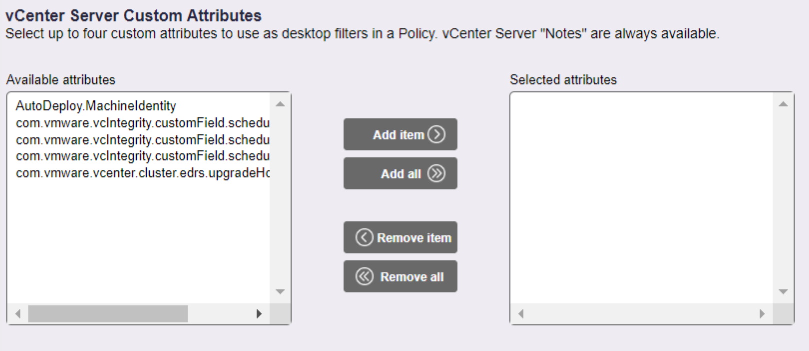
In the event your Connection Broker is exposed to the internet, you can leverage the Connection Broker's built-in rate limiting to mitigate a denial-of-service attack due login attempts for domain and local Connection Broker users. Configure the **Throttle login attempts** drop-down menu to indicate the throttling method to use.

If three failed login attempts originate from the source indicated by the selection in the **Throttle login attempts** drop-down menu, the Connection Broker waits for a pre-determined period of time before resuming checks against your LDAP server for submitted credentials from that source.

Specifying VMware vCenter Server Clusters for Desktop Filters

After you define centers for VMware vCenter Server (see **VMware® Centers**), you can use the custom attributes defined in that center as desktop filters in policies (see **Policy Filters**). You can specify up to four custom attributes for use as desktop filters.

Use the **vCenter Server Custom Attributes** section in the **> System > Settings** page, shown in the following figure, to indicate which custom attributes you want to use as desktop filters.



vCenter Server Custom Attributes

Select up to four custom attributes to use as desktop filters in a Policy. vCenter Server "Notes" are always available.

Available attributes

AutoDeploy.MachineIdentity
com.vmware.vcIntegrity.customField.schedu
com.vmware.vcIntegrity.customField.schedu
com.vmware.vcIntegrity.customField.schedu
com.vmware.vcenter.cluster.edrs.upgradeHc

Selected attributes

To select custom attributes for desktop filters:

1. Select up to four attributes in the **Available attributes** list.

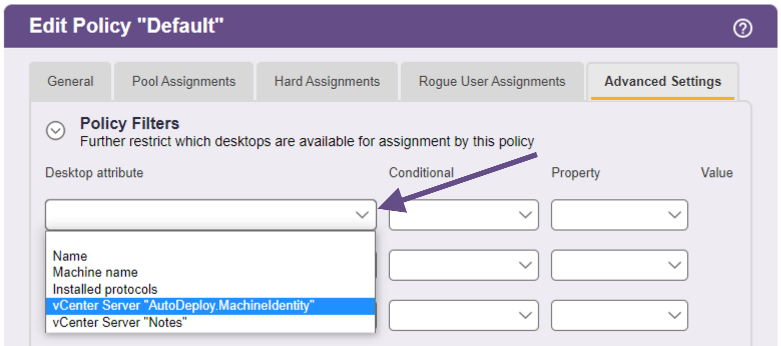
2. Move the attributes to the **Selected attributes** list by clicking the **Add item** button. Alternatively, if you have four or less attributes, click the **Add all** button to move all attributes to the **Selected attributes** list.

3. Click **Save** to store the settings.

If you move more than four items into the **Selected attributes** list, you cannot save the form. If this is the case, use the **Remove item** button or **Remove all** button to clear items out of the **Selected attributes** list.

If the same custom attribute exists in multiple vCenter Server centers, that attribute appears once in the **Available attributes** list.

The selected custom attributes appear at the bottom of the **Desktop attribute** drop-down menu in the **Pool Filters** and **Policy Filters** in every policy. The **vCenter Server “Notes”** attribute is always available for filtering. Additional custom attributes are listed directly above the notes item, as shown, for example, in the following figure.



Policy Filters

Further restrict which desktops are available for assignment by this policy

For more information on building pool and policy filters, see **Policy Filters**.

The custom attributes selected on **> System > Settings** page also become available as columns on the **> Resources > Desktops** page (see **Available Desktop Characteristics**).

Chapter 4: Preparing Remote Workstations and Virtual Machines

Leostream recommends that you install the Leostream Agent on all remote Linux, Microsoft Windows, and Apple macOS desktops. The Connection Broker requires the agent to perform advanced policy logic. In addition, the Leostream Agent is required if you plan to use Leostream USB management or location-based printing features. The Leostream Agent should be installed on any image used for provisioning in Leostream.

The Leostream Agent installs on all Microsoft Windows operating system versions currently covered by Mainstream Support under the Microsoft Fixed Lifecycle Policy, or in service under the Microsoft Modern Lifecycle Policy.

The Leostream Agent for Linux and macOS is a Java application, which requires an Oracle Java Run Time Environment (JRE) version 1.8 or higher. The Leostream Agent supports the following Linux operating systems:

- CentOS
- Debian
- Fedora
- SUSE Linux Enterprise
- Red Hat Enterprise Linux
- Ubuntu

For instructions on installing the Leostream Agent, see the Leostream **Installation Guide**.

Chapter 5: Authenticating Users

Overview

Authentication is the process of verifying the identity of an individual in order to authorize access to resources. Leostream supports a wide range of authentication methods, with different methods supported for different types of client and workflows.

First, users can log into Leostream using three distinct types of clients:

1. Leostream Connect clients – a software client that runs on Microsoft Windows, Linux, and macOS
2. Leostream Web clients
3. PCoIP (HP Anyware) Zero, Software, or Mobile clients

Second, Leostream supports two types of authentication workflows:

1. Leostream validates the user's credentials, either locally or against external authentication systems
2. A third-party Identity Provider, such as Okta, validates the user's credentials

When using a third-party Identity Provider (IdP), the IdP sends a SAML assertion to the Leostream Connection Broker after the IdP successfully authenticates the user. This authentication workflow is ideal for Zero Trust Architectures because the Connection Broker never holds the user's password and never obtains more information about the user than what you include in the SAML assertion. See the **Leostream Guide on Integration with SAML-based Identify Providers**) for complete instructions.

The remainder of this chapter focuses on workflows where Leostream validates the user's credentials.

When using Leostream to validate credentials - from a Leostream Web client, Leostream Connect, or HP Anyware client login - the Leostream Connection Broker requires a username and password, and optionally requests multi-factor authentication (MFA).

Username and password authentication can be accomplished using:

- Microsoft® Active Directory® (see **Adding Microsoft® Active Directory® Authentication Servers**)
- OpenLDAP™ (see **Adding OpenLDAP Authentication Servers**)
- Credentials stored locally in the Connection Broker (see **Locally Authenticated Users**)

The available MFA options depend on the type of client, as described in the following table.

Client Type	MFA Option
Leostream Connect	1. OTP or Push notice from any IdP that supports the RADIUS protocol 2. Proximity cards used with RF IDeas pcProx card readers (see the **Leostream Connect Administrator Guide**)
HP Anyware Client (any)	OTP or Push notice from any IdP that supports the RADIUS protocol (see **Enabling RADIUS Authentication**)

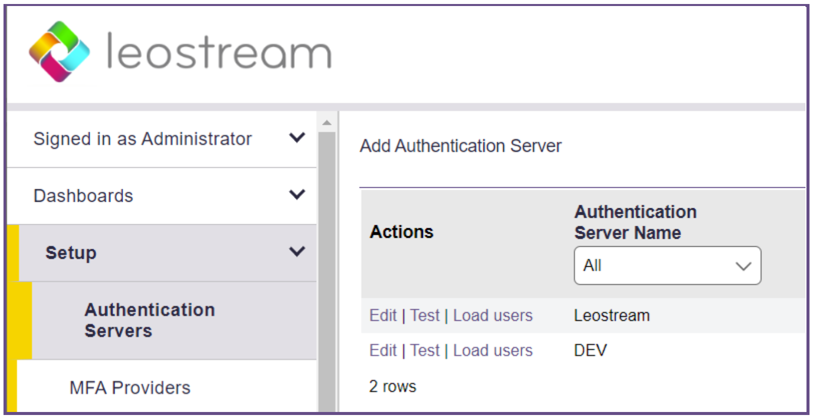
Client Type	MFA Option
Leostream Web client	1. OTP or Push notice from any IdP that supports the RADIUS protocol (see **Enabling RADIUS Authentication**) 2. Duo (see the Leostream Guide on using **Duo MFA for Leostream Logins**)

After a successful authentication, Leostream queries the attributes of the authorized user from the system that verified their username and password. You can use these attributes to assign Leostream policies that control the user’s access to hosted resources.

When using Leostream Connect, the Connection Broker can identify users by reading their smart cards. The smart card is used only for identification and is not validated. Leostream Connect redirects smart cards to the remote desktops for authentication on the remote operating system. See the **Leostream Connect Administrator Guide** for more information.

Configuring Username/Password Authentication

The **> Setup > Authentication Servers** page, lists your third-party username/password and SAML authentication servers, for example:



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

2 rows

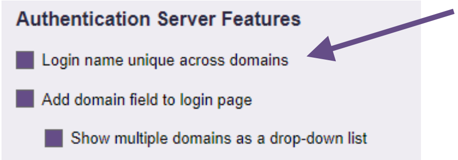
When searching for users in the registered authentication servers, the Connection Broker queries the servers according to their **Position** variable. If the user does not specify their domain, the Connection Broker logs the user into the first domain that authenticates the user. If a user name exists in multiple domains, the Connection Broker can assume that username belongs to the same physical user or to a different user, as described in the following section.

The Connection Broker removes any leading and trailing edge spaces when the user enters their username.

Working with Duplicate Usernames

When multiple domains are defined on the **> Setup > Authentication Servers** page, the Connection Broker can treat a username that exists in more than domains as belonging to a single unique physical user or belonging to multiple distinct physical users. The **Login name unique across domains** option on the **>**

System > Settings page, shown in the following figure, configures this behavior.



Authentication Server Features

■ Login name unique across domains

■ Add domain field to login page

■ Show multiple domains as a drop-down list

1. When this option is selected, the physical user is assumed to be *unique across domains*, indicating that the same username applies to a same physical user across all domains. In this case:

   - The **> Resources > Users** page maintains a single record for each user name. For example, if a user with user name `jsmith` logs into the Development domain on Monday, the Connection Broker creates a record for this user. If, on Tuesday, a user with the username `jsmith` logs into the QA domain, the Connection Broker replaces the original record with this new information.

   - When logging into the Connection Broker, entering or selecting **<Any>** for the domain indicates that the Connection Broker should search for the user in all authentication servers. For first time users, the Connection Broker logs the user into the first authentication server that successfully authenticates the user. For returning users, the Connection Broker checks the authentication server the user first logged into, then searches other authentication servers if the user is not found in their previous authentication server.

2. When this option is *not* selected, the Connection Broker assumes the same username is associated with different physical users on each domain. In this case:

   - The **> Resources > Users** page maintains multiple records for each user name. For example, The Connection Broker creates two records for two users with the same username `jsmith`, logging into two different domains.

   - When logging into the Connection Broker, entering **<None>** for the domain indicates that the Connection Broker should search for a user that was created locally in the Connection Broker. If a local user is not found, the Connection Broker then searches through the remaining authentication servers. The Connection Broker breaks this rule if a fully qualified username, such as UPN, is entered in the username field. In this case, the Connection Broker does not look for a local user; it looks for the user in the appropriate domain.

Adding Microsoft® Active Directory® Authentication Servers

You can add an Active Directory authentication server, as follows:

1. Go to the **> Setup > Authentication Servers** page.

2. Click the **Add Authentication Server** link. The **Add Authentication Server** form opens.

3. Select **Active Directory** from the **Type** drop-down list.

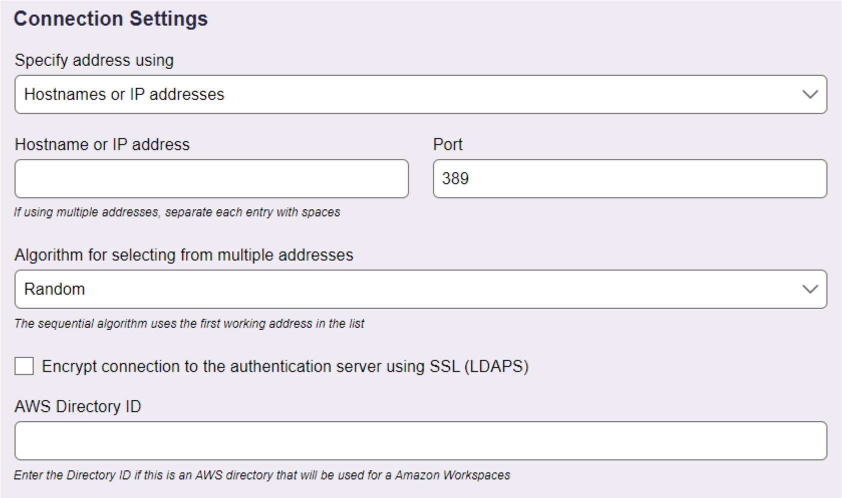
4. In the **Authentication Server name** field, enter a unique name to identify this authentication

server. If this name is not the domain name associated with this authentication server, you must specify the domain name in the **Domain** field, described in step 4.

5. In the **Domain** edit field, enter the domain name associated with this authentication server.

6. Use the **Include domain in drop-down** option to indicate if this domain should be displayed to end users logging in from a client device that includes a **Domain** field. See **Displaying the Domain Field and Setting the Default Domain** for information on setting the default domain.

7. In the **Connection Settings** section, shown in the following figure:



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

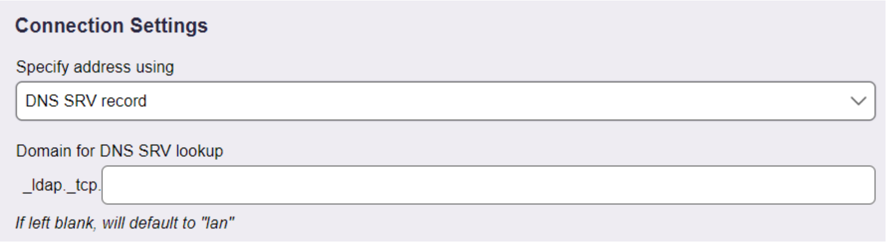
□ Encrypt connection to the authentication server using SSL (LDAPS)

AWS Directory ID:

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

a. From the **Specify address using** drop-down menu, indicate if you are using a DNS SRV record to define the authentication server, or if you are manually entering the server’s address information.

- Select **DNS SRV record** to indicate that the DNS record is defined by the `ldap` SRV record, as shown in the following figure.



Connection Settings

Specify address using: DNS SRV record

Domain for DNS SRV lookup: _ldap._tcp.

If left blank, will default to "lan"

To use the `ldap` SRV record from a specific domain, enter that domain into the **_ldap._tcp** edit field.

The Connection Broker does not query the SRV record at every authentication request. Instead, the Connection Broker honors any TTL value associated with the record, for example, and queries the SRV record only after the TTL expires.

- Select **Hostname or IP addresses** to manually enter the address information.

b. If defining the authentication server using hostnames or IP addresses, enter hostnames or IP addresses in the **Hostname or IP address** edit field. To associate multiple authentication servers with this authentication server record, enter multiple authentication server addresses separated by blank spaces.

c. If defining the authentication server using hostnames or IP addresses, enter the port number into the **Port** edit field. If you entered multiple authentication server addresses in the **Hostname or IP address** edit field, all authentication servers must use the same port.

📝 If you have a multi-domain forest and need to search the global catalog to locate users across domains, you must use the default Global Catalog port. Modify the **Port** field to use 3268 for LDAP and 3269 for LDAPS.

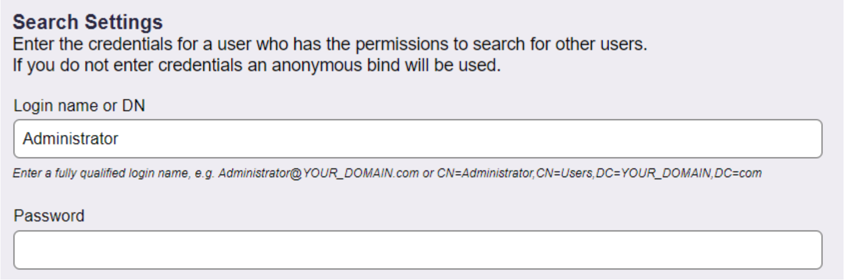
d. Use the **Algorithm for selecting from multiple addresses** drop-down menu to indicate how the Connection Broker selects an address from the list when authenticating a particular user login. Select one of the following options.

- **Random**: The Connection Broker randomly selects an address from the list.
- **Circular / Round Robin**: The Connection Broker uses the addresses in the order they are entered in the **Hostname or IP address** edit field. For example, the first user is authenticated using the first address, the second user is authenticated using the second address, etc. The Connection Broker circles back to the first address in the list after all addresses have been used.
- **Sequential / Failover**: The Connection Broker continues to use the first address in the list until that address can no longer be reached.

e. Click 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. Edit the **Port** edit field if you are not using port 636 for secure connections.

f. Enter in the directory service’s ID in the **AWS Directory ID** field if this is an AWS Directory Service that you plan to use with Amazon WorkSpaces. Otherwise, leave this field blank.

8. In the **Search Settings** section, shown in the following figure, enter the username and password for an account that has read rights to the user records. If you plan to create an Active Directory center, the account requires read rights to computer records, as well.



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

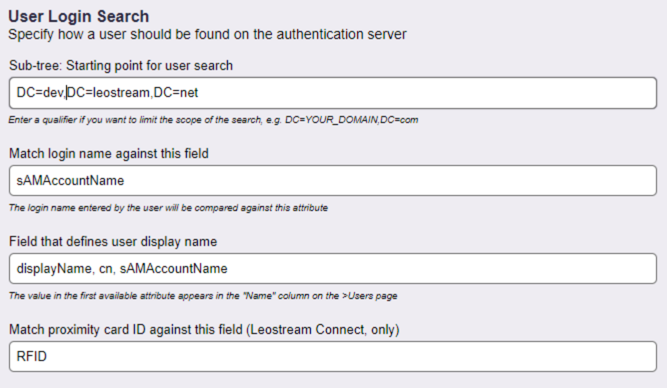
Enter a fully qualified login name, e.g. Administrator@YOUR_DOMAIN.com or CN=Administrator,CN=Users,DC=YOUR_DOMAIN,DC=com

Password

To perform an anonymous bind, leave the **Login** and **Password** fields blank. You must leave both fields blank or the Connection Broker will not save the form.

9. If users log in using PCoIP Zero clients and will authenticate using PIV or CAC smart cards, use the **Smart/PIV Card Authentication** section to prepare the Connection Broker to use this Active Directory authentication server to validate the smart card certificate. See the **Leostream Quick Start Guide for PCoIP Remote Workstation Cards** for complete details.

10. The **User Login Search** section, shown in the following figure, defines where and how the Connection Broker looks for a user in the Active Directory tree.



User Login Search
Specify how a user should be found on the authentication server

Sub-tree: Starting point for user search

DC=dev,DC=leostream,DC=net

Enter a qualifier if you want to limit the scope of the search, e.g. DC=YOUR_DOMAIN,DC=com

Match login name against this field

sAMAccountName

The login name entered by the user will be compared against this attribute

Field that defines user display name

displayName, cn, sAMAccountName

The value in the first available attribute appears in the "Name" column on the >Users page

Match proximity card ID against this field (Leostream Connect, only)

RFID

a. In the **Sub-tree: Starting point for user search** field, enter the fully qualified path in LDAP format to the point on the authentication server tree from which you want the Connection Broker to search for users.

   For example, to configure a search tree that starts at a domain called `leostream.net` enter:

   `DC=leostream, DC=net`

b. In the **Match Login name against this field** edit field, enter the attribute that the Connection Broker should match the user's entered login name against. The default for Active Directory authentication is `sAMAccountName`.

c. In the **Field that defines user display name** edit field, enter one or more authentication server attributes to use as the contents of the **Name** field on the **> Resources > Users** page. Use commas to separate multiple values. The Connection Broker uses the first attribute with a valid entry.

   d. If your users log into the Connection Broker using an RF IDeas proximity card, use the **Match proximity card ID against this field** edit field to indicate the attribute in Active Directory that contains the user’s proximity card ID (see “Chapter 5: Smart Card, Biometric and Proximity Card Support” in the Leostream Connect Administrator’s Guide and End User’s Manual).

11. In the **Other** section, configure any additional options for this authentication server. The settings in this section allow you to do the following:

    a. **Query order**: Sets the **Position** property of this authentication server. The Connection Broker uses the position to determine the order in which it searches for users in your different authentication servers.

    b. **Allow user logins from this authentication server**: Indicates that the Connection Broker should search this authentication server for users.

    c. **Allow unauthenticated logins**: Allows users in this authentication server to log in using only a username. This option appears only if the **Enable the unauthenticated login feature** is select on the **> System > Settings** page.

    d. **Allow users to log in with an expired password**: Allows users with a valid, but expired, password to log into the Connection Broker and be assigned to a desktop. The Windows operating system prompts the user to reset their password.

    e. **Verbose error message for failed login**: When selected, presents the user with a detailed explanation if their login fails.

    You must select **Yes** or **Yes, as default** from the **Include domain in drop-down** menu option for this authentication server to display verbose error messages, even if you are not displaying the **Domain** field on the **Login** dialog.

    f. **Query for LDAP group information**: When creating a new authentication server, this option indicates if the Connection Broker automatically loads the group information from Active Directory. Loading group information can place a significant load on the Connection Broker.

    This option does not appear when you edit an authentication server. To change the setting for the **Query for LDAP group information** option after creating the authentication server, go to the **> Configuration > Assignments** page associated with that authentication server.

    g. **Notes**: Optional notes for this authentication server.

12. Click **Save** to store the authentication server.

At this point, test your authentication server to ensure your setup is complete and accurate. See **Testing the Authentication Server** for more information.

The Connection Broker loads group information from your Active Directory server when you create your authentication server, then stores the groups in local memory. If you make changes to your Active Directory groups while you are logged into Leostream, you must sign out and sign back into the Administrator Web interface to see the new groups on the **> Configuration > Assignments** page.

Adding OpenLDAP Authentication Servers

The Connection Broker can authenticate users from any OpenLDAP™ directory service. Register your OpenLDAP directory service with the Connection Broker, as follows.

1. Go to the **> Setup > Authentication Servers** page
2. Click the **Add Authentication Server** link. The **Add Authentication Server** form opens.
3. Select **OpenLDAP** from the **Type** drop-down list.
4. In the **Authentication server name** edit field, enter a unique name for this authentication server. If this name is not the domain name associated with this authentication server, you must specify the domain name in the **Domain** field, described in step 4.
5. In the **Domain** edit field, enter a name to use for this authentication server.
6. Use the **Include domain in drop-down** option to display this domain to end users logging in from a client device that includes a **Domain** field. See **Populating the Domain Drop-Down and Setting Default Domain** for information on setting the default domain.
7. In the **Connection Settings** section:

    a. From the **Specify address using** drop-down menu, indicate if you are using a DNS SRV record to define the authentication server, or if you are manually entering the server’s address information.

    - Select **DNS SRV record** to indicate that the DNS record is defined by the `ldap` SRV record.

      The Connection Broker does not query the SRV record at every authentication request. Instead, the Connection Broker honors any TTL value associated with the record, for example, and queries the SRV record only after the TTL expires.

    - Select **Hostname or IP addresses** to manually enter the address information.

    b. If defining the authentication server using hostnames or IP addresses, enter hostnames or IP addresses in the **Hostname or IP address** edit field. To associate multiple authentication servers with this authentication server record, enter multiple authentication server addresses separated by blank spaces

    c. If defining the authentication server using hostnames or IP addresses, enter the port number into the **Port** edit field

d. Use the **Algorithm for selecting from multiple addresses** drop-down menu to indicate how the Connection Broker selects an authentication server from the list when authenticating a user login. Select one of the following options.

- **Random**: The Connection Broker randomly selects an address from the list.

- **Circular / Round Robin**: The Connection Broker uses the addresses in the order they are entered in the **Hostname or IP address** edit field. For example, the first user is authenticated using the first address, the second user is authenticated using the second address, etc. The Connection Broker circles back to the first address in the list after all addresses have been used.

- **Sequential / Failover**: The Connection Broker continues to use the first address in the list until that address can no longer be reached.

e. Click 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. Edit the **Port** edit field if you are not using port 636 for secure connections.

6. In the **Search Settings** section, enter the username and password for an account that has read rights to the user records.

   For OpenLDAP, this entry typically takes the form `cn=Manager,dc=`*`myorg`*.

   To perform an anonymous bind, leave the **Login** and **Password** fields blank. You must leave both fields blank or the Connection Broker will not save the form.

7. The **User Login Search** section defines where and how the Connection Broker looks for a user in the OpenLDAP tree.

   a. In the **Sub-tree: Starting point for user search** edit field, enter the fully qualified path in LDAP format to the point on the authentication server tree from which you want the Connection Broker to search for users.

   b. In the **Match Login name against this field** edit field, enter the attribute that the Connection Broker should match the user's entered login name against. For OpenLDAP, the default is `uid`.

   c. In the **Field that defines user display name** edit field, enter one or more authentication server attributes to use as the contents of the **Name** field on the **> Resources > Users** page. Use commas to separate multiple values. The Connection Broker uses the first attribute with a valid entry.

   d. If your users log into the Connection Broker using an RF IDeas proximity card, use the **Match proximity card ID against this field** edit field to indicate the attribute in Active Directory that contains the user's proximity card ID (see "Chapter 5: Smart Card, Biometric and Proximity Card Support" in the Leostream Connect Administrator's Guide and End User's Manual).

8. In the **Other** section, configure any additional options for this authentication server. The settings in this section allow you to do the following:

   a. **Query order**: Sets the **Position** property of this authentication server. The Connection Broker uses the position to determine the order in which it searches for users in your different authentication servers.

   b. **Allow user logins from this authentication server**: Indicates that the Connection Broker should search this authentication server for users.

   c. **Allow unauthenticated logins**: Allows users in this authentication server to log in using only a username. This option appears only if the **Enable the unauthenticated login feature** is select on the **> System > Settings** page.

   d. **Allow login with an expired password**: Allows users with a valid, but expired, password to log in into the Connection Broker and be assigned a desktop. The operating system should be configured to prompt the user to reset their password.

   e. **Verbose error message for failed login**: When selected, presents the user with a detailed explanation if their login fails.

   f. **Notes**: Optional notes for this authentication server.

9. Click **Save** to store the authentication server.

At this point, test your authentication server to ensure your setup is complete and accurate. See **Testing the Authentication Server** for more information.

⚠ OpenLDAP allows you to encrypt users' passwords using DES, MD5, or SHA, or to store the passwords in plain text. You must use MD5 or SHA encryption, or plain text when using OpenLDAP with the Connection Broker. The Connection Broker cannot decrypt passwords encrypted using DES.

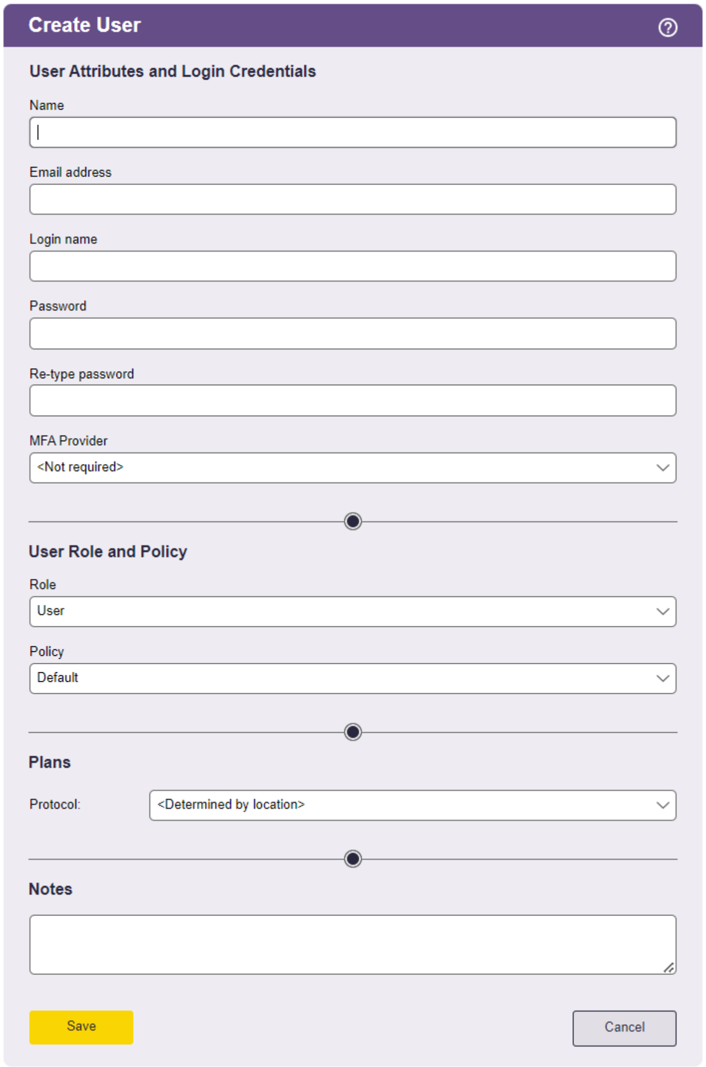
Locally Authenticated Users

To treat the Connection Broker as a local authentication system, manually add users to the **> Resources > Users** page. You can manually add individual users or use the bulk upload method to add multiple users. See **Uploading Users** for information on using CSV-files to upload multiple users.

To manually create individual local users:

1. Go to the **> Resources > Users** page.

2. Click the **Create User** link to open the **Create User** dialog, shown in the following figure.



Name

Email address

Login name

Password

Re-type password

MFA Provider
<Not required>

Role
User

Policy
Default

Protocol: <Determined by location>

3. Enter a **Name** for the new user. This is the value that appears in the **Name** column of the **> Resources > Users** page.

4. Enter an optional **Email address** for the user. Users can subsequently change their email address settings.

5. Enter a **Login name** for the user, using the same format as used for logging into Microsoft Windows® operating systems. The Connection Broker does not treat login names as case sensitive.

6. Enter an initial password for the user in the **Password** and **Re-type password** edit fields. Users can subsequently change their password. Passwords are case sensitive.

7. Indicate if this user requires multifactor authentication by selecting one of the available identify providers in the **MFA Providers** drop-down menu.

8. Select the appropriate **Role** for the user from the drop-down menu. See **Chapter 10: Configuring User Roles and Permissions** for information on creating new roles to customize user access to the

Connection Broker interface. Select **Administrator** to make this user an Administrator.

9. Select the appropriate **Policy** for the user from the drop-down menu.

   After a user is assigned to a policy, if you edit the user and assign a different policy, that policy will not take effect until all jobs scheduled by their original policy are completed or cancelled. For example, if the user's policy schedules a `logout_after_idle` job on the **> System > Job** queue page, the user's existing policy continues to control the user's session and is applied to any subsequent Leostream logins until the logout job completes.

10. To override the protocol plans used in the selected policy, choose a protocol plan from the **Protocol** drop-down menu. See **Which Protocol Plans Applies?** for a description of how the Connection Broker selects the plan to use.

11. Enter any **Notes** to save with the user definition.

12. Click **Save**.

Allowing Logins Without Password Validation

Leostream can identify a user based on their username and skip password validation. This form of Leostream login is called an *unauthenticated login*. In this case, the Connection Broker assigns a policy based on the user attributes associated with the provided username, without validating the user's password.

When using unauthenticated Leostream logins, another system should authenticate the user, such as the operating system within the desktop. Using unauthenticated logins, you can:

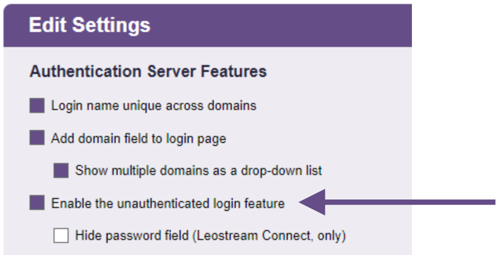
- Hard-code the client, such as Leostream Connect, with the user's username. When the user launches the client, the Connection Broker automatically assigns their policy and connects the user to their desktop for authentication.

- Allow users who have authenticated through an SSL VPN to log into the Connection Broker without having to reenter their credentials.

- Allow users to authenticate using a fingerprint reader or smart card on the desktop, without requiring a password for Leostream.
- Allow users to log into the Connection Broker using their Windows username, but enter Linux credentials on their remote desktop.

To enable unauthenticated logins:

1. Select the **Enable the unauthenticated login feature** on the **> System > Settings** page, shown in the following figure.



Edit Settings

Authentication Server Features

☑ Login name unique across domains

☑ Add domain field to login page

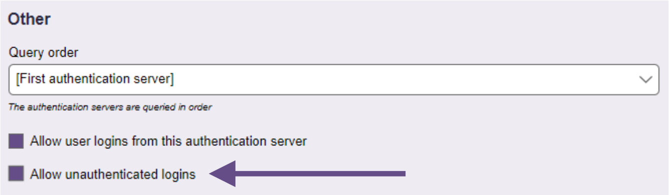
☑ Show multiple domains as a drop-down list

☑ Enable the unauthenticated login feature

□ Hide password field (Leostream Connect, only)

2. If users log in through Leostream Connect, you can select the **Hide password field** option to remove the **Password** field from the **Login** dialog, making it clear to end users that a password is not required.

3. To indicate which authentication servers allow unauthenticated logins, go to the **> Setup > Authentication Servers** page and edit the appropriate authentication servers. At the bottom of the **Edit Authentication Server** form, select the **Allow unauthenticated logins** option near the bottom of the form, shown in the following figure.



Other

Query order

[First authentication server]

The authentication servers are queried in order

☑ Allow user logins from this authentication server

☑ Allow unauthenticated logins

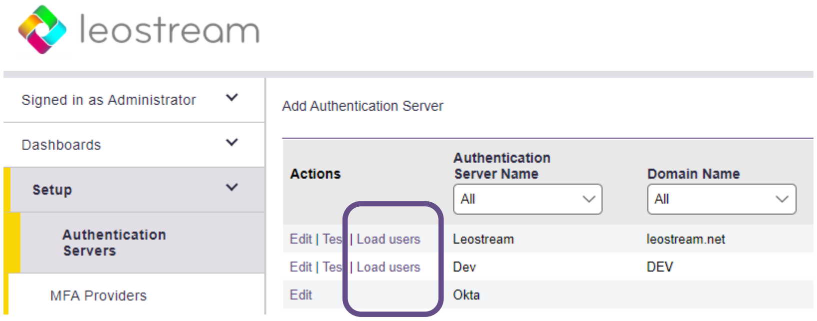
If you select the **Allow unauthenticated logins** option and your user enters a password, the Connection Broker validates the password. If the user enters an invalid password, the Connection Broker rejects the login. Users must enter either a valid password or leave the password blank.

Loading Users

Users appear on the **> Resources > Users** page the first time they log into Leostream. Therefore, in most circumstances, you do not need to load users before they start logging in. The exception is if you need to hard-assign users to desktops before they log in.

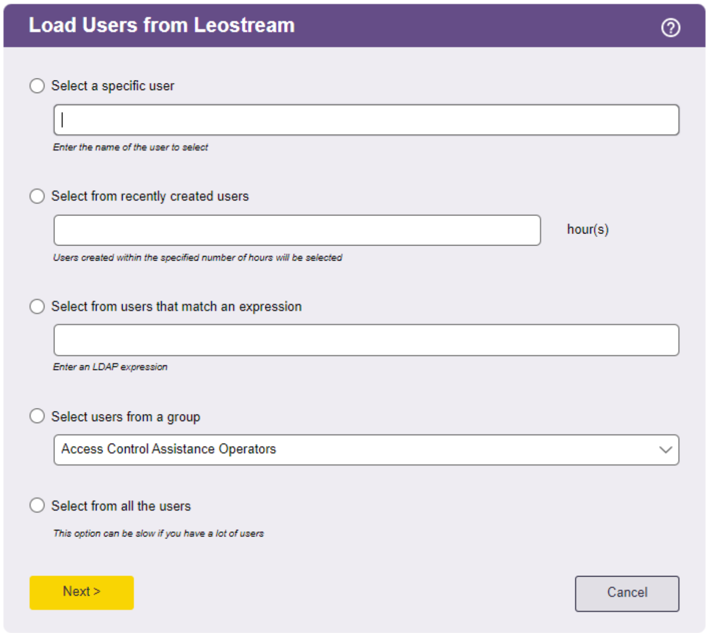
You can load users from an authentication server using the **Load users** action, as follows:

1. Select the **Load users** action for the appropriate authentication server on the **> Setup > Authentication Servers** page, as shown in the following figure.



Actions	Authentication Server Name	Domain Name
	All	All
Edit | Tes | Load users	Leostream	leostream.net
Edit | Tes | Load users	Dev	DEV
Edit	Okta	

2. In the **Load Users from** form that opens, shown in the following figure, define the scope to choose from when selecting users to load.



Load Users from Leostream

○ Select a specific user

Enter the name of the user to select

○ Select from recently created users

hour(s)

Users created within the specified number of hours will be selected

○ Select from users that match an expression

Enter an LDAP expression

○ Select users from a group

Access Control Assistance Operators

○ Select from all the users

This option can be slow if you have a lot of users

Select one of the following options and configure the search scope, as follows.

- **Select a specific user**: Enter the username for the user you want to load. The Connection Broker looks for user records with usernames that exactly match the name entered in this field. The format of the username is defined by the setting of the **Match Login name against this field** edit field in the authentication server.

- **Select from recently created users**: Enter a number, in hours. The Connection Broker looks for user records that were created anywhere in the range from the present time back to the indicated number of hours ago.

- **Select from users that match an expression**: Enter an LDAP expression. The Connection Broker looks for user records that satisfy the LDAP expression.

- **Select users from a group**: If the authentication server has the **Query for group information** option selected, select the group to load users from. The Connection Broker displays only users in this group.

- **Select from all the users**: Select this option to select from all users in the authentication server.

3. Click **Next >**.

4. In the dialog that opens select the users to import from the **Available users** list at the left.

5. Click the **Add item** link to add the users to the **Selected users** list.

6. Click **Save**.

The selected users are loaded into the **> Resources > Users** page. To load additional users from this authentication server, click the **Load more users** link.

Displaying the Domain Field and Setting the Default Domain

The appearance of the **Domain** field on Leostream Connect and the Leostream Web client depends on the following settings in the Connection Broker.

- To include the **Domain** field on the login screen, select the **Add domain field to login page** option in the **Authentication Server Features** section of the **> System > Settings** page.

- By default, the **Domain** field is an edit field. To convert the edit field to a drop-down menu, select the **Show domain as drop-down** option in the **Authentication Server Features** section of the **> System > Settings** page.

  If you have a single authentication server, the **Domain** field remains an edit field, even if you select the **Show domain as drop-down** option.

When showing the domain field as a drop-down menu, you must select which authentication servers appear in the drop-down menu and specify the default domain value. Use the **Include domain in drop-down** option on the **Edit Authentication Server** page to configure the contents of the **Domain** drop-down menu, as follows.

- Select **No** if you do not want to include the authentication server in the **Domain** drop-down menu.

- Select **Yes** if you want to include the authentication server in the **Domain** drop-down menu, but do not want to set this authentication server as the default.

- Select **Yes, as default** if you want to include the authentication server in the **Domain** drop-down menu and set this authentication server as the default.

The default domain value is used the first time any user logs in at a client device. Leostream Connect and the Leostream Web client cache any subsequent domain selection and display that domain value the next time any user launches the client.

If the **Domain** field is not shown as a drop-down menu, the domain that selects **Yes, as default** from the **Include domain in drop-down** option is shown in the **Domain** edit field.

The **Domain** drop-down menu contains only the authentication servers that have **Yes** or **Yes, as default** selected in the **Include in drop-down menu** option. The **Domain** menu also contains an additional option that depends on the setting for the **Login name unique across domains** option.

- If the **Login name unique across domains** option is *not* selected, the **Domain** drop-down menu contains a **<None>** option. Selecting **<None>** instructs the Connection Broker to authenticate users only if they are defined locally in the Connection Broker.

- If the **Login name unique across domains** option *is* selected, the **Domain** drop-down menu contains an **<Any>** option. Selecting **<Any>** instructs the Connection Broker to search through all the authentication servers in the order of their priority.

See **Unique Versus Non-Unique User Identification** for more information on using the **Login name unique across domains** option.

Testing the Authentication Server

After you create the authentication server, test it using the **Test** action associated with the server.

In the **Test User** Login form, enter the name and, optionally, password of a user in the authentication server and click **Authenticate**. The Connection Broker queries the authentication server and presents the user’s information. The user’s role and policy are shown at the bottom of the report.

If the Connection Broker cannot bind with the authentication server, it displays the associated LDAP bind error. The following table describes some common bind errors.

Code	Definition	Notes
525	User not found	The specified username is invalid
52e	Invalid credentials	The username is valid however the password is not correct
530	Not permitted to logon at this time	The username and password are valid however the account is restricted from logging in at this time of day
532	Password expired	The username and password are valid however the password has expired
533	Account disabled	The username and password are valid however the account is currently disabled
701	Account expired	The username and password are valid however the account has expired
733	User must reset password	The username and password are valid however the password must be reset before they can log in
755	Account locked	The username and password are valid however the account is locked

If the Connection Broker can bind with the authentication server but displays the error `LDAP Error: Unable to locate the user`, first ensure that you correctly entered the username for the test. If the username is correct, check the permissions for the account used to create the authentication server in your Connection Broker. The account must have at least Read permissions for user objects in the authentication server.

For example, in Active Directory, check the *access control list* (ACL) for the Users group, as follows.

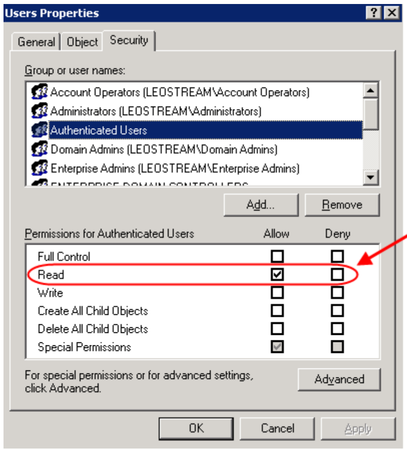
1. In the **Active Directory Users and Computers** dialog, right-click on the **Users** node in the console tree.

2. Select **Properties** from the right-click menu.

3. In the **Users Properties** dialog, go to the **Security** tab.

4. Ensure that the account you entered when defining your Authentication Server in the Connection Broker is part of a group included in the **Group and user names** list. If the user does not fall into any of the groups in this list, you must add the necessary group, or individual user, to this list.

5. After an appropriate group or user is included in the **Group and user names** list, check the **Permissions** list to ensure that this user has Read permissions for users, as shown in the following figure.



Group or user names:

- Account Operators (LEOSTREAM\Account Operators)
- Administrators (LEOSTREAM\Administrators)
- Authenticated Users
- Domain Admins (LEOSTREAM\Domain Admins)
- Enterprise Admins (LEOSTREAM\Enterprise Admins)

Permissions for Authenticated Users	Allow	Deny
Full Control	□	□
Read	☑	□
Write	□	□
Create All Child Objects	□	□
Delete All Child Objects	□	□
Special Permissions	☑	□

For special permissions or for advanced settings, click Advanced.

If the user has Read permissions in this list, check the Special Permissions (by clicking the **Advanced**) button to ensure that the account does not inherit a Deny permission.

If your authentication server account does not have, or is explicitly denied, read permissions for users, the Connection Broker successfully binds with the authentication server, but displays the `LDAP Error: Unable to locate the user` error. The following article provides a summary on checking and setting Active Directory permissions:

`http://www.tech-faq.com/active-directory-objects.shtml`

Using RADIUS Servers for MFA

Leostream can communicate with RADIUS servers to enable multi-factor authentication (MFA) for your end-user logins. Any RADIUS server or Identity Provider with a RADIUS component or agent, such as Okta and Duo, can be used with Leostream to request push notifications or one-time passcodes.

RADIUS MFA is supported when users log into Leostream using any of the following client devices.

- The Leostream Web client
- Leostream Connect for Windows
- Leostream Connect for Linux and macOS
- PCoIP Zero clients
- HP Anyware Software clients

For a complete description of using RADIUS Servers for MFA, see the Leostream Guide for **Using RADIUS Servers for MFA with Leostream.**

Managing Users

The Connection Broker maintains a list of all users currently managed by the Connection Broker. The database contains one pre-configured user called **Administrator**, with a login name **admin**, password **leo**, and **Administrator** role. Additional users appear in the Connection Broker in one of the following ways:

1. The Connection Broker automatically enters users into the database the first time they sign in.
2. You can manually enter individual users into the database (see **Locally Authenticated Users**).
3. You can upload users from a CSV-file (see **Uploading Users**).
4. You can load users from external authentication servers, including Microsoft® Active Directory® and OpenLDAP™ servers (see **Loading Users**).

Displaying User Characteristics

The **> Resources > Users** page lists all users entered into the Connection Broker database. You can modify the order and type of characteristics displayed on this page by clicking the **Customize columns** link at the top-right side of the page (see **Customizing Tables**).

The following sections describe the available user characteristics.

Bulk actions
Checkboxes that allow you to select multiple users for performing a batch process; currently, only **Remove** (see **Removing Multiple Users**).

Actions
Drop-down menu or list of links indicating the actions you can perform on a user. Available actions include:

- **Edit**: Open the **Edit User** form for this user.

- **Sign out**: Log the user out of a desktop session, if any active sessions exist. See **Logging Users Out** for more information.

- **Test Login**: Determine the role, policy, and desktop assignment that will be used when this user logs in. See **Testing User Role and Policy Assignment** for more information.

Name
The user's name as entered in the **Name** field on the **Edit User** page.

Login name
The name used to authenticate the user against the authentication server when they log in.

Email
The user's email address.

Signed in
Indicates when the user last signed into a desktop via the Connection Broker. If the user never signed in, this field is empty.

Current Desktops
The desktops currently assigned to the user.

Role
The user's role.

Policy
The user's policy.

Protocol Plan Override
The user's protocol plan, if specified. The user's protocol plan overrides any protocol plan set by the user's policy or by the location of the user's client device.

Authentication Server
The authentication server used to authenticate the user and assign their role and policy.

AD distinguished Name
The user's Active Directory distinguished name.

AD Email
The user's Active Directory email address.

AD userPrincipalName
The user's Active Directory UPN name.

AD CN
The user's Active Directory CN name.

AD sAMAccountName
The user's Active Directory sAMAccount name.

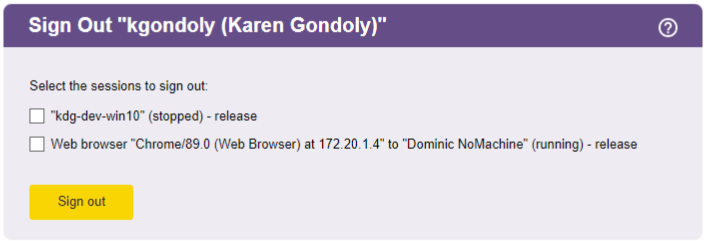
Client/IP Address
The client name and/or IP address the user last logged in from.

Client Location
The client location associated with the user's last login.

Uploaded
Indicates if the user was uploaded using the bulk upload option on the **> System > Maintenance** page.

Logging Users Out

Select the **Sign out** action associated with a user to see a list of their currently assigned desktops. For example, in the following figure the user is assigned to two desktops.



Sign Out "kgondoly (Karen Gondoly)"

Select the sessions to sign out:

□ "kdg-dev-win10" (stopped) - release

□ Web browser "Chrome/89.0 (Web Browser) at 172.20.1.4" to "Dominic NoMachine" (running) - release

To release or release-and-logout the user, check the box for that desktop and click **Sign out**. The results are shown at the top of the **> Resources > Users** page.

After the Connection Broker unassigns the machine from the user, it runs the **When Desktop is Released** section of the user's Release and Power Control plans. Because the user has already been logged out, the **When user Logs Out of Desktop** section of the plans are not invoked.

Removing Multiple Users

If your Connection Broker is licensed by active users, removing users from the **> Resources > Users** page releases licenses for new users. You can simultaneously remove multiple users, as follows.

1. Go to the **> Resources > Users** page.

2. Check the box associated with every user to remove. If check boxes do not appear in your **> Resources > Users** table, customize the table so the **Bulk action** column appears (see **Customizing Tables**).

3. Select **Remove** from the **Bulk action** drop-down menu at the top of the table.

4. Click **OK** in the confirmation window that appears.

Editing User Characteristics

You can edit a subset of the user's characteristics by selecting the **Edit** action for that user.

The **Edit User** form displays the following user characteristics:

- **Name**: Enter the name to display in the **Name** column on the **> Resources > Users** page. For Active Directory users, this value defaults to the user's `displayName` attribute. This is not the same as the user's login name.

- **Email address**: Enter the user's email address.

- **Login name/Password**: Enter the username and password for this user. These fields are only editable if you manually created this user. Otherwise, the Connection Broker displays the username, and indicates what authentication server is used to authenticate the user.

- **HID proximity number**: If users log in with a proximity card, this field displays the HID number associated with their card. You cannot edit this number. If the user is issued a new proximity card, select the **Clear the HID proximity number** checkbox and save the form to enroll the new HID.

- **Role/Policy**: Select the role and policy to assign to this user. These fields are only available if you manually created this user. Otherwise, the authentication server determines the role and policy.

  Users and administrators that are signed into the Connection Broker cannot edit their own role.

- **Protocol**: Select the protocol plan to assign to this user. If a user has a specified protocol plan, that protocol plan is always used, and overrides any protocol plans specified by the user's policy or by the location of the user's client device.

Chapter 6: Connecting to your Hosting Platforms

Overview

Leostream defines centers as the external, third-party platforms that host your desktops. The Connection Broker uses the hosting platform's native APIs to inventory desktops available for assignment to end users, as well as to provision and delete desktops based on demand. You can create centers for any of the following platforms.

- **VMware®** and **Red Hat Virtualization** hosts
- **OpenStack**, **Amazon Web Services,** **Microsoft Azure**, and Google Cloud Platform clouds
- Amazon WorkSpaces Core
- **Nutanix AHV** clusters
- **VergeIO** Virtualization Software
- **Scale Computing Platform** clusters
- **Microsoft Windows Remote Desktop Services** servers or **multi-user Linux** servers
- **Microsoft Active Directory®** services
- **HPE Moonshot Systems**
- **PCoIP** Remote Workstation cards
- **Printers** registered in an Active Directory service

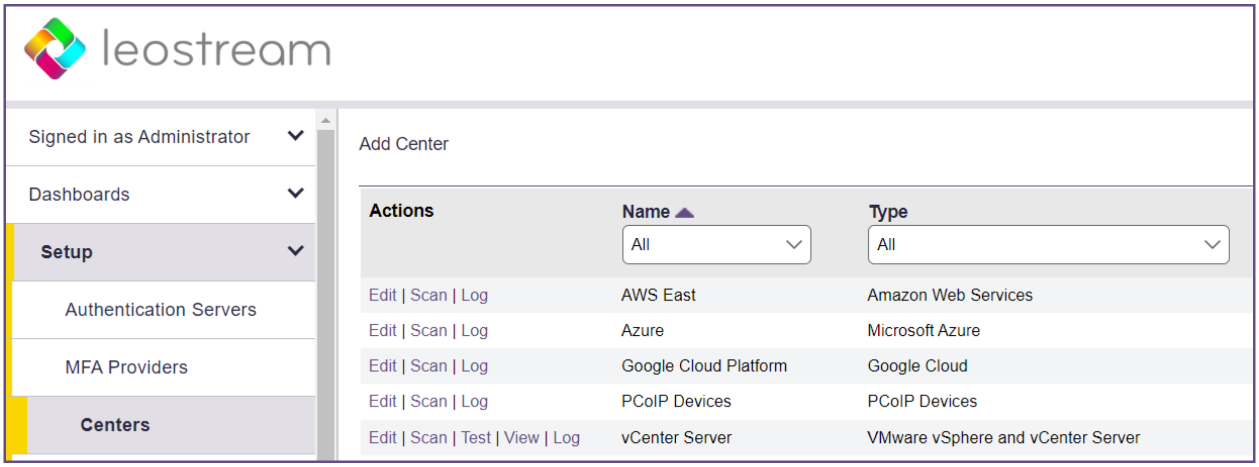
Your Leostream license determines which center types you can create. Contract **sales@leostream.com** if you need to create a center type that is not listed in your Connection Broker.

If you use a hosting platform that the Connection Broker does not integrate with using the platform's APIs, you can manually register the desktops in that platform with the Connection Broker, in two ways:

- By installing a Leostream Agent
- By manually creating a desktop record (see **Registering a Desktop by IP Address**)

Manually registered desktops are placed in the **Uncategorized Desktops** center. See **Chapter 7: Working with Desktops** for information on manually registering desktops. The remainder of Chapter 6 focuses on creating resource centers.

The **> Setup > Centers** page, shown in the following figure, provides a summary of all hosting platforms registered with the Connection Broker.



Actions	Name	Type
	All	All
Edit | Scan | Log	AWS East	Amazon Web Services
Edit | Scan | Log	Azure	Microsoft Azure
Edit | Scan | Log	Google Cloud Platform	Google Cloud
Edit | Scan | Log	PCoIP Devices	PCoIP Devices
Edit | Scan | Test | View | Log	vCenter Server	VMware vSphere and vCenter Server

After you add a center, you can view the imported resources on one of the following pages:

- The **> Resources > Desktops** page lists the desktops imported from all centers, including physical machines, virtual machines, cloud-hosted machines and Amazon WorkSpaces. Use the **Centers** column in the desktop table to see which center each desktop originated in. See **Using the Desktops Page** for more information on displaying desktops.

- The **> Resources > Images** page lists all the templates, AMIs, etc., inventoried from all your centers. These images are available when provisioning new desktops in Leostream pools or to launch individual Amazon WorkSpaces.

- The **> Resources > Printers** page lists all the printers imported from the **Printer Repository** center or manually entered in the Connection Broker. See **Attaching Network Printers** for information on using the Connection Broker to manage and assign printers.

- The **> Resources > PCoIP Host Devices** page lists all PCoIP Remote Workstation cards installed in remote workstations. This page is available only when your Leostream license enables PCoIP connections. See the **Leostream Quick Start for PCoIP Remote Workstation Cards** for more information.

Creating Centers

Active Directory Centers

The Connection Broker uses Active Directory to manage physical and virtual machines that are part of your domain. After you add an Active Directory authentication server to the Connection Broker (see **Adding Microsoft® Active Directory® Authentication Servers**), you can add the machines associated with that domain into the Connection Broker inventory.

⚠ You must add an Active Directory authentication server before you can add an Active Directory center.

To add an Active Directory center:

1. Go to the **> Setup > Centers** page.

2. Click **Add Center**. The **Add Center** form opens.

3. Select **Active Directory** from the **Type** drop-down menu.

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

5. Select an authentication server from the **Authentication Server** drop-down menu. This drop-down menu contains the Active Directory centers you entered in the **> Setup > Authentication Servers** page. See **Adding Microsoft® Active Directory® Authentication Servers** for instructions on adding an authentication server.

6. In the **Sub-tree** edit field, specify the sub-tree within Active Directory that contains the computer records. If you do not specify a sub-tree, the Connection Broker assumes the same sub-tree starting point as specified in the Active Directory authentication server selected in step 3.

   📝You can begin the search at a node higher up the search tree than what is specified in the Active Directory authentication server.

7. Enter an optional filter expression in the **Advanced filter expression** edit field. See the example in **Determining Appropriate Sub-Tree Strings** for more information.

8. Select the **Inventory scan interval**. This setting tells the Connection Broker how often to query the center for information on existing or new desktops in this center. The refresh interval is the length of time between when one refresh action completes and the next refresh action begins.

9. Select the **Power state scan interval**. During a power state scan, the Connection Broker uses the Nmap command to probe the ports associated with all display protocols used in your protocol plans and a set of common third-party ports. If any of the scanned ports are open, the Connection Broker marks the desktop as **Running**. If all ports are closed, the Connection Broker marks the desktop as **Stopped**.

   📝 Please contact **support@leostream.com** for a full list of the ports included in a power state scan.

   To limit the number of ports that the Connection Broker probes during a power state refresh, ensure that all protocol plans, including the Default protocol plan, select **Do not use** for the priority unused protocols you do not plan to offer to users.

10. Uncheck the **Offer desktops from this center** option if the Connection Broker should not offer desktops from this center when users log in. The Connection Broker continues to offer assigned desktops in this center to the assigned user, even when this option is not selected.

11. Select **Assign rogue users to desktops from this center (requires Agent)** if you want the Connection Broker to manage users that log into desktops in this center when they do not log in through Leostream. The desktop must have a running Leostream Agent, which informs the Connection Broker of user logins (see **Assigning Desktops to Rogue Users**).

12. Select the **Initialize newly-discovered desktops as "unavailable"** option if the Connection Broker should mark desktops as unavailable as they are discovered. Otherwise, leave this option unchecked.

    You can manually mark any **Unavailable** desktop as **Available** using the **Availability** drop-down menu on the desktop's **Edit Desktop** page. To access the **Edit Desktop** page, go to the **> Resources > Desktops** page and select the **Edit** action associated with that desktop.

13. Select the **Continuously apply any Auto-Tags** option if you want to set tags on desktops that are discovered when the center is refreshed (see **Continuously Applying Tags to Desktops** for more information). Leave this option unchecked if you do not want to tag desktops.

14. Select the **Resolve addresses in this center using short hostnames** option to instruct the Connection Broker to reference the desktop using only the portion of the hostname before the first dot.

15. Click **Save**.

⚠ The Connection Broker registers a desktop in a single Active Directory center. If you create multiple Active Directory centers and each contains a desktop record, that desktop is a member of the first center you created. Therefore, if you create pools based on your Active Directory centers, the desktop appears in only one pool.

Determining Appropriate Sub-Tree Strings

You can use the `ldp.exe` tool to determine an appropriate sub-tree string. A typical string takes the form:

```
CN=Computers,DC=leostream,DC=net
```

Where `CN=Computers` narrows the search down to computers, as opposed to users. If you include the user string `CN=Users`, the Connection Broker does not find any computers.

To group machines, place them in an Active Directory group and specify the group in the sub-tree string. For example, if you have two pools of machines, Red and Blue, define one group using the string;

```
CN=Computers,DC=leostream,DC=net,CN=Red
```

To add the second Blue group of machines, use `CN=Blue` instead of `CN=Red`.

Use the **Advanced filter** expression to narrow down the selection of desktops from the Active Directory tree. The default expression is `&(objectclass=Computer)`. You can override the default with a more complex Microsoft SQL Server® search command that, for example, searches only for computers whose `cn` value start with `a` or `b`, as shown by the following line:

```
(&(objectCategory=computer) (objectClass=computer)(|(cn=a*)(cn=b*)))
```

Refer to the Microsoft **sample scripts** for searching Active Directory services for more information.

Amazon Web Services EC2 Centers

The Connection Broker can inventory the instances and images in your AWS account, and manage provisioning and terminating instances based on the pool, policy, and plan settings in your Connection Broker.

To manage connections to AWS instances, create an Amazon Web Services center, as follows.

1. Go to the **> Setup > Centers** page.
2. Click on **Add Center**. The **Add Center** form opens.
3. Select **Amazon Web Services** from the **Type** drop-down menu.
4. Enter a name for the center in the **Name** edit field.
5. Select the AWS region you want to manage from the **Region** drop-down menu. Create separate centers for each region you want to manage in the Connection Broker.
6. If your Connection Broker is installed on an AWS EC2 instance, you can use the **Authentication** drop-down menu to indicate how the Connection Broker authenticates against the AWS API.

   Select **Use attached IAM role** if your Connection Broker EC2 instance has an attached IAM role with appropriate permissions.

   The `heartbeat` work queue job queries for attached IAM roles. If you recently attached a new IAM role to your Connection Broker, it is discovered when the next `heartbeat` job runs.

   If you do not have an attached IAM role, select **Enter IAM Access Key** and enter the following information. If your Connection Broker is not installed in EC2, the **Authentication** drop-down menu is not available and you must specify the **Access Key ID** and **Secret Access Key**, as follows.

   a. Enter your AWS access key into the **Access Key ID** edit field. You can create an IAM user to use with Leostream. Ensure that user has sufficient privileges to access EC2.

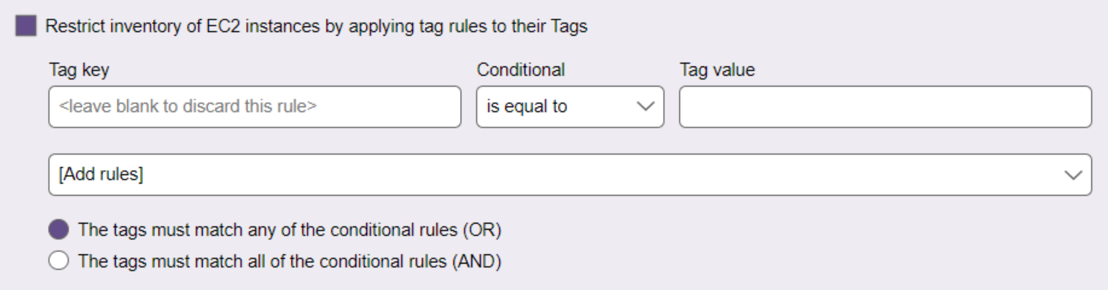
   b. Enter the secret key associated with your access key into the **Secret Access Key** field.

      See the **Leostream Quick Start for AWS** for a list of EC2 permissions required for the IAM user associated with the entered Access keys.

7. If access to your AWS account must go through a proxy server, specify its address in the **Proxy Address (optional)** edit field.

8. Select a time from the **Inventory scan interval** drop-down menu. This setting tells the Connection Broker how often to refresh the desktops imported from this center. The scan interval is the length of time between when one refresh action completes and the next refresh action begins.

9. By default, the Connection Broker inventories all instances in your selected Region. To limit the inventoried instances based on AWS Tags, select the **Restrict inventory of EC2 instances by applying tag rules to their Tags** checkbox, as shown in the following figure.



☑ Restrict inventory of EC2 instances by applying tag rules to their Tags

Tag key	Conditional	Tag value
<leave blank to discard this rule>	is equal to	

[Add rules]

● The tags must match any of the conditional rules (OR)
○ The tags must match all of the conditional rules (AND)

Use the **Tag key**, **Conditional**, and **Tag value** fields to build rules that filter the instances that are inventoried out of your AWS region. To make rules for multiple tag values, use the **[Add rules]** drop-down menu to add rows to the table.

Note that the radio buttons below the table indicate if multiple rules are combined using AND or OR logic. Use OR logic to inventory all of the instances that match any of the configured tag rules. Use AND logic to inventory only the instances that satisfy all of the tag rules.

10. Uncheck the **Offer desktops from this center** option if the Connection Broker should not offer desktops from this center to users who log into the Connection Broker. The Connection Broker continues to offer assigned desktops to the assigned user, even when this option is not selected.

11. Select **Assign rogue users to desktops from this center (requires Agent)** to have Leostream assign users to desktops in this center when the user connects to the desktop from a non-Leostream client, such as mstsc.exe or the HP ZCentral Remote Boost Receiver. The desktop must have a running Leostream Agent, which informs the Connection Broker of user logins (see **Assigning Desktops to Rogue Users**).

12. Select the **Initialize newly-discovered desktops as "unavailable"** option if the Connection Broker should mark desktops as unavailable as they are discovered. Otherwise, leave this option unchecked.

    You can manually mark any **Unavailable** desktop as **Available** using the **Availability** drop-down menu on the desktop's **Edit Desktop** page. To access the **Edit Desktop** page, go to the **> Resources > Desktops** page and select the **Edit** action associated with that desktop.

13. If you plan to use the Connection Broker to manage capacity in AWS and allow Leostream to delete virtual machines that are already provisioned, select the **Initialize newly-discovered desktops as "deletable"** option. If a VM is marked as deletable, you can use Leostream Release Plans to delete the VM from disk after the user is released from the desktop.

If you do not plan to use Release Plans to delete your virtual machines, do not mark desktops as deleteable.

14. Select the **Continuously apply any Auto-Tags** option if you want to set tags on desktops that are discovered when the center is refreshed (see **Continuously Applying Tags to Desktops** for more information). Leave this option unchecked if you do not want to tag desktops.

15. The **Complete System Status checks before marking desktops "Running"** and **Complete Instance Status checks before marking desktops "Running"** options allow you to control if the Connection Broker waits for all EC2 status checks to complete when powering up an instance in AWS before connecting users to that instance. Unchecking one or both of these options may allow users to connect to their machines faster, however the Connection Broker cannot guarantee that the instance is healthy until both status checks complete.

    For more information on status checks for your AWS instance, see the **AWS EC2 documentation**.

16. Click **Save**.

After you create an AWS center, you can view the available instances on the **> Resources > Desktops** page. The Connection Broker displays the AMIs available in the region on the **> Resources > Images** page. These images can be used to provision new desktops in pools (see **Provisioning in Amazon Web Services**).

Amazon WorkSpaces Core Centers

In order to manage WorkSpaces instances, you create an Amazon WorkSpaces center in your Leostream Connection Broker.

Leostream defines ***centers*** as the external systems that inform the Connection Broker about desktops and other resources that are available for assignment to end users.

1. Go to the **> Setup > Centers** page.

2. Click the **Add Center** link.

3. In the **Add Center** form, select **Amazon WorkSpaces** from the **Type** drop-down menu.

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

5. Select the AWS Directory Services associated with this WorkSpaces account from the **Authentication Server** drop-down menu. Create separate centers for each region and Directory Services that you want to manage in Leostream.

6. If your Connection Broker is installed on an AWS EC2 instance, you can use the **Authentication** drop-down menu to indicate how the Connection Broker authenticates against the AWS API. Currently, to manage Amazon WorkSpaces, you must select **Enter IAM Access Key** and enter the following information.

a. Enter your AWS access key into the **Access Key ID** edit field. You can create an IAM user to use with Leostream. Ensure that user has sufficient privileges to access EC2.

b. Enter the secret key associated with your access key into the **Secret Access Key** field.

7. Click **Save** to create the center.

All WorkSpaces associated with the selected Directory Services appear on the **> Resources** > **Desktops** page. Your custom bundles available for provisioning new WorkSpaces appear on the **> Resources > Images** page.

For a detailed description of you to use Leostream to manage Amazon WorkSpaces Core, see the Leostream **Quick Start Guide for Amazon WorkSpaces Core**.

Google Cloud Platform Centers

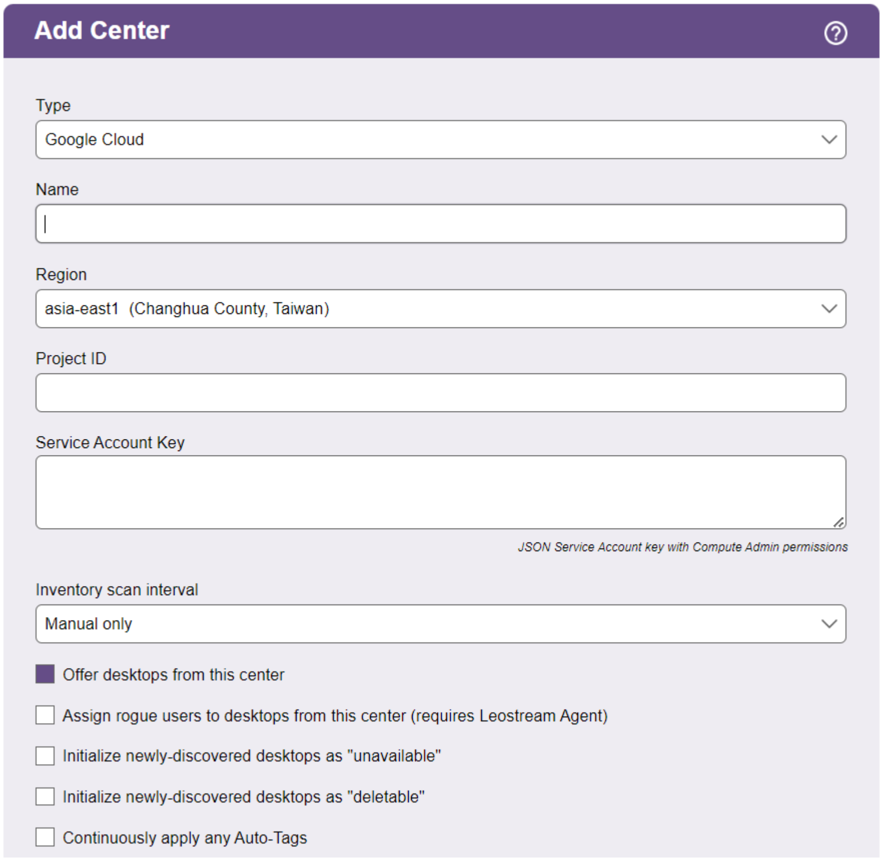
A Google Cloud Platform center allows you to inventory, power control, assign, and connect users to virtual machines hosted in a Google Cloud Platform region.

To add a Google Cloud Platform center:

1. Go to the **> Setup > Centers** page.

2. Click on **Add Center**. The **Add Center** form opens.

3. Select **Google Cloud** from the **Type** drop-down menu. The form updates as shown in the following figure.



Add Center

Type

Google Cloud

Name

Region

asia-east1 (Changhua County, Taiwan)

Project ID

Service Account Key

JSON Service Account key with Compute Admin permissions

Inventory scan interval

Manual only

☑ Offer desktops from this center

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

□ Initialize newly-discovered desktops as "unavailable"

□ Initialize newly-discovered desktops as "deletable"

□ Continuously apply any Auto-Tags

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

5. Select the region for this center from the **Region** drop-down menu.

6. Enter your project ID in the **Project ID** edit field. You can find your project ID in the **Project info** pane of the Google Cloud Platform Dashboard.

7. In the **Service Account Key** field, enter the service account key for a service account user in Google Cloud Platform with permission to execute the Google Cloud Platform APIs. This must be a JSON service account key with compute administrator permissions. Instructions for obtaining this key can be found in **Obtaining a Service Account Key for Google Cloud Platform**.

8. Select a time from the **Inventory scan interval** drop-down menu. This setting tells the Connection Broker how often to refresh the desktops imported from this center. The scan interval is the length of time between when one refresh action completes and the next refresh action begins.

9. Uncheck the **Offer desktops from this center** option if the Connection Broker should not offer desktops from this center to users who log into the Connection Broker. The Connection Broker continues to offer assigned desktops to the assigned user, even when this option is not selected.

10. Select **Assign rogue users to desktops from this center (requires Agent)** if you want the Connection Broker to manage users that log into desktops in this center when they do not log in through Leostream. The desktop must have a running Leostream Agent, which informs the Connection

Broker of user logins (see **Assigning Desktops to Rogue Users**).

11. Select the **Initialize newly-discovered desktops as "unavailable"** option if the Connection Broker should mark desktops as unavailable as they are discovered. Otherwise, leave this option unchecked.

    You can manually mark any **Unavailable** desktop as **Available** using the **Availability** drop-down menu on the desktop's **Edit Desktop** page. To access the **Edit Desktop** page, go to the **> Resources > Desktops** page and select the **Edit** action associated with that desktop.

12. If you plan to use the Connection Broker to manage capacity in Google Cloud Platform, and allow Leostream to delete virtual machines that are already provisioned, select the **Initialize newly-discovered desktops as "deletable"** option. If a VM is marked as deletable, you can use Leostream Release Plans to delete the VM from disk after the user is released from the desktop.

13. Select the **Continuously apply any Auto-Tags** option if you want to set tags on desktops that are discovered when the center is refreshed (see **Continuously Applying Tags to Desktops** for more information). Leave this option unchecked if you do not want to tag desktops.

14. Click **Save**.

Obtaining a Service Account Key for Google Cloud Platform

To create a service account with the required permissions for your Leostream center, log into your Google Cloud Platform console.

1. From the home dashboard, hover over **IAM & admin** and select **Service accounts**.
2. Click **Create Service Account** at the top.
3. In the **Service account details** form, enter a name, ID, and description for the account you are creating and click **Create**.
4. In the **Service account permissions** form, click the drop-down to **Select a role**.
    a. In the list on the left, find and select to **Compute Engine**.
    b. In the list on the right, select **Compute Admin** and click **Continue**.
5. In the **Grant user access to this service account** form, click the **Create Key** button in the **Create key** section.
    a. Select the **JSON** option and click **Create**.
    b. Save the downloaded .json file to a secure location. You will use the contents of the file when creating your Google Cloud Platform center in Leostream.

HPE Moonshot System Centers

The Connection Broker manages HPE Moonshot Systems using the HPE Chassis Manager RESTful API.

⚠ HPE Moonshot Systems Centers are deprecated and being removed in Leostream Platform 2025.1.

Ensure that the operating system installed on each Moonshot node contains an installed and running Leostream Agent. The Leostream Agent returns operating system information about the node, such as IP address, to the Connection Broker. Without a Leostream Agent, the Connection Broker gathers only MAC address information from the Chassis Manager, and you cannot offer Moonshot nodes to your end users.

To create a center that communicates with the chassis manager:

1. Go to the **> Setup > Centers** page.

2. Click on **Add Center**. The **Add Center** form opens.

3. Select **HPE Moonshot System** from the **Type** drop-down menu.

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

5. Enter the appropriate information in the **Hostname or IP address of Chassis Management Module** edit field.

6. In the **Username** and **Password** edit fields, enter the credentials for a user with administrator privileges to the Chassis Manager.

7. Select a time from the **Inventory scan interval** drop-down menu. This setting tells the Connection Broker how often to refresh the desktops imported from this center. The scan interval is the length of time between when one refresh action completes and the next refresh action begins.

8. Uncheck the **Offer desktops from this center** option if the Connection Broker should not offer desktops from this center to users who log into the Connection Broker. The Connection Broker continues to offer assigned desktops to the assigned user, even when this option is not selected.

9. Select **Assign rogue users to desktops from this center (requires Agent)** if you want the Connection Broker to manage users that log into desktops in this center when they do not log in through Leostream. The desktop must have a running Leostream Agent, which informs the Connection Broker of user logins (see **Assigning Desktops to Rogue Users**).

10. Select the **Initialize newly-discovered desktops as "unavailable"** option if the Connection Broker should mark desktops as unavailable as they are discovered. Otherwise, leave this option unchecked.

    You can manually mark any **Unavailable** desktop as **Available** using the **Availability** drop-down menu on the desktop’s **Edit Desktop** page. To access the **Edit Desktop** page, go to the **> Resources > Desktops** page and select the **Edit** action associated with that desktop.

11. Select the **Continuously apply any Auto-Tags** option if you want to set tags on desktops that are discovered when the center is refreshed (see **Continuously Applying Tags to Desktops** for more information). Leave this option unchecked if you do not want to tag desktops.

12. Click **Save**.

For more information on using Leostream with HPE Moonshot System, download the Leostream and HPE Moonshot System Reference Architecture or contact **sales@leostream.com**.

KubeVirt (Red Hat OpenShift) Centers

By creating a KubeVirt center, you can deploy, terminate, power control, and assign virtual machine-based workloads on common container platforms, such as the Red Hat OpenShift platform, within your Leostream environment.

The KubeVirt API listens on port 6443. Ensure that your Connection Broker is able to reach your container environment on this port before proceeding.

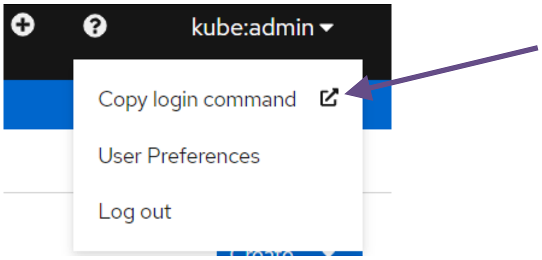
When working with Red Hat OpenShift, you must install the OpenShift Virtualization Operator in order to manage virtual machines with Kubernetes.

Before creating your KubeVirt center, you need to obtain:

- The API URL for your environment
- The API version
- An authentication token for a user who has permission to execute the KubeVirt API
- The namespace or project in your container platform that you want to manage in your Leostream environment.

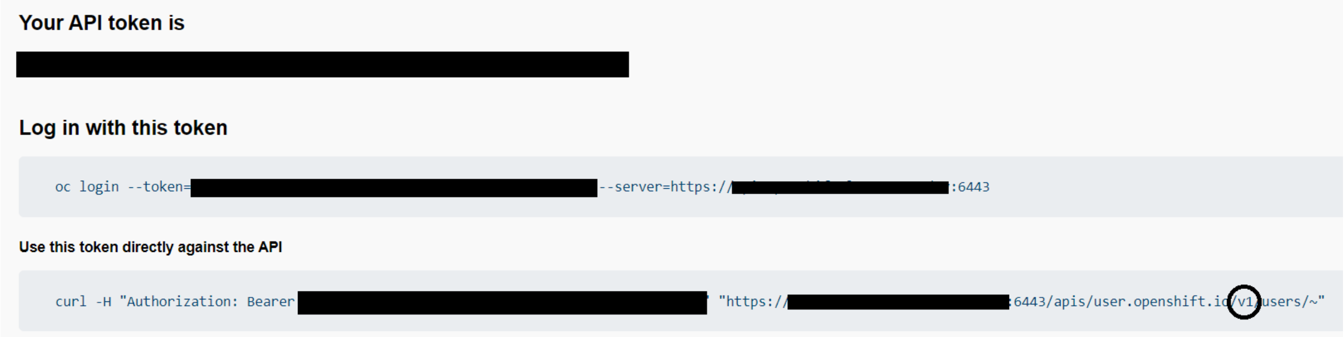
  It is best practice not to use the `default` namespace for running your Leostream workloads.

If you are using Red Hat OpenShift, you can obtain this information from the OpenShift console by clicking on the drop-down menu next to your login username on the top right-hand corner, for example:



Select **Copy login command**, indicated in the previous figure, and you will be directed to a new page for authentication. Login with the same credential you used to access the OpenShift console.

After logging in, click **Display token** to view the token and login information for the authenticated user, as shown for example in the following figure.



Your API token is

[redacted]

Log in with this token

```
oc login --token=[redacted]--server=https://[redacted]:6443
```

Use this token directly against the API

```
curl -H "Authorization: Bearer [redacted]" "https://[redacted]:6443/apis/user.openshift.io/v1/users/~"
```

Make note of:

- Your API token is the value in the **Your API token is** section
- Your API URL is the address, including the port number, shown for the `--server` parameter in the **Log in with this token** section
- Your API version is displayed in URL at the end of the **Use this token directly against the API** section, shown circled in the previous figure

To create a KubeVirt center:

1. Go to the **> Setup > Centers** page.

2. Click the **Add Center** link.

3. In the **Add Center** form, select **KubeVirt** from the **Type** drop-down menu.

4. Enter a name for the multi-user center in the **Name** edit field.

5. In the **API URL** edit field, enter the full URL, including the port number, for your KubeVirt API.

6. In the **API Token** edit field, enter the authentication token for a user with permission to execute the API.

7. Enter your API version in the **API Version** edit field.

8. In the **Namespace** edit field, enter the namespace (or project, in OpenShift) that you want to manage in your Leostream environment.

9. In the **Provisioning template** edit field, enter a YAML template to use for provisioning new virtual machines in your container platform. Currently, only a single template is supported.

10. Select a time from the **Inventory scan interval** drop-down menu. This setting tells the Connection Broker how often to refresh the desktops imported from this center. The scan interval is the length of time between when one refresh action completes and the next refresh action begins.

11. Uncheck the **Offer desktops from this center** option if the Connection Broker should not offer desktops from this center to users who log into the Connection Broker. The Connection Broker

continues to offer assigned desktops to the assigned user, even when this option is not selected.

12. If you plan to use the Connection Broker to manage capacity in your container platform and allow the Connection Broker to delete virtual machines that are already provisioned, select the **Initialize newly-discovered desktops as "deletable"** option. If a VM is marked as deletable, you can use Leostream Release Plans to delete the VM from disk after the user is released from the desktop.

    If you do not plan to use Release Plans to delete your virtual machines, do not mark desktops as deleteable.

13. Click **Save**.

Microsoft Azure Centers

Microsoft Azure centers allow you to provision, connect, and terminate instances in a Microsoft Azure cloud. Before you can connect Leostream to your Microsoft Azure account, you must do the following:

- Obtain your subscription ID
- Register the Connection Broker application and get the application ID
- Find the tenant ID for the application
- Generate a secret key
- Assign the Connection Broker application to an appropriate role

Consult the **Leostream Quick Start guide for Microsoft Azure Clouds** for detailed instructions on obtaining these items. After obtaining the previous information, to create an Azure center:

1. Go to the **> Setup > Centers** page.

2. Click the **Add Center** link.

3. In the **Add Center** form, select **Microsoft Azure** from the **Type** drop-down menu.

4. Enter a name for the multi-user center in the **Name** edit field.

5. Select the Azure region you want to manage from the **Region** drop-down menu. Create separate centers for each region you want to manage in the Connection Broker.

6. Enter your Azure subscription ID into the **Subscription ID** edit field.

7. Enter your tenant ID into the **Directory (tenant) ID** edit field.

8. Enter your client ID into the **Application (client) ID** edit field.

9. Enter the secret key associated with your Leostream application into the **Secret Access Key** field.

10. Select a time from the **Inventory scan interval** drop-down menu. This setting tells the Connection Broker how often to refresh the desktops imported from this center. The scan interval is the length

of time between when one refresh action completes and the next refresh action begins.

11. Uncheck the **Scan storage, images, and blobs for provisioning** option if you are not using the Connection Broker to launch new instances in Azure. Disabling the inventorying of storage, images, and blobs may improve the performance of Azure center scans

12. The Connection Broker must be able to reach out to the internet to communicate with the Azure APIs. If your Connection Broker is hidden in a private network without access to the internet, select the **Use a Leostream Gateway to communicate with this Center** option to use a Leostream Gateway to proxy traffic to the internet. Ensure that you have at least one Leostream Gateway registered on the **> Setup > Leostream Gateway** page.

13. Uncheck the **Offer desktops from this center** option if the Connection Broker should not offer desktops from this center to users who log into the Connection Broker. The Connection Broker continues to offer assigned desktops to the assigned user, even when this option is not selected.

14. Select **Assign rogue users to desktops from this center (requires Agent)** to have Leostream assign users to desktops in this center when the user connects to the desktop from a non-Leostream client, such as mstsc.exe or the HP ZCentral Remote Boost Receiver. The desktop must have a running Leostream Agent, which informs the Connection Broker of user logins (see **Assigning Desktops to Rogue Users**).

15. Select the **Initialize newly-discovered desktops as "unavailable"** option if the Connection Broker should mark desktops as unavailable as they are discovered. Otherwise, leave this option unchecked.

    You can manually mark any **Unavailable** desktop as **Available** using the **Availability** drop-down menu on the desktop’s **Edit Desktop** page. To access the **Edit Desktop** page, go to the **> Resources > Desktops** page and select the **Edit** action associated with that desktop.

16. If you plan to use the Connection Broker to manage capacity in Azure and allow Leostream to delete virtual machines that are already provisioned, select the **Initialize newly-discovered desktops as "deletable"** option. If a VM is marked as deletable, you can use Leostream Release Plans to delete the VM from disk after the user is released from the desktop.

    If you do not plan to use Release Plans to delete your virtual machines, do not mark desktops as deleteable.

17. Select the **Continuously apply any Auto-Tags** option if you want to set tags on desktops that are discovered when the center is refreshed (see **Continuously Applying Tags to Desktops** for more information). Leave this option unchecked if you do not want to tag desktops.

18. Click **Save** to create the center.

The instances in the center’s Azure region appear in the **> Resources** > **Desktops** page. Any images in that Azure region appear on the **> Resources > Images** page.

The Connection Broker inventories the Resource Groups in this region and stores those groups internally for future use when provisioning in pools. Virtual machines can be provisioned only into the region and Resource Groups associated with your Azure Center.

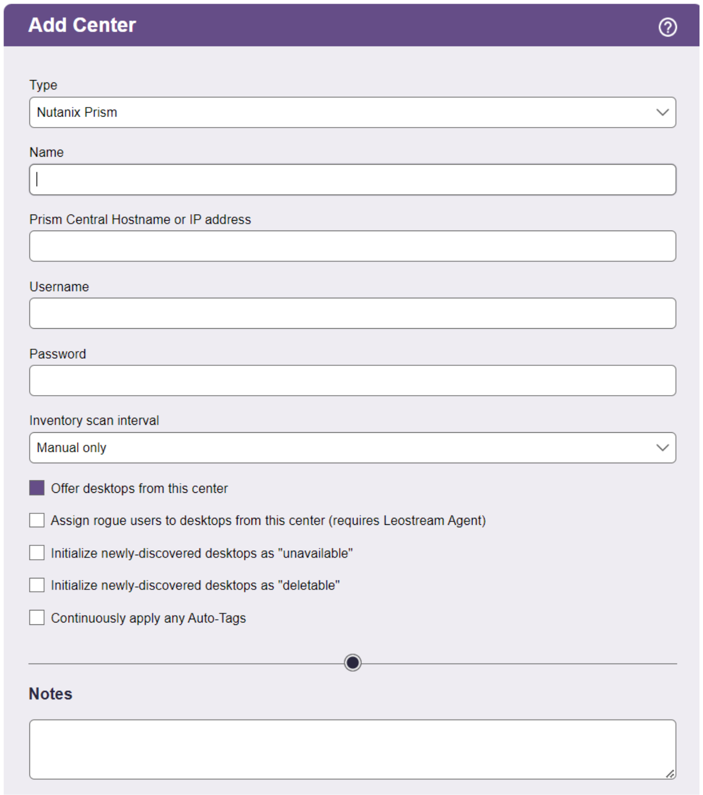
The Connection Broker supports Managed Images, only. You cannot currently provision virtual machines in Leostream using images in a Shared Image Gallery.

Nutanix Prism Central V4 API Centers

Create a Nutanix Prism center to manage virtual machines on modern Nutanix AHV clusters, and to create and delete VMs in Nutanix. The Prism Central V4 APIs are supported by Connection Broker 2024.5.19.1 and later. Use the **Nutanix Prism** center to integrate with the v4 APIs, as follows.

If your Nutanix environment uses a VMware hypervisor or includes OpenStack software, use the VMware or OpenStack center to manage your Nutanix cluster. Nutanix Prism centers in Leostream apply only to virtual machines hosted on the Acropolis Hypervisor (AHV).

1. Go to the **> Setup > Centers** page.
2. Click the **Add Center** link.
3. In the **Add Center** form, select **Nutanix Prism** from the **Type** drop-down menu. The **Add Center** form updates to display the fields shown in the following figure.



Add Center

Type: Nutanix Prism

Name

Prism Central Hostname or IP address

Username

Password

Inventory scan interval: Manual only

☑ Offer desktops from this center

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

□ Initialize newly-discovered desktops as "unavailable"

□ Initialize newly-discovered desktops as "deletable"

□ Continuously apply any Auto-Tags

Notes

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

5. In the **Prism Central Hostname or IP address** edit field, enter the Hostname or IP address of the Prism Central service for your cluster.

6. Enter the **Username** and **Password** for a user with the required permissions to execute the Prism APIs used by Leostream to manage your Nutanix cluster.

7. Select a time from the **Inventory scan interval** drop-down menu. This setting tells the Connection Broker how often to scan the center for changes. The scan interval is the length of time between when one scan completes and the next scan begins.

   If you create or delete virtual machines in Prism, the Connection Broker updates these records in Leostream when the next scan occurs.

8. Uncheck the **Offer desktops from this center** option if the Connection Broker should not offer desktops from this center to users who log into the Connection Broker. The Connection Broker continues to offer assigned desktops to the assigned user, even when this option is not selected.

9. Select **Assign rogue users to desktops from this center (requires Agent)** to have Leostream assign users to desktops in this center when the user connects to the desktop from a non-Leostream client, such as mstsc.exe. The desktop must have a running Leostream Agent, which informs the Connection Broker of user logins (see **Assigning Desktops to Rogue Users**).

10. Select the **Initialize newly-discovered desktops as "unavailable"** option if the Connection Broker should mark desktops as unavailable as they are discovered.

    You can manually mark any **Unavailable** desktop as **Available** using the **Availability** drop-down menu on the desktop's **Edit Desktop** page. To access the **Edit Desktop** page, go to the **> Resources > Desktops** page and select the **Edit** action associated with that desktop.

11. If you plan to use the Connection Broker to manage capacity and allow Leostream to delete virtual machines that are already provisioned, select the **Initialize newly-discovered desktops as "deletable"** option. If a VM is marked as deletable, you can use Leostream Release Plans to delete the VM from disk after the user is released from the desktop.

    If you do not plan to use Release Plans to delete your virtual machines, do not mark desktops as deleteable.

12. Select the **Continuously apply any Auto-Tags** option if you want to set tags on desktops that are discovered when the center is refreshed (see **Continuously Applying Tags to Desktops** for more information). Leave this option unchecked if you do not want to tag desktops.

13. Click **Save**.

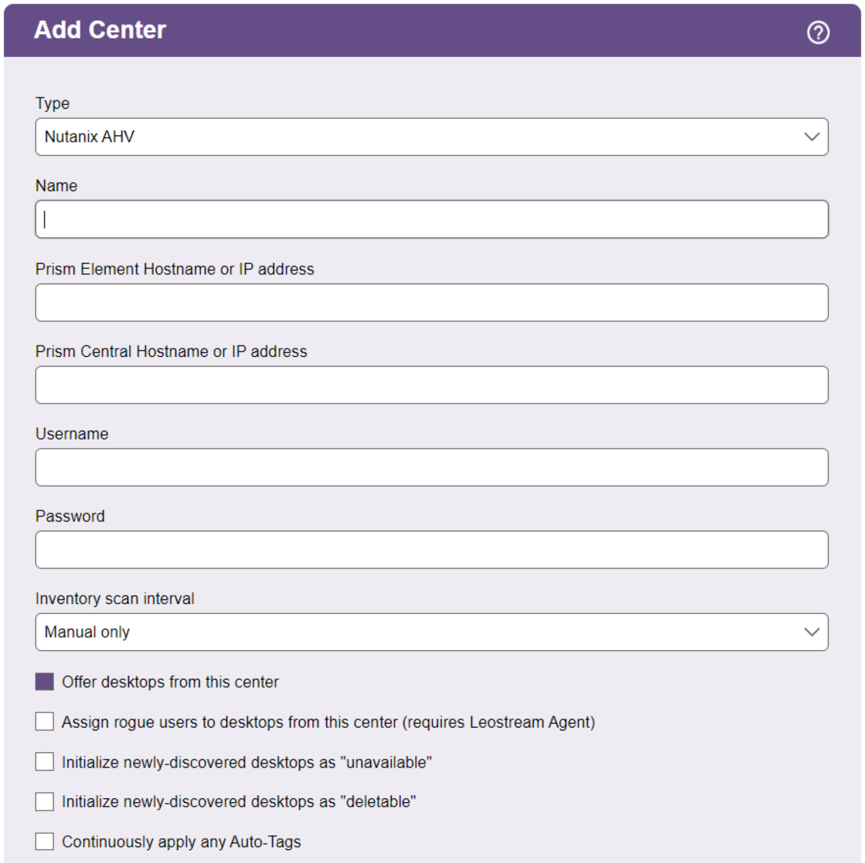
Nutanix AHV Clusters (Prism Element and Central v3 APIs)

Create a Nutanix AHV center to manage virtual machines on a Nutanix AHV cluster running v3 Prism APIs, and to create and delete VMs in Nutanix. For older versions of Nutanix, Connection Broker uses both the Prism Element and Central APIs in order to be fully functional.

If your Nutanix environment uses a VMware hypervisor or includes OpenStack software, use the VMware or OpenStack center to manage your Nutanix cluster. Nutanix AHV centers in Leostream apply only to virtual machines hosted on the Acropolis Hypervisor (AHV).

To create a Nutanix AHV center:

1. Go to the **> Setup > Centers** page.
2. Click the **Add Center** link.
3. In the **Add Center** form, select **Nutanix AHV** from the **Type** drop-down menu. The **Add Center** form updates to display the fields shown in the following figure.



Add Center

Type: Nutanix AHV

Name:

Prism Element Hostname or IP address:

Prism Central Hostname or IP address:

Username:

Password:

Inventory scan interval: Manual only

☑ Offer desktops from this center

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

☐ Initialize newly-discovered desktops as "unavailable"

☐ Initialize newly-discovered desktops as "deletable"

☐ Continuously apply any Auto-Tags

4. Enter a name for the center in the **Name** edit field.
5. In the **Prism Element Hostname or IP address** edit field, enter the Hostname or IP address of the Prism Element service for your cluster.

6. In the **Prism Central Hostname or IP address** edit field, enter the Hostname or IP address of the Prism Central service for your cluster.

7. Enter the **Username** and **Password** for a user with the required permissions to execute the Prism APIs used by Leostream to manage your Nutanix cluster.

   The center uses the same credentials for both Prism Element and Prism Central, so ensure that this user exists and has the appropriate permissions for both services.

8. Select a time from the **Inventory scan interval** drop-down menu. This setting tells the Connection Broker how often to scan the center for changes. The scan interval is the length of time between when one scan completes and the next scan begins.

   If you create or delete virtual machines in Prism, the Connection Broker updates these records in Leostream when the next scan occurs.

9. Click **Save** to create the center.

As soon as you save the form, the Connection Broker inventories all virtual machines and OVAs in your Connection Broker. Desktops are listed on the **> Resources > Desktops** page. All OVAs available for provisioning are listed on the **> Resources > Images** page. Snapshots available for provisioning are listed in the pools page when you enable provisioning from snapshots.

Any desktops that previously registered in the Enrolled Desktops center are marked as duplicate record when inventoried in your Nutanix center.

Any time new desktops are important during a center scan, the Connection Broker submits a job to scan each virtual machine for an installed Leostream Agent. You can find these jobs on the **> System > Job Queue** page as `hda_scan` jobs. The Leostream Agent must already be registered with your Connection Broker or the agent will not accept Connection Broker communications. If you specified your Connection Broker address when you installed the Leostream Agent, the agent registered with the Connection Broker when the installation completed.

After the `hda_scan` jobs complete, you can test the Leostream Agent communication by clicking the **Status** link on the **> Resources > Desktops** page for any desktop listed as having a running Leostream Agent.

OpenStack® Centers

OpenStack centers allow you to manage and provision desktops in an OpenStack environment that use the Keystone Identity API v3. To create an OpenStack center:

1. Go to the **> Setup > Centers** page.

2. Click on **Add Center**. The **Add Center** form opens.

3. Select **OpenStack** from the **Type** drop-down menu.

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

5. In the **Auth URL** edit field, enter the authentication URL for your OpenStack Environment. The authorization URL often takes the form:

   `http://`*`openstack.yourcompany.net`*`:5000/v3.0`

   where *`openstack.yourcompany.net`* is the hostname or IP address of your OpenStack environment.

6. If needed, enter the appropriate region into the **Region** edit field. Leave the **Region** field blank if you are using the default OpenStack Region.

7. Enter the OpenStack domain that contains your project and user in the **Project Domain** edit field.

8. Enter your project name into the **Project** edit field.

9. Enter an administrator domain, username, and password into the **User Domain**, **Username** and **Password** edit fields, respectively.

10. Select a time from the **Inventory scan interval** drop-down menu. This setting tells the Connection Broker how often to refresh the desktops imported from this center. The scan interval is the length of time between when one refresh action completes and the next refresh action begins.

11. Uncheck the **Offer desktops from this center** option if the Connection Broker should not offer desktops from this center to users who log into the Connection Broker. The Connection Broker continues to offer assigned desktops to the assigned user, even when this option is not selected.

12. Select **Assign rogue users to desktops from this center (requires Agent)** if you want the Connection Broker to manage users that log into desktops in this center when they do not log in through Leostream. The desktop must have a running Leostream Agent, which informs the Connection Broker of user logins (see **Assigning Desktops to Rogue Users**).

13. Select the **Initialize newly-discovered desktops as "unavailable"** option if the Connection Broker should mark desktops as unavailable as they are discovered. Otherwise, leave this option unchecked.

    You can manually mark any **Unavailable** desktop as **Available** using the **Availability** drop-down menu on the desktop's **Edit Desktop** page. To access the **Edit Desktop** page, go to the **> Resources > Desktops** page and select the **Edit** action associated with that desktop.

14. If you plan to use the Connection Broker to manage capacity in OpenStack, and allow Leostream to delete virtual machines that are already provisioned, select the **Initialize newly-discovered desktops as "deletable"** option. If a VM is marked as deletable, you can use Leostream Release Plans to delete the VM from disk after the user is released from the desktop.

15. Select the **Continuously apply any Auto-Tags** option if you want to set tags on desktops that are discovered when the center is refreshed (see **Continuously Applying Tags to Desktops** for more

information). Leave this option unchecked if you do not want to tag desktops.

16. Click **Save**.

The instances in the center's OpenStack project appear in the **> Resources** > **Desktops** page. Any images in that project appear on the **> Resources > Images** page.

Red Hat Virtualization Centers

You can provision and manage connections for virtual machines hosted on a Red Hat Virtualization host by creating a Red Hat Virtualization center in Leostream.

⚠ Red Hat has ended standard maintenance for Red Hat Virtualization and, therefore, Red Hat Virtualization centers are being removed in Leostream Platform 2025.1. Red Hat customers are encouraged migrate to Red Hat OpenShift and leverage the Leostream KubeVirt Centers for OpenShift integration.

⚠ The Connection Broker inventories only virtual machines and templates that have the **Optimized for** option set to **Desktop**. Virtual machines optimizing for Server or High Performance will not appear in your Connection Broker inventory.

To create a center for Red Hat Virtualization:

1. Go to the **> Setup > Centers** page.
2. Click **Add Center**. The **Add Center** form opens.
3. Select **Red Hat Virtualization** from the **Type** drop-down menu.
4. Enter a name for the center in the **Name** edit field.
5. In the **Hostname or IP address** field, enter the hostname or IP address of the management server for your Red Hat Virtualization hosts. This field takes the form of a URL, for example:

   ```
   https://<hostname-or-IP>
   ```

6. Enter the username and password for a user with permission to inventory, power control, and, if applicable, provision virtual machines in your Red Hat Virtualization environment.

   📝 The username takes the form of `user@domain`, for example `admin@internal`.

7. Select a time from the **Inventory scan interval** drop-down menu. This setting tells the Connection Broker how often to refresh the desktops imported from this center. The refresh interval is the length of time between when one refresh action completes and the next refresh action begins.
8. Uncheck the **Offer desktops from this center** option if the Connection Broker should not offer desktops from this center to users who log into the Connection Broker. The Connection Broker continues to offer assigned desktops to the assigned user, even when this option is not selected.

9. Select **Assign rogue users to desktops from this center (requires Agent)** to have Leostream assign users to desktops in this center when the user connects to the desktop from a non-Leostream client, such as mstsc.exe or the HP ZCentral Remote Boost Receiver. The desktop must have a running Leostream Agent, which informs the Connection Broker of user logins (see **Assigning Desktops to Rogue Users**).

10. Select the **Initialize newly-discovered desktops as "unavailable"** option if the Connection Broker should mark desktops as unavailable as they are discovered.

    You can manually mark any **Unavailable** desktop as **Available** using the **Availability** drop-down menu on the desktop's **Edit Desktop** page. To access the **Edit Desktop** page, go to the **> Resources > Desktops** page and select the **Edit** action associated with that desktop.

11. If you plan to use the Connection Broker to manage capacity and allow Leostream to delete virtual machines that are already provisioned, select the **Initialize newly-discovered desktops as "deletable"** option. If a VM is marked as deletable, you can use Leostream Release Plans to delete the VM from disk after the user is released from the desktop.

    📝 If you do not plan to use Release Plans to delete your virtual machines, do not mark desktops as deleteable.

12. Select the **Continuously apply any Auto-Tags** option if you want to set tags on desktops that are discovered when the center is refreshed (see **Continuously Applying Tags to Desktops** for more information). Leave this option unchecked if you do not want to tag desktops.

13. Click **Save**.

Remote Desktop Services / Multi-User Centers

The Connection Broker allows you to offer session from multi-user servers, such as Microsoft Remote Desktop Services (RDS), AVD servers, or Linux servers, alongside your other offered resources.

⚠ Before creating a multi-user center, you must install the Leostream Agent on the server. The Leostream Agent must register with your Connection Broker and the server must appear on the **> Resources > Desktops** page before you can add the RDS/Multi-User center to your Connection Broker.

You can alternatively use the **Bulk Edit** dialog to convert the desktop into a center. See **Converting Desktops to Remote Desktop Services / Multi-User Centers** for more information.

Adding a Remote Desktop Services / Multi-User Center

To add a center for managing multiple sessions on the same server:

1. Go to the **> Setup > Centers** page.

2. Click on **Add Center**. The **Add Center** form opens.

3. Select **Remote Desktop Services/Multi-User** from the **Type** drop-down menu.

4. Enter a name for the multi-user center in the **Name** edit field.

5. Use the **Select server to convert to a Remote Desktop Services/Multi-User Center** edit field to indicate the server for this center. This drop-down menu contains only virtual machines listed on the **> Resources > Desktops** page with a running Leostream Agent.

6. Enter the maximum number of concurrent user connections in the **Maximum concurrent connections** edit field.

7. Select a time from the **Inventory scan interval** drop-down menu. This setting tells the Connection Broker how often to refresh the sessions created for this center. The scan interval is the length of time between when one refresh action completes and the next refresh action begins.

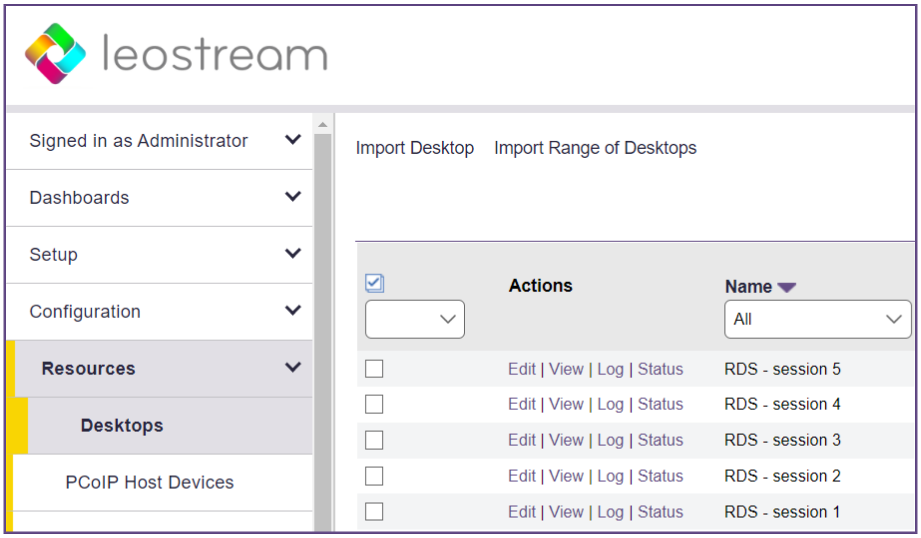
   If you select **Manual** from the **Inventory scan interval** drop-down menu, ensure that you manually refresh the center after it is created. The manual scan is required to correctly set the operating system and IP address of the sessions displayed in the **> Setup > Centers** page.

8. Uncheck the **Offer desktops from this center** option if the Connection Broker should not offer sessions from this center to users who log into the Connection Broker. The Connection Broker continues to offer assigned sessions to the assigned user, even when this option is not selected.

9. Select **Assign rogue users to desktops from this center (requires Agent)** if you want the Connection Broker to manage users that log into desktops in this center when they do not log in through Leostream (see **Assigning Desktops to Rogue Users**).

10. Click **Save**.

The sessions appear as a series of entries in the list of desktops, shown in the following figure.



☑	Actions	Name
		All
□	Edit | View | Log | Status	RDS - session 5
□	Edit | View | Log | Status	RDS - session 4
□	Edit | View | Log | Status	RDS - session 3
□	Edit | View | Log | Status	RDS - session 2
□	Edit | View | Log | Status	RDS - session 1

Modifying the Number of Available Sessions

You can add or remove sessions after the center is added, as follows.

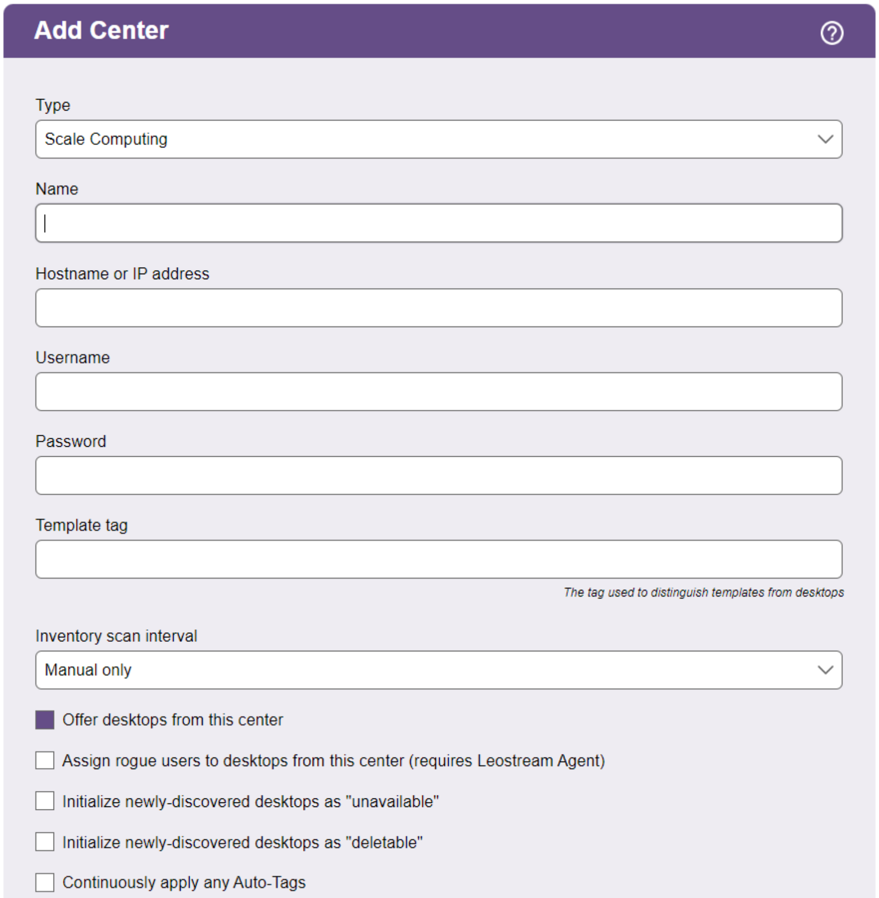
1. Go to the **> Setup > Centers** page.
2. Click the **Edit** action associated with the multi-user center. The **Edit Center** form opens.
3. Modify the number in the **Maximum concurrent connections** field.
4. Click **Save**.

When changing the number of available sessions, the Connection Broker first deletes all existing sessions then creates new sessions. The Connection Broker does *not* disconnect users logged into any of the previous sessions, however these sessions are no longer displayed in the Connection Broker Web interface.

Scale Computing Platform Clusters

You can create a Scale Computing center in Leostream using the following procedure. For more detail, see the **Quick Start Guide for the Scale Computing Platforms**.

1. Go to the **> Setup > Centers** page.
2. Click the **Add Center** link.
3. In the **Add Center** form, select **Scale Computing** from the **Type** drop-down menu. The **Add Center** form updates to display the fields shown in the following figure.



Add Center

Type: Scale Computing

Name

Hostname or IP address

Username

Password

Template tag

The tag used to distinguish templates from desktops

Inventory scan interval: Manual only

☑ Offer desktops from this center

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

□ Initialize newly-discovered desktops as "unavailable"

□ Initialize newly-discovered desktops as "deletable"

□ Continuously apply any Auto-Tags

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

5. Enter the Hostname or IP address of one of the SC//HyperCore nodes in your cluster.

   You do not need to enter the IP address or hostname of all the nodes in your cluster. The Connection Broker automatically discovers all of the nodes and internally enables failover so your Center remains online.

6. Enter the **Username** and **Password** for a Scale Computing Platform user with admin-level role access.

7. In the **Template** tag field, enter the tag you use in your Scale Computing Platform to indicate virtual machines you consider master golden images for provisioning.

   Virtual machines assigned to his tag in your Scale Computing Platform are inventoried on the **> Resources > Images** page, and do not appear on the **> Resources > Desktops** page. You can use these images in pools to provision persistent and non-persistent virtual machines.

8. Select a time from the **Inventory scan interval** drop-down menu. This setting tells the Connection Broker how often to refresh the desktops imported from this center. The scan interval is the length of time between when one refresh action completes and the next refresh action begins.

9. Uncheck the **Offer desktops from this center** option if the Connection Broker should not offer desktops from this center to users who log into the Connection Broker. The Connection Broker continues to offer assigned desktops to the assigned user, even when this option is not selected.

10. Select **Assign rogue users to desktops from this center (requires Agent)** to have Leostream assign users to desktops in this center when the user connects to the desktop from a non-Leostream client, such as mstsc.exe or the HP ZCentral Remote Boost Receiver. The desktop must have a running Leostream Agent, which informs the Connection Broker of user logins (see **Assigning Desktops to Rogue Users**).

11. Select the **Initialize newly-discovered desktops as "unavailable"** option if the Connection Broker should mark desktops as unavailable as they are discovered. Otherwise, leave this option unchecked.

    You can manually mark any **Unavailable** desktop as **Available** using the **Availability** drop-down menu on the desktop's **Edit Desktop** page. To access the **Edit Desktop** page, go to the **> Resources > Desktops** page and select the **Edit** action associated with that desktop.

12. If you plan to use the Connection Broker to manage capacity in your Scale Computing Platform and allow Leostream to delete virtual machines that are already provisioned, select the **Initialize newly-discovered desktops as "deletable"** option. If a VM is marked as deletable, you can use Leostream Release Plans to delete the VM from disk after the user is released from the desktop.

    📝 If you do not plan to use Release Plans to delete your virtual machines, do not mark desktops as deleteable.

13. Select the **Continuously apply any Auto-Tags** option if you want to set tags on desktops that are discovered when the center is refreshed (see **Continuously Applying Tags to Desktops** for more information). Leave this option unchecked if you do not want to tag desktops.

14. Click **Save**.

As soon as you save the form, the Connection Broker inventories all virtual machines as either desktops or images in your Connection Broker. Desktops are listed on the **> Resources > Desktops** page and images are listed on the **> Resources > Images** page.

📝 The Connection Broker relies on the Leostream Agent to obtain accurate IP address, hostname, and operating system information for the virtual machines hosted on your Scale Computing system.

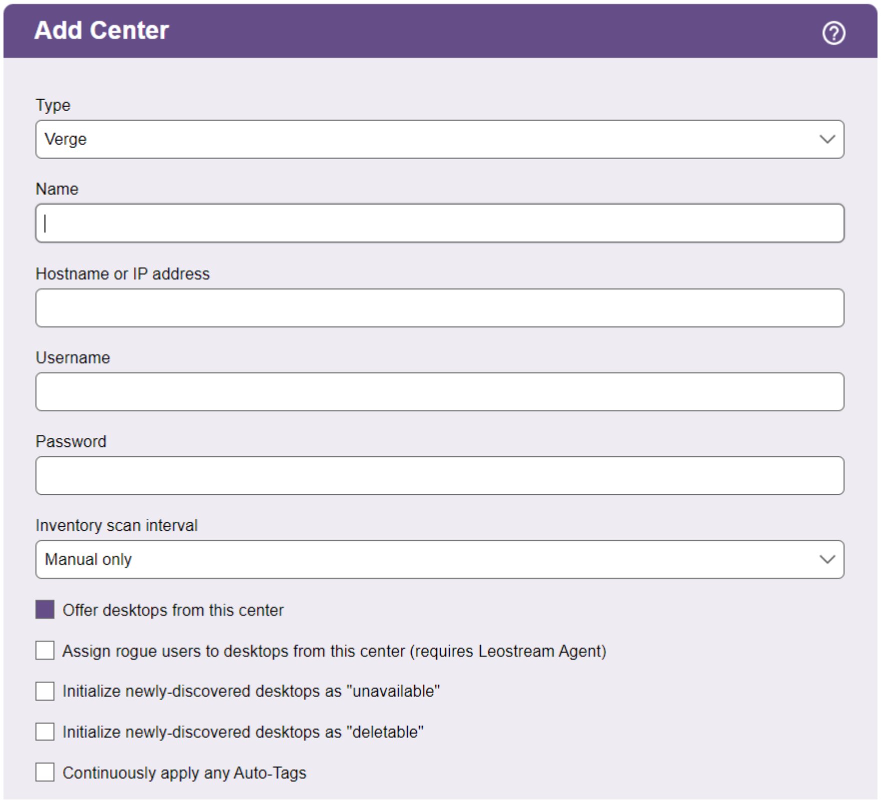
VergeIO Centers

VergeIO Virtualization Software allows you to build on-premises cloud solutions quickly and easily. You can use Leostream to inventory, provision, and managed connections to VDI instances hosted on Verge. You create a Verge center, as follows.

1. Go to the **> Setup > Centers** page.

2. Click the **Add Center** link.

3. In the **Add Center** form, select **Verge** from the **Type** drop-down menu. The **Add Center** form updates to display the fields shown in the following figure.



Add Center

Type: Verge

Name:

Hostname or IP address:

Username:

Password:

Inventory scan interval: Manual only

☑ Offer desktops from this center

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

☐ Initialize newly-discovered desktops as "unavailable"

☐ Initialize newly-discovered desktops as "deletable"

☐ Continuously apply any Auto-Tags

4. Enter the Hostname or IP address you use to access the VergeIO Web-based machine management console.

   Do not enter the hostname using a URL format.

5. Enter the **Username** and **Password** for a user with adequate permissions to execute the VergeIO API used by Leostream to integrate with the center.

6. Select a time from the **Inventory scan interval** drop-down menu. This setting tells the Connection Broker how often to refresh the desktops imported from this center. The scan interval is the length of time between when one refresh action completes and the next refresh action begins.

7. Uncheck the **Offer desktops from this center** option if the Connection Broker should not offer desktops from this center to users who log into the Connection Broker. The Connection Broker continues to offer assigned desktops to the assigned user, even when this option is not selected.

8. Select **Assign rogue users to desktops from this center (requires Agent)** to have Leostream assign users to desktops in this center when the user connects to the desktop from a non-Leostream

client, such as mstsc.exe or the HP ZCentral Remote Boost Receiver. The desktop must have a running Leostream Agent, which informs the Connection Broker of user logins (see **Assigning Desktops to Rogue Users**).

9. Select the **Initialize newly-discovered desktops as "unavailable"** option if the Connection Broker should mark desktops as unavailable as they are discovered. Otherwise, leave this option unchecked.

   You can manually mark any **Unavailable** desktop as **Available** using the **Availability** drop-down menu on the desktop’s **Edit Desktop** page. To access the **Edit Desktop** page, go to the **> Resources > Desktops** page and select the **Edit** action associated with that desktop.

10. If you plan to use the Connection Broker to manage capacity and allow Leostream to delete virtual machines that are already provisioned, select the **Initialize newly-discovered desktops as "deletable"** option. If a VM is marked as deletable, you can use Leostream Release Plans to delete the VM from disk after the user is released from the desktop.

    If you do not plan to use Release Plans to delete your virtual machines, do not mark desktops as deleteable.

11. Select the **Continuously apply any Auto-Tags** option if you want to set tags on desktops that are discovered when the center is refreshed (see **Continuously Applying Tags to Desktops** for more information). Leave this option unchecked if you do not want to tag desktops.

12. Click **Save**.

The Connection Broker lists all virtual machines in your Verge center on the **> Resources > Desktops** page and lists all snapshots and recipes on the **> Resources > Images** page.

VMware® vSphere and vCenter Server Centers

The Connection Broker uses VMware APIs to manage virtual machines hosted in vSphere. You can create a center that points either directly to vSphere, or to the vCenter Server management tools. You must create a center for vCenter Server if you want to use the Connection Broker to provision new virtual machines.

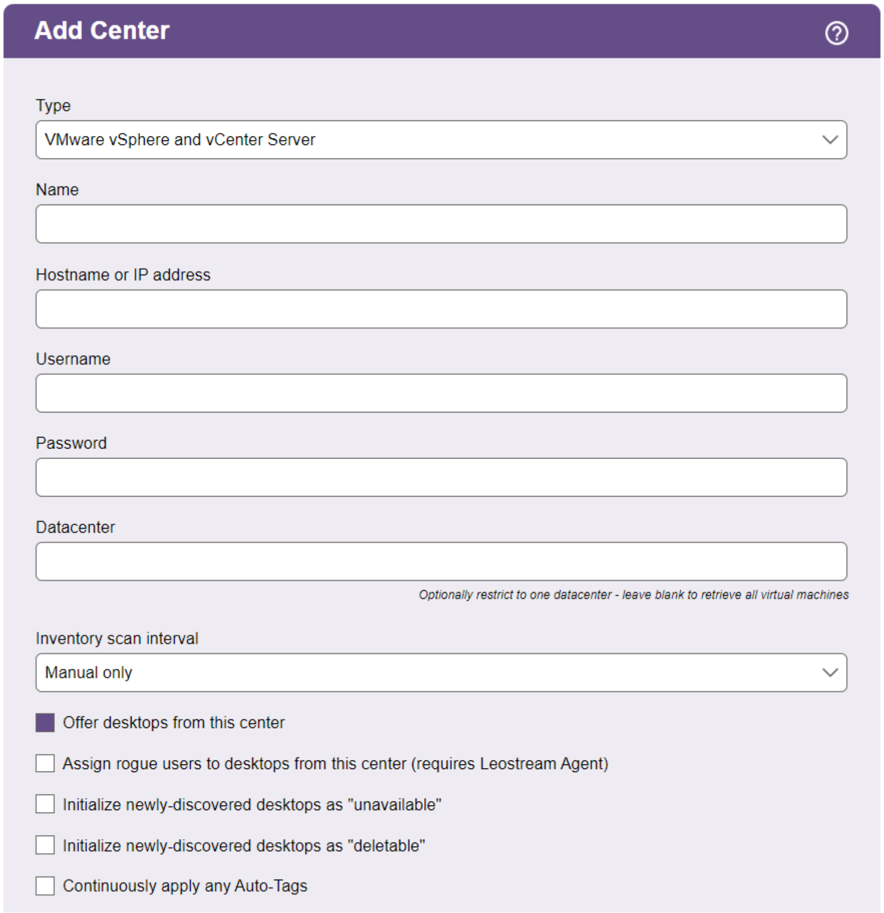
VMware tools must be installed on the virtual machines hosted in vSphere for the Connection Broker to obtain the IP address and other virtual machine attributes.

To add a center for either vSphere, ESXi, or vCenter Server 7 or 8:

1. Go to the **> Setup > Centers** page.

2. Click **Add Center**. The **Add Center** form opens.

3. Select **VMware vSphere and vCenter Server** from the **Type** drop-down menu. The form updates, as follows:



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)

□ Initialize newly-discovered desktops as "unavailable"

□ Initialize newly-discovered desktops as "deletable"

□ Continuously apply any Auto-Tags

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

5. Enter the vCenter Server address in the **Hostname or IP address** edit field.

6. In the **Username** edit field, enter the name of a user with administrative privileges (see **Required vCenter Server Permissions**).

7. Enter this user’s password into the **Password** edit field.

8. To import virtual machines from a particular datacenter, enter the name of the datacenter in the **Datacenter** edit field. Ignore the **Datacenter** option when pointing the center directly to a vSphere server, instead of to the vCenter Server management tool.

9. Select a time from the **Inventory scan interval** drop-down menu. This setting tells the Connection Broker how often to refresh the desktops imported from this center. The refresh interval is the length of time between when one refresh action completes and the next refresh action begins.

   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 rate. You can manually refresh the contents from the center at any time, using the **Scan** action associated with the center on the **> Setup > Centers** page.

10. Uncheck the **Offer desktops from this center** option if the Connection Broker should not offer desktops from this center to users. The Connection Broker continues to offer assigned desktops in this center to the assigned user, even when this option is not selected.

11. Select **Assign rogue users to desktops from this center (requires Agent)** to have Leostream assign users to desktops in this center when the user connects to the desktop from a non-Leostream client, such as mstsc.exe or the HP ZCentral Remote Boost Receiver. The desktop must have a running Leostream Agent, which informs the Connection Broker of user logins (see **Assigning Desktops to Rogue Users**).

12. Select the **Initialize newly-discovered desktops as "unavailable"** option if the Connection Broker should mark desktops as unavailable as they are discovered. Otherwise, leave this option unchecked.

    You can manually mark any **Unavailable** desktop as **Available** using the **Availability** drop-down menu on the desktop's **Edit Desktop** page. To access the **Edit Desktop** page, go to the **> Resources > Desktops** page and select the **Edit** action associated with that desktop.

13. If you plan to use the Connection Broker to manage capacity in AWS and allow Leostream to delete virtual machines that are already provisioned, select the **Initialize newly-discovered desktops as "deletable"** option. If a VM is marked as deletable, you can use Leostream Release Plans to delete the VM from disk after the user is released from the desktop.

    📝 If you do not plan to use Release Plans to delete your virtual machines, do not mark desktops as deleteable.

14. Select the **Continuously apply any Auto-Tags** option if you want to set tags on desktops that are discovered when the center is refreshed (see **Continuously Applying Tags to Desktops** for more information). Leave this option unchecked if you are not using tags.

15. Click **Save**.

If you defined custom attributes in your vCenter Server, you can use these attributes to filter desktops in a policy (see **Policy Filters**). You can use up to four custom attributes as policy filters. You define which custom attributes are available on the **> System > Settings** page (see **Specifying VMware vCenter Server Clusters for Desktop Filters**).

⚠ After you create your VMware center, ensure that you set the **Inventory scan interval** to **Manual** prior to performing any upgrades to your VMware environment. After switching the scan interval and saving the center, ensure that all `scan` jobs associated with your VMware center complete prior to beginning your VMware upgrade.

Required vCenter Server Permissions

The Connection Broker requires specific vCenter Server privileges in order to perform various actions, such as starting and stopping virtual machines or provisioning virtual machines from templates. In order to ensure that your Connection Broker functions properly, you must provide the Connection Broker with the credentials for a vCenter Server account that is assigned the required privileges.

The following table lists the privileges that the Connection Broker uses. Note that these privileges are accurate for vCenter and vSphere version 6.7.

Leostream Action	VMware Privileges	vCenter Role Terminology
Inventory	System.Anonymous System.Read System.View	
Power On	VirtualMachine.Interact.PowerOn	> Virtual Machine > Interaction > Power on
Power Off	VirtualMachine.Interact.PowerOff	> Virtual Machine > Interaction > Power off
Shutdown	VirtualMachine.Interact.PowerOff	> Virtual Machine > Interaction > Power off
Suspend	VirtualMachine.Interact.Suspend	> Virtual Machine > Interaction > Suspend
Resume	VirtualMachine.Interact.PowerOn	> Virtual Machine > Interaction > Power on
Reboot	VirtualMachine.Interact.PowerOn VirtualMachine.Interact.PowerOff VirtualMachine.Interact.Reset	> Virtual Machine > Interaction > Power on > Virtual Machine > Interaction > Power off > Virtual Machine > Interaction > Reset
Revert to snapshot	VirtualMachine.State.RevertToSnapshot	> Virtual Machine > Snapshot management > Revert to snapshot
Create snapshot	VirtualMachine.State.CreateSnapshot	> Virtual Machine > Snapshot management > Create snapshot
Provisioning	Datastore.AllocateSpace Host.Inventory.EditCluster Resource.AssignVMToPool VirtualMachine.Inventory.CreateFromExisting VirtualMachine.Provisining.Clone VirtualMachine.Provisioning.Customize VirtualMachine.Provisioning.DeployTemplate VirtualMachine.Provisioning.ReadCustSpecs	> Datastore > Allocate space > Host > Inventory > Modify cluster > Resource > Assign virtual machine to resource pool > Virtual Machine > Edit inventory > Create new > Virtual Machine > Clone virtual machine > Virtual Machine > Provisioning > Customize guest > Virtual Machine > Provisioning > Deploy template > Virtual Machine > Provisioning > Read customization specification
Delete VM	VirtualMachine.Inventory.Delete	> Virtual Machine > Edit inventory > Remove
Cold migration	Resource.AssignVMToPool Resource.ColdMigrate	> Resource > Assign virtual machine to resource pool > Resource > Migrate powered off virtual machine

Testing vCenter Server Centers

Use the center's **Test** action on the **> Setup > Centers** page to check the following:

- If you can successfully log into the vCenter Server
- If you provided a login account with sufficient privileges to perform the actions required by the Connection Broker

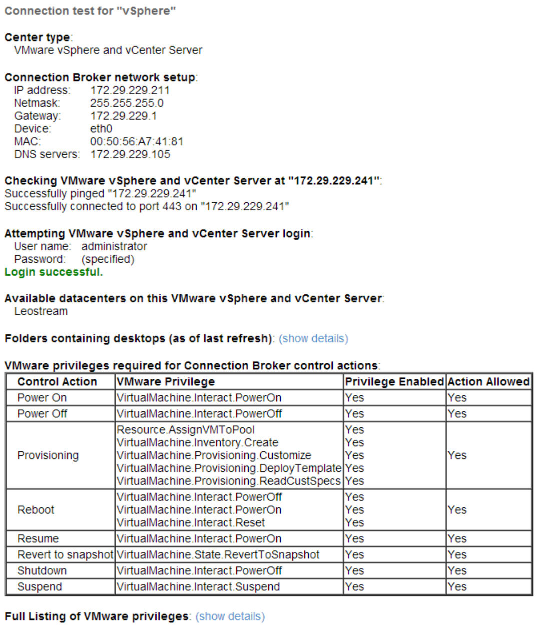
If the test fails to log in to the vCenter Server, check that you correctly entered the hostname or IP address and login credentials. If you still cannot log onto the vCenter Server, use a Web browser to point to the following page, and log in using the Web services username and password:

```
https://VCaddress/mob/?moid=ServiceInstance&doPath=content%2eabout
```

Where `VCaddress` is your vCenter Server address.

You may still have problems connecting to vCenter Server because the Virtual Infrastructure client does not use the same API, or port, as the SDK API. If this occurs, manually check the network settings in vCenter Server.

If the test login succeeds, the Connection Broker displays a report with the following format.



```
Connection test for "vSphere"

Center type:
  VMware vSphere and vCenter Server

Connection Broker network setup:
  IP address:    172.29.229.211
  Netmask:       255.255.255.0
  Gateway:       172.29.229.1
  Device:        eth0
  MAC:           00:50:56:A7:41:81
  DNS servers:   172.29.229.105

Checking VMware vSphere and vCenter Server at "172.29.229.241":
Successfully pinged "172.29.229.241"
Successfully connected to port 443 on "172.29.229.241"

Attempting VMware vSphere and vCenter Server login:
  User name:   administrator
  Password:    (specified)
Login successful.

Available datacenters on this VMware vSphere and vCenter Server:
  Leostream

Folders containing desktops (as of last refresh): (show details)

VMware privileges required for Connection Broker control actions:
```

Control Action	VMware Privilege	Privilege Enabled	Action Allowed
Power On	VirtualMachine.Interact.PowerOn	Yes	Yes
Power Off	VirtualMachine.Interact.PowerOff	Yes	Yes
Provisioning	Resource.AssignVMToPool VirtualMachine.Inventory.Create VirtualMachine.Provisioning.Customize VirtualMachine.Provisioning.DeployTemplate VirtualMachine.Provisioning.ReadCustSpecs	Yes Yes Yes Yes Yes	Yes
Reboot	VirtualMachine.Interact.PowerOff VirtualMachine.Interact.PowerOn VirtualMachine.Interact.Reset	Yes Yes Yes	Yes
Resume	VirtualMachine.Interact.PowerOn	Yes	Yes
Revert to snapshot	VirtualMachine.State.RevertToSnapshot	Yes	Yes
Shutdown	VirtualMachine.Interact.PowerOff	Yes	Yes
Suspend	VirtualMachine.Interact.Suspend	Yes	Yes

```
Full Listing of VMware privileges: (show details)
```

The table at the bottom of the report lists the permissions required to perform various Connection Broker actions and indicates which actions the user whose credentials were provided in the center can perform. The columns in this table include:

- **Control Action**: Actions that the Connection Broker may try to take, depending on your configuration.

- **VMware Privilege**: VMware vCenter Server privileges required to perform the action in the associated row.

- **Privilege Enabled**: Indicates if the user whose credentials were provided in the center is granted the associated VMware privileges.

- **Action Allowed**: Indicates if the user whose credentials were provided in the center is granted all the privileges required for performing this action. If set to **No** the Connection Broker cannot take the associated action. For example, if the **Action Allowed** for the **Provisioning** action is **No**, the Connection Broker cannot provision new virtual machines. In this case, if you configure your Connection Broker to try to provision new VMs, you see errors in the Connection Broker logs.

Uncategorized Desktops

The **Uncategorized Desktops** center is a repository for all desktops not inventoried from another center. When you install a Leostream Agent on a desktop, it registers with the Connection Broker. If that desktop is not already inventoried from an existing center, the Connection Broker creates a new desktop record and places it into the Uncategorized Desktops center. This allows you to manage connections to any desktop, regardless of if it is physical or virtual or hosted on a platform with no built-in support in Leostream

To add the **Uncategorized Desktops** center, as follows.

1. Go to the **> Setup > Centers** page.

2. Click **Add Center**. The **Add Center** form opens.

3. Select **Uncategorized Desktops** from the **Type** drop-down menu.

4. Enter a name for the center.

5. Select a time from the **Inventory refresh interval** drop-down menu. This setting tells the Connection Broker how often to refresh the desktops imported from this center. The refresh interval is the length of time between when one refresh action finishes and the next refresh action starts.

   The refresh interval checks the Leostream Agent status on each desktop in the Uncategorized Center and updates the Leostream Agent status and marks the desktop as duplicate if it matches a desktop found in another center.

6. Select a time from the **Power state refresh interval** drop-down menu. During a power state scan, the Connection Broker uses the Nmap command to probe the ports associated with all display protocols used in your protocol plans and a set of common third-party ports. If any of the scanned ports are open, the Connection Broker marks the desktop as **Running**. If all ports are closed, the Connection Broker marks the desktop as **Stopped**.

   Please contact **support@leostream.com** for a full list of the ports included in a power state scan.

7. Uncheck the **Offer desktops from this center** option if you do not want users to be offered desktops from this center when they log into the Connection Broker. Users assigned to desktops in this center will continue to be offered their assigned desktops, even if this option is not selected.

8. Select **Assign rogue users to desktops from this center (requires Agent)** if you want the Connection Broker to manage users that log into desktops in this center when they do not log in through Leostream. The desktop must have a running Leostream Agent, which informs the Connection Broker of user logins. (see **Assigning Desktops to Rogue Users**).

9. Select the **Initialize newly-discovered desktops as "unavailable"** option if the Connection Broker should mark desktops as unavailable as they are discovered. Otherwise, leave this option unchecked.

10. Select the **Continuously apply any Auto-Tags** option if you want to set tags on desktops that are discovered when the center is refreshed (see **Continuously Applying Tags to Desktops** for more information). Leave this option unchecked if you are not using tags.

11. Select the **Resolve addresses in this center using short hostnames** option to instruct the Connection Broker to reference the desktop using only the portion of the hostname before the first dot.

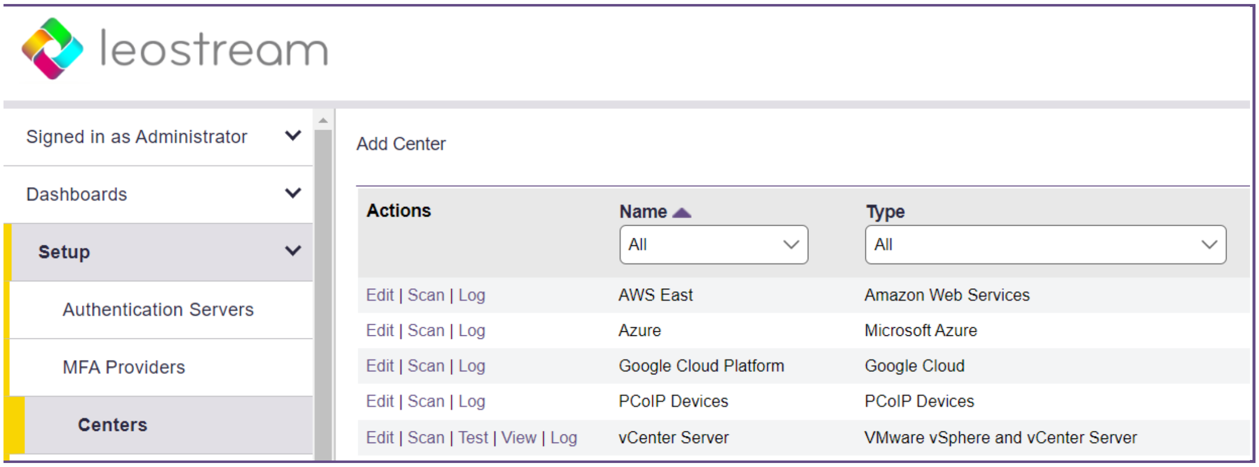
12. Click **Save**.

After you create the **Uncategorized Desktops** center, any desktop with a Leostream Agent that announces its presence to the Connection Broker and is not inventoried from another center is added to this center. You can delete the **Uncategorized Desktops** center at any time (see **Deleting Centers**).

For more information on adding desktops to the Uncategorized Desktops center, see **Registering Desktops in the Uncategorized Desktops Center**.

Displaying Center Characteristics

The **> Setup > Centers** page, shown in the following figure, displays the centers and their characteristics. You can modify the order and type of characteristics displayed on this page by clicking the **Customize columns** link at the top right side of the page (see **Customizing Tables**).



Actions	Name	Type
	All	All
Edit | Scan | Log	AWS East	Amazon Web Services
Edit | Scan | Log	Azure	Microsoft Azure
Edit | Scan | Log	Google Cloud Platform	Google Cloud
Edit | Scan | Log	PCoIP Devices	PCoIP Devices
Edit | Scan | Test | View | Log	vCenter Server	VMware vSphere and vCenter Server

The following sections describe the available centers characteristics.

Actions

Drop-down menu or list of links indicating the actions you can perform on a center. Available actions include:

- **Edit**: Opens the **Edit Center** form for this center
- **Scan**: Forces the Connection Broker to scan the contents from this center. If the center has separate scan intervals for inventory and power state, the forced scan performs both actions.
- **Test**: (Available for virtualization layer centers, only) Attempts to log in to the center using the credentials provided on the **Edit Center** page
- **View**: (Available for vCenter Server, only) Navigates to the vCenter Server URL
- **Log**: Displays the log entries and job queue for this center
- **Upgrade**: Indicates the Leostream Agent installed on the server needs to be upgraded

Assign Rogue Users

Indicates if the Assign rogue users to desktops from this center option is selected.

Datacenter

For vCenter Server, the data center used to retrieve virtual machines. For OpenStack centers, the project associated with the center.

Desktops

The number of desktops inventoried from this center.

Inventory Scan

The center's inventory scan interval. The scan interval is the length of time between when one scan completes and the next scan begins. For Active Directory and Uncategorized Desktops centers, this column corresponds to the setting in the **Inventory scan interval** drop-down menu.

During a scan, the Connection Broker scans the center for changes to the inventory of desktops, adding new desktops to the **> Resources > Desktops** page, as necessary, and removing records for desktops that no longer exist in the center. For centers that return information about the desktop's IP address or power state, the Connection Broker updates this information, as well. If the Connection Broker receives a list of empty desktops from the center, the Connection Broker does not remove any of the desktops from the inventory, to prevent inadvertently deleting active desktops when a center API call fails to retrieve the desktops.

After the scan completes, the Connection Broker contacts the Leostream Agents on the desktops to update any information provided by the agents.

Name
The name you specified for the center.

Offer Desktops
Indicates if the **Offer desktops from this center** option is selected. If the center is not offering its desktops, the desktops appear as Unavailable on the **> Configuration > Pools** page.

Online
Indicates if the center is online (Yes) or offline (No).

Power State Scan
For Active Directory and Uncategorized Desktops centers, the length of time between when the Connection Broker performs a port scan to determine the power state of the desktops in the center.

Server
Hostname or IP address for the server.

Status
Displays the center's status.

- **Deleting**: Displays when you choose to delete a center. During deletion, the virtual machines are removed, followed by the center. The center remains in the list until you navigate away from the page.
- **Disk Full**: Indicates the center's disk is full.
- **Needs Upgrade**: Indicates that the Leostream Agent in this center needs to be upgraded. This setting applies only to centers that use the Leostream Agent.
- **Offline**: Indicates the Connection Broker cannot contact this center.
- **Online**: Indicates this center is operating normally.
- **Refreshing**: Displays when the Connection Broker is refreshing the contents of this center.

Type
The center type selected when the center was created.

Version
The center's version, or the operating system version of the server running the center.

Connecting to External Services

Unlike Centers, where the Leostream Platform manages capacity, assignments, and connections to the resources hosted in that platform, External Services are third-party VDI or DaaS providers. External Services manage the assignment and lifecycle of the user's connection. The Leostream Platform integrates with these services in order to provide end users with a single portal for accessing all their assigned resources in a hybrid environment.

For example, by leveraging Leostream Centers and External Services, users can launch connections to their Windows 365 virtual machine, a racked workstation in their corporate data center, and an AWS EC2 instance all from their Leostream login.

Windows 365 Integration

The Connection Broker uses the Windows 365 API to authenticate users with Windows 365, query for their assigned Windows 365 virtual machines, and connect users to those machines. To integrate with Windows 365, you must create an App registration in Azure that provides the Leostream Platform with the required permissions.

To create an appropriate App registration:

1. Log into the Azure portal.
2. Go to the **> Home > App registrations** page.
3. On the **App Registration** page, click **New registration**.
4. Enter a name for the app in the **Name** edit field.
5. In the **Redirect URI** section:
    a. Select **Public client/native (mobile & desktop)** from the **Select a platform** drop-down menu.
    b. In the edit field to the right of the drop-down menu, enter:

       http://localhost:8400

    c. Click **Register**.
6. When the new registration's **Overview** page loads, make a note of the **Application (client) ID** and **Directory (tenant) ID** for later use.
7. While still viewing the new registration in the Azure portal, select the **Certificates & secrets** tab in the left-side menu bar.
8. In the **Client secrets** tab in the **Certificates & secrets** page, click **New client secret**.

9. In the **Add a client secret** form:

   a. Enter a description in the **Description** edit field.
   b. Select an appropriate expiration period from the **Expires** drop-down menu.
   c. Click **Add**.
   d. Make note of the new secret's **Value** for future use.

10. While still viewing the new registration in the Azure portal, select the **API permissions** tab on the left-side menu bar.

11. In the **API permissions** page, click **Add a permission**.

12. In the **Request API permissions** form:

    a. Below the **Select an API** header, select **Microsoft APIs**.

    b. Click the **Microsoft Graph** tile.

    c. In the **Microsoft Graph** page, click **Delegated permissions**.

    d. In the **Select permissions** search field, type **cloudpc**. The search results below the search field should update to show the **CloudPC** permission.

    e. Expand the **CloudPC** permission in the search results.

    f. Check the box in front of the **CloudPC.Read.All** permission.

    g. Click **Add permissions** at the bottom of the form.

13. In the **API permissions** page, click **Add a permission** to add a second permission

14. In the **Request API permissions** form:

    a. Below the **Select an API** header, select **Microsoft APIs**.

    b. Click the **Microsoft Graph** tile.

    c. In the **Microsoft Graph** page, click **Application permissions**.

    d. In the **Select permissions** search field, type **cloudpc**. The search results below the search field should update to show the **CloudPC** permission.

    e. Expand the **CloudPC** permission in the search results.

    f. Check the box in front of the **CloudPC.ReadWrite.All** permission.

    g. Click **Add permissions** at the bottom of the form.

15. At this point, note that the Status of the **CloudPC.ReadWrite.All** Application permission indicates consent has not yet been granted. Click the **Grant admin consent for…** option above the **API Permissions** list and confirm you want to provide consent by clicking **Yes** in the dialog that opens.

16. While still viewing the new registration in the Azure portal, select the **Owners** tab on the left-side menu bar.

17. In the **Owners** page, click the **Add owners** button.

18. In the **Owners** form, use the **Search** edit field to locate the user who should own this app registration

19. Check the box in front of this user and click the **Select** button at the bottom of the form.

20. While still viewing the new registration in the Azure portal, select the **Overview** tab on the left-side menu bar.

21. In the **Essentials** section, click the link to the right of the **Redirect URIs** label.

22. In the **Authentication** form:

    a. Click the **Add URI** link in the **Web Redirect URIs** section

    b. In the edit field that appears, enter a redirect URI of the form:

    ```
    https://<enter-your-Leostream-address>/oauth
    ```

    c. Click **Save**.

23. In the **Essentials** section, click the link after the **Managed application in local directory** prompt (note, the prompt may be truncated).

24. In the **Enterprise Application** page for your new registration, select **Users and groups** from the menu bar on the left.

25. In the **Users and groups** page, click **Add user/group**.

26. In the **Add Assignments** form, click the **None Selected** link below **Users and groups**.

27. In the **Users and groups** form, search for the name of the group that contains your Windows 365 users and click **Select**.

28. Back in the **Users and groups** form, click **Assign**.

Your App registration is now ready to use with your Connection Broker.

To integrate Windows 365 with your Leostream Platform:

1. Go to the **> Setup > External Services** page.

2. Click **Add External Service**.

3. In the **Add External Service** form that opens, select **Windows 365** from the **Type** drop-down menu (currently the only available option).

4. Enter a name for your External Service in the **Name** edit field.

5. Enter your client ID into the **Application (client) ID** edit field.

6. Enter your tenant ID into the **Directory (tenant) ID** edit field.

7. Enter the secret key associated with your Leostream application into the **Secret** field.

Chapter 7: Working with Desktops

Registering Desktops in the Uncategorized Desktops Center

The **Uncategorized Desktops** center contains desktops that have registered with the Connection Broker and are not inventoried from another center. See **The Uncategorized Desktops Center** for information on creating an Uncategorized Desktops center.

The **Uncategorized Desktops** center allows you to:

- Manage any physical machines without creating an Active Directory center
- Manage virtual machines from any cloud or hypervisor that does not have an associated Connection Broker center

Registering Desktops Using the Leostream Agent

You can install the Leostream Agent onto any physical or virtual machine you want to register with your Connection Broker. The Leostream Agent contacts the Connection Broker when the agent starts. If this is the first registration the Connection Broker receives from this desktop, the broker places the desktop in the **Uncategorized Desktops** center.

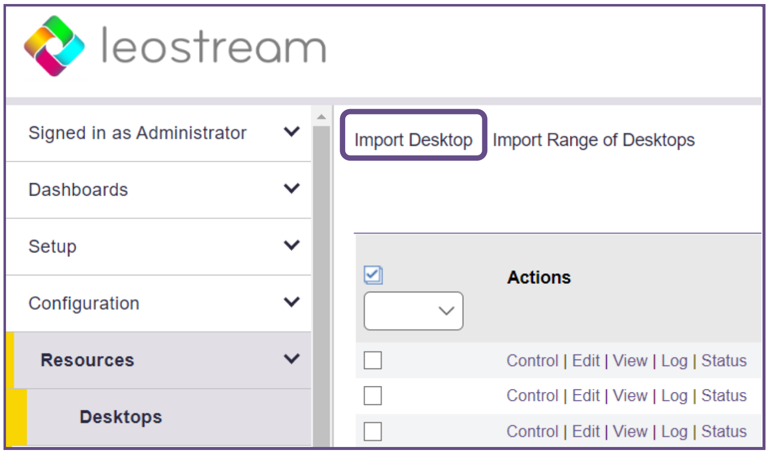
To determine which Connection Broker to register with, the Leostream Agent either queries the DNS server for the Connection Broker SRV record or uses the IP address entered in the Leostream Agent Control Panel dialog (see “Registering Desktops with the Connection Broker” in the Leostream Agent Administrator’s Guide).

The **Availability** property of a desktop registered by the Leostream Agent is determined by the state of the **Set newly-discovered desktops to “Unavailable”** option for the **Uncategorized Desktops** center. If this option is selected, the Connection Broker marks desktops registered by the Leostream Agent as **Unavailable**. Unavailable desktops are not offered to users.

Importing a Desktop by IP Address

You can import one or more desktops into the Connection Broker using the desktop’s IP address. To import an individual desktop:

1. Go to the **> Resources > Desktops** page.
2. Click **Import Desktop**, as shown in the following figure. The **Import Desktop** form opens.


leostream
Signed in as Administrator
Dashboards
Setup
Configuration
Resources
Desktops
Import Desktop
Import Range of Desktops
Actions
Control | Edit | View | Log | Status
Control | Edit | View | Log | Status
Control | Edit | View | Log | Status

3. In the **Name** field, enter a name for the desktop. This name appears in the **Name** column on the **> Resources > Desktops** page.

4. In the **Display Name** field, enter an optional display name for the desktop. This name can be displayed to the user at offer time. If left blank, the Connection Broker uses the value in the **Name** field as the display name.

5. In the **Desktop Attributes** section:

    1. Enter the desktops hostname in the **Hostname** edit field.

    2. Enter the desktop's IP address in the **IP Address** edit field.

    3. Optionally, select the desktop's operating system from the **Operating system** drop-down menu.

    4. Uncheck the **Allow changes to these desktop attributes** option if you do not want the Connection Broker to replace the IP address and operating system you specified with values it learns from the Leostream Agent that registers this desktop.

6. In the **Assignment** section:

    1. In the **Assignment mode** drop-down menu:

        - Select **Policy-driven** to assign this desktop to users via Connection Broker policies.

        - Select **Hard-assigned to specific user** to assign this desktop to a specific user. If you select this option, use the **Assigned User** drop-down menu to select the user to assign to this desktop.

    2. In the **Assign rogue users to this desktop (requires Leostream Agent)** drop-down menu, indicate if the Connection Broker should manage assignments for rogue users who log into the desktop. The setting defaults to the value associated with the primary center that inventories the desktop.

3. In the **Rogue user policy** drop-down menu, if the Connection Broker does manage rogue users, indicate the policy assigned to those users.

4. Use the **Log user into remote desktop as** drop-down menu to force the user to log in as either a domain or local user, regardless of the user's Role and Policy setting.

7. In the **Availability** section:

    1. Select **Unavailable** from the **Desktop status** drop-down menu if the Connection Broker should not offer this desktop to users, for example, because you need to perform some maintenance on the machine before it is ready for use.

    2. Check the **Mark as Unavailable on logout** option to instruct the Connection Broker to mark the machine as Unavailable the next time a user logs out of the desktop. Marking the desktop as unavailable ensures that the Connection Broker will not offer the desktop to another user, for example, so you can perform maintenance on the machine.

    3. Check the **Mark as Unavailable on release** option to instruct the Connection Broker to mark the machine as Unavailable the next time its assignment is released from a user. If this desktop will be hard assigned to a user, use the **Mark as Unavailable on logout** option, instead.

    4. Check the **Allow this desktop to be permanently deleted from disk** option to indicate that the Connection Broker has permission to delete this virtual machine. Do not select this option if this is a persistent VM that should never be terminated by Leostream.

8. In the **Tag Editing** section, assign any optional tags to the desktop. This section is not shown if you have not created any tags (see **Creating Tags**).

9. In the **Leostream Agent** section, enter the **Hostname or IP address** and **Port** for the **Leostream Agent** installed on the desktop. The Connection Broker assumes the agent's hostname or IP address is the same the desktop's unless you specify otherwise.

10. Click **Save**.

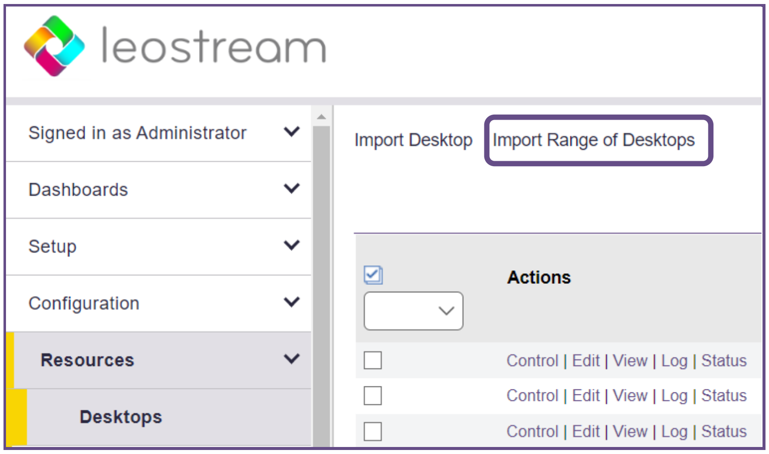
If you are importing a workstation with a PCoIP Remote Workstation Card, save the record and then select the **Edit** action associated with the desktop to associate the PCoIP Remote Workstation Card with the workstation.

Importing a Range of Desktops by IP Address

To import a range of desktops:

1. Go to the **> Resources > Desktops** page.

2. Click **Import Range of Desktops**, as shown in the following figure.


leostream
Signed in as Administrator
Dashboards
Setup
Configuration
Resources
Desktops
Import Desktop
Import Range of Desktops
Actions
Control | Edit | View | Log | Status
Control | Edit | View | Log | Status
Control | Edit | View | Log | Status

The **Import Range of Desktops** form opens.

3. In the **Naming template** field, enter a prefix for the display name for the desktop. This name appears in the **Name** column on the **> Resources > Desktops** page. The Connection Broker adds an index to the end of this name. You can subsequently modify the name of individual desktops.

4. Enter the range of desktop IP addresses in the **IP address range** edit field. Define the range according to mask. See the following Microsoft article for information on specifying a range of IP addresses using a mask;

   http://technet.microsoft.com/en-us/library/cc784393.aspx

5. Optionally, select the desktops' operating system from the **Operating system** drop-down menu. If the desktops have different operating systems, leave this option as **Unspecified** and edit the individual desktops to specify the operating system of each desktop.

6. Uncheck the **Allow changes to these desktop attributes** option if you do not want the Connection Broker to replace the IP address and operating system you specified with values it learns from the Leostream Agent that registers this desktop

7. In the **Assignment** section:

   1. In the **Assignment mode** drop-down menu:

      - Select **Policy-driven** to assign this desktop to users via Connection Broker policies.
      - Select **Hard-assigned to specific user** to assign this desktop to a specific user. If you select this option, use the **Assigned User** drop-down menu to select the user to assign to this desktop.

   2. In the **Assign rogue users to this desktop (requires Leostream Agent)** drop-down menu, indicate if the Connection Broker should manage assignments for rogue users who log into the desktop. The setting defaults to the value associated with the primary center that inventories the desktop.

    3. In the **Rogue user policy** drop-down menu, if the Connection Broker does manage rogue users, indicate the policy assigned to those users.

    4. Use the **Log user into remote desktop as** drop-down menu to force the user to log in as either a domain or local user, regardless of the user’s Role and Policy setting.

8. In the **Availability** section:

    1. Select **Unavailable** from the **Desktop status** drop-down menu if the Connection Broker should not offer this desktop to users, for example, because you need to perform some maintenance on the machine before it is ready for use.

    2. Check the **Mark as Unavailable on logout** option to instruct the Connection Broker to mark the machine as Unavailable the next time a user logs out of the desktop. Marking the desktop as unavailable ensures that the Connection Broker will not offer the desktop to another user, for example, so you can perform maintenance on the machine.

    3. Check the **Mark as Unavailable on release** option to instruct the Connection Broker to mark the machine as Unavailable the next time its assignment is released from a user. If this desktop will be hard assigned to a user, use the **Mark as Unavailable on logout** option, instead.

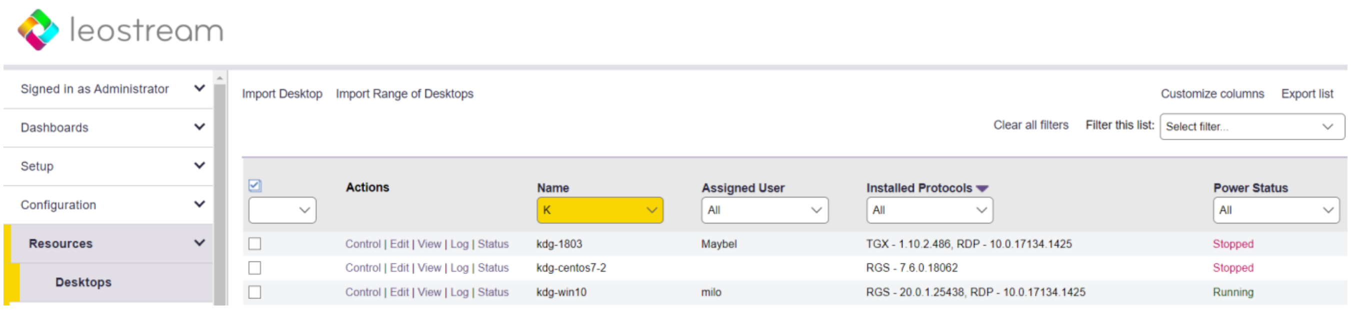
    4. Check the **Allow this desktop to be permanently deleted from disk** option to indicate that the Connection Broker has permission to delete this virtual machine. Do not select this option if this is a persistent VM that should never be terminated by Leostream.

9. In the **Tag Editing** section, assign any optional tags to the desktop. This section is not shown if you have not created any tags (see **Creating Tags**).

10. Click **Save**.

Using the Desktops Page

The **> Resources > Desktops** page, shown in the following figure, lists the desktops inventoried in your Connection Broker, and their characteristics. You can modify the order and type of characteristics displayed on this page by clicking the **Customize columns** link at the top-right side of the page (see **Customizing Tables**).



☑	Actions	Name	Assigned User	Installed Protocols	Power Status
		K	All	All	All
□	Control | Edit | View | Log | Status	kdg-1803	Maybel	TGX - 1.10.2.486, RDP - 10.0.17134.1425	Stopped
□	Control | Edit | View | Log | Status	kdg-centos7-2		RGS - 7.6.0.18062	Stopped
□	Control | Edit | View | Log | Status	kdg-win10	milo	RGS - 20.0.1.25438, RDP - 10.0.17134.1425	Running

Available Desktop Characteristics

Actions

Drop-down menu or list of links indicating the actions you can perform on a desktop. Available actions include the following:

- **Control**: Opens a dialog for controlling the power state of the desktop. See **Power Control for Desktops** for more information.

- **Edit**: Opens the **Edit Desktop** form for this desktop. See **Editing Desktop Characteristics** for more information.

- **View**: Opens a list of available remote viewers.

- **Log**: Displays the log entries and job queue for this desktop.

- **Status**: Queries the Leostream Agent on this desktop. You can use this option to test the Leostream Agent status if is listed as Unreachable. If the desktop has active sessions, you can log these users off by selecting the session and clicking **Log out the selected session**.

- **Release**: Releases an assigned desktop from the user and returns the desktop to the pool. See **Manually Releasing Desktops** for more information. After releasing the desktop, the Connection Broker applies the user's Release Plan, which may log the user out or reboot the desktop. This option does not appear for desktops that are hard-assigned to a user.

- **Upgrade**: If applicable, indicates the Leostream Agent needs to be upgraded.

  ⚠ The Connection Broker runs the same tasks during the upgrade as you specified for the original Leostream Agent installation. The Connection Broker always calls the Leostream Agent upgrade with the reboot flag.

Assigned User
The username associated with the user currently assigned to this desktop.

Assigned from Pool, Assigned from Backup Pool, Assigned from Policy
When a desktop is assigned to a user, the **Assigned from Pool** or **Assigned from Backup Pool** columns show which pool that desktop was pulled.

Availability
Indicates the availability of a desktop, either:

- **Available** indicates that the desktop is available for use.

- **Unavailable** indicates that the desktop has been taken out of service.

- **Duplicate** indicates that another desktop with the same IP address exists in the desktop list. Duplicate machines result when a desktop is imported from multiple centers. You may also see duplicate entries if you have multiple DNS records pointing to an identical machine. See **Handling Duplicate Desktops** for more information

- **Unreachable** indicates that this desktop failed a port check that the Connection Broker performed when offering this desktop to a user. If the user’s policy is configured with a backup pool, when the desktop was marked **Unreachable**, the Connection Broker offered the user an alternative desktop from a backup pool (see **Specifying Backup Pools**). The Connection Broker continues to offer desktops that are marked as **Unreachable**. If subsequent port checks pass, the Connection Broker automatically switches the desktop’s status back to **Available**.

To change the availability of a desktop:

1. Select the **Edit** action for that the desktop. The **Edit Desktop** form opens.

2. In the **Availability** section, use the **Desktop status** drop-down menu to change the desktop availability.

3. Click **Save**.

To simultaneously modify the availability of several desktops, use the bulk edit action for desktops (see **Performing Actions on Multiple Desktops**).

BIOS Serial Number
The desktop’s BIOS serial number. The desktop must have the most recent version of the Leostream Agent installed and this agent must have registered itself with the Connection Broker or this value will be blank.

Boot Time
Indicates the date and time the desktop powered up, as reported by the Leostream Agent on the desktop.

Bulk actions
Checkboxes that allow you to select multiple desktops for performing batch processes. Not all actions are available for batch processing (see **Performing Actions on Multiple Desktops**).

CPU Speed (GHz)

The desktop's processor speed. The desktop must have the most recent version of the Leostream Agent installed and this agent must have registered itself with the Connection Broker or this value will be blank.

Center

The name of the center that is managing this desktop.

Client Assignment Mode

Indicates if this desktop is hard-assigned to a client device. Possible values include:

- **Hard-assigned**: The desktop is hard-assigned to a particular user. The Connection Broker will not include this desktop in any pool or offer it to another user
- **Policy-driven**: The desktop is assigned to a user via a policy.

See **Hard-Assigning a Desktop to a Client** for more information.

Computer Model

The desktop's model number. The desktop must have the most recent version of the Leostream Agent installed and this agent must have registered itself with the Connection Broker or this value will be blank.

Computer UUID

Displays the reported `ComputerSystemProduct` UUID.

Connected

Displays **Yes** if a user is connected to the desktop. Otherwise, displays **No**.

Current Client

The client currently connected to this desktop.

Current Policy

The policy from which this desktop is currently offered.

Current Protocol

Indicates the display protocol currently used to connect to this desktop.

Desktop Type

The type of desktop as determined by the center that registers the desktop, such as VMware.

Display Name

A customizable name that can be displayed to the user when the desktop is offered to the user.

HP Blade Location

For HP ProLiant Blades within an HP BladeSystem enclosure, displays the rack name, enclosure name, and blade location (see **Viewing HP Blade Locations**).

Host UUID

Displays the reported SMBIOS UUID.

Hostname

The hostname as reported by the desktop’s center. For physical machines, the Active Directory services reports the hostname. For virtual machines, the virtualization tools installed on the VM return this information, for example VMtools installed on VMs hosted in VMware. Alternatively, you can install the Leostream Agent on the remote desktop.

IP Address

The IP address as reported by the desktop’s center. For physical machines, the Active Directory services reports the IP address. For virtual machines, the virtualization tools installed on the VM return this information, for example VMtools installed on VMs hosted in VMware. Alternatively, you can install the Leostream Agent on the remote desktop.

IP Address (Private)

For desktops from an OpenStack or AWS center, the IP address seen by the operating system.

IP Address (Public)

For desktops from an OpenStack or AWS center, the floating IP address, if available.

Installed Protocols

Where possible, the display protocols currently supported by this desktop, as reported by the Leostream Agent installed on the desktop.

Last Connect Time

The last time a user connected to the desktop, as reported by the Leostream Agent on the desktop.

Last Disconnect Time

The last time a user disconnected from the desktop, as reported by the Leostream Agent on the desktop.

Last Login Time

The last time a user logged into the desktop, as reported by the Leostream Agent on the desktop.

Last Logout Time

The last time a user logged out of the desktop, as reported by the Leostream Agent on the desktop.

Last Offered Time

The last time a user was offered this desktop. You can configure policies to offer desktops with the older previous offer time.

Leostream Agent Address

The hostname or IP address of the Leostream Agent, if applicable.

Leostream Agent Status

The last known status of the Leostream Agent. The Leostream Agent reports its status to the Connection Broker when the Leostream Agent registers. The Leostream Agent Status column is blank if there is no Leostream Agent installed on the desktop or if a previously registered Leostream Agent is no longer running. The status can take one of the following three values.

- **Running:** The Connection Broker located a Leostream Agent on the desktop and the broker is successfully communicating with the Agent.

- **Unreachable:** The Leostream Agent's incoming port is blocked or closed, or the Leostream Agent does not accept communications from this Connection Broker. This state indicates that the Connection Broker did, at some point, contact the Leostream Agent, but can no longer contact the Agent. An unreachable Leostream Agent may be blocked by a firewall or the desktop it is installed on may not be running. In this state, the Connection Broker cannot use the Agent to distinguish between a user logging out and disconnecting. Therefore, any policy settings based on this information are ignored.

- **Unresponsive:** The Leostream Agent is running on the desktop and the Connection Broker can contact it, but the Leostream Agent is unable to initiate calls back to the Connection Broker. In this state, the Connection Broker may not be able to distinguish between a user logging out and disconnecting. Any of the following configurations may block the Leostream Agent from calling the Connection Broker.
  - A firewall may be blocking the communication
  - The Leostream Agent may not have the correct Connection Broker address
  - The **Connection Broker VIP** on the **> System > Settings** page may not be set correctly (see **Setting the Connection Broker VIP for Leostream Agent Responses**).

Leostream Agent Version
The last known version of the Leostream Agent, if it was ever present. This entry is blank if no Leostream Agent has ever been detected on this desktop. If the desktop shows a value for the Leostream Agent Version, but the Leostream Agent Status is empty, an agent registered with the Connection Broker, but was subsequently uninstalled or stopped.

Logged In
Displays **Yes** if a user is logged into the desktop. Otherwise, displays **No**. If the **User Logged In** column displays **Yes** and the **User Connected** column display **No**, the user is logged in, but disconnected from their remote desktop.

Logged In User
Displays the domain and username of the user who is currently logged into the desktop. The user may not be assigned to the desktop if they logged in from a non-Leostream client.

MAC Address
The desktop's MAC address

Machine Name
The machine name. For physical machines, the Active Directory services reports the machine name. For virtual machines, the virtualization tools, such as VMtools, installed on the VM return the machine name. Alternatively, you can install the Leostream Agent on the remote desktop.

Name
The name given by the management system controlling this desktop.

Notes

Displays the contents of the desktop's **Notes** field. If the field contains 70 characters or more, the Connection Broker truncates the text and displays a **(show all)** link. Click the **(show all)** link to expand the row to display the entire **Notes** field. Use the **(hide all)** link to collapse the row and hide the **Notes** field.

Number of CPUs

The number of CPUs

Number of NICs

The number of network interface cards available on the desktop.

Number of Disks

The number of disks installed in the desktop.

OS Service Pack

For applicable Windows desktops, the installed service pack for the operating system hosted within each virtual or physical machine, as reported by the Leostream Agent installed on the desktop.

OS Version

For Windows desktops, the version of the operating system hosted within each virtual or physical machine, as reported by the Leostream Agent installed on the desktop.

Operating System

The operating system hosted within each virtual or physical machine.

With VMware hosts, the Connection Broker displays the operating system specified when the virtual machine was created. For physical machines, the Connection Broker obtains the operating system from the Leostream Agent installed on the machine.

Other MAC Addresses

For desktops with more than one MAC address, displays all additional MAC addresses.

PCoIP Host Device

For workstations, the PCoIP host card associated with this machine. This property is available only if your Leostream license enables PCoIP support.

PCoIP Host Device 2

For workstations, the optional second PCoIP host card associated with this machine. This property is available only if your Leostream license enables PCoIP support.

Power Status

Reflects the overall power state of the desktop, including the virtual machine, the operating system, and the remote viewer software.

When a virtual machine is first powered up, the power status values may differ from those displayed for the machine in vCenter Server. The Connection Broker considers a desktop as **Running** when the remote viewer service on the desktop is available, not when the virtualization layer considers the desktop as running.

Possible status values include:

Starting	Power is on, operating system (if present) is booting
Running	Power is on, operating system is running
Rebooting	Stopping and then restarting
Resuming	Restarting after being suspended
Reverting	Returning to the pre-snapshot state
Suspending	Memory is being suspended to disk
Suspended	Memory is suspended to disk
Pausing	CPU is halting, Virtual Machine is kept in memory
Paused	CPU is halted, Virtual Machine is kept in memory
Stopping	Power is on, operating system is shutting down
Stopped	Power is off
Failed	Power up failed
Unavailable	The Connection Broker cannot determine the desktop's power state

The **Failed** status generally occurs when you try to power up a machine. If the power up fails, the **Failed** status briefly appears before the status changes to **Stopped**. The **Unavailable** state appears when a desktop is registered by an Active Directory center, and the Connection Broker cannot determine the desktop's power state.

To see the log entries associated with a desktop, select the **Log** action for that desktop. Selecting **Log** opens the relevant log page, showing all the actions that have occurred to that desktop.

RAM (MB)

The total amount of RAM in the desktop. On Linux operating systems, the Leostream Agent determines RAM using the `meminfo` function. When used in a virtual machine, `meminfo` may not include reserved memory, resulting in a RAM in the Connection Broker that differs slightly from the RAM reported in vCenter Server.

Snapshot Available

Indicates if a snapshot is available. If there is a snapshot image of the desktop available, this column displays **Yes**.

Only VMware virtual machines display snapshots.

Tag Group

Displays the tag assigned to this desktop from each of the four different tag groups.

Trunked Client

For desktops with multiple PCoIP Remote Workstation Cards, lists the PCoIP client connected to the secondary workstation card.

Uploaded

Indicates if the desktop record in the Connection Broker was modified using the bulk upload functionality on the **> System > Maintenance** page.

User AD CN, User AD distinguishedName, User AD Email, User AD sAMAccountName, User AD userPrincipalName
The Active Directory attributes associated with the user currently assigned to this desktop.

User Assignment Mode
Indicates if this desktop is hard-assigned to a user. Possible values include:

- **Hard-assigned**: The desktop is hard-assigned to a particular user. The Connection Broker does not consider hard-assigned desktop as available in a pool to offer to another user.
- **Policy-driven**: The desktop is assigned to a user via a policy.

To change the **User Assignment Mode**, edit the desktop. See **Hard-Assigning a Desktop to a User** for more information.

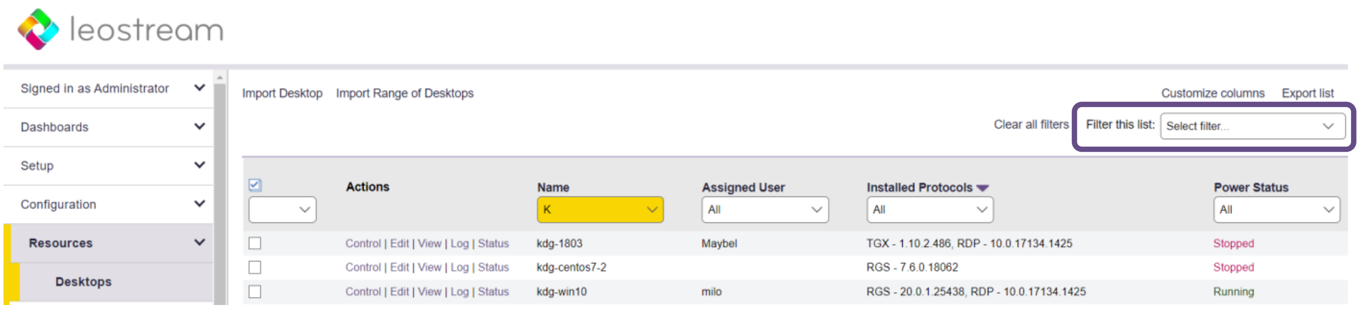
Using License
Indicates if this desktop is consuming a Leostream license. The information in this column applies only if your Leostream Platform is licensed by managed Desktops, not by named Users.

vCenter Server Custom Attributes
If custom attributes are selected on the **> System > Settings** page, up to four additional columns may be available on the **> Resources > Desktops** page. These columns display the value for the selected custom attributes.

vCenter Server “Notes”
Displays the contents of the **Notes** field entered in VMware vCenter Server. If the field contains 70 characters or more, the Connection Broker truncates the text and displays a **(show all)** link. Click the **(show all)** link to expand the row to display the entire field. Use the **(hide all)** link to collapse the row and hide the field.

Filtering the Desktop List

You can filter the list of desktops in the **> Resources > Desktops** page using the **Filter this list** drop-down menu, shown in the following figure.



Filter this list: Select filter...

☑	Actions	Name	Assigned User	Installed Protocols	Power Status
		K	All	All	All
□	Control | Edit | View | Log | Status	kdg-1803	Maybel	TGX - 1.10.2.486, RDP - 10.0.17134.1425	Stopped
□	Control | Edit | View | Log | Status	kdg-centos7-2		RGS - 7.6.0.18062	Stopped
□	Control | Edit | View | Log | Status	kdg-win10	milo	RGS - 20.0.1.25438, RDP - 10.0.17134.1425	Running

Select the **Select filter** option to list all desktops currently registered with the Connection Broker, divided into a series of pages if applicable.

Every time you create a desktop pool (see **Chapter 8: Creating Desktop Pools**) the Connection Broker automatically creates a corresponding filter in the drop-down menu. Select one of the pool filters to limit the list to desktops within the chosen pool.

To edit an existing filter, or create a new filter:

1. Select **Edit an existing filter** or **Create a new filter** from the **Filter this list** drop-down menu.
2. If editing an existing filter, select the filter to edit from the **Select a filter** drop-down menu.
3. Enter a name for the filter in the **Filter name** edit field.
4. Select the pool to associate with this filter from the **Pool** drop-down menu.
5. Use the controls in the **Include data that matches** section to create rules that further filter the desktops from this pool.
6. By default, only the user that creates a filter can use it. To allow other user to access your filter, check the **Share the filter with other users** option when you create the filter. This filter then appears in the **Filter this list** drop-down menu of other users that log into this Connection Broker. Shared filters are useful if you have additional users with administrative privileges in the Connection Broker, for example, a Help Desk group that can manage the desktops.
7. Click **Save**.

Editing Desktop Characteristics

Use the **Edit Desktop** page to view and modify desktop characteristics. The information to the right of the **Edit Desktop** form provides details about the desktop, including any duplicate desktops registered with the Connection Broker

You cannot edit a desktop marked as a duplicate (see **Handling Duplicate Desktops**). You must use the **Edit Desktop** page of the master desktop to edit the desktop attributes.

The form allows you to modify:

- **Name**: This field appears only if you are editing a desktop in the **Uncategorized Desktops** center. Specify a name to use for this desktop, typically the machine name.
- **Display name**: Optionally specify a customized name to display when this desktop is offered to a user. If this field is left blank, the display name defaults to the desktop name
- **Hostname**: Specify the desktop’s hostname. In general, modify this field only if the Connection Broker is unable to correctly determine the desktop’s hostname. If you select the **Allow changes to these desktop attributes** option, the Connection Broker may overwrite any changes you made to the hostname when the broker subsequently scans the desktop’s center or receives a registration from the desktop’s installed Leostream Agent.

- **IP address**: Specify the desktop's IP address. In general, modify this field only if the Connection Broker is unable to correctly determine the desktop's IP address. If you select the **Allow changes to these desktop attributes** option, the Connection Broker may overwrite any changes you made to the IP address when the broker subsequently scans the desktop's center or receives a registration from the desktop's installed Leostream Agent.

- **Operating system**: Specify the desktop's operating system. If you select the **Allow changes to these desktop attributes** option, the Connection Broker may overwrite any changes you made to the operating system when the broker subsequently scans the desktop's center or receives a registration from the desktop's installed Leostream Agent.

- **Allow changes to these desktop attributes**: By default, the Connection Broker gather information about the desktop's attributes from the center containing the desktop and the installed Leostream Agent. To manually overwrite the desktop attributes, uncheck the **Allow changes to these desktop attributes** option.

- **Assignment mode**:

    - Select **Policy-driven** to assign this desktop to users via policy logic (see **Chapter 12: Configuring User Experience by Policy**).

    - Select **Hard-assigned to specific user** to limit this desktop to a user. If you choose this option, select the user from the **Assigned user** drop-down menu. See **Desktop Assignment Modes** for more information on the different types of assignment modes.

- **Rogue user settings:**
    - In the **Assign rogue users to this desktop (requires Agent)** drop-down menu, indicate if the Connection Broker should manage assignments for rogue users who log into the desktop. The setting defaults to the value associated with the primary center that inventories the desktop.

    - In the **Rogue user policy** drop-down menu, if the Connection Broker does manage rogue users, indicate the policy assigned to those users.

- Use the **Log user into remote desktop as** drop-down menu to force the user to log in as either a domain or local user, regardless of the user's Role and Policy setting.

- Use the **Log user into remote desktop with this *X*** fields to specify optional fixed desktop operating system credentials:

    - **Username:** An optional username that can be used with the {VM:USERNAME_OVERRIDE} dynamic tag in Protocol Plans to log the user into their remote desktop using this username instead of the user's Leostream username.

    - **Password:** Enter the optional user's password to use with the {VM:PASSW0RD_OVERRIDE} dynamic tag in Protocol Plans to log the user into their remote desktop.

  - **Domain:** Enter the optional user’s domain to use with the {VM:DOMAIN_OVERRIDE} dynamic tag in Protocol Plans to log the user into their remote desktop.

- **Desktop status**:

  - **Available** indicates the desktop can be assigned to a user.
  - **Unavailable** indicates the desktop cannot be assigned to a user.
  - **Duplicate** indicates this desktop is a duplicate of another desktop in the list. Duplicate machines result, for example, when a desktop is imported from multiple centers. Duplicate desktop records are not considered as part of any pool.

- Check the **Mark as Unavailable on logout** option to instruct the Connection Broker to mark the machine as Unavailable the next time a user logs out of the desktop. Marking the desktop as unavailable ensures that the Connection Broker will not offer the desktop to another user, for example, so you can perform maintenance on the machine.

- Check the **Mark as Unavailable on release** option to instruct the Connection Broker to mark the machine as Unavailable the next time its assignment is released from a user. If this desktop is hard assigned to a user, use the **Mark as Unavailable on logout** option to perform this action, instead.

- Check the **Allow this desktop to be permanently deleted from disk** option to indicate that the Connection Broker has permission to delete this virtual machine. Do not select this option if this is a persistent VM that should never be terminated by Leostream. Machines inventoried from an Active Directory or Uncategorized Desktops center cannot be marked as deletable.

- **Tag Editing**: (Not shown in the previous figure) Use the drop-down menus in this section to select the appropriate tags from any tag group. The **Tag Editing** section does not appear if you have not defined any tags (see **Defining Pools Using Tags**).

- **Leostream Agent**: Sets an alternate IP address for the Leostream Agent on this desktop. Leave blank if the Leostream Agent is available on the same IP address as the desktop

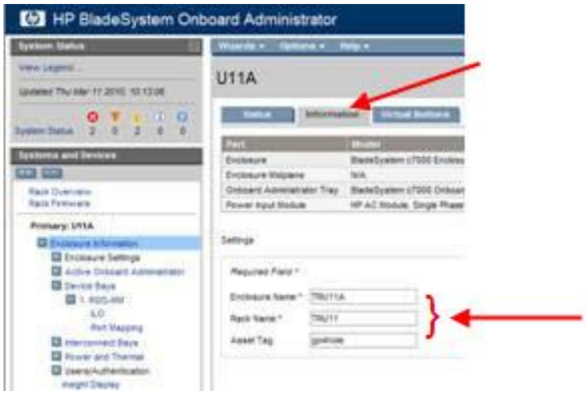
- **Plans**: The **Protocol** drop-down menu allows you to hard-code the display protocol used to connect to this desktop by all users and from all client devices. The desktop’s selected protocol plan overrides any other protocol plans set at the policy, location or user level.

- **PCoIP Host Device**: Selects the PCoIP host cards installed on this desktop, if relevant.

Viewing HPE Blade Locations

The Connection Broker can display the physical location of HPE ProLiant Blades within an HPE BladeSystem enclosure, if the Leostream Agent is installed on the blade.

To correctly display blade location, you must enter the blade location, enclosure name, and rack name in the BladeSystem Onboard Administrator, shown in the following figure. For the Leostream Agent to correctly pick up the location information, after entering the information, reboot the blade.



Part	Model
Enclosure	BladeSystem c7000 Enclosure
Enclosure Midplane	N/A
Onboard Administrator Tray	BladeSystem c7000 Onboard
Power Input Module	HP AC Module, Single Phase

Settings

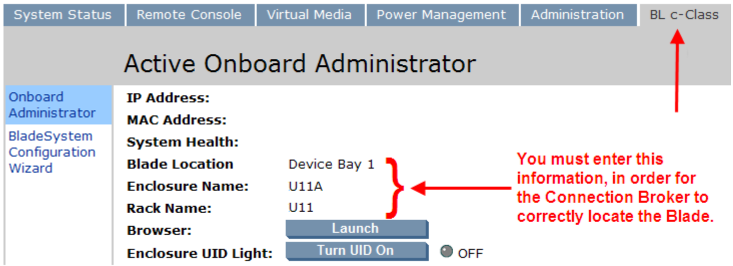
Required Field *

Enclosure Name *: TRU11A

Rack Name *: TRU11

Asset Tag: [illegible]

After you enter this information into the BladeSystem enclosure, you can view the location in the Onboard Administrator for the individual blade on the **BL c-class** tab, shown in the following figure.



IP Address:

MAC Address:

System Health:

Blade Location Device Bay 1

Enclosure Name: U11A

Rack Name: U11

Browser:

Enclosure UID Light: OFF

You must enter this information, in order for the Connection Broker to correctly locate the Blade.

The Connection Broker queries the Leostream Agent installed on the blade for the location information. The Connection Broker then displays the location information on the right side of the blade’s **Edit Desktop** page.

You can display this information directly on the **> Resources > Desktops** page by adding the **HPE Blade Location** column, which is off, by default. See **Customizing Tables** for information on adding this column to the **> Resources > Desktops** page.

After you add the **HPE Blade Location** column, any HPE blade that provides location information includes a partial display of this information.

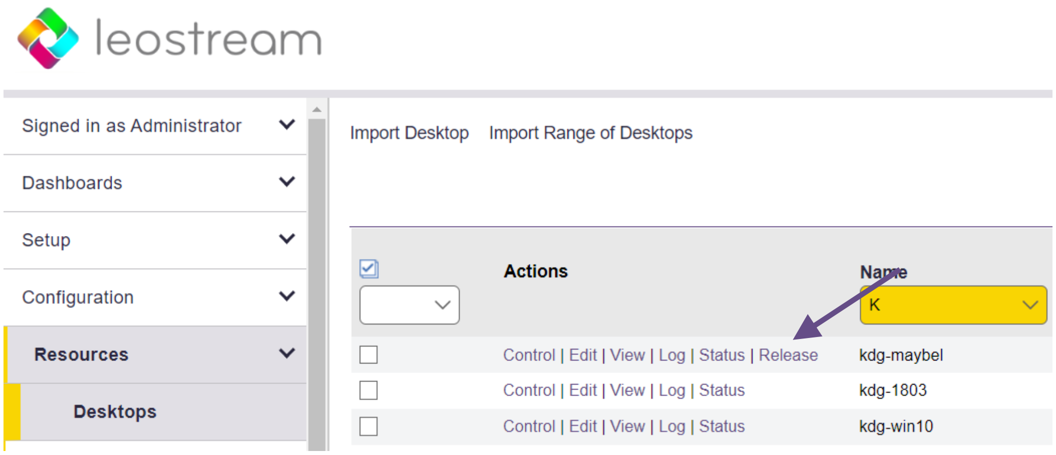
The information is displayed in the following format.

```
Rack: Enclosure: Blade location
```

Where *Rack*, *Enclosure*, and *Blade location* are replaced with the values for the rack name, enclosure name, and blade location you entered in the BladeSystem Onboard Administrator.

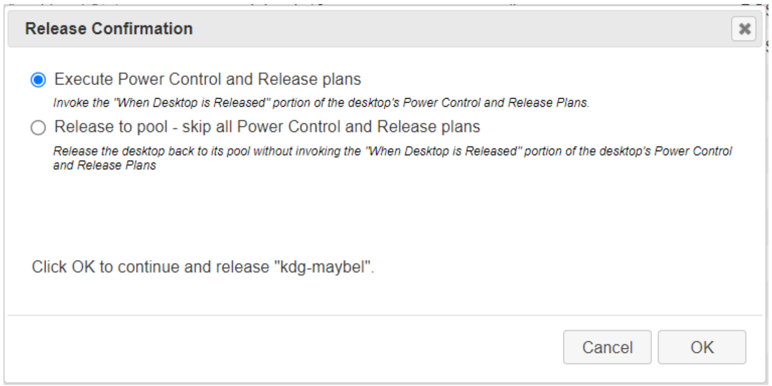
Manually Releasing Desktops

You can release a desktop that is assigned to a user by selecting the **Release** action associated with the desktop, as shown in the following figure.



☑	Actions	Name
		K
□	Control | Edit | View | Log | Status | Release	kdg-maybel
□	Control | Edit | View | Log | Status	kdg-1803
□	Control | Edit | View | Log | Status	kdg-win10

The Connection Broker prompts you to confirm the release action. When manually releasing a desktop, you can indicate what actions the Connection Broker should take, using the dialog shown in the following figure.



Release Confirmation

● Execute Power Control and Release plans

Invoke the "When Desktop is Released" portion of the desktop's Power Control and Release Plans.

○ Release to pool - skip all Power Control and Release plans

Release the desktop back to its pool without invoking the "When Desktop is Released" portion of the desktop's Power Control and Release Plans

Click OK to continue and release "kdg-maybel".

- Select **Execute Power Control and Release plans** and click **OK** to execute all applicable actions in the user's Release and Power Control plan. Depending on how you configured the user's plans, selecting this option may log out the user and power off or terminate the machine, for example.

  If the Release Plan suspends logging out the user or deleting the virtual machine, the Connection Broker places associated jobs in the Job Queue and changes the status of the desktop to **Releasing**. You can click the **Releasing** action to view the current status of the scheduled jobs.

- Select **Release to pool – skip all Power Control and Release plans** and click **OK** to unassign the desktop without taking further actions. This option is useful if you are removing an assignment after a failed connection or do to other issues that resulted in an incomplete assignment.

  If you need to log the user out of the machine after releasing the assignment, use the desktop's **Status** option on the **> Resources > Desktops** page to query the Leostream Agent for the user's session and request the Leostream Agent to log out the user. Because the user is no longer assigned to the machine, no Release or Power Control plans are invoked.

Use the **Release** bulk action if you need to release several desktops, simultaneously (see **Bulk Release,**

Refresh, and Remove for Desktops).

The Connection Broker Web interface may be unresponsive while the log out action is taking place. If you encounter this issue, instead use the bulk action to release the desktop (see **Bulk Release, Refresh, and Remove for Desktops**). Bulk actions are submitted as jobs to the work queue, freeing up the Connection Broker web interface to respond to new requests.

Using Virtual Machine Snapshots

VMware virtualization layers allow you to take snapshots of running or stopped virtual machines. This snapshot contains a complete system image (disk and memory) of a virtual machine at a moment in time, providing a way to restore a machine to a previous state. Users can continue to use machines after a snapshot is taken.

You can use snapshots to revert a desktop back to a known state after a user is finished using that desktop. The power control plan assigned to the desktop decides when to revert to a snapshot. See **Power Control Plans** for more information.

Performing Actions on Multiple Desktops

You can perform the following actions simultaneously on several desktops:

- **Control:** Perform power control actions, such as shut down or start up, on a group of desktops. You must have the necessary Role permissions to complete the requested power control action.

- **Delete:** Deletes a virtual machine from disk within its virtualization host. The desktop must be marked as deletable for the Connection Broker to allow this action

- **Edit**: Perform actions such as upgrading installed Leostream Agents, changing the desktop status, and converting a desktop to a multi-user center. The remaining bulk actions are described in the following sections.

- **Scan**: If one of the selected desktops is part of an Active Directory center, perform a refresh of that center.

- **Release**: Releases the desktop from the assigned user. The Connection Broker immediately performs any actions on the associated release and power control plans.

- **Remove**: Removes these desktops from the **> Resources > Desktops** page but retains the virtual machine in its virtualization host. The desktops may reappear after a subsequent scan of a center that inventories this virtual machine.

- **Upgrade:** Push out upgrades to the Leostream Agent installed on the selected desktops. The desktop must have an existing Leostream Agent.

- **Deploy:** Deploy a Windows operating system to an HPE Moonshot System node. See the Leostream and HPE Moonshot System Reference Architecture for complete details.

To perform an action on multiple desktops:

1. In the **Bulk Action** column, select the checkbox associated with each desktop. To select all the listed desktops, click the check box at the top of the **Bulk action** column (see **Performing Bulk Actions**).

   If the check boxes are not visible, click the **customize** link at the bottom of the page and add the **Bulk actions** column. See **Customizing Tables** for more information.

2. Select the action to perform from the drop-down menu at the top of the column of checkboxes.

Removing User's Affinity to Previously Assigned Desktops

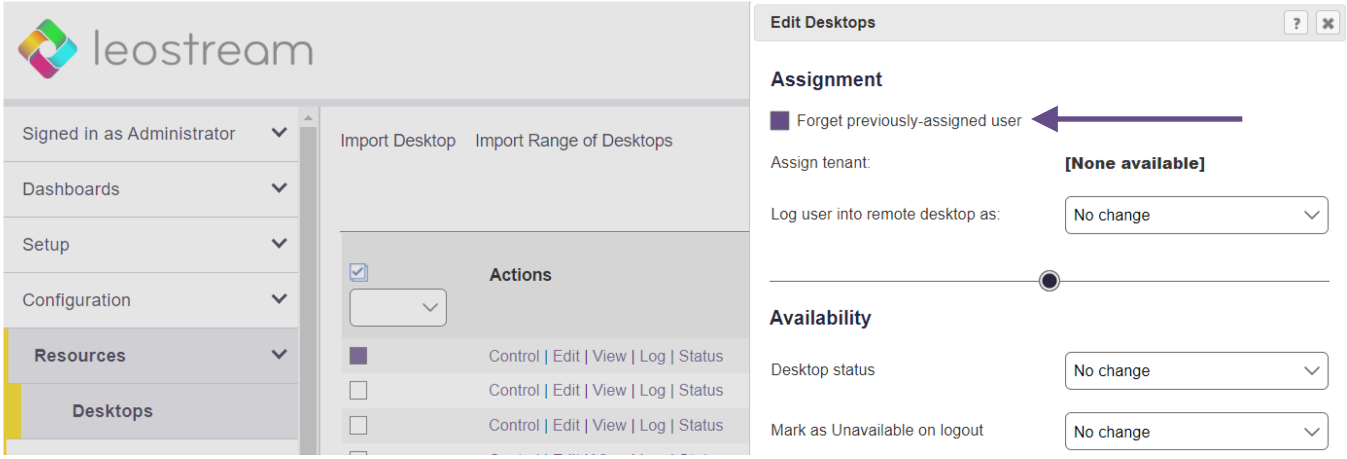
When the user's policy selects **Favor desktops previously assigned to this user** from the **Desktop selection preference** drop-down menu, the Connection Broker always attempts to offer the user the last desktop they were assigned from a pool.

In some cases, you may want to force the Connection Broker to select a new desktop from the pool, instead of automatically offering the last assigned desktop, for example, if you need to perform maintenance on the user's desktop. You can remove the user's affinity to their previously assigned desktop, as follows.

1. Go to the **> Resources > Desktops** page.

2. In the **Bulk Action** column, select the checkbox associated with the user's desktop.

3. Select the **Forget previously assigned user**, as shown in the following figure.


leostream
Signed in as Administrator
Dashboards
Setup
Configuration
Resources
Desktops
Import Desktop
Import Range of Desktops
Actions
Control | Edit | View | Log | Status
Control | Edit | View | Log | Status
Control | Edit | View | Log | Status
Edit Desktops
?
✖

Assignment

■ Forget previously-assigned user

Assign tenant: **[None available]**

Log user into remote desktop as: No change

Availability

Desktop status: No change

Mark as Unavailable on logout: No change

4. Click **Save**.

The next time the user logs into the Connection Broker, the broker will select a desktop from the pool using the rules defined in the policy, without giving preference to this desktop.

Changing the Availability of Multiple Desktops

When editing multiple desktops, the setting in the **Desktop status** drop-down menu indicates if the desktops are available for assignment to a user. To change the availability of all the desktops being edited, select either **Available** or **Unavailable** from the **Desktop status** drop-down menu. After you save the bulk **Edit** form, all the edited desktops have the selected availability.

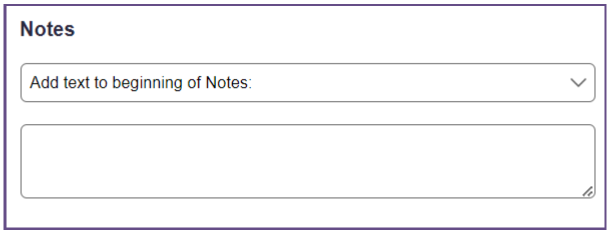
Updating the Leostream Agent on Multiple Desktops

You can use the **Upgrade** option in the **Bulk actions** column to push out Leostream Agent upgrades to multiple desktops. Alternatively, you can use the bulk **Edit** form to upgrade the Leostream Agent on all selected desktops by checking the **Upgrade Agent to latest version** option in the **Leostream Agent** section.

When you request a Leostream Agent upgrade, the Connection Broker updates all desktops running a Leostream Agent older than the version shown on the **> Dashboards > Downloads** page.

Updating Notes on Multiple Desktops

The **Bulk Edit** for allows you to add a common note to multiple desktops. The common note does not replace any existing note. Instead, use the drop-down menu in the **Notes** section of the **Bulk Ed**it form, shown in the following figure, to indicate if the note should be added to the beginning of the note or placed after any existing note.



- Select **Add text to beginning of Notes** to insert the text entered in the **Bulk Edit** notes field in front of the existing notes for each selected desktops.

- Select **Add text at the end of Notes** to append the text entered in the **Bulk Edit** notes field after the notes already entered for each selected desktop.

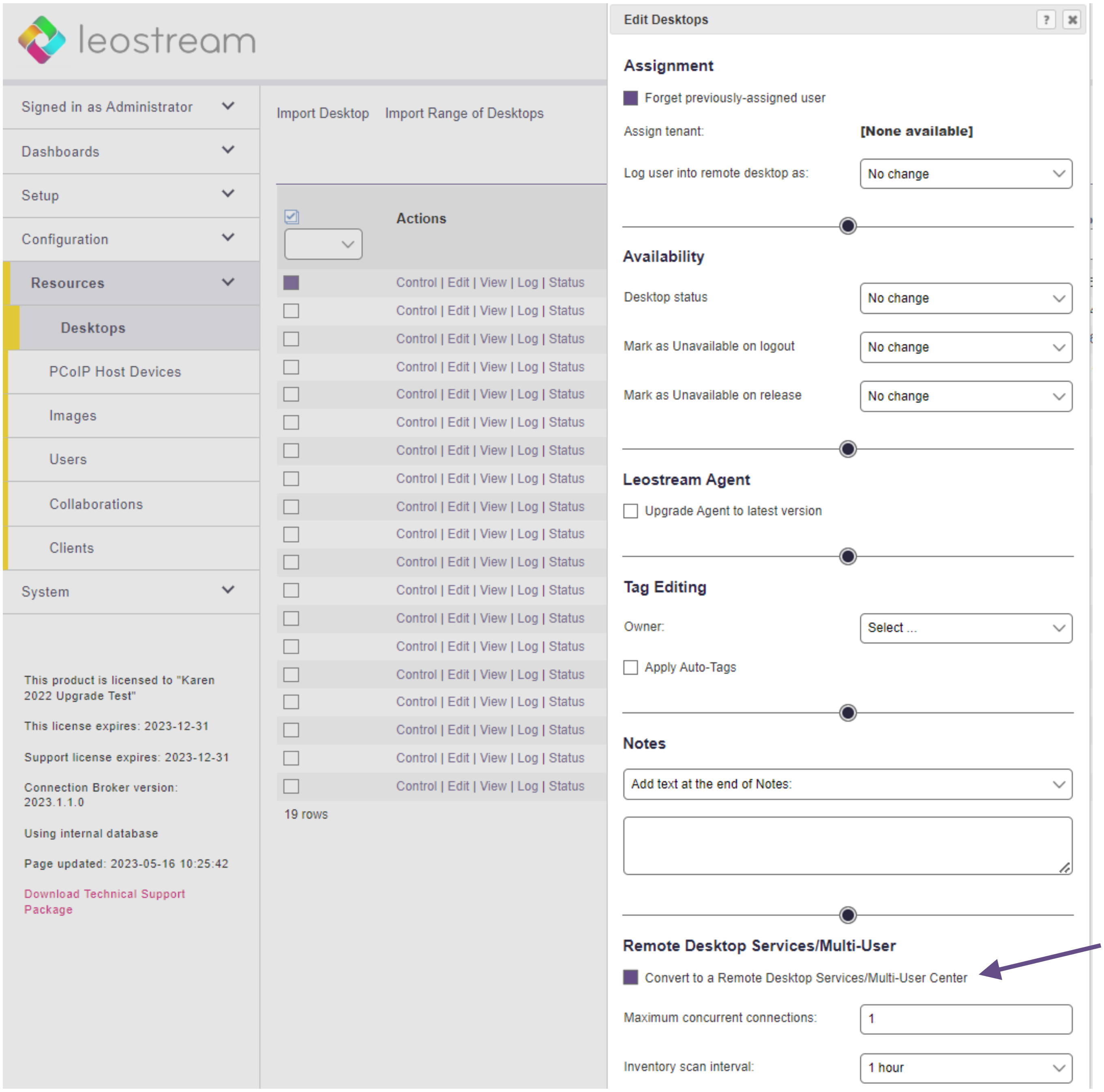
Applying Tags to Multiple Desktops

See **Bulk Tagging Desktops** for a description of using the **Tag Editing** section in the bulk **Edit** page.

Converting Desktops to Remote Desktop Services / Multi-User Centers

You can use the bulk **Edit** action to convert desktops listed on the **> Resources > Desktops** page into Remote Desktop Services / Multi-User Centers. If, for example, you inventoried Windows Servers using an Active Directory center, this feature simplifies setting up the RDS sessions to offer out to users.

To convert the desktops into centers, in the **Edit Desktops** form, select the **Convert to a Remote Desktop Services / Multi-User Center** option, as shown in the following figure.



☑	Actions
■	Control | Edit | View | Log | Status
□	Control | Edit | View | Log | Status
□	Control | Edit | View | Log | Status
□	Control | Edit | View | Log | Status
□	Control | Edit | View | Log | Status
□	Control | Edit | View | Log | Status
□	Control | Edit | View | Log | Status
□	Control | Edit | View | Log | Status
□	Control | Edit | View | Log | Status
□	Control | Edit | View | Log | Status
□	Control | Edit | View | Log | Status
□	Control | Edit | View | Log | Status
□	Control | Edit | View | Log | Status
□	Control | Edit | View | Log | Status
□	Control | Edit | View | Log | Status
□	Control | Edit | View | Log | Status
□	Control | Edit | View | Log | Status
□	Control | Edit | View | Log | Status
□	Control | Edit | View | Log | Status

19 rows

This product is licensed to "Karen 2022 Upgrade Test"

This license expires: 2023-12-31

Support license expires: 2023-12-31

Connection Broker version: 2023.1.1.0

Using internal database

Page updated: 2023-05-16 10:25:42

Download Technical Support Package

Assignment

■ Forget previously-assigned user

Assign tenant: **[None available]**

Log user into remote desktop as: No change

Availability

Desktop status: No change

Mark as Unavailable on logout: No change

Mark as Unavailable on release: No change

Leostream Agent

□ Upgrade Agent to latest version

Tag Editing

Owner: Select ...

□ Apply Auto-Tags

Notes

Add text at the end of Notes:

Remote Desktop Services/Multi-User

■ Convert to a Remote Desktop Services/Multi-User Center

Maximum concurrent connections: 1

Inventory scan interval: 1 hour

After selecting this option, enter the number of sessions to allocate for each center in the **Maximum concurrent connections** edit field and set the interval at which the Connection Broker queries the Leostream Agent on the server using the **Inventory scan interval** drop-down.

After you click **Save**, the Connection Broker automatically creates a Remote Desktop Services / Multi-User center for each selected desktop and initializes the specified number of sessions for each center. The new centers appear on the **> Setup > Centers** page, while the new sessions appear on the **> Resources > Desktops** page. The Connection Broker marks the original desktops as **Unavailable** on the **> Resources > Desktops** page, to ensure that the sessions, and not the desktop, are offered to users via policies.

Bulk Release, Scan, Remove and Delete for Desktops

After you select either the **Release**, **Scan**, **Remove**, or **Delete** bulk action, the Connection Broker opens a confirmation window. See the section on **Manually Releasing Desktops** for more information on the options available when bulk releasing desktops.

Click **OK** to proceed with the action or **Cancel** to close the window without completing the action. The **Remove** action marks the virtual machine's record as deleted in the Connection Broker database and removes the desktop from the **> Resources > Desktops** page.

The **Delete** option terminates the virtual machine and removes it from disk in your virtualization environment. The **Delete** option is not reversible and requires the **Edit Desktop** page to have the **Allow this desktop to be permanently deleted from disk** option selected.

When scanning multiple desktops, the Connection Broker scans every center that contains those desktops.

Submitting a bulk action places a job in the Connection Broker work queue, which you can see on the **> System > Job Queue** page.

Deleting Virtual Machines from Disk

The Connection Broker has permission to delete from disk any virtual machine that selects the **Allow this desktop to be permanently deleted from disk** option on its **Edit Desktop** form. You can use release plans to schedule virtual machines to be deleted when the desktop's assignment is broker (see **Example: Deleting Virtual Machines After Use**.)

In addition, you can manually delete virtual machines using the **Delete** bulk action on the **> Resources > Desktops** page.

To delete one or more virtual machines:

1. In the **Bulk Action** column, select the checkbox associated with each virtual machine to delete.

   If the check boxes are not visible, click the **Customize columns** link at the top-right of the page and add the **Bulk actions** column. See **Customizing Tables** for more information.

2. Select the **Delete** action from the drop-down menu at the top of the column of checkboxes.

3. The Connection Broker opens a confirmation dialog, indicating that this action is not reversible. Click **OK** only if you want to permanently delete the virtual machine from disk.

The Connection Broker deletes all the selected virtual machine that check the **Allow this desktop to be permanently deleted from disk** option. If that option is not checked, the Connection Broker does not delete the VM.

Handling Duplicate Desktops

If the same desktop (physical or virtual) is registered with the Connection Broker from multiple centers, the Connection Broker marks the **Availability** of a single record for the desktop as **Available** and the remaining records as **Duplicate** on the **> Resources > Desktops** page. Duplicates may occur, for example, if you create both a VMware and an Active Directory center in your Connection Broker and you are managing domain-joined virtual machines. All duplicate destkop records become aliases for the available desktop record.

The Connection Broker sets the available desktop as the record registered from the center that provides the most power control options, as follows:

1. The record registered from a cloud or virtualization layer, such as VMware vCenter Server
2. The record registered from an Active Directory center
3. The record manually registered with the **Uncategorized Desktops** center

If you create a center associated with an Active Directory tree that contains multiple records for the same desktop, the Connection Broker marks a single instance as available.

The Connection Broker uses the union of desktop attributes from the **Available** and **Duplicate** desktop records when determining if a desktop is part of a pool, as well as if a desktop is policy-offered to a user. The Connection Broker places only the **Available** desktop into the pool. Desktops that are marked as **Duplicates** are never members of a pool nor are they offered to users.

The text on the right-hand side of the **Edit Desktop** page shows the union of the attributes for all available and duplicate desktop instances. Use the **Edit Desktop** page associated with the available desktop to edit the desktop attributes. You cannot modify desktop attributes on the **Edit Desktop** page associated with a duplicate desktop record.

Power Control for Desktops

The Connection Broker uses a combination of methods to power control hosted desktops, including (in order) calling out to the Leostream Agent, leveraging the hosting platform APIs, and using Wake-on-LAN or IPMI. The types of power control actions the Connection Broker supports include the following.

- **Shutdown**: Preforms a graceful operating system shutdown. If the desktop has an operational Leostream Agent, the Connection Broker first attempts to call the agent to shutdown the operating system. Otherwise, if available, the Connection Broker uses the hosting platform API.

- **Reboot**: Performs a graceful reboot of the operating system. If the desktop has an operational Leostream Agent, the Connection Broker first attempts to call the agent to reboot the operating system. Otherwise, if available, the Connection Broker uses the hosting platform API.

- **Power off**: Analogous to pulling the plug, forcefully powers off the desktop. If the desktop has an operational Leostream Agent, the Connection Broker first attempts to call the agent to power off the desktop. Next, if available, the Connection Broker calls the hosting platform API. Finally, for physical machines, the Connection Broker.

- **Hard Reset**: For IPMI-enabled physical workstations, issues an IPMI reset for the machine.

The Connection Broker provides different levels of power control, depending on the center that registers the desktop. If a desktop is inventoried from multiple centers, such as a Windows virtual machine that is inventoried from a VMware and an Active Directory center, the center containing the Available desktop record determines the level of power control the Connection Broker has for that desktop. Centers that contain any Duplicate records are not considered when executing power control actions.

- **AWS, Azure, Google Cloud Platform:** Shutdown, power off, start, and reboot is available for virtual machines hosted in all cloud Centers. Suspend is available for Azure virtual machines and places the VM in hibernation. You can reboot the machine gracefully using the **Reboot** option or forcefully using the **Power Off and Start** option. The Connection Broker uses the virtualization layer APIs to perform the power control action.

  Virtual machines hosted in Azure are returned to a Deallocated state when any shutdown or power off action is taken.

- **VMware, Red Hat:** Shutdown, power off, suspend, resume, start, and reboot are available for virtual machines hosted in VMware vSphere.

  If a power down or reboot is requested for a VMware virtual machine that does not have a running version of VMware Tools, the Connection Broker attempts to power control that VM using the Leostream Agent, if an agent is present.

  The **Reboot** options first attempts to shut down the guest OS. In VMware virtualization layers, this is identical to the reboot option and requires fewer resources then completely shutting down the VM. If the Connection Broker cannot shutdown the guest OS, it completely shuts down the desktop before the restart.

- **OpenStack:** Shutdown, power off, suspend, pause, resume, start, and reboot are available for VMs hosted in OpenStack. Pause stores the instance state in memory (RAM) while suspend stores the state on disk. In addition, OpenStack VMs can be placed in a shelved state.

- **Nutanix AHV, Scale Computing Platform, VergeIO:** Shutdown, power off, start, and reboot are available for VMs hosted in hyperconverged infrastructure centers. Suspend and resume is not supported for virtual machines hosted on these platforms.

- **Active Directory and Uncategorized Desktops:** Shutdown and reboot is available for desktops with an installed Leostream Agent. Reboot must be done using the **Reboot** option.

  Start is available for physical desktops that are support Wake-on-LAN or IPMI. In addition to **Start**, the **Power off** and **Hard Reset** options are available for desktops and workstations that support IPMI.

- **Remote Desktop Services Sessions:** No power control is available for servers running RDS or multi-user sessions.

Determining Power State for Active Directory or Uncategorized Desktops

The Connection Broker uses the VM management system to determine the power state of virtual machines registered from a virtualization, cloud, or hyperconverged center. To determine the power state of desktops from an Active Directory or Uncategorized Desktops center, the Connection Broker polls the desktops in the center, checking for an open port from a list of ports that includes display protocol ports, Leostream Agent ports, and a set of common third-party ports. If any of the scanned ports are open, the Connection Broker marks the desktop as **Running**. If all ports are closed, the Connection Broker marks the desktop as **Stopped**.

Please contact **support@leostream.com** for a full list of the ports included in a power state scan.

By default, when new desktops appear in the Connection Broker from an Active Directory or Uncategorized Desktops center, their **Power Status** is shown as **Unknown**. During the poll, the Connection Broker marks the desktop as **Running** if it finds an open display protocol or Leostream Agent port. If the Connection Broker cannot locate the desktop, for example the desktop has no IP address and the hostname does not resolve, the desktop power status remains set to **Unknown**.

Desktops from Active Directory or Uncategorized Desktops centers that are marked as **Running** will continue to be marked as **Running** if the machine is powered off or shutdown, but the Connection Broker does not receive a Guest OS Shutdown notification from the Leostream Agent. Desktops in these centers must have an installed and running Leostream Agent in order for the destkop be marked as **Stopped**.

Manually Changing a Desktop’s Power State

To manually power control a desktop, on the **> Resources > Desktops** page, select the **Control** action associated with the desktop. Select one of the available power control options and click **OK**. When using the bulk action for power control, all power control options are displayed, although not all may apply to the selected desktops.

All **Power Off** options forcefully power off the machine, with no attempt to gracefully shutdown the operating system.

Configuring Wake-on-LAN for Physical Desktops

Your Leostream license determines if you can use Wake-on-LAN to power on physical machines.

To use Wake-on-LAN to power control a physical machine, the target desktop must be on the same subnet as at least one of the Connection Brokers in your cluster and the machine must be powered on when the Connection Broker first discovers it. In addition, the machine must have an installed Leostream Agent that is successfully communicating with the Connection Broker.

The Leostream Agent provides the Connection Broker with a list of the machine’s MAC addresses. When Wake-on-LAN is enabled, the Connection Broker sends out a magic packet to every MAC address in the list every time a request is made to power up a physical machine.

Use the **Wake-on-LAN port** edit field on the **> System > Settings** page to indicate the port that should receive the Wake-on-LAN magic packets from the Connection Broker. This setting is found in the

Connection Broker Monitoring and Performance Tuning section of the page.

If the Connection Broker is not successfully powering up one of your physical desktops, ensure that the Connection Broker has the correct MAC address listed to the right of the **Edit Desktop** page. You can use the **Customize columns** link on the **> Resources > Desktops** page to add the MAC address column to the page, to make it easy to inspect this value for multiple desktops.

The machine’s NIC must *not* be password protected for the Connection Broker to power up the machine using a Wake-on-LAN packet. In addition, the Connection Broker and desktop must be in the same subnet.

Configuring IPMI for Physical Desktops

The Connection Broker defaults to using Wake-on-LAN for physical desktops. If you have workstations that are IPMI-enabled, the Connection Broker can leverage the IPMI device for power control, including providing end-users with an option to perform a hard reset on their machine.

The Connection Broker uses one of the following IPMI commands, depending on if your Connection Broker Power Control Plans or Policies are configured to perform a soft reboot or a forceful power off and start.

- Reboot: `chassis power reset`
- Power off and Start: `chassis power cycle`
- Hard Reset: `chassis power cycle`

: The **Reboot** and **Power off and Start** options first attempt to power cycle the machine using the Leostream Agent then by making a Center API call before sending the IPMI command. The **Hard Reset** option immediately sends the IPMI command.

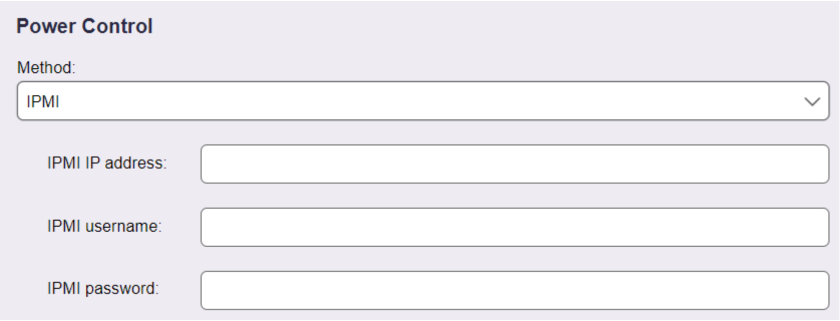
You enable IPMI power control on a per-desktop basis, as follows.

1. Go to the **> Resources > Desktops** page.

2. Click the **Edit** action for a desktop that is IPMI-enabled.

3. Scroll down to the **Power Control** section

4. Select **IPMI** from the **Method** drop-down menu, as shown in the following figure.



Power Control

Method:

IPMI

IPMI IP address:

IPMI username:

IPMI password:

5. Enter in the IP address of the IPMI NIC in the **IPMI IP address** edit field.

   Ensure that the IPMI NIC is functioning properly before saving the form. The Connection Broker attempts to establish an IPMI v2 / RMCP+ session when you save the for.

6. Enter the **IPMI username** and **IPMI password** in the appropriate edit fields.

If you need to enable IPMI power control for a large number of desktops, you can use the Bulk Upload feature available on the **> System > Maintenance** page (see **Uploading IPMI Settings for Desktops**).

Desktop Assignment Modes

The Connection Broker provides several different modes for assigning desktops to a user, including:

- **Policy assignments** - The desktop is assigned to users from a Connection Broker policy. Policy-assigned desktops can be in one of two modes:
  - In *follow me* mode, the user's assigned desktops *follow* the user from client to client, assuming the user is offered the same policy at the new client (see **Follow Me Mode**). Therefore, if the user establishes a connection to a desktop from one client, Leostream moves that desktop connection to the user's next client.
  - *Kiosk* mode supports generic user accounts (see **Kiosk Mode**). When using kiosk mode, you have one login identity that is shared by multiple users, and each user needs a unique desktop. In kiosk mode, if a user establishes a connection to a desktop at one client and then that same username logs in at a different client, Leostream does not move the original desktop connection to the new client. Instead, the user is offered a different desktop.
- **Hard assignments** - A desktop is dedicated to a particular client or user. Hard-assigned desktops can be in one of two modes:
  - *User hard-assigned* desktops are always offered to the hard-assigned user regardless of which client device they use (see **Hard-Assigning a Desktop to a User**). Users with hard-assigned desktops are still assigned to a Leostream policy, and that policy may or may not offer policy-assigned desktops.
  - *Client hard-assigned* desktop are assigned to a particular client device and, therefore, offered to any user that logs in at a client device (see **Hard-Assigning a Desktop to a Client**). If a user logs into Leostream at a client that is hard-assigned to a desktop, the user is still assigned to a Leostream policy however they are *not* offered their policy-assigned desktops. The user can connect only to the desktop that is hard-assigned to that client.
- **Rogue assignments** - The Connection Broker can assign desktops to a user after the user logs into the desktop as rogue (see **Assigning Desktops to Rogue Users**).

Follow Me (“User”) Mode

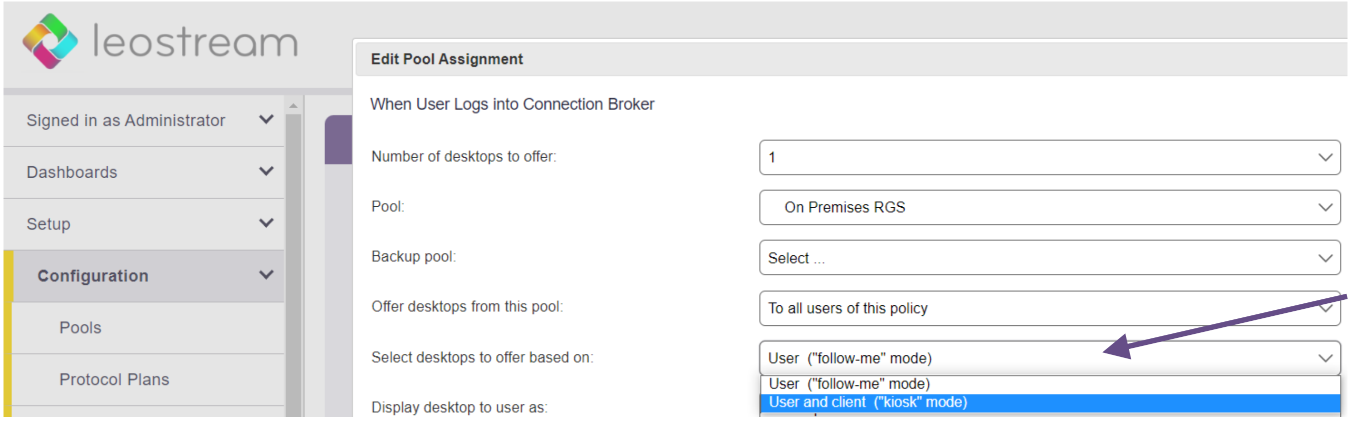
By default, Connection Broker policies assign desktops using follow-me mode. The policy assigns a desktop to the user irrespective of the client they are using. In this case, if user `A` logs into their desktop from the thin client on their desk, the policy assigns them a desktop. If user `A` then logs in from another client at another desk, the policy disconnects user `A` from their previous client and reconnects them to their original desktop at the new client.

Kiosk (“User and Client”) Mode

Using kiosk mode allows the same username to log in simultaneously at different clients and be offered different desktops, meaning the Connection Broker selects desktops to offer based on the username and client, not just the username.

Kiosk mode is commonly used in call centers, classrooms, and public computer kiosks where a single login identity is shared by multiple users. In this case, all users enter the same username to log into Leostream at different clients, for example, in a classroom of computers all using the user name `student`. Each client requires its own desktop, even though the user name is the same on each client.

To enable kiosk mode for a policy, select **User and client (“kiosk” mode)** from the **Select desktops to offer based on** drop-down menu on the **Edit Policy** page, shown in the following figure. See **Chapter 12: Configuring User Experience by Policy** for information on configuring user policies.



Edit Pool Assignment

When User Logs into Connection Broker

Number of desktops to offer: 1

Pool: On Premises RGS

Backup pool: Select ...

Offer desktops from this pool: To all users of this policy

Select desktops to offer based on: User ("follow-me" mode)

User ("follow-me" mode)
User and client ("kiosk" mode)

Display desktop to user as:

Use the **Current Client** column on the **> Resources > Desktop** page to differentiate between desktops assigned to the same user from different clients.

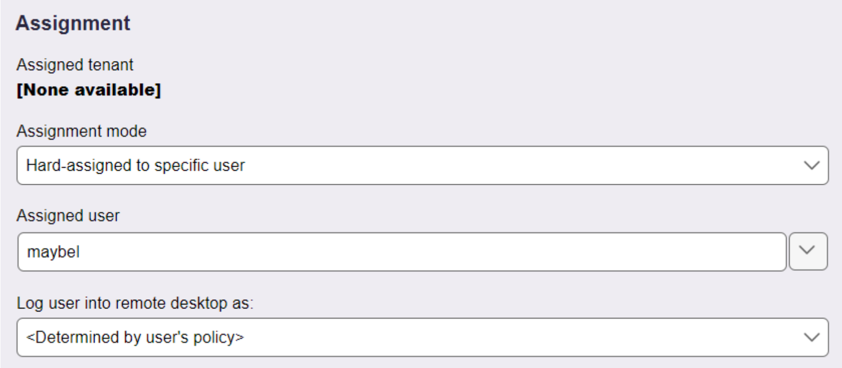
Hard-Assigning a Desktop to a User

You can hard assign a desktop to users that require a persistent desktop. The Connection Broker always offers users their hard-assigned desktops, in addition to any policy-assigned desktops.

To hard-assign a desktop to a user:

1. Go to the **> Resources > Desktops > Edit** page.

2. Select the **Hard-assigned to specific user** option from the **Assignment mode** drop-down menu. The **Assigned user** drop-down menu appears, as shown in the following figure.



Assignment

Assigned tenant
[None available]

Assignment mode: Hard-assigned to specific user

Assigned user: maybel

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

3. Select the user you want to hard-assign to this desktop from the **Assigned user** drop-down menu.

   To filter the list, begin typing the username that you want to select. Only users who have already logged into the Connection Broker are listed. To add a new user, enter their full username and select the **[No users found; create new user "<username>"]** option.

4. You can use the **Log user into remote desktop as** drop-down menu to override the setting in the user's policy and force the user to be logged in as either a domain or local user.

5. Click **Save**.

When hard-assigning the desktop to a new user, the Connection Broker creates a placeholder for that user on the **> Resources > Users** page. The first user with that username who logs into the Connection Broker is associated with that placeholder and is offered the hard-assigned desktop.

The Connection Broker uses the settings on the **Hard Assignments** tab of the user's policy to determine how to manage hard-assigned desktops.

Hard-Assigning a Desktop to a Client

You can hard-assign a desktop to a client device, to ensure that any user logging in through that client receives the same desktop.

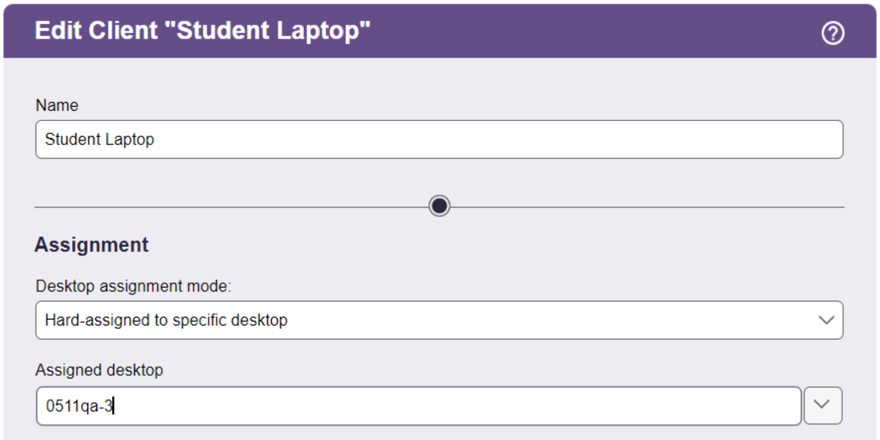
A user who logs in at a client that is hard-assigned to a desktop is *not* offered their user-hard-assigned or policy-assigned desktops.

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.



Edit Client "Student Laptop"

Name

Student Laptop

Assignment

Desktop assignment mode:

Hard-assigned to specific desktop

Assigned desktop

0511qa-3

4. Select the desktop you want to assign to this client from the **Assigned desktop** drop-down menu.

   The desktops available for hard-assignment are filtered based on the desktops your role gives you permission to access (see **Customizing Access to Desktops**)

5. Click **Save**. All users that log in at this client receive same hard-assigned desktop.

The Connection Broker uses the settings on the **Hard Assignments** tab of the user's policy to determine the policy settings for desktops that are hard-assigned to a client.

You can instruct PCoIP clients to connect to their hard-assigned desktop as soon as the client boots. See the **Leostream Quick Start Guide for PCoIP Remote Workstation Cards** for more information.

Assigning Desktops Based on a Calendar of Events

If you have multiple users who need to share a hard-assigned desktop, you can leverage Leostream Schedules to define a calendar of events indicating what users have access to the desktop and during which times and dates. For more information and instructions, see **Assigning Desktops Based on a Schedule**.

Assigning Desktops to Rogue Users

The Connection Broker manages all users that log in using a Leostream client, such as the Leostream Web clients, Leostream Connect, PCoIP clients, or any thin client that communicates with Leostream. In some cases, however, users may connect to a desktop using a display protocol client without first logging into a Leostream client. For example, users may log into the HP ZCentral Remote Boost Receiver and connect directly to a desktop running an HP ZCentral Remote Boost Sender. In this latter case, the Connection Broker considers the user as *rogue*.

If a Leostream Agent is running on the remote desktop, the Connection Broker receives notifications for rogue user logins. You can treat rogue users as Leostream users, and assign a policy to the user to manage their remote sessions.

Rogue user management is enabled at the center level, with override options available for individual desktops. To indicate that the Connection Broker should manage rogue user logins for a center.

1. Select the **Assign rogue users to desktops from this center** option on the **Edit Center** page.

2. From the **Rogue user policy** drop-down menu, indicate the policy to assign to the user. The Connection Broker users the **Rogue User Assignments** tab of the policy to determine the power control and release plan to associate with the desktop after the Connection Broker assigns the desktop to the user.

You can override both of these settings for individual desktops using the related options on the **Edit Desktop** page.

The Connection Broker uses the following logic after receiving notification of a rogue user login to a desktop that is set to assign desktops to rogue users:

- If the desktop is marked as Unavailable, the Connection Broker logs the rogue user login notification but does not assign the user to the desktop or apply the rogue user policy.

- If the desktop is policy-assigned or hard-assigned to another user or client, the Connection Broker logs the rogue user login notification but does not assign the user to the desktop or apply the rogue user policy.

- If the desktop is available for assignment, the Connection Broker looks for a user on the **> Resources > Users** page that matches the domain and username sent in the rogue user login notification.

  📝 The Leostream Agent may not be able to send a reliable Domain parameter when it detects a rogue user login.

- If the Connection Broker locates a matching user on the **> Resources > Users** page, the Connection Broker assigns the desktop to that user and applies the **Rogue User Assignments** settings from the policy assigned to the rogue user.

  📝 If the Connection Broker locates a matching user on the **> Resources > Users** page *and* the desktop is hard-assigned to that user, the Connection Broker uses the **Hard Assignments** settings from the policy assigned to the rogue user.

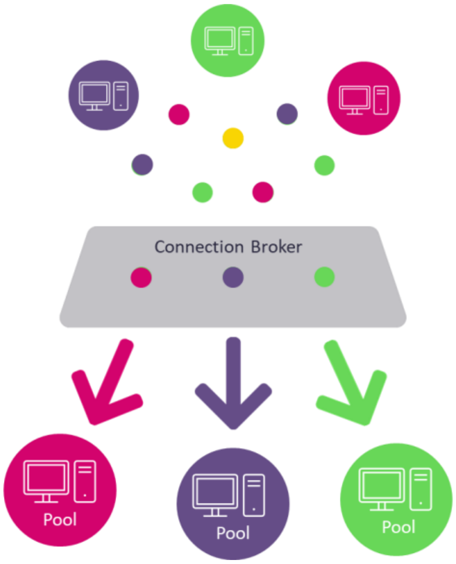
- If the Connection Broker cannot locate a matching user on the **> Resources > Users** page, the Connection Broker creates a new user, assigns the desktop to that user, and applies the **Rogue User Assignments** settings from the policy assigned to the rogue user.

After the user is assigned to the desktop, the Connection Broker no longer considers them as rogue.

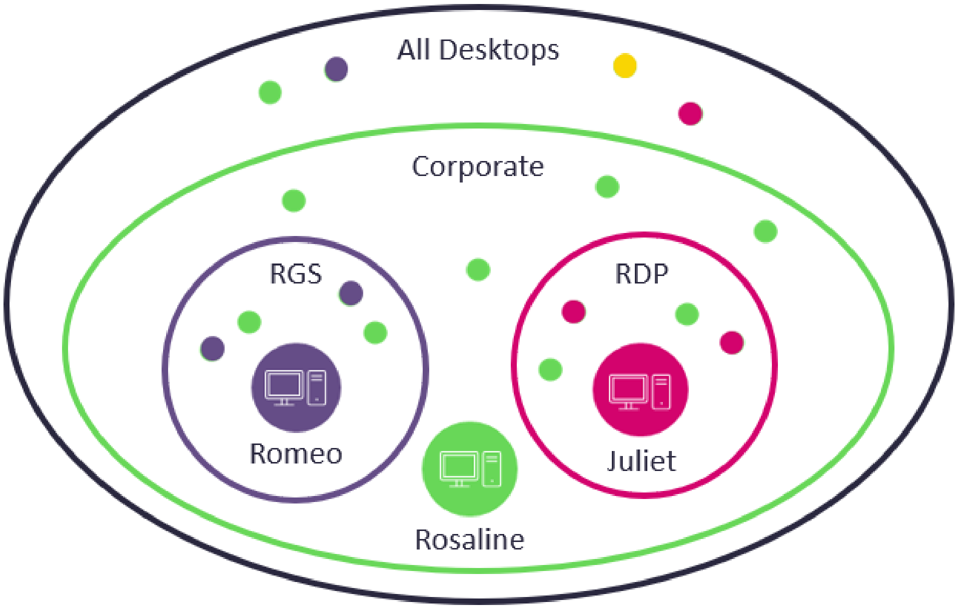
Chapter 8: Creating Desktop Pools

Overview

A *pool* is a collection of desktops. Your policies use pools to control which resources are presented to different users. The Connection Broker places all discovered desktops into the **All Desktops** pool and then sorts desktops into additional pools based on how you configure the Pool Attributes. A desktop's pool membership is dynamic and the Connection Broker determines which desktops are sorted into a pool at the time the information is needed.



Nested pools are pools within another pool, as illustrated for desktops in the following figure.



In this figure:

- The **Corporate** pool is a subset of the **All Desktops** pool and contains three desktops, **Romeo**, **Juliet**, and **Rosaline**.
- The **RGS** and **RDP** pools are mutually exclusive subsets of the **Corporate** pool.
    - The **RGS** pool contains a desktop called **Romeo**.
    - The **RDP** pool contains a desktop called **Juliet**.

Therefore:

- The **Romeo** desktop is a member of the **Corporate** and **RGS** pool
- The **Juliet** desktop is a member of the **Corporate** and **RDP** pool
- The **Rosaline** desktop is a member of only the **Corporate**

When a Leostream user is assigned to a policy that offers desktops from the **Corporate** pool, the Connection Broker selects any desktop from that pool, using the policy settings described in **Offering Desktops from Pools** to determine the best destkop to offer. In this example, any of the three desktops are eligible, regardless of if they are also in a subpool.

Assume the Connection Broker offers the **Juliet** desktop to the first user assigned to a policy that references the **Corporate** pool. If that user requests a connection to the **Juliet** desktop, the Connection Broker assigns that desktop to that user and the **Juliet** desktop is no longer available to offer to another user. Therefore, if a second user subsequently logs into Leostream and is assigned a policy that specifically offers desktops from the **RDP** pool, that user receives a **Desktop Unavailable** message as the **RDP** pool is empty.

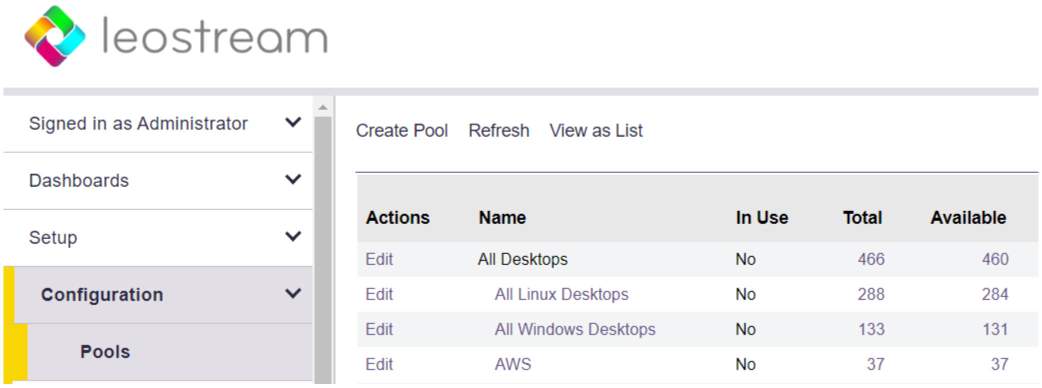
You can define pools in the following ways:

- From centers (see **Defining Pools Using Centers**)
- Using desktop attributes (see **Defining Pools Using Desktop Attributes**)
- From VMware vCenter Server clusters (see **Defining Pools Using VMware vCenter Server Clusters**)
- From VMware vCenter Server Resource Pools (see **Defining Pools Using VMware vCenter Server Resource Pools**)
- Via tags (see **Defining Pools Using Tags**)
- Using LDAP attributes (see **Defining Pools Using LDAP Attributes**)
- Individually selecting resources from the parent pool (see **Selecting Desktops from Parent Pool**)

The following sections describe how to create the different types of pools. For information on enabling provisioning in a pool, see **Chapter 9: Provisioning New Desktops**.)

Displaying Pools

The **> Configuration > Pools** page, shown in the following figure, lists all defined pools.



Actions	Name	In Use	Total	Available
Edit	All Desktops	No	466	460
Edit	All Linux Desktops	No	288	284
Edit	All Windows Desktops	No	133	131
Edit	AWS	No	37	37

Initially, the following four default pools are listed.

- The **All Desktops** pool contains all your inventoried desktops. You cannot delete this pool. Nested pools are indented to indicate the pool hierarchy.

- The **All Windows Desktops** pool is a subset of the **All Desktops** pools and contains all desktops running a Microsoft Windows operating system.

- The **All Linux Desktops** pool is a subset of the **All Desktops** pools and contains all desktops running a Linux operating system.

By default, the pools are displayed as a hierarchy that depicts how the pools are nested. You can switch to a flat list of pools by clicking the **View as List** link at the top of the **> Configuration > Pools** page. After switching to a flat list, you can sort the list alphabetically, for example.

You can display the following columns in the table. To add or remove columns from this table, click the **Customize column** link at the top-right side of the page (see **Customizing Tables**).

- The **Action** column provides options to edit or refresh the pool.

- The **Name** column displays the pool's name.

- The **Display Name** column displays the pool's optional display name, which allows you to display a different user-friendly pool name to end users.

- The **Subset of** column indicates this pool's parent pool. Each pool is indented underneath its parent pool.

- The **In Use** column indicates if the pool is referenced in any policies.

- The **Total** column shows the total number of desktops in the pool. A desktop can belong to more than one pool.

⚠ The value shown in the **Total** column must equal the sum of the numbers show in the **Available**, **Unavailable**, and **Assigned** columns. If these values are not equal, click the **Refresh** link at the top of the page. If these numbers are not equal after refreshing the pool, refresh the centers that host the desktops included in the pool.

- The **Assigned** column indicates how many desktops in that pool are already assigned to a user, including desktops that are hard-assigned to a user.

- The **Available** column indicates how many desktops in that pool are available for assignment to users. For desktop pools, this column includes desktops that are hard-assigned to a client, but not desktops that are hard-assigned to a user.

- The **Unavailable** column shows how many desktops in that pool are unavailable for assignment.

- The **Running** column indicates how many of the desktops in this pool are currently running.

- The **Stopped** column indicates the number of desktops in this pool that are not running.

- The **Suspended** column indicates the number of desktops in this pool that are suspended.

- The **Agent Running** column shows the number of desktops in this pool with a running Leostream Agent. Desktops with installed Leostream Agents that are either unreachable or unresponsive are not included in this count.

- The **Logged In** column displays the number of desktops in the pool that have a logged in user, including any users that logged in as a rogue user. (A *rogue user* is a user that logged into a desktop without logging into the Connection Broker.)

- The **Connected** column indicates the number of logged in users that are actively connected to the session. Users that are logged in, but not connected, have disconnected from their remote session. This column includes rogue users.

- The **Running Threshold** column indicates the number of running, available desktops the Connection Broker maintains. The Connection Broker automatically powers on desktops in the pool if the number of running available desktops drops below this threshold.

- The **Utilization Sample Interval** column shows how often the Connection Broker stores pool usage data (see **Collecting Pool Statistics to Track Desktop Usage**). Only pools that enable the **Track historical pool assignments and connections** option display sample interval. This data is required to display pool statistics on the Leostream Dashboard.

- The **Utilization Retention Period** column shows how long the Connection Broker retains pool usage data (see **Collecting Pool Statistics to Track Desktop Usage**). Only pools that enable the **Track historical pool assignments and connections** option display sample interval. This data is required to display pool statistics on the Leostream Dashboard.

- The **Provisioning Enabled** column indicates if provisioning is enabled for this pool. The provisioning thresholds determine when provisioning will occur.

- The **Provisioning Threshold** column indicates the nominal lower bound for the number of desktops in this pool that are available for assignment. When the number of available desktops in this pool reaches this threshold, the Connection Broker provisions new desktops. This column appears only if you enable provisioning on the **> System > Settings** page.

- The **Provisioning Max Pool Size** column shows the nominal upper bound for the number of desktops in this pool. When the total number of desktops in the pool reaches this limit, the Connection Broker no longer provisions new virtual machines, even if the number of available desktops is below the provisioning threshold.

- The **Current Threshold** column shows the current lower bound for provisioning, if the nominal provisioning threshold is being overridden based on the settings to enforce provisioning limits based on time-of-day.

- The **Current Max Pool Size** column shows the current maximum pool size, if the nominal upper bound is being overridden based on the settings to enforce provisioning limits based on time-of-day.

- The **Provisioning Template** column displays the master template, image, or snapshot used for provisioning in this pool.

- The **Provision as Deletable** column indicates if newly provisioned machines in this pool are marked as deletable.
- The **Provision as Unavailable** column indicates if newly provisioned machines in this pool are marked as Unavailable.

- The **Join Domain** column indicates if the Connection Broker instructions the Leostream Agent to join the machine to an Active Directory domain.

- The **Assign Any User** column indicates if the **Associate initial user notifications with assigned user** option is selected for this pool.

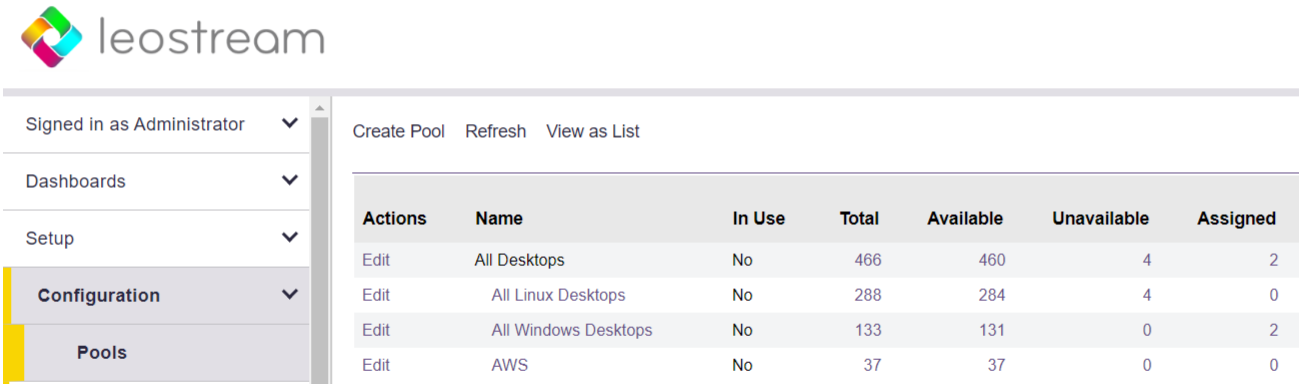
Clicking on a number in the table opens a page that lists the desktops in that state. Unavailable desktops indicate why they are unavailable in square brackets next to the desktop name.

If the number of desktops in the generated list does not match the number shown in the **> Configuration > Pools** page, click the **Refresh** link at the top of the page. The desktops included in the generated list is calculated when you request the list, however the values on the **> Configuration > Pools** page may be stale (see **Refreshing Pools**).

Creating Desktop Pools

To create a new desktop pool:

1. Go to the **> Configuration > Pools** page, shown in the following figure



Actions	Name	In Use	Total	Available	Unavailable	Assigned
Edit	All Desktops	No	466	460	4	2
Edit	All Linux Desktops	No	288	284	4	0
Edit	All Windows Desktops	No	133	131	0	2
Edit	AWS	No	37	37	0	0

2. Click the **Create Pool** link. The **Create Pool** form opens.

3. Enter a name for the pool in the **Name** edit field.

4. If your policies are configured to display a user-friend pool name to end-users, enter that name in the **Display name** field. Otherwise, leave the **Display name** field empty.

5. Select a desktop pool from the **Subset of Pool** drop-down menu. The pool you create is nested inside the selected pool.

6. Select the method for defining the pool from the **Define Pool Using** drop-down menu.

7. Define the contents of the pool. You can define desktop pools using one of the following methods.

    - **Defining Pools Using Centers**
    - **Defining Pools Using Tags**
    - **Defining Pools Using Desktop Attributes**
    - **Defining Pools Using VMware vCenter Server Clusters**
    - **Defining Pools Using VMware vCenter Server Resource Pools**
    - **Defining Pools Using LDAP Attributes** (Requires an Active Directory center)
    - **Selecting Desktops from Parent Pool**

8. Define any logging thresholds in the **Logging** section (see **Logging Desktop Pool Levels** and **Collecting Pool Statistics to Track Desktop Usage**).

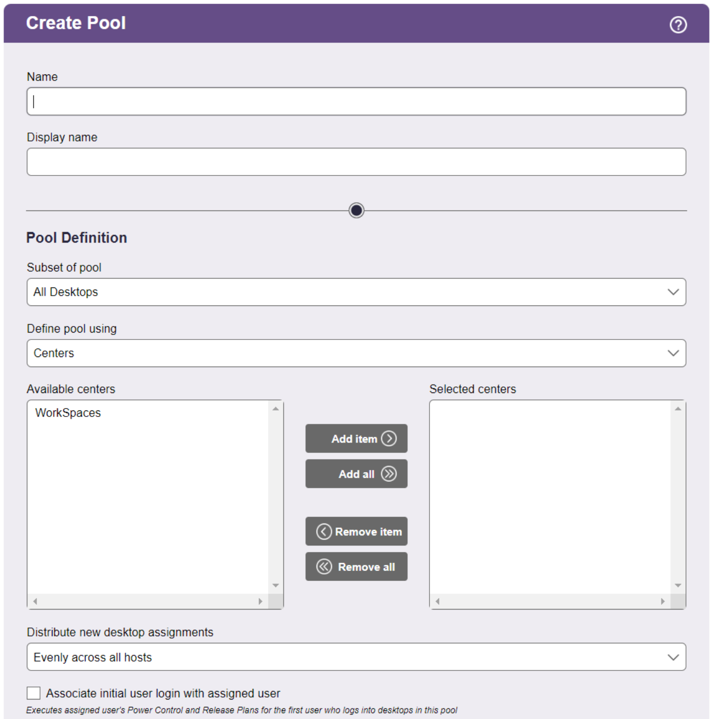
9. Define any provisioning settings (see **Chapter 9: Provisioning New Desktops**).

10. Click **Save**.

Defining Pools Using Centers

To create a pool of desktops from a center, in the **Create Pool** form:

1. Select **Centers** from the **Define pool using** drop-down menu. The form updates to display the Center selection fields, shown in the following figure.



Create Pool

Name

Display name

Pool Definition

Subset of pool: All Desktops

Define pool using: Centers

Available centers: WorkSpaces

Selected centers

Distribute new desktop assignments: Evenly across all hosts

□ 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

2. Select one or more centers from the **Available centers** list.

3. Move the center to the **Selected centers** list by clicking the **Add item** or **Add all** button.
4. Use the **Distribute new desktop assignments** drop-down menu to indicate the method used for distributing desktop assignments across the centers, either:

   - **Evenly across all hosts**: This option evenly distributes desktop offers across all centers in the pool, when possible. To maximize the benefit of using this option, ensure that the users' policies set the **Desktop selection preference** option for this pool to **Any available desktops**.

   - **To center with most available desktops**: This option randomly selects an available desktop from the center that contains the most desktops available for assignment.

   - **To center with least number of assignments**: This option randomly selects a desktop from the available desktops in the center with the least number of assigned desktops.

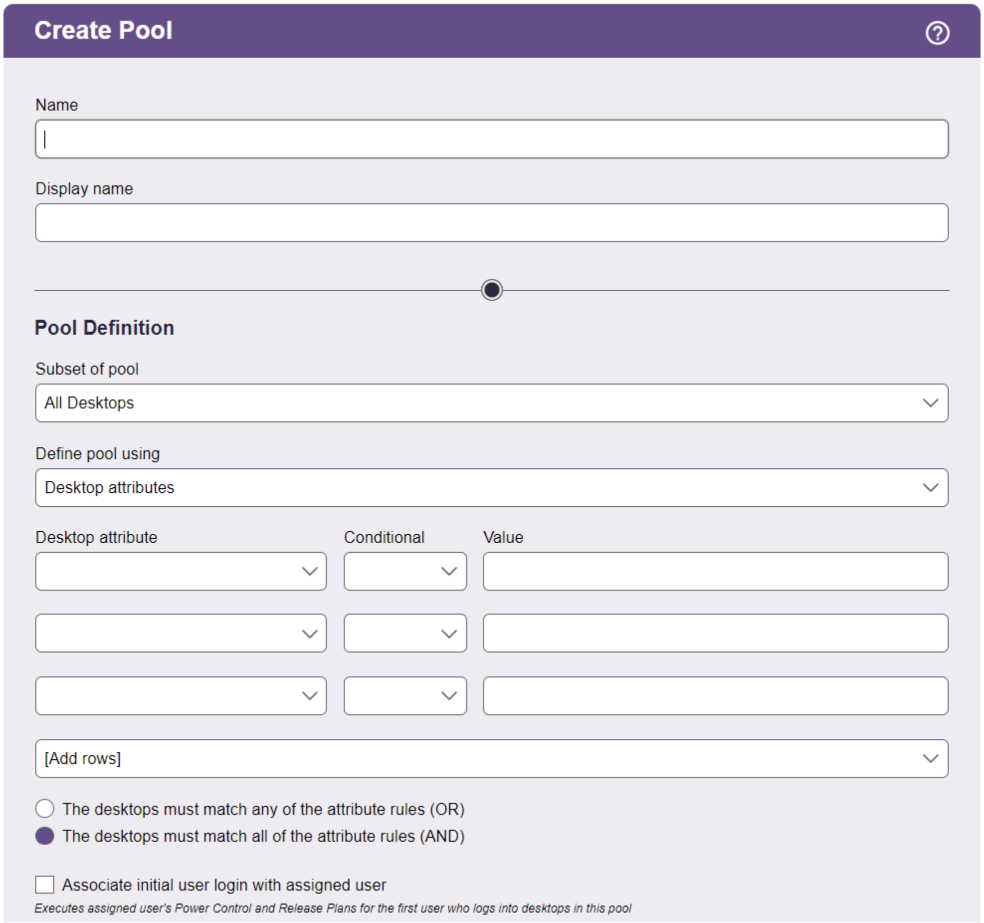
5. Select the **Associate initial user notifications with assigned user** option if the Connection Broker should map the user identity of the first login notification that comes from the Leostream Agent to the user identity that logged into Leostream. After that association is made, all subsequent log off, disconnect, and connect notifications provided by the Leostream Agent for that user invoke actions for the Release and Power Control plans of the assigned user. This option is useful if users log into the desktop using different credentials than used to log into Leostream (see **Mapping Login Notifications to Assigned User ID**).

6. Click **Save**.

Defining Pools Using Desktop Attributes

To create a pool using desktop attributes, in the **Create Pool** form:

1. Select **Desktop attributes** from the **Define pool using** drop-down menu. The form updates to display the **Desktop Attribute Selection** fields, shown in the following figure.



Create Pool

Name

Display name

Pool Definition

Subset of pool: All Desktops

Define pool using: Desktop attributes

Desktop attribute	Conditional	Value

[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

2. Select an item from the **Desktop attribute** drop-down menu. The options include:

    - Name
    - BIOS serial number
    - Centers
    - Computer model
    - CPU speed (GHz)
    - Disk partition name
    - Display name
    - GPU Model
    - GPU RAM (in GB)
    - Installed protocols
    - IP address
    - Machine name
    - Memory (in MB)
    - Notes (defined in the Connection Broker)
    - Number of CPUs
    - Number of disks
    - Number of NICs
    - Operating system
    - Operating system version
    - Partition mount point
    - Tags
    - vCenter Server Notes

    To pool based on internal computer attributes, such as the BIOS serial number, memory, or CPU speed, the desktops must have the latest Leostream Agent installed and the Leostream Agent must have registered the desktop with the Connection Broker.

    On Linux operating systems, the Leostream Agent determines RAM using the `meminfo` function. When used in a virtual machine, `meminfo` may not include reserved memory, resulting in a RAM in the Connection Broker that differs slightly from the RAM reported in vCenter Server.

3. Select the logic condition from the **Conditional** drop-down menu.

4. Enter an appropriate **Text value** for the condition. Each row in the **Desktop Attribute Selection** section reads as a rule that defines desktops in this pool.

    Connection Broker dynamic tags are *not* supported in the **Text value** edit field.

5. Indicate if desktops can match any rule (the **OR** radio button) or must match all rules (the **AND** radio button) in the **Desktop Attribute Selection** section, in order to be included in this pool.

6. Select the **Associate initial user notifications with assigned user** option if the Connection Broker should map the user identity of the first login notification that comes from the Leostream Agent to

the user identity that logged into Leostream. After that association is made, all subsequent log off, disconnect, and connect notifications provided by the Leostream Agent for that user invoke actions for the Release and Power Control plans of the assigned user. This option is useful if the user logs into the desktop using different credentials than used to log into Leostream (see **Mapping Login Notifications to Assigned User ID**).

7. Click **Save**.

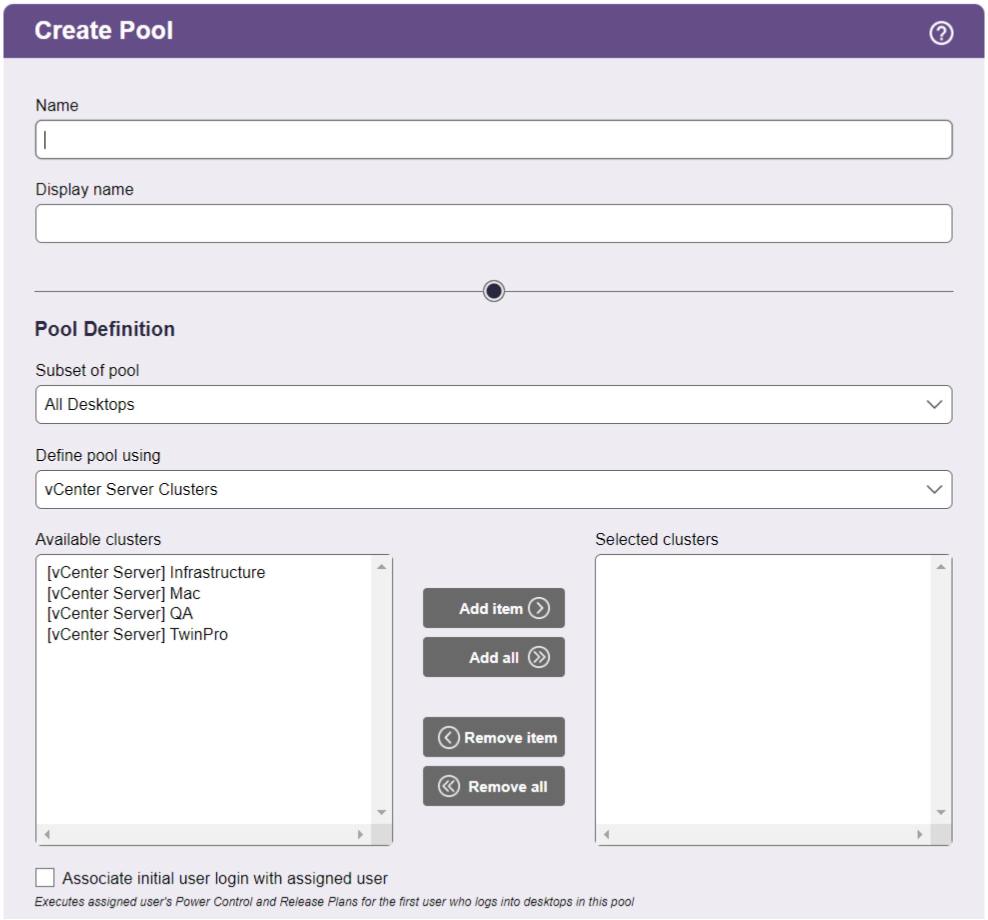
Desktops that match the conditions in the **Desktop Attribute Selection** section are assigned to this pool. If the desktop's attribute changes for some reason (for example, the desktop is renamed), the desktop is immediately re-assigned to the appropriate pool.

Defining Pools Using VMware vCenter Server Clusters

This option is available only if your vCenter Server contains clusters.

To create a pool using vCenter Server clusters, in the **Create Pool** form:

1. Select **vCenter Server Clusters** from the **Define pool using** drop-down menu. The form updates to display the **VMware Cluster** section, shown in the following figure.



Create Pool

Name

Display name

Pool Definition

Subset of pool: All Desktops

Define pool using: vCenter Server Clusters

Available clusters

[vCenter Server] Infrastructure
[vCenter Server] Mac
[vCenter Server] QA
[vCenter Server] TwinPro

Selected clusters

□ 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

The **Available clusters** field contains a list of all the clusters, including the name of the center that contains the cluster. For example:

```
[Center_Name] Cluster_Name
```

2. Select one or more clusters from the **Available clusters** list.

3. Move these clusters to the **Selected clusters** list by clicking the **Add item** or **Add all** button.

4. Select the **Associate initial user notifications with assigned user** option if the Connection Broker should map the user identity of the first login notification that comes from the Leostream Agent to the user identity that logged into Leostream. After that association is made, all subsequent log off, disconnect, and connect notifications provided by the Leostream Agent for that user invoke actions for the Release and Power Control plans of the assigned user. This option is useful if the user logs into the desktop using different credentials than used to log into Leostream (see **Mapping Login Notifications to Assigned User ID**).

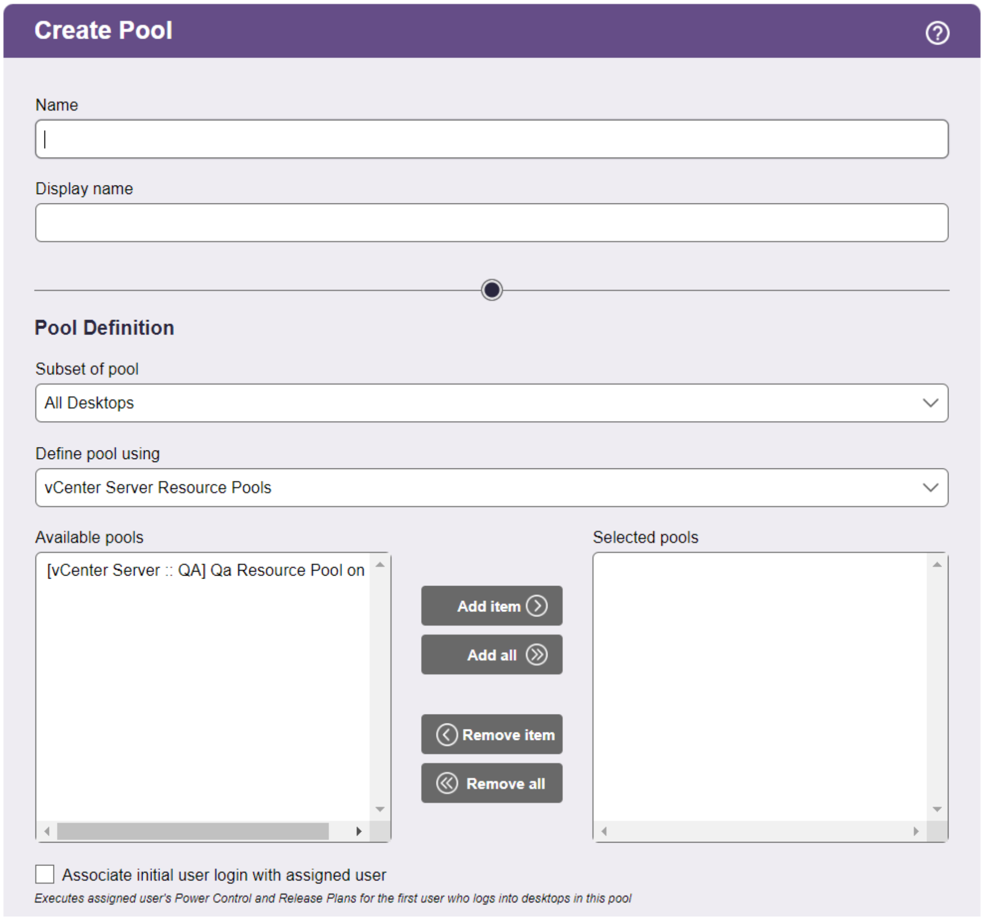
5. Click **Save**.

Defining Pools Using VMware vCenter Server Resource Pools

This option is available only if your vCenter Server contains Resource Pools.

To create a pool using vCenter Server Resource Pools, in the **Create Pool** form:

1. Select **vCenter Server Resource Pools** from the **Define pool using** drop-down menu. The form updates to display the **VMware Resource Pool** section, shown in the following figure.



Create Pool

Name

|

Display name

Pool Definition

Subset of pool

All Desktops

Define pool using

vCenter Server Resource Pools

Available pools

[vCenter Server :: QA] Qa Resource Pool on

Selected pools

□ 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

The **Available pools** field contains a list of all the resource pools, including the name of their parent cluster. For example:

```
[Center :: Primary] Pod1
```

Represents the resource pool `Pod1` residing within the cluster `Primary` in the center named `Center`.

2. Select one or more resource pools from the **Available pools** list.

3. Move these resource pools to the **Selected pools** list by clicking the **Add item** or **Add all** button.

4. Select the **Associate initial user notifications with assigned user** option if the Connection Broker should map the user identity of the first login notification that comes from the Leostream Agent to the user identity that logged into Leostream. After that association is made, all subsequent log off, disconnect, and connect notifications provided by the Leostream Agent for that user invoke actions for the Release and Power Control plans of the assigned user. This option is useful if the user logs into the desktop using different credentials than used to log into Leostream (see **Mapping Login Notifications to Assigned User ID**).

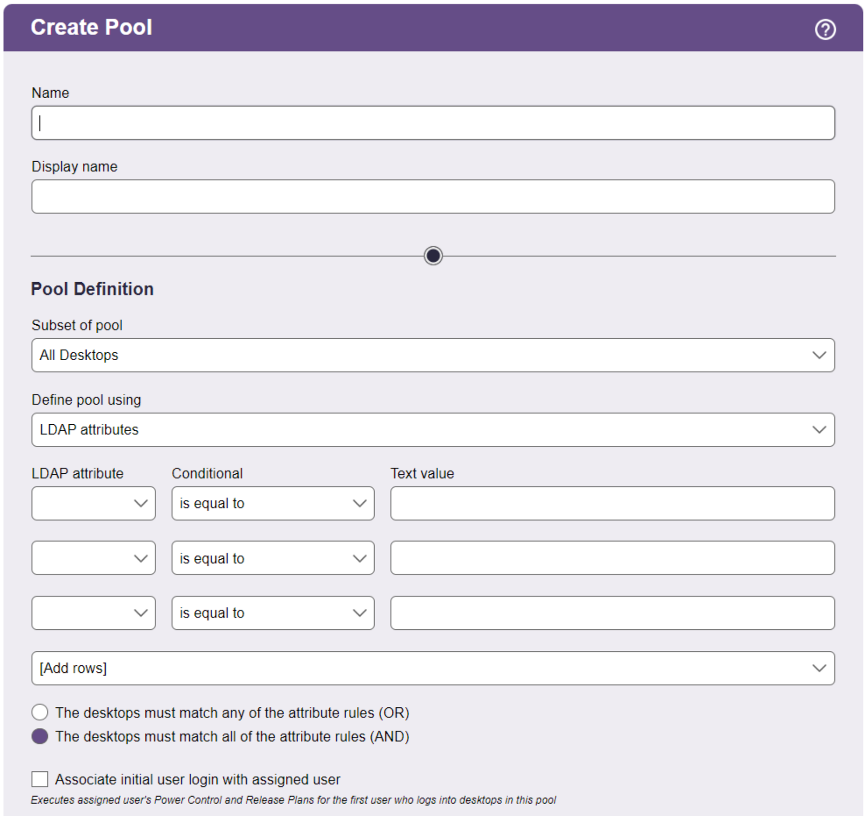
5. Click **Save**.

Defining Pools Using LDAP Attributes

The **LDAP Attribute** option allows you to group desktops based on attributes of the desktop’s Computer record in Active Directory. This option is available only after you defined an Active Directory center (see **Active Directory Centers**).

To create a pool using LDAP attributes, in the **Create Pool** form:

1. Select **LDAP attributes** from the **Define Pool Using** drop-down menu. The form updates to display the **Attribute Selection** fields, shown in the following figure.



Create Pool

Name

Display name

Pool Definition

Subset of pool: All Desktops

Define pool using: LDAP attributes

LDAP attribute	Conditional	Text value
	is equal to	
	is equal to	
	is equal to	

[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

2. Select an item from the **LDAP attribute** drop-down menu.

3. Select the logic condition from the **Conditional** drop-down menu.

4. Enter an appropriate **Text value** for the condition. Each row in the **Attribute Selection** section reads as a rule that defines desktops in this pool.

   Connection Broker dynamic tags are *not* supported in the **Text value** edit field.

5. Indicate if desktops can match any rule (the **OR** radio button) or must match all rules (the **AND** radio button) in the **Attribute Selection** section, in order to be included in this pool.

6. Select the **Associate initial user notifications with assigned user** option if the Connection Broker should map the user identity of the first login notification that comes from the Leostream Agent to the user identity that logged into Leostream. After that association is made, all subsequent log off, disconnect, and connect notifications provided by the Leostream Agent for that user invoke actions for the Release and Power Control plans of the assigned user. This option is useful if the user logs into the desktop using different credentials than used to log into Leostream (see **Mapping Login Notifications to Assigned User ID**).

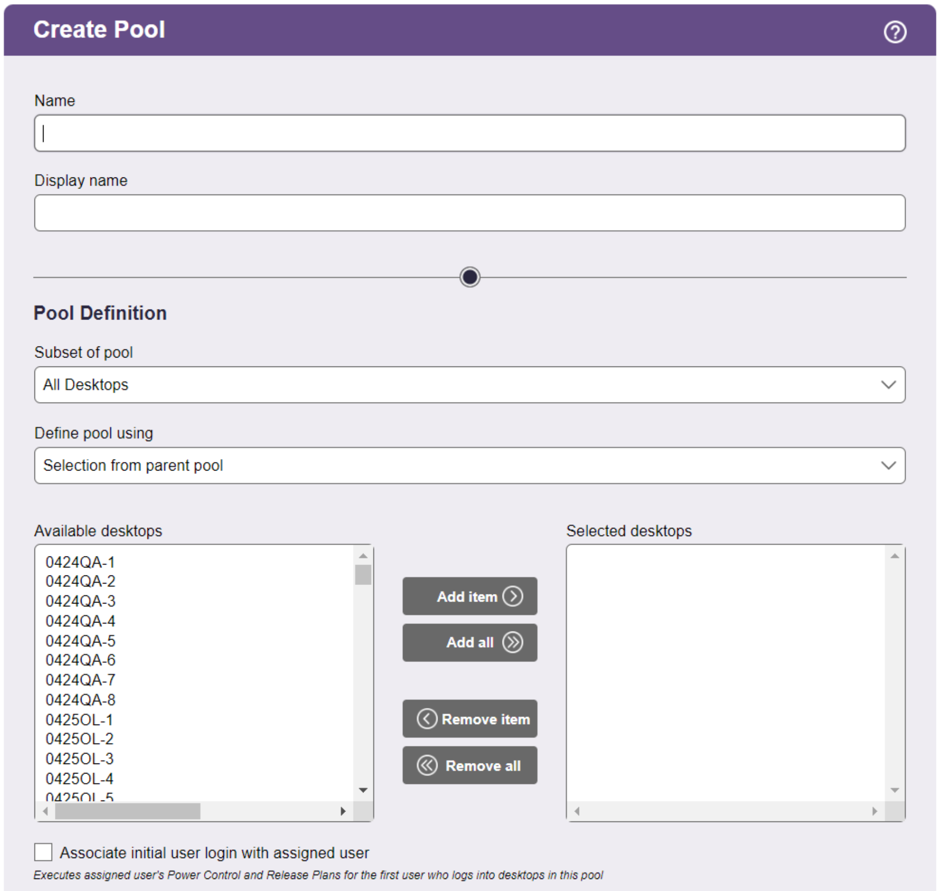
7. Click **Save**.

Selecting Desktops from Parent Pool

To create a pool by manually selecting desktops, in the **Create Pool** form:

1. In the **Subset of Pool** drop-down menu, specify the pool to manually select desktops from.

2. Select **Selection from parent pool** from the **Define Pool Using** drop-down menu. The form updates to display the **Available Desktops** fields, shown in the following figure.



Create Pool

Name

Display name

Pool Definition

Subset of pool: All Desktops

Define pool using: Selection from parent pool

Available desktops

0424QA-1
0424QA-2
0424QA-3
0424QA-4
0424QA-5
0424QA-6
0424QA-7
0424QA-8
0425OL-1
0425OL-2
0425OL-3
0425OL-4
0425OL-5

Selected desktops

□ 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

3. Select the desired desktops from the **Available desktop** list.

4. Move the desktops to the **Selected desktops** list by clicking the **Add item** or **Add all** button.

5. Select the **Associate initial user notifications with assigned user** option if the Connection Broker should map the user identity of the first login notification that comes from the Leostream Agent to the user identity that logged into Leostream. After that association is made, all subsequent log off, disconnect, and connect notifications provided by the Leostream Agent for that user invoke actions for the Release and Power Control plans of the assigned user. This option is useful if the user logs into the desktop using different credentials than used to log into Leostream (see **Mapping Login Notifications to Assigned User ID**).

6. Click **Save**.

Defining Pools Using Tags

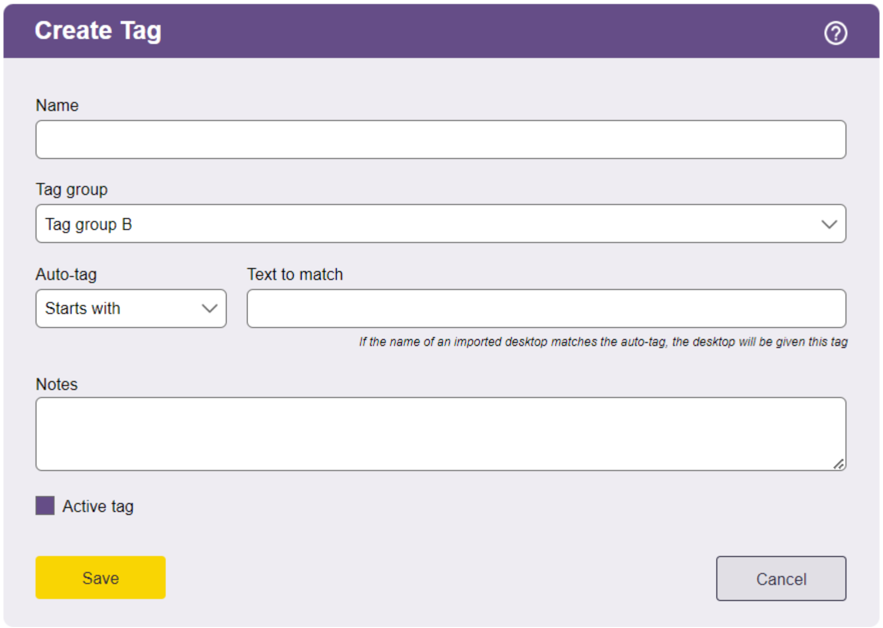
A *tag* is an identifier that can be assigned to a particular desktop. Every tag belongs to one of the four Connection Broker *tag groups*. You can assign one tag from every tag group to each desktop in your Connection Broker. You can then use these tags to make a desktop a member of a particular pool.

Creating Tags

To create tags:

1. Go to the **> Setup > Tags** page.

2. Click **Create Tag**. The **Create Tag** form, shown in the following figure, opens.



Create Tag

Name

Tag group: Tag group B

Auto-tag: Starts with

Text to match

If the name of an imported desktop matches the auto-tag, the desktop will be given this tag

Notes

☑ Active tag

3. Enter a name for the tag in the **Name** field.

4. Select the tag group to place this tag into from the **Tag group** drop-down menu.

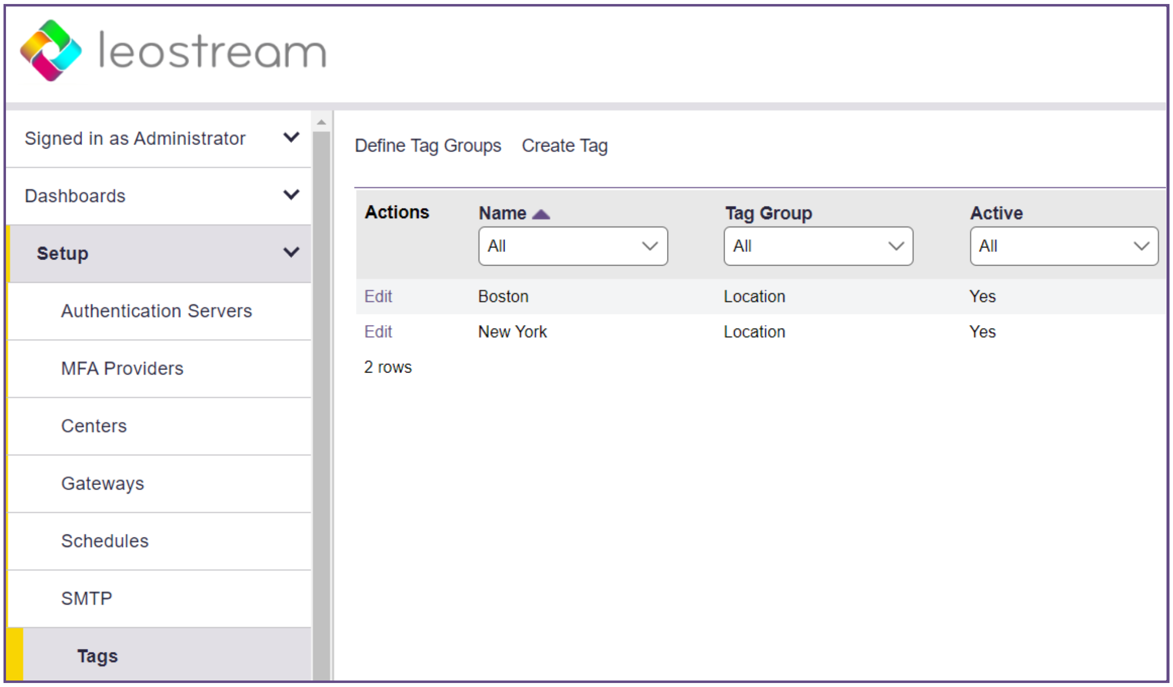
5. If you want to automatically apply this tag to new desktops:

    a. Select the appropriate condition from the **Auto-tag** drop-down menu.
    b. Enter the appropriate text in the **Text to match** edit field. If you do not want to automatically assign this tag, leave the **Text to match** edit field empty.

    The auto-tag feature applies only to centers that have the **Continuously apply any Auto-Tags** option selected. See **Continuously Applying Tags to Desktops** for more information.

6. Click **Save**.

The **> Setup > Tags** page lists all available tags, as shown in the following figure.



Actions	Name ▲	Tag Group	Active
	All	All	All
Edit	Boston	Location	Yes
Edit	New York	Location	Yes

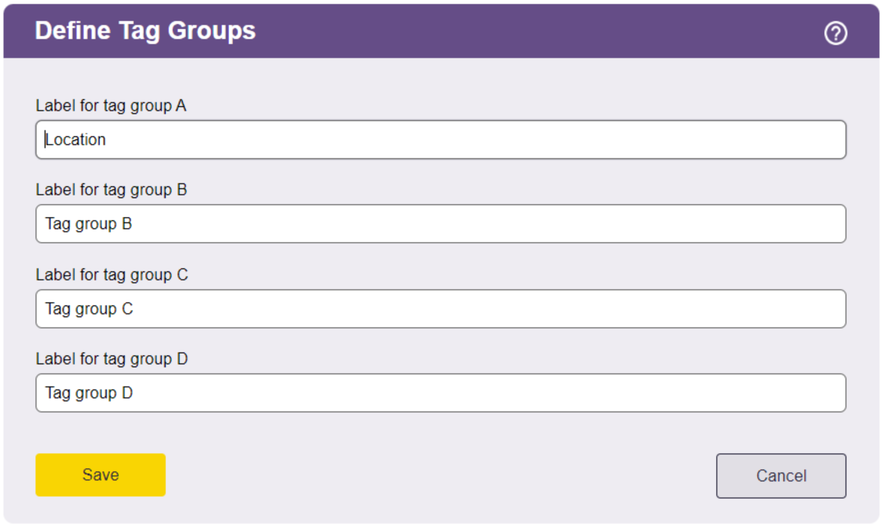
2 rows

You can display tag groups in the table on the **> Resources > Desktop** page, allowing you to sort and classify desktops by tag group. See **Customizing Tables** for information on how to add tag groups to the table.

Naming Tag Groups

To rename tag groups:

1. Select **> Setup > Tags > Define Tag Groups**. The form shown in the following figure opens.



Define Tag Groups

Label for tag group A: Location

Label for tag group B: Tag group B

Label for tag group C: Tag group C

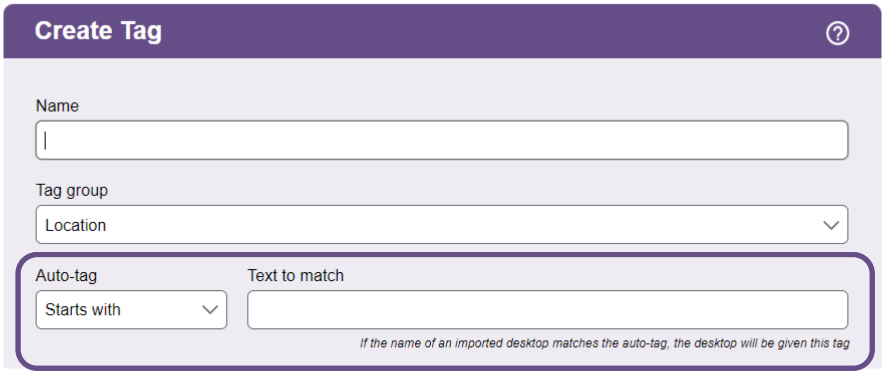
Label for tag group D: Tag group D

2. Enter new tag group names for any groups you want to rename.
3. Click **Save** to store the new names.

You can set tag group names to any alphanumeric string.

Continuously Applying Tags to Desktops

You can automatically assign tags to desktops using the **Auto-tag** feature, shown in the following figure.



Create Tag

Name:

Tag group: Location

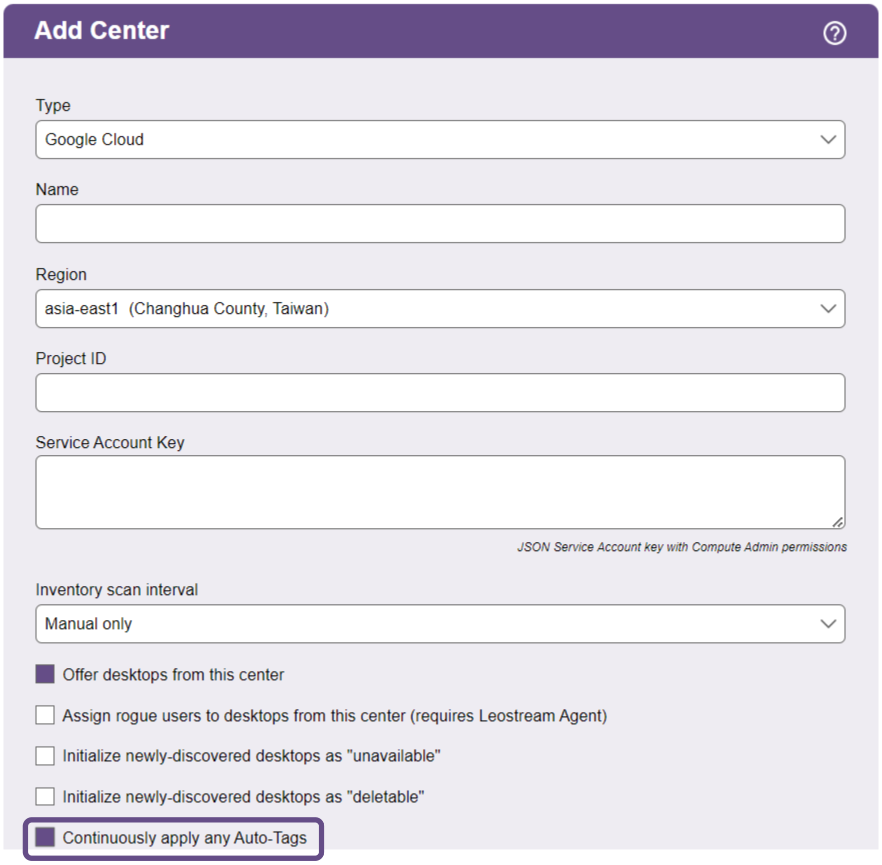
Auto-tag: Starts with

Text to match:

If the name of an imported desktop matches the auto-tag, the desktop will be given this tag

With the auto-tag feature enabled, when the Connection Broker imports a desktop, it assigns tags to the desktop if the desktop's name satisfies the logic condition selected in the **Auto-tag** drop-down menu.

To enable the auto-tag feature, you must select the **Continuously apply any Auto-Tags** option on the **> Setup > Centers > Edit Center** page, shown in the following figure. The Connection Broker applies auto-tagging rules to desktops associated with that center during every center refresh interval.



Add Center

Type: Google Cloud

Name:

Region: asia-east1 (Changhua County, Taiwan)

Project ID:

Service Account Key:

JSON Service Account key with Compute Admin permissions

Inventory scan interval: Manual only

☑ Offer desktops from this center

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

□ Initialize newly-discovered desktops as "unavailable"

□ Initialize newly-discovered desktops as "deletable"

☑ Continuously apply any Auto-Tags

You can automatically assign multiple tags to the same desktop. For example, assume you have the following two tags:

- **Finance**, with **Auto-tag** set to **Starts with** and **Text to match** set to **Fin**
- **English**, with **Auto-tag** set to **Ends with** and **Text to match** set to **Eng**

The Connection Broker assigns the **Finance** tag and the **English** tag to a desktop named **Fin87Eng**.

Tagging Individual Desktops

You can change the tag assignments of a particular desktop using the **Tag Editing** section of the **> Resources > Desktops > Edit Desktop** page.

The **Tag Editing** section does not appear if you have not defined any tags.

Select all tags that you want to apply to this desktop and click **Save**.

Changing the tag assigned to a particular desktop can change its pool membership. Changes in pool membership take effect immediately.

Simultaneously Tagging Multiple Desktops

You can change the tags of multiple desktops by selecting the **Bulk Action** check boxes on the left-hand side of the **> Resources > Desktops** page and then selecting the **Edit** action from the drop-down menu at the top of the column. To select all the listed desktops, click the check box at the top of the **Bulk action** column.

If the check boxes are not visible, click the **Customize columns** link at the bottom of the page and add the **Bulk actions** column. See **Customizing Tables** for more information.

When editing multiple desktops, the **Tag Editing** section shows all the tag groups that currently contain tags. Change the relevant tags or select **Apply Auto-Tags** to apply any auto tagging rules associated with the selected desktops (see **Continuously Applying Tags to Desktops**). For example, assume you are bulk editing three desktops name **Win1**, **Win2**, and **Lin1** and select **English** from the **Language** tag drop-down menu. The **English** tag has the following auto-tag rule:

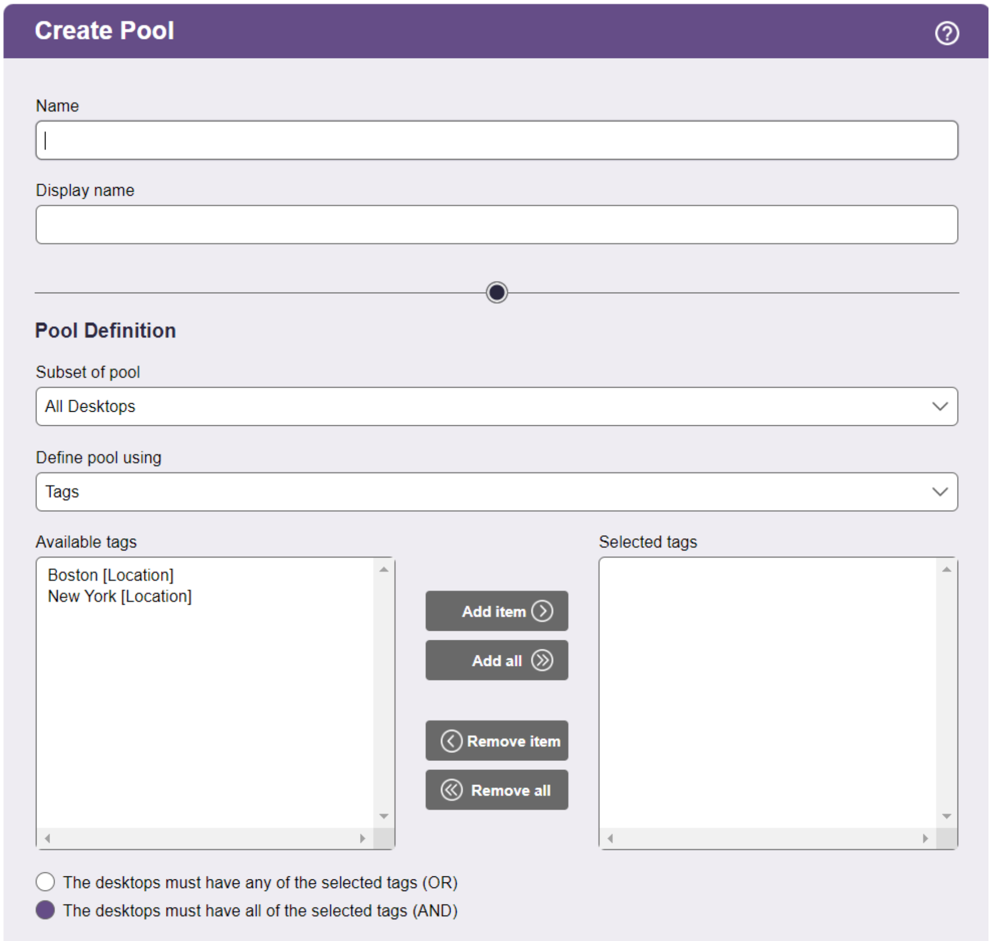
Auto-tag: Starts with
Text to match: Win

If you select **Apply Auto-Tags** on the bulk **Edit Desktop** form and click **OK**, the Connection Broker applies the **English** tag only to **Win1** and **Win2**. Explicitly selecting a tag overrides the auto-tagging rules, however any subsequent scan of a center that enables the **Continuously apply any Auto-Tags** option reapplies the auto-tagging rules and may change your selected tag values.

Creating Pools Using Tags

To create a pool using tags, in the **Create Pool** form:

1. Select **Tags** from the **Define Pool Using** drop-down menu. The form updates to display the **Tag Selection** fields, shown in the following figure.



Create Pool

Name

Display name

Pool Definition

Subset of pool

All Desktops

Define pool using

Tags

Available tags

Boston [Location]
New York [Location]

Selected tags

○ The desktops must have any of the selected tags (OR)
● The desktops must have all of the selected tags (AND)

The **Available tags** list is empty if you have not defined any tags.

2. Select one or more tags from the **Available tags** list.

3. Move the tag to the **Selected tags** list by clicking the **Add item** or **Add all** button.

4. Indicate if desktops can match any tag (the **OR** radio button), or must match all tags (the **AND** radio button), in order to be included in this pool.

5. Select the **Associate initial user notifications with assigned user** option if the Connection Broker should map the user identity of the first login notification that comes from the Leostream Agent to the user identity that logged into Leostream. After that association is made, all subsequent log off, disconnect, and connect notifications provided by the Leostream Agent for that user invoke

actions for the Release and Power Control plans of the assigned user. This option is useful if the user logs into the desktop using different credentials than used to log into Leostream (see **Mapping Login Notifications to Assigned User ID**).

6. Click **Save**.

Example: Using Tags to Define the Contents of a Pool

You can use tags to group computers into pools that match your user groups. For example, consider the example where you want to create two pools of desktops, one to offer to your Windows support team and another to offer to your Linux support team. First, establish a naming convention for the desktops to place in these pools, for example:

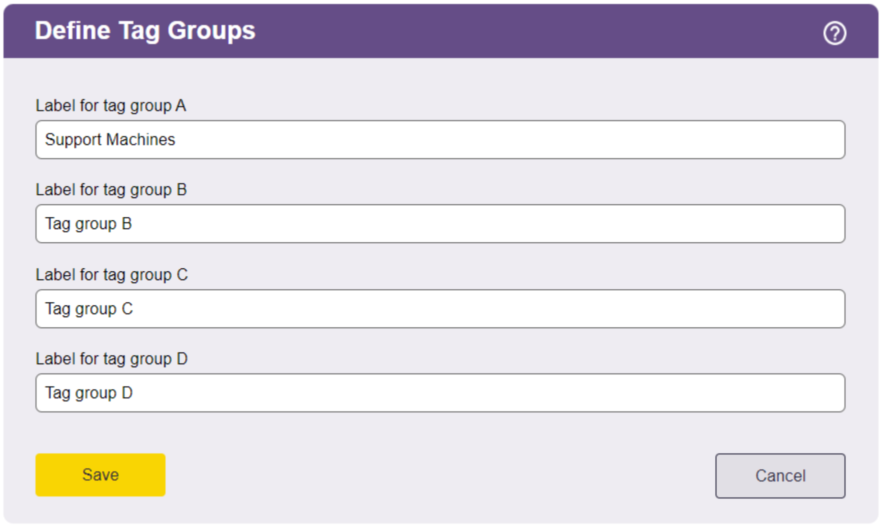
- The machine name of all Windows desktops starts with **Windows**.
- The machine name of all Linux desktops starts with **Linux**.

Before you create desktop centers to register your desktops with the Connection Broker: 1) create a tag group to hold your tags, 2) define the tags in this group, and 3) configure the automatic tag assignment feature, as follows.

1. To create the tag group:

    a. On the **> Setup > Tags** page, select **Define Tag Groups**. The **Define Tag Groups** form opens.

    b. Rename the first tag group to **Support Machines**, as shown in the following figure.



Define Tag Groups

Label for tag group A: Support Machines

Label for tag group B: Tag group B

Label for tag group C: Tag group C

Label for tag group D: Tag group D

    c. Click **Save**.

2. Add a tag for the Windows Support team:

    a. On the **> Setup > Tags** page, select **Create Tag**. The **Create Tag** form opens.

b. Enter **Windows Team** in the **Name** edit field.

c. Select **Support Machines** from the **Tag group** drop-down menu.

d. Select **Starts with** from the **Auto-tag** drop-down menu.

e. Enter **Windows** in the **Text to match** edit field.

f. Click **Save**.

3. Add a tag for the Linux Support team:

   a. On the **> Setup > Tags** page, select **Create Tag**. The **Create Tag** form opens.

   b. Enter **Windows Team** in the **Name** edit field.

   c. Select **Support Machines** from the **Tag group** drop-down menu.

   d. Select **Starts with** from the **Auto-tag** drop-down menu.

   e. Enter **Linux** in the **Text to match** edit field.

   f. Click **Save**.

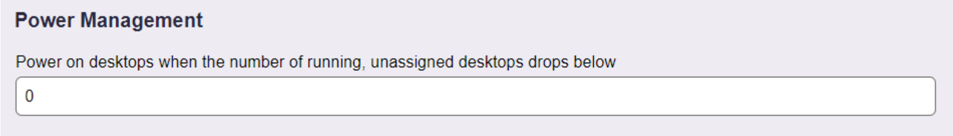
4. After you save your tags, create your desktop centers. When the Connection Broker discovers desktops in your centers, it automatically applies these tags to desktops with names that match the auto-tag criterion.

The Connection Broker provides a number of advanced methods for building pools of desktops. Consider using one of these predefined pooling methods, before you begin defining tags.

Specifying Number of Running Desktops in a Pool

To avoid making users wait for desktops to power on, you can set a threshold on the minimum number of running desktops available for assignment to users. A desktop is available for assignment if it is not already assigned to another user or marked as unavailable.

Use the **Power on desktops when the number of running, unassigned desktops drops below** edit field in the **Power management** section of the **Edit Pool** page to set the minimum number of available desktops that should be running, for example:



Power Management

Power on desktops when the number of running, unassigned desktops drops below

0

The Connection Broker checks the running machine thresholds at the following times:

- When you edit and save a pool that has a running machine threshold
- When a user is assigned to a desktop that was offered from a pool with a running machine threshold

The Connection Broker checks the running machine threshold associated with every pool whenever a user assignment occurs. If the pool already contains more available, running desktops than the running machine threshold, then no desktops are powered up. Otherwise, if the number of available, running desktops falls below the threshold, the Connection Broker automatically starts a desktop in the pool.
Use power control plans to shut down desktops after they have been used.

Joining Pooled Desktops to a Domain

If you have new or existing desktops that are part of a local Microsoft Workgroup, you can use Leostream to join those desktops to an Active Directory domain and optionally add them to Active Directory groups. Before using Leostream to join desktops to a domain, ensure that you do the following.

- Create an authentication server for your domain on the **> Setup > Authentication Servers** page. Ensure that you enter the full DNS domain name in the **Domain** field, not the NetBIOS name.

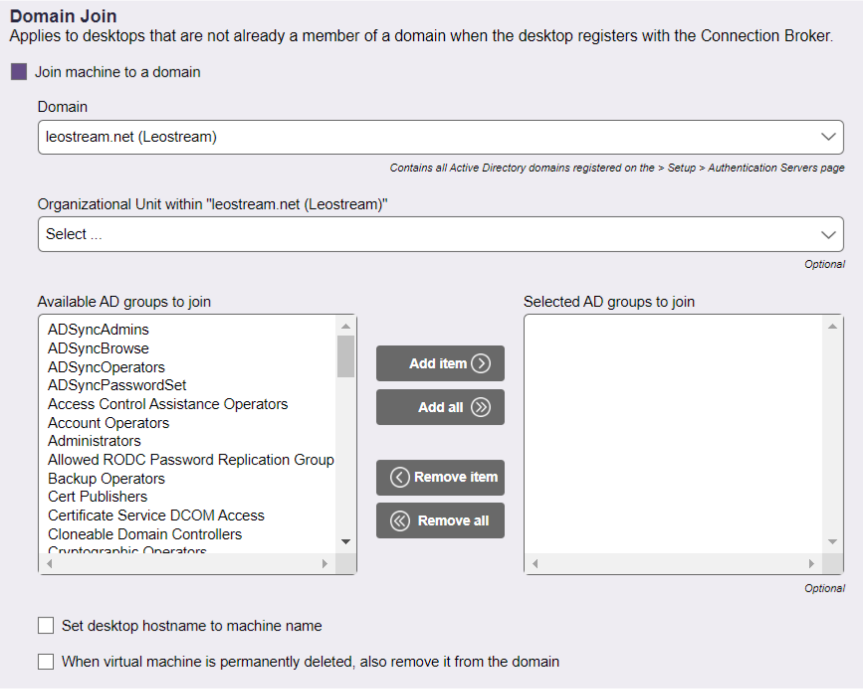
- Install a Leostream Agent on the desktops that you want to join to the domain. Enter your Connection Broker address in the Leostream Agent.

- When creating an image or template to use when provisioning new desktops, ensure that the image is a member of a local Workgroup and that it contains a Leostream Agent that is registered with your Connection Broker.

You create a pool that joins desktops to a domain, as follows:

1. Create a new pool or edit an existing pool.

2. Select the **Join machine to a domain** option in the **Domain Join** section, shown in the following figure.



Domain Join
Applies to desktops that are not already a member of a domain when the desktop registers with the Connection Broker.

☑ Join machine to a domain

Domain: leostream.net (Leostream)

Contains all Active Directory domains registered on the > Setup > Authentication Servers page

Organizational Unit within "leostream.net (Leostream)": Select ...

Optional

Available AD groups to join:
ADSyncAdmins
ADSyncBrowse
ADSyncOperators
ADSyncPasswordSet
Access Control Assistance Operators
Account Operators
Administrators
Allowed RODC Password Replication Group
Backup Operators
Cert Publishers
Certificate Service DCOM Access
Cloneable Domain Controllers
Cryptographic Operators

Selected AD groups to join:

Optional

□ Set desktop hostname to machine name

□ When virtual machine is permanently deleted, also remove it from the domain

3. Select the domain from the **Domain** drop-down menu.

4. Optionally, from the **Organizational Unit** drop-down menu, select an OU for the desktops.

5. Optionally move groups from the **Available AD groups to join** list box to the **Selected AD groups to join** list box, to add the desktop to one or more AD groups.

6. If you want to reset the desktops hostname when joining it to the domain, select the **Set desktop hostname to machine name** check box. With this option selected, the Leostream Agent attempts to set the hostname to the value shown in the **Name** column on the **> Resources > Desktops** page. The **Name** field must contain a valid hostname, as follows:

   - The name uses only the standard character set for Computer Name, which includes letters, numbers, and the following symbols: ! @ # $ % ^ & ') (. - _ { } ~

   - Then name cannot be longer than 15 characters.

7. If you are provisioning non-persistent virtual machines, check the **When virtual machine is permanently deleted, also remove it from the domain** option to have the Connection Broker remove the record from your Active Directory server.

   The Connection Broker attempts to delete the record from Active Directory when the user's Release Plan deletes the virtual machine or when you manually delete the virtual machines from the **> Resources > Desktops** page. Deleting the virtual machine using the hosting platform's management console does not remove the record from Active Directory.

The Connection Broker attempts to join a desktop to the domain when the Leostream Agent on the desktop registers with the Connection Broker, for example, when you reboot the desktop. At that point, the Connection Broker checks the desktop's pool membership and instructs the Leostream Agent to join the desktop to a domain, as appropriate.

If the desktop is a member of multiple pools, the Connection Broker ignores the domain join request if the pools have conflicting settings in the **Domain Join** section.

The Connection Broker will not move a desktop from one domain to another, nor will it reset the hostname of a desktop that is already joined to a domain.

Mapping Login Notifications to Assigned User ID

In some cases, your users may log into their remote desktop using a different username than they use to log into the Leostream Connection Broker. For example, they may log into a Linux VM using their Linux credentials, but use their Active Directory credentials to log into Leostream.

By default, Leostream requires that the username on the remote desktop match the username that logged into Leostream, and ignores all notifications provided by the Leostream Agent that pertain to other usernames. You can change this default behavior by selecting the **Associate initial user notifications with assigned user** option in the **Pool Definition**.

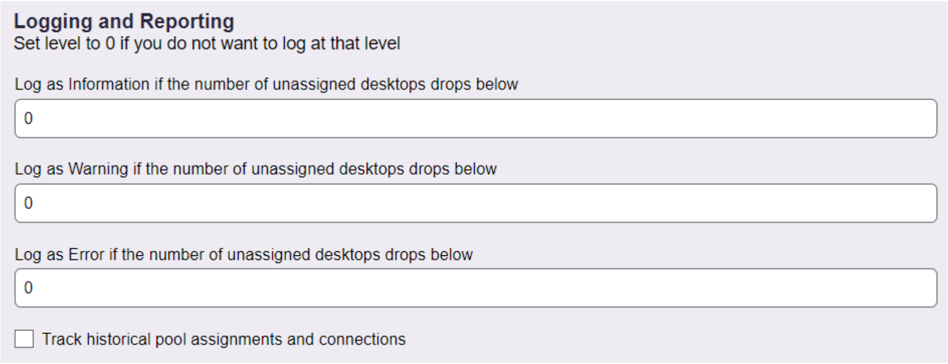
With this option selected, the Connection Broker associates the first user login reported by the Leostrea Agent with the Leostream user, and evaluates all subsequent log off, disconnect, and connect notifications for that user as if those actions were taken by the currently assigned user.

For example, assume Joe logs into Leostream with his Active Directory username `joe_smith`. However, when Joe connects to his policy-assigned desktop, he enters his Linux username `jsmith`. In this scenario, the Connection Broker assigns the desktop to `joe_smith`, but the Leostream Agent provides a login notification for `jsmith`.

With the **Associate initial user notifications with assigned user** option selected, the Connection Broker assumes `jsmith` is the same physical user as `joe_smith` and processes the login notification from the Leostream Agent as if it was for `joe_smith`. Similarly, when Joe logs out, and the Leostream Agent provides a logoff notification for `jsmith`, the Connection Broker associates that logoff notification with `joe_smith`, and executes and power control and release plans for that user.

Logging Desktop Pool Levels

The **Logging and Reporting** section, shown in the following figure, allows you to add information, warnings, or errors to the Connection Broker logs when the number of desktops in the pool drops below a specified threshold.



Logging and Reporting
Set level to 0 if you do not want to log at that level

Log as Information if the number of unassigned desktops drops below
0

Log as Warning if the number of unassigned desktops drops below
0

Log as Error if the number of unassigned desktops drops below
0

□ Track historical pool assignments and connections

Use the edit fields to enter lower bounds for the number of available desktops in the pool. The information, warning, and error thresholds must have decreasing values. For example, the threshold for warnings must be less than the threshold for information; the threshold for errors must be less than the threshold for warnings.

Whenever the pool limit falls below a specified threshold, the Connection Broker logs the event with the most restrictive threshold. For example, if the warning threshold is 5 and the error threshold is 4, the Connection Broker logs a warning when the pool level drops to four and an error when the pool level drops to three.

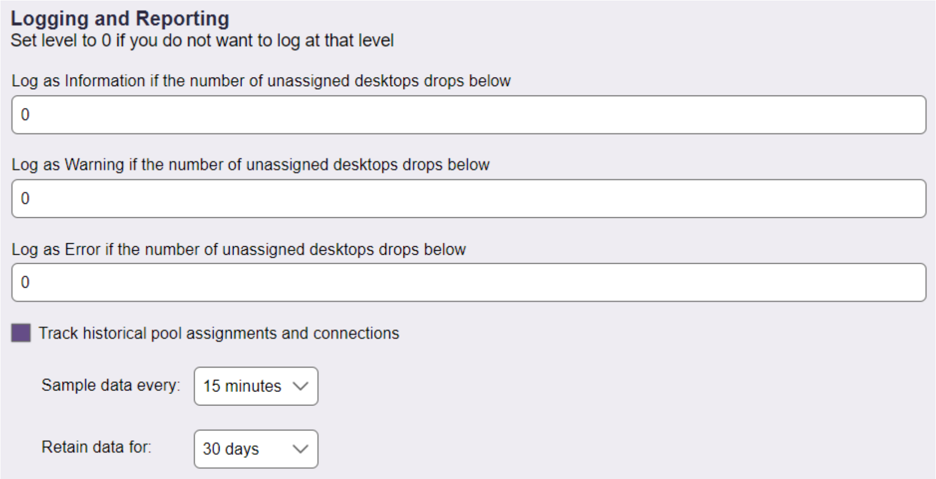
You can use logging events to issue SNMP traps or integrate them into syslog servers. See **Issuing SNMP Traps** and **Integrating with Syslog Servers** for more information.

The Connection Broker checks the pool thresholds at the following times.

- After saving the **Edit Pool** form, when the selection in the **Check provisioning thresholds at least every** drop-down menu changed.
- When a desktop in the pool is assigned to a user.
- When a desktop in the pool is released from a user.

Collecting Pool Statistics to Track Desktop Usage

The Leostream Dashboard requires historical pool usage information to display pool statistics. By default, pools do not collect statistics to avoid storing too much information in the database. You can use the **Logging and Reporting** section to enable historical usage tracking by selecting the **Track historical pool assignments and connections** option**,** shown in the following figure.



Logging and Reporting
Set level to 0 if you do not want to log at that level

Log as Information if the number of unassigned desktops drops below
0

Log as Warning if the number of unassigned desktops drops below
0

Log as Error if the number of unassigned desktops drops below
0

☑ Track historical pool assignments and connections

Sample data every: 15 minutes

Retain data for: 30 days

The **Sample data every** drop-down menu indicates the interval at which the Connection Broker calculates pool assignments and connections. The **Retain data for** drop-down menu indicates how long the Connection Broker stores the calculated information in the database. Set these values appropriately based on the amount of information you want to store and how often desktop states (such as assignments or power states) change.

At each sample interval, the Connection Broker stores the following information in the `pool_history` table in the Connection Broker database:

- `pool_id` - The associated pool
- `total_vm` - Total number of desktops in this pool (`available_vm + unavailable_vm + assigned_vm`)
- `available_vm` - Total number of available desktops in this pool.
- `unavailable_vm` - Total number of unavailable desktops in this pool
- `assigned_vm` - Total number of assigned desktops in this pool
- `total_agent_running` - Total number of desktops with running agent in this pool
- `total_logged_in` - Total number of desktops with logged-in users in this pool
- `total_connected` - Total number of desktops with connected users in this pool
- `total_vm_running` - Total number of running desktops in this pool
- `total_vm_stopped` - Total number of stopped desktops in this pool
- `total_vm_suspended` - Total number of suspended desktops in this pool

You can use this information to create custom reports that show trends in pool load over a period of time, for example:

- Number of disconnected sessions = `total_logged_in - total_connected`
- Percentage of desktops assigned = `assigned_vm / total_vm`
- Percentage of desktops available to be assigned `available_vm / total_vm`

You can also view this information on the **> Dashboards > Statistics** page.

Refreshing Pool Statistics

The **> Configuration > Pools** page displays information about the number of desktops in each pool based on the pool statistics currently stored in the Connection Broker database. The Connection Broker updates the statistics stored in the database at the following times.

- When an administrator logs into the Connection Broker
- When a pool is created
- When a pool is edited and saved
- When an administrator navigates to the **> Configuration > Pools** page
- When you click the **Refresh** link at the top of the **> Configuration > Pools** page
- When a `pool_stats` or `pool_history_stats` job runs

To improve web browser rendering in environments with heavily populated pools, the Connection Broker may draw the **> Configuration > Pools** page before the pool statistics finish calculating. If the numbers displayed on the **> Configuration > Pools** page appear stale, check the status of the `pool_stats` jobs on the **> System > Job Queue** page. If a `pool_stats` job has a status of **Running**, the Connection Broker has not completed the pool statistics calculation.

⚠ The Connection Broker calculates pool statistics based on the currently known state of each desktop in the pool. If the desktop's state has changed, but the Connection Broker did not receive notification of the state change, the pool statistics may be incorrect. If the pool statistics do not look correct, refresh the centers that contain the desktops in the pool, and ensure that any Leostream Agents installed on the desktops are properly communicating with the Connection Broker.

📝 The Connection Broker dynamically determines desktop membership in a pool during user login, guaranteeing users receive the correct desktops based on the pools in their policy.

Chapter 9: Provisioning New Desktops

Overview

Provisioning allows you to generate new virtual machines when the number of desktops in a pool reaches a specified lower threshold. For a discussion on creating pools, see **Chapter 8: Creating Desktop Pools**.

Your Leostream license determines if you have access to the Connection Broker provisioning features. Please, contact **sales@leostream.com** if you need to update your serial number to include this feature.

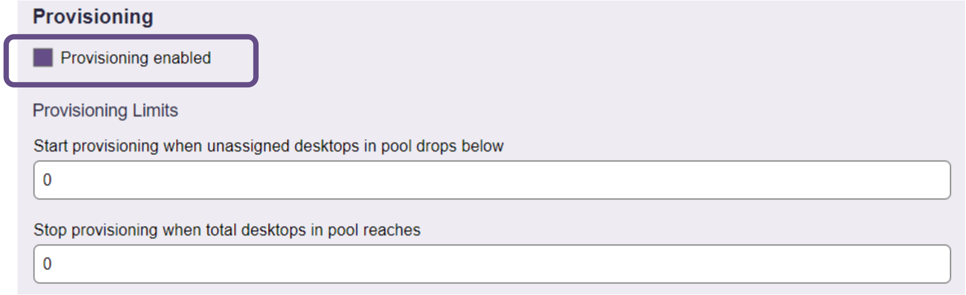
You can provision new machines from any of the following sources:

- OVAs and snapshots in Nutanix AHV (see **Provisioning in Nutanix AHV Clusters**)
- Master VMs in Scale Computing Platform (see **Provisioning in a Scale Computing Platform**)
- OpenStack images (see **Provisioning in OpenStack**)
- vCenter Server templates (see **Provisioning from VMware Templates**)
- vCenter Server snapshots (see **Provisioning VMware Linked Clones**)
- Amazon Web Services AMIs (see **Provisioning in Amazon Web Services**)
- Microsoft Azure images (see **Provisioning in Microsoft Azure**)
- VergeIO templates and recipes
- Templates in KubeVirt Centers
- Bundles in Amazon WorkSpaces (see **Deploying Amazon WorkSpaces**)
- An external URL-based provisioning system (see **Provisioning from External Sources**)

For best performance, all master images, virtual machines, or snapshots you plan to use for provisioning in Leostream should include an installed Leostream Agent configured to communicate with your Leostream Connection Broker.

Enabling and Disabling Virtual Machine Provisioning

The **Provisioning** section of the **Edit Pool** page allows you to configure when and how the Connection Broker creates new virtual machines in one of your hosting environments. To begin, check the **Provisioning enabled** checkbox, as shown in the following figure.



Provisioning

☑ Provisioning enabled

Provisioning Limits

Start provisioning when unassigned desktops in pool drops below

0

Stop provisioning when total desktops in pool reaches

0

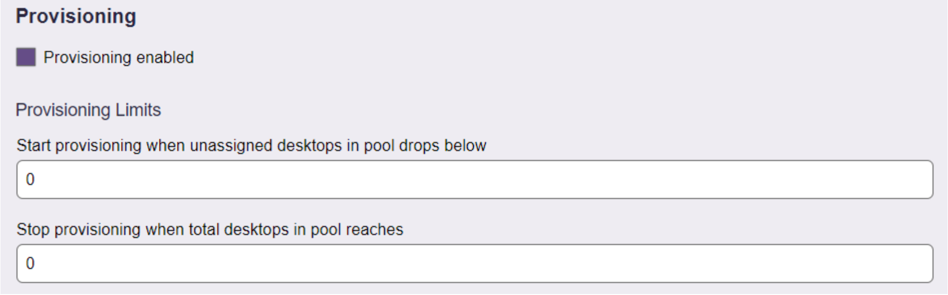
The Connection Broker creates new virtual machines based on the thresholds specified in the **Provisioning Limits** section (see **Defining Provisioning Limits for a Pool**. By default, the value in the **Start provisioning when unassigned desktops in pool drops below** edit field is set to zero and the Connection Broker never creates new virtual machines in this pool.

If you've set non-zero provisioning limits and need to temporarily disable provisioning for a pool, uncheck the **Provisioning enabled** check box. In cases where the Connection Broker is unable to provision new virtual machines due to configuration errors in your pool, the Connection Broker automatically disables provisioning for this pool. If this occurs, please check and correct your provisioning parameters before re-enabling provisioning.

The Connection Broker also disables provisioning in the pool if the **Provisioning Parameters** are configured in such a way that newly provisioned virtual machines do not become members of the pool that invoked the provisioning action. A provisioned VM must meet the criteria used to define the pool's contents in the **Pool Definition** section of the pool, to be consider a member of that pool.

Defining Nominal Provisioning Limits for a Pool

The **Provisioning Limits** section, shown in the following figure, allows you to specify lower and upper bounds on the number of unassigned desktops and total desktops in the pool.



Provisioning

☑ Provisioning enabled

Provisioning Limits

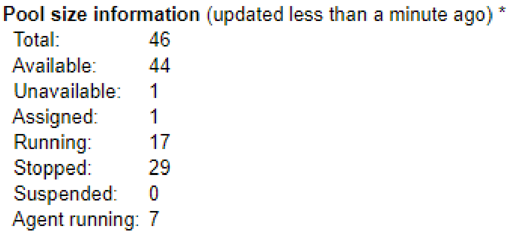
Start provisioning when unassigned desktops in pool drops below

0

Stop provisioning when total desktops in pool reaches

0

The Connection Broker determines when to create new instances by comparing the thresholds specified in the **Provisioning Limits** section to the current contents of the pool. If you edit an existing pool, the Connection Broker displays the current contents of the pool size to the right of the **Edit Pool** form, for example:



Pool size information (updated less than a minute ago) *

Total:	46
Available:	44
Unavailable:	1
Assigned:	1
Running:	17
Stopped:	29
Suspended:	0
Agent running:	7

The number entered into the **Start provisioning when unassigned desktops in pool drops below** field specifies a lower bound on the number of unassigned desktops in the pool, where the number of unassigned desktops is the total number of desktops minus the number of assigned desktops.

For example, the previous figure shows one assigned desktop and 46 total desktops. Therefore, there are

45 unassigned desktops. An unassigned desktop can have a desktop status of either available or unavailable.
The Connection Broker checks this threshold, and provisions new desktops, at the following times

- When the pool is saved.
- When a user is assigned to a desktop in this pool.
- When a `pool_stats` or `pool_history_stats` job runs.

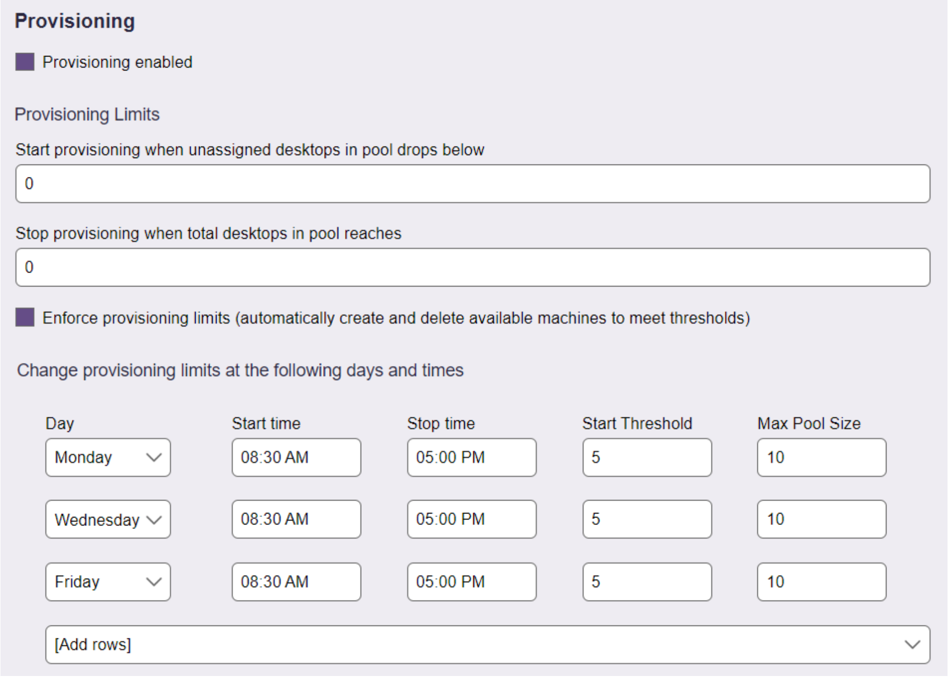
The Connection Broker continues to provision new desktops whenever the lower threshold is crossed, until the upper threshold specified in the **Stop provisioning when total desktops in pool reaches** field is reached, indicated by the **Total** value in the pool size information.

After defining provisioning limits, use the **Provisioning Parameters** described in the following sections to configure how the Connection Broker provisions new machines based on your hosting platform.

Provisioning Based on Time-of-Day

In some cases, you may want the pool to remain empty until the moment when users require a desktop. Scheduling provisioning is useful in cases where desktops are not always needed, for example for shift workers, for classroom environments, or for demonstration systems. When using a cloud, spinning up desktops only for the period of time they are needed can help lower your compute costs in that cloud.

Select the **Enforce provisioning limits** checkbox in the **Provisioning** section of the pool to allow the Connection Broker to add and delete virtual machines over the course of the week. When this option is selected, the **Change provisioning limits at the following days and times** table allows you to set the size of the pool based on the days and time of the week. Consider the configuration in the following figure.



Provisioning

■ Provisioning enabled

Provisioning Limits

Start provisioning when unassigned desktops in pool drops below: 0

Stop provisioning when total desktops in pool reaches: 0

■ Enforce provisioning limits (automatically create and delete available machines to meet thresholds)

Change provisioning limits at the following days and times

Day	Start time	Stop time	Start Threshold	Max Pool Size
Monday	08:30 AM	05:00 PM	5	10
Wednesday	08:30 AM	05:00 PM	5	10
Friday	08:30 AM	05:00 PM	5	10

The global **Provisioning Limits** determine the nominal number of desktops in the pool (see **Defining**

Nominal Provisioning Limits for a Pool). For example, in the previous figure, the pool contains no unassigned desktops as the **Start provisioning when unassigned desktops in pool drops below** field is set to zero. The number of assigned desktops in the pool is unbounded, as the **Stop provisioning when total desktops in pool reaches** edit field is also set to zero.

Based on the first row in the previous figure, on Monday at 8:30AM, the Connection Broker provisions five desktops to meet the new minimum threshold set in the **Start Threshold** edit field. As users log in and are assigned to one of these machines, the Connection Broker will provision additional desktops until the total pool sizes reaches 10.

The Connection Broker uses the time zone of its current database to compare against the times specified in the provisioning intervals. If the Connection Broker uses its internal database, the time zone is determined by the operating system. If you switched your Connection Broker to an external database, the time zone is set by that external data base.

On Monday at 5:00PM, the Connection Broker reverts to the nominal number of unassigned desktops, which is zero in the previous figure. At that time, the Connection Broker deletes unassigned desktops to reach the nominal value. Any assigned desktops are not deleted.

Assigned desktops should be deleted by the user’s Release Plan (see **Example: Deleting Virtual Machines After Use**).

In the example in the previous figure, the Connection Broker restarts provisioning until Tuesday at 8:30AM.

Provisioning in OpenStack

Before provisioning instances in an OpenStack environment, you must configure the following:

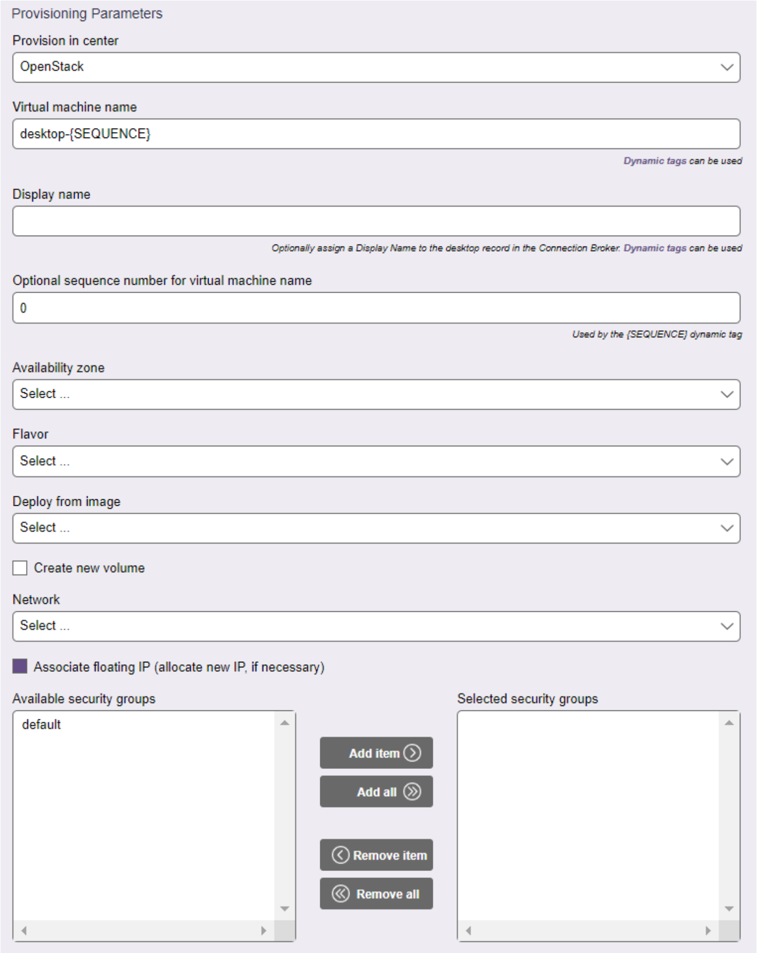
1. Create master images. These images are displayed in OpenStack on the **> Project > Compute > Images** page. Ensure that your master images contain an installed Leostream Agent.

2. Configure a network on the OpenStack **> Project > Network > Networks** page.

⚠ If you do not configure a network, the Connection Broker cannot provision new instances in OpenStack.

Use the **Provisioning Parameters** section to configure provisioning in OpenStack:

1. From the **Provision in center** drop-down menu, select the OpenStack center, and therefore project, to provision new machines into. The remainder of the form updates based on the contents of your selection. The following figure shows a subset of the **Provisioning Parameters**.



Provisioning Parameters

Provision in center: OpenStack

Virtual machine name: desktop-{SEQUENCE}

Dynamic tags can be used

Display name:

Optionally assign a Display Name to the desktop record in the Connection Broker. Dynamic tags can be used

Optional sequence number for virtual machine name: 0

Used by the {SEQUENCE} dynamic tag

Availability zone: Select ...

Flavor: Select ...

Deploy from image: Select ...

☐ Create new volume

Network: Select ...

■ Associate floating IP (allocate new IP, if necessary)

Available security groups: default

Selected security groups:

2. Enter a name for the virtual machine in the **Virtual machine name** edit field. You can use dynamic tags to create a name from a mixture of static and dynamic variables. See **Using Dynamic Tags in Provisioning Parameters** for an example.

3. Optionally enter a user-friendly display name into the **Display name** edit field. You can specify in the user’s policy if the Connection Broker should display the desktop to the user with its display name instead of virtual machine name.

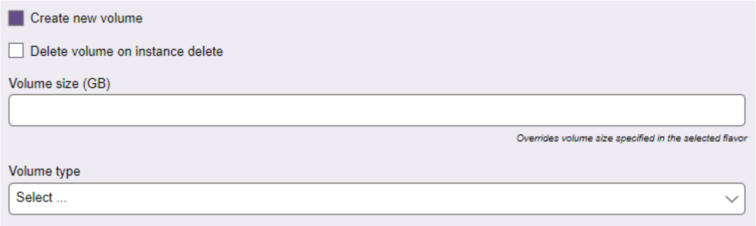
4. If either of the names contains a `{SEQUENCE}` dynamic tag, enter the starting number for the sequence in the **Optional sequence number for virtual machine name** edit field. The Connection Broker starts naming virtual machines at this number and increments the number for each machine created.

5. Select the availability zone to provision the new instance into from the **Availability zone** drop-down menu.

6. Select the instance size from the **Flavor** drop-down menu.

7. Select the image to use from the **Deploy from image** drop-down menu. This menu contains all the public and project images available in the OpenStack center you selected.

8. By default, the Connection Broker creates an instance with ephemeral storage. To create a new volume from the image to use for the provisioned instance, select the **Create new volume** checkbox. The form expands to show the fields in the following figure.



☑ Create new volume

☐ Delete volume on instance delete

Volume size (GB)

Overrides volume size specified in the selected flavor

Volume type

Select ...

   a. If you are provisioning non-persistent virtual machines, select the **Delete volume on instance delete** checkbox to have the Connection Broker delete the volume along with the instance, when instructed to do so by the user's Release Plan.

   b. If create a volume of a different size than that of the selected flavor, enter the desired volume size in the **Volume size** edit field.

   c. Select the desired volume type from the **Volume type** drop-down menu.

9. Select a network location for the instances from the **Network** drop-down menu.

10. Select the **Associate floating IP (allocate new IP, if necessary)** option if Leostream should assign a floating IP address to the new instance. If a floating IP address is not available, Leostream attempts to allocate a new address.

11. In the **Available security groups** field, select the security groups to assign to the new instance. Click the **Add item** button to place them into the **Selected security groups** field.

12. Use the **Actions to execute after provisioning completes** section to schedule actions such as joining the newly provisioned machine to your domain and powering it down. See **Scheduling Post-Provisioning Actions** for more details.

    You must add the **Join domain** action to this table to indicate if newly provisioned machines are joined to your domain at the time they are provisioned. Otherwise, the Connection Broker will not join the machine to your domain until a subsequent Leostream Agent registration arrives, for example when the machine is next rebooted.

    The default action marks the machine as available for assignment to end users. If you are pre-provisioning machines and do not want them to be immediately available for assignment, switch the default **Action to execute** to **Mark desktop as Unavailable for assignment**.

13. Select the **Initialize newly-provisioned desktops as deletable** option to indicate that the Connection Broker is allowed to terminate this instance from OpenStack. When this option selected, the **Edit Desktop** page for the newly provisioned desktop has the **Allow this desktop to be permanently deleted from disk** option selected, by default. Use release plans to schedule instance deletion.

14. Click **Save**.

When the number of unassigned desktops in the pool falls below the lower threshold, the Connection Broker creates a new instance from the selected image.

Provisioning in Amazon Web Services (AWS) EC2

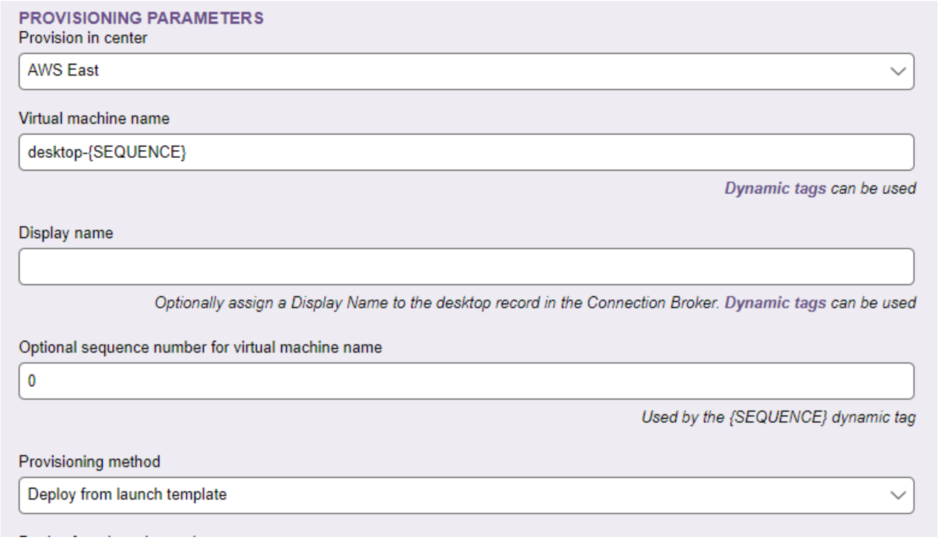
Before provisioning instances in an AWS environment, you must configure the following:

1. Create master images from an instance with a running Leostream Agent. These images are displayed as AMIs in your AWS account.

2. Configure a virtual private network for the new desktops.

Use the **Provisioning Parameters** section to configure provisioning in AWS:

1. Select the AWS center to provision new machines into from the **Provision in center** drop-down menu. The remainder of the form updates based on the contents of your selection. The following figure shows an example of part of the **Provisioning Parameters** section.



PROVISIONING PARAMETERS

Provision in center: AWS East

Virtual machine name: desktop-{SEQUENCE}

Dynamic tags can be used

Display name:

Optionally assign a Display Name to the desktop record in the Connection Broker. Dynamic tags can be used

Optional sequence number for virtual machine name: 0

Used by the {SEQUENCE} dynamic tag

Provisioning method: Deploy from launch template

2. Enter a name for the virtual machine in the **Virtual machine name** edit field. If the pool is defined as instance names that begin with a certain string, ensure that the **Virtual Machine Name** field starts with that string.

3. Optionally enter a user-friendly display name into the **Display name** edit field. You can specify in the user’s policy if the Connection Broker should display the desktop to the user with its display name instead of virtual machine name.

4. If either of the names contains a `{SEQUENCE}` dynamic tag, enter the starting number for the sequence in the **Optional sequence number for virtual machine name** edit field. The Connection Broker starts naming virtual machines at this number and increments the number for each machine created.

5. From the **Provisioning method** drop-down menu, indicate if you are launching instances from an image (AMI) or a launch template, by selecting **Deploy from image** or **Deploy from launch template**, respectively.

   If deploying from a launch template, use the **Deploy from launch template** and **Launch template version** drop-down menus to select the appropriate template and version to use. Select **Unspecified (use default version)** from the **Launch template version** drop-down menu to indicate that the Connection Broker should provision new instances using the **Default version** specified in the AWS Console. After configuring the launch template and version, skip to step 13.

6. If deploying from an AMI, select the image to use from the **Deploy from image** drop-down menu. This menu contains all the AMIs available in your account in the AWS region associated with the selected center, even if you filtered the inventoried instances using Tag rules.

7. Select the instance size from the **Instance type** drop-down menu.

8. If you chose an applicable T instance type, select the **Enable T2/T3/T3a/T4g Unlimited** option to indicate the instance is allowed to burst beyond its baseline CPU usage.

9. Select the VPC from the **Network** drop-down menu.

   If you add the instance to a VPC that does not provide public IP addresses, you can use the Leostream Gateway to connect clients that are outside of the private network. See the **Leostream Gateway Guide** for more information.

10. Indicate the Availability Zones where the Connection Broker should attempt to locate new instances by moving AZs from the **Available subnets/Availability Zones** list to the **Selected subnets/Availability Zones** list.

    Every time the Connection Broker needs to provision a virtual machine, it attempts to place it in the first Availability Zone in the list. If that Availability Zone no longer has capacity to provision an instance of the selected type, the Connection Broker looks through the remaining Availability Zones to find capacity. If the Connection Broker cannot find capacity in any of the selected Availability Zones, provisioning is disabled for the pool

11. Select the security group to assign to the instance from the **Security group** drop-down menu.

12. In the **IAM Instance Profile name** edit field, optionally enter the name of an IAM instance profile to attach to the provisioned instances. If you created your IAM role using the console, the instance profile has the same name as your IAM role.

13. Use the **Actions to execute after provisioning completes** section to schedule actions such as joining the newly provisioned machine to your domain and powering it down. See **Scheduling Post-Provisioning Actions** for more details.

    You must add the **Join domain** action to this table to indicate if newly provisioned machines are joined to your domain at the time they are provisioned. Otherwise, the Connection Broker will not

join the machine to your domain until a subsequent Leostream Agent registration arrives, for example when the machine is next rebooted.
The default action marks the machine as available for assignment to end users. If you are pre-provisioning machines and do not want them to be immediately available for assignment, switch the default **Action to execute** to **Mark desktop as Unavailable for assignment**.

14. Select the **Initialize newly provisioned desktops as deletable** option to indicate that the Connection Broker is allowed to delete this VM from disk. When this option selected, the **Edit Desktop** page for the newly provisioned VM has the **Allow this desktop to be permanently deleted from disk** option selected, by default. Use release plans to schedule VM deletion.

    For more information on using release plans to terminate AWS instances, see the example on deleting virtual machines in the "Release Plans" section of Chapter 11.

15. Click **Save.**

When the number of unassigned desktops in the pool falls below the lower threshold, the Connection Broker creates a new instance from the selected image.

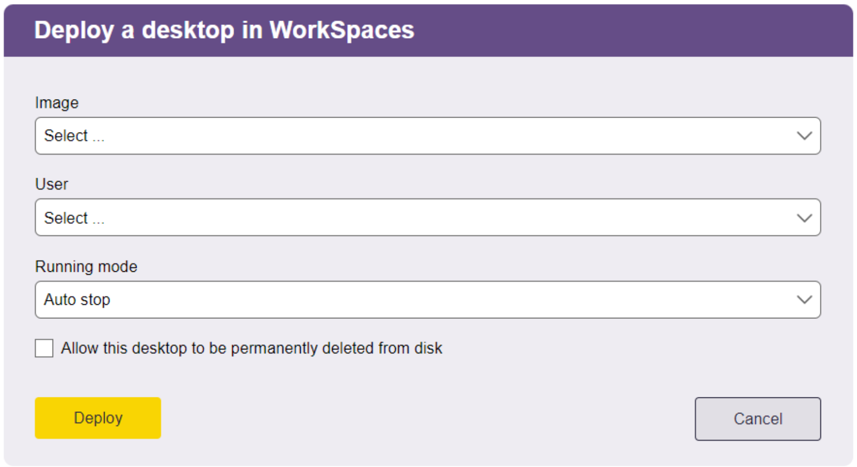
Deploying Amazon WorkSpaces

You deploy Amazon WorkSpaces from custom BYOL bundles created in the Amazon WorkSpaces console.

Amazon WorkSpaces are one-to-one associated with a user and, therefore, are not provisioned from a pool. Instead, you deploy Amazon WorkSpaces in Leostream from the Amazon WorkSpaces centers, as follows.

1. Go to the **> Setup > Centers** page

2. Click the **Deploy** option for your Amazon WorkSpaces center



Deploy a desktop in WorkSpaces

Image
Select ...

User
Select ...

Running mode
Auto stop

☐ Allow this desktop to be permanently deleted from disk

3. From the **Images** drop-down menu, select the bundle to use for the new WorkSpaces instance.

Ensure that you select a WorkSpaces Core bundle. These bundles are labeld with a BYOP Client protocol in the Amazon WorkSpaces console. Leostream cannot currently distinguish WorkSpaces from WorkSpaces Core bundles.

4. From the **User** drop-down menu, select the user to assign to the new WorkSpaces instance.

   Amazon WorkSpaces limits users to a single WorkSpaces instance per Directory Services.

5. Select the **Running mode** to use for the WorkSpaces instance.

   - Auto stop: Not supported for WorkSpaces Core bundles
   - Always on: The WorkSpaces Core Instance is billed monthly
   - Manual: The WorkSpaces Core Instance is billed hourly

   The Connection Broker controls the power state of your new WorkSpaces Instances based on the settings in your Leostream Policies. Depending on the usage patterns of your users, you may want to configure those policies to leave the WorkSpaces running instead of automatically powering them down. To determine which option works best for you, consult the **WorkSpaces Core Pricing** page.

6. Check the **Allow this desktop to be permanently deleted from** disk option if you want to use Leostream to delete Workspaces instances. You can delete instances manually on the **> Resources > Desktops** page or automatically by configuring Release Plans to delete the WorkSpaces instance when it is released from the user.

7. Click **Deploy**.

When the WorkSpaces instance is launched, the selected user is associated with the WorkSpaces instance and appears in the **Assigned Users** column on the **> Resources > Desktops** page. This assignment is initialized as a policy-assignment instead of a hard-assignment, so you can leverage Leostream Release Plan options to terminate the WorkSpaces, if required.

If the WorkSpaces instances takes a long time to deploy, the wait_for_start job associated with that new instance may complete prior to the WorkSpaces instance reaching an **Available** state. If that occurs, the Connection Broker releases the user assignment and marks the WorkSpace as Stopped on the **> Resources > Desktops** page. If this occurs, monitor the Amazon WorkSpaces console for the WorkSpace to reach an **Available** state and then return to the **> Setup > Centers** page in the Connection Broker and click the **Scan** option for the Amazon WorkSpaces center.

For more information, see the **Leostream Quick Start for Amazon WorkSpaces Core**.

Provisioning in Nutanix AHV Clusters

Use the **Provisioning Parameters** section to configure how Leostream provisions new virtual machines on your Nutanix cluster.

1. Select your Nutanix center from the **Provision in center** drop-down menu.

2. Configure the **Virtual machine name** for the newly provisioned machines.

   Note: If you created your pool based on the desktop name, make sure the **Virtual machine name** is set to satisfy the naming convention so the newly provisioned machines are placed in this pool. Creating a desktop in a particular pool does not guarantee it is placed in that pool if the desktop does not satisfy the rules in the pool definition.

3. Optionally enter a display name for the provisioned virtual machines in the **Display name** edit field. You can use the display name in policies to display a user-friendly name when these machines are offered to users.

4. If one of the names contains one of the `{SEQUENCE}` dynamic tag, enter the starting number for the sequence in the **Optional sequence number for virtual machine name** edit field. The Connection Broker starts naming virtual machines at this number and increments the number for each machine created.

5. From the **Provisioning method** drop-down menu, select the appropriate option to indicate if you want to deploy new virtual machines from an OVA or from a snapshot.
6. In the **Deploy from image** or **Parent virtual machine and snapshot image** drop-down menu, select your master OVA or snapshot, respectively.

7. Use the **Actions to execute after provisioning completes** section to schedule actions such as joining the newly provisioned machine to your domain and powering it down. See **Scheduling Post-Provisioning Actions** for more details.

   You must add the **Join domain** action to this table to indicate if newly provisioned machines are joined to your domain at the time they are provisioned. Otherwise, the Connection Broker will not join the machine to your domain until a subsequent Leostream Agent registration arrives, for example when the machine is next rebooted.

   The default action marks the machine as available for assignment to end users. If you are pre-provisioning machines and do not want them to be immediately available for assignment, switch the default **Action to execute** to **Mark desktop as Unavailable for assignment**.

8. If you want give Leostream permission to delete virtual machines when the user logs out, ensure that you select the **Initialize newly-provisioned desktops as “deletable”** checkbox as shown in the following figure.

9. Click **Save**.

Provisioning in a Scale Computing Platform

Use the **Provisioning Parameters** section to configure how Leostream provisions new virtual machines in your Scale Computing Platform, as follows.

1. Select your Scale Computing Platform from the **Provision in center** drop-down menu.

2. Configure the **Virtual machine name** for the newly provisioned machines.

   Note: If you created your pool based on the desktop name, make sure the **Virtual machine name** is set to satisfy the naming convention so the newly provisioned machines are placed in this pool. Creating a desktop in a particular pool does not guarantee it is placed in that pool if the desktop does not satisfy the rules in the pool definition.

3. Optionally enter a user-friendly display name into the **Display name** edit field. You can specify in the user’s policy if the Connection Broker should display the desktop to the user with its display name instead of virtual machine name.

4. If either of the names contains a `{SEQUENCE}` dynamic tag, enter the starting number for the sequence in the **Optional sequence number for virtual machine name** edit field. The Connection Broker starts naming virtual machines at this number and increments the number for each machine created.

5. Select your master image from the **Deploy from template** drop-down menu. This menu contains all virtual machines on your Scale Computing Platform that are tagged as templates based on the tag you specified in your Scale Computing center. Ensure that you select an image that contains a Leostream Agent that is registered with your Connection Broker.

   📝 If you assigned additional tags in your Scale Computing Platform to your master image, the Connection Broker copies those tags to all virtual machines provisioned from that image. The tag used to indicate the master image is a template is not copied over to the newly provisioned machines.

6. Use the **Actions to execute after provisioning completes** section to schedule actions such as joining the newly provisioned machine to your domain and powering it down. See **Scheduling Post-Provisioning Actions** for more details.

   📝You must add the **Join domain** action to this table to indicate if newly provisioned machines are joined to your domain at the time they are provisioned. Otherwise, the Connection Broker will not join the machine to your domain until a subsequent Leostream Agent registration arrives, for example when the machine is next rebooted.

   The default action marks the machine as available for assignment to end users. If you are pre-provisioning machines and do not want them to be immediately available for assignment, switch the default **Action to execute** to **Mark desktop as Unavailable for assignment**.

7. If you want Leostream to delete virtual machines when the user logs out, ensure that you select the

Initialize newly-provisioned desktops as “deletable” checkbox.

8. Click **Save**.

Provisioning in VergeIO

You can provision new virtual machines in VergeIO from either snapshots or recipes. When provisioning in VergeIO, ensure that you select a snapshot or recipe created from a virtual machine with an installed and registered Leostream Agent.

You configure pools to provision in VergeIO, as follows.

1. Select your VergeIO system from the **Provision in center** drop-down menu.

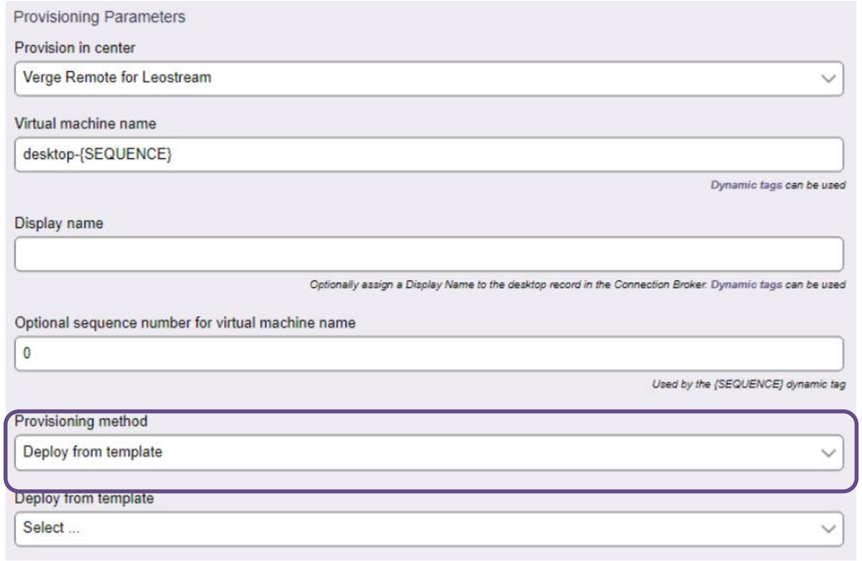
2. Configure the **Virtual machine name** for the newly provisioned machines.

   Note: If you created your pool based on the desktop name, make sure the **Virtual machine name** is set to satisfy the naming convention so the newly provisioned machines are placed in this pool. Creating a desktop in a particular pool does not guarantee it is placed in that pool if the desktop does not satisfy the rules in the pool definition.

3. Optionally enter a user-friendly display name into the **Display name** edit field. You can specify in the user’s policy if the Connection Broker should display the desktop to the user with its display name instead of virtual machine name.

4. If either of the names contains a `{SEQUENCE}` dynamic tag, enter the starting number for the sequence in the **Optional sequence number for virtual machine name** edit field. The Connection Broker starts naming virtual machines at this number and increments the number for each machine created.

5. From the **Provisioning method** drop-down menu, shown in the following figure, select either **Deploy from template** or **Deploy from recipe** to indicate how you want to provision new machines.



Provisioning Parameters

Provision in center

Verge Remote for Leostream

Virtual machine name

desktop-{SEQUENCE}

Dynamic tags can be used

Display name

Optionally assign a Display Name to the desktop record in the Connection Broker. Dynamic tags can be used

Optional sequence number for virtual machine name

0

Used by the {SEQUENCE} dynamic tag

Provisioning method

Deploy from template

Deploy from template

Select ...

6. Based on your provisioning method, select either the appropriate template or recipe from the **Deploy from template** or **Deploy from recipe** drop-down menu.

7. If you are deploying from a recipe that requires user-inputted answers or need to configure the deployed virtual machines using a payload, use the **Recipe payload** field to enter a JSON that specifies all the required values.

8. Use the **Actions to execute after provisioning completes** section to schedule actions such as joining the newly provisioned machine to your domain and powering it down. See **Scheduling Post-Provisioning Actions** for more details.

   You must add the **Join domain** action to this table to indicate if newly provisioned machines are joined to your domain at the time they are provisioned. Otherwise, the Connection Broker will not join the machine to your domain until a subsequent Leostream Agent registration arrives, for example when the machine is next rebooted.

   The default action marks the machine as available for assignment to end users. If you are pre-provisioning machines and do not want them to be immediately available for assignment, switch the default **Action to execute** to **Mark desktop as Unavailable for assignment**.

9. If you want Leostream to model non-persistent desktops and delete the provisioned virtual machines after user, ensure that you select the **Initialize newly-provisioned desktops as “deletable”** checkbox.

10. Click **Save**.

Provisioning in Microsoft Azure

Before provisioning instances in an Azure cloud, you must configure the following:

1. Create master image from an Azure virtual machine with a running Leostream Agent. Ensure that you capture a managed image. Do not share the image to a gallery as an image version, for example
2. Configure a virtual network for the new desktops, including any required subnets.

Then, use the **Provisioning Parameters** section to configure provisioning in Azure:

1. Select the Azure center to provision new machines into from the **Provision in center** drop-down menu. The remainder of the form updates based on the contents of your selection.
2. Enter a name for the virtual machine in the **Virtual machine name** edit field. If the pool is defined as instance names that begin with a certain string, ensure that the **Virtual Machine Name** field starts with that string.
3. Optionally enter a user-friendly display name into the **Display name** edit field. You can specify in the user’s policy if the Connection Broker should display the desktop to the user with its display name instead of virtual machine name.
4. If either of the names contains a `{SEQUENCE}` dynamic tag, enter the starting number for the sequence in the **Optional sequence number for virtual machine name** edit field. The Connection Broker starts naming virtual machines at this number and increments the number for each machine created.
5. In the **Administrator user name** edit field, enter the name for an administrator user to create on the provisioned instance.
6. In the **Administrator user password** edit field, specify this user’s password.
7. Select the **Resource group** to add the virtual machine into.
8. Indicate if all resources created for the new virtual machines should be placed in the selected Resource group. If the **Use the same Resource group for all desktop resources** option is selected, you can provision only from images contained in the same Resource group as the destination Resource group. If the **Use the same Resource group for all desktop resources** option is *not* selected:

   • The **Deploy from image** drop-down menu contains all images across all Resource groups. Therefore, to provision from an image that is not in the selected Resource group, ensure that you uncheck this option.

   • Network interfaces are placed in the Resource group associated with the virtual network you select in step 11.

9. In the **Deploy from** drop-down menu, indicate if you are provisioning from an Image or an Azure Computer Gallery.

10. If you are provisioning from an Azure Compute Gallery, use the **Gallery** drop-down menu to select the appropriate gallery.

11. Select the image to use from the **Deploy from image** drop-down menu.

12. Select the instance size from the **Instance size** drop-down menu.

13. Use the **OS disk size in GB** edit field to increase the operating system disk size for the provisioned instances. You cannot specify a value less than the current disk size.

14. By default, Leostream creates persistent OS disks for provisioned VMs. For stateless workflows, you may prefer to leverage Ephemeral OS disks, which are not saved to remote Azure Storage. Select the **Use Ephemeral OS disk** option to provision new VMs with Ephemeral disks.

    Shutting down or powering off a VM with an Ephemeral disk results in the VM being deleted from Azure. Leostream does not support the **Reboot** or **Power off and Start** power control options for VMs with Ephemeral disks.

15. Specify the **Virtual Network** for the new virtual machines.

16. Select the subnet from the **Network/Subnet** drop-down menu.

    If you add the instance to a subnet that does not provide public IP addresses, you can use the Leostream Gateway to connect clients that are outside of the private network. See the **Leostream Gateway Guide** for more information.

17. Select the **Create and associate new public IP address** check box if you want the Connection Broker to allocate and assign a public IP address to new instances. Leave this option unchecked to isolate the instance in their private network.

18. Select the security group to assign to the instance from the **Security group** drop-down menu.

19. Use the **Actions to execute after provisioning completes** section to schedule actions such as joining the newly provisioned machine to your domain and powering it down. See **Scheduling Post-Provisioning Actions** for more details.

    You must add the **Join domain** action to this table to indicate if newly provisioned machines are joined to your domain at the time they are provisioned. Otherwise, the Connection Broker will not join the machine to your domain until a subsequent Leostream Agent registration arrives, for example when the machine is next rebooted.

    The default action marks the machine as available for assignment to end users. If you are pre-provisioning machines and do not want them to be immediately available for assignment, switch the default **Action to execute** to **Mark desktop as Unavailable for assignment**.

20. Select the **Initialize newly provisioned desktops as deletable** option to indicate that the Connection Broker is allowed to delete this VM from disk. When this option selected, the **Edit Desktop** page for the newly provisioned VM has the **Allow this desktop to be permanently deleted from disk** option selected, by default. Use release plans to schedule VM deletion.

21. Click **Save**.

Provisioning from VMware Templates

In order to provision virtual machines using vCenter Server templates, you must provide your Connection Broker vCenter Server center with the credentials for an account with the following VMware privileges.

> Datastore > Allocate space
> Host > Inventory > Modify cluster
> Resource > Assign virtual machine to resource pool
> Virtual Machine > Edit inventory > Create new
> Virtual Machine > Clone virtual machine
> Virtual Machine > Provisioning > Customize guest
> Virtual Machine > Provisioning > Deploy template
> Virtual Machine > Provisioning > Read customization specification

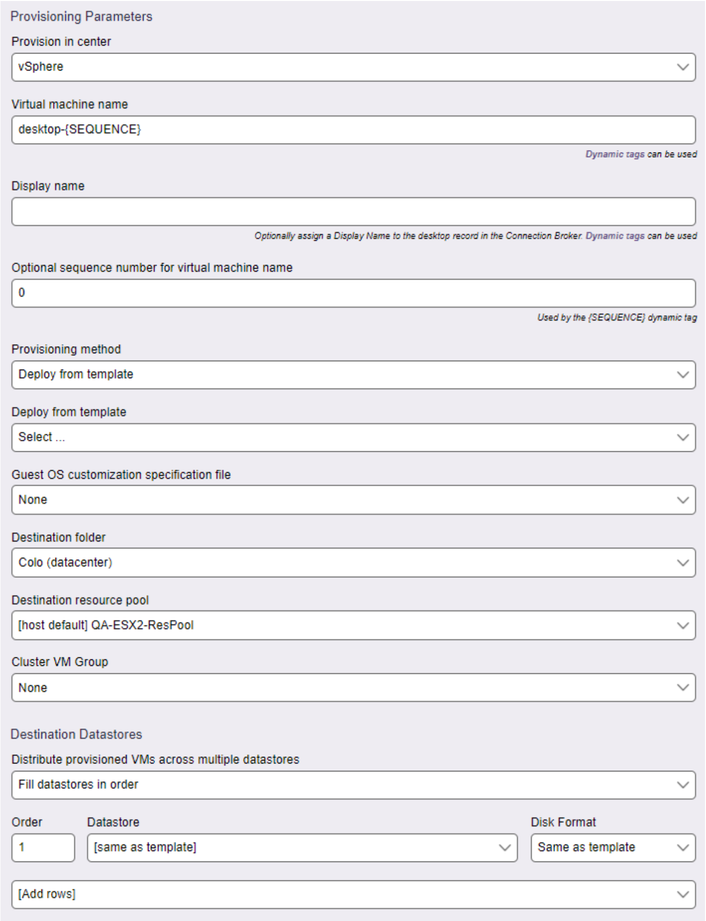
See the **Leostream Security Guide** for a complete list of permissions required for VMware Centers.

To provision from a VMware template, you must first create the template in vCenter Server. When provisioning Windows VMs, the Leostream Agent can reset the desktop's hostname and join it to your domain. If you require any other customizations, create a VMware customization file for the template.

Before creating your template, make sure you sign out of the Windows operating system and power down the VM by using the **Shut down** option on the Windows login screen. If you do not log out and shutdown the VM, the Connection Broker receives a connection notification from the Leostream Agent every time you provision a new VM from the template. The Connection Broker subsequently updates the **Last Connect Time** for the desktop record even through no Leostream user connected to the desktop, resulting in misleading information displayed on the **> Resources > Desktops** page.

Use the **Provisioning Parameters** section to configure provisioning using a vCenter Server template:

1. Select the center to provision new machines into from the **Provision in center** drop-down menu. The remainder of the form updates based on the contents of your selection. The following figure shows an example of the **Provisioning Parameters** section.



Provisioning Parameters

Provision in center: vSphere

Virtual machine name: desktop-{SEQUENCE}

Dynamic tags can be used

Display name:

Optionally assign a Display Name to the desktop record in the Connection Broker. Dynamic tags can be used

Optional sequence number for virtual machine name: 0

Used by the {SEQUENCE} dynamic tag

Provisioning method: Deploy from template

Deploy from template: Select ...

Guest OS customization specification file: None

Destination folder: Colo (datacenter)

Destination resource pool: [host default] QA-ESX2-ResPool

Cluster VM Group: None

Destination Datastores

Distribute provisioned VMs across multiple datastores: Fill datastores in order

Order	Datastore	Disk Format
1	[same as template]	Same as template

[Add rows]

2. Enter a name for the virtual machine in the **Virtual Machine Name** edit field. You can use dynamic tags to create a name from a mixture of static and dynamic variables. See **Using Dynamic Tags to Create Provisioning Variables** for an example.

3. Optionally enter a user-friendly display name into the **Display name** edit field. You can specify in the user's policy if the Connection Broker should display the desktop to the user with its display name instead of virtual machine name.

4. If either of the names contains a `{SEQUENCE}` dynamic tag, enter the starting number for the sequence in the **Optional sequence number for virtual machine name** edit field. The Connection Broker starts naming virtual machines at this number and increments the number for each machine created.

5. Select **Deploy from template** from the **Provisioning method** drop-down menu. For information on provisioning linked clones from snapshots, see **Provisioning VMware Linked Clones**.

6. Select the template to use from the **Deploy from template** drop-down menu. This menu contains all the templates available in the center you selected.

7. Select the customization file from the **Guest OS Customization Specification File** drop-down menu.

8. From the **Destination folder** drop-down menu, select the folder to use for newly provisioned virtual machines.

9. Select the resource pool in which to create the new virtual machine from the **Destination resource pool** drop-down menu.

10. Optionally select a destination from the **Cluster VM Group**.

11. In the **Destination Datastore** section, define the data store in which to create the new virtual machines, as follows.

    a. If using multiple datastores for new virtual machines, use the **Distribute provisioned VMs across multiple datastores** drop-down menu to indicate how the Connection Broker should select the datastore for each new VM. Options include:

       Fill datastores in order: The Connection Broker places new VMs into the first datastore, until that datastore is full. After each datastore fills, the Connection Broker uses the next datastore, in order.

       Distribute randomly across all datastores: The Connection Broker randomly chooses a datastore from the list of specified datastores.

       Place on datastore with most free space: The Connection Broker always uses the datastore with the most free space at the time the virtual machine is being provisioned.

    b. When selecting **Fill datastores in order** from the **Distribute provisioned VMs across multiple datastores** drop-down menu, use the **Order** column to indicate the order in which to fill the datastores.

    c. From the **Datastore** drop-down menu, select the datastores that the Connection Broker should use for provisioned machines.
    d. From the **Disk format** drop-down menu, select the disk format to use for virtual machines provisioned to each datastore.

    e. Use the **Add rows** drop-down menu to specify additional datastores for provisioning.

       To remove a row from the **Destination Datastore** table, select **<Remove this datastore>** from the **Datastore** drop-down in that row. After you save the form, the datastore associated with this row is no longer used for newly provisioned virtual machines.

12. Use the **Actions to execute after provisioning completes** section to schedule actions such as joining the newly provisioned machine to your domain and taking a snapshot. See **Scheduling Post-Provisioning Actions** for more details.

    You must add the **Join domain** action to this table to indicate if newly provisioned machines are joined to your domain at the time they are provisioned. Otherwise, the Connection Broker will not join the machine to your domain until a subsequent Leostream Agent registration arrives, for example when the machine is next rebooted.

The default action marks the machine as available for assignment to end users. If you are pre-provisioning machines and do not want them to be immediately available for assignment, switch the default **Action to execute** to **Mark desktop as Unavailable for assignment**.

13. Select the **Initialize newly provisioned desktops as deletable** option to indicate that the Connection Broker is allowed to delete this VM from disk. When this option selected, the **Edit Desktop** page for the newly provisioned VM has the **Allow this desktop to be permanently deleted from disk** option selected, by default. Use release plans to schedule VM deletion.

14. Click **Save**.

Provisioning VMware Linked Clones

To create virtual machines that are linked clones, use the **Provisioning Parameters** section to configure provisioning from virtual machine snapshots, as follows.

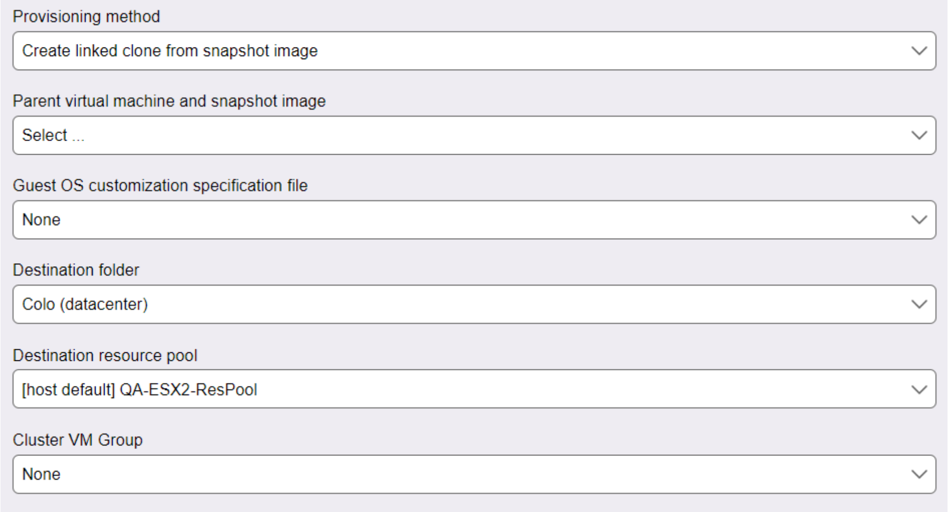
1. Select the center to provision new machines into from the **Provision in center** drop-down menu. The remainder of the form updates based on the contents of your selection.

2. Enter a name for the virtual machine in the **Virtual Machine Name** edit field. You can use dynamic tags to create a name from a mixture of static and dynamic variables. See **Using Dynamic Tags to Create Provisioning Variables** for an example.

3. Optionally enter a user-friendly display name into the **Display name** edit field. You can specify in the user's policy if the Connection Broker should display the desktop to the user with its display name instead of virtual machine name.

4. If either of the names contains a `{SEQUENCE}` dynamic tag, enter the starting number for the sequence in the **Optional sequence number for virtual machine name** edit field. The Connection Broker starts naming virtual machines at this number and increments the number for each machine created.

5. Select **Create linked clone from snapshot image** from the **Provisioning method** drop-down menu, as shown in the following figure.



Provisioning method

Create linked clone from snapshot image

Parent virtual machine and snapshot image

Select ...

Guest OS customization specification file

None

Destination folder

Colo (datacenter)

Destination resource pool

[host default] QA-ESX2-ResPool

Cluster VM Group

None

6. Select the snapshot to use from the **Parent virtual machine and snapshot image** drop-down menu. This menu contains all the templates available in the center you selected.

7. Select the customization file from the **Guest OS Customization Specification File** drop-down menu.

8. From the **Destination folder** drop-down menu, select the folder to use for newly provisioned virtual machines.

9. Select the resource pool in which to create the new virtual machine from the **Destination resource pool** drop-down menu.

10. Optionally select a destination from the **Cluster VM Group**.

11. In the **Destination Datastore** section, define the data store in which to create the new virtual machines, as follows.

    a. If using multiple datastores for new virtual machines, use the **Distribute provisioned VMs across multiple datastores** drop-down menu to indicate how the Connection Broker should select the datastore for each new VM. Options include:

       Fill datastores in order: The Connection Broker places new VMs into the first datastore, until that datastore is full. After each datastore fills, the Connection Broker uses the next datastore, in order.

       Distribute randomly across all datastores: The Connection Broker randomly chooses a datastore from the list of specified datastores.

       Place on datastore with most free space: The Connection Broker always uses the datastore with the most free space at the time the virtual machine is being provisioned.

    b. When selecting **Fill datastores in order** from the **Distribute provisioned VMs across multiple datastores** drop-down menu, use the **Order** column to indicate the order in which to fill the datastores.

c. From the **Datastore** drop-down menu, select the datastores that the Connection Broker should use for provisioned machines.

d. Use the **Add rows** drop-down menu to specify additional datastores for provisioning.

To remove a row from the **Destination Datastore** table, select **<Remove this datastore>** from the **Datastore** drop-down in that row. After you save the form, the datastore associated with this row is no longer used for newly provisioned virtual machines.

12. Use the **Actions to execute after provisioning completes** section to schedule actions such as joining the newly provisioned machine to your domain and powering it down. See **Scheduling Post-Provisioning Actions** for more details.

    You must add the **Join domain** action to this table to indicate if newly provisioned machines are joined to your domain at the time they are provisioned. Otherwise, the Connection Broker will not join the machine to your domain until a subsequent Leostream Agent registration arrives, for example when the machine is next rebooted.

    The default action marks the machine as available for assignment to end users. If you are pre-provisioning machines and do not want them to be immediately available for assignment, switch the default **Action to execute** to **Mark desktop as Unavailable for assignment**.

13. Select the **Initialize newly provisioned desktops as deletable** option to indicate that the Connection Broker is allowed to delete this VM from disk. When this option selected, the **Edit Desktop** page for the newly provisioned VM has the **Allow this desktop to be permanently deleted from disk** option selected, by default. Use release plans to schedule VM deletion.

14. Click **Save**.

Provisioning in Red Hat Virtualization

Use the **Provisioning Parameters** section to configure how Leostream provisions new virtual machines in your Red Hat Virtualization environment, as follows.

1. Select your Red Hat Virtualization environment from the **Provision in center** drop-down menu. The **Provisioning Parameters** update to include the platform specific options.

2. Configure the **Virtual machine name** for the newly provisioned machines.

   Note: If you created your pool based on the desktop name, make sure the **Virtual machine name** is set to satisfy the naming convention so the newly provisioned machines are placed in this pool. Creating a desktop in a particular pool does not guarantee it is placed in that pool if the desktop does not satisfy the rules in the pool definition.

3. Optionally enter a user-friendly display name into the **Display name** edit field. You can specify in the user’s policy if the Connection Broker should display the desktop to the user with its display name instead of virtual machine name.

4. If either of the names contains a `{SEQUENCE}` dynamic tag, enter the starting number for the sequence in the Optional sequence number for virtual machine name edit field. The Connection Broker starts naming virtual machines at this number and increments the number for each machine created.

5. Use the **Cluster** drop-down menu to select the cluster for the new virtual machines.

6. Select your master image from the **Deploy from template** drop-down menu. This menu contains all templates in your Red Hat Virtualization environment. Ensure that you select an image that contains a Leostream Agent that is registered with your Connection Broker.

7. Use the **Actions to execute after provisioning completes** section to schedule actions such as joining the newly provisioned machine to your domain and powering it down. See **Scheduling Post-Provisioning Actions** for more details.

   You must add the **Join domain** action to this table to indicate if newly provisioned machines are joined to your domain at the time they are provisioned. Otherwise, the Connection Broker will not join the machine to your domain until a subsequent Leostream Agent registration arrives, for example when the machine is next rebooted.

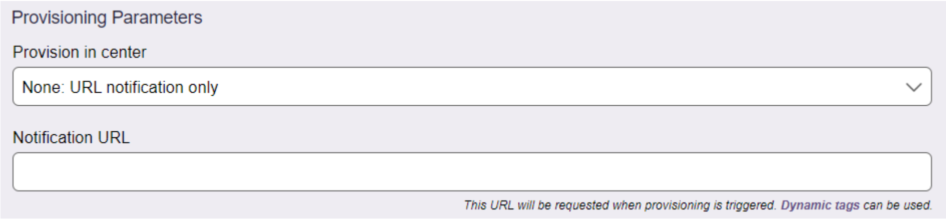
   The default action marks the machine as available for assignment to end users. If you are pre-provisioning machines and do not want them to be immediately available for assignment, switch the default **Action to execute** to **Mark desktop as Unavailable for assignment**.

8. If you want Leostream to delete virtual machines when the user logs out, ensure that you select the **Initialize newly-provisioned desktops as “deletable”** checkbox.

9. Click **Save**.

Provisioning using URL notification

In addition to using the built-in provision supported for each center, you can call out to any third-party system to perform provisioning by selecting **None: URL notification only** from the **Provision in center** drop-down menu. In this case, the **Provisioning Parameters** section appears as follows.



Provisioning Parameters

Provision in center

None: URL notification only

Notification URL

This URL will be requested when provisioning is triggered. Dynamic tags can be used.

To provision from an external source:

1. In the **Notification URL** field, enter the URL to call to perform the provisioning. The Connection Broker sends an HTML-based request to the external provisioning system. For example:

```
http://10.1.1.1/provision?for_pool={POOL_NAME}
```

This URL can contain a limited set of dynamic tags, such as `{POOL_NAME}`, `{TEMPLATE_NAME}`, and `{SNAPSHOT_NAME}`, that are dynamically changed to provide the external system with the name of the pool requiring another desktop.

2. Click **Save**.

Using Dynamic Tags in Provisioning Parameters

Dynamic tags allow you to create a name or URL from a mixture of static and dynamic variables. The Connection Broker parses and replaces dynamic tags in provisioning strings at run-time. In the URL field, the replacement is URL-encoded.

Provisioning strings support the following dynamic tags:

- `{POOL_NAME}` - The name of the pool triggering the provisioning
- `{TEMPLATE_NAME}` - The name of the template used for deployment
- `{SNAPSHOT_NAME}` - The name of the snapshot used for deployment from a Linked Clone.

Virtual machine and display names also support the following `{SEQUENCE}` tags.

- `{SEQUENCE}` - Used for sequential virtual machine names
- `{SEQUENCE_n}` - Where n is a string of zeros specifying the maximum length of the sequence number. The result is similar to the `{SEQUENCE}` tag, but pads the sequence number with leading zeros.
- `{SEQUENCE_min-to-max}` - Where min and max are minimum and maximum values for a sequence.

For example, if you provision from a VMware template named `Sales` and enter the number `4` in the **Optional sequence number for virtual machine name** edit field, the following string in the **Virtual Machine Name**:

```
New{TEMPLATE_NAME}{SEQUENCE}
```

Results in the first provisioned virtual machine being named `NewSales4`, the second virtual machine being named `NewSales5`, and so on.

Entering the string `{TEMPLATE_NAME}{SEQUENCE_0003-to-0012}` in the **Virtual Machine Name** field results in virtual machines names like `Sales0003`, `Sales0004`, and up to `Sales0012`, before rotation back to the name `Sales0003`.

⚠ The `{SEQUENCE}` tags cannot be used in notification URLs.

Scheduling Post-Provisioning Actions

The **Actions to execute after provisioning completes** section of the **Provisioning Parameters** allows you to execute a set of ordered actions after the instance is fully provisioned, with the final action being the option to make the desktop available for assignment to an end user.

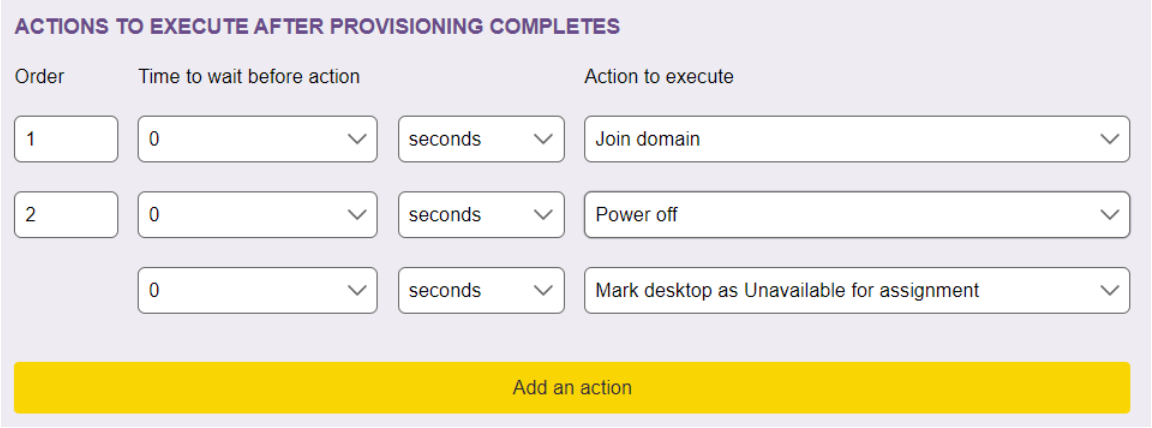
The currently supported actions include:

- Create a snapshot – When provisioning into VMware centers, only, take a snapshot of the machine that can be used with the Policy and Plan options to revert machines back to their most recent snapshot.
- Join domain – Join newly provisioned VMs to the domain configured in the **Domain Join** section of the pool when the **Join machine to a domain** option is selected.
- Power off – Stop the instance. Powering the machine off after it is provisioned may lower compute costs in the cloud. When using this option ensure that your Policies are configured to offer stopped machines and to either power the machine on when the user requests a connection or allow users to start their offered machines (enabled via Role and Policy options).
- Power on – By default, machines are provisioned in a running state. Use this action to power the machine back on if it was powered off by a previously scheduled action.
- Mark desktop as Available for assignment – Indicate that the machine is ready to be offered to a user by the Connection Broker.
- Mark desktop as Unavailable for assignment – Place the machine into maintenance mode so that the Connection Broker will not offer it to a user. Use this option if you need to perform some post-provisioning actions on the machine prior to offering it to a user. You must manually switch the machine back to an Available state.

Each action can be delayed by a customizable amount of time, allowing you to perform a series of external actions on the desktop, such as running an initialization script to install applications, etc., before moving to the action.

Example: Joining Provisioned Machines to a Domain and Powering them Off

When pre-provisioning desktops in a cloud, you can save money by keeping the machine powered off until a user requests a connection. The following figure shows how to configure the **Actions to execute after provisioning completes** section to achieve this workflow.



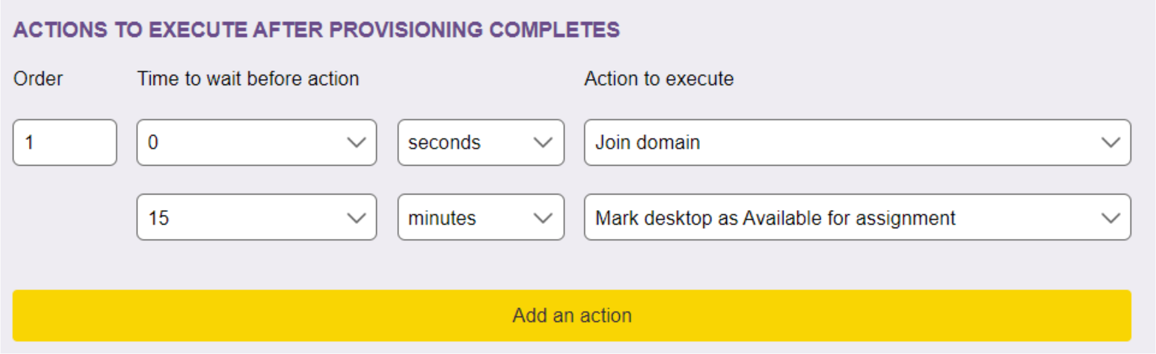
ACTIONS TO EXECUTE AFTER PROVISIONING COMPLETES

Order	Time to wait before action		Action to execute
1	0	seconds	Join domain
2	0	seconds	Power off
	0	seconds	Mark desktop as Unavailable for assignment

In this example, the Connection Broker joins the newly provisioned machine to your domain as soon as the machine finishes provisioning. Immediately after the domain join completes, the Connection Broker powers down the machine and then marks it as available for assignment

Example: Waiting for User-Defined Scripts to Execute

If you need to perform actions on a newly provisioned desktop, such as installation applications or running any customization scripts, you can indicate that the Connection Broker should delay marking the machine as available to give your customizations enough time to complete, as shown in the following figure.



ACTIONS TO EXECUTE AFTER PROVISIONING COMPLETES

Order	Time to wait before action		Action to execute
1	0	seconds	Join domain
	15	minutes	Mark desktop as Available for assignment

In this example, the **Actions to execute after provisioning completes** section is configured to join the newly provisioned machine to your domain as soon as the machine finishes provisioning, but then wait for 15 minutes after the domain join completes before marking the desktop as available.

The Connection Broker does not monitor processes or scripts running on the desktop. Ensure that you set any wait times appropriately so the desktop is not marked available before it is ready for assigment.

Chapter 10: Configuring User Roles and Permissions

Overview

Roles determine what Connection Broker functionality a particular user can view and use. A particular role consists of a set of permissions, which are grouped into three types.

- **Connection Broker Login Permissions:** Define if the user has permission to log in as an end user, an administrator, and/or to access the Leostream RESTful API.
- **End User Session Permissions:** Define what tasks a user has permission to perform when they log into a Connection Broker client, such as the Web client or Leostream Connect, for example:
  - Power control their desktops
  - Release their desktops
  - Manage another user's resources
  - Log in as a local user on the remote desktop
  - Use the Leostream API
- **Connection Broker Administrator Web Interface Permissions:** Define Connection Broker settings in the Connection Broker Administrator Web interface the user has permission to view or edit.

The Connection Broker assigns a role to all users, including the default Connection Broker Administrator. You can create as many roles as required by your environment. By default, the Connection Broker provides two default roles, described in the following sections.

The Default Administrator Role

The default Administrator role has permission to edit all Connection Broker configuration settings in the Administrator Web interface.

You cannot limit the amount of access to the Connection Broker Administrator Web interface provided by the default Administrator role, nor can you delete the default Administrator role. Create new roles to define sub-administrators with more limited access to your Connection Broker configuration.

The default local Leostream administrator (`admin`) is assigned this default Administrator role. You can also assign the default Administrator role to other user and indicate if they also need access to the Leostream Web client to connect to their policy-offered resources (see **Controlling Access to the Administrator Web Interface**). For these users, you can modify the session permissions that apply to their login. See **Session Permissions** for more information.

The Default User Role

The default user role allows the user to log in through any client device, including the Leostream Web client, and access their offered desktops. The default User role cannot log into the Connection Broker Administrator Web interface.

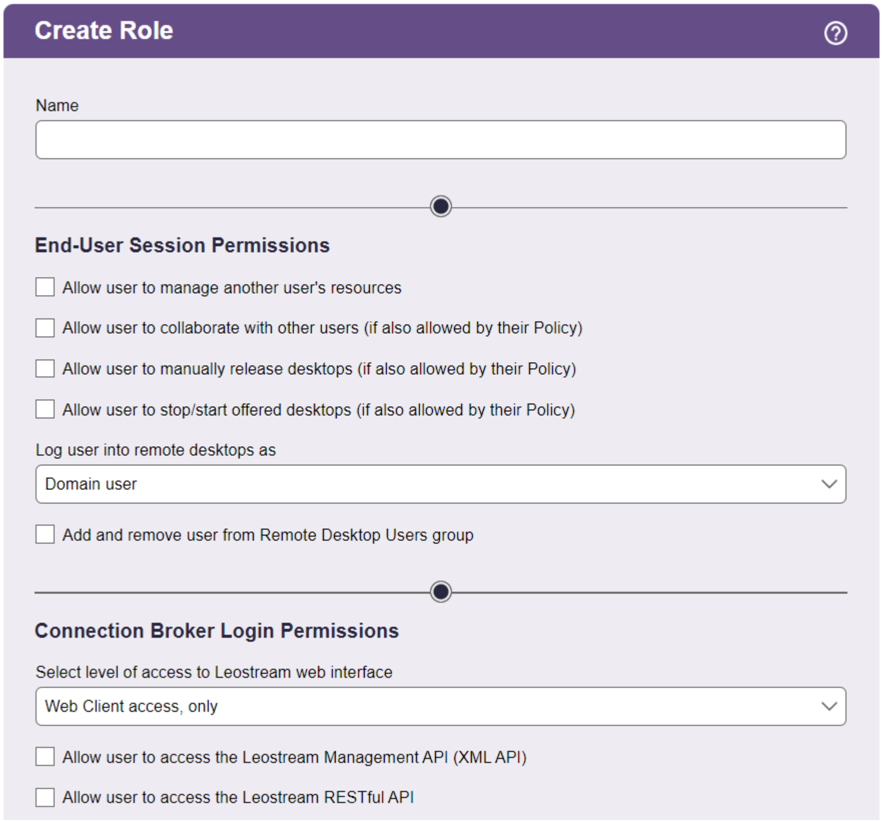
You can modify the session permissions in the default user role or update it to provide access to the Connection Broker Administrator Web interface. See **Session Permissions** for a description of the available session permissions in the default User role. If you prefer to retain a User Role that does not have any access to the Connection Broker Administrator Web interface, but do need to delegate some level of administrator access to users, create new roles that provide the necessary permissions.

Adding Roles

To create a new role:

1. Go to the **> Configuration > Roles** page.

2. Click on the **Create Role** link to open the **Create Role** dialog, shown in the following figure:



Create Role

Name

End-User Session Permissions

□ Allow user to manage another user's resources

□ Allow user to collaborate with other users (if also allowed by their Policy)

□ Allow user to manually release desktops (if also allowed by their Policy)

□ Allow user to stop/start offered desktops (if also allowed by their Policy)

Log user into remote desktops as: Domain user

□ Add and remove user from Remote Desktop Users group

Connection Broker Login Permissions

Select level of access to Leostream web interface: Web Client access, only

□ Allow user to access the Leostream Management API (XML API)

□ Allow user to access the Leostream RESTful API

3. Enter a name for the new role in the **Name** edit field.

4. Configure the **End-User Session Permissions** to provide access to Connection Broker actions. See **Session Permissions** for a description of the available session permissions.

5. Use the **Connection Broker Login Permissions** section to provide access to additional functionality (see **Controlling Access to the Administrator Web Interface** and **Defining Roles for RESTful API Access**).

6. If the selection in the **Select level of access to Leostream web interface** drop-down menu indicates that the user can log into the Administrator Web interface, use the remainder of the form to specify the Connection Broker Administrator Web interface permissions (see Administrator Web Interface Permissions).

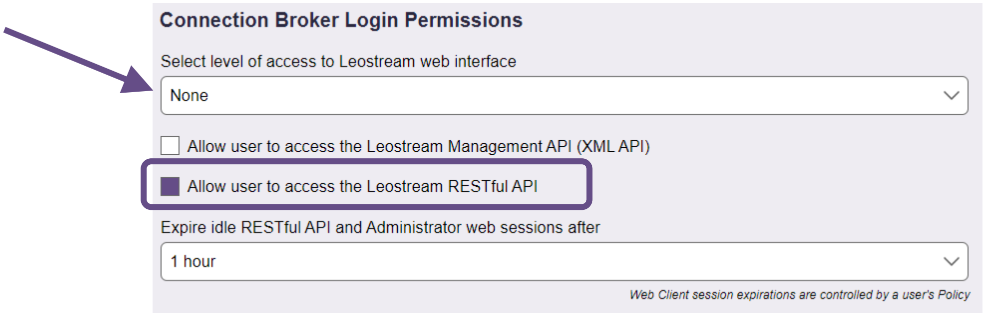
7. Enter any **Notes** that you wish to save with the role definition.

8. Click **Save**.

Defining Roles for Leostream API Access

If you are creating a role for users that will call the Leostream RESTful API or XML API, ensure that you select the **Allow user to access the Leostream RESTful API** option or **Allow user to access the Leostream Management API (XML API)** option, respectively, in the **Connection Broker Login Permission** section. Without this option selected, the login API returns a 403 Forbidden error.

For example, to give a user account permission to execute the RESTful API but not to login to the Administrator Web interface, prohibit logins to the Leostream Web interface by selecting **None** from the **Select level of access to Leostream web interface** drop-down menu, as shown in the following figure, and select the **Allow user to access the Leostream RESTful API** option.



Connection Broker Login Permissions

Select level of access to Leostream web interface

None

□ Allow user to access the Leostream Management API (XML API)

☑ Allow user to access the Leostream RESTful API

Expire idle RESTful API and Administrator web sessions after

1 hour

Web Client session expirations are controlled by a user's Policy

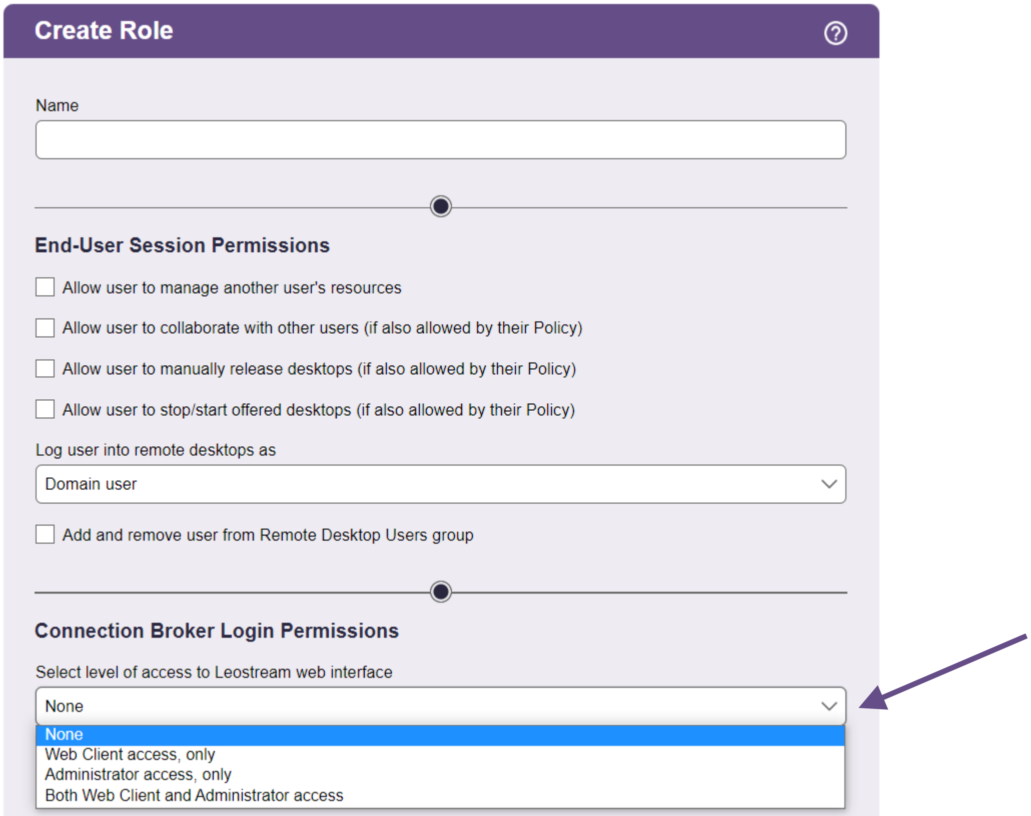
If the role is used by users who only execute the RESTful API, you can disable access to the Leostream Web interface by selecting **None** from the **Select level of access to Leostream web interface** drop-down menu, as shown in the previous figure. The **Expire idle RESTful API and Administrator web sessions after** drop-down menu allows you to time out idle sessions. After the session expires, you must reauthenticate with the RESTful API to perform additional actions.

The remainder of the role should set the appropriate level of permissions for the different objects in the Connection Broker. For example, if you plan to modify pools via the API, ensure that the role sets the permission for the **Pools** page to **Full** access. See **Controlling Access to the Administrator Web Interface** for a description of the permissions available for scoping access to the Administrator Web interface.

Controlling Access to the Administrator Web Interface

The user's role determines if and how much access the user has to the Connection Broker Administrator Web interface. Users with the default **User** role have no access to the Administrator Web interface, while users with the default **Administrator** role have complete access.

To provide access to a subset of the Administrator Web interface functionality, or to allow end users to access both the Leostream Web client and the Administrator Web interface, create new roles and specify the level of access from the **Select level of access to Leostream web interface** option, shown in the following figure.



Create Role

Name

End-User Session Permissions

□ Allow user to manage another user's resources

□ Allow user to collaborate with other users (if also allowed by their Policy)

□ Allow user to manually release desktops (if also allowed by their Policy)

□ Allow user to stop/start offered desktops (if also allowed by their Policy)

Log user into remote desktops as: Domain user

□ Add and remove user from Remote Desktop Users group

Connection Broker Login Permissions

Select level of access to Leostream web interface: None

None
Web Client access, only
Administrator access, only
Both Web Client and Administrator access

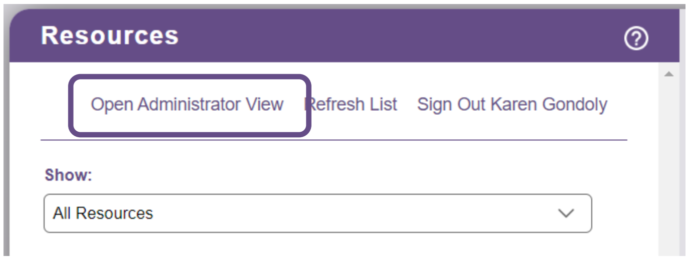
The options are:

- **None:** Users with this role are blocked from logging into the Administrator Web interface and Leostream web client. Use this setting to create a role for accounts whose only purpose is to execute the Leostream RESTful API.

- **Web Client access, only** – When the user logs into Leostream from a Web browser, they are presented with their policy-assigned and hard-assigned desktops. The user cannot access any functionality in the Administrator Web interface.

- **Administrator access, only** – When the user logs into Leostream from a Web browser, they are taken directly into the Administrator Web interface. The **Administrator Web Interface Permissions** determines the functionality presented to the user. If the user also has policy or hard-assigned desktops, they must log in from a different client type, such as Leostream Connect, to access those desktops.

- **Both Web Client and Administrator access** – When the user logs into Leostream from a Web browser, they see their policy and hard-assigned desktops. They user can click the **Open Administrator View** link, shown in the following figure, to launch a second Leostream Web session with access to the Administrator Web interface.

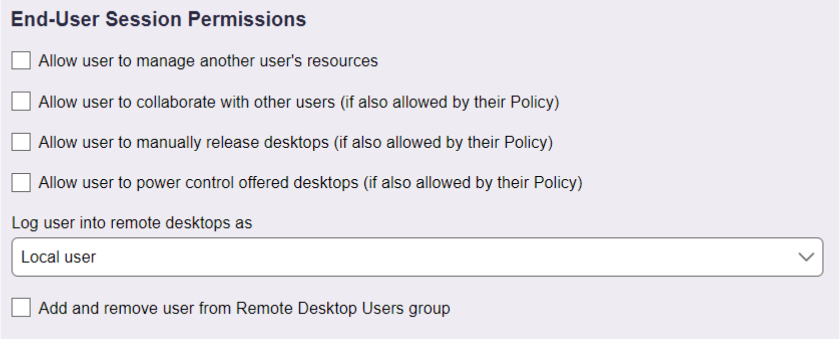


If either of the options that provide access to the Administrator Web interface is selected, you can indicate how long the user's session is valid using the **Expire idle RESTful API and Administrator web sessions after** drop-down menu. After the selected time frame passes, the user must re-authenticate to access any page in the Administrator Web interface.

This option does not apply to end users' Leostream sessions established from the Leostream Web client, Leostream Connect, or a PCoIP client. Use the **Expire user's resource offers and Connection Broker session after specified elapsed time** option in the user's general policy settings to indicate when an end-user session expires.

Session Permissions

Session permissions, shown in the following figure, define what actions a user with this role is allowed to perform when logged into a Leostream Client, either the Leostream Web client, Leostream Connect, or a PCoIP client. Different session permissions apply to different types of clients.



End-User Session Permissions

□ Allow user to manage another user's resources

□ Allow user to collaborate with other users (if also allowed by their Policy)

□ Allow user to manually release desktops (if also allowed by their Policy)

□ Allow user to power control offered desktops (if also allowed by their Policy)

Log user into remote desktops as

Local user

□ Add and remove user from Remote Desktop Users group

Overview

The current session permissions are as follows:

- **Allow user to manage another user's resources**: (*This option apply to PCoIP clients and the*

Windows version of Leostream Connect.) Select this option if a user with this role should be able to view the desktops offered to another user, and then log into those desktops. Use this option for user's that are allowed to perform administrative tasks on another user's desktop, or for users that need to log into their own desktop using different credentials from those they provided when logging into the Connection Broker.

The managed user must have the same policy as the manager.

- **Allow user to collaborate with other users**: (*This option applies to the Leostream Web client and the Windows version of Leostream Connect.)* Select this option if the user connects to their desktop using the NoMachine, Mechdyne TGX, or HP ZCentral Remote Boost (RGS) display protocols and they need to invite other users to shadow their session. Both the user who owns the session and the user who shadows the session must have this permission enabled. The user's policy indicates which pools contain desktops that support collaboration via shadowing (see "Session Shadowing and Collaboration" in the Leostream Guide for Working with Display Protocols).

- **Allow user to manually release desktops**: (*This option applies to the Leostream Web client and the Windows version of Leostream Connect.)* Select this option if a user with this role may manually release a desktop back to its pool. By default, when a user connects to a desktop, the Connection Broker assigns that desktop to that user. When a desktop is assigned to a user, the Connection Broker will not offer that desktop to another user.

  If a user manually releases one of their desktops back to its pool, the Connection Broker unassigns the desktop from that user and invokes the release plan associated with the desktop. If the user is not logged out of the desktop after it is released, the Connection Broker considers the logged in user as a *rogue* user. Because the desktop is placed back in its pool, the Connection Broker may offer that desktop to another user. If this new user tries to connect to the desktop, and their policy is set to log off rogue users, the Connection Broker forcefully logs out the original user.

  If the **Prevent user from manually releasing desktop** option is selected for a pool in the user's policy, the user is not able to release desktops from this pool, even though their role gives them the permission.

  The user can never release a hard-assigned desktop.

- **Allow user to power control offered desktops**: (*This option applies to the Leostream Web client and both versions of Leostream Connect.)* Select this option if a user with this role may stop, start, restart, or hard-reset their desktop. The user's policy indicates which power control options the user is presented. For example, if the **Allow user to stop/start offered desktop** policy option is set to **No** for a pool in the user's policy, the user cannot stop and start the desktops in this pool, even though their role gives them the permission.

- **Allow user to access the Leostream Management API**: Select this option if the user executes scripts using one of the Leostream APIs. When executing APIs that query or configure settings in the Connection Broker, the user's role must also provide the required permission for the associated functionality on the Administrator Web interface. For information and documentation on the Leostream APIs, contact sales@leostream.com.

- **Log user into remote desktops as**: Use this option to indicate if the Connection Broker logs the user into the remote desktop using a domain account or local user account. Use local users to support, for example, LDAP or non-domain users that need to log in to remote desktops.

  This setting determines the value the Connection Broker sets for the user's domain either in their protocol plan or when sending domain information directly to Leostream Connect. When logging users in as a local user, the Connection Broker sets the user's domain to the hostname of their remote destkop.

  Options in the **Log user in as** drop-down include.

  - **Domain user**: When using an Active Directory domain user account, the Connection Broker uses the information specified by the authentication server that authenticated the user when they logged into the Connection Broker.
  - **Local user**: When logging in as a local user, the Connection Broker requires an existing user account on the remote desktop. This user account must have the same login name as the user that logged into the Connection Broker. When using this option, you must manually create the appropriate local user account on the remote desktop.

    If you want the Connection Broker to manage the local user account, use one of the following two options.
  - **Local user (create on login)**: (*Windows and Linux, only. Requires a Leostream Agent on the remote desktop.*) You can instruct the Connection Broker to create new local user accounts, to avoid manually creating accounts on each remote desktop. When this option is selected, the Connection Broker automatically creates an appropriate local user on the desktop the first time the user logs in. If an appropriate user account already exists, the Connection Broker uses that account.

    If the existing user account has a different password from the password used to log into the Connection Broker, the Connection Broker changes the password for the local user on the remote desktop.
  - **Local user (create on login; delete user on logout):** (*Windows and Linux, only. Requires a Leostream Agent on the remote desktop.*) You can instruct the Connection Broker to create and delete local user accounts, to avoid managing the accounts on each remote desktop. When this option is selected, the Connection Broker automatically creates an appropriate local user account on the desktop the first time the user logs in. The Connection Broker removes the user account as soon as the user logs out of the desktop.

    The Connection Broker does not delete the profile folder associated with the user. Any information stored in the profile folder can be recovered by the desktop's administrator.

    ⚠ When the user subsequently logs into the desktop, the Connection Broker creates a new local user account. Because this is a new account, the Windows desktop does not associate this user with the profile created the last time the user logged in. If user's need persistent access to their profile, use the **Local user (create on login)** option.

- **Local user (create on login; delete user and profile on logout):** When this option is selected, the Connection Broker automatically creates an appropriate local user account on the desktop the first time the user logs in. The Connection Broker removes the user account and the user's profile folder as soon as the user logs out of the desktop.

  ⚠ The user loses all locally stored information when their profile folder is deleted.

- **Add and remove user from Remote Desktop Users group**: (*Windows, only. Requires a Leostream Agent on the remote desktop.*) Use this option if your users are not already members of the Remote Desktop Users group on their offered Windows desktops. The desktop must already contain a group exactly named "Remote Desktop Users".

  By default, Windows desktops do not provide remote access using RDP. After you enable remote access for a particular desktop, you must indicate which users are allowed to remotely log into that desktop by placing those users in the Remote Desktop Users group.

  When a user is part of the Remote Desktop Users group, they can remotely log into the desktop from any client. To restrict the user to log in only through the Connection Broker, do not manually add users to the Remote Desktop Group and, instead, select the **Add and remove user from Remote Desktop Users group** option. With this option selected, the Connection Broker automatically adds the user to the Remote Desktop Users group when the user logs into the desktop from the Connection Broker. When the user logs out, the Connection Broker automatically removes the user from the Remote Desktop Users group.

  ⚠ The Connection Broker takes control of the user's membership in the Remote Desktop Users group. If the user was already a member of the Remote Desktop Users group before they logged into the desktop via Leostream, the Connection Broker removes the user from the group when they log out of the desktop. The Connection Broker adds the user back to the Remote Desktop Users group the next time they log into the Connection Broker.

Managing another User's Resources

The **Allow user to manage another user's resources** session permission allows a user to log into the Connection Broker and retrieve the list of resources offered to another user. This permission is useful in situations where members of your organization must be able to access their own desktops, while also being able to log in to and troubleshoot other staff members' desktops. When managing a resource, you log into the other user's desktops using credentials other than those you provided when logging into the Connection Broker.

The following client devices currently support this feature.

- The Windows version of Leostream Connect
- PCoIP clients

The following sections describe, in general, the functionality behind managing another user's resources. See the **Leostream Connect Administrator Guide and End User's Manual** for information on how to manage another user's resources from Leostream Connect. See the **Leostream Quick Start Guide for PCoIP Remote Workstation Cards** for information on managing another user's session from a PCoIP client device.

How the Connection Broker Determines the Offered Resource List

When you manage another user's resources, the Connection Broker offers you resources based on the managed user's policy. The policy assigned to the managed user is determined by the **Assignments** form for each authentication server in the Connection Broker.

The managed user and the manager must be assigned to the same policy.

After the Connection Broker finds the managed user's policy, it looks at the following policy sections to determine what resources to show to the manager.

- The **Filters** section for constraining which desktops to pull from all desktop pools.
- The **When User Logs into the Connection Broker** section for all pools in the **Desktop Assignment from Pools** section, with the exception of the **Allow users to reset offered desktops** option. You cannot restart a managed dekstop.
- The selection in the **Protocol** plan drop-down menu for each pool.
- In the **Desktop Hard Assignments** section, the **Display to user as** and **Protocol** plans drop-down menus.

All other aspects of the managed user's policy are ignored. Based on the previously listed sections, the Connection Broker offers you, as the manager, the following resources to manage.

- All desktops hard-assigned to the managed user.
- For each pool in the **Desktop Assignment from Pools** section of the managed user's policy, the desktops determined by the **When User Logs into the Connection Broker** section after any constraints in the **Filters** section have been applied.

When determining which desktops to offer from the pool, the Connection Broker always offers any desktops that are currently assigned to the managed user. The Connection Broker then picks the remaining desktops based on the availability of desktops in the pool. The Connection Broker preferentially selects any desktops that were previously assigned to the user, if that desktop is still available, then randomly selects additional available desktops. The resulting offer list may not exactly match the list of desktops that would be offered to the user.

Connecting to a Managed Resource

The Connection Broker connects you to the managed desktop using the protocol determined by the protocol plan in the managed user's policy. If the managed user typically connects to their desktops using HP ZCentral Remote Boost (RGS), you must log into their desktop from a client that supports Remote Boost.

When you log into a managed resource, the Connection Broker does *not* assign that resource to you. Because you are not assigned to the desktop:

- The Connection Broker does not honor any settings in the **When User is Assigned to Desktop** section of the managed user's policy.
- The Connection Broker does not use the selections in the **Power control** or **Release** plan drop-down menus in the managed user's policy.
- You do not appear in the **User** column for that desktop in the Connection Broker **> Resources > Desktops** page.
- You will not appear in any resource usage reports run from the Connection Broker **> Dashboards > Reports** page.

Managing Your Own Resources

Managing your own resources allows you to log into your offered desktops using different credentials from what you provided to the Connection Broker. If your Connection Broker account does not have administrative privileges for your desktop, you can use the manage resource feature to, for example, log into your desktop using administrator credentials.

Managing another User's Resources

Managing another user's resources allows you to perform administrative tasks on the user's desktop. The user's policy determines which resources are offered by the Connection Broker.

You and the managed user must have the same policy.

When you try to log into a managed desktop, if the managed user is still logged in and you provide non-administrator credentials, you will not automatically log the user out. Only administrators are allowed to automatically log another user out of their desktop.

Similarly, because the Connection Broker does not assign you to the desktop you are managing, you are technically a rogue user on that desktop. The Connection Broker may offer that desktop to another user. If you are not logged into the desktop as an administrator and the Connection Broker offers that desktop to a user with a policy that logs out rogue users, the Connection Broker automatically logs you out to accommodate the new user.

Administrator Web Interface Permissions

The Connection Broker Administrator Web Interface permissions allow you to provide or deny access to the various tasks involved in managing your Connection Broker configuration.

Setting Permission Levels

The permissions are controlled by a selection in their associated drop-down menus. The menus may contain any or all of the following options. Select the appropriate option from each permission drop-down menu.

- **No access**: Removes the related controls from the Connection Broker Administrator Web interface. With a few exceptions (see **Permissions that Control Multiple Connection Broker Pages**) each permission controls one tab in the Connection Broker Administrator Web interface.

- **View only**: Shows the related controls on the Connection Broker Administrator Web interface, but does not allow the user to modify the contents. For example, a **View only** access setting for **Pools** allows the user to view how the pools are constructed, but does not allow them to save changes to the pool.

- **Full**: Allows the user to view and modify this portion of the Connection Broker Administrator Web interface, with the exception of aspects of the interface reserved for Administrator access.

- **Administrator**: Allows the user to view and modify all aspects of this portion of the Connection Broker Administrator Web interface (see **Providing Administrator Access to Users, Roles, and Desktops**).

- **Custom**: Allows you to control access to particular functionality on this portion of the Connection Broker Administrator Web interface. See the following sections for more information.

  Customizing Access to Desktops
  Customizing Access to the Authentication Server Page
  Customizing Access to the Maintenance Page

Permissions that Control Multiple Features

Most permissions control access to a particular page, section, or functionality in the Connection Broker Administrator Web interface. The following permissions control access to multiple pages. You cannot individually control the access to pages that are controlled by these permissions.

- The **Reports** permission controls access to the **> Dashboards > Reports** page and the **> Dashboards > Connection Broker Metrics** page.

- The **Desktops in Pool** permission controls the PCoIP host devices displayed on the **> Resources > PCoIP Host Devices** page. The page lists only PCoIP host devices that are associated with desktops selected in the **Desktops in Pool** permission or PCoIP host devices that are not associated with any desktop.

You must also have a role that provides access to the **> Resources > PCoIP Host Devices** page.

- If the **Desktops in Pool** permission is set to **No access** then the **Desktops – Imports** permission is ignored. The Connection Broker internally sets the **Desktops – Imports** permission to **No access**.

Providing Administrator Access to Users, Roles, and Desktops

The following permissions provide Administrator and Full access:

- **Users**
- **Roles**
- **Desktops in Pool (Custom) > Edit (Custom) > Availability**

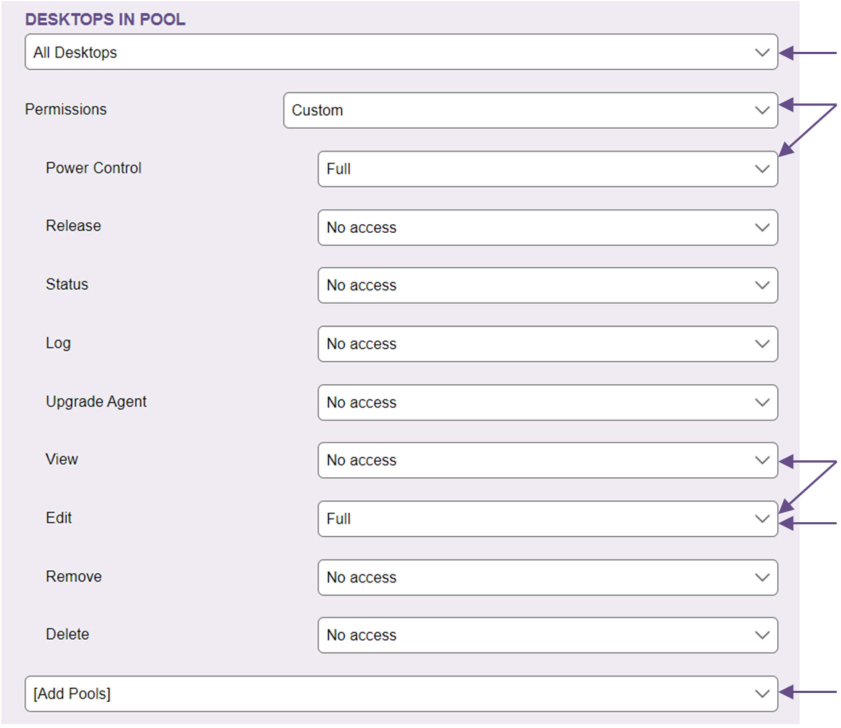
The Administrator permission provides access to additional functionality in these portions of the Connection Broker Administrator Web interface. This level of access is restricted to the highest level of Connection Broker administrators.

The following table describes the difference between Full and Administrator level access.

Permission	Full Access	Administrator Access
Users	You can edit all accounts on the **> Resources > Users** page, except for the main Connection Broker Administrator account.	You can edit all accounts on the **> Resources > Users** page, including the main Connection Broker Administrator account.
Roles	You can edit all roles on the **> Configuration > Roles** page, except for the default Connection Broker Administrator role.	You can edit all roles on the **> Configuration > Roles** page, including the default Connection Broker Administrator role.
Availability	On the **Edit Desktop** page, you can mark an Unavailable desktop as Available; you cannot mark an Available desktop as Unavailable or change the deletable state of the desktop.	On the **Edit Desktop** page, you have full control over the availability and deletability of the desktop.

Customizing Access to Desktops

The following figure shows the available custom permissions for pools of desktops.



DESKTOPS IN POOL

All Desktops

Permissions: Custom

Power Control: Full

Release: No access

Status: No access

Log: No access

Upgrade Agent: No access

View: No access

Edit: Full

Remove: No access

Delete: No access

[Add Pools]

Select the desktop pool to manage.

Select “Custom” to provide granular control.

Set the permission level for the different actions the user is allowed to perform on the desktops in this pool.

“Edit” also provides customized permissions.

Use this option to add pools to this role.

Using these controls, you can allow different users to administer different pools of desktops, as well as restrict the level of interaction for the desktops in that pool. To remove the **> Resources > Desktops** page entirely, select **All Desktops** from the **Desktops in Pool** drop-down menu and **No access** from the **Permissions** drop-down menu. To allow a restricted set of permissions for desktops:

1. Select the pool to set the permissions for from the **Desktops in Pool** drop-down menu. Select **All Desktops** to apply these permissions to all desktops. Select a sub-pool to set permissions for desktops in that pool.

2. From the **Permissions** drop-down menu, select the level of access a user with this role should have to the desktops in the selected pool. Select **Custom** to provide more granular levels of access.

3. If providing custom access to the desktops, use the individual drop-down menus to determine which actions a user with this role can perform.

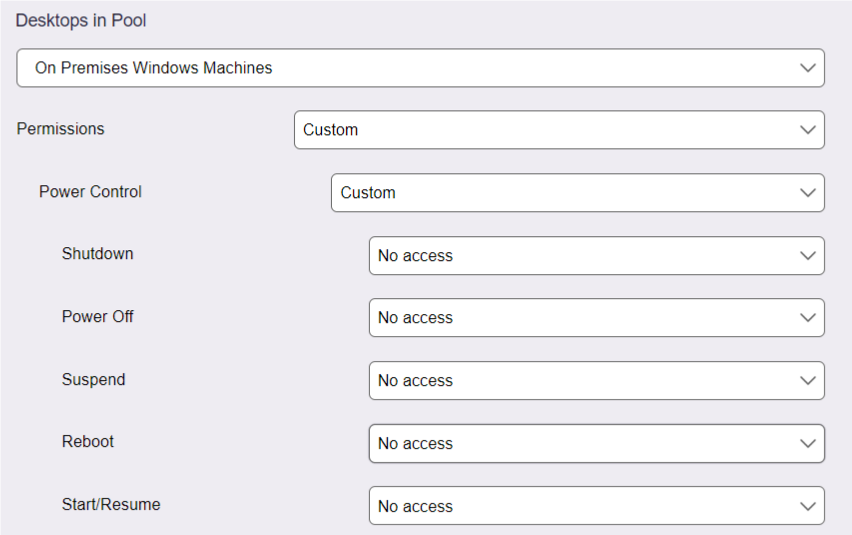
4. Select **Custom** from the **Power Control** and **Edit** drop-down menus to set granular permissions for these two options. These options are described in the following sections.

5. Select a number from the **[Add Pools]** drop-down menu to create a role that sets permissions for multiple pools.

⚠ You cannot save the role if the **Desktops in Pool** section contains multiple references to the same pool.

Permissions for Power Control

The **Custom** option for the **Power Control** permission allows you to limit the control a user with this role has over the power state of desktops in a particular pool. Selecting **Custom** opens the submenus shown in the following figure.



Desktops in Pool

On Premises Windows Machines

Permissions: Custom

Power Control: Custom

Shutdown: No access

Power Off: No access

Suspend: No access

Reboot: No access

Start/Resume: No access

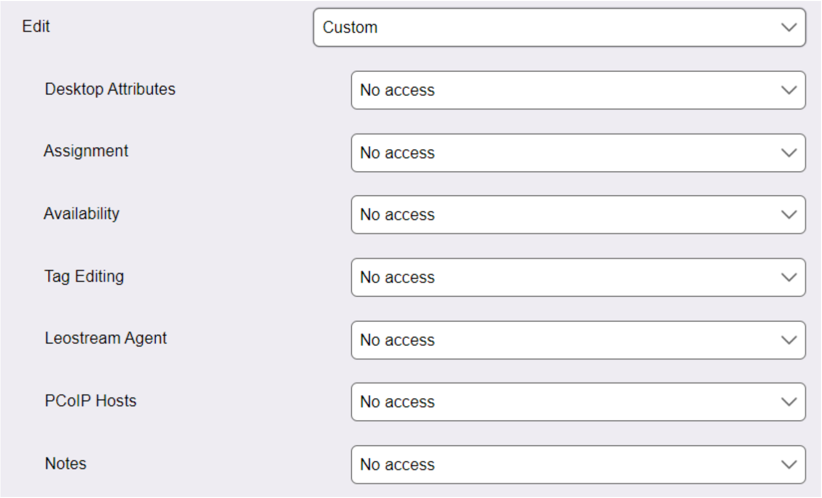
The power control permissions determine which actions appear on the **Control desktop** page, accessed by selecting the **Control** action on the **> Resources > Desktops** page.

The **Reboot** permission controls access to the **Reboot** action. To provide access to the **Power Off and Start** action, you must select **Full** for the **Power Off** permission.

When providing **Full** access for the **Start/Resume** permission, the **Control desktop** page for a virtual machine contains the **Start** and **Resume** options. However, the **Control desktop** page for a desktop from an Active Directory center contains only the **Start** option. The **Suspend** option never appears on the **Control desktop** page for a desktop from an Active Directory center.

Permissions for Editing Desktops

The **Custom** option for the **Edit** permission limits which items on the **Edit Desktop** page a user with this role can view and modify. Selecting **Custom** opens the submenus shown in the following figure.



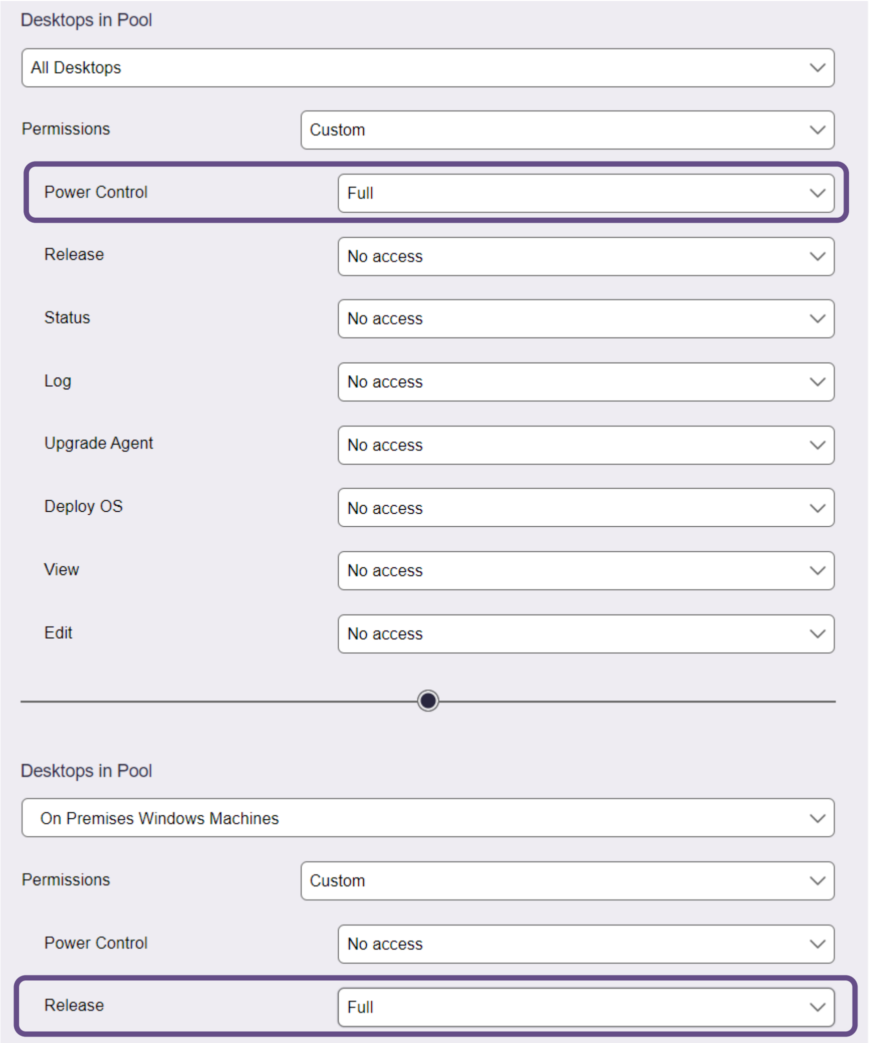
Edit	Custom
Desktop Attributes	No access
Assignment	No access
Availability	No access
Tag Editing	No access
Leostream Agent	No access
PCoIP Hosts	No access
Notes	No access

The permissions control individual sections of the **Edit Desktop** page. If a permission is set to **No access**, that section does not appear in the **Edit Desktop** page. If the permission is set to **View only**, the section appears in the **Edit Desktop** page, but the contents are read-only. If the permission is set to **Full** or **Administrator**, the section appears and is modifiable.

Desktop Permissions for Multiple Pools

The **Desktops in Pools** section allows you to specify which pools of desktops a user with this role is allowed to access. All desktops in a particular pool are assigned the permissions selected for this pool.

A particular desktop can fall into more than one pool. In this case, the Connection Broker assigns the union of all permissions assigned to that desktop from all the pools it resides in. For example, the role shown in the following figure provides full access to the power control actions for the **AWS Desktops** pool. The role then provides full access to the release actions for the **TGX Desktops - AWS** pool. Because the **TGX Desktops - AWS** pool is a subset of the desktops in the **AWS Desktops** pool, when a user logs in with this role, Connection Broker assigns full access to the power control *and* release actions for the desktops in the **TGX Desktops - AWS** pool.



Desktops in Pool

All Desktops

Permissions	Custom
Power Control	Full
Release	No access
Status	No access
Log	No access
Upgrade Agent	No access
Deploy OS	No access
View	No access
Edit	No access

Desktops in Pool

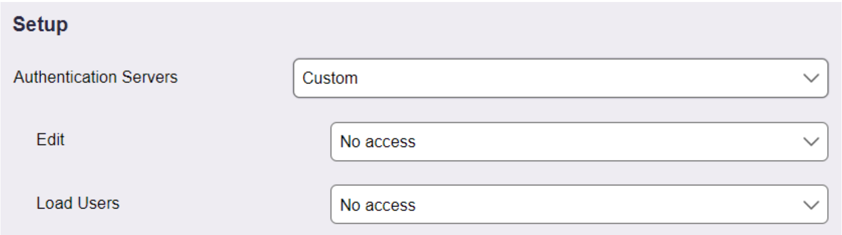
On Premises Windows Machines

Permissions	Custom
Power Control	No access
Release	Full

The Connection Broker always assigns the highest level of permissions for a particular desktop.

Customizing Access to the Authentication Servers Page

The **Authentication Servers** permissions allow you to restrict access to the functionality for loading users. When you select **Custom** from the **Authentication Servers** drop-down menu, the following additional menus appear.



Setup

Authentication Servers	Custom
Edit	No access
Load Users	No access

The **Edit** sub-menu controls the permission level to the **Edit Authentication Server** form, as follows.

- Select **No access** to remove the **Edit** action from the **> Setup > Authentication Servers** page.

- Select **View only** to allow the user to view the **Edit Authentication Servers** pages, but not allow the user to save changes to the authentication servers.

- Select **Full** to allow the user to modify and save settings on the **Edit Authentication Servers** page.

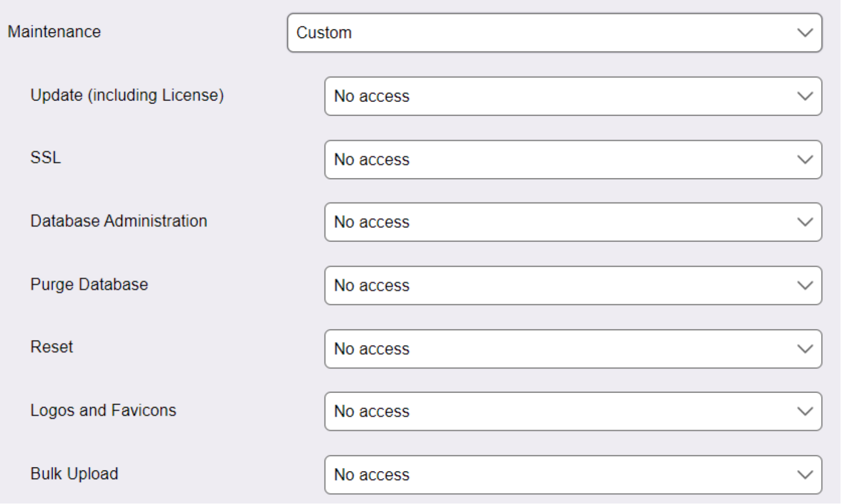
The **Load Users** sub-menu controls access to the **Load User** action on the **> Setup > Authentication Servers** page.

- Select **No access** to remove the **Load User** action from the **> Setup > Authentication Servers** page.

- Select **Full** to allow the user to modify and save settings on the **Edit Authentication Servers** page.

Customizing Access to the Maintenance Page

The **Maintenance** permission allows you to restrict access to individual sections of the **> System > Maintenance** page. When you select **Custom** from the **Maintenance** drop-down menu, the following additional menus appear.



Maintenance	Custom
Update (including License)	No access
SSL	No access
Database Administration	No access
Purge Database	No access
Reset	No access
Logos and Favicons	No access
Bulk Upload	No access

In each sub-menu, selecting **No access** hides the associated section of the **> System > Maintenance** page, with the exception of the database options, which are controlled as follows.

- **Database Administration**: Hides/shows the options in the **Database options** section for backing up, restoring, and switching databases. This option does not apply to the **Purge the database** option.

- **Purge Database**: Hides/shows the **Purge the database** option in the **Database options** section.

Chapter 11: Building Pool-Based Plans

Overview of Policies and Plans

The Leostream Connection Broker defines a ***policy*** as a set of rules that determine how resources are offered, connected, and managed for a user, including:

- The desktop pools the Connection Broker offers desktops from
- How many resources from each of these pools are offered to the user
- If the user's remote desktop is required to have a running Leostream Agent
- Which desktops the user can reboot or release
- Which display protocol is use to connect to these resources
- If, when, and how the power state of the remote desktop is managed
- How long the user is assigned to a particular desktop, i.e., is the desktop persistent or temporary
- And more…

The Connection Broker applies portions of the policy based on events that occur in the user's session. Policy options that configure the end-user experience at login time and when the user is assigned to a desktop are set directly in the **Edit Policy** page (see **Chapter 12: Configuring User Experience by Policy**). Other aspects of the policy are configured in Connection Broker plans.

The Connection Broker defines ***plans*** as building blocks that describe standard behaviors to apply to resources. Each plan can be applied to any number of pools within an unlimited number of policies.

Policies use three types of pool-based plans.

- Protocol plans determine which display protocols can be used to connect to the remote desktop
- Power control plans determine how the Connection Broker manages the power state of the remote desktops
- Release plans determine how long the user remains assigned to the remote desktop

The Connection Broker provides location-based plans that configure the user experience based on the user's client device. See **Chapter 13: Configuring User Experience by Client Location** for information on location-based plans.

To configure your Connection Broker to offer resources to users:

1. Create protocol, power control, and release plans that define the experience you want to provide for your end users. The remainder of this chapter describes this step.

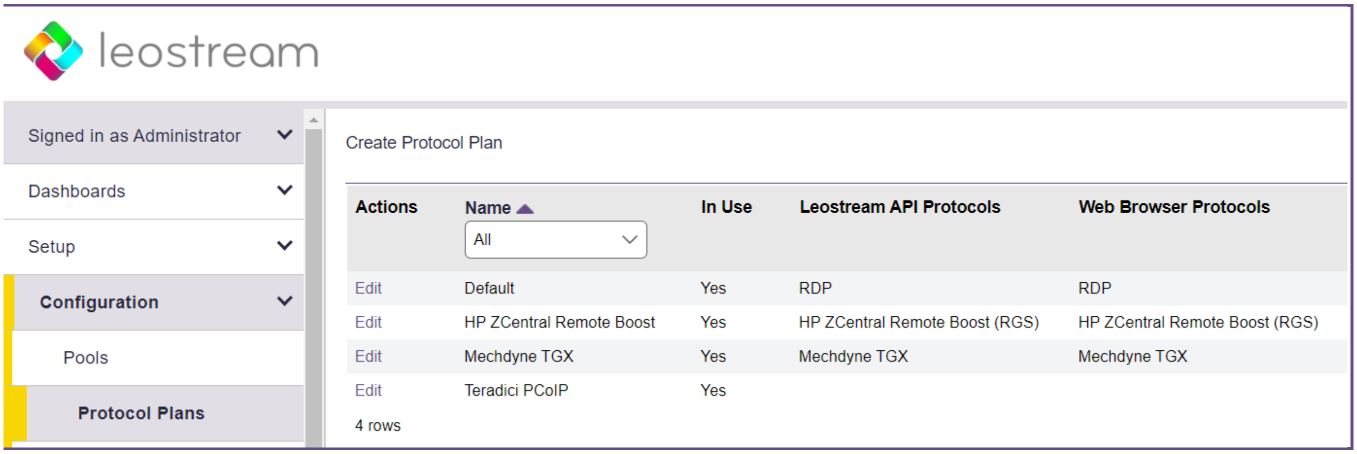
2. Build policies that define which resources to offer to the user, and which plans are applied to the pool in the policy. **Chapter 12: Configuring User Experience by Policy** describes this step.

3. If you need to tailor the user experience based on the location of the user's client, configure the location-based plans (see **Chapter 13: Configuring User Experience by Client Location)**.

4. Assign the policies to users. **Chapter 14: Assigning User Roles and Policies** describes this step.

Protocol Plans

Protocol plans define which display protocols the Connection Broker uses when connecting to a desktop from a pool. The Connection Broker provides one default protocol plan, which is shown on the **> Configuration > Protocol Plans** page, shown in the following figure.

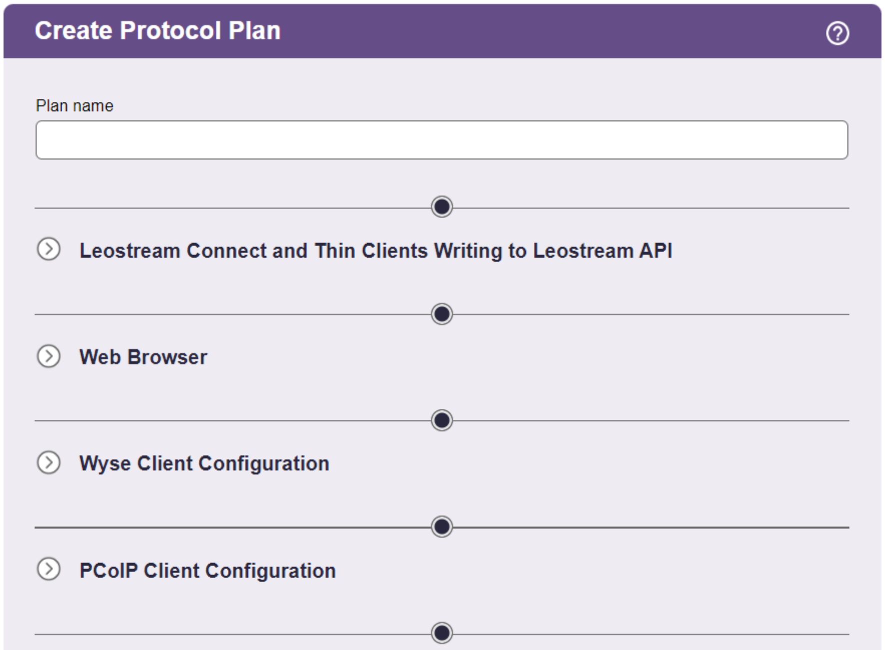


Create Protocol Plan

Actions	Name ▲	In Use	Leostream API Protocols	Web Browser Protocols
	All			
Edit	Default	Yes	RDP	RDP
Edit	HP ZCentral Remote Boost	Yes	HP ZCentral Remote Boost (RGS)	HP ZCentral Remote Boost (RGS)
Edit	Mechdyne TGX	Yes	Mechdyne TGX	Mechdyne TGX
Edit	Teradici PCoIP	Yes		

4 rows

Each protocol plan is separated into sections that apply to different client types, such as Leostream Connect, the Leostream Web client, or a PCoIP client. Configure the display protocols for each client type separately, using the appropriate section in the protocol plan, shown collapsed in the following figure.



Create Protocol Plan

Plan name

Leostream Connect and Thin Clients Writing to Leostream API

Web Browser

Wyse Client Configuration

PCoIP Client Configuration

⚠ Your Leostream license determines what sections and protocols are included on the **Create Protocol Plan** form. If you require an option not currently displayed in the form, please contact sales@leostream.com.

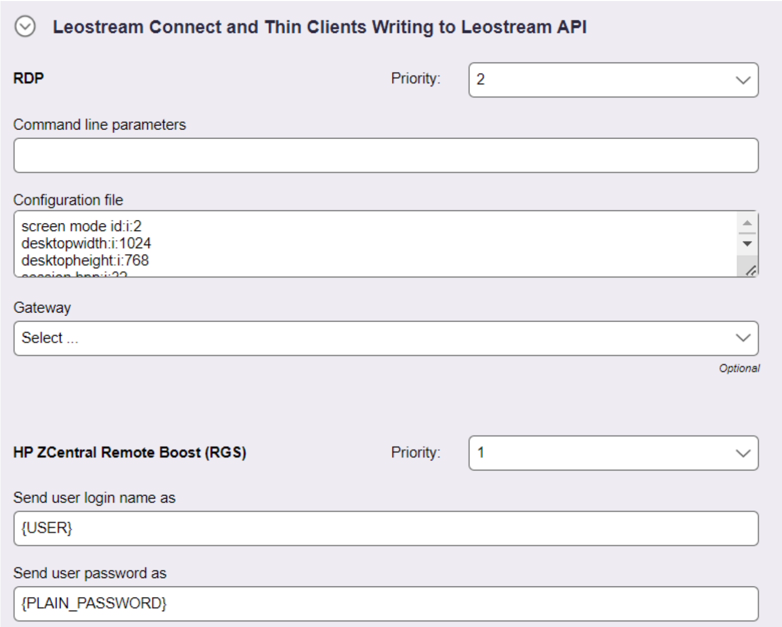
How Protocol Plans Work

The Leostream Connection Broker can connect users to their desktops using a wide range of technologies, including:

- HP ZCentral Remote Boost (RGS)
- Leostream HTML5 RDP, VNC, and SSH (covered in the **Leostream Gateway guide**)
- Microsoft RDP and RemoteFX (including FreeRDP, xrdp, and rdesktop clients)
- Mechdyne TGX
- Amazon DCV
- NoMachine
- Scale Logic Remote Access Portal (RAP) - VDI
- Scyld Cloud Workstation from Penguin Computing
- HP Anyware PCoIP (including Remote Workstation Cards)
- VNC (RealVNC, TigerVNC, TightVNC, and UltraVNC)
- Any external viewer launched via a URL

The following sections describe creating protocol plans, in general. For specific information on setting up the protocol plan for each supported display protocol, see the Leostream **Working with Display Protocols** Guide.

A protocol plan tells the Connection Broker what display protocol to use when connecting users to desktops from a pool, and how that connection is configured. To understand how the Connection Broker interprets a protocol plan, consider the configuration in the following figure.



Leostream Connect and Thin Clients Writing to Leostream API

RDP Priority: 2

Command line parameters

Configuration file

```
screen mode id:i:2
desktopwidth:i:1024
desktopheight:i:768
```

Gateway: Select ...

Optional

HP ZCentral Remote Boost (RGS) Priority: 1

Send user login name as: {USER}

Send user password as: {PLAIN_PASSWORD}

The selection in the **Priority** drop-down menu indicates the order in which the Connection Broker checks if the remote desktop supports a particular display protocol. The Connection Broker performs a port check on the remote desktop to determine if it supports particular display protocol. In the previous example, the Connection Broker checks the default HP ZCentral Remote Boost Sender port 42966. If port 42966 is open on the remote desktop, the Connection Broker connects to the desktop using HP ZCentral Remote Boost. Otherwise, the Connection Broker checks if port 3389 is open, to failover to an RDP connection. If the RDP port on the remote desktop is also closed, the Connection Broker returns a warning that it cannot establish a connection to the remote desktop.

⚠ The Connection Broker cannot distinguish between sections of the protocol plan that use the same port, for example Microsoft RDP and rdesktop. Therefore, if a protocol plan sets the priority for Microsoft RDP to 1 and the priority of rdesktop to 2, the Connection Broker always uses the Microsoft RDP section of the Protocol Plan if port 3389 is open on the remote desktop, even if you are connecting from a Linux client that supports only rdesktop. For this example, you need a second protocol plan that assigns a priority of 1 to rdesktop, to support users logging in from a Linux client.

Why Protocol Plans?

Protocol Plans simplify heterogeneous, enterprise-level deployment. Using protocol plans, you:

- Reuse standard configurations. By providing reusable components, you can build policies faster.
- Use the right protocol for each desktop. By setting protocol plans on a pool-by-pool basis in each policy, you can build policies that offer Windows and Linux desktops, and use a display protocol appropriate for each desktop.
- Set defaults that match your business requirements. By allowing you to set the order in which display protocols are used, you have granular control over your environment

Which Protocol Plan Applies?

Protocol plans can be specified at four levels.

1. Per pool within a policy (see **Configuring Pool Assignment Options**): You must specify a protocol plan for each pool in the policy.
2. Per client location (see **Creating Locations**): You can optionally create per-location protocol plans to support users that move between client devices that require different display protocols, for example:
    - Users that connect from outside the corporate network may need to use the Leostream Gateway and HTML5 RDP viewer to connect to their desktop.
    - Users that connect to a Windows desktop from the Windows version of Leostream Connect will use RDP, while those connecting from the Java version of Leostream Connect will use rdesktop.
3. Per user (see **Editing User Characteristics**): You can optionally create per-user protocol plans to support users with particular requirements, for example, a user that must always have a particular drive redirected while other users should never have any drives redirected.
4. Per desktop (see **Editing Desktop Characteristics**): You can hard-code a desktop to a certain display protocol using the **Protocol** drop-down menu in the **Plans** section of the **Edit Desktop** form. You

may prefer to set the protocol on the desktop if you users have multiple hard-assigned desktops and need to connect to each using a different display protocol, for example.

When connecting a user to a desktop, the Connection Broker applies protocol plans, as follows.

1. When a desktop sets its preferred protocol plan, that protocol plan is used for every user logging in from any client device. Otherwise, the Connection Broker looks at the protocol plan specified for the user.

2. If a per-user protocol plan is specified for this user, that plan is used for all resources launched by this user, including policy-assigned desktops and hard-assigned desktops. Otherwise, the Connection Broker looks at the protocol plan specified for the user's location.

3. If no per-user protocol plan is specified, but the user logged in at a client in a location with a specified protocol plan, the per-location protocol plan is used for all resources launched from this client, including policy-assigned desktops and hard-assigned desktops. Otherwise, the Connection Broker looks at the protocol plan specified in the user's policy.

4. If no per-user or per-location protocol plan is specified, the Connection Broker launches the resource using the protocol plan specified in the policy, based on how the resource was assigned.

The **> Users** and **> Desktops** pages allow you to add a column to display which records set protocol plan overrides. See **Customizing Tables** for information on how to modify the columns shown on the **> Resources** lists.

Building Protocol Plans

To determine how many protocol plans you need and how they should be configured, think about all the ways your end users need to connect to their desktops, for example:

- Do all users access their desktops using the same display protocol? If not, which protocols will they use? If these protocols communicate over the same port, you will need a protocol plan for each protocol.

- For each display protocol that you use, will the command line parameters and configuration file be the same for all users? If not, you will need a protocol plan for each configuration of command line parameters and configuration file.

- Do your remote desktops support multiple display protocols, such as RDP, TGX, and VNC? If so, and you want to allow different users to access different protocols, you will need a protocol plan that defines the appropriate priorities for each type of user.

The above questions are examples of the things you should think about when building protocol plans. Begin with a simple scenario then create your protocol plan as follows.

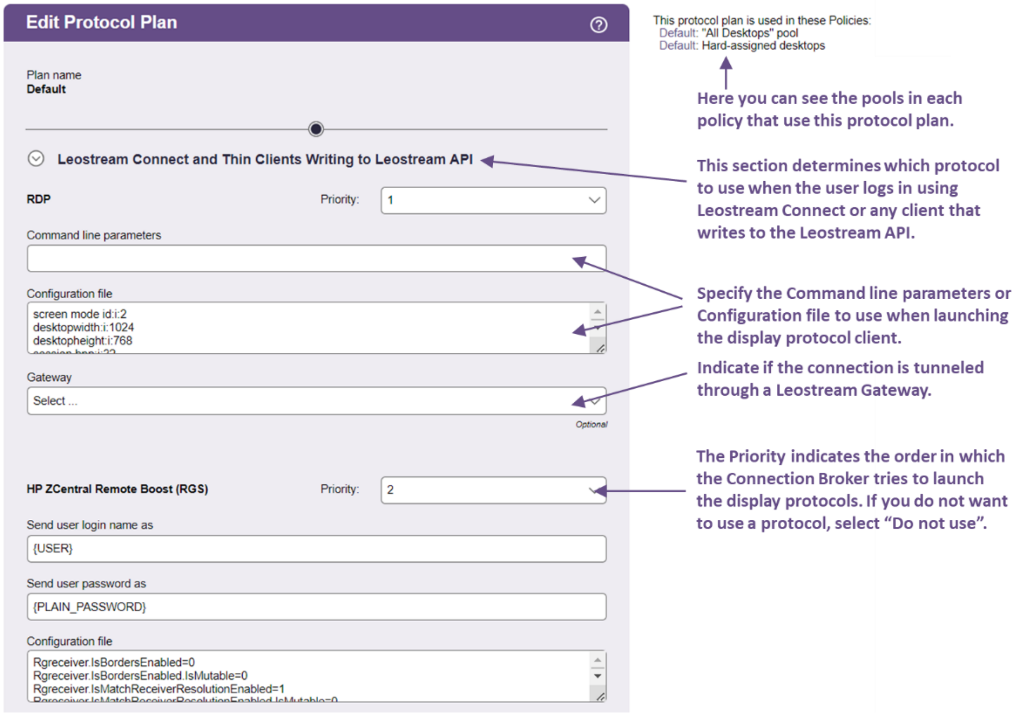
1. Go to the **> Configuration > Protocol Plans** page.

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

3. In the **Plan name** edit field, enter the name to use when referring to this protocol plan.

4. In the **Leostream Connect and Thin Clients Writing to Leostream API** section, shown in the following figure, configure the display protocols to use when a user logs in using one of the following client devices:

    - The Windows or Java version of Leostream Connect
    - A thin client with an installed Leostream Connect client
    - A thin client with a custom Leostream client



Edit Protocol Plan

Plan name
Default

Leostream Connect and Thin Clients Writing to Leostream API

RDP Priority: 1

Command line parameters

Configuration file

```
screen mode id:i:2
desktopwidth:i:1024
desktopheight:i:768
```

Gateway
Select ...
Optional

HP ZCentral Remote Boost (RGS) Priority: 2

Send user login name as
{USER}

Send user password as
{PLAIN_PASSWORD}

Configuration file

```
Rgreceiver.IsBordersEnabled=0
Rgreceiver.IsBordersEnabled.IsMutable=0
Rgreceiver.IsMatchReceiverResolutionEnabled=1
```

This protocol plan is used in these Policies:
Default: "All Desktops" pool
Default: Hard-assigned desktops

Here you can see the pools in each policy that use this protocol plan.

This section determines which protocol to use when the user logs in using Leostream Connect or any client that writes to the Leostream API.

Specify the Command line parameters or Configuration file to use when launching the display protocol client.

Indicate if the connection is tunneled through a Leostream Gateway.

The Priority indicates the order in which the Connection Broker tries to launch the display protocols. If you do not want to use a protocol, select “Do not use”.

⚠ Your Leostream license determines what sections and protocols are included on the **Create Protocol Plan** form. If you require an option not currently displayed in the form, please contact **sales@leostream.com**.

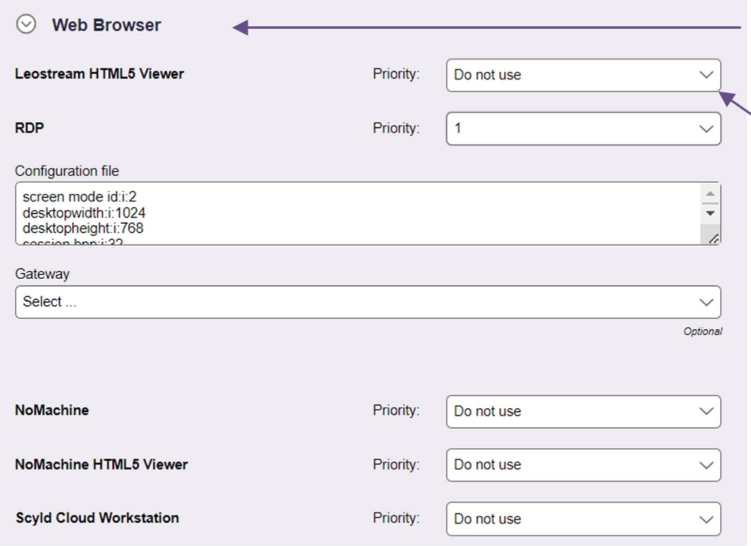
Users logging in from Leostream Connect can use any of the following display protocols. The list notes the display protocols supported by the Windows and Java version of Leostream Connect.

Display Protocol	Required Client Software or Device	Leostream Connect version
HP® ZCentral Remote Boost (RGS)	HP ZCentral Remote Boost Receiver	Windows, Linux, and macOS
Mechdyne TGX	Mechdyne TGX client	Windows and Linux
Amazon DCV	Amazon DCV Client	Windows and Linux
NoMachine	NX Enterprise Client	Windows and Linux
PCoIP	HP Anyware Client	Windows, Linux, and macOS
PCoIP (hardware)	PCoIP Zero Client	N/A
Scale Logic RAP - VDI	RAP – VDI Client or Web browser	Windows, Linux, and macOS

Scyld Cloud Workstation	Scyld Cloud Workstation Client or Web browser	Windows, Linux, and macOS
RDP / Remote FX	Remote Desktop Connection	Windows
rdesktop	rdesktop	Linux and macOS
VNC	RealVNC, TigerVNC, TightVNC, UltraVNC	Windows and Linux

For specific information on configuring command line parameters and configuration files for each supported display protocol, see the Leostream guide for **Working with Display Protocols**.

5. In the **Web Browser** section, shown in the following figure, configure the display protocols to use when a user logs in through the Leostream Web client.



Web Browser

Leostream HTML5 Viewer — Priority: Do not use

RDP — Priority: 1

Configuration file

```
screen mode id:i:2
desktopwidth:i:1024
desktopheight:i:768
session bpp:i:32
```

Gateway: Select ... (Optional)

NoMachine — Priority: Do not use

NoMachine HTML5 Viewer — Priority: Do not use

Scyld Cloud Workstation — Priority: Do not use

This section determines which display protocol to use when the user logs in using the Leostream Web client.

For in-browser RDP, VNC, or SSH connections using the Leostream Gateway, set the Priority for the "Leostream HTML5 Viewer" to 1.

The "External viewer" option (not shown) allows you to launch any third party viewer. You can load custom viewers into your Connection Broker using options on the > System > Maintenance page.

See **Display Protocols for Web Client Access** for a full description of the different display protocols available when logging in through the Leostream Web client.

6. Configure the **PCoIP Client Configuration** section of the protocol plan if your end users log into Leostream from a PCoIP client. See the Leostream Quick Start guides for PCoIP for more information.

7. Use the **Notes** field to store any additional information with your protocol plan.

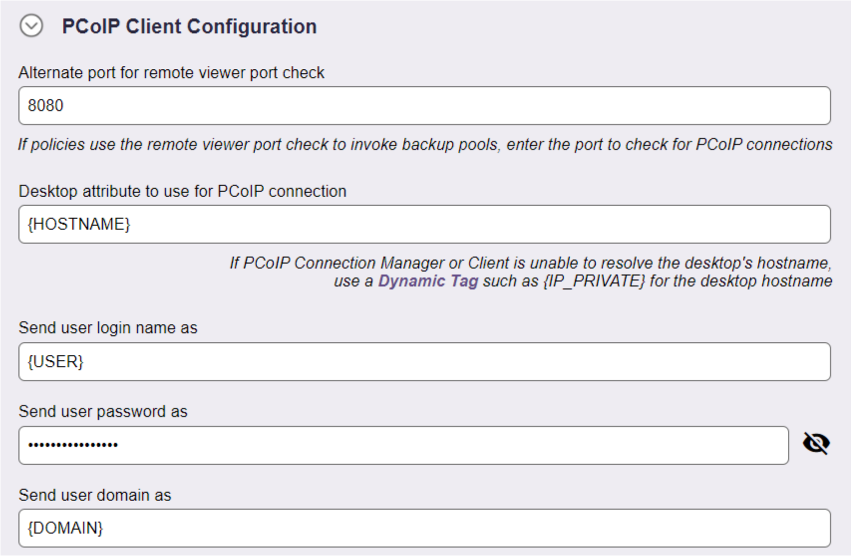
8. Click **Save** to store any changes to the plan.

Using Fixed Desktop Credentials

By default, the Connection Broker uses the user's Leostream login credentials (username, password, and domain) whenever authentication is required during the user's remote session, for example to authenticate an Amazon DCV connection or log the user into their remote operating system.

If the user's desktop requires a different set of credentials, you can use Protocol Plans to override the default username and domain and, in some cases, password.

Protocols such as RDP allow you to specify which credentials are used in the configuration file or command line parameters. For certain display protocols that do not support that method, Protocol Plan includes edit fields where you can enter the new credentials, as shown in the following figure for PCoIP connections launched from a PCoIP client.



PCoIP Client Configuration

Alternate port for remote viewer port check: 8080

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

Send user login name as: {USER}

Send user password as: •••••••••••••••

Send user domain as: {DOMAIN}

The Connection Broker evaluates the default dynamic tags of {USER} and {DOMAIN} at the time the user requests the connection, and substitutes the user's Leostream login information. You can replace these default values to accomplish the following workflows.

- If you have multiple desktops that use the same operating system credentials, enter those values into these edit fields to override the default credentials for every desktop launched using this Protocol Plan.

- If every desktop has a unique set of operating system credentials that are shared across multiple users, enter those credentials in the **Log user into remote desktop with this *XXX*** fields on the **Edit Desktop** page then use the `{VM:USERNAME_OVERRIDE}`, `{VM:PASSWORD_OVERRIDE}`, and `{VM:DOMAIN_OVERRIDE}` dynamic tags in the Protocol Plan edit fields.

  The Connection Broker evaluates these dynamic tags at the time the user requests a connection to a desktop and replaces the tags with the credentials entered into that desktop's Edi Desktop page.

Currently, only the following connection types support overriding the user's password.

- Remote Boost connections launched from a Leostream Connect client
- PCoIP connections launched from a Leostream Connect client
- PCoIP connections launched from a PCoIP Zero client or HP Anyware client

Other connection types support overriding the username and domain anywhere you see the `{USER}` and `{DOMAIN}` dynamic tag. Do not override any `{SCRAMBLED_PASSWORD}` dynamic tags as `{VM:PASSWORD_OVERRIDE}`is replaced in plain text.

Using Dynamic Tags

Configuration files allow you to customize certain display protocol behaviors. The Connection Broker supports dynamic tags in the **Command line parameters** and **Configuration file** fields for any of the protocols. When establishing a remote session, the Connection Broker replaces dynamic tags with the appropriate information.

The following table contains a complete list of the supported dynamic tags. If the configuration file contains text enclosed in braces that is not included in the list of supported dynamic tags, the Connection Broker does not alter the text in the configuration file.

Dynamic Tags	Purpose
`{IP}`	The IP address of the Leostream Agent on the desktop. If no Leostream Agent is installed on the desktop, `{IP}`is replaced with the hostname of the desktop or, if the hostname is not available or does not resolve, the IP address of the desktop.
`{IP_ADDRESS}`	The IP address of the desktop.
`{IP_PRIVATE}`	For desktops hosted in OpenStack, AWS, and Azure, the internal IP address seen by the operating system.
`{IP_PUBLIC}`	For desktops in OpenStack, AWS, and Azure, the IP address, if allocated, that is accessible from the outside network.
`{IP_PRIVATE-or-IP_PUBLIC}`	The private IP address of a cloud-hosted desktop or, if no private IP address exists, the public IP address of the desktop.
`{IP_PUBLIC-or-IP_PRIVATE}`	The public IP address of a cloud-hosted desktop or, if no public IP address exists, the private IP address of the desktop.
`{IP_AGENT}`	The Leostream Agent hostname or IP address. (If not available, `{IP_ADDRESS}` is returned.)
`{HOSTNAME}`	The hostname of the desktop.
`{HOSTNAME_PRIVATE}`	For desktops hosted in AWS, the instance's local hostname, as returned by the Leostream Agent
`{HOSTNAME_PUBLIC}`	For desktops hosted in AWS, the instance's public hostname, as returned by the Leostream Agent
`{IP_ADDRESS-or-HOSTNAME}`	The IP address of the desktop or, if the IP address is not available, the hostname of the desktop. (see **Example: Specifying a Dynamic Tag Backup**)
`{HOSTNAME-or-IP_ADDRESS}`	The hostname of the desktop or, if the hostname is not available, the IP address of the desktop. (see **Example: Specifying a Dynamic Tag Backup**)
`{SHORT_HOSTNAME}`	The short hostname of the desktop, or the hostname cut at the first dot. For example, if the hostname is `desktop.example.com`, the `{SHORT_HOSTNAME}` tag returns `desktop`.

Dynamic Tags	**Purpose**
{MACHINE_NAME}	The internal host name of the desktop, as returned by the Leostream Agent. Empty if no Leostream Agent is installed on the desktop.
{DCV_PORT}, {VNC_PORT}	For DCV and VNC connections, the port for the VNC session, as returned by the Leostream Agent.
{SESSION_ID_NAME}	For DCV connections, a unique session ID to pass to the Leostream Agent for starting the DCV session. Enter this dynamic tag for the sessionid parameter in the DCV configuration file.
{USER}, {USER:USER}, {USER:LOGIN_NAME}, or {LOGIN:NAME}	The user's login name. This value corresponds to the value shown in the **Login name** column on the **> Resources > Users** page. To force the login name on the remote desktop to upper or lower case, include the :lowercase or :uppercase modifier, for example {USER:lowercase} or {USER:LOGIN_NAME:uppercase}.
{AD:USER:*attribute_name*}	The value found in the user's Active Directory attribute given by *attribute_name*. Use this dynamic tag if you need to replace the user's login name for their remote session with a value different from the login name used for their Leostream session.
{NAME} or {USER:NAME}	The user's display name. This value corresponds to the value shown in the **Name** column on the **> Resources > Users** page.
{AD_DN} or {USER:AD_DN}	The user's Active Directory Distinguished Name. This value corresponds to the value shown in the **AD Distinguished Name** column on the **> Resources > Users** page.
{EMAIL} or {USER:EMAIL}	The user's email address. This value corresponds to the value shown in the **Email** column on the **> Resources > Users** page.
{PRE_EMAIL} or {USER:PRE_EMAIL}	The portion of the user's email address before the @ symbol.
{POST_EMAIL} or {USER:POST_EMAIL}	The portion of the user's email address after the @ symbol.
{DOMAIN}	The name entered into the **Domain** field for the authentication server that authenticated a user. If the **Domain** field is empty, the Connection Broker replaces this dynamic tag with the value entered or selected in the **Domain** field of the login dialog on the user's client.
{AUTH_DOMAIN}	The name entered in the **Authentication Server name** field of the authentication server that authenticated the user.
{PLAIN_PASSWORD}	The user's password, in plain text.
{RDP_PASSWORD}	For Leostream Connect, the user's password encrypted for RDP usage.

Dynamic Tags	**Purpose**
`{SCRAMBLED_PASSWORD}`	For NoMachine, only, the user's password scrambled to prevent casual eavesdropping.
`{STANDARD_RDP_PASSWORD:`*`xxxx`*`}`	For Leostream Connect, a specific password encrypted for RDP usage.
`{CREDENTIALS_MECHDYNE}`	Encrypted user credentials to pass to the TGX Sender to provide single sign-on.
`{PCOIP_HOST1}` or `{PCOIP_HOST2}`	The last know IP address of the PCoIP Remote Workstation Card associated with the desktop for the connection. If the Connection Broker does not have an IP address for the card, then the dynamic tag is replaced with the card's hostname.
`{CLIENT}` or `{CLIENT:NAME}`	The name of the client device used to log into the Connection Broker. This value corresponds to the value shown in the **Name** column on the **> Resources > Clients** page.
`{CLIENT:IP}`	The IP address of the client device used to log into the Connection Broker. This value corresponds to the value shown in the **IP Address** column on the **> Resources > Clients** page.
`{CLIENT:MAC}`	The MAC address of the client device used to log into the Connection Broker. This value corresponds to the value shown in the **MAC Address** column on the **> Resources > Clients** page.
`{CLIENT:TYPE}`	The type of client used to log into the Connection Broker. This value corresponds to the value shown in the **Type** column on the **> Resources > Clients** page.
`{CLIENT:MANUFACTURER}`	The manufacturer of client used to log into the Connection Broker. This value corresponds to the value shown in the **Manufacturer** column on the **> Resources > Clients** page.
`{CLIENT:UUID}`	The UUID of the client used to log into the Connection Broker. This value corresponds to the value shown for the **Client UUID** on the **> Resources > Clients** page.
`{POOL:NAME}`	The name of the pool that contains the desktop that the user is connecting to
`{VM:NAME}`	The name of the desktop the user is connecting to, as shown in the **Name** field on the **> Resources > Desktops** page.
`{WINDOWS_NAME}`	(Deprecated: See `MACHINE_NAME`) The guest host name of the desktop, as returned by the Leostream Agent
`{FQDN}`	If the user authenticated against an authentication server, the user's fully qualified name, e.g., `cn=Fred,ou=Users,o=Company`

Dynamic Tags	Purpose
{DRIVE:CD}	For the RDP configuration file, use `drivestoredirect:s:{DRIVE:CD}` to redirect all CD drives found on system. No other drives are directed.
{DRIVE:DVD}	For the RDP configuration file, use `drivestoredirect:s:{DRIVE:DVD}` to redirect all DVD drives found on system. No other drives are directed.
{LOGOUT_URL}	The URL to log the user out of the session.
{LIST_URL}	The URL to view the list of desktops.
{ENV:*}	The value of the client side variable specified in *. So `{ENV: HTTP_COOKIE}` might return `uid=25157202`.
{MATCHED_IP:*partial_IP_address*}	Specifies a preferred IP address to use for the connection (see **Specifying Subnet for Desktop Connections**)
{REMAPPED_IP:*X.X.X.X*}	Re-maps IP addresses by replacing the non-*X* portion of the IP address with the specified tag.
{REMAPPED_IP:*subnet_mask*}	Re-maps IP addresses on different subnets.
{SESSION}	For use with the Java version of Leostream Connect. The session ID associated with session-based HP ZCentral Remote Boost Receiver configuration file parameters.
{USB_SESSION}	Indicates that the Java version of Leostream Connect should manage which remote Remote Boost session has access to USB devices.

{VM:USERNAME_OVERRIDE}
{VM:PASSWORD_OVERRIDE}
{VM:DOMAIN_OVERRIDE}
	Can be used in Protocol Plans to override the user's Leostream credentials and use the desktop's fixed operating system credentials to log the users into the remote machine.

Example: Specifying a Dynamic Tag Backup

You can use the `or` syntax to specify a backup value in the event the initial dynamic tag resolves to an empty value. The backup value can be a static value or another dynamic tag. For example:

`{HOSTNAME-or-IP_PRIVATE}` resolves to the hostname of the desktop or, if the hostname is not available, the private IP address of the desktop.

To fail over to a static text value, enclose the text in double quotes, for example:

`{DOMAIN-or-"leostream.com"}` resolves to the domain of the authentication server that authenticated the user or to "leostream.com" in the case where the user's domain is empty, as it would be if they logged into the Leostream environment from a SAML-based identity provider.

Example: Using Different Login Names for User Connections

In some cases, you may need to use a login name for the user's remote desktop that is different from the login name used for the Leostream session. One example is the case where the user logs into Leostream with their Windows Active Directory credential, but needs to use their Linux username to connect to their Linux desktop. For these cases, you can use custom Active Directory attributes and dynamic tags to change the default user login.

First, you must populate an Active Directory attribute in the user's account with the value of the user's alternate login name. The Active Directory attribute can be a standard attribute, or you can create a custom attribute. For example, create a custom attribute named `linuxLogin`.

Second, in the protocol plan, replace the `{USER}` dynamic tag with the `{AD:USER:`*`attribute_name`*`}` dynamic tag. For example, when using the custom attribute named `linuxLogin` the dynamic tag is `{AD:USER:linuxLogin }`.

If the username varies only by case, you can use the `lowercase` and `uppercase` dynamic tag modifiers, instead of specifying a new Active Directory attribute. For example, if the user's Windows login is `JSmith`, but their Linux login is `jsmith`, use the `{USER:lowercase}` dynamic tag.

Example: Specifying Subnet for Desktop Connections

When a remote desktop has multiple network interfaces, the Leostream Agent and Connection Broker negotiate which IP address to use for remote connections. You can alternatively use the `{MATCHED_IP}` dynamic tag to specify a preferred IP address for the Connection Broker to use when establishing the remote connection. For example, you can modify the default line in the RDP configuration file to the following:

```
full address:s:{MATCHED_IP:partial_IP_address}
```

Where *`partial_IP_address`* indicates the beginning of the IP address that the Connection Broker should favor for the connection. When specifying *partial_IP_address*, trailing zeros are optional, for example, {`MATCHED_IP:172.29.0.0}` is equivalent to `{MATCHED_IP:172.29}`.

The `MATCHED_IP` dynamic tag instructs the Connection Broker to favor a specific IP address. For example, if the desktop returns two IP addresses of 172.29.229.151 and 10.110.1.14 and the tag is `{MATCHED_IP:10.110.1}` the IP address used for the connection is 10.110.1.14.

If the desktop does not have an IP address beginning with the values to match, the Connection Broker will not establish a remote connection to the desktop. To allow the Connection Broker to fail over to any available IP address, use the following syntax:

```
{MATCHED_IP:partial_IP_address-or-IP}
```

For example, if the tag is `{MATCHED_IP:10.110.1-or-IP}` and the desktop returned a single IP address of 172.29.229.151 the Connection Broker uses the 172.29.229.151 for the connection even though it does not match the preferred IP address.

Dynamic Remapping of Desktop IP Address

You can enable display protocol traffic to traverse one or more NATed firewalls by dynamically changing the IP address provided to the remote viewer client to reflect the address of the desktop seen from the client's perspective as opposed to that seen from within the desktop.

To do this, use the `{REMAPPED_IP}` dynamic tag in place of the `{IP}` dynamic tag. The Connection Broker takes the IP address of the desktop and applies the IP address mask specified in the dynamic tag so that the address is modified.

As an example, imagine an offshore development center than runs on a 192.168.1.xxx network. One of its customers has a series of desktops running on a 172.29.229.xxx network. A NATed firewall makes the transition between the two networks. Therefore, a desktop at 172.29.229.131 appears to the offshore development center as a desktop at 192.168.1.131.

To accomplish this transition, in the configuration file, change instances of the `{IP}` tag to `{REMAPPED_IP:192.168.1.X}`.

To remap IP addresses on multiple subnets, use the advanced form of the `{REMAPPED_IP}` dynamic tag. This version of the dynamic tag supports specifying a network mask length and a target range for the source and destination.

The `{REMAPPED_IP:X.X.X.X}` syntax can be used to perform DNS resolution without remapping the IP address.

Use the wildcard (*) to map all subnets. For example:

- `{REMAPPED_IP:*/24->192.168.1.0}` replaces the first 24 bits of the IP address on all subnets with 192.168.1. Therefore, the IP address 10.153.172.5 maps to 192.168.1.5.
- `{REMAPPED_IP:*/8->194.0.0.0}` replaces the first 8 bits of the IP address on all subnets with 194. Therefore, the IP address 10.153.174.9 maps to 194.153.174.9.

To map different subnets to different IP address ranges, use the syntax in the following example.

```
{REMAPPED_IP:10.153.174.0/24 -> 192.168.204.0, 10.153.172.0/24 -> 192.168.201.0}
```

Each subnet map is separated by a comma. A subnet map can be defined using a wildcard, as described in the earlier `{REMAPPED_IP}` examples.

In this example, the first 24 bits of IP addresses in the subnet 10.153.174 are mapped to 192.168.204, while the first 24 bits of the IP addresses in the subnet 10.153.172 are mapped to 192.168.201. Therefore:

10.153.174.9 maps to 192.168.204.9
10.153.172.5 maps to 192.168.201.5
10.153.173.7 remains 10.153.173.7

In cases where multiple subnet maps are included, the order of the subnet maps is irrelevant. More specific maps take precedence over less specific maps. When a wildcard is provided, any IP addresses that are not mapped by one of the other rules will be mapped by the wildcard. The Connection Broker always performs wildcard mappings last.

Do not specify multiple wildcard mappings. If multiple wildcards are specified, the Connection Broker uses one of the mappings and ignores all other maps.

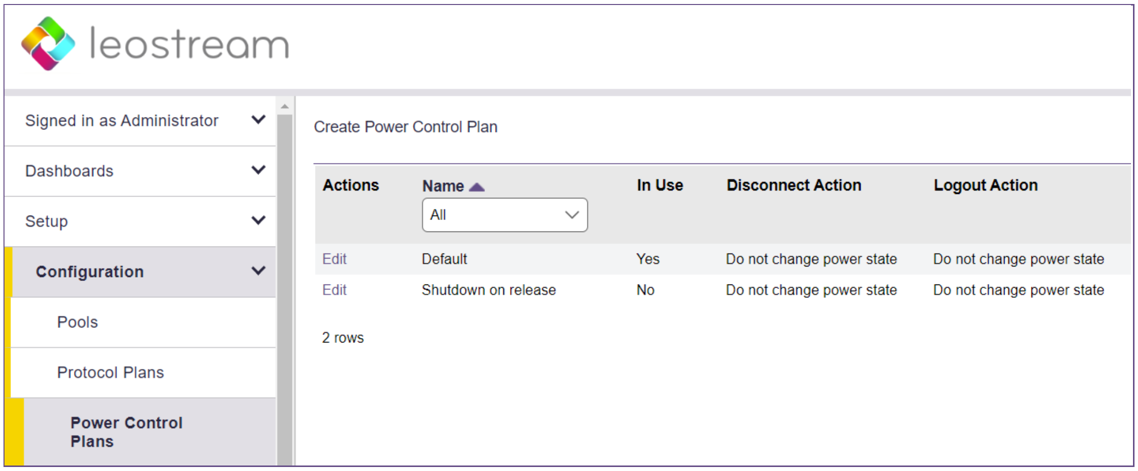
Power Control Plans

Power control and release plans allow you to take actions on the user's session based on 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

⚠ Not all display protocols allow the Connection Broker to perform actions on disconnect events.

Available power control plans are shown on the **> Configuration > Power Control Plans** page, shown in the following figure.



Create Power Control Plan

Actions	Name	In Use	Disconnect Action	Logout Action
	All			
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 (see **Creating Power Control Plans**).

Using Power Control Options

The Connection Broker provides the following options for controlling a desktop:

- Do not change power state, i.e., take no action
- Shutdown (attempts to shut down the machine gracefully)
- Power off (forcefully shuts down the machine)
- Shutdown and Power off (attempts to shut down the machine gracefully. If a graceful shutdown is not possible, the Connection Broker forcefully shuts down the machine.)
- Suspend
- Reboot (attempts to gracefully shut down the machine before restarting)
- Power Off and Start (forcefully shuts down the machine before restarting)
- Revert to snapshot

Different power control options apply to different types of machines, as follows.

- VMware virtual machines: Support all power control options.

- OpenStack virtual machines: Support all power control options, with the exception of reverting to a snap shot.

- AWS, Google Cloud Platform, Scale Computing Platform, and Nutanix AHV virtual machines: Support all power control options, with the exception of suspending and reverting to a snap shot.

- Azure virtual machines: Support all power control options, with the exception of reverting to a snap shot.

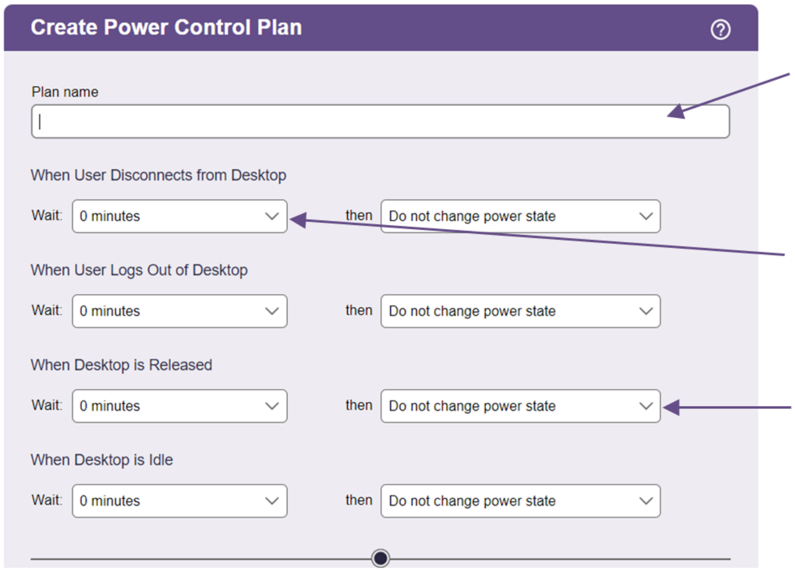
- Active Directory, HPE Moonshot, and Enrolled Desktops: Support **Shutdown** and **Reboot** if the Leostream Agent is installed on the machines.

- Physical Workstations: If a machine inventoried from Active Directory or the Enrolled Desktops centers is Wake-on-LAN or IPMI-enabled, it can be powered on using Wake-on-LAN or IPMI. IPMI machines can also be powered down. In this case, a graceful reboot calls the `chassis power reset` command. Any power control option that uses a forceful Power Off calls the `chassis power cycle` command.

Creating Power Control Plans

To build a new power control plan:

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



Create Power Control Plan

Plan name

When User Disconnects from Desktop

Wait: 0 minutes then Do not change power state

When User Logs Out of Desktop

Wait: 0 minutes then Do not change power state

When Desktop is Released

Wait: 0 minutes then Do not change power state

When Desktop is Idle

Wait: 0 minutes then Do not change power state

Enter a descriptive name for the plan. You'll refer to this name when selecting the plan in policies.

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 take the selected action.

Choose to change the desktop's power state or revert it to a snapshot. For the Connection Broker to take actions based on disconnect or idle-time events, you must install the Leostream Agent on your desktops.

Not all display protocols support disconnect actions.

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

3. For each of the four remaining sections:

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

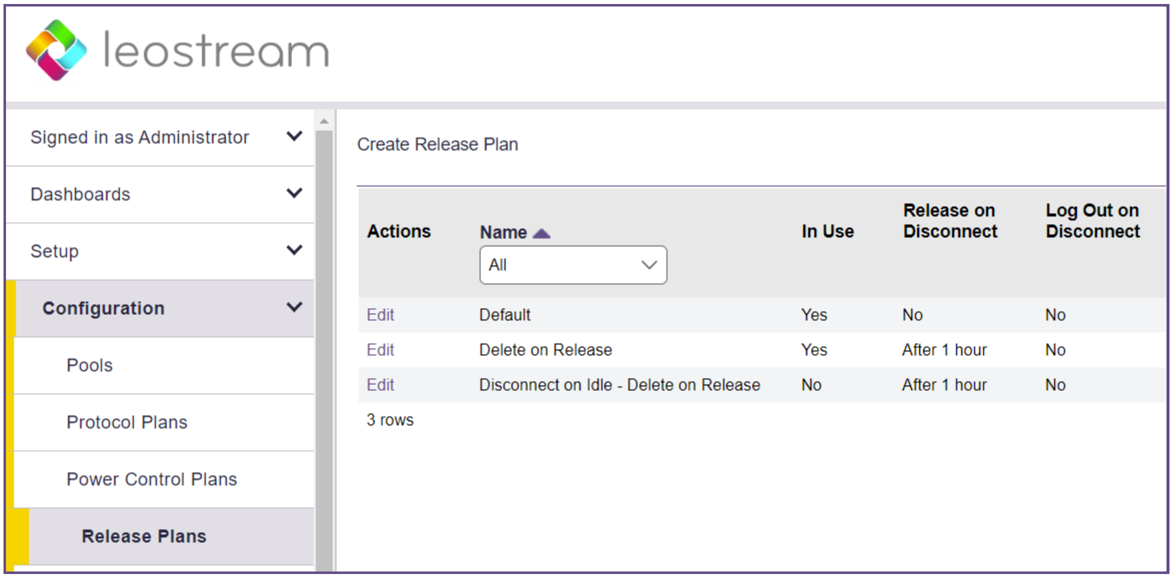
   b. From the **then** drop-down menu, select the power control action to apply. Selecting **Do not change power state** renders the setting in the **Wait** drop-down menu irrelevant, as no action is ever taken.

4. Enter any optional **Notes**.

5. Click **Save** to create the plan 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. 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, called **Default**. You can create as many additional release plans as needed for your deployment.

Using Release Options

The release options allow you to optimize the allocation of computing resources. Release options are triggered after an elapsed time.

If you release a desktop back to its pool, the Connection Broker attempts to offer the same desktop to the user the next time they log back into the Connection Broker, if the user's policy has the **Favor previously assigned desktops** option selected. This behavior improves performance in some Windows environments. If that desktop is unavailable, the Connection Broker assigns a new desktop.

Creating Release Plans

To build a new release plan:

1. Select the **Create Plan** link on the **> Configuration > Release Plans** page. The **Create Release Plan** form opens.

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

3. In the **When User Disconnects from Desktop** section:

    a. To release the desktop to its pool, select a time value from the **Release to pool** drop-down menu.

    b. To log the user out after they disconnect, select a time value from the **Log user out** drop-down menu. Select **No** to keep the user logged in. A user that remains logged in can return to their remote session in the state it was when they disconnected. If the user remains logged into a desktop that was released to its pool, the user is considered *rogue*.

    c. To make an HTTP GET request as soon as the user disconnects from one of their remote sessions, enter the URL in the **URL to call** edit field. Using GET requests, you can perform additional configuration actions necessary for your environment.

4. In the **When User Logs Out from Desktop** section:

    a. To release the desktop to its pool, select a time value from the **Release to pool** drop-down menu. The desktop is available for other users only after it is released to the pool. If it is not released to the pool, it remains assigned to the user and will be re-offered to that user the next time they log into the Connection Broker.

    b. To make an HTTP GET request as soon as the user logs out of their remote sessions, enter the URL in the **URL to call** edit field. Using GET requests, you can perform additional configuration actions necessary for your environment.

5. The Connection Broker requires a Leostream Agent to receive disconnect events. If no Leostream Agent is installed on the desktop, the Connection Broker may receive a connection-close event from Leostream Connect.

    Use the **When Connection is Closed** section of the plan to indicate which section of the release Plan to invoke when the Connection Broker receives a connection closed event from Leostream Connect without any associated Leostream Agent notification.

    The selection made for this option determines which section of the power control plan is invoked, as well.

6. In the **When Desktop is Idle** section:

    a. Use the **Lock desktop**, **Disconnect**, and **Log user out** drop-down menus to take actions when the user's session is idle. Multiple actions can be taken, for example, you can lock the desktop after 5 minutes then disconnect after 30 minutes of idle time.

   b. When using the **Log user out** action, use the **Suspend logout until CPU falls below** option to monitor the desktop's CPU levels and perform the logout only after the CPU level falls below the specified threshold for the specified length of time. The Leostream Agent begins monitoring the desktop's CPU level after the elapsed user idle time specified by the **Logout** drop-down menu.

   c. Also when using the **Logout** action, use the **Suspend logout and display warning message to user** option to popup a warning dialog on the user's desktop, to alert them they are about to be logged out and may lose any unsaved work (see **Example: Displaying a Warning to Idle Users Before Forcing a Logout**).

   Idle-time monitoring is not available for sessions originating from a **Remote Desktop Services/Multi-User** center.

   d. To make an HTTP GET request after the user's session is idle, enter the URL in the **Call URL** edit field.

7. In the **When Desktop is First Assigned** section:

   a. Select a time value from the **Release if user does not log in** drop-down menu to schedule a release for some elapsed time after the user is first assigned to the desktop, but before they log into that desktop.

   When this setting is configured, the Connection Broker places a `check_logon` job in the job queue after the user is policy-assigned to a desktop. If the `check_logon` job does not detect that a user has logged into the destkop before the specified wait time elapses, the Connection Broker releases the desktop back to its pool. The Connection Broker cancels the `check_logon` job when it detects that a user logged into the desktop.

   b. Select a time value from the **Release to pool** drop-down menu to schedule a release for some elapsed time after the user is first assigned and logs into the desktop. When this setting is configured, the Connection Broker places an `unassign_after_login` job in the job queue after a user is policy-assigned to a desktop. This job automatically releases the desktop to a pool when it runs.

   To schedule the release based on a day and time of the week instead of after a set elapsed time, select **Custom** from the **Release to pool** drop-down menu. Use the **Release at** drop-down menu to indicate the time-of-day and use the day-of-the-week checkboxes to select on which days to perform the release (see **Example: Releasing Desktops at Specific Times and Days**).

   Releasing the desktop to its pool does not automatically log out the user. After the desktop is released, if the user remains logged in, the Connection Broker considers them rogue user, i.e., a user that is logged into a desktop that is not assigned in the Connection Broker.

c. To make an HTTP GET request after the desktop is assigned, enter the URL in the **URL to call** edit field. Using GET requests, you can perform additional configuration actions necessary for your environment.

8. In the **When Desktop is Released** section:

   a. Check the **Log user out of the Desktop** option to log the user out when the desktop is released back to the pool. Use this option in conjunction with releasing a desktop to its pool in the **Time Release After Initial Assignment** section to avoid rogue users.

   b. Use the **Delete virtual machine from disk** option to indicate that the Connection Broker should attempt to delete the virtual machine. Not all virtual machines are deletable (see **Release Plan Example: Deleting Virtual Machines After Use**).

   c. To make an HTTP GET request after the desktop is released, enter the URL in the **URL to call** edit field. Using GET requests, you can perform additional configuration actions necessary for your environment.

9. Enter any optional **Notes**.

10. Click **Save** to store the changes or **Cancel** to return to the **> Configuration > Release Plans** page without creating the plan.

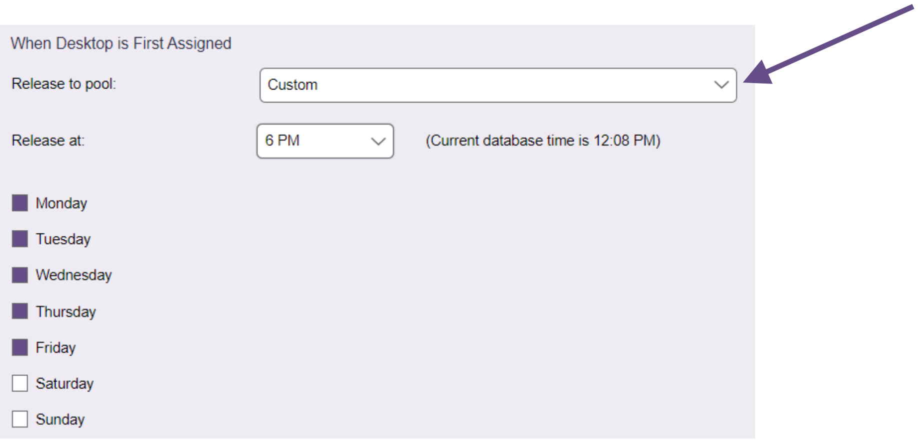
⚠ When managing connections to macOS, to using Leostream to log users out of their desktop, ensure that **automatic login** is off on the macOS device.

You can set Automatic login to Off by selecting **System Preferences** from the Apple menu and clicking **Users & Groups**. In **Users & Groups**, click the **Login Option** link at the lower-left corner and set the **Automatic login** drop-down menu to **Off**.

Example: Releasing Desktops at Specific Times and Days

You can release desktops at a specific time and day after the desktop was initially assigned to the user, as follows.

1. In the **When Desktop is First Assigned** section of the release plan, select **Custom** from the **Release to pool** drop-down menu, as shown in the following figure.



When Desktop is First Assigned

Release to pool: Custom

Release at: 6 PM (Current database time is 12:08 PM)

☑ Monday
☑ Tuesday
☑ Wednesday
☑ Thursday
☑ Friday
□ Saturday
□ Sunday

2. From the **Release at** drop-down menu, select the hour of the day to release the desktop.

3. Select the check boxes for each day of the week to release the desktop. The desktop is released at the same time on each selected day.

Example: Deleting Virtual Machines After Use

You can schedule virtual or cloud-hosted machines for deletion after the desktop has been released back to its pool. To enable virtual machine deletion:

1. Mark the virtual machines as deletable, using one of the following methods.

   a. Go to the **Edit Desktop** page of an existing virtual machine and select the **Allow this desktop to be permanently deleted from disk** option.

   b. When provisioning new machines into Connection Broker pools, select the **Initialize newly-provisioned desktops as deletable** option. With this option selected, the Connection Broker automatically selects the **Allow this desktop to be permanently deleted from disk** option when the provisioned VM appears in the Connection Broker.

2. Instructs the Connection Broker to delete virtual machines by selecting a wait time from the **Delete virtual machine from disk** option from the **When Desktop is Released** section.

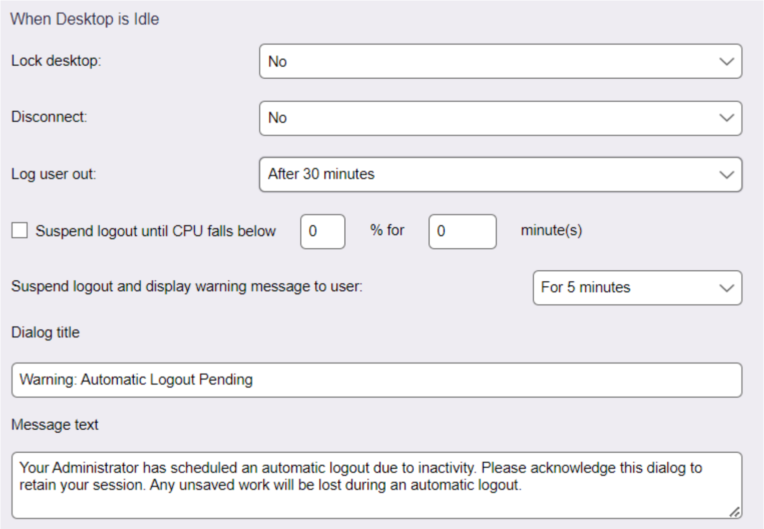
3. Create a policy that assigns this release plan to pool of deletable desktops.

After the desktop is released back to its pool, the Connection Broker deletes the virtual machine *only* if the **Allow this desktop to be permanently deleted from disk** option is selected *at the time the release plan is invoked*. The Connection Broker does not store the value of the desktop’s deletable state at the time the desktop was assigned to the user. Therefore, after a desktop is in use, you can change the deletable state to retain or delete the desktop, as necessary.

If the Connection Broker joined this Windows desktop to your Active Directory domain and the desktop is running Leostream Agent 7.4.11 or later, the Connection Broker removes the Active Directory records associated with this desktop. Older versions of the Leostream Agent do not provide adequate information for the Connection Broker to identify the record in Active Directory and, therefore, the record is not deleted.

Example: Displaying a Warning to Idle Users Before Forcing a Logout

For users connecting to Microsoft Windows operating systems, you can popup a warning dialog before they are forcefully logged out due to being idle. When you select any time frame from the **Log user out** option in the **When Desktop is Idle** section, the new options shown in the following figure appear.



When Desktop is Idle

Lock desktop: No

Disconnect: No

Log user out: After 30 minutes

☐ Suspend logout until CPU falls below 0 % for 0 minute(s)

Suspend logout and display warning message to user: For 5 minutes

Dialog title

Warning: Automatic Logout Pending

Message text

Your Administrator has scheduled an automatic logout due to inactivity. Please acknowledge this dialog to retain your session. Any unsaved work will be lost during an automatic logout.

Use the **Suspend logout and display warning message to user** option to indicate how long the user has to acknowledge the warning before being logged out. For example, in the previous figure, the warning dialog opens after the user is idle for an hour. If the user does not acknowledge the warning dialog, or more their mouse or hit a key to perform any other action, for five minutes then the Connection Broker continues to log the user out.

If the user does acknowledge the warning dialog, move their mouse, or use their keyboard, the idle-time action is cancelled. In this example, the user would need to be idle for another hour before they are forcefully logged out.

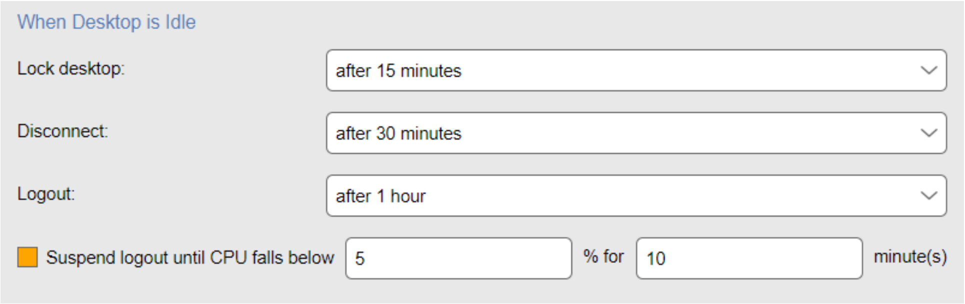
Use the **Dialog title** and **Message text** fields to customize the contents of the warning dialog.

If you first disconnect the user session then log them out, the user will not have an opportunity to acknowledge the warning dialog and will always be logged out.

Example: Performing Actions Based on User and System Idle Time

Desktops must be running a Leostream Agent in order to perform idle time actions.

The following figure shows how to configure a Release Plan to lock the user’s desktop after 15 minutes of user idle time; disconnect the desktop after 30 minutes; and logout the desktop after 30 minutes. After an hour of idle time, the Release Plan instructs the Leostream Agent on the desktop to monitor the desktop’s CPU level and report when the CPU level falls below 5% for 10 minutes. At that point, the Connection Broker performs the logout action.



When Desktop is Idle

Lock desktop: after 15 minutes

Disconnect: after 30 minutes

Logout: after 1 hour

□ Suspend logout until CPU falls below 5 % for 10 minute(s)

The Connection Broker defines user idle time by the lack of mouse or keyboard actions.

Chapter 12: Configuring User Experience by Policy

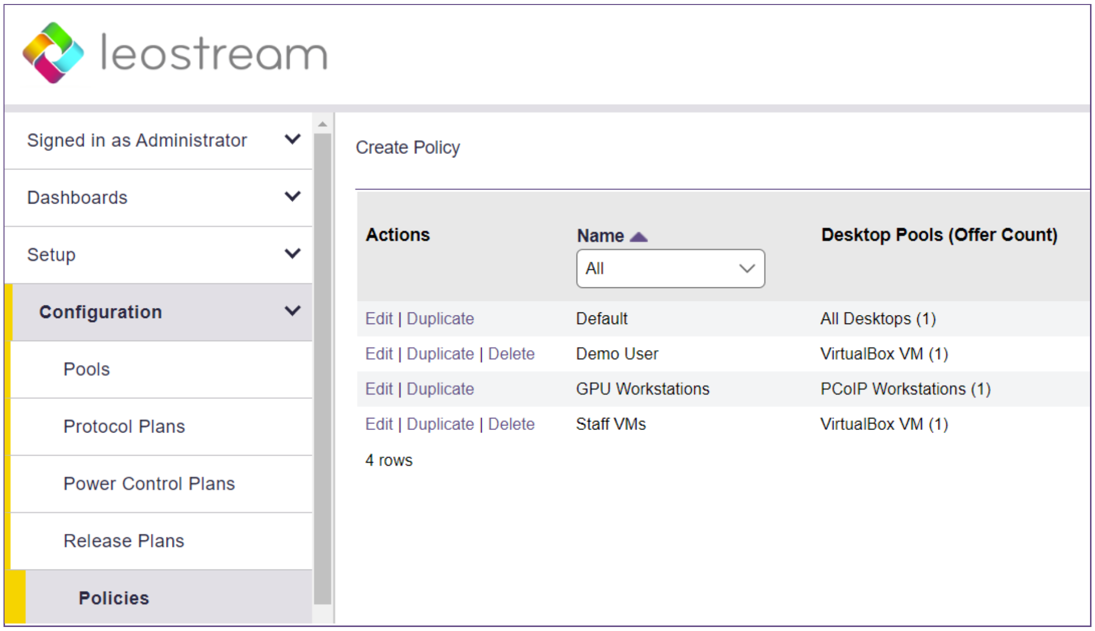
Overview

Connection Broker policies are a set of rules that determine how resources are offered, connected, and managed for a user (see **Overview of Policies and Plans** in Chapter 11). Setting up a policy includes:

- **Configuring Pool Assignment Options** to instruct the Connection Broker as to which pools to offer desktops from and how to manage the desktops in each pool when the user logs in and is assigned to a desktop
- **Configuring Policies for Hard-Assigned Desktops**
- **Configuring USB device management**.

Displaying Available Policies

The **> Configuration > Policies** page, shown in the following figure, lists the available policies. The list always contains a **Default** policy, which you can edit, but not delete.



Actions	Name ▲ All	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

The **Default** policy assigns a single desktop from the **All Desktops** pool and keeps the user assigned to that desktop until the user logs out. Additional policies appear in the order you create them, unless you have sorted your policy list.

You can modify the order and type of information displayed on this page by clicking the **Customize columns** link at the top-right side of the page (see **Customizing Tables**). The available characteristics are as follows.
Action

Drop-down menu or list of links indicating the actions you can perform on a particular policy. Currently, you can **Edit** or **Duplicate** a policy.

Name
The name given in the **Edit Policy** dialog.

Desktop Pools (Offer Count)
Lists the desktop pools used by this policy and the number of desktops offered from each pool.

For example, the following entry:

```
Operations(2) All Desktops(1)
```

indicates that the policy offers two desktops from the `Operations` pool and one desktop from the `All Desktops` pool.

Current Users
Indicates how many users are currently assigned desktops from this policy.

Current Desktops
Indicates the number of desktops currently assigned via this policy.

Assignments
Indicates the number of authentication servers that include this policy in the authentication server's assignments table (found on the **> Configuration > Assignments**) page. You cannot delete a policy that is in use in an authentication server's assignments table.

Max Desktops
Indicates the maximum number of desktops a user of this policy can be assigned.

Expire Offers After
Indicates the length of time after login when the user's session expires. A user cannot connect to additional resources after their session expires.

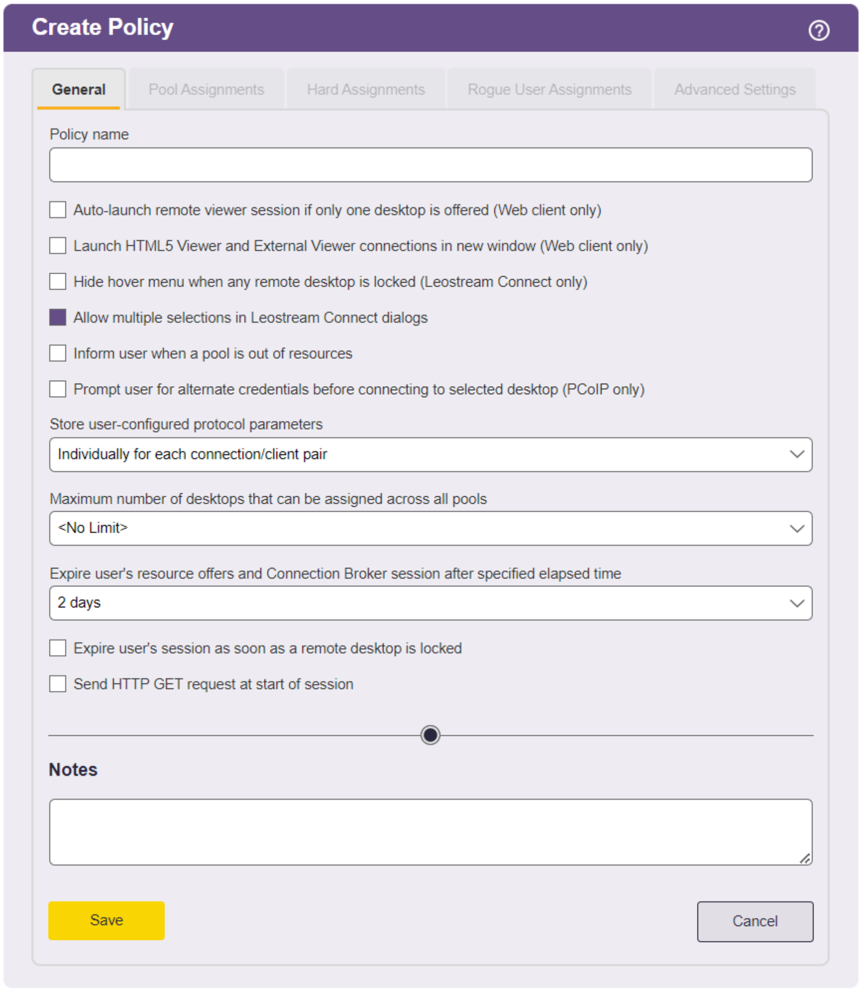
Expire Offers When Desktop is Locked
Indicates if the user's session expires after they lock one of their connected remote desktops. A user cannot connect to additional resources after their session expires.

Adding a New Policy and Configuring General Policy Options

To create a new policy:

1. Go to the **> Configuration > Policies** page.

2. Click **Create Policy**. The **Create Policy** form opens, as shown in the following figure.



Create Policy

Policy name

☐ 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)

Store user-configured protocol parameters

Individually for each connection/client pair

Maximum number of desktops that can be assigned across all pools

<No Limit>

Expire user's resource offers and Connection Broker session after specified elapsed time

2 days

☐ Expire user's session as soon as a remote desktop is locked

☐ Send HTTP GET request at start of session

Notes

3. Enter a unique name for the policy in the **Policy Name** edit field.

4. If users of this policy are logging in through the Leostream Web client and have a single desktop assigned to them, select the **Auto-launch remote viewer session if only one desktop is offered** option. With this option selected, the Connection Broker launches a remote viewing session to the remote desktop as soon as the user logs into the Connection Broker.

5. If users connect to desktops offered by this policy using a display protocol with a Java applet, an external viewer, or using the Leostream HTML5 Viewer, select the **Launch Leostream HTML5 and External Viewer connections in new window** option to indicate these connections should launch in a new window. By launching these connections in new windows, users continue to have access to their list of offered resources.

   If this option is not selected, the client launches in the window that contains the user's list of offered resources and they cannot launch additional connections.

   You can use the **Parameters for connections opened in new window** field in protocol plans to specify `window.open` parameters for external viewers. See **Launching Connections in New Windows** for complete instructions and an example.

6. Select the **Hide hover menu when any remote desktop is locked** option to instruct Leostream Connect not to open its hover menu after the user locks any of their open desktop connections. Hiding the hover menu allows you to restrict users from launching additional desktops after they lock their connected desktop.

   ⚠ The locked connection does not need to be in the forefront. If the user opens multiple desktops, the hover menu does not appear if any of the desktops are locked. Therefore, enabling this feature is most user-friendly when the user’s desktops open in full screen mode. In that case, locking the remote desktop appears to the user as if they locked the client device.

7. Select the **Allow multiple selections in Leostream Connect dialogs** option to allow the user to check multiple desktops in the **Connect** dialog that opens after the user logs in. If this option is not selected, the user can select only a single item in the **Connect** dialog.

   NOTE: This option replaces the `single_desktop_only` configuration file parameter for the Java version of Leostream Connect

8. By default, if a particular pool does not contain any available desktops, the Connection Broker skips that pool and the user receives no notification. If you want to let the user know when they are missing an offer from a particular pool, select the **Inform user when a pool is out of resources** option.

   With this option selected, the user is notified of pools with no available resources.

9. If the policy references protocol plans that allow users to configure display protocol parameters, use the **Store user-configured protocol parameters** drop-down menu to indicate if settings are stored globally or individually per desktop/client pair. See “User Configurable Protocol Plan Parameters” in the Leostream guide for **Working with Display Protocols** for more information.

10. From the **Maximum number of desktops that can be assigned across all pools** drop-down menu, select the maximum number of desktops that a user of this policy can be assigned. This number limits the number of assigned desktops across all pools in the policy, as well as of hard-assigned desktops. For example, consider a policy with three pools, configured as follows.

    - Pool 1 offers three desktops
    - Pool 2 offers one desktop
    - Pool 3 offers two desktops

    This policy offers the user a total of six desktops. If the **Maximum number of desktops assigned** drop-down menu is set to **<No Limit>** the user can be assigned, and connect to, all six desktops. If, however, the **Maximum number of desktops assigned** drop-down menu is set to **2**, the user can be assigned, and connect to, only two desktops.

    If the user is hard-assigned to one desktop, the hard-assigned desktop counts as one of their assignments. In this case, the user can be assigned and connect to only one of their policy-assigned desktops before they reach their assignment limit. In either case, if they try to connect to a third desktop, the Connection Broker issues a warning.

In the case where the user’s policy does not release their desktops, if the user logs out of those desktops and logs back into the Connection Broker, the broker offers them six desktops. However, the user can launch only the two desktops that are already assigned to them. If they need to access a different desktop, one of the assigned desktops must be released to its pool.

11. Use the **Expire user’s resource offers and Connection Broker session after specified elapsed time** option to indicate how long the user’s Leostream session is valid before they must reauthenticate. After the user’s session expires, the user can continue to use any resources that are already connected, however they cannot connect additional USB devices to these desktops or launch additional resources until they log back into the Connection Broker.

    This option applies to users logging in using Leostream Connect, the Leostream Web client, or any thin client device that writes to the Leostream API. It does not apply to users logging into the Leostream Administrator Web interface, which honors the setting in the user’s role.

12. Select the **Expire user’s session as soon as a remote desktop is locked** option to force the user to log back into the Connection Broker after they lock their remote desktop. The user’s desktop must be running a Leostream Agent in order for the Connection Broker to receive notifications when the user locks their remote desktop.

13. If you have a custom URL that the Connection Broker should call when the user logs in, select the **Send HTTP Get request at start of session** option and configure the following setting.

    - Enter the URL to call in the **URL to call at start of session** edit field. See **Sending HTTP GET Requests** for more information.

    - Enter a timeout for the call to return in the **Timeout in seconds** edit field.

    - Select the **Block Connection Broker login if call to URL fails** option to prevent the user from logging in if the URL returns a failure code to the Connection Broker. You can use the **Message to user on failed call** edit field to specify a customized error message to send to the user if their login is blocked.

14. Enter any optional information in the **Notes** field.

15. Click **Save** to continue configuring the policy.

Configuring Pool Assignment Options

Policy options for desktop pools allow you to customize the end-user experience, for example, with regards to what desktops they are offered from a pool, how long they can use that desktop, and what happens to the desktop's power state. You configure policy options separately for each pool in the policy. These options do not apply to desktops that are hard-assigned to the user or their client device. See **Configuring Policies for Hard-Assigned Desktops** for information on configuring policy options for hard-assigned desktops.

Before configuring desktop policies, ensure that you have an understanding of protocol, power control, and release plans. See **Chapter 11: Building Pool-Based Plans** for a complete description of plans.

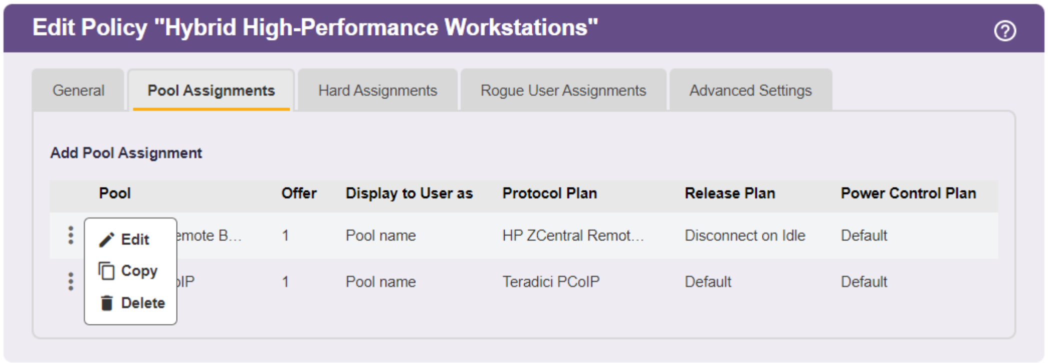
Offering Desktops from Pools

The **Pool Assignments** tab defines the pools this policy offers desktops from, how the Connection Broker selects desktops from those pools, and what happens when a user connects to one of the offered desktops.

Adding and Removing Pools in a Policy

By default, a new policy does not offer desktops from any desktop pools. To add pools, go to the **Pool Assignments** tab and click the **Add Pool Assignments** link. A modal **Edit Pool Assignment** form opens, as described in the following sections.

After configuring the pool assignment, click **Save** to add the pool to your policy. Click **Cancel** to close the modal dialog without adding the pool assignment or saving any changes. After pool assignments are added to the policy, you can edit, duplicate, or delete them using the kebab menu on the left-side of the associated row, for example:



Edit Policy "Hybrid High-Performance Workstations"

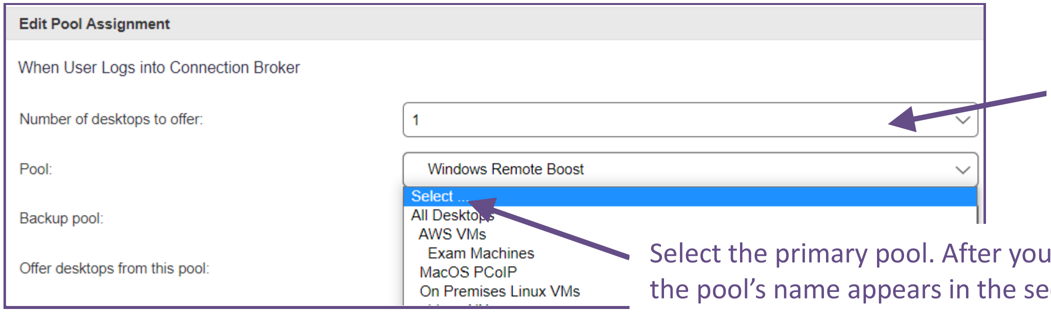
Add Pool Assignment

Pool	Offer	Display to User as	Protocol Plan	Release Plan	Power Control Plan
emote B…	1	Pool name	HP ZCentral Remot…	Disconnect on Idle	Default
IP	1	Pool name	Teradici PCoIP	Default	Default

- Select **Edit** to access the modal **Edit Pool Assignment** form.
- Click **Copy** to open the modal **Edit Pool Assignment** form prepopulated with the settings for the selected pool.
- Click **Delete** to remove the pool assignment from the policy.

Selecting Primary Pools and Number of Offered Desktops

The first step in configuring a pool assignment is to select the primary pool and the number of desktops to offer from this pool, as shown in the following figure.



Edit Pool Assignment

When User Logs into Connection Broker

Number of desktops to offer: 1

Pool: Windows Remote Boost

Backup pool:

Offer desktops from this pool:

Select the number of desktops to offer from the pool.

Select the primary pool. After you make a selection, the pool's name appears in the section header.

By default, the Connection Broker searches the primary pool for desktops to offer based on the remainder of the settings in the **When User Logs into Connection Broker** section.

Specifying Backup Pools

The Connection Broker allows you to specify backup pools to ensure that users receive an alternative desktop in the event their primary desktop is unreachable.

Backup pools provide pool-based failover at *offer* time. They are available for hard-assigned and policy-assigned desktops. The failover criteria used to determine if the Connection Broker leverages the backup pool depends on the number of desktops offered out of the pool.

- Offering one (1) desktop: In this scenario, you can fail over to the backup pool if the primary pool is empty, if the user's primary desktop has an unreachable Leostream Agent, or if the user's primary desktop has an unreachable display protocol port.

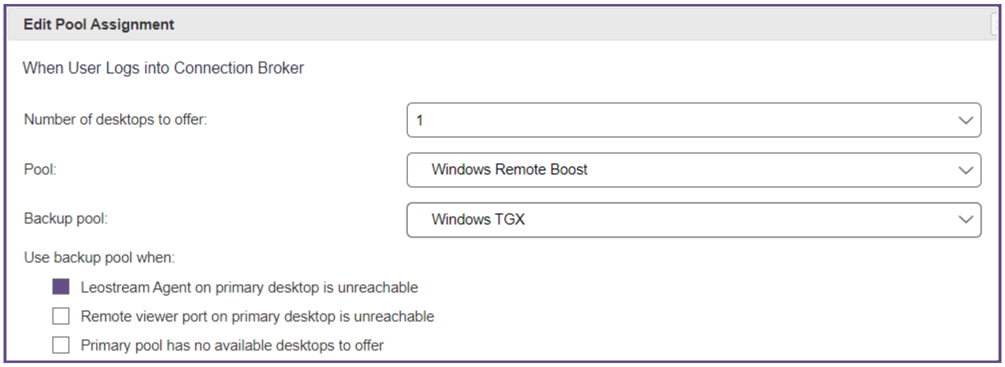
  When offering a single desktop and using backup pools, the user never sees which primary desktop they would have been offered and, therefore, does not necessarily know they are being connected to a backup desktop.

- Offering more than one desktop: In this scenario, you can fail over to the backup pool only after the primary pool is empty.

  After the user becomes assigned to a backup desktop, the Connection Broker continues to offer that assigned backup desktop until it is unassigned, even after desktops become available in the primary pool. Therefore, if desktops become available in the primary pool, users may be offered a combination of primary and backup desktops.

To enable backup pools in a policy:

1. Select the desired backup pool from the **Backup pool** drop-down menu, as shown in the following figure.



Edit Pool Assignment

When User Logs into Connection Broker

Number of desktops to offer: 1

Pool: Windows Remote Boost

Backup pool: Windows TGX

Use backup pool when:

- ■ Leostream Agent on primary desktop is unreachable
- □ Remote viewer port on primary desktop is unreachable
- □ Primary pool has no available desktops to offer

2. After selecting a backup pool, use from the **Use backup pool when** options to select the conditions that invoke the backup pool. The available options are:

    a. **Leostream Agent on primary desktop is unreachable**: The Connection Broker attempts to contact the Leostream Agent at the port indicated on the **Edit Desktop** page for the offered desktop.

    b. **Remote viewer port on primary desktop is unreachable**: The Connection Broker attempts to reach the port for the display protocol specified in this pool’s protocol plan, as selected in the **Protocol** drop-down menu in the **Plans** section of this policy.

    c. **Primary pool has no available desktops to offer**: The Connection Broker cannot find any available desktops in the primary pool, potentially because all desktops are already assigned or marked as unavailable.

3. Select protocol, power control, and release plans to associate with desktops offered from the backup pool (see **Assigning Plans**).

The Connection Broker uses the following logic when pulling a desktop from a primary pool with a specified backup pool.

1. If the **Primary pool has no available desktops to offer condition** is selected, and the primary pool has no available desktops, the Connection Broker selects a desktop from the backup pool and skips to step 5.

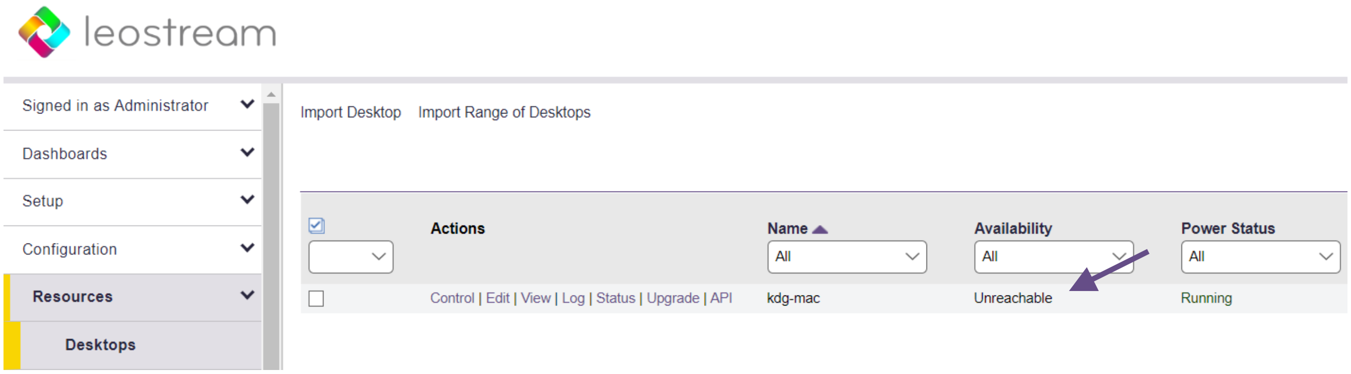
2. If the Connection Broker can pull an available desktop from the primary pool, it checks if the appropriate port on this desktop is reachable. If the port check passes, the Connection Broker:

    1. Switches the status to **Available**, if the desktop was previously **Unreachable**

    2. Offers that desktop from the pool.

    3. Skips to step 6

3. If the Connection Broker cannot successfully perform the port check, the Connection Broker marks the desktop as **Unreachable** on the **> Resources > Desktops** page, shown in the following figure. The Connection Broker continues to offer desktops that are marked as **Unreachable**.



☑	Actions	Name	Availability	Power Status
		All	All	All
□	Control | Edit | View | Log | Status | Upgrade | API	kdg-mac	Unreachable	Running

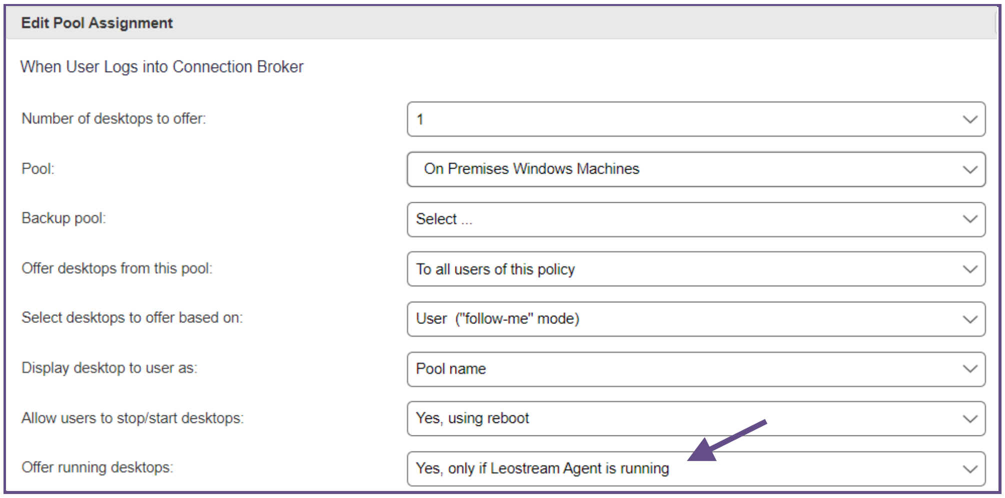
To put a desktop back in use, edit the desktop and change the **Desktop status** to **Available.**

4. The Connection Broker then selects a desktop from the backup pool.

5. The Connection Broker does not perform a port check on the backup desktop. The backup desktop is always offered.

6. The Connection Broker repeats step 1 through 5 for each pool in the policy.

If you select the Leostream Agent port check as a backup pool condition, ensure that the desktop offered from the primary pool has a running Leostream Agent by selecting **Yes, only if Leostream Agent is running** from the **Offer running desktops** drop-down menu, as shown in the following figure. Otherwise, if the offered desktop does not have an installed and running Leostream Agent, the Connection Broker always fails over to the backup pool.



Edit Pool Assignment

When User Logs into Connection Broker

Number of desktops to offer:	1
Pool:	On Premises Windows Machines
Backup pool:	Select ...
Offer desktops from this pool:	To all users of this policy
Select desktops to offer based on:	User ("follow-me" mode)
Display desktop to user as:	Pool name
Allow users to stop/start desktops:	Yes, using reboot
Offer running desktops:	Yes, only if Leostream Agent is running

Offering Pools to Groups of Users, Optionally Based on a Schedule

The **Offer desktops from this pool** option controls which pools are offered to each user who is assigned to this policy. By default, this option is **To all users of this policy** and the Connection Broker attempts to offer a desktop from this pool to every user assigned to the policy.

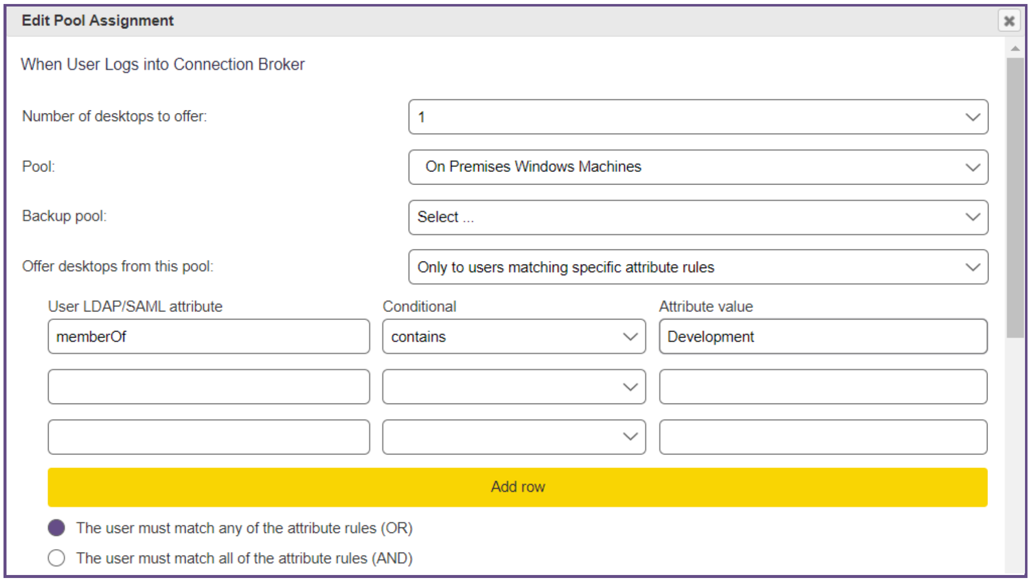
You can modify this setting to model one of the following additional scenarios:

- Offer desktops from this pool only to certain groups of users – This is useful if you have a top-level group of users assigned to the policy, but then need to restrict access to the pools based, for example, on the projects those users are working on.

- Offer desktops from this pool only to certain groups of users and only at certain days and times – This is useful for scheduling access, for example, for restricted access to classroom, project, or lab resources.

To restrict this pool to users in specific groups or with specific attributes, select the **Only to users matching specific attribute rules** option. In this case, the form modifies to contain fields for defining rules that limit which users are offered desktops from this pool.

For example, the following figure defines a rule that restricts the Connection Broker to offer desktops from this pool only to users who are a member of the `Development` group.



Edit Pool Assignment

When User Logs into Connection Broker

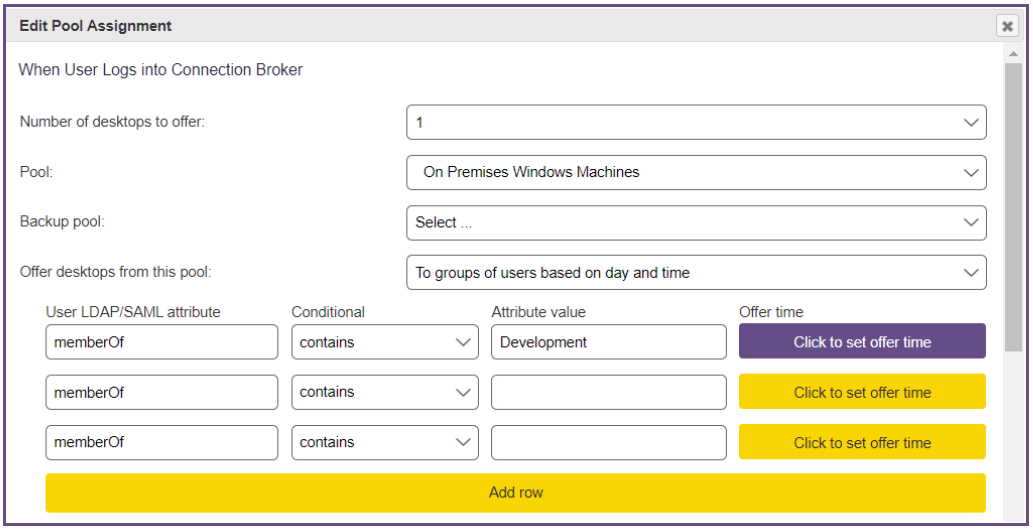
Number of desktops to offer:	1
Pool:	On Premises Windows Machines
Backup pool:	Select ...
Offer desktops from this pool:	Only to users matching specific attribute rules

User LDAP/SAML attribute	Conditional	Attribute value
memberOf	contains	Development

● The user must match any of the attribute rules (OR)

○ The user must match all of the attribute rules (AND)

To restrict this pool to users with specific attributes *and* based on a schedule, select the **To groups of users based on day and time** option. In this case, the form modifies to contain fields for defining rules that limit which groups of users are offered desktops at certain days and times, for example:



Edit Pool Assignment ✖

When User Logs into Connection Broker

Number of desktops to offer: 1

Pool: On Premises Windows Machines

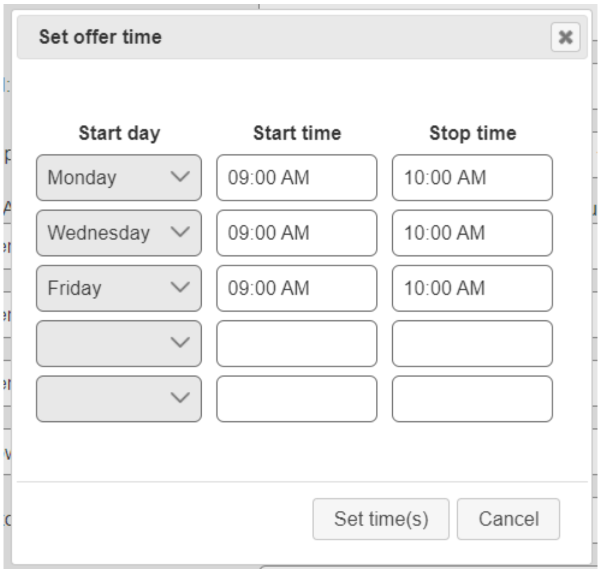
Backup pool: Select ...

Offer desktops from this pool: To groups of users based on day and time

User LDAP/SAML attribute	Conditional	Attribute value	Offer time
memberOf	contains	Development	Click to set offer time
memberOf	contains		Click to set offer time
memberOf	contains		Click to set offer time

Add row

Specify the groups of users as you would in the previous example, then click the **Click to set offer time** button to specify when this group of users has access. For example, for a class that runs Monday, Wednesday, and Friday from 9am to 10am, configure the form as follows.

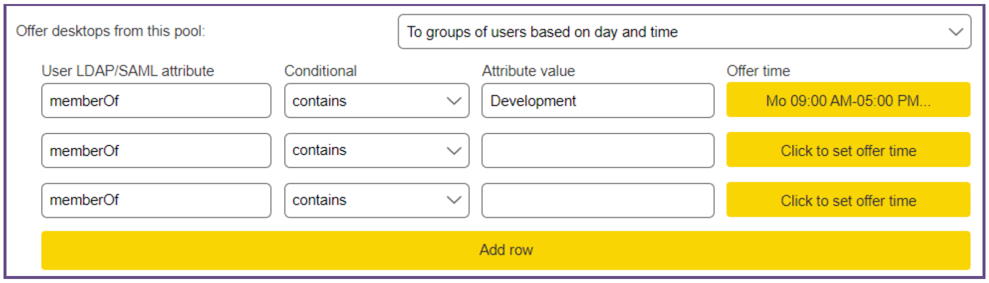


Set offer time ✖

Start day	Start time	Stop time
Monday	09:00 AM	10:00 AM
Wednesday	09:00 AM	10:00 AM
Friday	09:00 AM	10:00 AM

Set time(s) Cancel

Click **Set times(s)** to accept the schedule. The policy form then updates with a preview of the entered schedule. If this was a Math 101 class, for example, the complete policy form could then assign this schedule to employees who are a member of “Development”, for example:



Offer desktops from this pool: To groups of users based on day and time

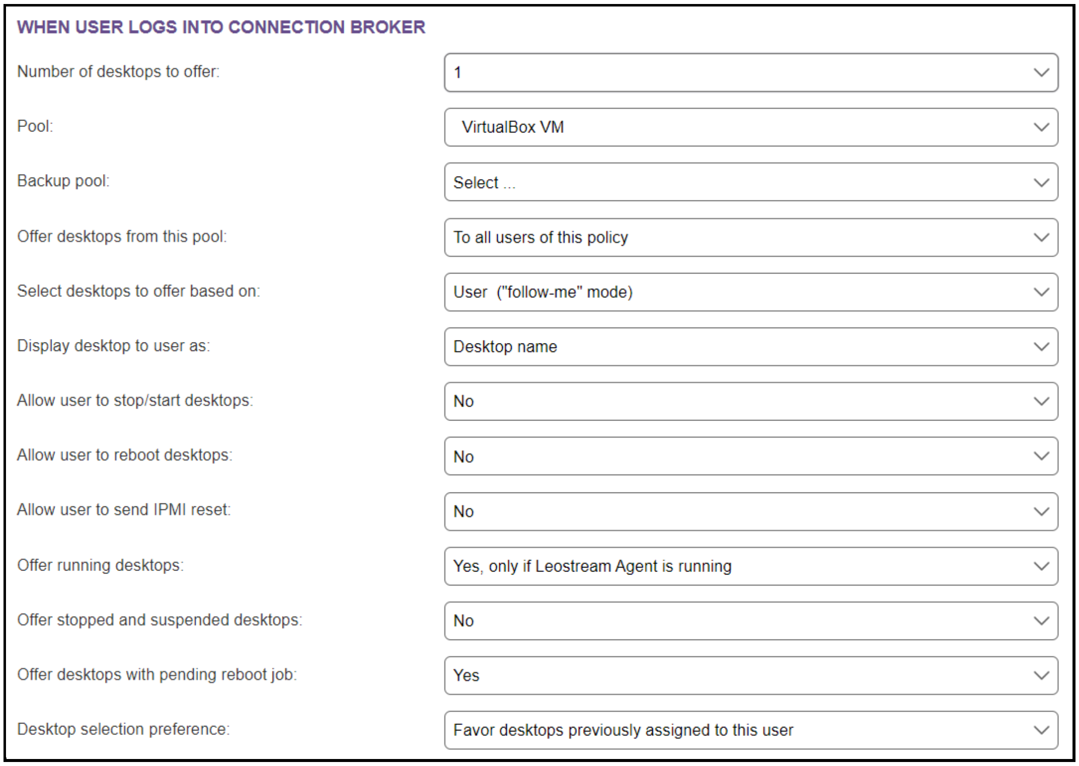
User LDAP/SAML attribute	Conditional	Attribute value	Offer time
memberOf	contains	Development	Mo 09:00 AM-05:00 PM...
memberOf	contains		Click to set offer time
memberOf	contains		Click to set offer time

Add row

Currently, scheduled access cannot span across days. The start and stop time must be on the same day of the week. All times are evaluated in the Connection Broker time zone, which is the time zone associated with the Connection Broker database.

Setting Rules for Selecting Desktops from Pools

After you select your pools and backup pools, the remainder of the **When User Logs into Connection Broker** section, shown in the following figure, defines how the Connection Broker selects which desktops to offer the end-user from these pools.



WHEN USER LOGS INTO CONNECTION BROKER

Number of desktops to offer:	1
Pool:	VirtualBox VM
Backup pool:	Select ...
Offer desktops from this pool:	To all users of this policy
Select desktops to offer based on:	User ("follow-me" mode)
Display desktop to user as:	Desktop name
Allow user to stop/start desktops:	No
Allow user to reboot desktops:	No
Allow user to send IPMI reset:	No
Offer running desktops:	Yes, only if Leostream Agent is running
Offer stopped and suspended desktops:	No
Offer desktops with pending reboot job:	Yes
Desktop selection preference:	Favor desktops previously assigned to this user

- **Offer desktops from this pool**: Determines which users of this policy are offered desktops from this pool. By default, the **To all users of this policy** option is selected, and the Connection Broker offers desktops to all users. For more information on using this option, see Offering Pools to Groups of Users, Optionally Based on a Schedule.

- **Select desktops to offer based on**: Determines how the Conn ection Broker decides which desktops to offer. You can select between the following two assignment modes:

  - **User (“follow-me” mode)**: When selected, the Connection Broker assigns the desktop based only on the user’s identity. In this mode, if the same user credentials are used to log into a second client, the Connection Broker moves any existing desktop connections from the first client device to the user’s new client. In follow-me mode, each user can be simultaneously logged in from only one client.

  - **User and client (“kiosk” mode)**: When selected, the Connection Broker assigns the desktop based on the client and the user, rather than just the user. In this mode, if the same user credentials are used to log into a second client, the Connection Broker assigns a different desktop to each client. In kiosk mode, one user can simultaneously log in from multiple clients.

See **Desktop Assignment Modes** for more information on the different assignment modes.

- **Display to users as**: Configures how desktops are listed by the client. You can display desktops as:
  - Desktop name
  - Desktop display name
  - Machine name
  - Pool name
  - Pool name: Desktop name
  - Pool name: Desktop display name
  - Pool name: Machine name
  - Pool display name
  - Pool display name: Desktop name
  - Pool display name: Desktop display name
  - Pool display name: Machine name

- **Allow users to stop/start desktops**: Use this option to display the **Start** and **Stop** actions to users who log in using the Leostream Web client or Leostream Connect.
  - Select **No** to restrict the user from starting or stopping desktops from this pool
  - Select **Yes, using reboot** to allow the user to start and stop their desktops using a graceful power down and restart
  - Select **Yes, using power off and start** to allow the user to start and stop their desktop using a forceful power down and restart

- **Allow users to reboot desktops**: Use this option to display the **Restart** action to users who log in using the Leostream Web client or Leostream Connect.
  - Select **No** to restrict the user from restarting their desktops from this pool
  - Select **Yes, using reboot** to allow the user to restart their desktops using a graceful power down and restart
  - Select **Yes, using power off and start** to allow the user to restart their desktop using a forceful power down and restart

- **Allow user to send IPMI reset**: Select **Yes** to present the user with a **Hard Reset** option for their IPMI-enabled physical desktops. The Connection Broker calls the `chassis power cycle` function whenever a hard reset is requested.

  The previous three policy settings that provide users with power control actions also require the user be assigned a role that gives them permission to restart their desktops (see **Session Permissions**).

- **Offer running desktops**: Use this option if the Connection Broker can offer a running desktop only if it has an installed and running Leostream Agent.

  - Select **Yes, only if Leostream Agent is running** if the user should be offered only those desktops with an installed Leostream Agent that is successfully communicating with the Connection Broker. Also, select this option if you are using a port check on the Leostream Agent to determine if the Connection Broker should offer desktops from the backup pool (see **Specifying Backup Pools**)
  - Select **Yes, regardless of Leostream Agent status** to indicate the Connection Broker can ignore the Leostream Agent status when selecting a running desktop to offer from the pool.

- **Offer stopped and suspended desktops**: Use this option to indicate if the Connection Broker may offer stopped or suspended desktops. When a user requests a connection to a stopped or suspended desktop, the Connection Broker attempts to start or resume the desktop when the desktop is assigned.
  - Select **No** if the Connection Broker should never offer a stopped or suspended desktop. In particular, select this option if the Connection Broker is unable to power up a user's desktop, for example if the desktop is a physical machine that is not Wake-on-LAN enabled.
  - Select **Yes, only if Leostream Agent is installed** to limit the Connection Broker to offer stopped desktops only if the Connection Broker knows the desktop has an installed Leostream Agent. The desktop and its installed Leostream Agent must have been running when the desktop registered with the Connection Broker, or during a subsequent center refresh, for the Connection Broker to learn about the Leostream Agent.
  - Select **Yes, regardless of Leostream Agent status** to allow the Connection Broker to offer any stopped desktop.
- **Offer desktops with pending reboot job**: Use this option to indicate if the Connection Broker can offer desktops with a scheduled reboot job. The Connection Broker cancels the reboot job as soon as a new user is assigned to the desktop. Uncheck this option if your desktops must finish their scheduled reboot jobs before being assigned to a new user.

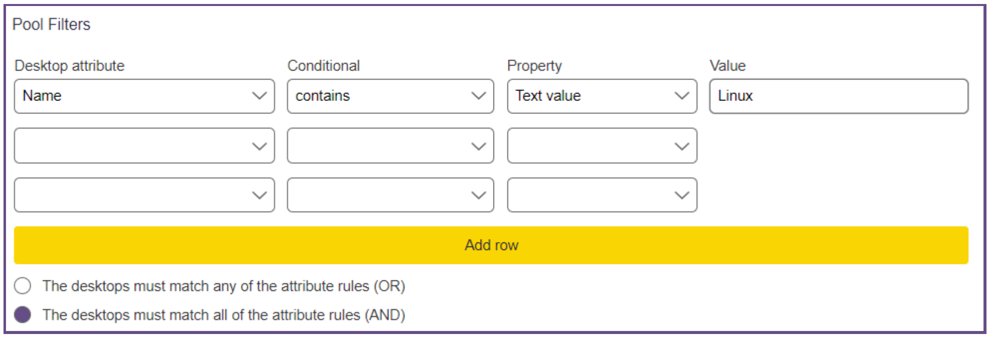
  This option applies only to reboot jobs that were scheduled by the Connection Broker, for example, by a power control plan.
- **Desktop selection preference**: Use this option to indicate if the Connection Broker should look for desktops that were previously assigned to the user.
  - **Favor desktops previously assigned to this user**: When this option is selected, the Connection Broker tries to offer a user any desktops that were previously assigned to that user, before offering different desktops from the pool. Select this option to optimize roaming profile performance.

    You can use the **Bulk Edit** form for the user's desktop to remove the user's affinity to their previously assigned desktop. See **Removing Desktop Affinities** for more information.

- **Select random available desktops**: Select this option to offer any desktops from the pool.
- **Offer oldest desktops first:** Select this option to offer the oldest desktops in the pool, where the desktop's age is determined by when its record was created in the Connection Broker. Use the `created` field in the `vm` table to determine when the desktop record was added to the Connection Broker.
- **Favor least recently offered desktops:** Select this option to prefer desktops that have not been recently offered. The Connection Broker uses the value in the **Last Offered Time** column to find desktops that were offered the longest time ago.
- **Favor running desktops:** Select this option to offer all running desktops before offering any stopped desktops from the pool. This option may optimize the end-user experience by removing the need for users to wait for their machine to power on before they can connect.

Using Pool Filters to Limit Available Desktops in the Pool

The **Pool Filters** section at the bottom of the **Edit Pool Assignment** form, shown in the following figure, allows you to restrict which desktops the Connection Broker can potentially offer from the pool. A pool filter applies only to its associated pool; it does not apply to any other pool in the policy.



Pool Filters

Desktop attribute	Conditional	Property	Value
Name	contains	Text value	Linux

○ The desktops must match any of the attribute rules (OR)

● The desktops must match all of the attribute rules (AND)

Each row in the **Pool Filters** section reads as a rule that checks if a desktop in this pool can be offered by this policy. To specify a filter:

1. Select an attribute from the **Desktop attribute** drop-down menu. You can filter desktops based on the following attributes:

   - Name
   - Machine name
   - Installed protocols – Based on the display protocols reported by the Leostream Agent on the remote desktop. You can add the **Installed Protocols** column to the **> Resources > Desktops** page to see which desktops have reported protocols.
   - vCenter Server Notes
   - Any Active Directory attribute associated with the desktop, such as `managedBy`. You must create an Active Directory center for these attributes to appear (see **Active Directory Centers**).

2. Select a logic condition from the **Conditional** drop-down menu.

3. In the **Property** drop-down menu, indicate the type of attribute to filter against. Options include:

   - User Attribute
   - Client Attribute
   - Text Value

   You can use certain dynamic tags when filtering based on a text value. In particular, the following dynamic tags are supported.

   - `{AD:USER:`*`attribute_name`*`}`: Filters based on the value found in the user's Active Directory attribute given by *`attribute_name`*.

   - `{AD:CLIENT:`*`attribute_name`*`}`: Filters based on the value found for the attribute given by *`attribute_name`* in the client's Computer Active Directory object.

     The user must authenticate with the Connection Broker using Active Directory. If this is the case, the Connection Broker uses the name of the client computer, determined as either the NetBIOS or DNS name, to search for the correct Computer object in Active Directory.

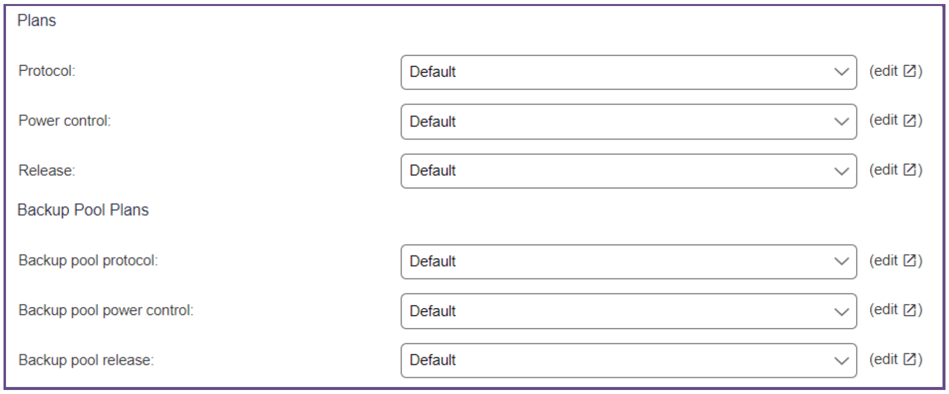
4. In the **Value** field, select or enter the actual attribute value to test against.
   ⚠ Not all clients return their MAC address. If you plan to filter pools using the client MAC address attribute, go to the **Edit Client** page for each client and ensure that they are correctly returning their MAC address.

5. Indicate if the desktop can match any rule (OR) or must match all rules (AND), in order to be available in this policy.

The Connection Broker applies the pool filter and any defined policy-wide filter when determining which desktops can be offered from a particular pool.

Assigning Plans

The **Plans** section, shown in the following figure, allows you to associate a protocol, power control, and release plan with the desktops offered from a pool. The selections in the **Protocol**, **Power control**, and **Release** drop-down menus define the plans associated with desktops offered from the primary pool. The **Backup pool protocol**, **Backup pool power control**, and **Backup pool release** drop-down menus define the plans associated with a desktop that is offered from the backup pool. If the primary pool does not have a backup pool, these three drop-down menus are not shown.



Plans

Protocol:	Default	(edit)
Power control:	Default	(edit)
Release:	Default	(edit)

Backup Pool Plans

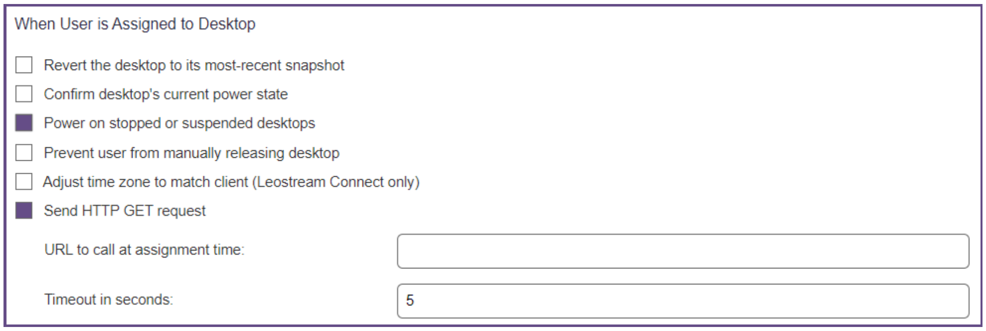
Backup pool protocol:	Default	(edit)
Backup pool power control:	Default	(edit)
Backup pool release:	Default	(edit)

See **Chapter 11: Building Pool-Based Plans** for instructions on creating plans.

These plans are associated with the desktop at the time that desktop is policy-assigned to the user. The same desktops may be assigned to different plans when offered from another pool or policy.

Policy Options for When Desktops are Assigned

For desktops offered from pools, the Connection Broker assigns the desktop to the user at the time the user requests a connection to that desktop. The **When User is Assigned to Desktop** section of the **Edit Pool Assignment** form, shown in the following figure, controls what happens when a desktop from this pool is assigned to a user.



When User is Assigned to Desktop

☐ Revert the desktop to its most-recent snapshot
☐ Confirm desktop's current power state
☑ Power on stopped or suspended desktops
☐ Prevent user from manually releasing desktop
☐ Adjust time zone to match client (Leostream Connect only)
☑ Send HTTP GET request

URL to call at assignment time:	
Timeout in seconds:	5

The following options also apply when a user reconnects to a policy-assigned desktop that was never released back to the pool, i.e., the user remained assigned to the desktop after they log out.

- **Revert the desktop to its most recent snapshot**: For VMware virtual machines, revert the VM back to its most recent snapshot prior to connecting the user. This option is done only when the desktop is first assigned.
- **Confirm desktop's current power state**: Select this option to have the Connection Broker check the desktop's power state when the user requests a connection to the desktop. Use this option if your centers have a long power state refresh interval, which occasionally causes a desktop's power status in the Connection Broker to be out-of-sync with the desktop's actual power state. If this option is not selected, the Connection Broker does not confirm that a desktop is running or stopped when assigning the desktop to the user.

  Consider an example where a desktop's last known power state is **Stopped** and the **Power on stopped or suspended desktops** option is selected. If you manually powered on this desktop from, for example, vCenter Server, the Connection Broker may believe this desktop is stopped even though the desktop is now running. If you do not have the **Confirm desktop power state** option selected, the Connection Broker sends a power on command to the stopped desktop, which delays the user's connection to the desktop.

- **Power on stopped or suspended desktops:** Select this option to have the Connection Broker send a power on command to any desktop with a current power state of stopped.

- **Prevent user from manually releasing desktop**: For users logging in with a role that gives them permission to release their desktops (see **Session Permissions**), this option allows you to restrict the user from manually releasing desktops from this pool.

- **Adjust time zone to match client**: Select this option to instruct the Connection Broker to change the time zone of a Windows remote desktop to match the time zone of the user's client device. The Connection Broker does *not* revert the time zone to its original value after the user logs out. This option applies when the user logs in from the Windows or Java version of Leostream Connect, or an HP SAM client.

- **Send HTTP GET request:** Select this option to perform an HTTP GET request when the user is assigned to their desktop. When selected, you can use the **URL to call at assignment time** field to specify your URL and the **Timeout in seconds** field to indicate how long the URL has to return a result. URLs that return a failure to not block the user from proceeding with their desktop connection.

  You can use a small subset of the available dynamic tags in your URL, including {IP}, {IP_ADDRESS}, {HOSTNAME}, {SHORT_HOSTNAME}, and {USER}. See Using Dynamic Tags for more information on these dynamic tags.

Policy Options for When User Connects to Desktop

The **When User Connect to** Desktop section of the policy controls the actions that occur when the user first connects to their desktop and whenever they reconnect to a disconnected session.

- **Log user into remote desktop as:** Indicates if the user should be logged into the remote desktop as a domain user, or as a local user. By default, the user's role determines this setting. If you are creating a policy that offers both Windows and Linux desktops, you can use this setting to log the user into Windows as a Domain user, but Linux as a local user.

- **Log out any rogue users**: Forcefully logs out users who logged into a machine without going through the Connection Broker. The desktop must be running the Leostream Agent to use this feature.

- **Enable single-sign-on to desktop console**: Select **Yes, with username and password** to instruct the Connection Broker to use the Leostream Agent to log users into the remote operating system. Enabling this option has no affect if you did not install the single sign-on component of the Leostream Agent.

  Leave this option set to **No** when connecting users with a display protocol, for example HP Anyware software, that has built-in single sign-on.

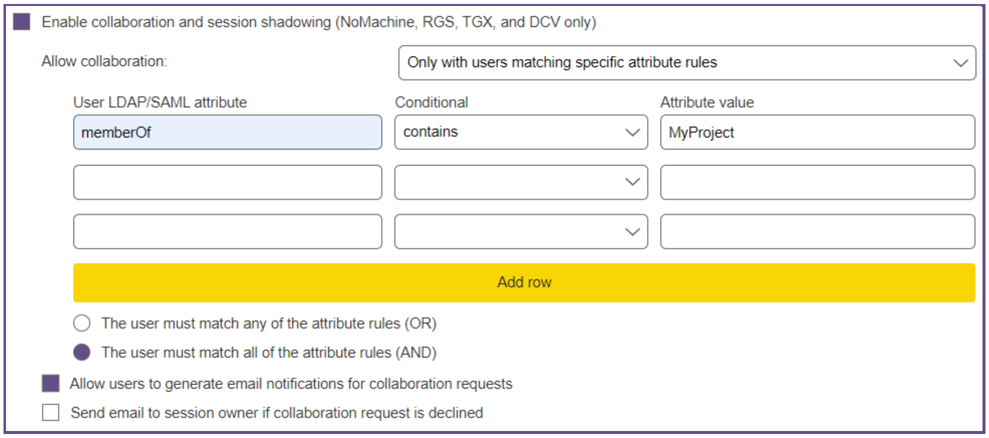
⚠ When offering Linux or Windows remote desktops, this option applies if the user connects to workstations with an installed PCoIP Remote Workstation Card. When connecting to Windows operating systems, you can also leverage this option with DCV, VNC, NoMachine, and Scyld Cloud Workstation.

By default, the Connection Broker sends the username and password that were used to log into the Connection Broker and the domain specified by the user’s Role or Policy (either their authentication server domain or the desktop’s local hostname.) Use the **Send user login name as**, **Send user password as**, and **Send user domain as** edit fields to override these user credentials, for example, to provide SSO on the remote desktop using a generic account without sharing those credentials with the users.

Use the {VM:USERNAME_OVERRIDE}, {VM:PASSWORD_OVERRIDE}, and {VM:DOMAIN_OVERRIDE} dynamic tags in these edit fields if you’ve specified desktop-specific credentials in the **Log user into remote desktop with this *XXX*** edit fields on the **Edit Desktop** page.

- **Enable collaboration and session shadowing**: Select this option to allow the user to invite another user to collaborate on their NoMachine, HP ZCentral Remote Boost (RGS), or Mechdyne TGX session (see “Session Shadowing and Collaboration” in the Leostream Guide for Working with Display Protocols).

  - Use the **Allow collaboration** to indicate which users the session owner may invite to collaborate. By default, this value is set to **With all users**. If your users log in using the Leostream Web client, you can restrict who they may invite to collaborate by selecting **Only with users matching specific attribute rules**, for example, the following figure allows users with this policy to invite only users who are a member of the `MyProject` group.



☑ Enable collaboration and session shadowing (NoMachine, RGS, TGX, and DCV only)

Allow collaboration: Only with users matching specific attribute rules

User LDAP/SAML attribute	Conditional	Attribute value
memberOf	contains	MyProject

○ The user must match any of the attribute rules (OR)

● The user must match all of the attribute rules (AND)

☑ Allow users to generate email notifications for collaboration requests

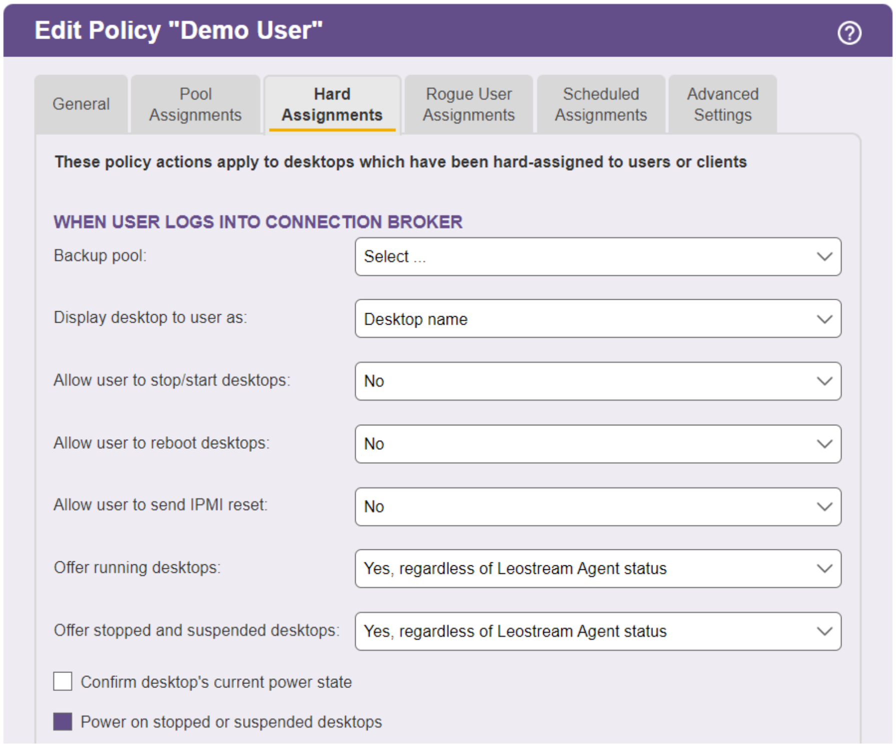
□ Send email to session owner if collaboration request is declined

  - When collaboration is enabled, select the **Allow users to generate email notifications for collaboration requests** option, shown in the previous figure, if the session owner should have the ability to send an email to the user they are inviting to their session. The email is sent by the SMTP server configured in Leostream (see **Configuring an SMTP Server for Alerts**).

- Select the **Send email to session owner if collaboration request is declined** option to have Leostream automatically send an email to the session owner if the collaborator explicitly declines the invitation.

Configuring Policies for Hard-Assigned Desktops

The **Hard Assignments** tab, shown in the following figure, applies to desktops that are hard-assigned to the user as well as to desktops that are hard-assigned to a client. This section includes a subset of the policy options available for policy-assigned desktops.



These policy actions apply to desktops which have been hard-assigned to users or clients

WHEN USER LOGS INTO CONNECTION BROKER

Backup pool: Select ...

Display desktop to user as: Desktop name

Allow user to stop/start desktops: No

Allow user to reboot desktops: No

Allow user to send IPMI reset: No

Offer running desktops: Yes, regardless of Leostream Agent status

Offer stopped and suspended desktops: Yes, regardless of Leostream Agent status

☐ Confirm desktop's current power state

☑ Power on stopped or suspended desktops

When User Logs into the Connection Broker

- **Backup pool:** Provides a pool of backup desktops to use in the event that the Connection Broker cannot establish a connection to the hard-assigned desktop (see Specifying Backup Pools.)

- **Display to users as**: Configures how desktops are listed by the client. You can display desktops as:
  - Desktop Name
  - Desktop display name
  - Machine Name

- **Allow users to stop/start desktops**: Use this option to display the **Start** and **Stop** actions to users who log in using the Leostream Web client or Leostream Connect.
  - Select **No** to restrict users from starting or stopping desktops from this pool

  - Select **Yes, using reboot** to allow users to start and stop their desktops using a graceful power down and restart

  - Select **Yes, using power off and start** to allow users to start and stop their desktops using a forceful power down and restart

- **Allow users to reboot desktops**: Use this option to display the **Restart** action to users who log in using the Leostream Web client or Leostream Connect.

  - Select **No** to restrict users from restarting their desktops from this pool
  - Select **Yes, using reboot** to allow users to restart their desktops using a graceful power down and restart
  - Select **Yes, using power off and start** to allow users to restart their desktops using a forceful power down and restart

- **Allow user to send IPMI reset**: Select **Yes** to present users with a **Hard Reset** option for their IPMI-enabled physical desktops. The Connection Broker calls the `chassis power cycle` function whenever a hard reset is requested.

  The previous three policy settings that provide users with power control actions also require the user be assigned a role that gives them permission to restart their desktops (see **Session Permissions**).

- **Offer running desktops**: Use this option if the Connection Broker can offer a running desktop only if it has an installed and running Leostream Agent.

  - Select **Yes, only if Leostream Agent is running** if the user should be offered only those desktops with an installed Leostream Agent that is successfully communicating with the Connection Broker. Also, select this option if you are using a port check on the Leostream Agent to determine if the Connection Broker should offer desktops from the backup pool (see **Specifying Backup Pools**)

  - Select **Yes, regardless of Leostream Agent status** to indicate the Connection Broker can ignore the Leostream Agent status when selecting a running desktop to offer from the pool.

- **Offer stopped and suspended desktops**: Use this option to indicate if the Connection Broker should offer the hard-assigned desktop if it is stopped or suspended. When a user requests a connection to a stopped or suspended desktop, the Connection Broker attempts to start or resume the desktop when the user requests a connection.

  - Select **No** if the Connection Broker should never offer a stopped or suspended desktop. In particular, select this option if the Connection Broker is unable to power up a user’s desktop, for example if the desktop is a physical machine that is not Wake-on-LAN enabled.

  - Select **Yes, only if Leostream Agent is installed** to limit the Connection Broker to offer stopped desktops only if the Connection Broker knows the desktop has an installed Leostream Agent. The desktop and its installed Leostream Agent must have been running when the desktop registered with the Connection Broker, or during a subsequent center refresh, for the Connection Broker to learn about the Leostream Agent.

- Select **Yes, regardless of Leostream Agent status** to allow the Connection Broker to offer any stopped desktop.

- **Confirm desktop power state:** Select this option to have the Connection Broker check the desktop's power status when the user requests a connection to the desktop. Use this option if your centers have a long power state refresh interval, which occasionally causes a desktop's power status in the Connection Broker to be out-of-sync with the desktop's actual power status. If this option is not selected, the Connection Broker does not confirm that a desktop is running or stopped when assigning the desktop to the user.
- **Adjust time zone to match client (Leostream Connect and HP SAM only):** Select this option to instruct the Connection Broker to change the time zone of a Windows remote desktop to match the time zone of the user's client device. The Connection Broker does *not* revert the time zone to its original value after the user logs out.

- **Associate initial user login with assigned user**: Select this option if the Connection Broker should map the user identity of the first login notification that comes from the Leostream Agent to the user identity of the hard-assigned user. After that association is made, all subsequent log off, disconnect, and connect notifications provided by the Leostream Agent for the mapped user invoke the policy and plan actions of the hard-assigned user (see **Mapping Login Notifications to Assigned User ID**).

When User Connects to Desktop

- **Close Leostream Gateway port if user hasn't logged in after**: Allows you to close Leostream Gateway port forwarding rules if users request a connection to their hard-assigned desktop, but never log into the remote operating system. After the user requests a connection to the destkop, the Connection Broker waits to receive a login notification from the Leostream Agent on the desktop for the length of time specified by this option. If the Connection Broker does not receive the login notification, the Connection Broker instructs the Leostream Gateway to close the forwarding port associated with this connection.

  After the port is closed, users must initiate the desktop connection from their Leostream session in order to reopen the port and connect to the destkop.

- **Log out any rogue users**: Enables you to log out users who logged into a machine without going through the Connection Broker. The desktop must be running the Leostream Agent to use this feature.

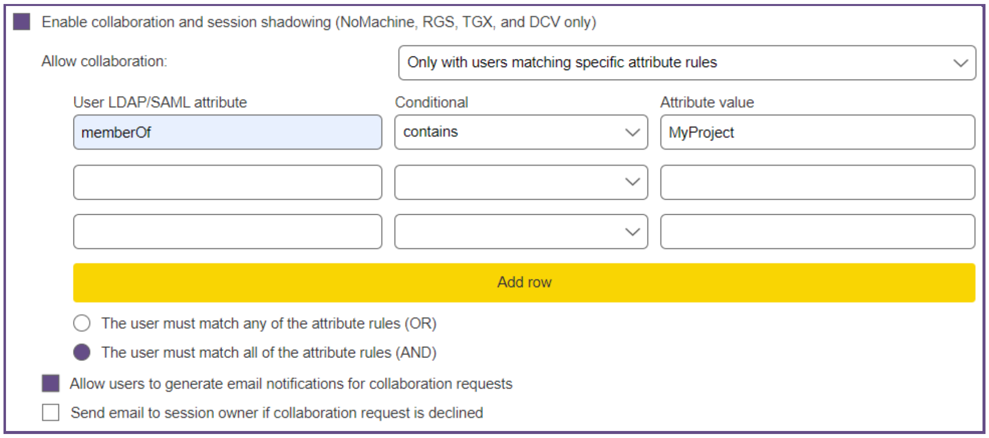
- **Enable single-sign-on to desktop console**: Select **Yes, with username and password** to instruct the Connection Broker to use the Leostream Agent to log users into the remote operating system. Enabling this option has no affect if you did not install the single sign-on component of the Leostream Agent.

  Leave this option set to **No** when connecting users with a display protocol, for example HP Anyware software, that has built-in single sign-on.

By default, the Connection Broker sends the username and password that were used to log into the Connection Broker and the domain specified by the user's Role or Policy (either their authentication server domain or the desktop's local hostname.) Use the **Send user login name as**, **Send user password as**, and **Send user domain as** edit fields to override these user credentials, for example, to provide SSO on the remote desktop using a generic account without sharing those credentials with the users.

Use the {VM:USERNAME_OVERRIDE}, {VM:PASSWORD_OVERRIDE}, and {VM:DOMAIN_OVERRIDE} dynamic tags in these edit fields if you've specified desktop-specific credentials in the **Log user into remote desktop with this *XXX*** edit fields on the **Edit Desktop** page.

- **Enable collaboration and session shadowing**: Select this option to allow the user to invite another user to collaborate on their NoMachine, HP ZCentral Remote Boost (RGS), or Mechdyne TGX session (see "Session Shadowing and Collaboration" in the Leostream Guide for Working with Display Protocols).
    - Use the **Allow collaboration** to indicate which users the session owner may invite to collaborate. By default, this value is set to **With all users**. If your users log in using the Leostream Web client, you can restrict who they may invite to collaborate by selecting **Only with users matching specific attribute rules**, for example, the following figure allows users with this policy to invite only users who are a member of the `MyProject` group.



☑ Enable collaboration and session shadowing (NoMachine, RGS, TGX, and DCV only)

Allow collaboration: Only with users matching specific attribute rules

User LDAP/SAML attribute	Conditional	Attribute value
memberOf	contains	MyProject

○ The user must match any of the attribute rules (OR)
● The user must match all of the attribute rules (AND)
☑ Allow users to generate email notifications for collaboration requests
□ Send email to session owner if collaboration request is declined

-
    - When collaboration is enabled, select the **Allow users to generate email notifications for collaboration requests** option, shown in the previous figure, if the session owner should have the ability to send an email to the user they are inviting to their session. The email is sent by the SMTP server configured in Leostream (see **Configuring an SMTP Server for Alerts**).
    - Select the **Send email to session owner if collaboration request is declined** option to have Leostream automatically send an email to the session owner if the collaborator explicitly declines the invitation.

When User Disconnects from Desktop

A hard-assigned desktop is never released from a user. Therefore, release plans do not apply to hard-assigned desktops. You can perform a subset of release actions, using the options described in the following sections.

The **Forced logout** drop-down menu provides options to log the user out after they disconnect from their remote session.

- Select **No** to allow the user to disconnect from their desktop, but remain logged into that desktop and retain their session’s state. The next time the user logs in, they are presented with their session in the state it was at when they originally disconnected.
- Select **Immediately** to log a user out of their desktop as soon as they disconnect, or delay the logout by selecting a delay time. After the user is forcefully logged out, their session is terminated and any unsaved changes made in their previous session are lost. The user receives a new session the next time they log in.

You must install the Leostream Agent on the desktop to use the **Forced logout** policy option.

To perform an HTTP GET request as soon as the user disconnects from their remote sessions, enter the URL in the **URL to call** edit field. By sending GET requests, you can perform additional configuration actions necessary for your environment

When User Logs Out of Desktop

To perform an HTTP GET request as soon as the user logs out of their remote sessions, enter the URL in the **URL to call** edit field. By sending GET requests, you can perform additional configuration actions necessary for your environment

If the user is connecting to the desktop using PCoIP or VNC, you can instruct the Connection Broker to retain the console connection after the user logs out by selecting the **Retain console connection (DCV, VNC, and PCoIP only)** option. With this option selected, the user is returned to the operating system login page, not the client login page. This option is most useful for users logging into desktops that are hard-assigned to particular clients.

When Connection is Closed

If the user’s hard-assigned desktop does not have an installed and running Leostream Agent, the Connection Broker cannot distinguish between a log out and a disconnect. In this case, the Connection Broker receives a *connection closed* event from Leostream Connect and executes the **When Connection is Closed** section of the user’s policy. Use this section to indicate if an undistinguishable connection-closed event is treated as a logout or disconnect.

When Desktop is Idle

If the hard-assigned desktop has an installed, running Leostream Agent, you can perform actions when the user’s remote session is idle. A session is idle when there are no mouse or keyboard actions. Use the **Lock**

Desktop, **Disconnect**, **Logout**, and **Call URL** drop-down menus to indicate the actions to take after the specified elapsed idle time. You can perform multiple actions, for example, to lock the desktop after 5 minutes of user idle time, then disconnect after 30 minutes of idle time.

Assigning Plans to Hard-Assigned Desktops

From the **Protocol** and **Power control** drop-down menus, select a protocol plan and power control plan to associate with hard-assigned desktops.

The Connection Broker never releases hard-assigned desktops back to their pool. Therefore, the power control action in the **When Desktop is Released** section of the power control plan is never executed.

Configuring Policy Options for Rogue Users

The **Rogue User Assignment** tab assigns power control and release plans to rogue users after they log into a desktop that is set to manage rogue users. See **Assigning Desktops to Rogue Users** for complete details.

Assigning Desktops Based on a Schedule

The **Scheduled Assignments** tab indicates how the Connection Broker manages user connections to desktops that were assigned to the user based on a calendar of events. The options in this section are identical to the related Policy options on other tabs within the Policy. Please reference **Configuring Pool Assignment Options** for information on how to use the options on the **Scheduled Assignments** tab.

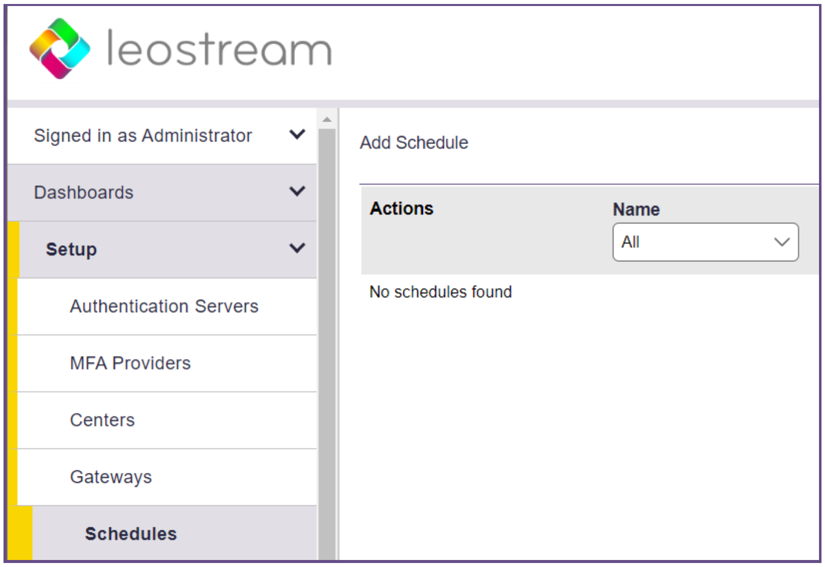
The following sections describe how to build or import a schedule that assigns desktops to users.

Assigning desktops based on schedules allows you to dedicate workstations to classrooms, projects, etc., that have a well-define roster of users who require the desktops on specific days and times. Unlike traditionally hard-assigned desktops, a desktop that is schedule-assigned automatically adjusts its assignment based on the different events associated with it.

You define schedules either as a set of events in the Connection Broker or on a calendar application that is then imported into your Connection Broker.

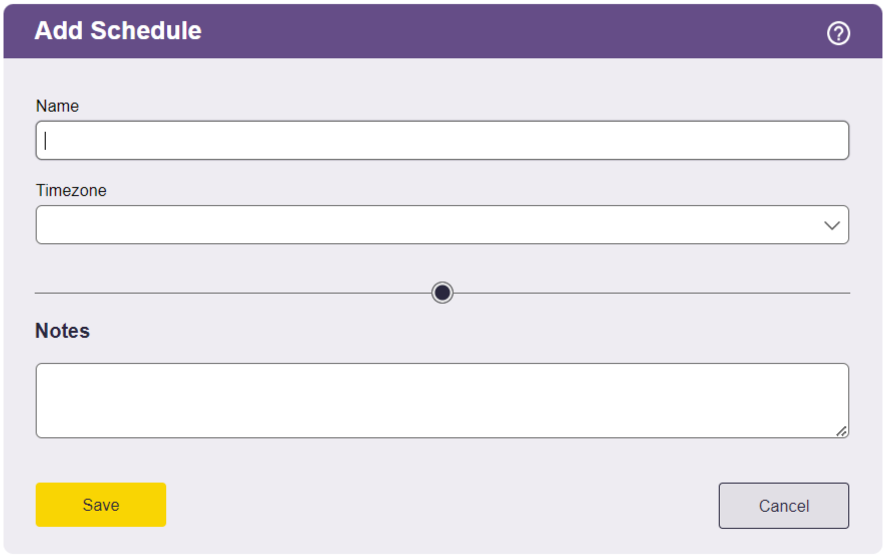
Creating a Connection Broker Schedule

To define a schedule, go to the **> Setup > Schedules** page in the Administrator web interface, shown in the following figure.



No schedules found

Click **Add Schedule** to define a new schedule. The **Add Schedule** form opens, as shown in the following figure.



1. Enter a name for the schedule in the **Name** edit field.

2. Select the time zone for the schedule from the **Timezone** drop-down menu.

3. Enter any optional notes in the **Notes** field.

4. Click **Save**.

Each schedule contains a series of events, either defined manually, imported from an ICS-file, or a combination of both, as described in the following sections.

Manually Adding Events to Schedules

Individual, static events can be added manually to a schedule by defining:

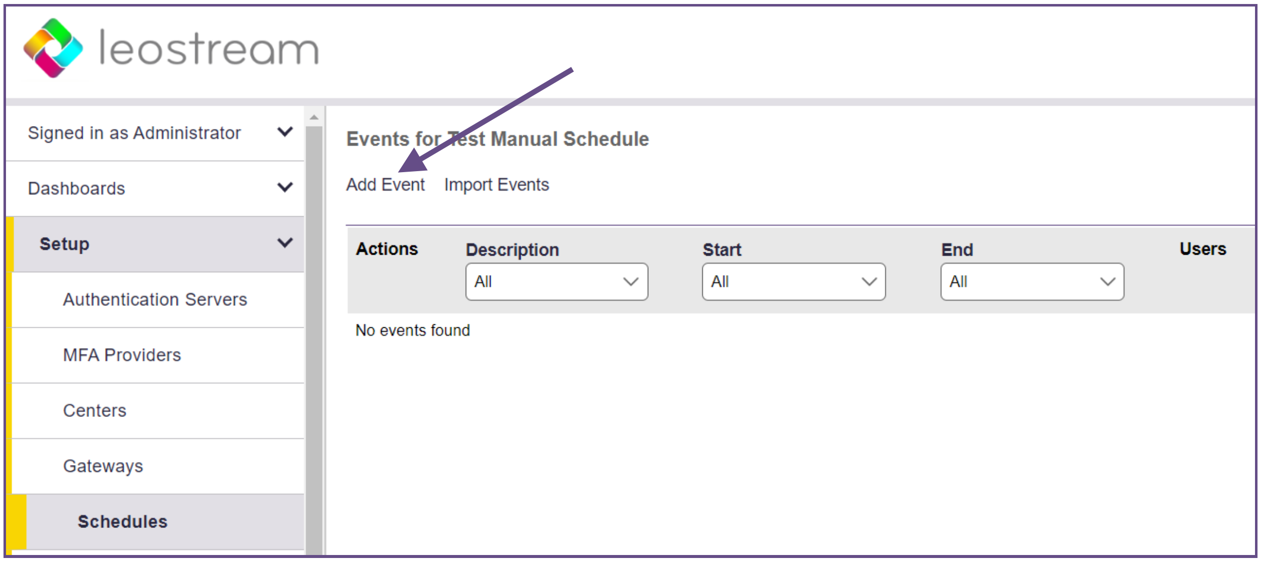
1. The calendar start date
2. A start time
3. A calendar end date
4. An end time
5. A list of usernames associated with the event

To create an event:

1. Go to the **> Setup > Schedules** page.

2. Click the **Events** link associated with the appropriate schedule.

3. Click **Add Event** at the top of the **Events** page, indicated in the following figure.



Actions	Description	Start	End	Users
	All	All	All	

No events found

4. In the **Add an event** form that opens, enter a description for the event in the **Description** edit field.

5. Click in the **Start** field to select a calendar date and time for the start of the event.

6. Click in the **End** field to select a calendar date and time for the end of the event.

7. In the **Event users** section of the form, move the user(s) associated with this event from the **Available Users** to the **Selected Users** list. Users must be loaded into the Connection Broker before they can be scheduled-assigned to a desktop.

8. Click **Save**.

Only users associated with an event will be schedule-assigned to a desktop assigned to this schedule.

Building Calendars to use with Leostream

You can import events from any file that follows the iCalendar specification, such as an ICS-file, in order to build schedules in Leostream using your corporate calendaring application. Using a calendar allows you to easily build repeating events, reserve desktops for groups of users based on project times, and inform users when they are scheduled for access.

When building a calendar to use with Leostream, keep in mind the following:

- Use a unique calendar for Leostream events to avoid unwanted meetings and events. The Connection Broker imports all events on the calendar within the date range you specify.
- Add users to each event in the external calendar before you export the calendar as an ICS-file. Users can be added as attendees for the calendar event, be listed in the title of the event, or be included in the event's description.
- Users associated with events in a calendar must have email addresses that match the email address associated with their Leostream account. These users must be listed on your Connection Broker **> Resources > Users** page prior to importing your calendar.
- If you edit an external calendar after importing it into your Connection Broker, export the calendar and re-import it into your Connection Broker to update the previous events.

Importing Events from a Calendar

⚠ Ensure that you load all users associated with your events into your Connection Broker before you import your calendar events.

To import events from a calendar:

1. Go to the **> Setup > Schedules** page.
2. Click the **Events** link associated with the appropriate schedule.
3. Click **Import Events** at the top of the **Events** page.
4. Click in the **Start** field to select a calendar date and time when you want to start importing events from the calendar.
5. Click in the **End** field to select a calendar date and time to stop importing events from the calendar.

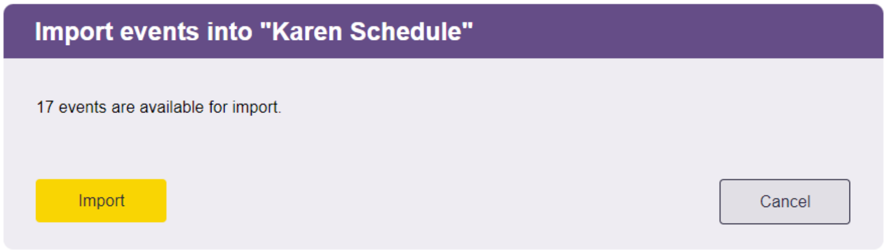
   ⚠ The Connection Broker imports events with the times as they appear on the calendar from which you downloaded the ICS-file. The time zone associated with the Schedule may shift these events if the Schedule's time zone does not match your local calendar time zone.

For example, if your ICS-file has an event scheduled at 17:00 EDT but the Schedule sets a time zone of CDT the Connection Broker interprets that event as occurring at 17:00 CDT.

6. Click **Choose File** and upload the ICS-file exported from the calendar that contains your events.

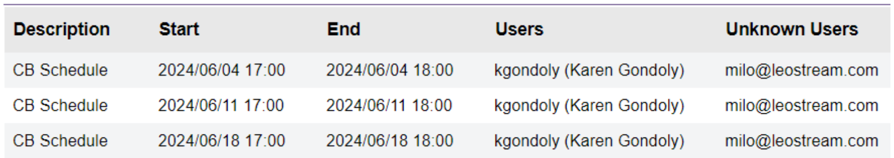
7. Click **Upload**.

8. The **Import events** dialog appears, indicating the number of events that will be imported and showing a list of events, for example:



Import events into "Karen Schedule"

17 events are available for import.



Description	Start	End	Users	Unknown Users
CB Schedule	2024/06/04 17:00	2024/06/04 18:00	kgondoly (Karen Gondoly)	milo@leostream.com
CB Schedule	2024/06/11 17:00	2024/06/11 18:00	kgondoly (Karen Gondoly)	milo@leostream.com
CB Schedule	2024/06/18 17:00	2024/06/18 18:00	kgondoly (Karen Gondoly)	milo@leostream.com

⚠ The Connection Broker assigns users to the event by matching the email addresses invited to the events in the ICS-file to the email address of users already loaded into your Leostream environment. If users are not shown for their events, you can load the users by going to the **> Setup > Authentication Servers** page. After uploading the users, step through this process to upload the ICS-file, again.

9. Click **Import** to import all events.

   The Connection Broker imports all events in the selected range. You cannot select which events to import.

   The **Event** list shows an entry for all the unique events.

If you make changes to your calendar in the calendar application, you can update the schedule in your Connection Broker, as follows.

1. Export the ICS-file from your calendar application

2. Go to the **> Setup > Schedules** page.

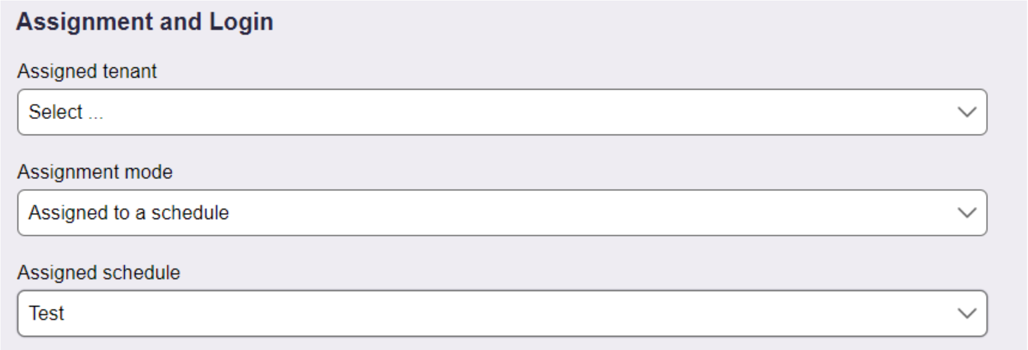
3. Click the **Events** for the Schedule you need to update.

4. Click **Import Events**

The Connection Broker updates all events associated with your Calendar. Any manually created events in this Schedule are unchanged.

Schedule-Assigning Desktops

To assign a desktop based on schedules, go to the **> Resources > Desktops** page and click the **Edit** action associated with that destkop. From the **Assignment mode** drop-down menu in the **Assignment** section of the **Edit Desktop** page, shown in the following figure, select the **Assigned to a schedule** option and then select the desired schedule from the **Assigned schedule** drop-down menu, as shown in the following figure.



Assignment and Login

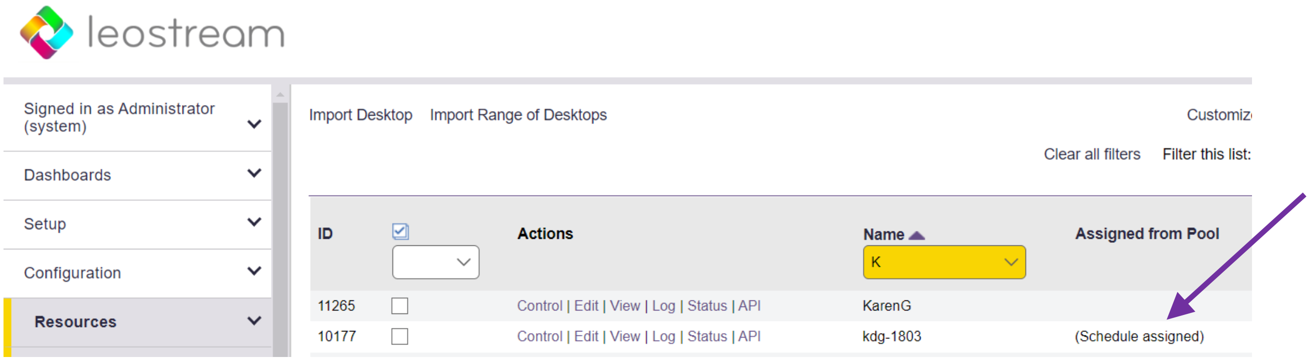
Assigned tenant: Select ...

Assignment mode: Assigned to a schedule

Assigned schedule: Test

A desktop that is assigned to a schedule is no longer considered an available desktop for pool or hard assignments. The Connection Broker offers the destkop only to users who are members of the scheduled events and only when there is an active event.

The **Assigned from Pool** column on the **> Resources > Desktops** page indicates which desktops are currently assigned to a schedule, as shown in the following figure.

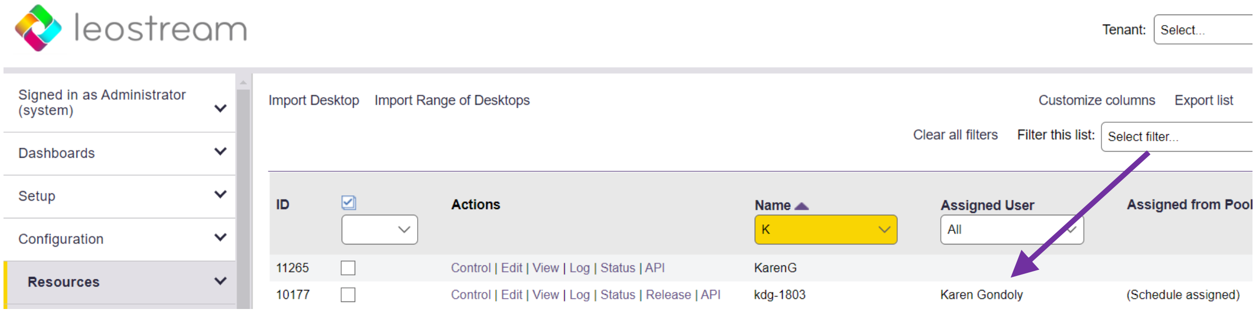


ID	☑	Actions	Name ▲	Assigned from Pool
			K	
11265	□	Control | Edit | View | Log | Status | API	KarenG	
10177	□	Control | Edit | View | Log | Status | API	kdg-1803	(Schedule assigned)

Managing Scheduled Assignments

When a user logs into Leostream, the Connection Broker looks for all scheduled events associated with that user and offers the assigned desktops. The user’s offer, connection, and session lifecycle are defined by the settings on the **Scheduled Assignments** tab of the user’s Policy.

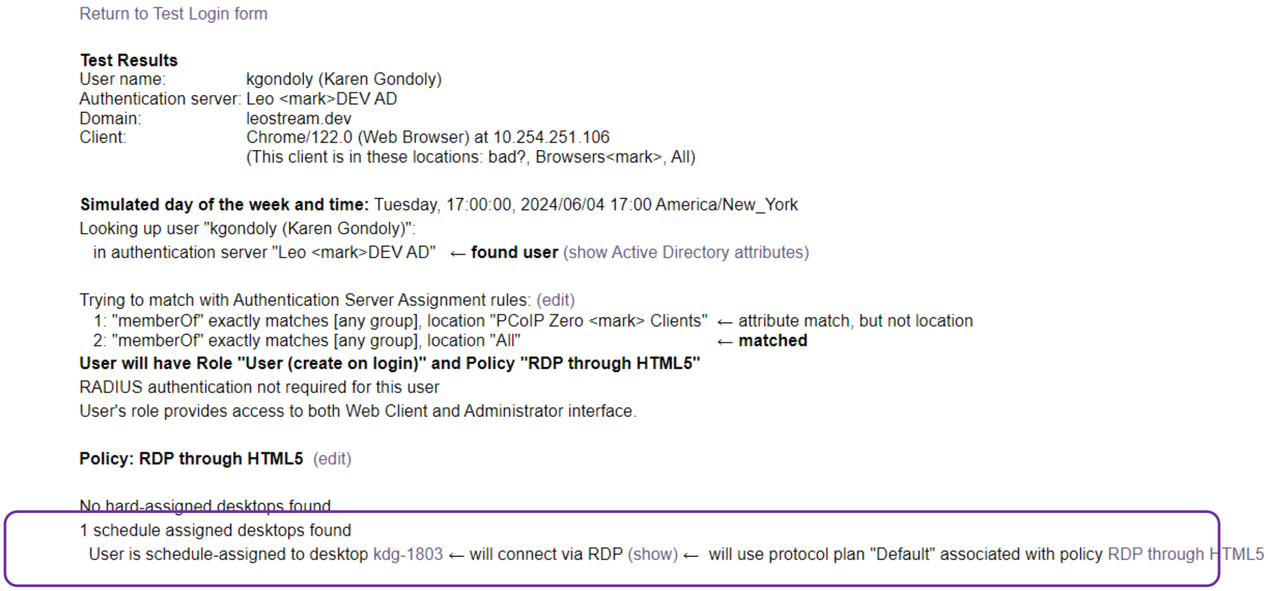
When the user requests a connection to one of their scheduled machines, the Connection Broker adds that user as the **Assigned User**, as shown in the following figure:



ID	☑	Actions	Name	Assigned User	Assigned from Pool
			K	All	
11265	□	Control | Edit | View | Log | Status | API	KarenG		
10177	□	Control | Edit | View | Log | Status | Release | API	kdg-1803	Karen Gondoly	(Schedule assigned)

Testing Scheduled Assignments

The **Test Login** page includes a new **Login date and time** field and **Time zone** drop-down menu that allow you to test if a scheduled assignment is being properly offered.



Return to Test Login form

Test Results
User name: kgondoly (Karen Gondoly)
Authentication server: Leo <mark>DEV AD
Domain: leostream.dev
Client: Chrome/122.0 (Web Browser) at 10.254.251.106
(This client is in these locations: bad?, Browsers<mark>, All)

Simulated day of the week and time: Tuesday, 17:00:00, 2024/06/04 17:00 America/New_York
Looking up user "kgondoly (Karen Gondoly)":
in authentication server "Leo <mark>DEV AD" ← **found user** (show Active Directory attributes)

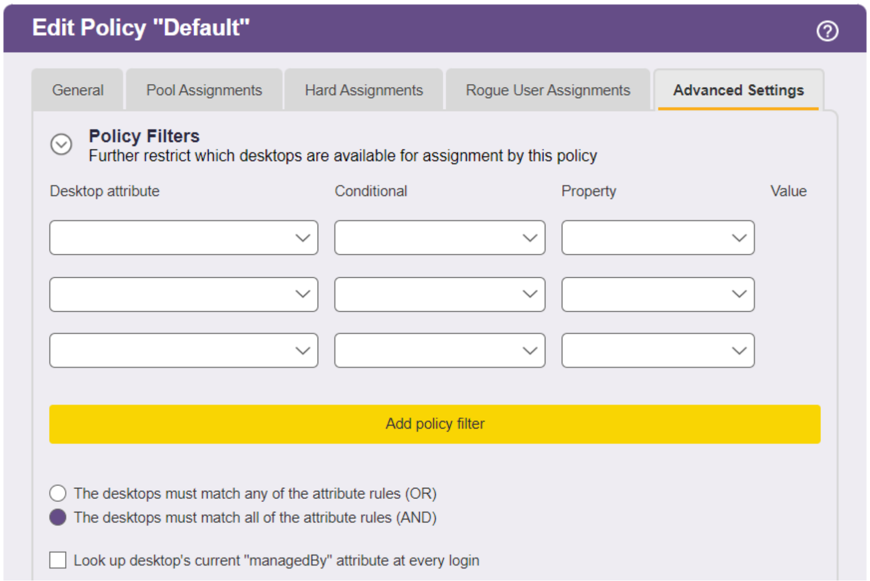
Trying to match with Authentication Server Assignment rules: (edit)
1: "memberOf" exactly matches [any group], location "PCoIP Zero <mark> Clients" ← attribute match, but not location
2: "memberOf" exactly matches [any group], location "All" ← **matched**
User will have Role "User (create on login)" and Policy "RDP through HTML5"
RADIUS authentication not required for this user
User's role provides access to both Web Client and Administrator interface.

Policy: RDP through HTML5 (edit)

No hard-assigned desktops found
1 schedule assigned desktops found
User is schedule-assigned to desktop kdg-1803 ← will connect via RDP (show) ← will use protocol plan "Default" associated with policy RDP through HTML5

Policy Filters

You can use policy filters on the **Advanced Settings** tab to narrow down the selection of desktops from all the pools associated with a policy. Policy filters allow you to restrict what type of desktops can be assigned, to the point of strictly assigning a particular desktop to a user. Set these rules in the **Policy Filters** section, shown in the following figure:



Policy Filters
Further restrict which desktops are available for assignment by this policy

○ The desktops must match any of the attribute rules (OR)
● The desktops must match all of the attribute rules (AND)

□ Look up desktop's current "managedBy" attribute at every login

Each row in the **Policy Filters** section reads as a rule that checks if a desktop in the pool can be offered by this policy. For a particular pool, the policy filter applies in addition to the pool filter. To specify a policy filter:

1. Select an item from the **Desktop attribute** drop-down menu to indicate how to filter the desktops, either:

   - Name
   - Machine name
   - vCenter Server annotation
   - Any Active Directory attribute associated with the desktop, such as `managedBy`. You must create an Active Directory center for these attributes to appear in the **Desktop attribute** drop-down menu (see **Active Directory Centers**).

2. Select a logic condition from the **Conditional** drop-down menu.

3. In the **Property** drop-down menu, indicate the type of attribute to filter against, either:

   - User Attribute
   - Client Attribute
   - Text Value

   You can use dynamic tags when filtering based on a text value. The following dynamic tags are supported.

   - `{AD:USER:`*`attribute_name`*`}`: Filters based on the value found in the user's Active Directory attribute given by *`attribute_name`*.

   - `{AD:CLIENT:`*`attribute_name`*`}`: Filters based on the value found for the attribute given by *`attribute_name`* in the client's Computer Active Directory object.

The user must authenticate with the Connection Broker using Active Directory. If this is the case, the Connection Broker uses the name of the client computer, determined as either the NetBIOS or DNS name, to search for the correct Computer object in Active Directory.

4. In the **Value** field, select or enter the actual attribute value to test against.

   ⚠ Not all clients return their MAC address. If you plan to filter pools using the client MAC address attribute, go to the **Edit Client** page for each client and ensure that they are correctly returning their MAC address.

5. Indicate if the desktop can match any rule (OR) or must match all rules (AND), in order to be available in this policy.

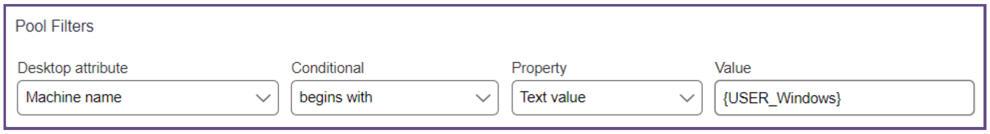
6. Select the **Look up desktop's current "managedBy" attribute at every login** option if the value of the desktop's `managedBy` field frequently changes. If this option is *not* selected, the Connection Broker caches the `managedBy` attribute obtained when the center was last refreshed, improving performance at login time. This setting also applies to filters in all **Pool Filters** sections.

📝 Policy filters apply to *all* pools in the policy. Use pool filters if you want to filter desktops from a single pool (see **Using Pool Filters to Limit Available Desktops in the Pool**).

Using Dynamic Tags in Policy Filters

When creating filters based on text values, you can use dynamic tags to specify all or part of the text. The Connection Broker evaluates dynamic tags when determining which desktops to offer from the pools.

For example, in the following figure, the filter uses the `{USER}` dynamic tag, to reference the login name of the user who logged into the Connection Broker. When determining which desktops to offer this user, the Connection Broker filters the contents of the pool by looking for desktops whose Windows machine name begins with the user's login name appended with `_Windows`.



Pool Filters

Desktop attribute: Machine name

Conditional: begins with

Property: Text value

Value: {USER_Windows}

Because the Connection Broker evaluates dynamic tags before offering desktops to the user, certain dynamic tags are not available as filters. The Connection Broker supports the following dynamic tags in policy filters. All dynamic tags listed together resolve to the same value. See **Using Dynamic Tags** for a complete description of these dynamic tags.

- `{NAME}`, `{USER:NAME}`
- `{USER}`, `{USER:USER}`, `{USER:LOGIN_NAME}`, `{LOGIN_NAME}`
- `{FQDN}`
- `{DOMAIN}`
- `{AUTH_DOMAIN}`
- `{AD_DN}`, `{USER:AD_DN}`
- `{EMAIL}`, `{USER:EMAIL}`

- {PRE_EMAIL},{USER:PRE_EMAIL}
- {POST_EMAIL},{USER:POST_EMAIL}
- {CLIENT},{CLIENT:NAME}
- {CLIENT:IP}
- {CLIENT:MAC}
- {CLIENT:TYPE},{CLIENT:CLIENT_TYPE}
- {CLIENT:MANUFACTURER}
- {CLIENT:UUID}

Using VMware Custom Attributes in Filters

The Connection Broker allows you to filter the desktops in a pool or policy based on the value of up to four vCenter Server custom attributes. Go to the **> System > Settings** page to indicate which custom attributes you want to use as filters. See **Specifying VMware vCenter Server Clusters for Desktop Filters** for complete instructions on indicating the custom attributes to use as desktop filters.

Custom attributes appear at the bottom of the **Desktop attributes** drop-down menu in the filters. Each custom attribute is labelled as:

```
vCenter Server "attribute_name"
```

where *attribute_name* is the name of the custom attribute. If the same custom attribute appears in multiple vCenter Servers, the attribute appears once in the drop-down menu. When using this attribute as a filter, the Connection Broker looks at all VMs from all vCenter Servers that contain this attribute. The `vCenter Server "Notes"` attribute is always available for use as a filter.

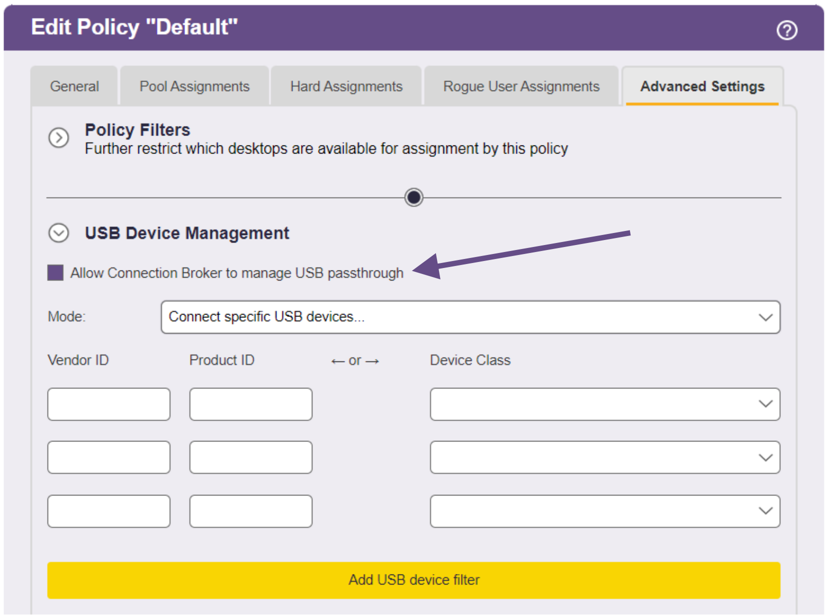
Configuring USB Device Management

Policy settings for USB device management apply to all offered desktops from a particular policy. Users must log into Leostream using either Leostream Connect to utilize the Leostream USB device passthrough feature. Also, you must install the Leostream Agent on the remote desktop. When installing the Leostream Agent and Leostream Connect client, ensure that the **Enable USB over IP** option is selected.

⚠ Your Leostream license controls if the **USB Device Management** section appear in your **Edit Policy** form. If you need to enable USB device control, please contact **sales@leostream.com** to update your license.

The **USB Device Management** section is located on the **Advanced Settings** tab of the **Edit Policy** page. These controls allow you to specify which USB devices end users can redirect to their remote desktops. By default, policies do not provide USB device management.

To enable USB device management in a policy, select the **Allow Connection Broker to manage USB passthrough** option, as shown in the following figure.



Use the **Mode** drop-down menu to specify which USB devices end users can assign to desktops, as follows:

- **To pass through all USB devices to the desktop**: Select **Connect all USB devices** from the **Mode** drop-down menu.

- **To block all USB devices from being passed through to the desktop**: Select **Block all USB devices** from the **Mode** drop-down menu.

- **To specify particular devices to passthrough**: Select **Connect specific USB devices** from the **Mode** drop-down menu. Configure the devices to passthrough, as follows:

  - Select an item from the **Device Class** drop-down menu to pass through an entire class of devices, or

  - Enter a **Vendor ID** and **Product ID** to pass through a specify type of device.

Leostream Connect allows end users to attach and detach their offered USB devices from their remote desktops. See the **Leostream Connect Administrator's Guide and End User's Manual** for instructions on working with USB passthrough support. Leostream Connect does not control how the device or any associated applications run or perform on the remote desktop. You must manually install any drivers required by a particular device.

Testing Policies

To test if your policies are correctly offering desktops from pools:

1. Create and configure an authentication server in your Connection Broker and edit that authentication server's assignments table so it uses this policy (see **Chapter 14: Assigning User Roles and Policies**).

2. Use the **Test Login** link on the **> Resources > Users** page to simulate a user login. The Connection Broker presents a report, indicating if the user was matched to a role and policy rule in the authentication server, and what desktops were selected based on the policy. See **Testing User Role and Policy Assignment** for more details.

Sending HTTP GET Requests

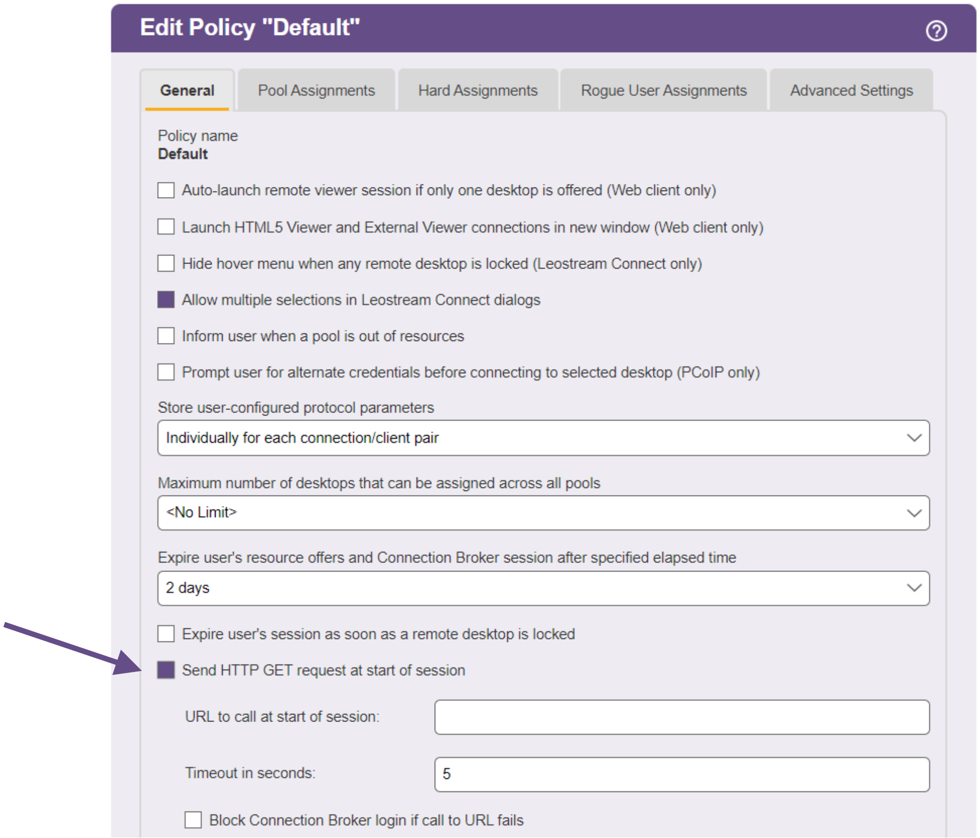
The Connection Broker can send an HTTP GET request at the following times during the user’s session:

- As soon as the user logs into the Connection Broker
- When the user is assigned to a desktop
- When the user disconnects form a desktop
- When the user logs out of a desktop

Using HTTP GET requests, you can perform additional configuration actions necessary for your environment. Use Connection Broker policies and release plans to call your URL.

Defining Custom Actions at Login

To send an HTTP GET request as soon as the user logs into the Connection Broker, select the **Send HTTP GET request at start of session** option, shown in the following figure.



Edit Policy "Default"

Policy name
Default

☐ 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)

Store user-configured protocol parameters: Individually for each connection/client pair

Maximum number of desktops that can be assigned across all pools: <No Limit>

Expire user's resource offers and Connection Broker session after specified elapsed time: 2 days

☐ Expire user's session as soon as a remote desktop is locked

☑ Send HTTP GET request at start of session

URL to call at start of session:

Timeout in seconds: 5

☐ Block Connection Broker login if call to URL fails

The **URL to call at the start of session** can contain a limited number of Connection Broker dynamic tags, which the Connection Broker replaces before calling the URL. Dynamic tags, such as `{IP}`, cannot be used in this URL as the Connection Broker does not have a value to assign to this tag at the time the session starts. If you include an invalid dynamic tag in the URL, the Connection Broker leaves the literal string for the dynamic tag in the URL. For a full list of dynamic tags, see **Using Dynamic Tags**.

Use the **Timeout in seconds** field to indicate how long the HTTP GET request has to return a result.

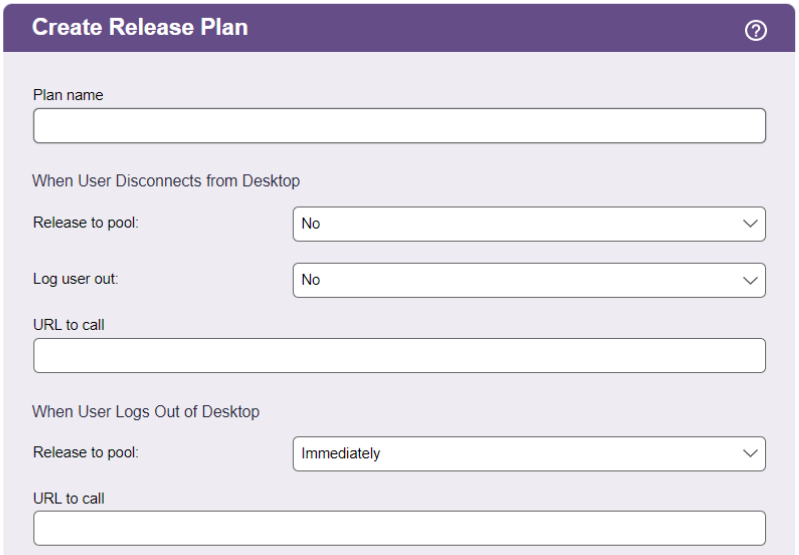
Select the **Block Connection Broker login if call to URL fails** option if the user should not be able to complete their Leostream login if the URL returns a failure. When selected, the **Message to user on failed call** edit field allows you to enter a message to display to the user if their login is blocked.

Defining Custom Actions on Log Out and Disconnect

You use either policies or release plans to send HTTP GET requests when the user logs out or disconnects from one of their desktops, depending on how the user was assigned to the desktop.

- For policy-assigned desktops, specify the URL in the release plan
- For hard-assigned desktops, specify the URL in the **Hard Assignments** tab of the policy

In either case, use the **URL to call** edit fields associated with the **When User Disconnects from Desktop** and **When User Logs Out of Desktop** sections, shown in release plans in the following figure, to specify the URL to call at each time.



Create Release Plan

Plan name

When User Disconnects from Desktop

Release to pool: No

Log user out: No

URL to call

When User Logs Out of Desktop

Release to pool: Immediately

URL to call

Example HTTP GET Request

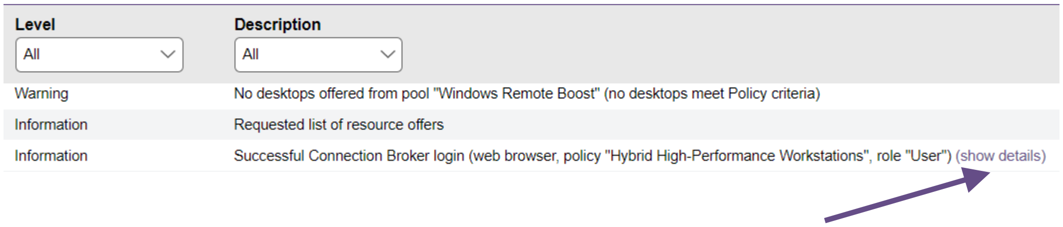
The Connection Broker provides a simple URL that returns the Connection Broker status. This URL takes the following form:

```
https://cb-address/index.pl?action=cb_status
```

Where *cb-address* is your Connection Broker IP address or hostname. As an example, enter this into the

URL to call at start of session edit field of a policy.

When a user logs into the Connection Broker and is assigned this policy, the Connection Broker calls the specified URL and registers the results in the Connection Broker logs. To view the results, click the **show details** link for the line on the **> System > Logs** page that logs the user's Connection Broker login, as shown in the following figure.



Level All	Description All
Warning	No desktops offered from pool "Windows Remote Boost" (no desktops meet Policy criteria)
Information	Requested list of resource offers
Information	Successful Connection Broker login (web browser, policy "Hybrid High-Performance Workstations", role "User") (show details)

Chapter 13: Configuring User Experience by Client Location

Overview

When a user logs into the Connection Broker from a client device, the Connection Broker registers that client device on the **> Resources > Clients** page. The Connection Broker also assigns that client to one or more locations. A *client location* is similar to a desktop pool, in that the location represents a group of clients with similar attributes.

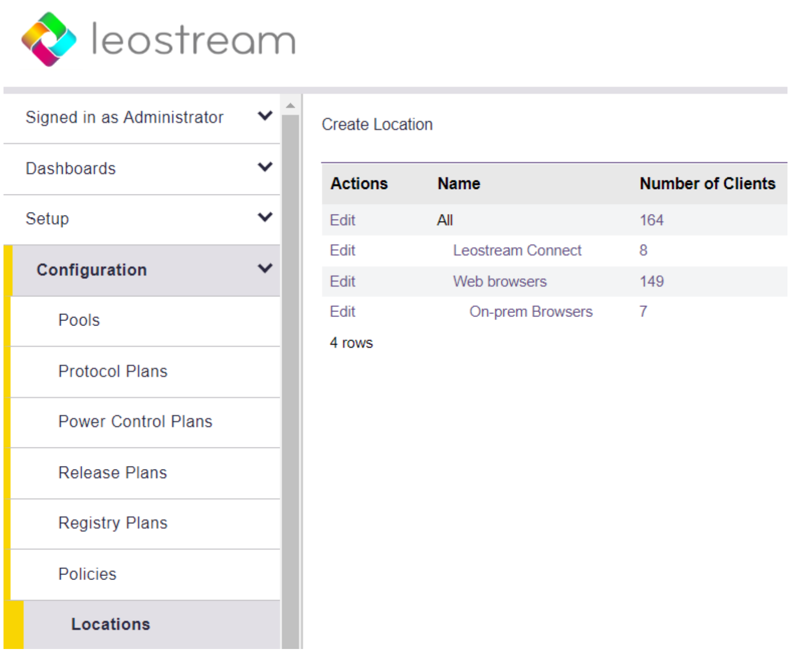
Creating Locations

You can group clients into *locations* using reported client attributes such as manufacturer, device type, OS version, or IP address. Similar to desktop pools, client locations can be nested.

Locations allow you to tailor the end-user experience based on where the user logs in, including:

- Assign different roles and policies to users. The roles and policies, in turn, determine which desktops are offered to different users. See **Assigning Users to a Role and Policy** for information on setting up role and policy rules.
- Override the protocol plan assigned in the policy. The protocol plan determines which display protocol will be used to connect to the desktop when the user logs into the Connection Broker from this location.
- Assign printers to the user’s remote desktop.
- Modify registry keys on the user’s remote desktop.
- Monitor and control access based on which Leostream Gateway a user connects through.

Locations are listed on the **> Configuration > Locations** page, shown in the following figure.



Actions	Name	Number of Clients
Edit	All	164
Edit	Leostream Connect	8
Edit	Web browsers	149
Edit	On-prem Browsers	7

4 rows

You define locations using a series of logic rules based on client attributes. To define a location:

1. On the **> Configuration > Locations** page click **Create Location**.

2. Enter a name for the location in the **Name** edit field.

   ⚠ If you are using the Leostream feature to allow one user to manage another user’s resources, do not set the location names longer than 80 characters. Leostream Connect truncates the name in the dialog for managing another user’s resources.

3. From the **Subset of location** drop-down menu, select the parent location. Only clients that are part of the parent location are eligible to exist in this new location.

4. Use the **Attribute Selection** section to define which clients reside in this location.

   a. Select an attribute from the **Client attribute** drop-down menu.

   b. Select a logic condition from the **Conditional** drop-down menu.

   c. Enter or select the appropriate **Value** for this rule.

5. Indicate if the client can match any rule (OR) or must match all rules (AND), to be in this location.

6. Configure the **Plans** section, if applicable (see **Assigning Plans to Locations**).

7. Click **Save**.

To edit existing locations, select the **Edit** action for the appropriate location.

Using Subnet Masks (CIDR) to Create Locations

You can use subnet maps to create a location containing all clients on a particular subnet or with an HTTP X-Forwarded-For header containing an IP address in a particular subnet. To do so, in the **Attribute Selection** section:

1. From the **Client attribute** drop-down menu, select **IP address** or **HTTP X-Forwarded-For header**.

2. From the **Conditional** drop-down menu, select **matches (CIDR notation)**.

3. In the **Value** edit field, enter the subnet for this location, specified using the network prefix notation (`/n`) for the subnet mask. For example:

   `10.153.174.0/24` creates a location of all clients in the range of 10.153.174.0 to 10.153.174.255
   `10.153.174.0/25` creates a location of all clients in the range of 10.153.174.0 to 10.153.174.127
   `10.153.0.0/16` creates a location of all clients with an IP address of 10.153.*x.x*

   ⚠ Ensure that you enter a valid CIDR notation when using the **matches (CIDR notation)** conditional. If you do not want to specify the IP address range using the network prefix notation, use the **begins with** conditional, instead of **matches (CIDR notation)**.

When using the `/n` notation, the `n` is a count of the number of ones in the binary representation of the subnet mask, for example:

255.255.255.128 = `/25`
255.255.255.192 = `/26`
`etc...`

When defining the location based on the X-Forwarded-For header, the Connection Broker checks all IPv4 IP addresses in the header to see if there is a match.

Creating Locations based on Leostream Gateways

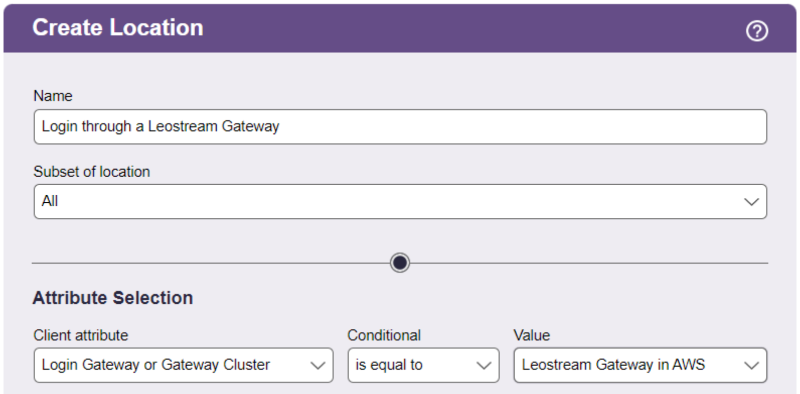
If you configured your Leostream Gateways to forward login traffic to your Connection Broker, you can define locations based on the gateway or gateway cluster that forwarded the login. This allows you to control end-user access based on if the user logs in on-premises or offsite through a Leostream Gateway.

To create a location based on Leostream Gateways, in the **Attribute Selection** section:

1. Select **Login Gateway or Gateway Cluster** from the **Client attribute** drop-down menu.

2. Select **is equal to** or **is not equal to**, depending of if you want this location to be all clients logging in through a particular gateway or all clients logging in without going through a particular gateway.

3. Select the Leostream Gateway or Gateway Cluster from the **Value** drop-down menu, for example:



Create Location

Name: Login through a Leostream Gateway

Subset of location: All

Attribute Selection

Client attribute	Conditional	Value
Login Gateway or Gateway Cluster	is equal to	Leostream Gateway in AWS

You can then use the **Assignments** table associated with your authentication servers to change the user's role and policy based on the gateway that forwarded their login.

Attaching Network Printers

⚠ Your Leostream license controls if the feature for managing network printers appear in your Connection Broker. If you need to enable printer management, please contact **sales@leostream.com** to update your license.

When using the Windows version of Leostream Connect, Microsoft RDP provides native printer redirection. To redirect all client printers, include the following line in the RDP configuration file found in the user's protocol plan.

```
redirectprinters:i:1
```

For cases that do not use RDP or do not use RDP to redirect printers, the Connection Broker allows you to attach network printers to remote desktops based on the location of the user's client device. End-users can then access these printers from their remote desktops.

Using this *location-based printing* feature, you can:

- Register printers in Microsoft® Active Directory® servers with the Connection Broker
- Manually register a network printer with the Connection Broker
- Create printer plans, consisting of a group of printers with one default printer
- Assign printer plans to clients using locations defined in the Connection Broker
- Provide end-users with access to the network printers physically closest to their client device, no matter what type of client device and display protocol they are using

How it Works

The Connection Broker determines which printers to attach to a remote desktop based on the location of the user's client. To configure your Connection Broker, perform the following steps.

1. Register network printers with your Connection Broker, either manually (see **Adding Individual Printers**) or using Active Directory servers (see **Adding Printers from Microsoft Active Directory Servers**)

2. Group printers into printer plans, and assign a default printer to each plan (see **Creating Printer Plans**)

3. Create client locations (see **Creating Locations**)

4. Assign a printer plan to a particular client (see **Assigning Plans to Clients**) or client location (see **Assigning Plans to Locations**)

When a user logs in at a particular client, the Connection Broker does the following.

1. When the user logs into the Connection Broker, the Connection Broker finds the printer plans assigned to all the locations associated with their client device. If the client falls into multiple locations, the Connection Broker uses the printers included in all associated plans.

2. When the user logs into their desktop, the Connection Broker disconnects all network printers already attached to that desktop. Any local printers remain attached.

   ⚠ If using the Connection Broker location-based printer feature, do not manually attach any network printers to remote desktops that are connected to by clients managed by the Connection Broker. These attachments are lost when a user logs in from a client associated with a Connection Broker printer plan.

3. The Connection Broker attaches all appropriate printers and sets the default printer. If no default printer is selected in the printer plan, the Connection Broker leaves the currently selected default printer on the desktop.

📝 The Connection Broker detaches the printers in the printer plan when the user logs out or disconnects from the remote desktop. Any printers that were attached to the desktop before the printer plan was applied remain attached to the desktop after the user logs out or disconnects.

System Requirements

In order for the Connection Broker to successfully attach a network printer to a remote desktop, all of the following requirements must be met.

- The Leostream Agent must be installed and running on the remote desktop, and reachable by the Connection Broker.

- The network printers must be shared and DNS accessible. You cannot currently specify the printer by IP address.

- The network printer must have a fully qualified printer name (UNC name).

- The user and printer do not need to be in the same domain. However, the domain of the printer must give the user privileges to access the printer.

- If the printer drivers are not installed on the remote desktops, you must have a shared printer driver folder. By default, when you share a printer, a shared folder is automatically created. Do not manually change the permissions or delete this shared folder.

- If the printer drivers are not installed on the remote desktop, the domain user on the remote desktop must have permissions to install drivers, as determined by the security policies applicable to this user on the desktop.

- The domain user on the remote desktop must have access to the printers.

Registering Printers with the Connection Broker

The **> Resources > Printers** page lists all the printers currently available for assignment by your Connection Broker. You can add printers to this list in two ways.

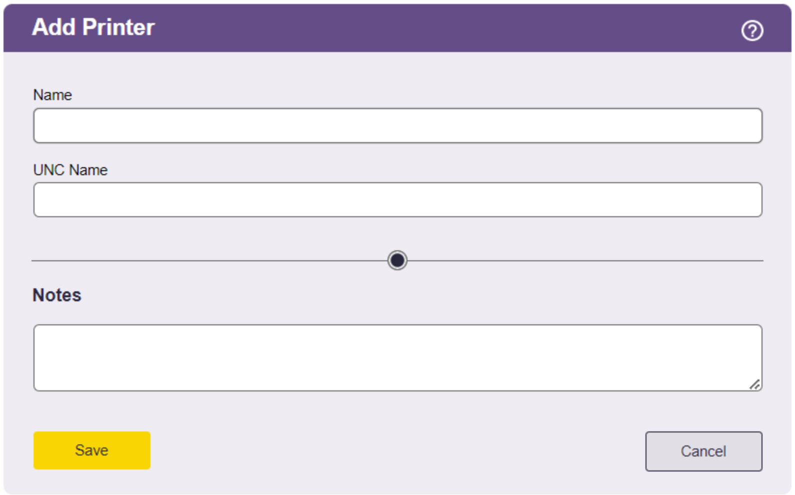
- Create a **Printer Repository** center to register printers from Active Directory services
- Add individual network printers by entering the printers UNC name

Adding Individual Printers

In addition to scanning Active Directory servers for all available printers, you can manually specify individual network printers to include in the **> Resources > Printers** page, as follows.

1. Go to the **> Resources > Printers** page.

2. Click **Add Printer**. The **Add Printer** form, shown below, opens.



3. Enter a display name for the printer into the **Name** edit field. This is the name the user will see in their printers list on the remote desktop.

4. Enter the printer's full UNC (Universal Naming Convention) name in the **UNC Name** field. This name has the following format.

```
\\server\printer
```

The UNC name must be unique. The Connection Broker will not save the form if it has already registered a printer with the same UNC name.

5. Enter any optional information to store with this printer in the **Notes** edit field.

6. Click **Save**.

After you click **Save**, the Connection Broker adds the printer to the **> Resources > Printers** page. Also, if you did not previously create a **Printer Repository** Center, the Connection Broker automatically creates this center.

Adding Printers from Microsoft Active Directory Servers

Create a **Printer Repository** center to indicate to the Connection Broker which Active Directory servers to scan for printers.

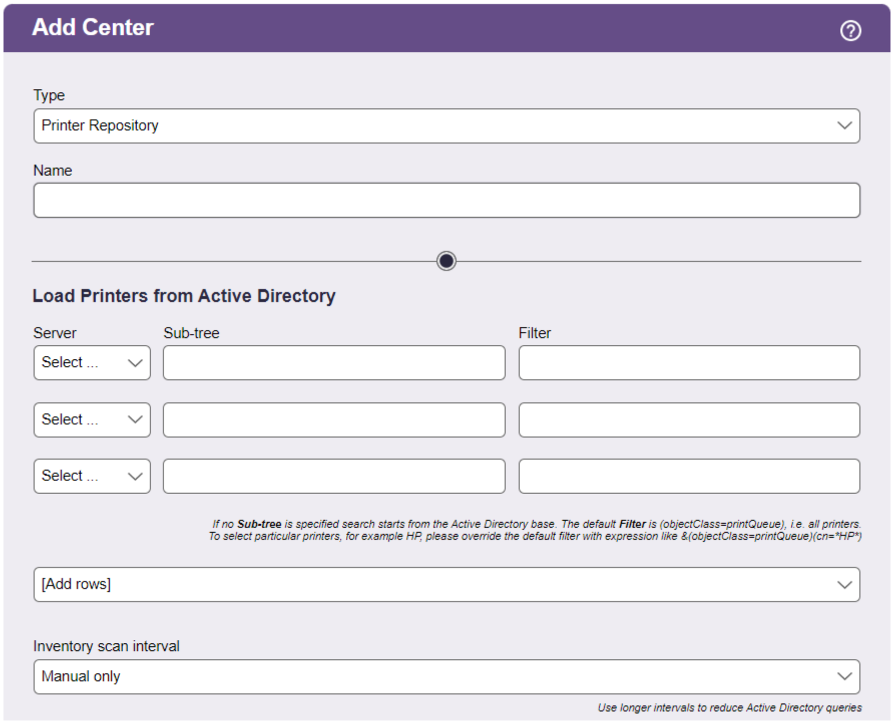
⚠ You must add an Active Directory authentication server on the **> Setup > Authentication Servers** page before you can add printers from that Active Directory server. If you have not yet defined your authentication servers, complete the steps in **Adding Microsoft® Active Directory® Authentication Servers** before proceeding with this section.)

To create a **Printer Repository** center:

1. Go to the **> Setup > Centers** page.

2. Click **Add Center**. The **Create Center** form opens.

3. Select **Printer Repository** from the **Type** drop-down menu. The form updates, as shown in the following figure.



Add Center

Type: Printer Repository

Name:

Load Printers from Active Directory

Server	Sub-tree	Filter
Select ...		
Select ...		
Select ...		

*If no **Sub-tree** is specified search starts from the Active Directory base. The default **Filter** is (objectClass=printQueue), i.e. all printers.*
*To select particular printers, for example HP, please override the default filter with expression like &(objectClass=printQueue)(cn=*HP*)*

[Add rows]

Inventory scan interval: Manual only

Use longer intervals to reduce Active Directory queries

4. Enter a name for the center into the **Name** field.

5. In the **Load Printers from Active Directory** section:

   a. From the **Server** drop-down menu, select the Active Directory authentication server to scan for printers. The drop-down menu contains only authentication servers already defined in the **> Setup > Authentication Servers** page.

   b. In the **Sub-tree** edit field, enter the top of the search path to scan for printers. If you leave this field blank, the Connection Broker uses the sub-tree specified for this authentication server on the **> Setup > Authentication Servers** page.

   c. In the **Filter** edit field, enter an optional filter string to limit the type of printers to include in the **> Resources > Printers** page. The default filter is:

      ```
      (objectclass=printQueue)
      ```

      You can append additional filters to this string, for example:

      ```
      (objectclass=printQueue)(cn=*HP*)
      ```

      The Connection Broker only filters based on the printer’s `distinguishedName` value.

6. In the **Refresh interval** drop-down menu, select how often the Connection Broker should refresh the printer list obtained from the Active Directory servers in this center. If you do not regularly add or remove printers, select **Manual only**, to reduce the number of Active Directory queries.

If you select **Manual only**, use the **Refresh** action associated with the **Printer Repository** center to rescan the Active Directory server for printers.

7. Click **Save**.

After you click **Save**, the Connection Broker scans the included Active Directory servers for printers and lists these printers on the **> Resources > Printers** page. If the Connection Broker finds multiple printers with the same UNC Name, it includes only one of the printers in the list. In addition, if you manually added a printer to the list, and that printer has the same UNC name as a printer in the Active Directory tree, the Connection Broker overwrites the manually added printer with the information from the Active Directory entry.

⚠ If you delete the Printer Repository center after you create printer plans, the Connection Broker removes all printers from the plans. When an empty printer plan is assigned to a location, users logging in from clients in those locations will not see any network printers.

Viewing Available Printers

The Connection Broker displays all registered printers, and their characteristics, on the **> Resources > Printers** page. This list is empty until you manually add a printer or define a **Printer Repository** center.

You can modify the order and type of characteristics displayed on this page by clicking the **Customize columns** link at the top-right side of the page (see **Customizing Tables**). The following sections describe the available printer characteristics.

Action
Drop-down menu or list of links indicating the actions you can perform on a particular printer. Available actions include the following:

- **Edit**: Opens the **Edit Printer** dialog

- **Delete**: Deletes this printer from the list. If you delete a printer that was manually added to the list, selecting this action permanently deletes the printer from the Connection Broker. If you delete a printer that was added via the **Printer Repository** center, the printer may reappear in the list the next time the Connection Broker refreshes the center.

Name
The printer name, as it will be displayed to users when they connect to their remote desktops.

Share Name
The printer's share name, as reported by Active Directory. This field is blank for manually added printers.

UNC Name
The printer's UNC name. The Connection Broker requires a unique UNC name for all printers.

AD distinguishedName
The printer's distinguishedName, as reported by Active Directory. This field is blank for manually added printers.

URL

The URL that can be called to reach this printer, as reported by Active Directory. This field is blank for manually added printers.

Port

The port used to communicate with this printer, as reported by Active Directory. This field is blank for manually added printers.

Printer Source

Indicates if this printer was manually added to the Connection Broker or added from the **Printer Repository** center.

Color

Indicates if Active Directory reported this printer as a color printer (Yes) or black-and-white printer (No). This field always displays No for manually added printers.

Duplex

Indicates if Active Directory reported that this printer supports duplex mode (Yes) or not (No). This field always displays No for manually added printers.

Collate

Indicates if Active Directory reported that this printer supports collation (Yes) or not (No). This field always displays No for manually added printers.

Staple

Indicates if Active Directory reported that this printer can staple (Yes) or not (No). This field always displays No for manually added printers.

Printer Server

Indicates the printer server that shares this printer.

Plan

Indicates all the printer plans that reference this printer.

UUID

The printer's unique identifier.

Identifying Duplicate Printers

The Connection Broker identifies duplicate entries for the same printer using the printer's UNC name. Duplicates may occur if a printer is listed multiple times in Active Directory, or if you manually entered a printer that is also registered in Active Directory. If you have duplicates that were manually added, you can delete them by selecting the **Delete** action associated with the printer.

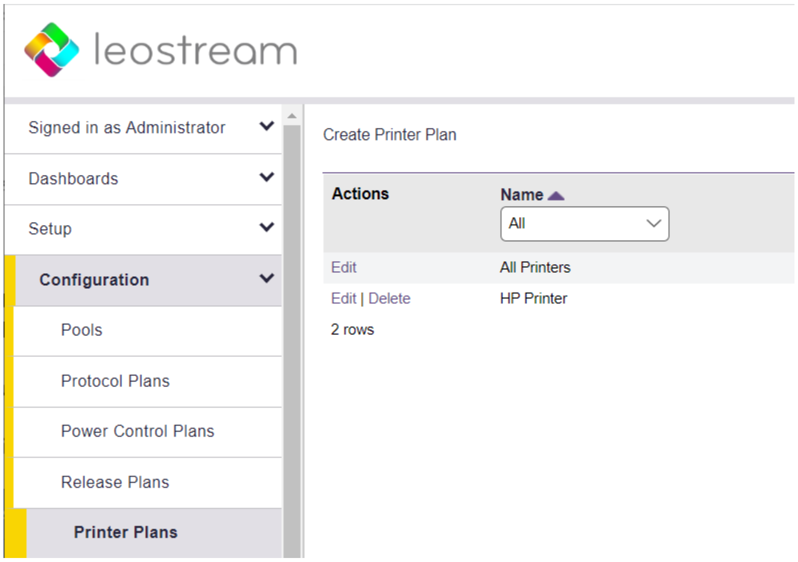
Creating Printer Plans

Connection Broker *printer plans* allow you to create groups of printers, and indicate which printer is the default. You assign these plans to client based on the client's locations.

The Connection Broker provides a default printer plan called **All Printers**. When a user logs into a client that is assigned to this default printer plan, the Connection Broker first detaches any existing network printers attached to the remote desktop, then attaches all printers listed in the **> Resources > Printers** page.

You cannot edit the default printer plan. However, you can create additional printer plans, as follows.

1. Go to the **> Configuration > Printer Plans** page, shown in the following figure.



Actions	Name
	All
Edit	All Printers
Edit | Delete	HP Printer

2 rows

2. Click **Create Plan**. The **Create Printer Plan** form opens.

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

4. In the **Select Printers in Plan** section, highlight the printers you want to include in this plan in the **Available Items** list, and click the **Add item** to the right of the list.

5. Select the default printer for this plan from the **Default printer** drop-down menu.

   If you do not define a default printer in the Connection Broker, the Leostream Agent on the remote desktop does not change the currently selected default printer on the desktop.

6. Enter any optional information you want to store with this plan into the **Notes** edit field.

7. Click **Save**.

After creating your printer plans, assign them to clients based on the client's location (see **Assigning Plans to Locations**).

When you edit a printer plan, text to the right of the form indicates all locations that use this plan. You cannot delete a printer plan when it is in use in any location.

📝 If a user logs in from a client device that is assigned a printer plan *and* the user’s protocol plan is configured to redirect the client printers, the remote desktop has access to the printers from the printer plan *and* from the client device.

Manipulating Registry Keys

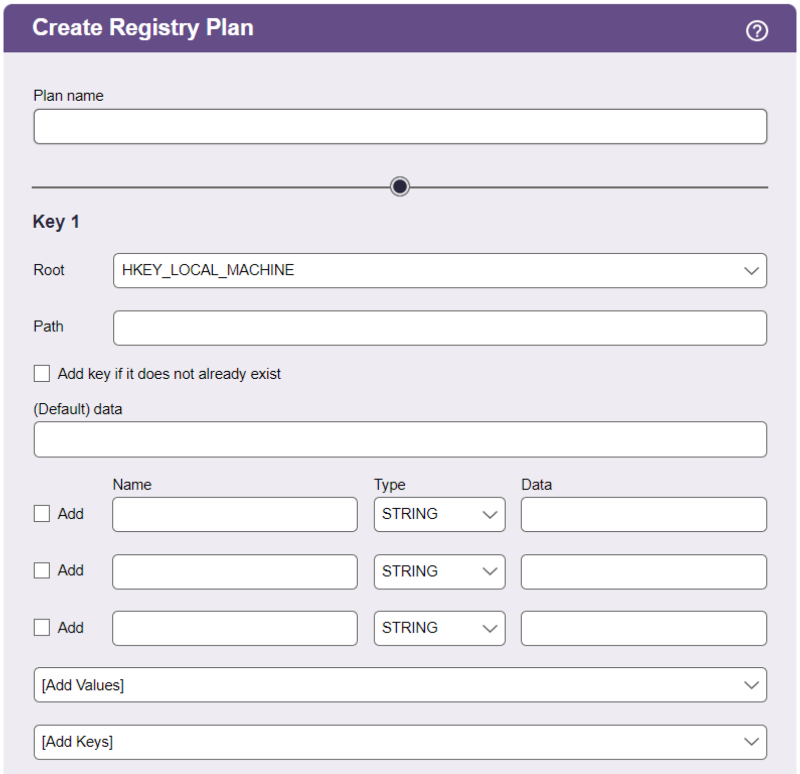
⚠ Your Leostream license controls if the feature for manipulating registry keys appear in your Connection Broker. If you need to enable this feature, please contact **sales@leostream.com** to update your license.

Registry plans specify a set of local machine Windows registry keys to create or modify on the remote desktop. The Connection Broker applies a registry plan to the remote desktop based on a client’s location. Use registry plans when registry keys on the remote desktop need to be modified based on the user’s client device

📝 Registry plans currently apply only when the user logs in using Leostream Connect.

⚠ Registry plans are an advanced Connection Broker feature. Aside from casting the data type correctly, the Connection Broker does not perform any validation or error checking on the values you assign to registry keys. Proceed with caution, as incorrectly setting certain registry keys on a desktop can have adverse effects.

The Connection Broker does not provide any default registry plan. To create a registry plan, go to the **> Configuration > Registry Plans** page and click the **Create Registry Plan** link. The **Create Registry Plan** form, shown in the following figure, opens. The next section describes how to use this form.



Create Registry Plan

Plan name

Key 1

Root: HKEY_LOCAL_MACHINE

Path

□ Add key if it does not already exist

(Default) data

	Name	Type	Data
□ Add		STRING	
□ Add		STRING	
□ Add		STRING	

[Add Values]

[Add Keys]

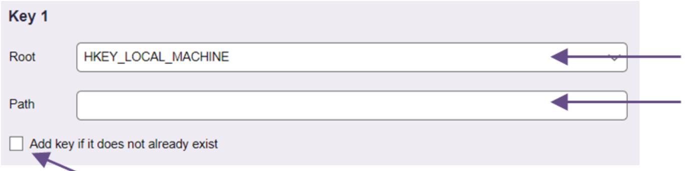
Creating Registry Plans

To create a registry plan using the **Create Registry Form**:

1. In the **Plan name** edit field, enter a name for this plan. You will use this name to assign the plan to a client or location.

2. In the **Root** edit field for **Key 1**, shown in the following figure, select the root key. If this registry plan modifies registry keys on a remote desktop running a 32-bit Windows operating system, the two root options have identical results. If the remote desktop is running a 64-bit operating system, the two options are as follows:

   HKEY_LOCAL_MACHINE: Modifies the key associated with the native 64-bit operating system
   HKEY_LOCAL_MACHINE - 32-bit: Modifies the key associated with 32-bit applications.



Key 1

Root: HKEY_LOCAL_MACHINE

Path

□ Add key if it does not already exist

Select the root for this key. Currently, the Connection Broker supports only local machine keys.

Enter the full path to the key, excluding the root. For example: SOFTWARE\Leostream\LeostreamConnect

Select this option if the Connection Broker should create this key. If this option is selected and the key already exists, the Connection Broker modifies the values in the key. If the key does not exist, and this option is *not* selected, the Connection Broker will not create any values associated with this key.

3. In the **Path** edit field, enter the full path to the key, excluding the root.

4. If the key entered in the **Path** edit was not previously created on the remote desktop, select the **Add key if it does not already exist** option.

5. In the **(Default) data** edit field, enter the value you want to assign to the default value for this key. The default value always has a string data type. Leave this field blank if you do not want to change the existing default value. See **Using Dynamic Tags in Registry Plans** for information on how to use dynamic tags to configure the default value.

6. For each row in the table, shown in the following figure, enter the following information:

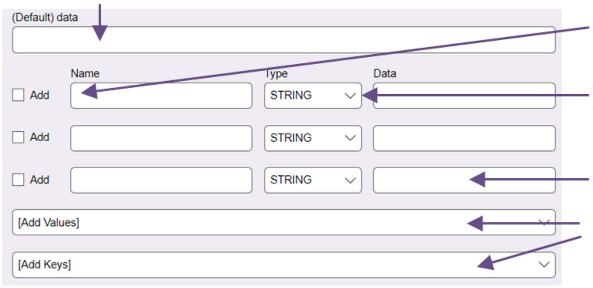
    a. In the **Name** edit field, enter the name of the value to set.

    b. From the **Type** drop-down menu, select the data type for the value, either `STRING` or `DWORD`.

    c. In the **Data** edit field, enter the data to assign to this value. See **Using Dynamic Tags in Registry Plans** for information on how to use dynamic tags to specify the data.

    d. If this value has not already been created on the remote desktop, check the **Add** option.

Enter data to place in the (Default) value. If left blank, no changes are made to the existing (Default) value.



Enter the name of each value to add or set.

Select the type of value to add or set. Currently, the Connection Broker supports STRING and DWORD types.

Enter the data to set for this value.

Use these drop-down menus to set additional values or keys in the registry plan.

7. To set more than three values for this key, use the **Add Values** drop-down menu to add rows to the table.

8. To set more than one registry key, use the **Add Keys** drop-down menu to add keys to the plan.

9. Use the **Notes** edit field to store any additional information with the registry plan.

10. Click **Save** to store any changes.

Using Dynamic Tags in Registry Plans

The Connection Broker supports a number of dynamic tags for setting the **Data** field for any of the registry key values, including the **(Default)** value. You can use any of the following dynamic tags.

- `{EMPTY}`: *Clears* any existing data from the registry key and leaves the value blank.

- `{AD:USER:`*`attribute_name`*`}`: Replaces the existing registry key data with the value found in the user's Active Directory attribute given by *attribute_name*.

- `{AD:CLIENT:`*`attribute_name`*`}`: Replaces the existing registry key data with the value found for the attribute given by *attribute_name* of the client's Computer Active Directory object.

  The user must authenticate with the Connection Broker using Active Directory. If this is the case, the Connection Broker uses the name of the client computer, determined as either the NetBIOS or DNS name, to search for the correct Computer object in Active Directory.

- `{AD:MACHINE:`*`attribute_name`*`}`: Replaces the existing registry key data with the value found for the attribute given by *attribute_name* of the remote desktop's Computer Active Directory object. The Connection Broker resolves this type of dynamic tag when either of the following conditions is met.

  - The user is authenticated by the same domain as contains the selected remote desktop. In this case, the remote desktop can be registered with the Connection Broker from any type of center, for example a vCenter Server center.

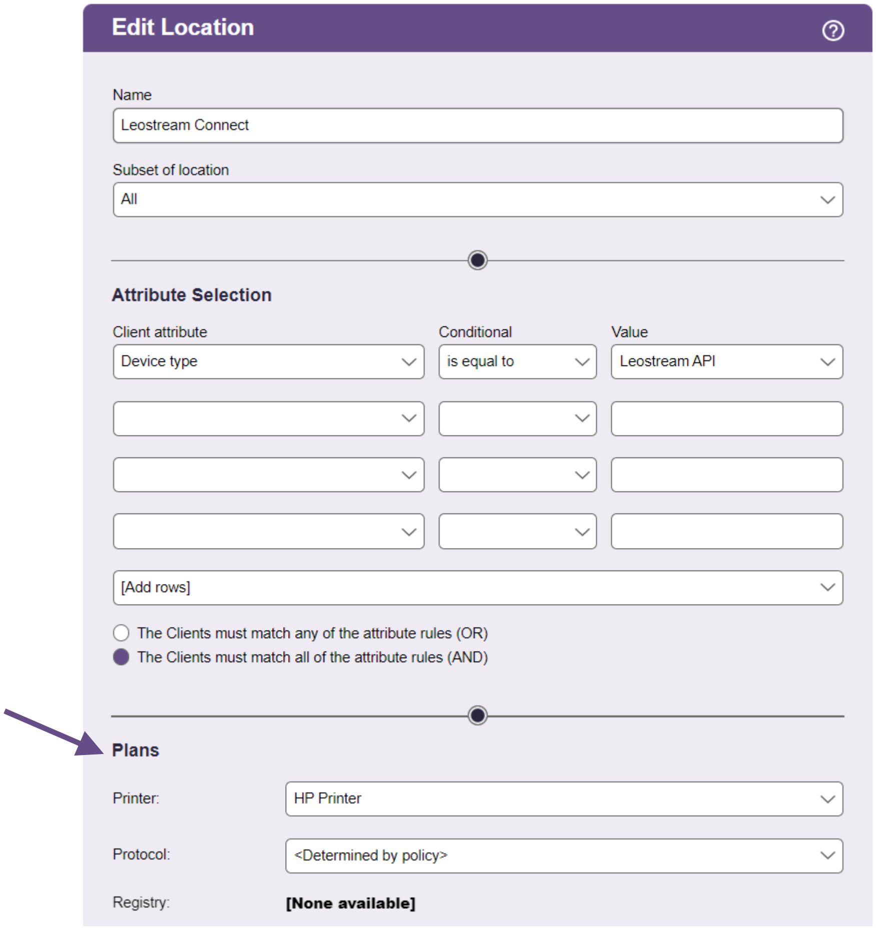
  - The remote desktop was registered with the Connection Broker from an Active Directory center. In this case, the desktop from the Active Directory center must be marked as Available, *not* as Duplicate. If the Active Directory desktop is available, the user does not have to authenticate with the same domain as contains the remote desktop.

Assigning Plans to Locations

Location-based plans allow you to tailor the end user experience based on the user's client. Connection Broker *locations* are essentially groups of clients made up of clients with common attributes, such as manufacturer, device type, OS version, IP address, etc. See **Creating Locations** for information on how to create locations.

By default, the Connection Broker does not assign any plans to a location. To assign plans to an existing location:

1. Open the **Edit Location** form, shown in the following figure.



Edit Location

Name: Leostream Connect

Subset of location: All

Attribute Selection

Client attribute	Conditional	Value
Device type	is equal to	Leostream API

[Add rows]

○ The Clients must match any of the attribute rules (OR)
● The Clients must match all of the attribute rules (AND)

Plans

Printer: HP Printer

Protocol: <Determined by policy>

Registry: [None available]

2. Select the printer plan to associate with this location from the **Printer** drop-down menu in the **Plans** section, indicated in the previous figure. Leave the drop-down menu on **Select…** if you do not want to assign a printer plan to this location.

   If a client falls into more than one location with a printer plan, the Connection Broker attaches the union of all printers included in all plans. For the default printer, the Connection Broker chooses the first printer in the list, determined as the first printer in the first plan, alphabetically, of all the plans associated with the locations.

   If your users connect using RDP and RDP printer redirection is turned on, the user's remote desktop will show the printers attached by any relevant printer plan, as well as any printers redirected by RDP.

3. Select the protocol plan to associate with this location from the **Protocol** drop-down menu. When the user logs in from this location, this protocol plan selection overrides the protocol plan selected in the user's policy. Leave the drop-down menu on **<Determined by policy>** to use the protocol plan assigned in the policy.

4. Select the registry plan to associate with this location from the **Registry** drop-down menu. You can override this registry plan on a client-by-client basis, using the **Edit Client** page (see **Editing Clients**).

If a client falls into multiple locations, the Connection Broker alphabetically sorts the locations, excluding the **All** location. The Connection Broker then applies the first protocol plan and registry plan it finds in the alphabetically sorted list of location. As a result, the protocol plan and registry plan can come from different locations.

The Connection Broker handles printer plans differently. For printer plans, the Connection Broker applies the printer plans for all the locations that the client falls into, ensuring that the user is always able to access the correct printer for their location. The Connection Broker attaches all printers from all the printer plans, setting the first printer as the default.

⚠ If no printers are associated with any of the printer plans for this location, the user will not have access to any network printers.

Using the Clients Page

The **> Resources > Clients** page lists all the client devices that have registered with the Connection Broker. Clients register with the Connection Broker when a user logs in from that client. You can also use the Connection Broker bulk-upload feature to load clients from a CSV-file (see **Uploading Data from CSV Files**).

Available Client Characteristics

You can modify the order and type of characteristics displayed on this page by clicking the **Customize column** link at the top-right side of the page (see **Customizing Tables**). The following sections describe the available client characteristics.

Action
Drop-down menu or list of links indicating the actions you can perform on a particular client, currently only **Edit** (see **Editing Clients**).

Bulk actions
Checkboxes that allow you to select multiple clients for performing a batch process, currently, **Edit** (see **Bulk Editing Clients**) and **Delete** (see **Deleting Clients**).

Name
The name given in the **Edit Client** dialog.

Asset Tag
The client asset tag.

Assigned Desktop
The desktop currently assigned to this client. This column is blank if no desktop is assigned.

Attached Displays
Number of monitors attached to the client.

Chassis Type
The chassis type as returned by Leostream Connect.

Client Binding
For PCoIP clients, indicates if this client is a slave or master client in a bonded client pair. If bonded, shows the associated master or slave client.

Client Software
The type of client software running on the client device.

Client Software Version
The version of the client software running on the client device.

Client UUID
The client UUID as reported by the client device, typically Leostream Connect.

Connected Desktop
The desktop currently connected to the client device.

Desktop Assignment Mode
Indicates if the client is hard-assigned to a desktop, or if it allows users to access their policy-assigned desktops.

Device
The type of client device as reported by the client software.

Device Type
The type of client as classified by the Connection Broker, for use when defining client locations.

Device UUID
A unique identifier for the client device.

Device Version
The device’s version information. For Web browser, this field includes the browser’s User Agent String.

Direct Connect
For PCoIP clients, indicates if the **Direct connect client to desktop** option is selected.

HTTP Header
The HTTP header reported by the client. Not all client types provide HTTP Header information.

Hostname
The client hostname.

Installed Viewers
A list of all the display protocol software clients and versions installed on client device running Leostream Connect.

IP Address
The client IP address.

Language
The client language.

Language ID
The ID associated with the client's language.

Last used
The date and time the client was last used.

Login Gateway
The Leostream Gateway or Gateway Cluster that forwarded the last login from this client to the Connection Broker. This value is not resent until the next time a login is initiated from this client.

MAC Address
The client MAC address.

Manufacturer
The client manufacturer.

Operating System
The operating system running on the client, if applicable.

Serial number
The client serial number.

Syslog Host
Indicates the Connection Broker that currently receives syslog events from this PCoIP client.

Type
An internal Connection Broker variable used to categorize types of clients.

Uploaded
Indicates if this client was uploaded using the options on the **> System > Maintenance** page. If set to `No`, this client appeared on the **Clients** page after a user logged into the Connection Broker from this client.

Filtering the Client List

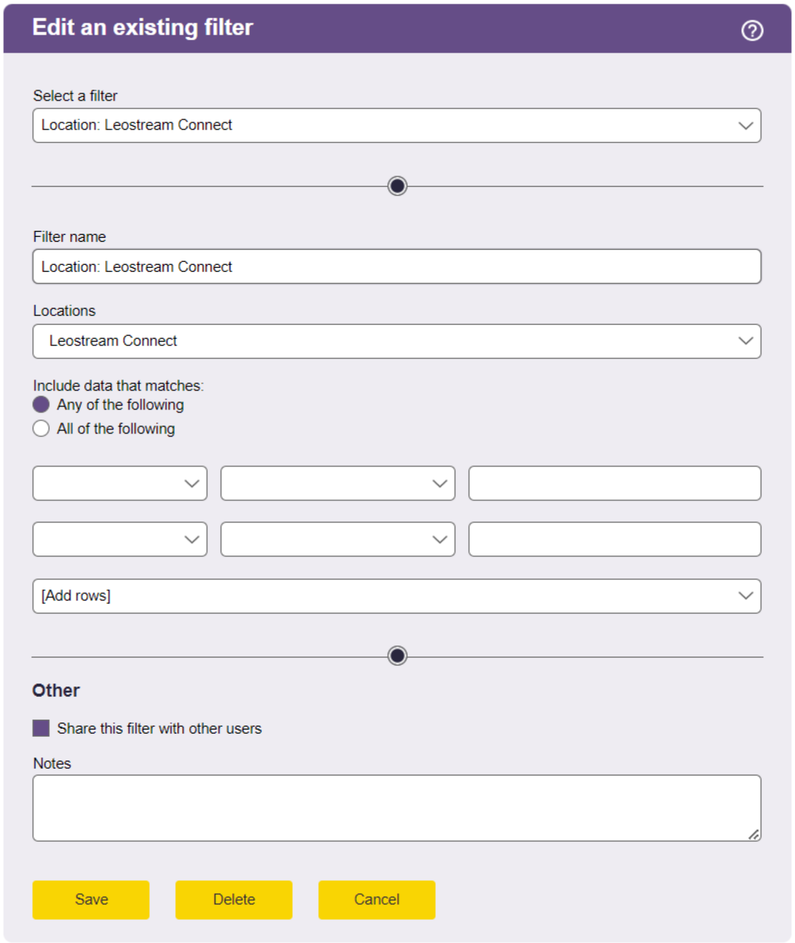
You can filter the list of clients in the **> Resources > Clients** page using the **Filter this list** drop-down menu at the top-right of the page.

When **Select filter** is selected, the list shows all clients that have logged into the Connection Broker, divided into a series of pages if applicable.

When you create a client location (see Creating Locations) the Connection Broker automatically creates a corresponding filter in the drop-down menu. Select one of these filters to limit the list to clients within the chosen location.

To edit an existing filter, such as one of the automatically created location filters:

1. Select **Edit an existing filter** from the **Filter this list** drop-down menu. The following form opens.



Edit an existing filter

Select a filter: Location: Leostream Connect

Filter name: Location: Leostream Connect

Locations: Leostream Connect

Include data that matches:
● Any of the following
○ All of the following

[Add rows]

Other

■ Share this filter with other users

Notes

2. Select the filter to edit from the **Select a filter** drop-down menu.

3. Enter a name for the filter in the **Filter name** edit field.

4. Select the location to associate with this filter from the **Location** drop-down menu. If you do not want to filter based on any location, select **All**.

5. Use the controls in the **Include data that matches** section to further filter the clients. You can filter clients based on the client’s name, asset tag, IP address, and device type, as shown in the previous figure.

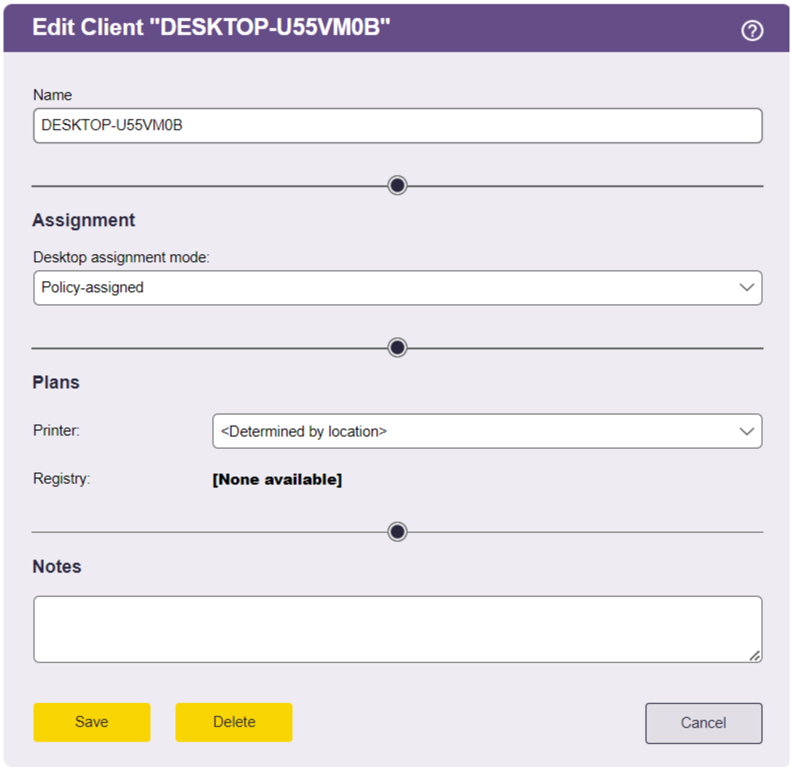
6. Click **Save**.

To create a new filter, select **Create a new filter** from the **Filter this list** drop-down menu, and follow steps 3 through 6 in the previous process. By default, only the user who creates a filter can use it. To allow other users to access your filter, check the **Share the filter with other users** option when you create the filter. This filter then appears in the **Filter this list** drop-down menu of other users that log into this Connection Broker.

Editing Clients

You can edit a particular client by selecting the **Edit** action associated with that client. Editing the client allows you to:

- Change the client’s name
- Set the client assignment mode (see **Hard-Assigning Clients to Desktop**)
- Select a printer and registry plan for this client (see **Assigning Plans to Clients**)



Edit Client "DESKTOP-U55VM0B"

Name
DESKTOP-U55VM0B

Assignment

Desktop assignment mode:
Policy-assigned

Plans

Printer: <Determined by location>

Registry: **[None available]**

Notes

Assigning Plans to Clients

By default, a client inherits its printer and registry plans from the locations that contain the client. If a client falls into multiple locations, the Connection Broker alphabetically sorts the locations, excluding the **All** location. The Connection Broker then applies the first registry plan it finds in the alphabetically sorted list of location.

The Connection Broker applies the printer plans for all the locations that contain the client. The Connection Broker attaches all printers from all the printer plans, setting the first printer as the default.

Use the **Printer** and **Registry** drop-down menus in the Plans section of the **Edit Client** page to override the location settings. When you select a printer plan for the client, only that printer plan is applied.

Bulk Editing Clients

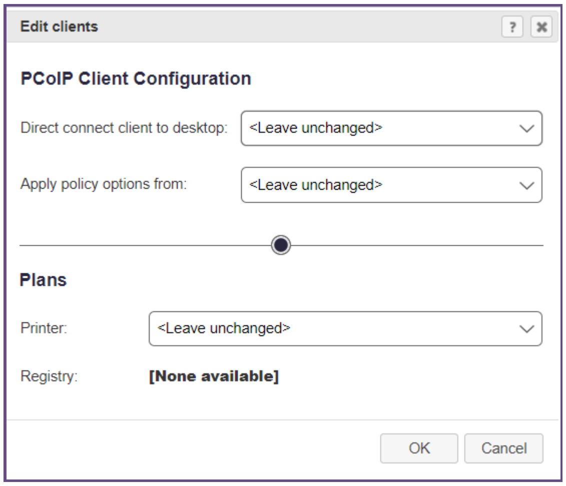
The **Bulk Edit** option for clients allows you to assign Printer and Registry plans to multiple clients. To edit multiple clients:

1. Go to the **> Resources > Clients** page.

2. In the **Bulk Action** column, select the checkboxes for all clients to edit. If the **Bulk Action** column is not displayed, click the **Customize column** link on the top-right of the list to add the column.

3. Select **Edit** from the drop-down menu at the top of the **Bulk Action** column.

4. In the **Edit clients** form, shown in the following figure, use the **PCoIP Client Configuration** section to configure parameters for PCoIP clients. This section appears, but does not apply to other client types. Select **<Leave unchanged>** for each parameter whose value you do not want to modify.



Edit clients

PCoIP Client Configuration

Direct connect client to desktop: <Leave unchanged>

Apply policy options from: <Leave unchanged>

Plans

Printer: <Leave unchanged>

Registry: [None available]

5. If the PCoIP clients have hard-assigned desktops, use the **Direct connect client to desktop** option, as follows:

   a. Select **Yes** to enable direct-connection mode. When using direct-connection mode, you must specify the policy to apply to the connection from the **Apply policy options from** drop-down menu.

   b. Select **No** to disable direct-connection mode.

6. Use the drop-down menus in the **Plans** section to set Printer and Registry plans for each client. These drop-down menus apply to all client types.

7. Click **Save** to apply the changes.

Deleting Clients

To remove clients from the client list, select the **Edit** action for appropriate client. In the **Edit client** form that opens, click **Delete** to remove the client.

You cannot delete the client you are currently using to log into the Connection Broker Administrator Web interface.

To simultaneously delete multiple clients, in the **> Resources > Clients** page:

1. Check the box associated with every client to delete. If check boxes do not appear in your **> Resources > Clients** table, customize the table so the **Bulk action** column appears.

2. Select **Delete** from the **Bulk action** drop-down menu at the top of the table.

3. Click **OK** in the confirmation window that appears.

Hard-Assigning Clients to Desktop

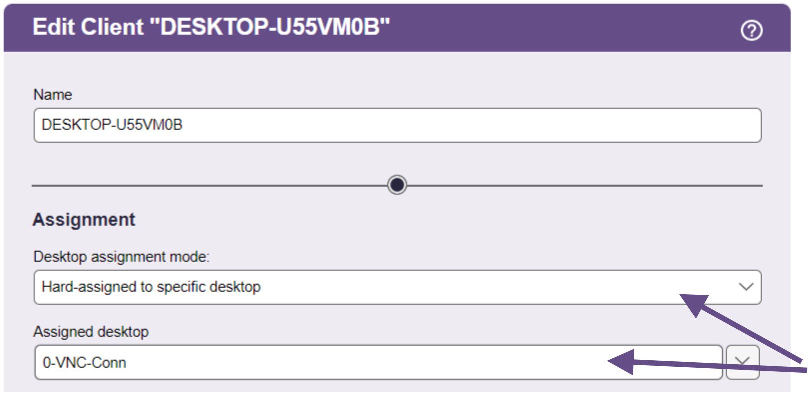
You can hard-assign a desktop to a client so that any user who logs into that client receives the same desktop. Desktops that are hard-assigned to a client are not available for policy assignment.

To hard-assign a client to a particular desktop:

1. On the **> Resources > Clients** page, select the **Edit** action for appropriate client. The **Edit Client** form opens.

2. In the **Assignment** section, select **Hard-assigned to a specific desktop** from the **Desktop assignment mode** drop-down menu.

3. Select the appropriate desktop from the **Assigned desktop** drop-down menu, as shown in the following figure.



Edit Client "DESKTOP-U55VM0B"

Name: DESKTOP-U55VM0B

Assignment

Desktop assignment mode: Hard-assigned to specific desktop

Assigned desktop: 0-VNC-Conn

4. Click **Save**.

When a user logs into a desktop that is hard-assigned to a client, the Connection Broker uses the settings n the **Hard Assignments** tab of the user’s policy. The user does not have access to their policy-assigned resources when they log into a client that is hard assigned to a desktop.

See **Desktop Assignment Modes** for more information on different desktop assignment modes.

Chapter 14: Assigning User Roles and Policies

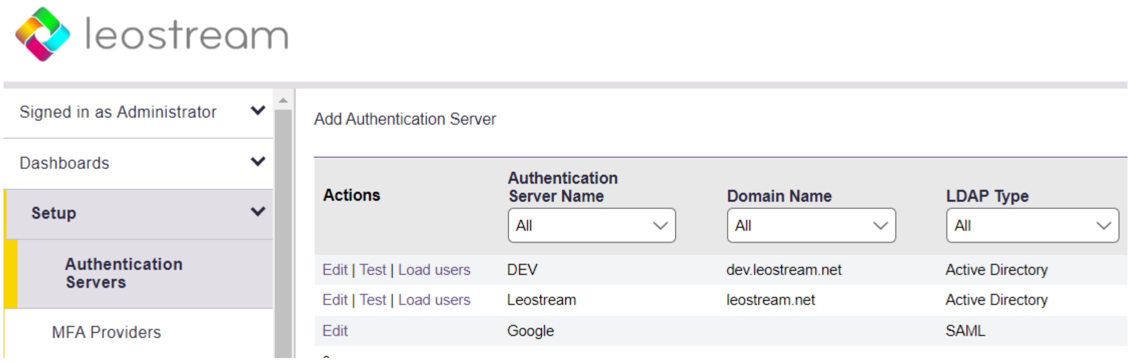
Overview

The Connection Broker uses roles and policies to determine what resources to offer to a particular user and the level of access the user has to these resources.

- A *role* is a set of permissions that defines the functionality an end user is allowed to access when they log into the Connection Broker, including the level of access to the Connection Broker Administrator Web interface (see **Chapter 10: Configuring User Roles and Permissions**)
- A *policy* is a set of rules that determine how desktops are offered, connected, and managed for a particular user (see **Chapter 12: Configuring User Experience by Policy**)

To determine which role and policy to assign to a particular user, the Connection Broker performs the following steps.

1. After the user provides their login credentials, the Connection Broker searches the authentication servers defined on the **> Setup > Authentication Servers** page, shown in the following figure, for a user that matches those credentials (see **Chapter 5: Authenticating Users**).

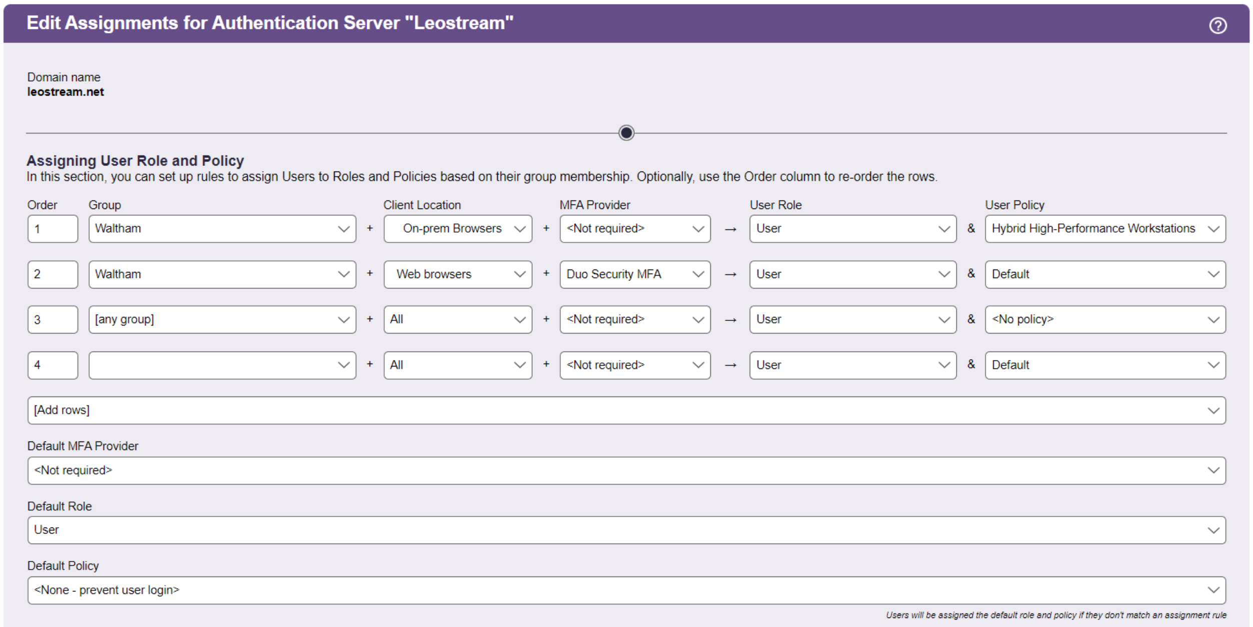


Actions	Authentication Server Name	Domain Name	LDAP Type
	All	All	All
Edit | Test | Load users	DEV	dev.leostream.net	Active Directory
Edit | Test | Load users	Leostream	leostream.net	Active Directory
Edit	Google		SAML

2. The Connection Broker then looks on the **> Configuration > Assignments** page for the assignment rules associated with that authentication server. For example, if the Connection Broker authenticated the user in the `Leostream` domain in the previous figure, the Connection Broker would look in the `Leostream` assignment rules.

3. The assignment rules, shown for example in the following figure, assign a role and policy to the user based on the user’s attributes in the authentication server and the location they are logging in from.

   The **Client Location** drop-down menu contains the locations you created in the **> Configuration > Locations** page.



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	Waltham	+	On-prem Browsers	+	<Not required>	→	User	&	Hybrid High-Performance Workstations
2	Waltham	+	Web browsers	+	Duo Security MFA	→	User	&	Default
3	[any group]	+	All	+	<Not required>	→	User	&	<No policy>
4		+	All	+	<Not required>	→	User	&	Default

[Add rows]

Default MFA Provider
<Not required>

Default Role
User

Default Policy
<None - prevent user login>

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

To assign a rule, the Connection Broker searches down the rows in the **Assigning User Role and Policy** table. As soon as the Connection Broker finds a match between the user's attribute/location and a row in the rules, the user is assigned that particular role and policy. If the user/location combination matches multiple rules, the Connection Broker uses the first rule based on the order defined by the **Order** column. If there are no matches, the Connection Broker assigns the role and policy selected in the **Default Role** and **Default Policy** drop-down menus, respectively.

For example, in the previous figure:

If:

- The user's `memberOf` attribute is **Waltham** AND
- The user is logging in from the **On-prem Browser** client location

Then:

- The user's role is **User**
- The user's policy is **Hybrid High-Performance Workstations**

If:

- The user's `memberOf` attribute is **Waltham** AND
- The user is logging in from the **Web browser** client location, presumably for an off-premises login

Then:

- MFA is required and, if that succeeds
- The user's role is **User**
- The user's policy is **Default**

All other user logins are blocked.

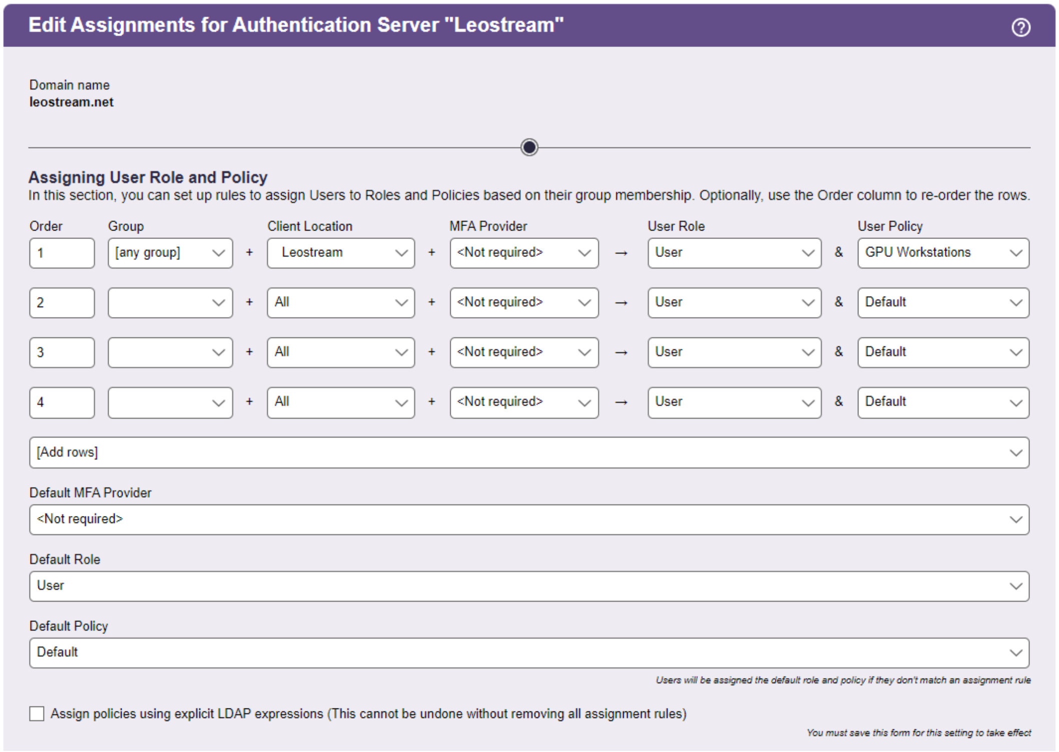
After a user is assigned to a policy, changes you make to your **Assignments** tables that would change that user’s policy upon login will not take effect until all jobs scheduled by their original policy are completed or cancelled. For example, if the user’s policy schedules a `logout_after_idle` job on the **> System > Job queue** page, the user’s existing policy continues to control the user's session and is applied to any subsequent Leostream logins until the logout job completes.

The Connection Broker provides the following options for assigning roles and policies to users.

- **Assigning Roles and Policies Based on Group Membership**
- **Assigning Roles and Policies Based on any Attribute**
- **Assigning Roles and Policies Based on Multiple Attributes**

Assigning Roles and Policies Based on Group Membership

If the **Query for group information** option was checked when you created the associated authentication server, the **Edit Assignment** form for this authentication server appears as 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

In this configuration, the Connection Broker matches the selection in the **Group** drop-down menu to the `memberOf` attribute for Active Directory authentication servers. You cannot use this method when authenticating users in an OpenLDAP authentication server.

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. If users in this location are required to pass MFA, select an MFA option from the **MFA Provider** drop-down menu. This column is not displayed if you have not defined any MFA providers in the **> Setup** section of your Connection Broker.

4. Assign permissions to this group and client location pair by selecting an item from the **User Role** drop-down menu

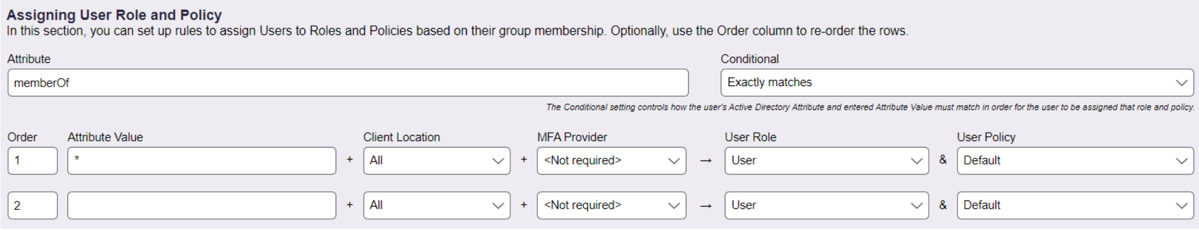
5. Assign a policy to this group and client location pair by selecting an item from the **User Policy** drop-down menu

📝 The Connection Broker loads group information from your Active Directory server when you create your authentication server, then stores the groups in local memory. Group information is reloaded only when you log into the Administrator web interface. If you make changes to your Active Directory groups while you are logged into Leostream, you must sign out and sign back into the Administrator Web interface to see the new groups on the **> Configuration > Assignments** page.

If you need to assign roles and policies based on a different authentication server attribute, check the **Assign policies using explicit LDAP expressions** 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. The following section describes how to define rules using any attribute. To assign roles and policies based on multiple attributes, see **Assigning Roles and Policies Based on Multiple Attributes**.

Assigning Roles and Policies Based on any Attribute

If the **Query for group information** option was *not* selected when you created your authentication server, or if you checked the **Assign policies using explicit LDAP expressions** option on the **Edit Assignment** form, the **Edit Assignment** form appears as shown in the following figure.



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.

Attribute: memberOf

Conditional: Exactly matches

The Conditional setting controls how the user's Active Directory Attribute and entered Attribute Value must match in order for the user to be assigned that role and policy.

Order	Attribute Value		Client Location		MFA Provider		User Role		User Policy
1	*	+	All	+	<Not required>	→	User	&	Default
2		+	All	+	<Not required>	→	User	&	Default

To assign rules based on a specific user attribute:

1. Enter the attribute to use when searching though the rules in the **Attribute** edit field. To search by group attribute:

   - Use `memberOf` for Active Directory authentication server
   - Use `ou` for an `organizationalPerson` in an OpenLDAP authentication servers

   The **Attribute** field supports matching against the `leostream_dn` property.

1. Select an option from the **Conditional** drop-down menu to restrict how the user's attribute should match the entry in each rule, either:
    - Contains
    - Starts with
    - Exactly matches
    - LDAP expression (see **Assigning Roles and Policies Based on Multiple Attributes**)
2. Enter a string in the **Attribute Value** edit field, which is used to match the user to this rule.

3. If users in this location are required to pass MFA, select an MFA option from the **MFA Provider** drop-down menu. This column is not displayed if you have not defined any MFA providers in the **> Setup** section of your Connection Broker.

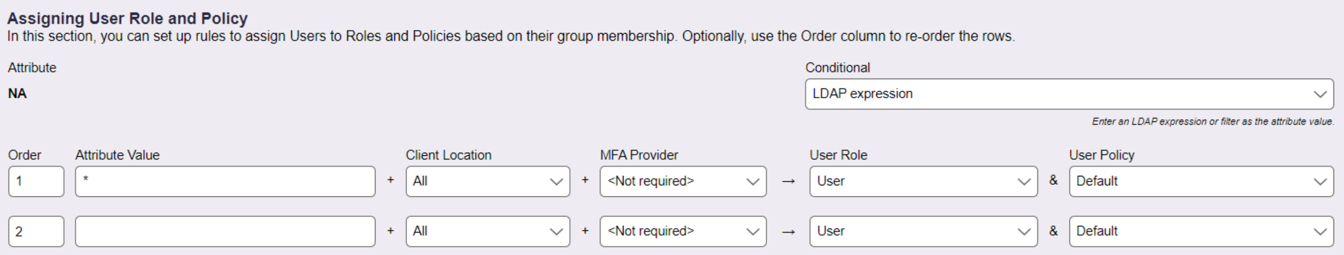
4. If you are using locations, select a location from the **Client Location** drop-down menu

5. Assign a role by selecting an item from the **User Role** drop-down menu.

6. Assign a policy by selecting an item from the **User Policy** drop-down menu.

Assigning Roles and Policies Based on Multiple Attributes

The advanced configuration of the **Assigning User Role and Policy** section, shown in the following figure, provides the option to use LDAP filters to identify users for a particular role and policy rule.



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.

Attribute: **NA**

Conditional: LDAP expression

Enter an LDAP expression or filter as the attribute value.

Order	Attribute Value		Client Location		MFA Provider		User Role		User Policy
1	*	+	All	+	<Not required>	→	User	&	Default
2		+	All	+	<Not required>	→	User	&	Default

To assign roles and policies based on multiple attributes:

1. Select **LDAP expression** from the **Conditional** drop-down menu, as shown in the previous figure. The **Attribute** field no longer applies and becomes non-editable.

2. In the **Attribute Value** edit field, enter an LDAP filter expression. For information on valid LDAP filter expressions, see the following Microsoft TechNet article:

    http://technet.microsoft.com/en-us/library/aa996205(EXCHG.65).aspx

    For example, if the user must be a member of both `Operations` and `RDPGroup` to be assigned this role and policy, enter the following in the **Attribute Value** edit field:

```
(&(memberOf=CN=Operations,CN=Users,DC=leostream,DC=net)(memberOf=CN=RDPGroup,CN=Users,DC=leostream,DC=net))
```

Conversely, if the user can be a member of either `Operations` or `RDPGroup` to be assigned this role and policy, enter the following in the **Attribute Value** edit field:

```
(|(memberOf=CN=Operations,CN=Users,DC=leostream,DC=net)(memberOf=CN=RDPGroup,CN=Users,DC=leostream,DC=net))
```

You can also assign the role and policy based on multiple attributes. For example, if the user must be a member of the `Operations` group and have a country code of `1`, enter the following in the **Attribute Value** edit field:

```
(&(countryCode=1)(memberOf=CN=Operations,CN=Users,DC=leostream,DC=net))
```

3. If you are using locations, select a location from the **Client Location** drop-down menu.

4. If users in this location are required to pass MFA, select an MFA option from the **MFA Provider** drop-down menu. This column is not displayed if you have not defined any MFA providers in the **> Setup** section of your Connection Broker.

5. Assign a role by selecting an item from the **User Role** drop-down menu.

6. Assign a policy by selecting an item from the **User Policy** drop-down menu.

When the Connection Broker steps through the assignment rules, it queries the associated authentication server to see if the LDAP filter matches the user.

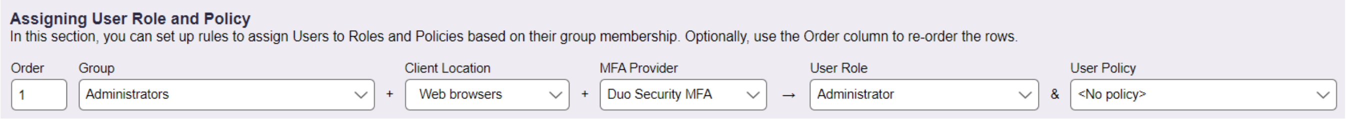
Assigning Roles without Policies

You may have users that have access to the Connection Broker Administrator Web interface who do not have resources assigned to them by the Connection Broker. For these users:

1. Create a role that gives the user access to the Administrator Web interface, only (see **Administrator Web Interface Permissions**) and configure the permissions for this role, as necessary.

2. In the **Assigning User Role and Policy** section, select this role from the **User Role** drop-down menu

3. Select **<No policy>** from the **User Policy** drop-down menu, for example:



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	Administrators	+	Web browsers	+	Duo Security MFA	→	Administrator	&	<No policy>

In this example, if:

- The user is a `memberOf` **Administrators** AND
- The user is logging in from the **Web Browser** client location
- And the successfully authenticate against Duo for MFA

Then:

- The user's role is **Administrator**
- The user is not assigned a policy

When a user matching this rule logs into the Leostream Web client, they log directly into the Administrator Web interface, where they see only the features that their role gives them permission to access.

Reordering User Role and Policy Rules

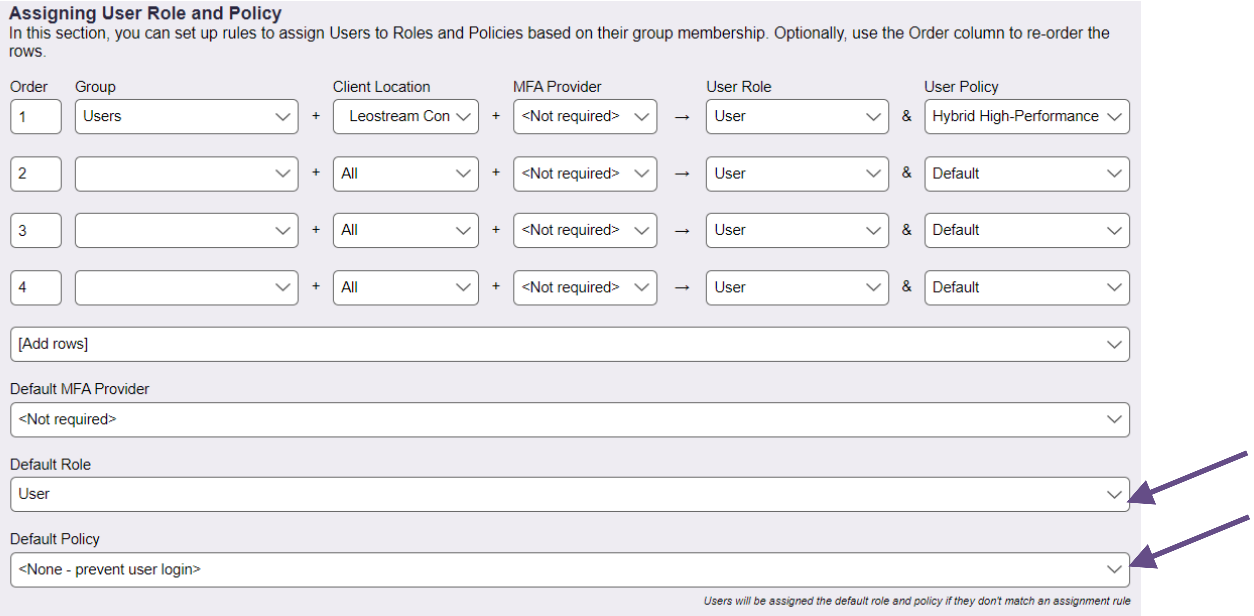
Use the **Order** column to reorder the rows in the **Assigning User Role and Policy** section.

To move a row, type a new row number into the **Order** edit box at the beginning of the row. You can enter new row numbers for as many rows as you want to move. To store the changes, click **Save**.

⚠ The new row numbers are not stored until you save the changes. Make sure you do not navigate away from the **Edit Assignments** page without clicking **Save**.

Using the Default Role and Policy

The **Default Role** and **Default Policy** drop-down menus, shown in the following figure, specify what happens if the user is found in the authentication server, but does not match any of the defined assignment rules.



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	Users	+	Leostream Con	+	<Not required>	→	User	&	Hybrid High-Performance
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

<None - prevent user login>

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

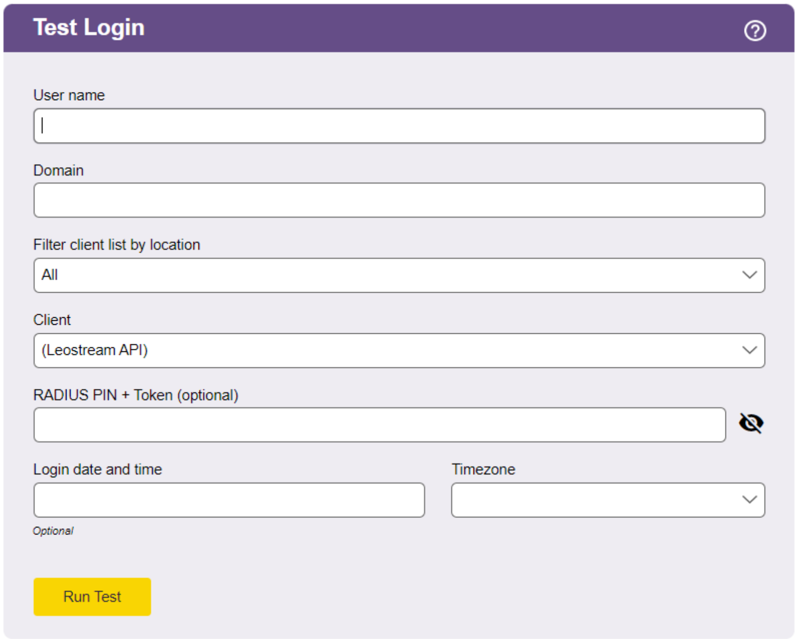
If you do not want to assign a desktop to users who do not match one of the assignment rules, select **<None- prevent user login>** from the **Default Policy** drop-down menu. If you are assigning a default role and policy, you can use the **Default MFA Provider** drop-down to indicate if these users must also successfully authenticate with one of your MFA providers before being allowed to log in. The **Default MFA Provider** drop-down is not available if you have not defined any MFA providers in the **> Setup** section of your Connection Broker

Testing User Role and Policy Assignment

The **Test Login** action provides an easy and efficient method for checking if your user role and policy rules are assigning desktops correctly. This feature simulates a user logging in and reports back on how the Connection Broker matches that user to a role and policy and assigns desktops.

Test a user login, as follows:

1. Go to the **> Resources > Users** page.
2. Click the **Test Login** link. The **Test Login** page, shown in the following figure, opens.



Filter client list by location: All

Client: (Leostream API)

3. In the **User name** edit field, enter the name of the user you want to simulate logging in. This user does not need to be registered in your Connection Broker.
4. Choose a domain to log the user into 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**.

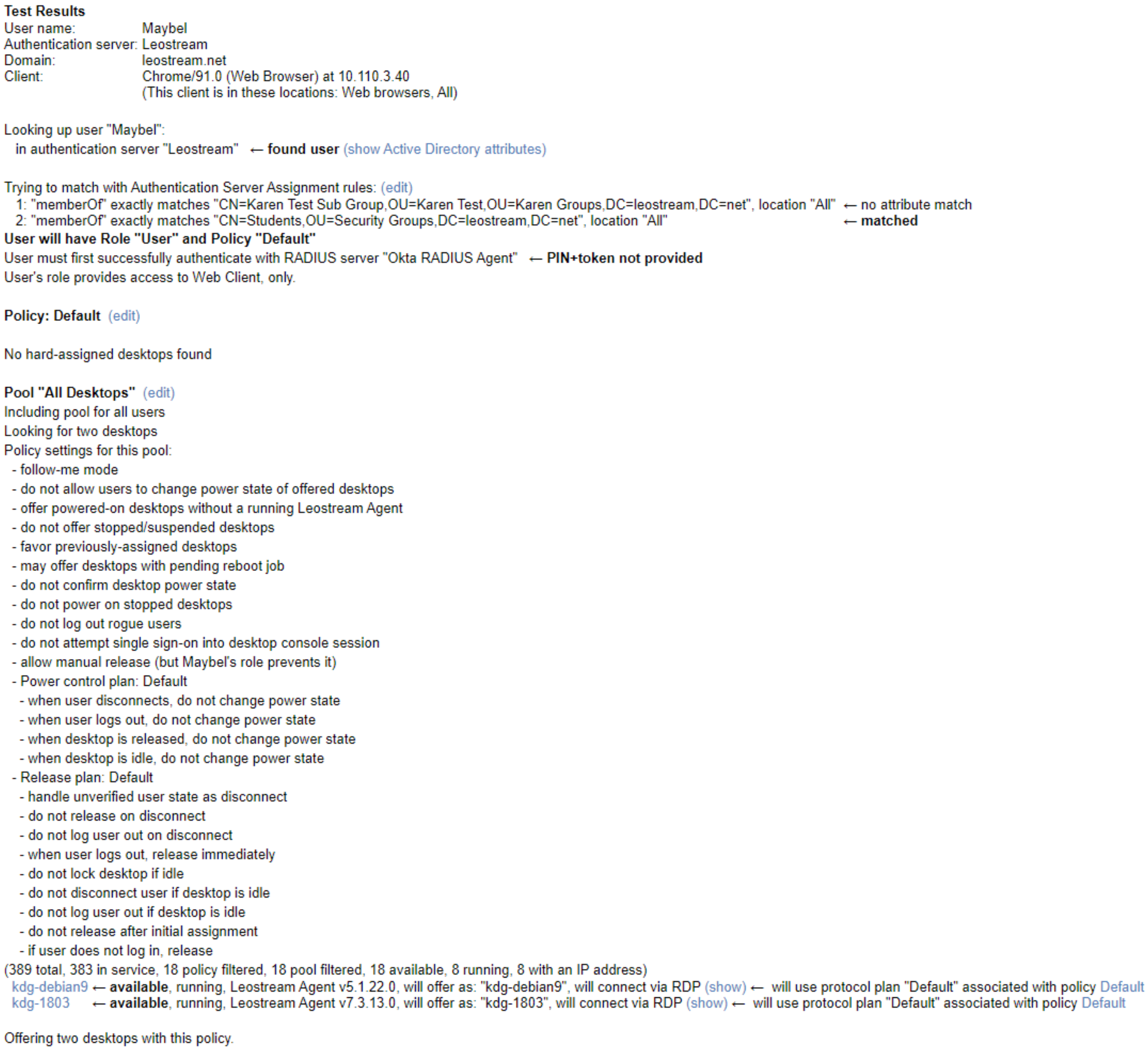
   If you perform a test login for a client that is in multiple locations, selecting a location in this drop-down menu does not guarantee that the test login uses this location. The Connection Broker uses its programmed logic to determine the client location.
6. Select the client the user is logging in from the **Client** drop-down menu. The items available in the **Client** menu reflect the clients available in the selected location.

7. If you have defined MFA providers o the **> Setup** page and want to validate the MFA provider is correctly authenticating users, you can enter the one-time token in the **RADIUS PIN + Token** field. If you leave this field blank, the test login results indicate that MFA would be required but complete the simulated login as if MFA succeeded.

8. If your policies offer desktops from pools based on the time-of-day, use the **Login date and time** and T**imezone** drop-down menus to simulate a login on a specific time and day.

9. Click **Run Test**.

The bottom of the page updates to show the current test results. 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.
```

In this example, the test results begin by reporting the user, location, and client you specified in the **Test**

Login form. The Connection Broker then searches for the user in the domains you specified in the **Test Login** form. The line:

```
  in authentication server “Leostream” ← found user
```

Indicates that the user `maybel` was found in the authentication server named `Leostream`. If the user is found, the report lists the user’s authentication server attributes. Click the **(show Active Directory attributes)** link next to this line to see the details of this user’s authentication server account.

The Connection Broker tries to map the user’s authentication server attributes to a rule in the **Assigning User Role and Policy** section of the associated **Edit Assignments** page. If the Connection Broker finds an entry that matches the user’s authentication server attribute, it assigns the role and policy in that row to the user. If no match is found, the Connection Broker assigns the `Default` policy to the user. In the previous example, the lines:

```
      “memberOf” exactly matches “CN=Students,OU=Security
Groups,DC=leostream,DC=net”, location “All” ← matched

      User will have role “User” and policy “Default”
```

Indicate that a rule was matched and that the Connection Broker assigns the user to the role `User` and policy `Default`.

The report lists the pools associated with the assigned policy and shows the policy settings for each pool. The bottom of the section for each pool indicates which desktops the user is offered from this pool and the display protocol used to connect the user to that desktop. Click the **(show)** link to display the command line parameters or configuration file that will be used to establish the connection.

Chapter 15: Using the Leostream Web Client

Logging into the Leostream Web Client

The Leostream Web client allows users to log in to Leostream from any type of client device type and web browser, including tablets. Depending on the display protocol used to connect the user to the desktop, additional client software may be required. If your users log in to Leostream using an Apple or Android tablet, ensure that their tablet has an installed app that can launch the display protocol used to connect them to their desktops or use the Leostream HTML5 viewer for in-browser connections.

To access the Leostream Web client, end users and administrators all log in using the Connection Broker **Sign In** page. By default, the Connection Broker **Sign In** page is at the following URL.

```
https://leostream-address
```

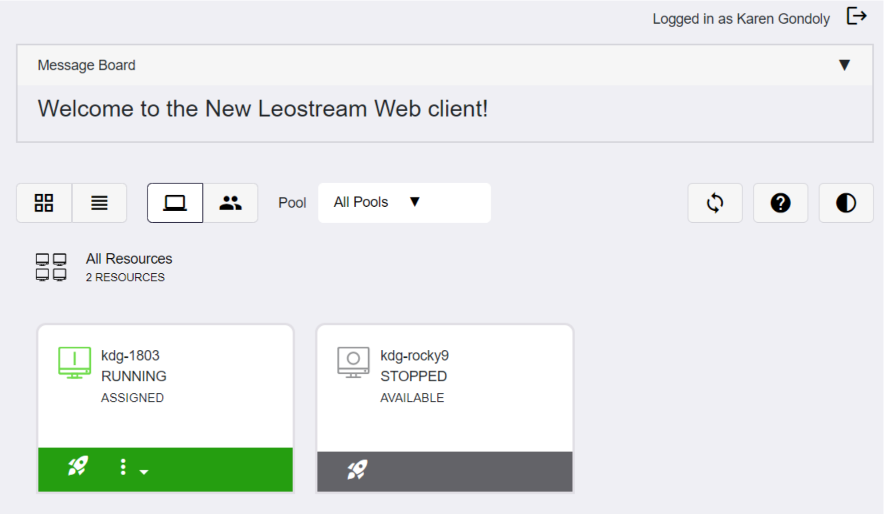
Where `leostream-address` is your Leostream environments IP address or hostname. For information on customizing the appearance of the **Sign In** page, see **Adding Customized Text, Links, and Images to the Sign In Page** or the **Sign-In Page Customization Guide**.

Connection Broker logins can be proxied through a Leostream Gateway, in which case the **Sign In** page is accessed at the Leostream Gateway address instead of the Connection Broker address. See the **Leostream Gateway Guide** for more information.

If you are leveraging a SAML-based Identity Provider (IdP) for authentication into your Leostream environment, the main login URL for your Leostream environment automatically redirects the user to the login page for your IdP. You can allow users to bypass your IdP by selecting the **Enable user logins without SAML at https://*<leostream-address>*/login** option on your SAML Authentication server. See the **Leostream Guide for using SAML-based Identity Providers** for more information.

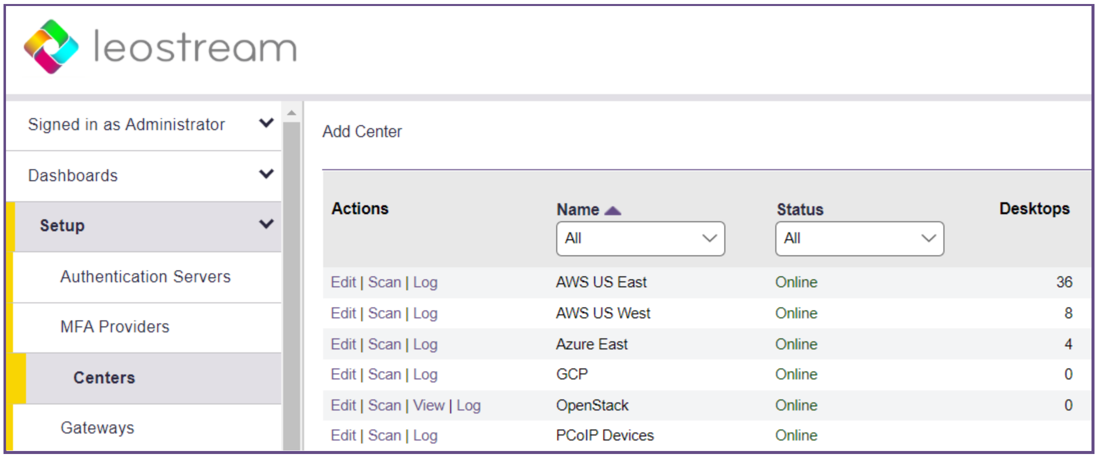
Regardless of if the user is authenticated by the Leostream Connection Broker or your SAML-based Identity Provider, after logging into the Leostream Web client, the default view depends on the user's Leostream role. See **Controlling Access to the Administrator Web Interface** for more information.

1. For end users, the Leostream Web client, shown in the following figure, is specialized for launching connections to their desktops.



Welcome to the New Leostream Web client!

2. For administrators, the Connection Broker Administrator Web interface, shown in the following figure, provides access to the Leostream configuration.



Actions	Name	Status	Desktops
	All	All	
Edit | Scan | Log	AWS US East	Online	36
Edit | Scan | Log	AWS US West	Online	8
Edit | Scan | Log	Azure East	Online	4
Edit | Scan | Log	GCP	Online	0
Edit | Scan | View | Log	OpenStack	Online	0
Edit | Scan | Log	PCoIP Devices	Online	

Client Certificate (Smart Card) Logins for the Leostream Web Client

Users logging in using the Leostream Web client can authenticate into your Leostream environment using a smart card or client certificate.

⚠ The Connection Broker leverages the underlying Apache configuration to enable certificate-based authentication. Therefore, enabling client certificate-based authentication is a global setting for your Leostream environment. All users logging in using the Leostream Web Client must have a valid certificate. Before proceeding, ensure you define a Leostream Administrator in the domain that issues your certificates and have a valid certificate for that user so they can log into your Connection Broker.

Prerequisites and Important Notes

Leveraging the client-certificate authentication feature requires the following:

- You must have the root CA certificate or CA bundle file for the Certificate Authority that manages certificate and/or smart card logins.
- The CA must be associated with an Active Directory domain.
- All users must be members of the same domain. You cannot use multiple domains in the Connection Broker after smart card logins are enabled.
- Users must have a valid certificate available to the Browser at the time they navigate to their Leostream Web client Login page. If a valid certificate is not present, the server presents an error.

  Certificates are available to the browser if a physical smartcard reader with an inserted smartcard is attached to the user’s client device or if the user uploads the certificate to their Web browser.
- Leostream Connect logins continue to require username/password authentication.

Enabling Client-Certificate Authentication

To enable client certificate-based authentication:

1. Upload your CA certificate or CA bundle file to your Connection Broker, as follows.

   a. Go to the **> Setup > Authentication Servers** page.

   b. Click **Edit** for the Active Directory authentication server that matches the domain of your certificates.

      See **Adding Microsoft® Active Directory® Authentication Servers** for instructions on adding an Active Directory authentication server.

   c. In the **Smartcard / PIV Card Authentication** section, click the **Choose File** button and browse to the location of your CA certificate or CA bundle file. After selecting the file, click **Open** to upload it to your Connection Broker

   d. In the **AD Account linking** drop-down menu, ensure that **userPrincipalName** is selected.

   e. In the **Smartcard or Certificate Account linking for web client** edit field, enter the smart card or certificate attribute that contains the smart card owner’s userPrincipalName, for example `SSL_CLIENT_SAN_OTHER_msUPN_0`.

      For a list of potential attributes, see:

      https://httpd.apache.org/docs/current/mod/mod_ssl.html

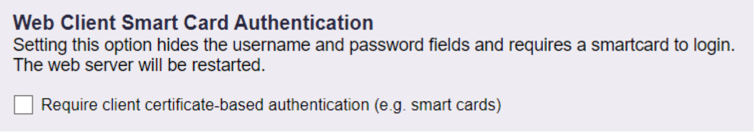
f. Scroll down to the **User Login Search** section. Ensure that userPrincipalName is entered in the **Match login name against this field** edit field.

g. Scroll down to the **Other** section in the **Edit Authentication Server** form and ensure that the **Query order** drop-down menu selects the **[First authentication server]** option.

h. Click **Save**.

2. Go to the **> System > Settings** page in your Connection Broker Administrator Web interface.

3. Select the **Require client certificate-based authentication (e.g. smart cards)** option, shown in the following figure.



Web Client Smart Card Authentication
Setting this option hides the username and password fields and requires a smartcard to login.
The web server will be restarted.

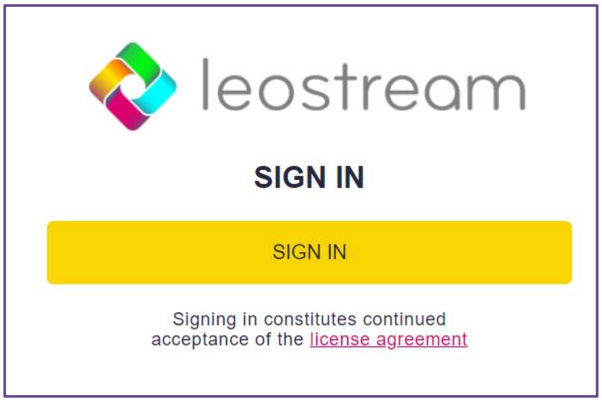
□ Require client certificate-based authentication (e.g. smart cards)

4. Click **Save**. The Connection Broker Apache service immediately restarts.

Client Certificate Login Process

After enabling client certificate authentication, any currently logged in users will remain logged in, including the administrator login used to enable the authentication. New users are taken through the following login process.

1. Navigating to the Connection Broker login page presented the following Login dialog to initiate a login. Username/password authentication is no longer supported for Web client logins.



Signing in constitutes continued acceptance of the license agreement

2. Clicking **Sign in** prompts the user to select a certificate or unlock their smartcard with their PIN.

3. After the user selects or unlocks their certificate, the Connection Broker retrieves the certificate from the Web browser.

4. The Connection Broker then locates the user in Active Directory by comparing the value found in the certificate for the attribute defined in the authentication server's **Smartcard or Certificate**

Account linking for web client field to the userPrincipalName of the users in Active Directory.

5. After locating the user record, the Connection Broker uses the Active Directory authentication server’s **> Configuration > Assignments** table to assign a policy to the user and display their offer list.

Disabling Client Certificate Authentication

If the administrator session you used to enable client certificate authentication has not expired, you can return to the **> System > Settings** page, uncheck the **Require client certificate-based authentication** checkbox, and **Save** the **Settings** page to disable client-certificate authentication and return to username/password authentication.

In the likely event that your administrator session has expired, you can use the Connection Broker machine console to disable the feature, as follows.

1. Log into the machine running your Connection Broker as the `root` user.

2. Issue the following command.

   ```
   su – leo
   ```

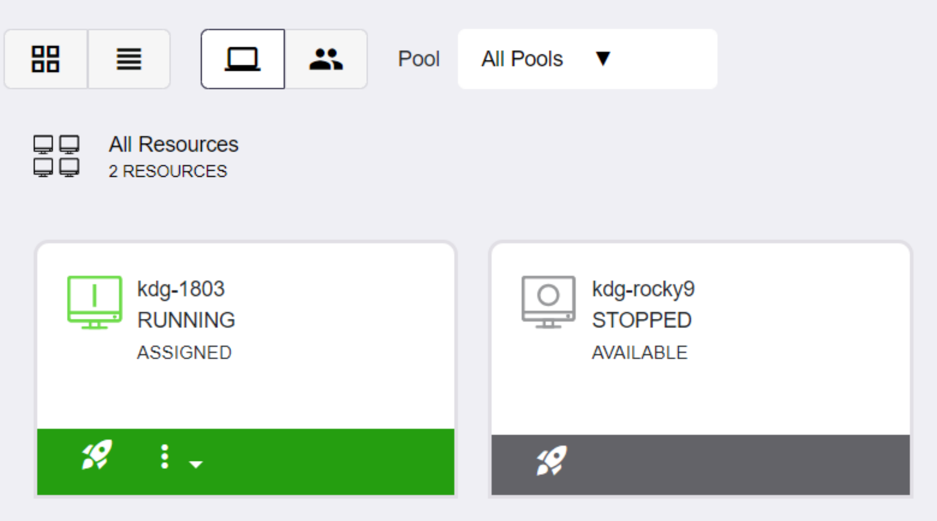
   The **Administration Menu** opens.

3. Select the **Advanced**.. option and press the <Enter> key.

4. Select the **Httpd** option to display smart card web client authentication and press the <Enter> key.

Working with Resources in the Web Client

The **Resources** box displays the user’s offered desktops along with their power state and any available actions the user is permitted to execute, for example:

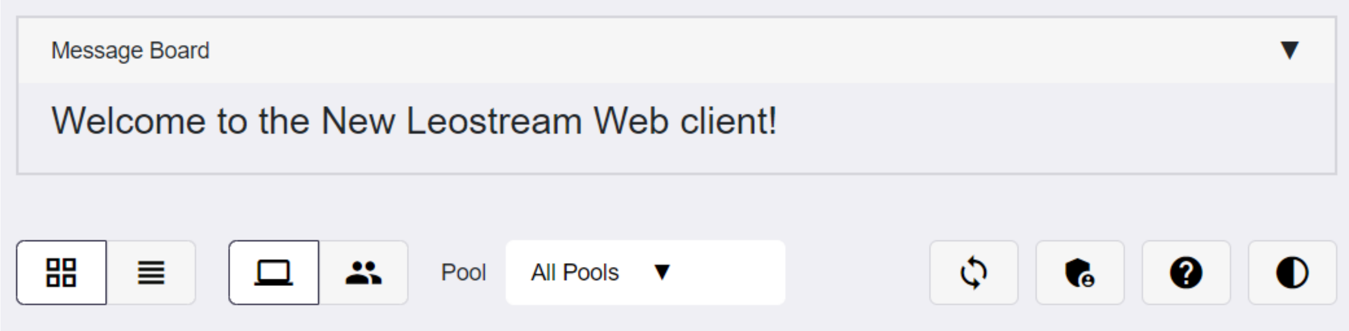


kdg-1803
RUNNING
ASSIGNED

kdg-rocky9
STOPPED
AVAILABLE

Filtering and Arranging the Offer List

The buttons and drop-down menus above the Resources, shown in the following figure, provide options for users to sort and change the layout of their offered Resources.



Message Board ▼

Welcome to the New Leostream Web client!

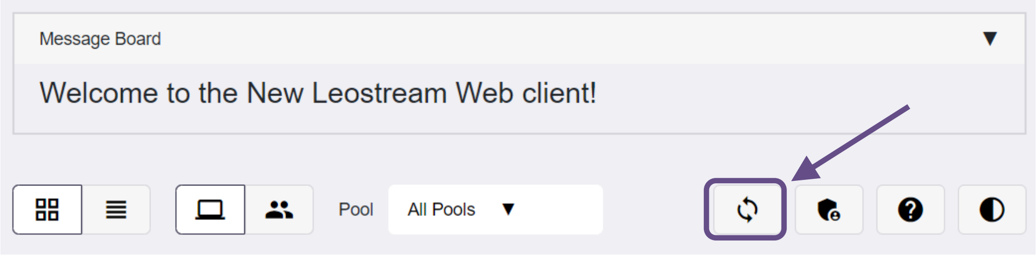
From left to right, the options include the following:

- Present the offered resources in a grid view. For each tile in the grid:
  - The color of the tile indicates the power state. Green indicates the resources is powered on and grey indicates the resources is powered off or in an unknown state.
  - The text on the tile displays the resource name, its power state, and if the machine is currently assigned or available for assignment
  - The toolbar on the bottom of the tile provides the available actions, including connecting to the resource or performing power control actions, as described in the following sections.
- Present the offered resources in list view. Each item in the list provides the same information as described for the grid view.
- Show all offered and assigned desktop resources.
- Show current sent or received collaboration invitations.
- Filter the displayed desktop resources by pool (does not apply when showing only invitations).
- Refresh the offer list
- Open Administrator View (this option is available based on the user's Role).
- Open the Web client help page.
- Toggle between light and dark mode.

Refreshing the Resource List

The Web client automatically refreshes the user offer list every time the user's focus leaves and subsequently returns to the Leostream Web client.

At any point after logging in, users can refresh the contents of their offer list by clicking the **Refresh** button, shown in the following figure.



Message Board

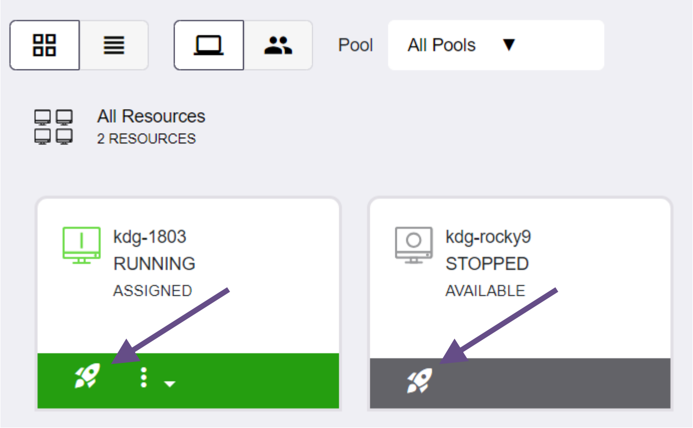
Welcome to the New Leostream Web client!

Refreshing the list may do any of the following.

- Offer new desktops, depending on the user's policy
- Update the available links for each resource, if the user's role has been modified to give them different permissions
- Remove or modify the contents of the Message Board, if the Connection Broker Administrator Web interface was modified, as such.

Connecting to Desktops from the Web Client

Users can launch individual desktops by clicking the **Launch** button associated with that desktop, represented as a rocket ship, as shown in the following figure for the grid layout.



If the desktop is Stopped, the Connection Broker powers on the machine prior to establishing the connection. The Web client displays a **Connecting** status until the remote session is established. If the user has a protocol plan that does not specify a display protocol for Web browser logins, the user receives a **No connection protocol defined** warning after they click the **Launch** button.

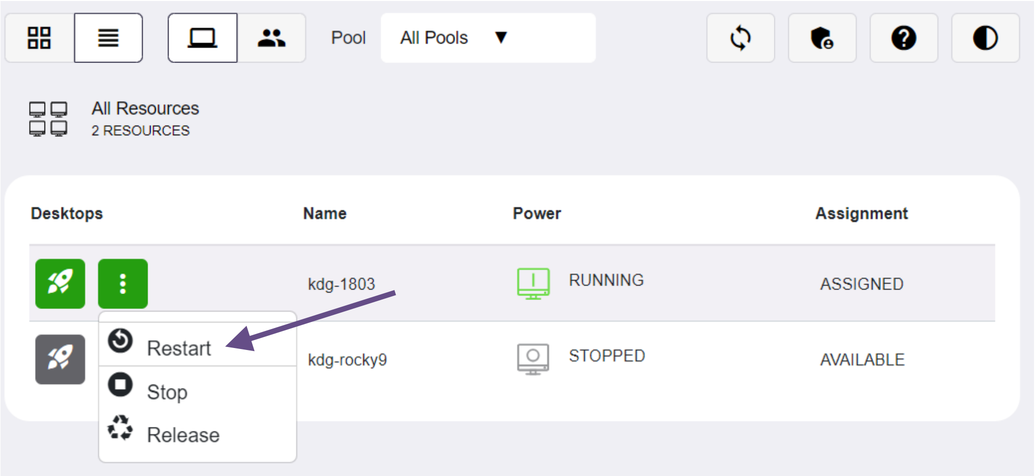
If the user is offered a single desktop, and their policy enables the **Auto-launch remote viewer session if only one desktop is offered** option, the Web client displays the **Connecting** status and connects to their desktop as soon as the user logs in.

Power Control for Desktops

The Web client may include **Restart**, **Stop**, **Start** and **Hard Reset** option for any desktop that the user is allowed to power control. The user's role and policy determine which desktops provide the power control action and which actions are available, as follows:

- The user's role must select the **Allow user to power control offered desktops** option.
- The user's policy must enable one of the three available power control actions:
    - If either **Yes, using reboot** or **Yes, using power off and start** is selected in the **Allow users to stop/start desktops** drop-down menu, desktops from this pool may have a **Start** or **Stop** action, depending on the desktops' current power state.
    - If either **Yes, using reboot** or **Yes, using power off and start** is selected in the **Allow users to reboot desktops** drop-down menu, desktops from this pool will have a **Restart** action.
    - If **Yes** is selected in the **Allow user to send IPMI reset** option and the desktop is IPMI-enabled, the desktops from this pool will have a **Hard Reset** action.

If a power control action is available, for example, if the user needs to restart their desktop, they open the kabob menu and select the **Restart** option, shown in the following figure. The selection in the **Allow users to stop/start desktops** drop-down menu in the user's policy determines if the restart is performed as a graceful reboot or as a forceful power off and start.



Desktops	Name	Power	Assignment
	kdg-1803	RUNNING	ASSIGNED
	kdg-rocky9	STOPPED	AVAILABLE

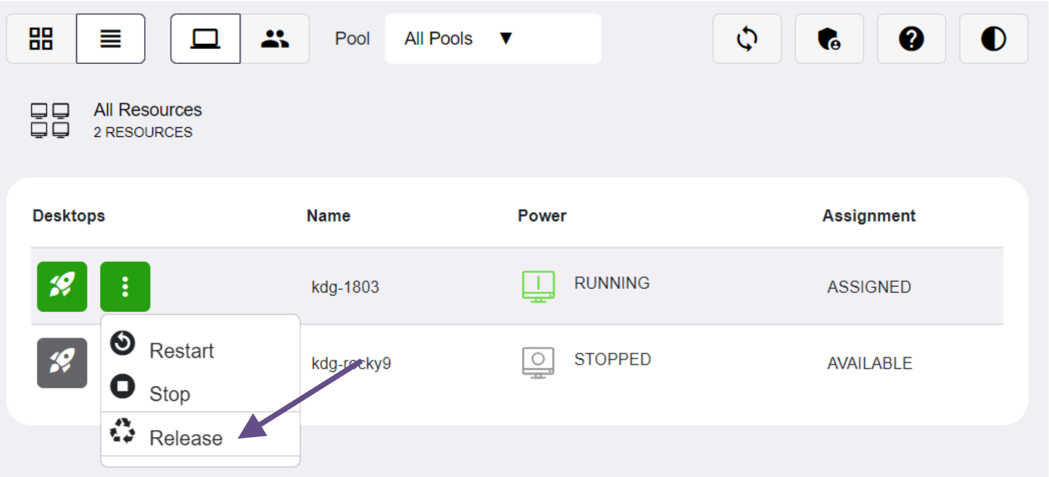
Releasing Desktops

The Connection Broker assigns a desktop to a user as soon as that user requests a connection to or powers on one of their offered desktops. As long as the desktop remains assigned to that user, it is not offered to any other user.

The Web client includes a **Release** option for any desktops that the user is allowed to release back to its pool. The user’s role and policy control which desktops provide the release action, as follows:

- The user’s role must select the **Allow user to manually release desktops** option.
- The user’s policy must *not* select the **Prevent user from manually releasing desktop** option**.**

If the user needs to release their desktop for any reason, open the kabob menu and select the **Release** option, as shown in the following figure for the list view.



Desktops	Name	Power	Assignment
	kdg-1803	RUNNING	ASSIGNED
	kdg-rocky9	STOPPED	AVAILABLE

The release plan associated with the desktop is invoked as soon as the desktop is released. If the user remains logged into the desktop after it is released, the Connection Broker considers that user as *rogue*.

Customizing the Web Client Message Board

By default, the Leostream Web client contains a message board on the right-hand side of the page. You can change the contents of the message board, or hide the Message Board for all Connection Broker users.

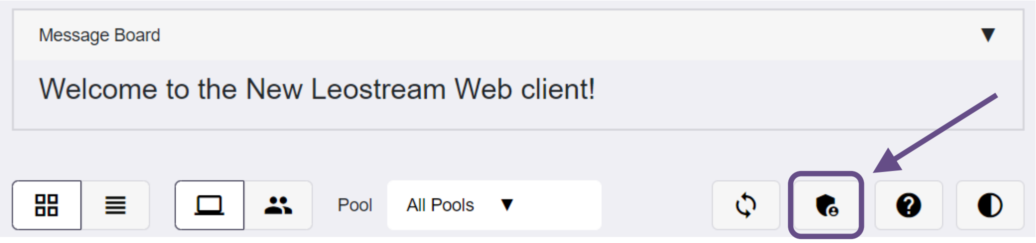
For information on modifying the contents of the message board, see **Setting Message Board Text**.

To remove the message board from the Web client:

1. In the Connection Broker Administrator Web interface, go to the **> System > Settings** page.
2. In the **Web Browser Configuration** section, uncheck the **Show Message Board in Web Client** option.
3. Click **Save**.

Opening the Administrator Web Interface

If the user's role provides access to the Connection Broker Administrator Web interface, the Web client includes an **Open Administrator View** button, shown in the following figure.


Message Board

Welcome to the New Leostream Web client!

Clicking this button opens a second Leostream session for the user, in a new tab, with access to the Administrator Web interface.

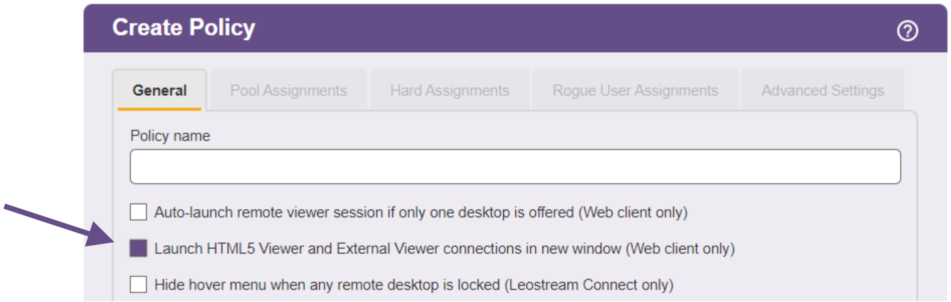
If the user is assigned a single resource and their policy is configured to automatically launch that resource, the user cannot access the **Open Administrator View** link.

The Administrator Web interface shows only the pages the user's role allows them to access. See **Administrator Web Interface Permissions** for a complete description of setting up access permissions to the Administrator Web interface.

Launching Connections in New Windows

By default, a user's desktop connection is launched in the same browser window as their list of resources. If you are using in-browser connections and the user is offered multiple resources, you can allow them to connect to multiple resources by opening each connection in a new browser window, as follows.

1. Edit the user's policy.
2. At the top of the **Edit Policy** page, select the **Launch Leostream HTML5 Viewer and External Viewer connections in new window** option, shown in the following figure.



Policy name

☐ 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)

3. To configure the appearance of the new window, edit the user's protocol plan.
4. For external viewers, use the **Parameters for connections opened in new window** edit field to

configure the appearance of the new window.

The Connection Broker uses the Javascript `window.open` function to launch the new window. For a list of parameters, see:

http://www.w3schools.com/jsref/met_win_open.asp
Enter parameters as a comma-separated list, for example:

```
left=0,height=500,width=700,toolbar=1,status=1
```

Setting URL for User Logout

By default, when the user logs out of the Leostream Web client, they return to the Connection Broker **Sign in** page. Use the **URL redirect on user logout** edit field on the **> System > Settings** page to specify a different Web page for users to visit when they log out of the Leostream Web client.

Supported Display Protocols for Web Client Access

Your Leostream license controls which display protocols you may use. Please, contact **sales@leostream.com** if you require access to protocols that are not currently displayed in your protocol plans.

Users who log in using the Leostream Web client can connect to their remote desktop using any of the following display protocols:

- HP ZCentral Remote Boost (RGS)
- Microsoft RDP and RemoteFX
- Leostream HTML5 RDP, VNC, and SSH viewer
- Mechdyne TGX
- Amazon DCV (client-based or HTML5-based)
- NoMachine (client-based or HTML5-based)
- PCoIP
- Penguin Computing Scyld Cloud Workstation (client-based or HTML5-based)
- Scale Logic RAP – VDI (client-based or HTML5-based)
- VNC
- External viewer – third party viewers that can be accessed via a URL

Use the **Web Browser** section of the protocol plan to determine which display protocol is used for the user's desktop connection. The settings in the **Priority** drop-down menus indicate the order in which the Connection Broker uses the display protocols when connecting to a desktop. The **Configuration file** then configures the display protocol settings.

For more details on different display protocols, see the Leostream Guide for **Working with Display Protocols**.

Using the Leostream Gateway and HTML5 RDP Viewer

The Leostream Gateway provides clientless access to remote resources using an HTML5 RDP, VNC, or SSH. When used with cloud environments such as OpenStack, AWS, and Azure, the Leostream Gateway allows you to isolate virtual machines on private networks. The Leostream Gateway then provides secure access to these virtual machines.

For complete instructions on installing and working with the Leostream Gateway, please see the **Leostream Gateway Guide** available on the Leostream Web site.

Using External Viewers

The **External viewer** option allows you to enter HTML or a URL to any third-party remote viewer that can be launched from a Web browser. The external viewer option is useful when building a protocol plan for users connecting through an SSL VPN device or for users that need to launch other URL based protocols, such as SSH or VMware View.

To launch an external viewer, set the **Priority** drop-down menu associated with **External Viewer** to `1`. Optionally, to return the user to a particular URL when the user logs out, enter the URL in the **URL redirect on user logout** edit field.

By default, the external viewer launches in the same window that displays the user's list of offered resources. For instructions on launching the viewer in a new browser window, see **Adding a New Policy and Configuring General Policy Options**.

External Viewer URLs

In the **Configuration file** edit field, enter the URL that redirects the user to the external viewer. The Connection Broker reaches out to the external server to run the URL.

Entering HTML-Code for External Viewers

In the **Configuration file** edit field, enter HTML code that redirects the user to an external viewer. The Connection Broker returns the HTML to the user.

Launching SSH, VMware View, and FTP as External Viewers

The Connection Broker recognizes a limited number of clients with Uniform Resource Indentifier (URI) schemes. If the Connection Broker recognizes the URI, the Connection Broker evaluates the URL entered into the **Configuration file**, instead of returning the URL to the user. In particular, you can use this functionality to launch the following connection types from the Leostream Web client.

- FTP
- SSH
- VMware View – for desktops with an installed VMware Horizon View Direct-Connection Plug-In

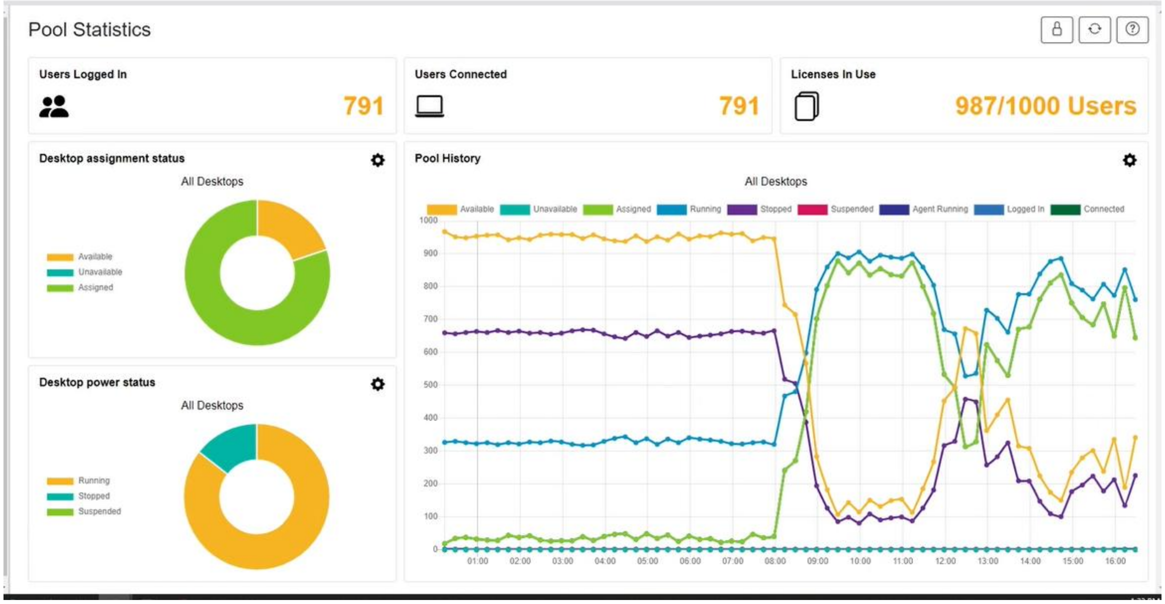
Use dynamic tags when constructing the URLs to ensure that the Connection Broker establishes the connection to the correct resource. For example, enter the following code into the **Configuration file** for the **External Viewer** to launch VMware View.

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

Chapter 16: Monitoring the Connection Broker

Using the Statistics Dashboard

The **> Dashboards > Statistics** page, shown in the following figure, provides an overview of user connections, desktop statuses, and license usage.



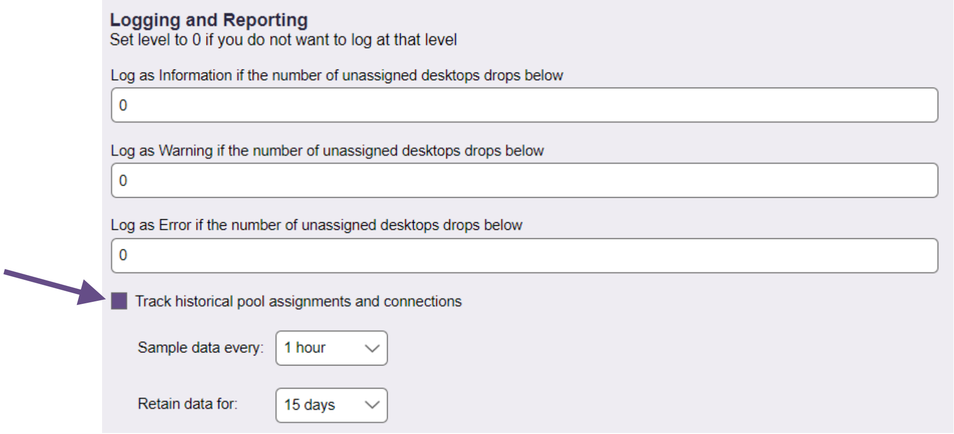
Pool Statistics

Users Logged In 791

Users Connected 791

Licenses In Use 987/1000 Users

Pool statistics are available only for pools that track historical pool usage. To enable tracking or to modify how often data is collected and how long it is retained, edit each pool in your environment and select the **Track historical pool assignments and connections** option, shown in the following figure.



Logging and Reporting
Set level to 0 if you do not want to log at that level

Log as Information if the number of unassigned desktops drops below
0

Log as Warning if the number of unassigned desktops drops below
0

Log as Error if the number of unassigned desktops drops below
0

☑ Track historical pool assignments and connections

Sample data every: 1 hour

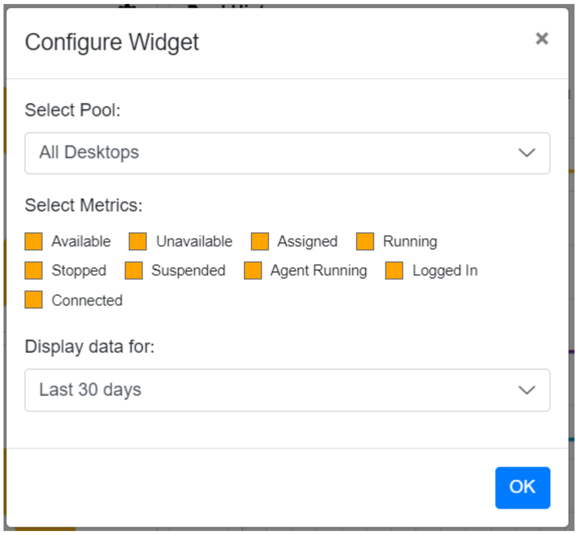
Retain data for: 15 days

Set the **Sample data every** and **Retain data for** values appropriately based on the amount of information you want to store and how often desktop states (such as assignments or power states) change. See **Collecting Pool Statistics to Track Desktop Usage** for more information.

Charting Pool Histories

The **Pool History** graph plots pool statistics over time. You can use this chart to look at trends in user assignments, desktop power states, or any of the other available statistics.

To manipulate the pool history chart, click the Gear icon at the top-right of the chart to open the following configuration dialog.


Configure Widget

Select Pool: All Desktops

Select Metrics:

☑ Available ☑ Unavailable ☑ Assigned ☑ Running
☑ Stopped ☑ Suspended ☑ Agent Running ☑ Logged In
☑ Connected

Display data for: Last 30 days

- The **Select Pool** drop-down menu allows you to select which pool to display. Only one pool may be charted at a time. The drop-down contains all pools in your Connection Broker, even if the pool is not tracking historical pool usage. The chart is empty if you select a pool that does not track pool usage.

- The **Select Metrics** check boxes determine which statistics are displayed. Check or uncheck options to change which metrics are plotted.

- Select a time range from the **Display data for** drop-down menu.

  When viewing the **Pool History** chart, you can use your mouse wheel to change the time period shows on the X-axis, however this does not replot the data. Use the **Refresh Data** button at the top-right of the Dashboard to redraw the charts if you zoom out beyond the originally displayed time period.

Charting Pool sizes

The **Pools** widget displays a bar chart based on the number of desktops in the pool. Click the gear at the top-right of the widget to indicate the pools you want to chart. You can then compare the size and usage of various pools side-by-side.

Displaying Desktop Statuses

The **Desktop Assignment Status** and **Desktop Power Status** charts summarize the assignment and power statuses of the desktop in the pool selected in the **Pool** drop-down menu.

For each chart, when all three metrics are displayed the chart includes the status of every desktop in the pool.

- Desktop assignments: Total in pool = Number Available + Number Unavailable + Number Assigned

  If Unavailable desktops are also assigned to users, the total number of desktops shown in the chart will exceed the actual number of desktops in the pool.

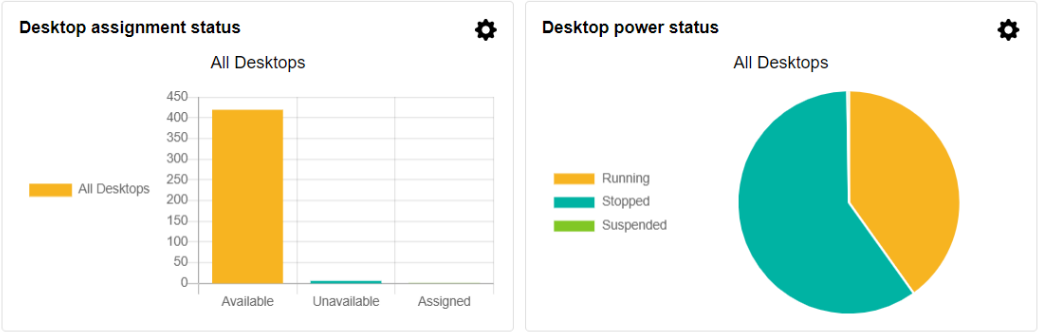
- Desktop Power Status: Total in pool = Number Running + Number Stopped + Number Suspended

Click the Gear icon at the top-right of each chart to customize the data shown on the chart.

- The **Select Pool** drop-down menu allows you to select which pool to display. Only one pool may be charted at a time.

- The **Select Metrics** check boxes determine which statistics are displayed. Check or uncheck options to change which metrics are plotted.

- The **Select Chart Type** drop-down menu allows you to change the default donut chart into a bar or pie chart, for example:



Monitoring License Use and User Statuses

The **Users Logged in**, **Users Connected**, and **Desktops Assigned** metrics do not rely on historical tracking. The values displayed in these fields are calculated when you open the **> Dashboards > Statistics** page.

The Connection Broker does not refresh the values in real time. To see if the values changed after you opened the page, click the Refresh icon ⟳ at the top-right of the Dashboard to update the data.

When the number of logged in users I greater than the number of connected users, some of your users have disconnected from their remote desktops without logging out of the remote operating system. You can use the columns on the **> Resources > Desktops** page to determine which users are connected and logged in, as follows.

- Display the **Logged In** column and filter by desktops with a value of **Yes**. This is the number of logged in users. You can then use the **Logged In User** column to see which user is logged into each desktop.

- Use the **Connected** column to see which logged in users are still connected to their remote desktop. If the value in this column is **No**, the user logged into their desktop then disconnected from the desktop without logout out.

The **Licenses in use** metric indicates how many of your current user or desktop licenses are currently consumed. You can find more detailed license information on the **> System > Maintenance** page.

To see license usage over time, add the **License History** widget using the instructions in the following section.

Updating the Dashboard Layout and Contents

Click the **Lock** icon at the top-right of the Dashboard to unlock the Dashboard layout and enable moving, adding, removing, and resizing dashboard widgets. After the Dashboard is unlocked, you can modify the dashboard, as follows.

- Click and hold on the bottom-right corner of any widget to resize the chart
- Click and hold in the center of the widget to drag it to a new location
- Click the X at the top-right of a widget to remove it from the Dashboard
- Click the plus (+) at the top-right of the dashboard to add a new widget to the Dashboard

To revert back to the factory default layout, click the **Reset** button at the top-right of the Dashboard.

Searching for Connection Broker Objects

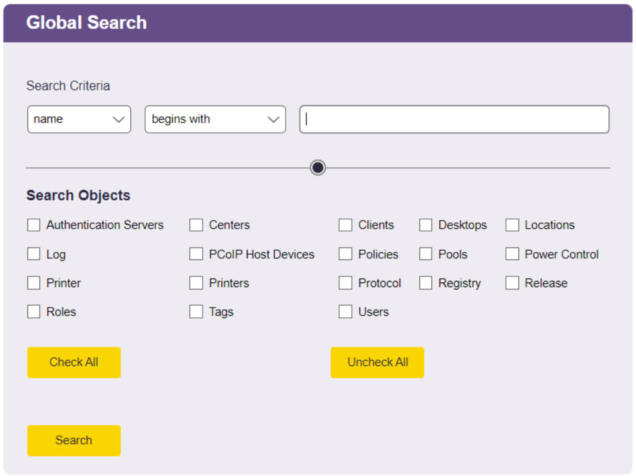
You can search for particular objects in Connection Broker tables, such as desktops and users, using the following two methods.

- The global search page scans all tables, searching for all objects with common names, notes, or users

- The per-page search focuses on a single table, searching for particular object types

Global Search

The **> System > Search** tab, shown in the following figure, allows you to locate particular objects within the Connection Broker.



name | begins with

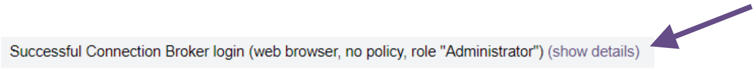
You can search for objects based on the following object attributes.

- **Name**: All Connection Broker objects have a name. The name is displayed in the **Name** column of any Connection Broker table, for example, the **Name** column on the **> Resources > Desktops** page.

  When searching the **> System > Logs** page, the name corresponds to the contents of the **Description** column.

- **Notes**: All Connection Broker objects allow you to include notes.

  When searching the **> System > Logs** page, the notes field corresponds to the contents shown when you expand the **show details** link, shown below.



Successful Connection Broker login (web browser, no policy, role "Administrator") (show details)

For other Connection Broker objects the name and notes fields are displayed in the **Edit** form for that object, as shown, for example.

- **User**: Only desktop objects and log entries have an associated user. The user corresponds to the name of the user that is currently assigned to that desktop or is the subject of the log entry, as displayed in the **User** column on the **> Resources > Desktops** page or **> System > Log** page, respectively.

Use the **Search Criteria** section to define the type of search. For example, to search for all objects with a name that starts with `qa`:

1. Select **name** from the first **Search Criteria** drop-down menu.
2. Select **begins with** from the second **Search Criteria** drop-down menu.

   When the search criteria is set to **is equal to** *and* you are using an internal Connection Broker database, the search string is case sensitive. If you are using a Microsoft® SQL Server® database, an

is equal to search is *not* case sensitive.

3. Type `qa` into the **Search Criteria** edit field.

4. Click **Check all** to select all objects in the **Search Objects** section. To search only for particular objects, click **Uncheck All** and select the individual objects.

5. Click **Search**.

The search results display the object type and name. The entries in the **Name** column of the search results are hyperlinks that go to one of the following two locations.

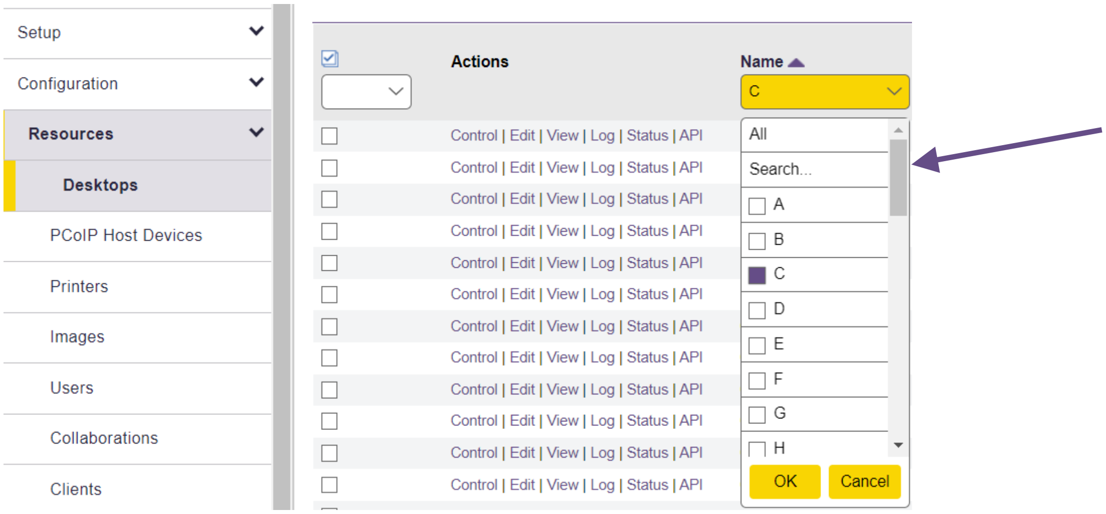
- If the entry in the **Object** column is **Log**, click on the entry in the **Name** columne to display additional information about that log entry.
- If the entry in the **Object** column corresponds to any other entity, such as a pool or policy, click on the entry in the **Name** column to go to the **Edit** form for that object.

Per-Page Search

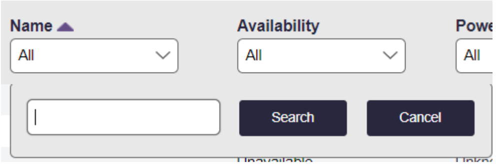
You can quickly search for objects in a particular Connection Broker table using the local search functions provided on each page. Each table allows you to search for objects based on the contents of any column that is filtered based on alphabet, for example, the **Name** or **Machine Name** columns on the **> Resource > Desktops** page.

To search for objects on a page:

1. From the filter drop-down menu associated with the column you want to search based on, select the **Search** option, as shown in the following figure.



2. In the search edit field that opens, enter the text to search for. For example, the following search will look for desktops with a name that begins with `qa`.



By default, the Connection Broker searches for objects that *begin with* the entered text. You can use the following wildcards to modify the search.

The percent (%) wildcard matches any character string. For example:

QA% searches for any string that begins with QA
%DEV% searches for any string that contains DEV
%PROD searches for any string that ends with PROD and does not contain trailing blanks

The underscore wildcard (_) matches any one character in a fixed position. For example:

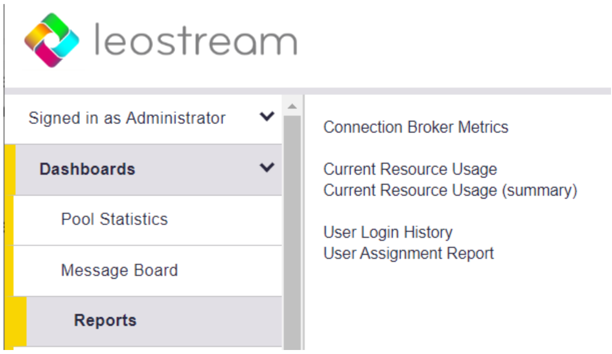
_EE_ searches for any four-letter string whose two middle characters are EE
%DEV_TEST% searches for any string that contains the pattern DEV_TEST. The strings DEV_TEST1, MYDEV-TEST, and MY-DEV-TEST2 all match this pattern.

3. Click **Search** to perform the search. The filter drop-down menu for that column now contains the text you entered for your search, and the contents of the table shows the results.

4. To change the contents of the table, change the selection for the filter drop-down menu. The filter table contains your search string until you select another filter and navigate away from the page.

Generating Connection Broker Reports

The Connection Broker provides a set of predefine reports on resource usage. Go to the **> Dashboards > Reports** page to view the available reports, as shown in the following figure.



Each report is a static snapshot of the specified information, at the time the report is generated.

- Connection Broker metric reports allow you to monitor the performance of each Connection Broker in a cluster
- Resource usage reports list the users and desktops currently assigned by the Connection Broker
- The history reports track resource usage over time.

You can download many of the reports to a CSV-file by clicking the **Export list** link at the top-right of the report.

Reporting Connection Broker Metrics

Connection Broker metrics provide information on disk space, load average, etc., for the Connection Brokers in your cluster. The reported metrics are configured on the **> Dashboards > Connection Broker Metrics** page, and the report generated using the **Connection Broker Metrics** link on the **> Dashboards > Reports** page. See the following sections for more information on configuring and generation this report.

The Connection Broker collects seven default types of metrics:

- Used disk space
- Free disk space
- Used memory
- Available memory
- Load average in the last minute
- Load average in the last 5 minutes
- Load average in the last 15 minutes.

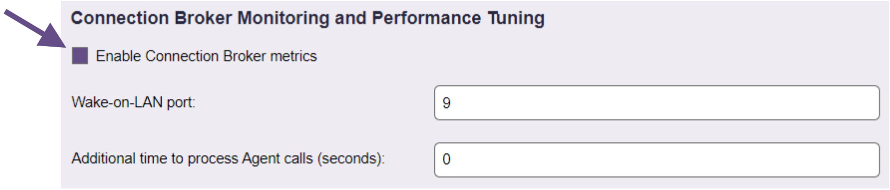
These metrics are collected at intervals configured on the **> Dashboards > Connection Broker Metrics** page for as long as the Connection Broker has a valid heartbeat. The `heartbeat` job checks the status of each Connection Broker in the cluster every five minutes. If a Connection Broker skips two heartbeats, the report no longer contains metrics for that Connection Broker. When the heartbeat resumes, the Connection Broker reappears in the report.

Generating Connection Broker Metrics Reports

In order to generate a Connection Broker Metrics Report, you must enable metrics collection, as follows.

1. Go to the **> System > Settings** page.

2. Select **Enable Connection Broker metrics** in the **Connection Broker Monitoring and Performance Tuning** section, shown in the following figure.



Connection Broker Monitoring and Performance Tuning

■ Enable Connection Broker metrics

Wake-on-LAN port: 9

Additional time to process Agent calls (seconds): 0

3. Click **Save**.

If your Connection Broker is running stand-alone, i.e., not in a cluster, the broker automatically begins collection metrics for itself. If the Connection Broker is part of a cluster, the broker must first restart all other Connection Brokers in the cluster before it can begin collecting metric data.

After Connection Broker metrics are being collected, you can generate a report on the **> Dashboards >**

Reports page. Click the **Connection Broker Metrics** link to generate the report.

For each Connection Broker with a valid heartbeat, the report indicates the time the metric was last collected and its value, along with the overall peak and average value for the metric. The time of the **Last heartbeat** indicates the last time a valid heartbeat was returned by this Connection Broker.

A Connection Broker may skip a heartbeat for any of the following reasons.

- The Connection Broker is shutdown
- The Connection Broker was removed from the cluster by pointing it to another database
- The Connection Broker work queue has stalled.

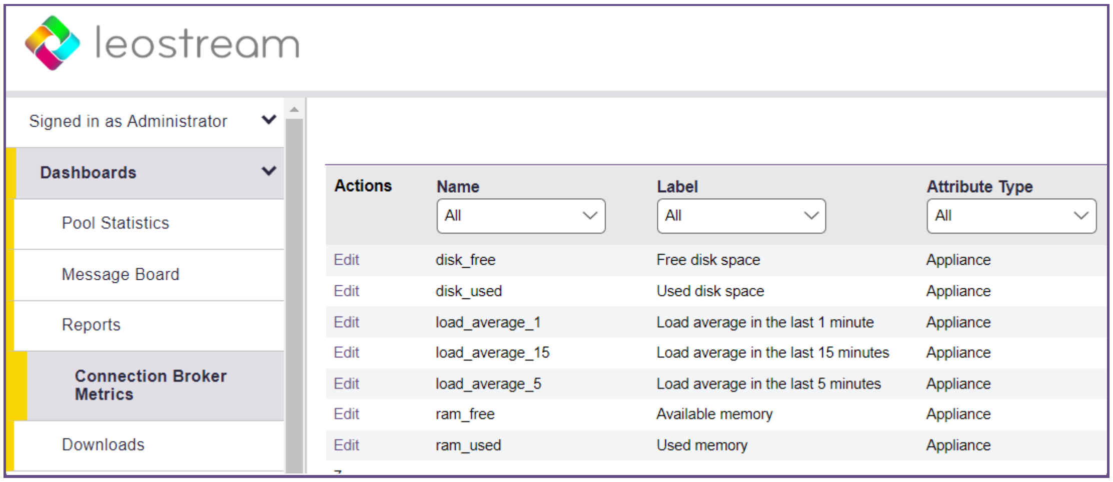
If a Connection Broker skips two heartbeats, and the Connection Broker is not marked as **Stopped**, the status for that Connection Broker changes to **Unavailable**. Connection Brokers that are stopped or unavailable can be hidden from the report by clicking the **Do not display** link.

You can return hidden Connection Brokers to the report by clicking the **Show all Connection Broker in this report** link at the top of the Connection Broker Metrics report.

Load average is a measure of CPU. It is a statistical concept, similar to a moving average, which shows how many processes had to wait for the Connection Broker processor to execute their jobs over the selected time interval. Different load average values indicate the Connection Broker responsiveness. For example, a load average of 8-10 may indicate that the Connection Broker CPU is becoming moderately busy, and that there will be a delay in processing jobs.

Configuring Connection Broker Metrics

You configure how often Connection Broker metrics are collected, how long data is retained, and if logging events should occur on the **> Dashboards > Connection Broker Metrics** page, shown in the following figure.



Actions	Name	Label	Attribute Type
	All	All	All
Edit	disk_free	Free disk space	Appliance
Edit	disk_used	Used disk space	Appliance
Edit	load_average_1	Load average in the last 1 minute	Appliance
Edit	load_average_15	Load average in the last 15 minutes	Appliance
Edit	load_average_5	Load average in the last 5 minutes	Appliance
Edit	ram_free	Available memory	Appliance
Edit	ram_used	Used memory	Appliance

To configure a particular metric, click the **Edit** action associated with that metric.

- To modify how often the metric is collected, select a new item from the **Frequency** drop-down menu.

- To modify how long the data is retained, select a new item from the **Days to retain attribute information** drop-down menu.

- To stop collection this particular metric, uncheck the **Collect** option.

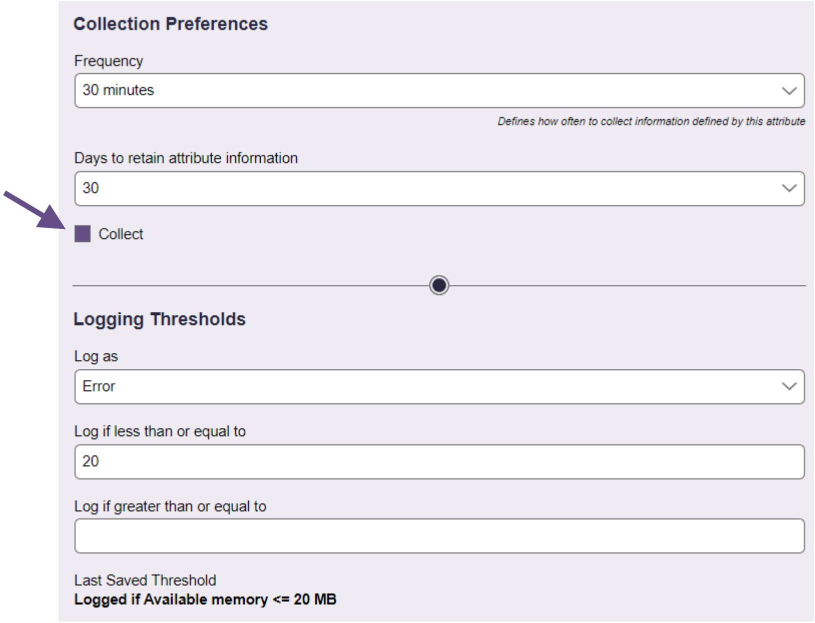
- If the **Collect** option is selected, use the **Logging Thresholds** section to trigger logging events that can be monitored with SNMP and syslog servers.

The Connection Broker changes the collection schedule as soon as you click **Save**. The next scheduled collection for that metric will be determined by the frequency, offset from the current time.

Logging Connection Broker Metric Thresholds

You can instruct the Connection Broker to log events when any of the Connection Broker metrics exceed a specified threshold. On the **Dashboards > Connection Broker Metrics** page, edit the desired metric and use the **Logging Thresholds** section, shown in the following figure, to turn on logging and specify the thresholds.

The **Collect** checkbox indicated in the following figure must be selected in the **Collection Preferences** section for the **Logging Thresholds** section to appear.



Collection Preferences

Frequency: 30 minutes

Defines how often to collect information defined by this attribute

Days to retain attribute information: 30

☑ Collect

Logging Thresholds

Log as: Error

Log if less than or equal to: 20

Log if greater than or equal to:

Last Saved Threshold
Logged if Available memory <= 20 MB

The setting in the **Log as** drop-down menu indicates what type of event the Connection Broker should log, either: information, warning, or error. Set the **Log as** drop-down menu to **No Logging** to disable logging for this metric.

When logging is enabled, use the **Log if less than or equal to** and **Log if greater than or equal to** edit fields to set upper and lower bounds on the logging threshold. For example:

- If **Log if less than or equal to** is set to 5 and **Log if greater than or equal to** is set to 10, the

Connection Broker logs the selected event whenever the metric is less than or equal to 5 OR greater than or equal to 10.

- If **Log if less than or equal to** is set to 10 and **Log if greater than or equal to** is set to 5, the Connection Broker logs the selected event whenever the metric is greater than or equal to 5 AND less than or equal to 10

You can use logging event to trigger SNMP traps or in conjunction with syslog servers, to monitor the Connection Broker health. See **Issuing SNMP Traps** and **Integrating with Syslog Servers** for more information.

Reporting Resource Usage

The **Resource Usage** report lists the different desktops that are currently policy-assigned or hard-assigned to an end user.

The **Resource Usage** report contains a snapshot at the time the report is generated and is not dynamically updated. To view trends in resource usage, periodically run the report, download the report to a CSV-file, and use a third-party tool to analyse the files.

The columns in this report provide the following information.

User Name: Name of the user assigned to the resource.

Authentication Server: The authentication server used to authenticate the user when they initially logged into the Connection Broker.

Organization Unit: The user’s OU, if applicable

Client: The name of the client device where the user logged into the Connection Broker.

Policy: The policy that the Connection Broker assigned to the user when they logged into the broker. Policy does not apply to hard-assigned desktops.

Assignment Mode: The method used to assign the resource to the user; either policy-assigned or hard-assigned.

Protocol Type: The display protocol used to connect to this resource.

Role: The role assigned to the user by the authentication server that the Connection Broker used to authenticate the user.

Resource: The name of the assigned resource.

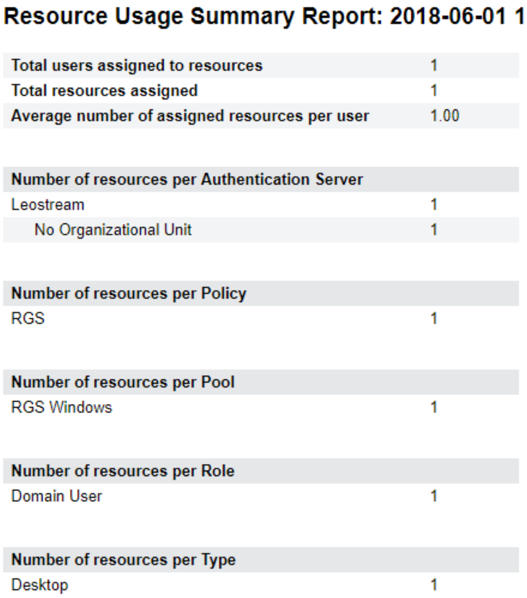
Pool: The pool from which the assigned resource was taken.

User Status: The user’s status, either **Assigned** or **Signed In**. A status of **Signed In** indicates that the user is actively logged into the resource. A user may be assigned a resource but not actively signed into that resource, for example, if the user disconnects from the resource and their policy leaves them assigned to the desktop upon disconnect.

Generating Resource Usage Summary Reports

The **Resource Usage (summary)** report gives an overview of the number of assigned resources, and their source. The **Resource Usage (summary)** report contains a snapshot at the time the report is generated and is not dynamically updated.

The following figure shows an example **Resource Usage (summary)** report.



Resource Usage Summary Report: 2018-06-01 15:08:16

Total users assigned to resources	1
Total resources assigned	1
Average number of assigned resources per user	1.00

Number of resources per Authentication Server	
Leostream	1
No Organizational Unit	1

Number of resources per Policy	
RGS	1

Number of resources per Pool	
RGS Windows	1

Number of resources per Role	
Domain User	1

Number of resources per Type	
Desktop	1

The sections in this report provide the following information.

Total users assigned to resources: The number of users assigned to a desktop in the Connection Broker. Users may not be actively logged into the assigned resource.

Total resources assigned: The number of resources assigned to all users. This number is not an indication of license use. Users assigned to multiple resources consume a single Connection Broker license.

Average number of assigned resources per user: Total users assigned to resources divided by total resources assigned.

Number of resources per Authentication Server: The number of resources assigned to users in each authentication server. This number can show which authentication servers contains users that are more actively using the Connection Broker. If applicable, the report shows an indented list of these users’ organizational units. The total number of indented resources equals the number of resources for the authentication server, as a whole.

Number of resources per Policy: The number of resources that are assigned by each policy.

Number of resources per Pool: The number of resources that are assigned from each pool. This number can show pools that are more heavily loaded with users.

Number of resources per Role: Number of resources assigned to users with various Connection Broker roles.

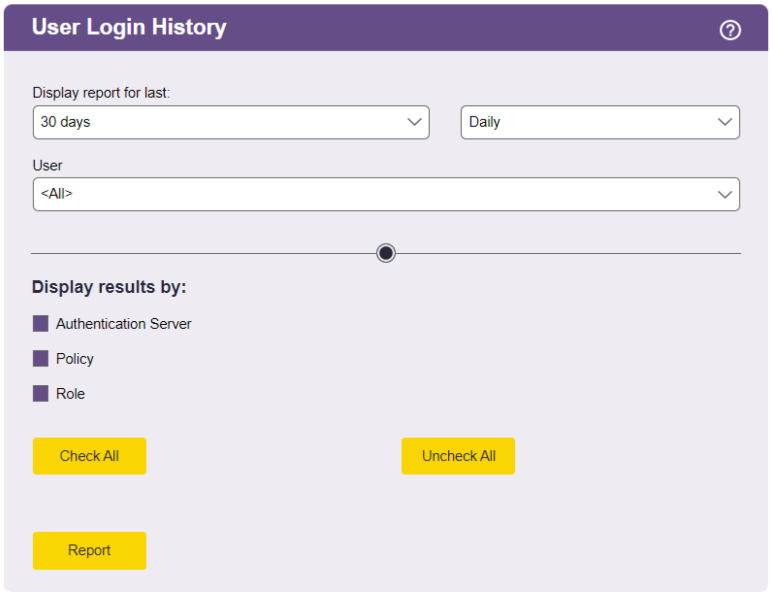
Number of resources per Type: Number of desktops assigned to users. The total equals the value for **Total resources assigned**.

User Login History Reports

User login histories indicate the number of users that logged in to the Connection Broker over a specified period of time, and indicate:

- When peak login times occur
- The overall load on your system
- How often and when individual users log in

To generate a user login history report, click the **User Login History** link on the **> Dashboards > Reports** page. The **User Login History** form, shown in the following figure, opens.



User Login History

Display report for last:
30 days
Daily

User
<All>

Display results by:

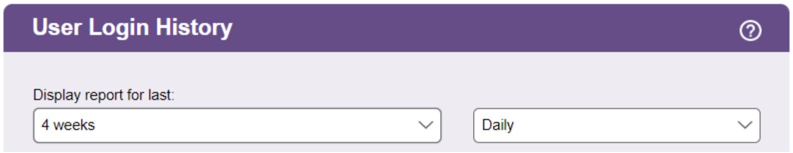
■ Authentication Server
■ Policy
■ Role

The **User Login History** form allows you to configure the time period, frequency, and display parameters for the report, as follows.

1. From the first **Display report for last** drop-down menu, select the length of history to display.

2. From the second **Display report for last** drop-down menu, select the time interval for grouping information.

   For example, the configuration for the **Display report for last** drop-down menus in the following figure results in a weekly report for the last four weeks.



User Login History

Display report for last: 4 weeks | Daily

3. To list Connection Broker logins for a particular user, select that user from the **User** drop-down menu. Select **<All>** do display an overview of all user activity.
4. Use the options in the **Display results as** section to select summary tables to generate.

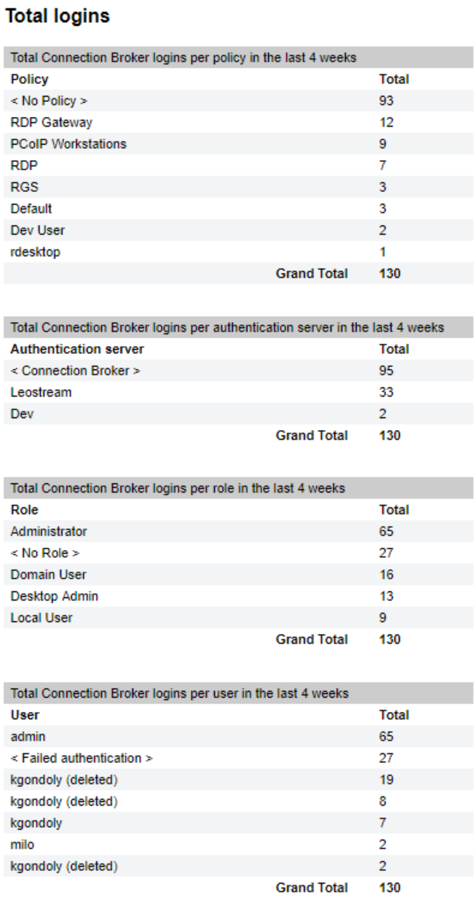
    a. **Authentication Servers:** Summarizes the number of user logins that were authenticated in each defined authentication server.

    b. **Policy:** Summarizes the number of times each policy was assigned to a logged in user.

    c. **Role:** Summarizes the number of times each role was assigned to a logged in user

5. Click **Report** to generate the report.

Any generated summary tables appear after the history. The following figure displays an example summary for authentication servers, policies, roles, and user. A per-user summary is always displayed and shows the total number of logins for each user over the selected time period.



Total logins

Total Connection Broker logins per policy in the last 4 weeks	
Policy	**Total**
< No Policy >	93
RDP Gateway	12
PCoIP Workstations	9
RDP	7
RGS	3
Default	3
Dev User	2
rdesktop	1
Grand Total	**130**

Total Connection Broker logins per authentication server in the last 4 weeks	
Authentication server	**Total**
< Connection Broker >	95
Leostream	33
Dev	2
Grand Total	**130**

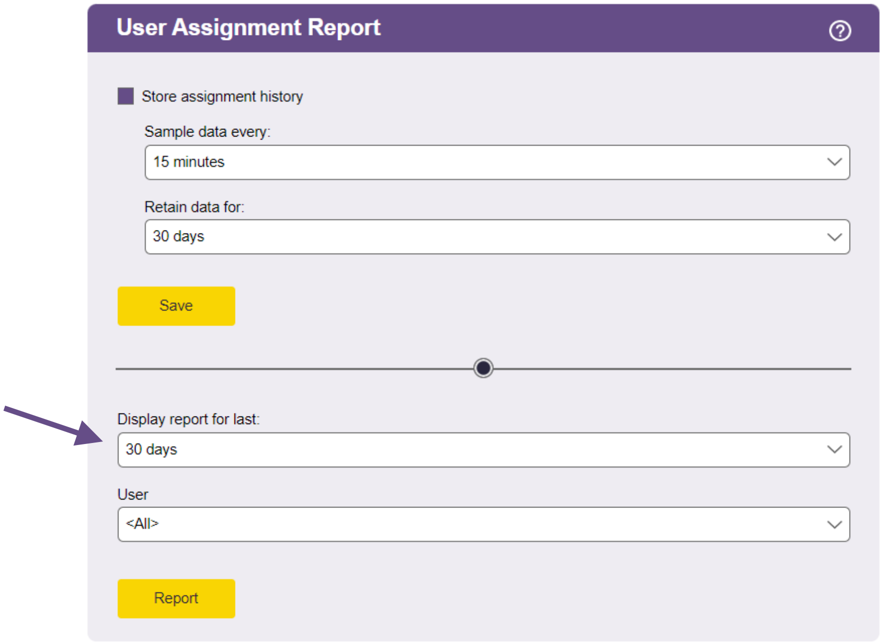
Total Connection Broker logins per role in the last 4 weeks	
Role	**Total**
Administrator	65
< No Role >	27
Domain User	16
Desktop Admin	13
Local User	9
Grand Total	**130**

Total Connection Broker logins per user in the last 4 weeks	
User	**Total**
admin	65
< Failed authentication >	27
kgondoly (deleted)	19
kgondoly (deleted)	8
kgondoly	7
milo	2
kgondoly (deleted)	2
Grand Total	**130**

Generating User Assignment Reports

User assignment reports compile information on which users were assigned to which desktops and how long the assignment was in place. The report includes the time the assignment started, ended, and its duration.

To generate a report, select a timeframe from the **Display report for last** drop-down menu, indicated in the following figure, and opt to display the assignments for all users or for only the user selected in the **User** drop-down menu.



User Assignment Report

☑ Store assignment history

Sample data every: 15 minutes

Retain data for: 30 days

Display report for last: 30 days

User

<All>

Use the **Export list** link at the top-right of the report to download a CSV-file of the results for further analysis.

The data available for the report depends on the state of the **Store assignment history** option.

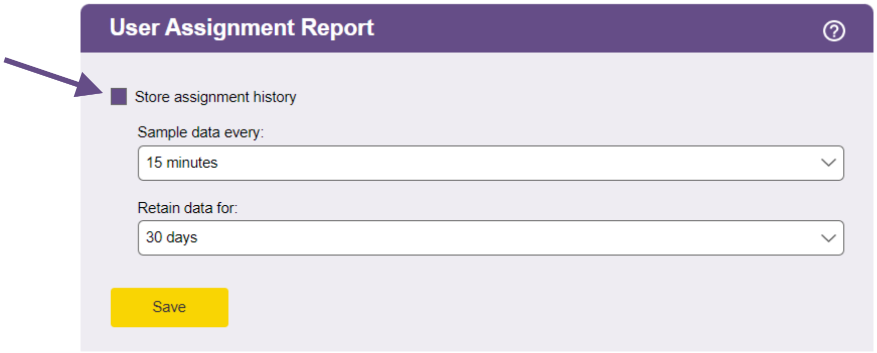
- If this option is unchecked, the report is generated based on information derived from messages in the **> System > Log** page. The duration of information available to display is determined by the value you set for the **Days to retain log entries** option in the **Log Settings**.

- If the option is checked, the report is generated using the information stored in the assign_log table in your Connection Broker database. The duration of information available to display is determined by the value you set for the **Retain data for** option. See **Storing User Assignment History** for more information.

Storing User Assignment History

In addition to generating user assignment reports within your Connection Broker, you can store the assignment history in your Connection Broker database for use with external reporting tools.

Check the **Store assignment history** option, shown in the following figure, to begin storing assignment information in the `assign_log` table in your Connection Broker database.



When this option is first selected, the Connection Broker analyses the messages in the **> System > Log** table to populate the assign_log with as much data as possible, based on the requested duration set in the **Retain data for** drop-down menu. For example, if you request 60 days of data in the **Retain data for** drop-down menu, but only retain data in the logs for 30 days, the assign_log initially contains 30 days of data.

The Connection Broker then schedules the sample_assign_log command in the job queue, to sample desktop assignment data at the rate specified in the **Sample data every** drop-down menu. This job updates the assign_log table to add or update assignments whose state has changed since the last sample time.

The fields in the assign_log are described in the Connection Broker database schema:

https://*cb-address*/download/account_db.html#assign_log

Where *cb-address* is your Connection Broker IP address or hostname.

The start_date field indicates when the assignment was first made. The event field indicates the event that triggered the latest update to the assignment. For example, a VM_RELEASE event indicates that that assignment was released and the end_date field then indicates when the release occurred.

The updated field indicates the last time the assignment information was sampled. If you query the table and the updated field is old, some assignment data may not reflect your current desktop assignments. Ensure that you set the **Sample data every** option to an appropriate value to track changes in your environment, based on your users' workflows.

A pool_id of -1 indicates the desktop was assigned to a rogue user. A pool_id of 0 indicates the desktop was hard-assigned to a user.

Integrating with Syslog Servers

The Connection Broker can function as a syslog sender, to forward log messages over the network. Integration with syslog servers allows for more effective compliance and auditing.

To enable the Connection Broker as a syslog sender:

1. Go to the **> System > Log** page.

2. Select the **Settings** link. The **Log Settings** form opens.

3. Select the type of messages to send to the syslog server from the **Events to Log** section. You can send some or all of the following:
   - Information
   - Warnings
   - Errors
   - Diagnostic

4. Select the **Enable syslog to remote host** option.

5. Use the **Forwarding protocol** radio buttons to indicate if the Connection Broker should send notifications to your syslog server using TCP or UDP. By default, the Connection Broker sends UDP traffic on port 514.

6. Enter the host name or IP address of your syslog server into the **Hostname or IP address** edit field. The change the default port, enter the address as:

   ```
   syslog_server_address:<port>
   ```

   To send notifications to multiple syslog servers, separate each entry by blank spaces or commas.

7. Click **Save**.

Beginning with Connection Broker version 2023.1, if your Connection Broker is part of a cluster, enabling syslog on one of the Connection Brokers in the cluster automatically enables syslog for all Connection Brokers in the cluster. If you are running an older Connection Broker version, you must individually enable syslog on each Connection Broker in your cluster.

The **Events to Log** section also defines the information shown in the Connection Broker logs (see **Customizing the Log Contents**).

Viewing the Connection Broker Log

The **> System > Log** page displays a log of Connection Broker activity. You can modify the columns included on this page by clicking the **Customize columns** link at the top of the page (see **Customizing Tables**).

The logs show the different stages of user connection, e.g., when a user signs in, is offered and assigned desktops, logs out, etc.

Using the logs, you can:

- Diagnose problems with your policy logic related to power and assignment controls, by looking at logs related to powering up and down desktops and releasing desktops back to the pool.
- Monitor the system load, such as the number of logins over a period of time.
- Monitor user access

Controlling the Log Time Zone

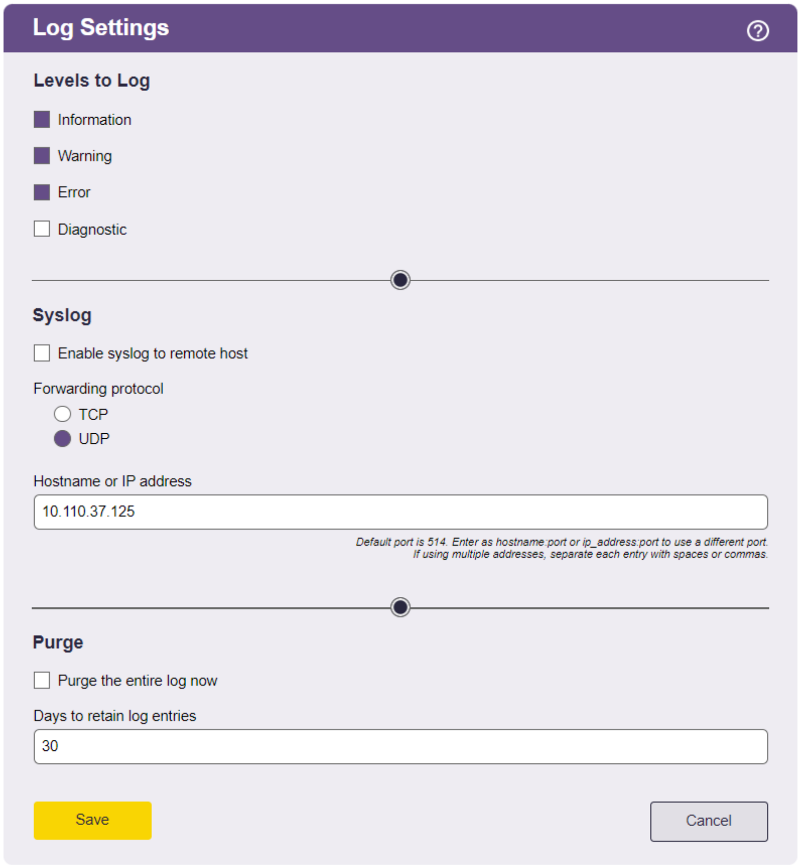
The Leostream Connection Broker takes its time zone from two sources, the time zone of the underlying operating system and the time zone of the Connection Broker database. Messages on the **> System > Log** page are shown in the time zone of your Connection Broker database. In a Connection Broker cluster, you can change the time zone for log messages by changing the time zone of your external database.

A downloaded Technical Support package, includes files in both time zones.

- Files with a `.log` extension are written in the Connection Broker operating system time zone
- Files that begin with `sql–` are written in the Connection Broker database time zone

Customizing Log Levels

To customize the type of events the Connection Broker logs, click the **Settings** link on the **> System > Log** page. Clicking on this link opens the **Log Settings** dialog, shown in the following figure. Select the events you want to log and click **Save**.



Log Settings

Levels to Log

☑ Information

☑ Warning

☑ Error

□ Diagnostic

Syslog

□ Enable syslog to remote host

Forwarding protocol

○ TCP

● UDP

Hostname or IP address: 10.110.37.125

Default port is 514. Enter as hostname:port or ip_address:port to use a different port.
If using multiple addresses, separate each entry with spaces or commas.

Purge

□ Purge the entire log now

Days to retain log entries: 30

7.

The **Syslog** section pertains to interacting with syslog servers (see **Integrating with Syslog Servers**)

Purging Connection Broker Logs

If your log files grow rapidly, you can purge the log file, as follows:

1. Click the **Settings** link on the **> System > Logs** page.
2. Select the **Purge the entire log now** option.
3. Click **Save**.

After you click **Save**, the Connection Broker wipes out the current log file and starts creating a new log with the items you selected in the **Log Settings** form.

If you do not manually purge the log file, the Connection Broker automatically purges the logs after 30 days. To change the automatic purge interval, enter a different number in the **Days to retain log entries** edit field.

Available Log Characteristics

Each row in the log provides some or all of the following information.

Agent Call UUID
The ID of the Leostream Agent call associated with the logged events. The same ID appears in the Leostream Agent log, allowing you to match messages in the Leostream Agent logs to those in the Connection Broker logs.

Authentication Server
Where applicable, the Connection Broker authentication server associated with this event.

Client
The client device associated with this log event, typically shown for login events.

Date
The date the entry was logged.

Description
A detailed account of the logged event. If available, click the **show details** link to expand the log entry.

Event
The category this log entry falls into. You can filter on events to create lists of activities, such as user login and logout (see **Filtering the Log List**). The Connection Broker reports the following types of events.

- Center scan
- Connection Broker alert
- Connection Broker login
- Connection Broker logout
- Connection Broker reboot
- Connection Broker shutdown
- Database backup

- Database restore
- Database switch
- Desktop Agent upgrade
- Desktop CPU utilization
- Desktop assign
- Desktop connect
- Desktop connect request
- Desktop connection close
- Desktop delete
- Desktop idle time
- Desktop lock
- Desktop offer
- Desktop pause
- Desktop protocol override
- Desktop provisioning
- Desktop reboot
- Desktop release
- Desktop release (manual)
- Desktop resume
- Desktop revert to snapshot
- Desktop start
- Desktop stop
- Desktop suspend
- Desktop unlock
- Desktop user disconnect
- Desktop user login
- Desktop user login (rogue)
- Desktop user logout
- Desktop user logout (rogue)
- Network start
- Network stop
- Object create
- Object delete
- Object update
- Pool out of resources
- Session expired

ID
The log message ID number, as stored in the log table in the Connection Broker database

Level
The log level for this entry, either: information, warning, or error. The log contains entries for the level selected on the **Log Settings** form.

Job Queue ID
The ID associated with the job queue entry that executed the job.

Object
The type of Connection Broker object that invoked the action logged in this entry.

Object name
The name of the object that invoked the action logged in this entry.

PID
The PID of the Apache process which made the log entry.

Policy
Where applicable, the Connection Broker policy associated with this event.

Pool
Where applicable, the Connection Broker pool associated with this event.

Protocol Plan
The protocol plan associated with this event.

Role
The Connection Broker role assigned to the user shown in the **User** column.

Site ID
The site ID associated with the Connection Broker that executed the job.

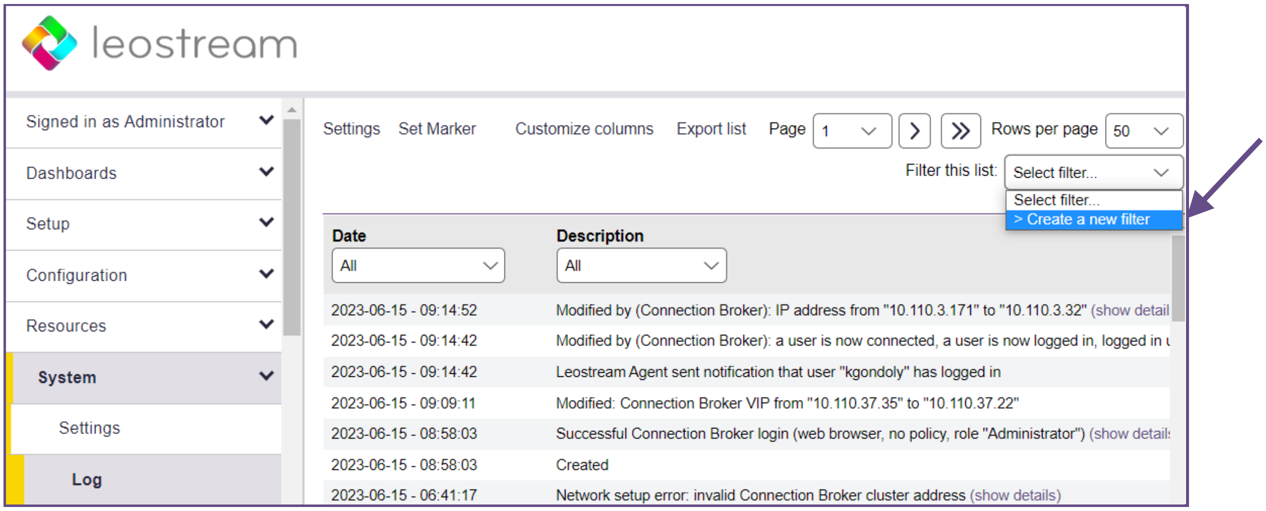
User
The user associated with this log event.

User Session ID
The session ID assigned to the user associated with this log event.

Filtering the Log List

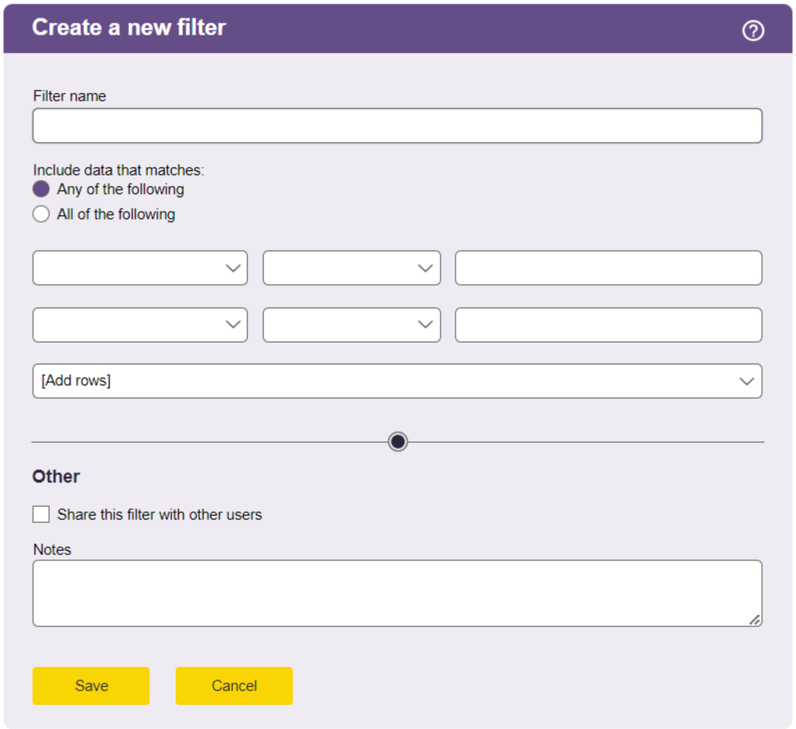
Log filters can be used to generate customized views for the logs, which can then be downloaded to a CSV-file. To create a log filter:

1. Select **Create a new filter** from the **Filter this list** drop-down menu, as shown in the following figure.



Date	Description
All	All
2023-06-15 - 09:14:52	Modified by (Connection Broker): IP address from "10.110.3.171" to "10.110.3.32" (show detail
2023-06-15 - 09:14:42	Modified by (Connection Broker): a user is now connected, a user is now logged in, logged in u
2023-06-15 - 09:14:42	Leostream Agent sent notification that user "kgondoly" has logged in
2023-06-15 - 09:09:11	Modified: Connection Broker VIP from "10.110.37.35" to "10.110.37.22"
2023-06-15 - 08:58:03	Successful Connection Broker login (web browser, no policy, role "Administrator") (show detail:
2023-06-15 - 08:58:03	Created
2023-06-15 - 06:41:17	Network setup error: invalid Connection Broker cluster address (show details)

The **Create a new filter** page opens, shown in the following figure.



Filter name

Include data that matches:
● Any of the following
○ All of the following

Other

□ Share this filter with other users

Notes

2. In the **Create a new filter** page, enter a descriptive name for your filter in the **Filter name** edit field.

3. Use the rows in the **Include data that matches** section to filter the displayed logs. You can filter the logs based on any number of log entry attributes.

4. If you specify multiple rows in the **Include data that matches** section, specify if the filter ANDs or ORs the rows together, as follows.

   a. Select **Any of the following** to perform an OR operation

   b. Select **All of the following** to perform an AND operation

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

To display only log entries that satisfy this filter, select the filter name from the **Filter this list** drop-down menu. Use global filters along with column-based filters to create customized list of log entries. You can then click the **Export list** link to download a CSV-file of the log list for analysis.

Using Logs to Track Connection Broker Configuration Changes

The Connection Broker generates log entries when certain Connection Broker configurations are changed, such as when editing a desktop or changing a pool setting. To view configuration changes, filter the logs based on one of the following events.

- `Object create`
- `Object delete`
- `Object update`

An `Object update` event can be triggered by any of the following:

- The object is manually edited in the Connection Broker Administrator Web interface
- The object is updated in the Connection Broker database
- A center scan updates the object
- The Leostream Agent reports a change that causes the object to be updated

The entry in the **Users** column indicates which user made the configuration change. Changes that were automatically made by the Connection Broker, such as changes made to a client when a user logs into the Connection Broker from that client, show **Connection Broker** in the **Users** column.

Exporting the Log Contents

You can extract the contents of the Connection Broker log in a number of ways:

- Download a CSV-file
- Click the **Download technical support package** link
- From the Connection Broker machine console. See the **Connection Broker Virtual Appliance Guide** for instructions.

CSV-File

To download a CSV:

1. Go to the **> System > Log** page

2. Click the **Export list** link at the top of the page.

3. When prompted, save the CSV-file

The CSV-file contains the entire contents of the **> System > Log**, not just the information on the currently displayed page.

Downloading Logs

When you click on the **Download Technical Support package** link at the bottom-left of the Connection Broker Web interface, the broker downloads a ZIP-file containing all the information stored in the broker.

To extract the log information from the ZIP-file:

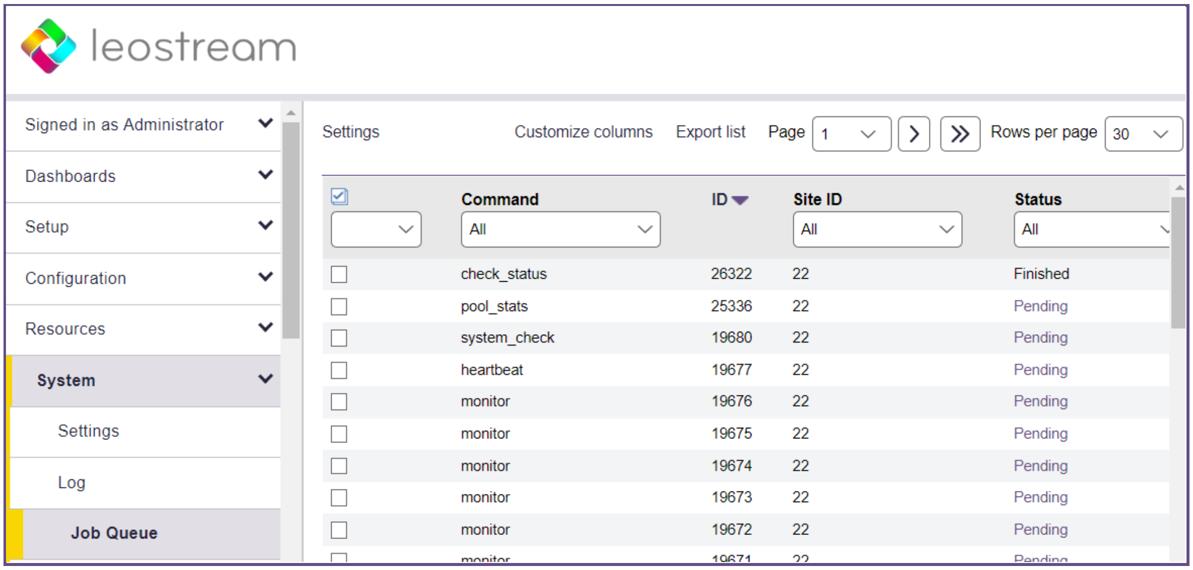
1. Extract the downloaded `.zip` file.
2. Extract the `sql-log.zip` file.

   The `sql-log`.directory contains a file called `sql-log.txt`, which is a tab delimited file containing the contents of the **> System > Log** table. You can import this table into an Excel spreadsheet for analysis.
3. Users are referenced in the table by their user ID. To see the mapping between users and user IDs, extract the `sql-user.zip` file.

The Connection Broker does not include any password information in the downloaded log files.

Viewing the Job Queue

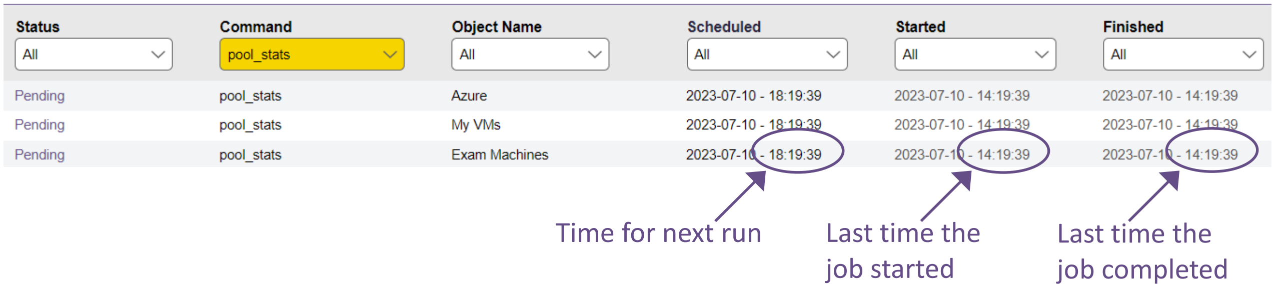
The **> System > Job Queue** page, shown in the following figure, displays the Connection Broker work queue, including all completed, running, and pending jobs. You can modify the columns included on this page by clicking the **Customize columns** link at the top-right side of the page (see **Customizing Tables**).



☑	Command	ID	Site ID	Status
	All		All	All
□	check_status	26322	22	Finished
□	pool_stats	25336	22	Pending
□	system_check	19680	22	Pending
□	heartbeat	19677	22	Pending
□	monitor	19676	22	Pending
□	monitor	19675	22	Pending
□	monitor	19674	22	Pending
□	monitor	19673	22	Pending
□	monitor	19672	22	Pending
□	monitor	19671	22	Pending

The job queue contains Connection Broker processes that are independent of the Web interface. The ID number indicates the order in which the Connection Broker placed jobs into the queue. The higher the ID number, the more recently the Connection Broker placed the job into the queue.

Recurring jobs, such as center scans, appear with a status of either pending or running. Pending jobs indicate the next time the Connection Broker runs the job, as well as the start and finish time for the last time the job ran, as shown in the following figure.



Status	Command	Object Name	Scheduled	Started	Finished
All	pool_stats	All	All	All	All
Pending	pool_stats	Azure	2023-07-10 - 18:19:39	2023-07-10 - 14:19:39	2023-07-10 - 14:19:39
Pending	pool_stats	My VMs	2023-07-10 - 18:19:39	2023-07-10 - 14:19:39	2023-07-10 - 14:19:39
Pending	pool_stats	Exam Machines	2023-07-10 - 18:19:39	2023-07-10 - 14:19:39	2023-07-10 - 14:19:39

Time for next run

Last time the job started

Last time the job completed

The Connection Broker logs a message on the **> System > Log** page in the event a job fails. To avoid stuck jobs, the Connection Broker monitors the job queue for any jobs that run over eight hours. At that point, the Connection Broker kills and restarts the job.

If you think your Connection Broker is not functioning correctly, use the job queue as a diagnostics tool.

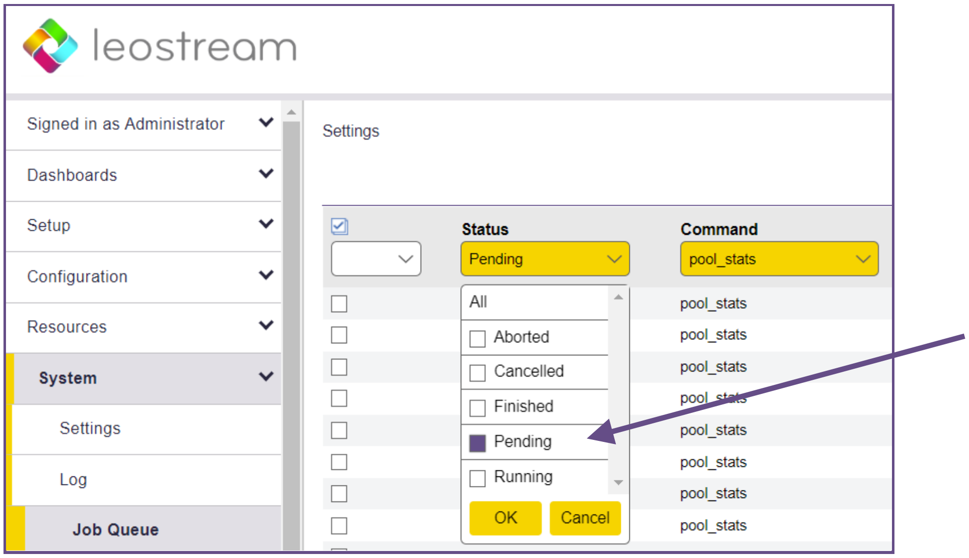
- If you requested an action and it hasn't taken place, check if the action is pending in the job queue.
- If upwards of 30 or more jobs are pending, the work queue may have stopped and you should reboot your Connection Broker

If the Connection Broker load average is above four, the Connection Broker stalls pending jobs until the load average goes below four. You can use the **Connection Broker Metrics report** to check the current Connection Broker load average.

Rescheduling Pending Jobs

The Connection Broker allows you to reschedule any pending work queue jobs. By rescheduling certain types of jobs, such as scanning centers, you can ensure that no Connection Broker jobs not related to handling logins occur during times of peak user login.

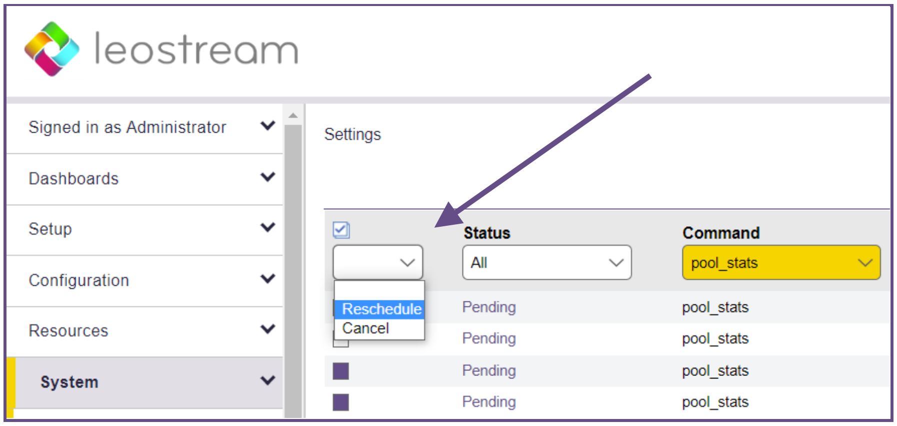
To see all pending work queue jobs, go to the **> System > Job Queue** page, and select **Pending** from the **Status** column's drop-down menu, as shown in the following figure.



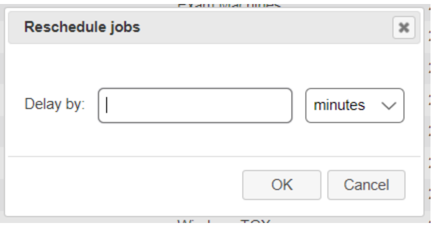
To reschedule one or more pending jobs:

1. On the **> System > Job Queue** page, check the checkbox before each pending job you want to reschedule. If the **Bulk Actions** column of checkboxes is not available, use the **Customize columns** link at the top of the table to add this column.

2. From the bulk action drop-down menu, select **Reschedule**, as show in the following figure.



3. The **Reschedule jobs** form opens, as shown in the following figure.


Reschedule jobs

Delay by: | minutes

4. In this form:

a. In the edit field, enter a numeric value for the amount of time to push the job forward.

b. From the drop-down menu, select the units for this value: minutes or hours.

c. Click **OK**.

The time shown in the **Scheduled** column for the selected jobs moves forward by the amount of time you selected.

Purging Completed Jobs

To purge completed jobs from the job queue table:

1. Click on the **Settings** link at the top of the **> System > Job Queue** page
2. Select the **Purge all complete jobs** option
3. Click **Save**

The Connection Broker removes all completed jobs from the job queue table, leaving any pending jobs in the queue.

Purging Pending and Running Jobs

Connection Brokers that are clustered around a common PostgreSQL or Microsoft SQL Server database are identified by their site ID. If you change the site ID for a Connection Broker or remove that Connection Broker from the cluster, some pending or running jobs associated with that site ID may remain in the job queue If that occurs, the pending jobs never run and running jobs never finish, as they are associated with a Connection Broker that is no longer part of the cluster.

Certain jobs, such as `pool_stats` jobs that refresh pool contents, can be run by any Connection Broker in the cluster. If pending `pool_stats` , `poll`, or `poll_power_state` jobs are associated with Connection Broker that are no longer part of the cluster, another Connection Broker will pick up the job when that job is scheduled to run. You do not need to delete these pending jobs.

If you have a cluster of Connection Brokers accessing a single work queue, you can delete pending or running jobs using the following two methods.

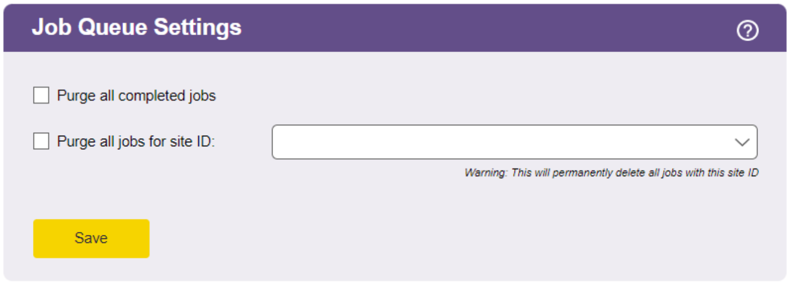
- The **Job Queue Settings** dialog provides an option to purge all pending or running jobs associated with a particular Connection Broker site ID. Use this option when you need to delete all the jobs for a Connection Broker that was removed from the cluster.

- The **Bulk action** drop-down menu provides a **Cancel** option that allows you to purge individual pending or running jobs from the work queue.

⚠ Purge pending and running jobs *only* if the Connection Broker associated with that site ID is no longer part of your Connection Broker cluster. Purging jobs associated with an existing Connection Broker can compromise the functioning of your Connection Broker

To purge all the pending or running jobs associated with a particular Connection Broker site ID:

1. Click **Settings** on the **> System > Job Queue** page. The **Job Queue Settings** dialog opens, as shown in the following figure.



Job Queue Settings

☐ Purge all completed jobs

☐ Purge all jobs for site ID:

Warning: This will permanently delete all jobs with this site ID

2. Check the **Purge all jobs for site ID** option.

3. From the associated drop-down menu, select the site ID associated with the pending and running jobs to purge.

⚠ Ensure that the selected site ID is no longer part of your Connection Broker cluster.

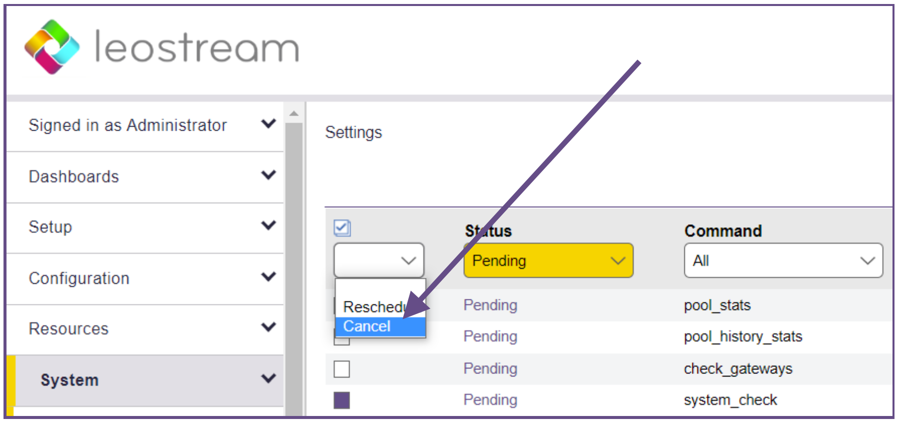
4. Click **Save**.

To purge individual pending or running jobs:

1. Ensure that the **Bulk action** column is displayed on your Connection Broker **> System > Job Queue** page. See **Customizing Tables** for information on how to display this column.

2. Select the checkbox in the **Bulk action** column for all pending and running jobs you want to cancel.

3. Select the **Cancel** option from the bulk action drop-down menu, as shown in the following figure.



☑	Status	Command
	Pending	All
	Pending	pool_stats
	Pending	pool_history_stats
☐	Pending	check_gateways
■	Pending	system_check

Using Web Queries to Obtain Connection Broker Status

You can monitor the Connection Broker using any of the following Web queries. These queries are useful, for example, if you use global or local load balancers and want to monitor the Connection Broker health at regular intervals.

```
https://CB_ADDRESS/index.pl?action=is_alive
https://CB_ADDRESS/index.pl?action=cb_status
https://CB_ADDRESS/index.pl?action=cb_version
```

Where *CB_ADDRESS* is your Connection Broker address. These queries perform the following functions.

- is_alive: Responds with CB_IS_OKAY if all of the following conditions are true:

1. The Connection Broker and its external database are online
2. All authentication servers defined in the Connection Broker are available
3. The Connection Broker load average is equal to or less than four

   Use the is_alive query with load balancers that direct user login requests. A Connection Broker that responds with CB_IS_OKAY, is ready to process the user login.

   If the Connection Broker cannot communicate with the database, the query returns an HTTP status of 503 (Service Unavailable). The query also returns an HTTP status of 503 (Service Unavailable) if the Connection Broker load average is above four or if any of the authentication servers defined in the Connection Broker are unavailable.

- cb_status: Responds with CB_IS_OKAY if the Connection Broker database is online. This function always returns a 200 Success header and returns an ERROR_MESSAGE if the database is not online.

  The cb_status query is lighter weight than the is_alive query and is a good option for performing general health checks on your Connection Broker. Leostream does not recommend using the cb_status query with load balancers that distribute user logins. A Connection Broker that responds to a cb_status query with **CB_IS_OKAY** may not be able to process user logins if, for example, an authentication server is offline.

- cb_version: Prints the current version of the Connection Broker when the Connection Broker application is running properly. Leostream recommends using the cb_version query in auto-scaling environments that are monitoring the Connection Broker application's health.

⚠ Before your auto-scaling system deletes or terminates a Connection Broker that fails a status call, check that your authentication servers and external database are healthy, communication from your Connection Broker to these systems is functioning properly, and all Connection Broker services are running. If the problem persists, please contact support@leostream.com prior to rebuilding your Connection Broker, as rebuilding the Connection Broker may destroy the records and logs required to diagnose the issue.

Sending Alerts to Email or Webhooks

The Connection Broker can send alerts to email addresses or to webhooks to warn administrators when certain events occur, such as centers going offline.

For email alerts, you can use the Connection Broker's internal SMTP server or your preferred external SMTP server to send the email alerts.

Configuring an SMTP Server for Alerts

You can use your Leostream Connection Broker as an SMTP server or configure a third-party SMTP server to use for email alerts and email invitations to session collaborators.

You currently can set up a single SMTP server for use with your Connection Broker.

To specify which SMTP server you want to use, add them to the **> Setup > SMTP** page, as follows.

1. Go to the **> Setup > SMTP** page.
2. Click the **Add SMTP Server** link.
3. Enter a display name in the **Name** edit field.
4. Enter the email address you want to use as the sender of all emails in the **Sender email address** edit field.
5. From the **Send email using** drop-down menu:
   - Select **Internal Connection Broker SMTP Server** to use the Connection Broker to send emails.

     Emails sent from the Connection Broker may be routed to your users Spam folders.
   - Select **External SMTP Server** to configure a third-party SMTP server, such as Gmail.
6. If using an external SMTP server:
   - Enter the **SMTP Server IP or Hostname** and **Port**
   - Enter the **User name** and **Password** to use to log into that SMTP server.
7. Click **Save**.

An easy way to test the SMTP server is to set up an alert based on the number of unassigned desktops then configure a pool to log an error when the number of unassigned desktops is below the number of unassigned desktops currently in that pool. See **Specifying Active Alerts** for information on setting up the alert and **Logging Desktop Pool Levels** for information on setting log levels in pools.

Specifying Active Alerts

You use the **> System > Alerts** page to indicate which alerts should send emails or call webhooks, as follows.

1. In the **Events** section, select the checkbox on the left-side of the row to enable that alert.
2. From the drop-down menu next to the checkbox, select the event that should trigger the alert. The available events are:
   - **Center goes offline**: Sent when a center goes offline. The email alert is not resent if the center remains offline the next time the center refreshes.
   - **Gateway goes offline**: Sent when the Connection Broker can no longer contact the Leostream Gateway and the gateway is then marked offline.
   - **License usage is exceeded**: Sent when the license limit is first exceeded. It is not resent for every user login.
   - **Pool drops below its error threshold of unassigned desktops**: Sent when any pool drops below the error threshold set in the **Logging and Reporting** section of the pool. The alert is sent once per pool when the threshold is first crossed.
   - **User is not offered a desktop from one of their pools**: Sent every time a user logs into the Connection Broker and one of their pools does not have an available desktop to offer.
3. For every active event, in the **Send as** drop-down menu, indicate if the alert should be sent as an **Email** or **Webhook**.
4. In the **Send to** edit field, enter a list of email addresses or URLs to receive the alerts.
5. To send multiple alerts, click the **Add alerts** button and return to step 1 to configure the new alert
6. If you are sending alerts as webhooks, use the **Webhook payload key** field to enter the payload. The same payload is sent to every alert you configured as a webhook.
7. Click **Save**.

Each row in the **Events** table must configure a unique alert. For example, to send alerts for one type of event to multiple email addresses, instead of creating multiple rows you enter a list of email addresses in step 4. Emails and webhooks are considered unique alerts. Therefore, you can send alerts for the same event as emails and webhooks by configuring two rows in the **Events** table for that event, one to send emails and the other to call a webhook.

To disable an alert and retain the alert configuration, uncheck the checkbox at the beginning of that row. To completely remove an alert from the **Events** table, remove any selection from the drop-down menu in the column next to the checkbox.

Using the Leostream API

The Connection Broker has a published Application Programming Interface (API) that allows you to control the broker using a RESTful API or XML-RPC (eXtensible Markup Language – Remote Procedure Calls).

The Leostream RESTful API allows you to configure the Administrator Web interface programmatically. Documentation for the currently available RESTful API methods can be found by clicking the links found on the **> System > Leostream API** page.

The XML-RPC allows you to query information from your Leostream environment, such as:

- List the pools a particular desktop is in
- Determine who is logged into a virtual machine
- Query the status of a virtual machine

Documentation for the XML API is available on the **> System > Leostream API** page.

Leostream Roles indicate which users have permission to execute the available Leostream APIs. See **Defining Roles for Leostream API Access** for more information on creating roles.

Testing the XML-RPC API

To test the XML-RPC API:

1. Enter the name of an XML-RPC function in the **Function name** edit field, for example **VM.Status**.

2. Enter the name and value of each parameter required by the function.

3. Click **Process**.

The Connection Broker pushes the request through the XML-RPC post and returns the function results.

Issuing SNMP Traps

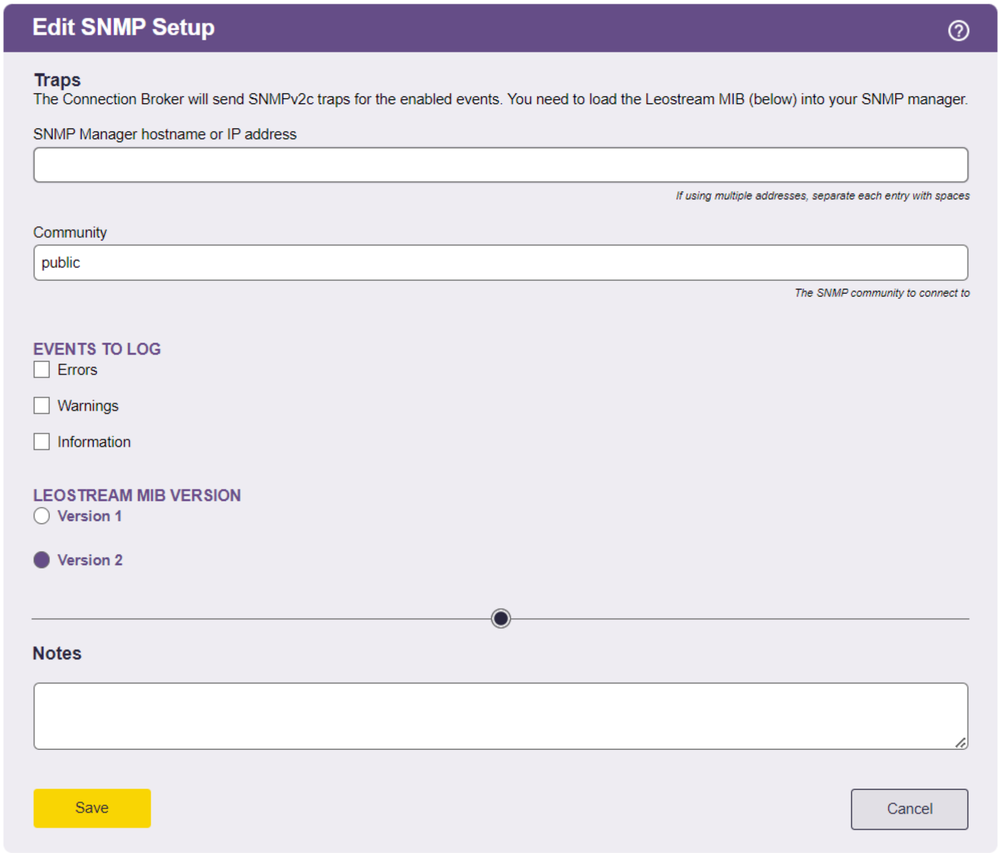
The Connection Broker provides basic SNMP trap support. Leostream sends traps using SNMPv2c format.

⚠ Leostream is phasing out support for sending SNMP traps using the Connection Broker. Customers should plan to migrate from SNMP traps to syslog messages as soon as possible. See **Integrating with Syslog Servers** for more information.

The Connection Broker does not support SNMP queries. You can only send requests using traps.

To setup SNMP support:

1. Go to the **> System > SNMP** page, shown in the following figure.



Edit SNMP Setup

Traps
The Connection Broker will send SNMPv2c traps for the enabled events. You need to load the Leostream MIB (below) into your SNMP manager.

SNMP Manager hostname or IP address

If using multiple addresses, separate each entry with spaces

Community

public

The SNMP community to connect to

EVENTS TO LOG

□ Errors

□ Warnings

□ Information

LEOSTREAM MIB VERSION

○ Version 1

● Version 2

Notes

2. Enter the hostname or IP address of the SNMP management system in the **SNMP Manager hostname or IP address** edit field. To send traps to multiple SNMP servers, enter multiple addresses separated by a comma.

   If you specify multiple SNMP servers, the Connection Broker sends the trap to all servers.

   To specify a non-standard SNMP port, use the format `host:port`.

3. Enter the community name in the **Community** edit field.

4. In the **Events to Log** section, select the events that should trigger the sending of a trap to the SNMP management system. You can send traps an any or all errors, warnings, and informational log events.

5. In the **Leostream MIB Version**, select which MIB version to use. The Leostream MIB has a Root OID (Organizational Identifier) of 1.3.6.1.4.1.18102.

   - Version 1 of the Leostream MIB has a single OID of 1.3.6.1.4.1.18102.50.
   - Version 2 of the Leostream MIB contains a hierarchical set of OIDs based on the different pages in the Connection Broker Web interface. Certain traps are sent using these OIDs. Traps that have not been migrated to the new version of the Leostream MIB use the original OID of 1.3.6.1.4.1.18102.50.

6. Click **Save**.

To setup the management system to recognize the Leostream traps, click on the link associated with the version of the MIB you will use. Copy the Leostream MIB and compile the MIB into the SNMP system using the supplied complier. The compiler creates a compiled version of the MIB which is stored alongside all the other compiled MIBs within the management system. The management system then displays the traps sent by the Connection Broker.

Both versions of the MIB report the following information:

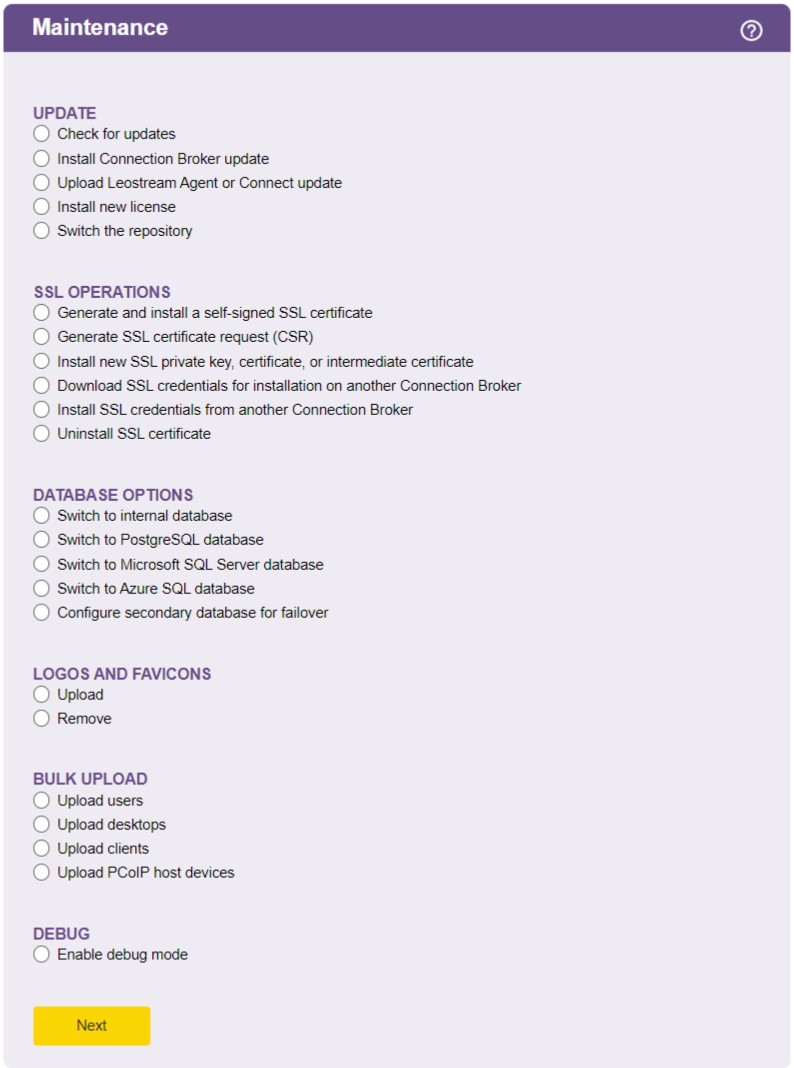
- The level of the trap: `2` for errors; `3` for warnings; `4` for information
- The UUID of the object affected, if applicable
- A text string describing the problem, in the format `object_name : message_text`

Chapter 17: Maintaining the Connection Broker

Overview

The **> System > Maintenance** page, shown in the following figure, allows you to:

- Update your Connection Broker
- Install new license keys
- Manage the Connection Broker database
- Manage SSL certificates
- Load and remove custom logos or new versions of the Leostream Agents and Clients
- Upload user, client, and desktop data into the Connection Broker



Maintenance ?

UPDATE

○ Check for updates
○ Install Connection Broker update
○ Upload Leostream Agent or Connect update
○ Install new license
○ Switch the repository

SSL OPERATIONS

○ Generate and install a self-signed SSL certificate
○ Generate SSL certificate request (CSR)
○ Install new SSL private key, certificate, or intermediate certificate
○ Download SSL credentials for installation on another Connection Broker
○ Install SSL credentials from another Connection Broker
○ Uninstall SSL certificate

DATABASE OPTIONS

○ Switch to internal database
○ Switch to PostgreSQL database
○ Switch to Microsoft SQL Server database
○ Switch to Azure SQL database
○ Configure secondary database for failover

LOGOS AND FAVICONS

○ Upload
○ Remove

BULK UPLOAD

○ Upload users
○ Upload desktops
○ Upload clients
○ Upload PCoIP host devices

DEBUG

○ Enable debug mode

The page also displays information such as your license expiration date, database information, Connection Broker operating system, and SSL certificate information.

The **Connection Broker information** displayed on the right side of the **> System > Maintenance** page displays the current Connection Broker version and the last time it was updated. You can remotely determine the Connection Broker version by querying:

```
http://cb-address/index.pl?action=cb_version
```

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

Updating Connection Brokers

For a description of updating Connection Brokers, see the **Leostream Connection Broker Application Guide**.

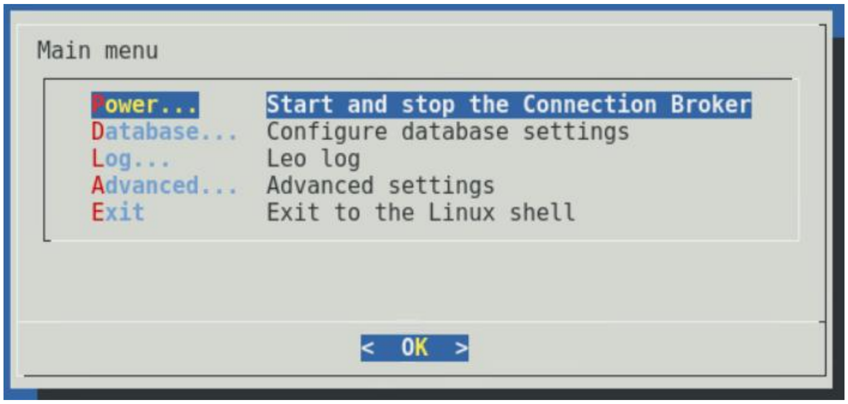
Removing the Update Option

In production environments, you may want to lock the Connection Broker version by prohibiting administrators from checking for and installing updates. You can do so by removing the update options from the **> System > Maintenance** page. To remove these option:

1. Log into the machine running your Connection Broker as the `root` user and, from a terminal, issue the following command.

   ```
   su - leo
   ```

   The Administration Menu, shown in the following figure, opens.

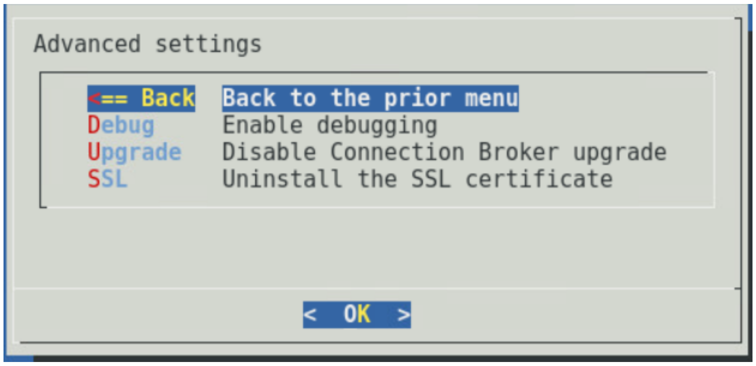


```
Main menu

    Power...        Start and stop the Connection Broker
    Database...     Configure database settings
    Log...          Leo log
    Advanced...     Advanced settings
    Exit            Exit to the Linux shell

                    < OK >
```

2. Select **Advanced** and hit **<Enter>**. The **Advanced settings** options, shown in the following figure, appear.



```
Advanced settings

   <== Back    Back to the prior menu
   Debug       Enable debugging
   Upgrade     Disable Connection Broker upgrade
   SSL         Uninstall the SSL certificate

                  <  OK  >
```

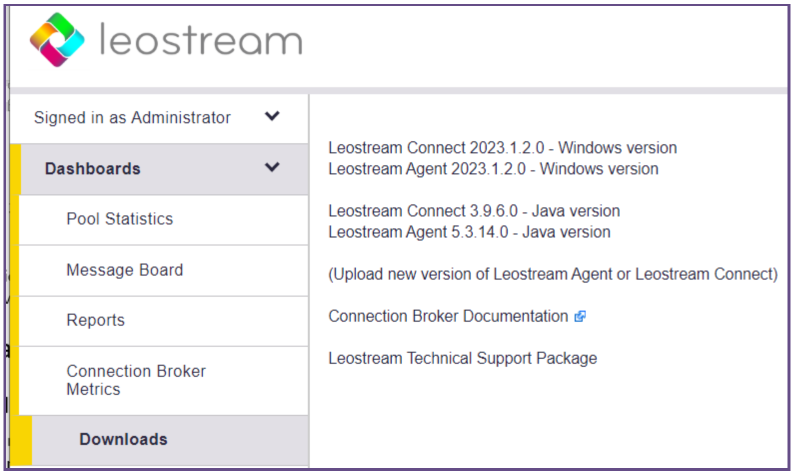
3. Select **Upgrade** and hit **<Enter>**.

The **> System > Maintenance** page no longer shows options to check for and install updates, including the option to upload new Leostream Connect and Leostream Agent versions. To restore this option, repeat the previous process.

Upgrading Leostream Connect and Leostream Agent

Uploading New Leostream Connect and Leostream Agent Versions

Connection Broker updates include the latest version of the Leostream Connect clients and Leostream Agents, available when the Connection Broker update was released. You can view and download these versions on the **> Dashboards > Downloads** page, shown in the following figure.



Leostream Connect 2023.1.2.0 - Windows version
Leostream Agent 2023.1.2.0 - Windows version

Leostream Connect 3.9.6.0 - Java version
Leostream Agent 5.3.14.0 - Java version

(Upload new version of Leostream Agent or Leostream Connect)

Connection Broker Documentation

Leostream Technical Support Package

You can automatically upgrade existing Leostream Connect and Leostream Agent installations to the versions displayed on the **> Dashboards > Downloads** page, using the options described in the following two sections.

If Leostream releases a Leostream Connect or Leostream Agent upgrade independent of a Connection Broker update, you can upload the new clients and agents into your Connection Broker, as follows.

1. Go to the **> System > Maintenance** page.

2. Select the **Upload Leostream Agent or Connect update** option.

3. Click **Next**.

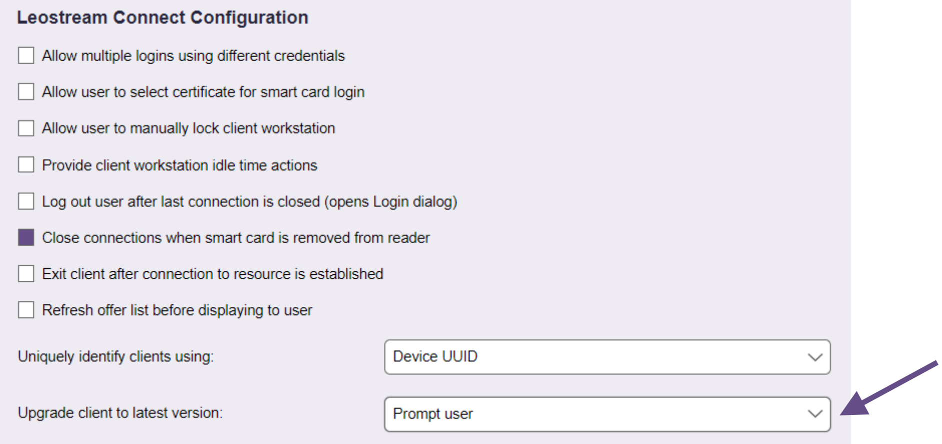
4. Browse for the new Leostream Agent or Leostream Connect installation file.

5. Click **Upload**.

The Connection Broker uploads the file and automatically places it into the `/var/lib/leo/app/download` directory. The **> Dashboards > Downloads** page displays the new version numbers.

Upgrading Leostream Connect

Use the **Upgrade client to latest version** drop-down menu on the **> System > Settings** page, shown in the following figure, to push Leostream Connect upgrades out to client devices.



Leostream Connect Configuration

□ Allow multiple logins using different credentials

□ Allow user to select certificate for smart card login

□ Allow user to manually lock client workstation

□ Provide client workstation idle time actions

□ Log out user after last connection is closed (opens Login dialog)

■ Close connections when smart card is removed from reader

□ Exit client after connection to resource is established

□ Refresh offer list before displaying to user

Uniquely identify clients using: Device UUID

Upgrade client to latest version: Prompt user

Select one of the options in this menu, to indicate when the client should be updated, as follows:

- **Never**: Do not update Leostream Connect. In this case, you must manually update end users' clients.

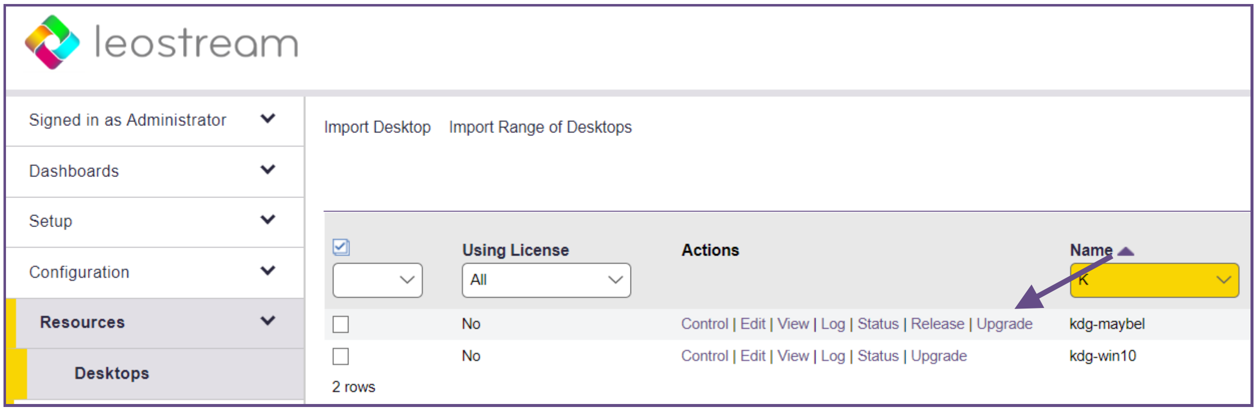
- **Always**: Always update Leostream Connect. In this case, the first time an end user runs Leostream Connect and an update is available, they are warned that an update is in process. Leostream Connect restarts when the update is finished.

- **Prompt user**: Lets the user decide if they want to update Leostream Connect. In this case, when the user launches Leostream Connect and an update is available, the client prompts the user to install the update. The Connection Broker continues to prompt the user every time the client is launched, until the upgrade is completed.

The Connection Broker runs the same tasks during the upgrade as you specified for the original Leostream Connect installation.

Upgrading Leostream Agents

You can push Leostream Agent out to remote desktops using the **Upgrade** option on the **> Resources > Desktops** page, shown in the following figure.



☑	Using License	Actions	Name ▲
	All		K
□	No	Control | Edit | View | Log | Status | Release | Upgrade	kdg-maybel
□	No	Control | Edit | View | Log | Status | Upgrade	kdg-win10

2 rows

The **Leostream Agent Version** column on the **> Resources > Desktops** page displays the currently installed version for each desktop. If this version is lower than the Leostream Agent version shown on the **> Dashboards > Downloads** page, the Connection Broker adds the **Upgrade** option to the **Actions** list.

The Connection Broker runs the same tasks during the upgrade as you specified for the original Leostream Agent installation and always requests a desktop reboot after the installation completes. If you did not start the Leostream Agent at the end of the original installation, the Connection Broker will not automatically start the Leostream Agent after the upgrade. In this case, you must manually restart the agent.

- To update an individual desktop, click the **Upgrade** action associated with that desktop.

- To simultaneously upgrade the Leostream Agents on multiple desktop:

    1. Ensure that the **Bulk actions** column is shown on the **> Resources > Desktops** page (see **Performing Bulk Actions**).

    2. In the **Bulk actions** column, select the checkbox associated with each desktop that has a Leostream Agent you want to upgrade.

    3. From the drop-down menu at the top of the **Bulk actions** column, select **Edit**.

    4. In the **Edit desktops** form that opens, select the **Upgrade Agent to latest version** option.

    5. Click **Save**.

The Connection Broker updates the Leostream Agents on all the selected desktops.

Entering a New License Key

Your Leostream license is generated from the Leostream serial number provided to you by Leostream sales. The license key enables features in your Connection Broker and is specific to the Connection Broker installation from which it was generated.

When you request access to additional features, Leostream sales updates your existing serial number. You can generate a new license key from your serial number to access the additional features.

To generate and enter your license key:

1. Go to the **> System > Maintenance** page.
2. Select the **Install new license** option in the **Update** section.
3. Click the **Next** button.
4. On the **Leostream License** page, click the link to go to **https://license.leostream.com**. The installation code for your Connection Broker is automatically populated.
5. Enter the serial number you obtained from Leostream sales, if it is not prepopulated.
6. Enter the email address associated with that serial number.
7. Click **Generate a license**.
8. Click the **Apply to the broker** button above the generated license key. The browser returns to the **Leostream License** page.

10. Select the **I have read and accept the License Agreement** check box.
11. Click **Save**.

Switching Databases

The Connection Broker includes a built-in PostgreSQL database, which is adequate for a proof-of-concept or small deployment. For larger deployments, or to build a highly available Connection Broker cluster, switch to an external PostgreSQL, Microsoft SQL Server, or Azure SQL database.

A ***cluster*** is defined as two or more Connection Brokers all communicating with the same PostgreSQL or Microsoft SQL Server database. For a complete description of using clusters to scale Leostream environments, see the **Leostream Scalability Guide** available on the Leostream Documentation Web page.

⚠ A cluster cannot contain a mixture of version 9 and version 2022 Connection Brokers.

Under normal operation, the Connection Broker creates, deletes and updates rows in the database. During upgrades it may also create, delete and/or update tables and indices in the database. Ensure that you define a database user with the appropriate permissions, for example, for Microsoft SQL Server the user must have permission to support the following functions:

- db_ddladmin
- db_datawriter
- db_datareader

This section covers the basics of switching to an external database. For additional information, including setting up database failover, see the **Leostream Scalability Guide** available as a supporting document on the **Leostream Documentation** page. For information on using the Connection Broker CLI to switch databases or update database parameters, see the **Leostream Connection Broker Application Guide**.

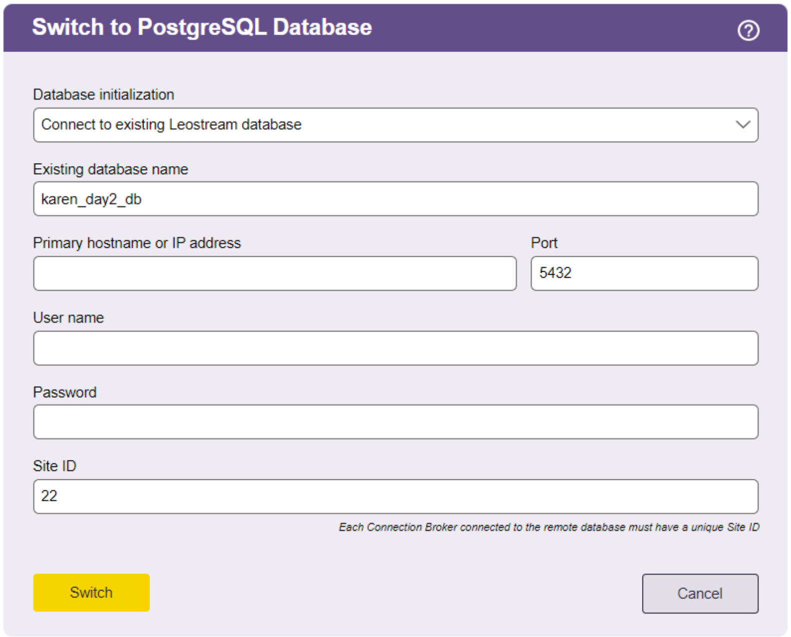
Connecting to a PostgreSQL Database

Leostream supports PostgreSQL version 13, or higher, as an external PostgreSQL database.

To connect the Connection Broker to an external PostgreSQL database:

1. Go to the **> System > Maintenance** page.

2. Select the **Switch to PostgreSQL database** option. The following **Switch to PostgreSQL database** form opens.



Switch to PostgreSQL Database

Database initialization: Connect to existing Leostream database

Existing database name: karen_day2_db

Primary hostname or IP address:

Port: 5432

User name:

Password:

Site ID: 22

Each Connection Broker connected to the remote database must have a unique Site ID

3. From the **Database initialization** drop-down menu, indicate if you are attaching to an existing database or if want to copy the contents of your current database to a new database.

   When connecting to an existing database that is populated with a Leostream configuration, the Connection Broker attaches to the database without copying any configuration information from its current database.

4. Enter a name for the database in the **Database name** edit field.

   ⚠ Do not use hyphens or other invalid characters in the database name.

5. Enter the PostgreSQL hostname or IP address in the **Principal hostname or IP Address** edit field.

6. Change the default outbound port listed in the **Port** edit field, if necessary.

7. Enter a username and associated password for a user with access to the database, in the **User name** and **Password** edit fields, respectively.

8. Enter a unique **Site ID**. If you are using a cluster of Connection Brokers, each broker must have a unique Site ID.

   You can enter the site ID associated with a Connection Broker that was removed from the cluster. The new Connection Broker takes over any jobs in the work queue associated with the previous Connection Broker.

9. Click **Switch** to complete the switch to the external database. The Connection Broker upgrades the old database.

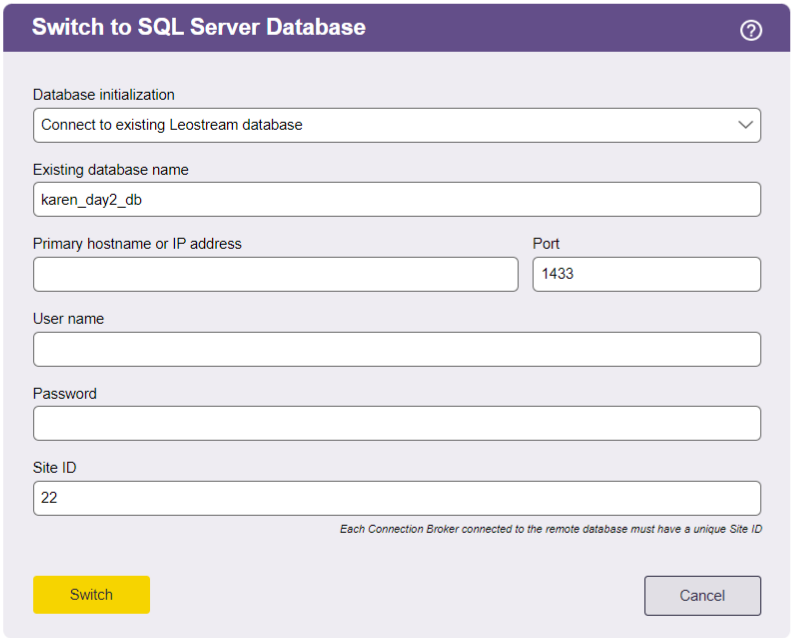
Connecting to a Microsoft SQL Server Database

Leostream supports Microsoft SQL Server versions currently covered by Mainstream Support under the Microsoft Fixed Lifecycle Policy and versions in service under the Microsoft Modern Lifecycle Policy.

To switch to a Microsoft SQL Server database:

1. Go to the **> System > Maintenance** page.

2. Select the **Switch to Microsoft SQL Server database** option. The following **Switch to SQL Server Database** form opens.



Switch to SQL Server Database

Database initialization: Connect to existing Leostream database

Existing database name: karen_day2_db

Primary hostname or IP address:

Port: 1433

User name:

Password:

Site ID: 22

Each Connection Broker connected to the remote database must have a unique Site ID

3. From the **Database initialization** drop-down menu, indicate if you are attaching to an existing database or if want to copy the contents of your current database to a new database.

   When connecting to an existing database that is populated with a Leostream configuration, the Connection Broker attaches to the database without copying any configuration information from its current database.

4. Enter a name for the database in the **Database name** edit field.

   ⚠ Do not use hyphens or other invalid characters in the SQL Server database name.

5. Enter the SQL Server hostname or IP address in the **Principal hostname or IP Address** edit field.

6. Change the default outbound port listed in the **Port** edit field, if necessary.

   📝 If you are using a named instance of SQL Server, ensure that you enter the correct port number for that instance. You can view the ports associated with this instance in the **Protocols for instance_name** dialog associated with this instance.

7. Enter a username (including the domain) and associated password for a user with access to the database, in the **User name** and **Password** edit fields, respectively. Leostream uses SQL authentication to connect to the database.

8. Enter a unique **Site ID**. If you are using a cluster of Connection Brokers, each broker must have a unique Site ID.

   If you enter the site ID associated with a Connection Broker that was previously removed from the cluster, the new Connection Broker takes over any jobs in the work queue associated that broker.

- Click **Switch** to complete the switch to the external database.

The Connection Broker restarts whenever you switch databases.

After you switch to an external database, the Connection Broker stops updating its internal database with configuration changes. Therefore, if you switch back to the internal database, the Connection Broker configuration reverts to the setup at the point when the original switch to the external database occurred.

For information on specifying a secondary failover database, see the **Leostream Scalability Guide.**

Required Permissions

The level or permissions required by Leostream depends on which actions you need the user to perform. The following table lists to various tasks the Connection Broker may try to perform and the required permission.

Action	**Permission**
Switch Broker to a SQL Server that does not yet have a Leostream database.	`dbcreator` access to the SQL Server
Switch Broker to a SQL Server with an existing, but empty Leostream database	`db_owner` access to the Leostream database
Switch Broker to a SQL Server with an existing, populated database	`db_owner` access to the Leostream database
Update Broker attached to a SQL Server database	`db_owner` access to the Leostream database

Possible Database Error Messages

If an incorrect IP address for the database is entered, or the database is not running, the following error is displayed:
ERROR 2003: Can’t connect to database.

If an incorrect username or password is entered, the error message is shown on the database page as follows:
ERROR 1045: Access denied.
After the database is switched, the Connection Broker continues to function as before but all data is written to the database. If the Connection Broker no longer logs into the database, the following error message displays:
Unable to connect to the database.

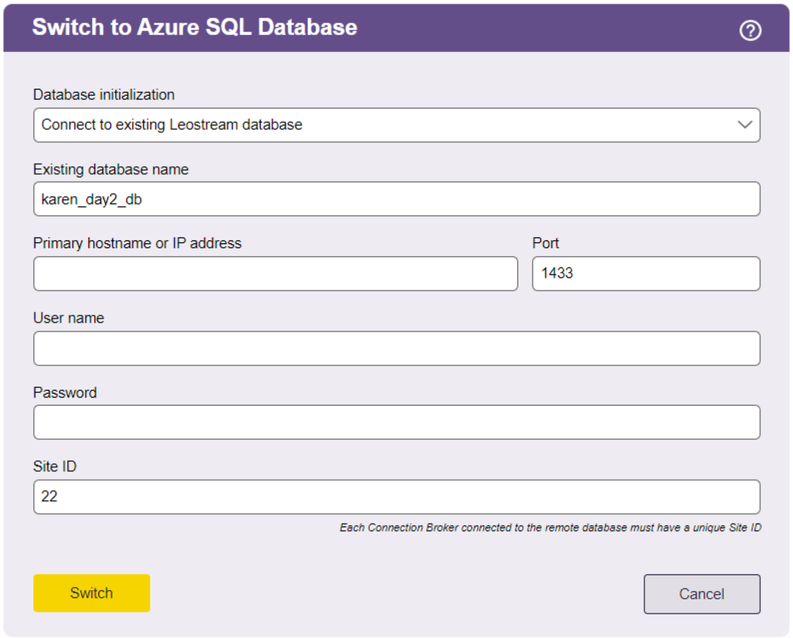
To determine the source of the error, go to `https://`*`cb-address`*`/database_error.pl`, where *`cb-address`* is your Connection Broker address.

Connecting to an Azure SQL Database

If you are building your Leostream environment in an Azure cloud, you can use Azure SQL as your external Leostream database. Before you begin, you must manually create a database for your Connection Broker in Azure. Ensure that the firewall rules for the database allows access to the database from your Connection Broker.

You can then switch to this Azure SQL database and instruct Leostream to copy the contents of the current Leostream database to the Azure SQL database, for example:

1. Go to the **> System > Maintenance** page.
2. Select the **Switch to Azure SQL database** option. The following **Switch to Azure SQL database** form opens.



Switch to Azure SQL Database

Database initialization
Connect to existing Leostream database

Existing database name
karen_day2_db

Primary hostname or IP address

Port
1433

User name

Password

Site ID
22

Each Connection Broker connected to the remote database must have a unique Site ID

3. From the **Database initialization** drop-down menu, select **Copy current Leostream database into existing database** if you are attaching to a new, empty Azure SQL database.

   Select **Connect to existing Leostream database** if this is not the first Connection Broker you are adding to your cluster. When connecting to an existing database that is populated with a Leostream configuration, the Connection Broker attaches to the database without copying any configuration information from its current database.

4. Enter the name of your Azure SQL database in the **Database name** edit field.
5. Enter the Azure SQL server hostname in the **Principal hostname or IP Address** edit field.
6. Change the default outbound port listed in the **Port** edit field, if necessary.
7. Enter the username and password for the Azure SQL server user with access to the database, in the **User name** and **Password** edit fields, respectively.
8. Enter a unique **Site ID**. If you are using a cluster of Connection Brokers, each broker must have a unique Site ID.

   You can enter the site ID associated with a Connection Broker that was removed from the cluster.

The new Connection Broker takes over any jobs in the work queue associated with the previous Connection Broker.

- Click **Switch** to complete the switch to the external database.

The Connection Broker must restart when it switches to a new database.

After you switch to an external database, the Connection Broker stops updating its internal database with configuration changes. Therefore, if you switch back to the internal database, the Connection Broker configuration reverts to the setup at the point when the original switch to the external database occurred.

For information on specifying a secondary failover database, see the **Leostream Scalability Guide.**

Switching Site IDs

After a Connection Broker joins a cluster, you can change the Site ID associated with that Connection Broker. Changing Site IDs allows you, for example, to instruct a Connection Broker to take over any jobs in the work queue associated with that Site ID.

To change the Site ID:

1. Select the appropriate **Switch to remote database** option on the **> System > Maintenance** page
2. Enter the new site ID in the **Site ID** edit field.
3. Click **Save**.

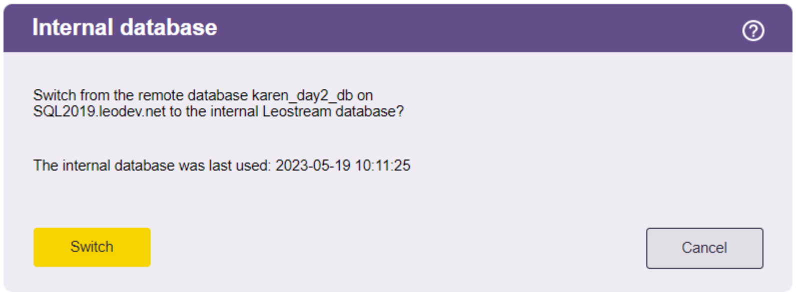
Changing the site ID, or any other remote database parameter, is conceptually identical to connecting the Connection Broker to a new database. The Connection Broker performs all the steps associated with switching to a new database, including restarting the Connection Broker.

Switching Back to the Internal Connection Broker Database

You can easily switch any Connection Broker that is attached to an external database back to its internal database.

To switch back to the internal database:

1. Go to the **> System > Maintenance** page.
2. Select the **Switch to internal database** option. The following **Internal database** form opens.



Internal database

Switch from the remote database karen_day2_db on SQL2019.leodev.net to the internal Leostream database?

The internal database was last used: 2023-05-19 10:11:25

3. Click **Switch** to switch back to the internal database.

4. Click **Cancel** to leave the form without switching back to the internal database.

After you switch the Connection Broker back to its internal database:

- The Connection Broker removes itself from the cluster associated with the external database.

- The internal database is configured *exactly* as it was directly before the Connection Broker was switched to the external database. Changes made in the external database are not moved back into the internal database.

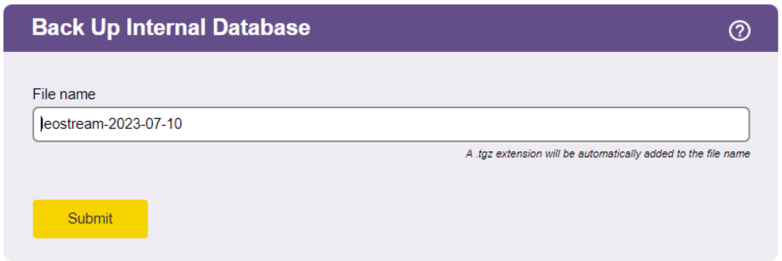
Backing Up and Restoring an Internal Connection Broker Database

This feature is not available if your Connection Broker uses an external database. If you are using an external database, back up the database using the standard tools and techniques for PostgreSQL or Microsoft SQL Server databases.

You can download an internal Connection Broker database and additional Connection Broker settings, as follows:

1. Select the **Backup internal database** option in the **Database options** section in the **> System > Maintenance** page.

2. Click **Next**. The following **Backup Internal Database** form opens.



Back Up Internal Database

File name: leostream-2023-07-10

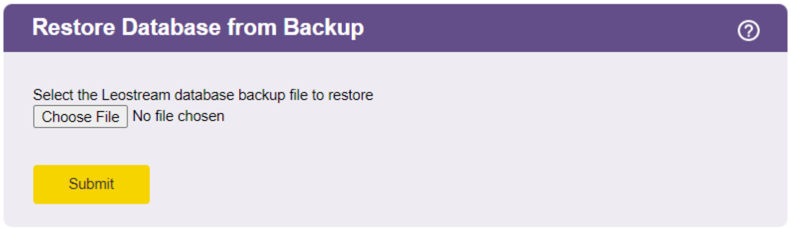
A .tgz extension will be automatically added to the file name

3. Enter a file name for the downloaded configuration or use the default file name.

4. Click **Submit**. The Connection Broker adds the postscript `.tgz` to any filename and downloads the file to the browser’s default download folder on your machine.

You can restore a downloaded Connection Broker database, as follows:

1. Select the **Restore database from backup** option in the **> System > Maintenance** page.
2. Click **Next**. The following **Restore Database from Backup** dialog opens.



Select the Leostream database backup file to restore

3. Enter the full path to the configuration file or locate the file using the **Browse** button.
4. Click **Submit** to upload the file.

⚠ This file overwrites the previous Connection Broker configuration database.

Backing up Your Connection Broker

Recommended Practices

Leostream recommends the following schedule for backing up your Connection Broker virtual machine:

- Make monthly clones
- Take weekly snapshots

By backing up the entire Connection Broker virtual machine, you do not need a separate backup procedure for the underlying Connection Broker operating system.

If you are using an external database, implement your site standard database backup procedure to protect the data. As with any backup procedure, test the restore process to make sure it is well documented and works as expected.

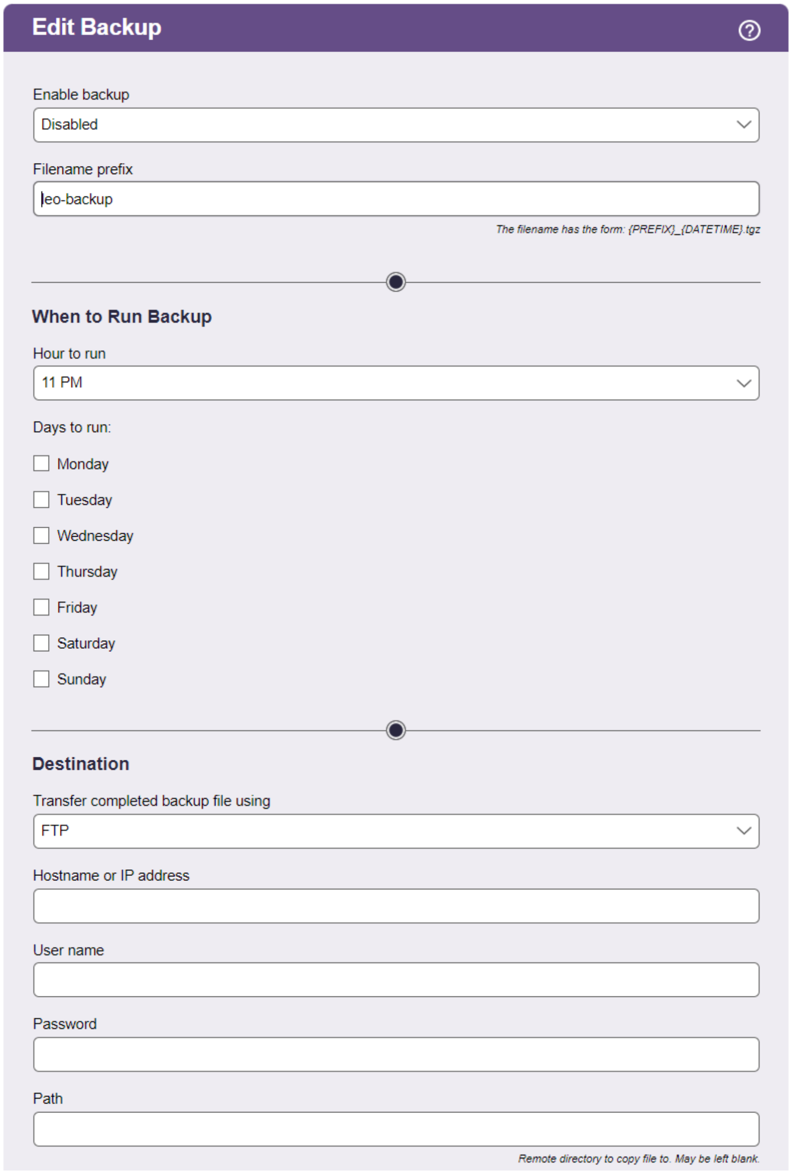
If you are using an internal database, use the **> System > Backup** page to schedule regular backups to an external FTP server. See the following section for more information.

Scheduling Connection Broker Backups

The **> System > Backup** page, shown in the following figure, allows you to schedule routine backups of your Connection Broker internal data base.

⚠ The scheduled backup does *not* back up information stored in an external PostgreSQL or Microsoft SQL Server database. If your Connection Broker is attached to an external database, the schedule backup includes:

- The unused data in the internal database, which is stale compared to the external database
- The external database connection information (IP, username, password) and local SSL cert and key



Edit Backup

Enable backup: Disabled

Filename prefix: leo-backup

The filename has the form: {PREFIX}_{DATETIME}.tgz

When to Run Backup

Hour to run: 11 PM

Days to run:

□ Monday

□ Tuesday

□ Wednesday

□ Thursday

□ Friday

□ Saturday

□ Sunday

Destination

Transfer completed backup file using: FTP

Hostname or IP address:

User name:

Password:

Path:

Remote directory to copy file to. May be left blank.

To schedule automatic remote backups:

1. Select **Enabled** from the **Enable backup** drop-down menu. Toggle the selection back to **Disabled** to turn off remote backup.
2. Enter a string into the **Filename prefix** edit field. The Connection Broker stores your backup files with the name `prefix_DATETIME.tgz`, where `prefix` is the string you enter in this edit field.
3. Select the time to run the backup from the **Hour to run** drop-down menu.

4. Select all the days to run the backup.

5. Select FTP or SFTP from the **Transfer completed backup file using** drop-down menu to indicate the transport method.

6. Enter the full path to the FTP or SFTP host in the **Hostname or IP address** edit field.

7. Enter the user name for a user with permission to copy files to your host in the U**ser name** edit field.

8. Enter the user's password in the **Password** edit field.

9. Optionally enter a directory to copy the backup file to in the **Path** edit field.

10. If you want to run the backup as soon as you click **Save**, in addition to the times you configured in this form, select the **Perform a backup now** option.

11. Click **Save**.

Working with SSL Certificates

The Connection Broker includes a default Leostream certificate that is used to encrypt communication between the Connection Broker and the Leostream Agents and Leostream Connect clients. Beginning with Connection Broker 2024.4, this certificate expires after one year and the Connection Broker automatically renews the default certificate upon expiration.

You can replace this certificate using any of the following options. When working with a Connection Broker cluster, the certificate is not automatically shared between the Connection Brokers in the cluster. You must install the certificate on each Connection Broker. Your options include:

- Generate a self-signed certificate on each Connection Broker, as described in **Generating and Installing Self-Signed SSL Certificates**. Self-signed certificates are simple and low cost, but will not remove the security warning issued by browsers.

- Generate a self-signed certificate on one Connection Broker in the cluster (see **Generating and Installing Self-Signed SSL Certificates**), then copy that certificate to all other Connection Brokers in the cluster (see **Sharing SSL Credentials between Connection Brokers**).

- Generate an SSL certificate request (CSR), as described in **Generating an SSL Certificate Request**, and use it to obtain a certificate from a certificate authority. You can then upload the certificate, as described in **Installing a Signed SSL Certificate and Intermediate Certificate**. Browsers recognize certificates generated by a certificate authority and, therefore, do not generate a security warning.

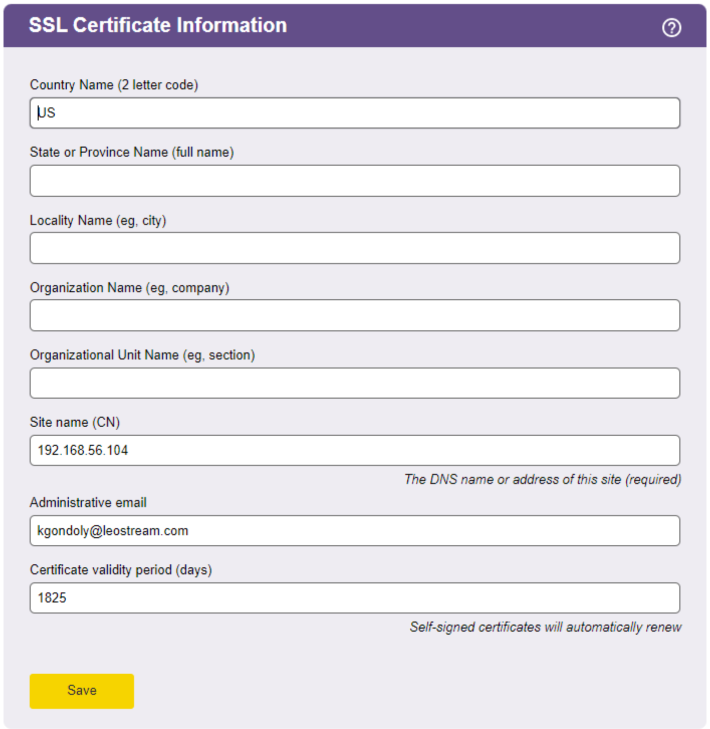
Generating and Installing Self-Signed SSL Certificates

To create a self-signed certificate:

1. Go to the **> System > Maintenance** page.

2. Select the **Generate and install a self-signed SSL certificate** option.

3. Click **Next**. The following form opens, requesting the information needed to generate an SSL certificate.



SSL Certificate Information

Country Name (2 letter code)
US

State or Province Name (full name)

Locality Name (eg, city)

Organization Name (eg, company)

Organizational Unit Name (eg, section)

Site name (CN)
192.168.56.104
The DNS name or address of this site (required)

Administrative email
kgondoly@leostream.com

Certificate validity period (days)
1825
Self-signed certificates will automatically renew

For a self-signed certificate, you have flexibility in completing the information in this form, but should follow guidelines if you want to transition to a certificate signed by a certificate signing authority in the future. Certificate signing authorities require official documentation to support each variable.

4. Enter some or all of the following information. The Site name is required. All other fields are optional.

   You can typically find this information by going to your organization’s official Web site, finding a secure page, and then using your browser to examine the certificate.

   - **Country name**: The IANA two letter country code (see **http://www.iana.org/cctld/cctld-whois.htm** for the official list).
   - **State or Province Name (full name)**: The full name of your state or province. Do not enter abbreviations.
   - **Locality name**: The city in which your company is incorporated.
   - **Organization Name**: The name by which your organization is officially recognized.

- **Organizational Unit Name**: The department name.
- **Site name**: (Required) Either a DNS name or IP address. It is recommended that you add the Connection Broker address into your DNS system then use the DNS name rather than the IP address. In this way, you can change the IP address of the Connection Broker without having to create new certificates.

  When generating certificates for a Connection Broker cluster, use the DNS name for your cluster.
- **Administrative email**: The email address of the person responsible for certificate maintenance.
- **Certificate validity period (days)**: Enter the number of days util the generated certificate expires. The Connection Broker automatically renews expired self-signed certificates.

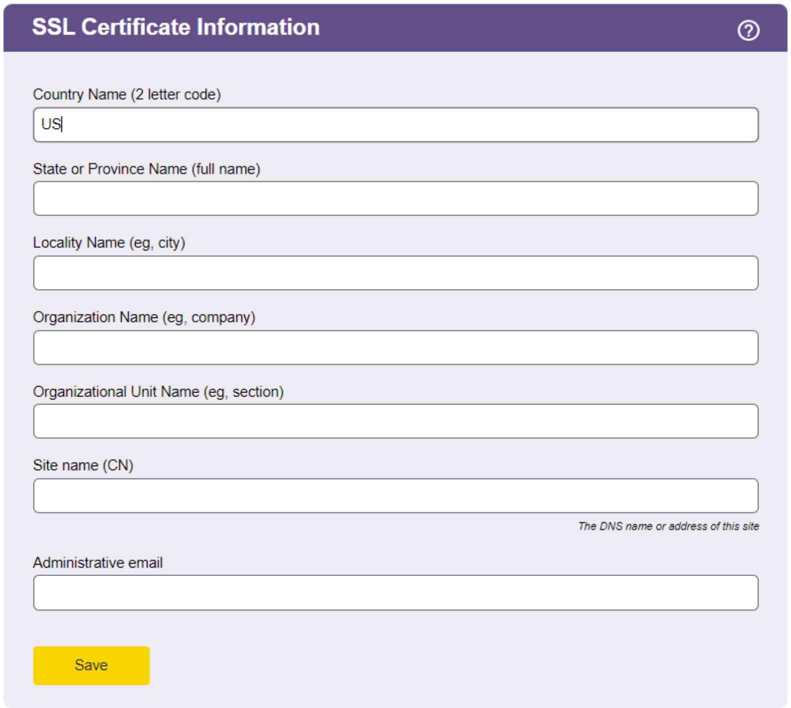
5. Click **Save**.

The Connection Broker creates the certificate request and installs the certificate. The Web interface is then encrypted with this certificate. The Connection Broker displays a message when the installation is complete.

Generating an SSL Certificate Request

To generate the information needed to request an SSL certificate from a third-party certificate signing authority:

1. Go to the **> System > Maintenance** page.
2. Select the **Generate SSL certificate request (CSR)** option.
3. Click **Next**. The following form opens, requesting the information needed to generate an SSL certificate.



SSL Certificate Information

Country Name (2 letter code): US

State or Province Name (full name):

Locality Name (eg, city):

Organization Name (eg, company):

Organizational Unit Name (eg, section):

Site name (CN):

The DNS name or address of this site

Administrative email:

4. Enter the SSL certification information, described in the previous section.

5. Click **Save**. The Connection Broker generates the CSR and displays a message page.

6. Click the **Click here** link in the message page to download the CSR file.

7. Cut-and-paste this block of text from the browser into the entry form for the certificate application.

⚠ The text must be copied as plain text. Either cut-and-paste the text from the browser window into another browser window or into a plain text email (not HTML enhanced).

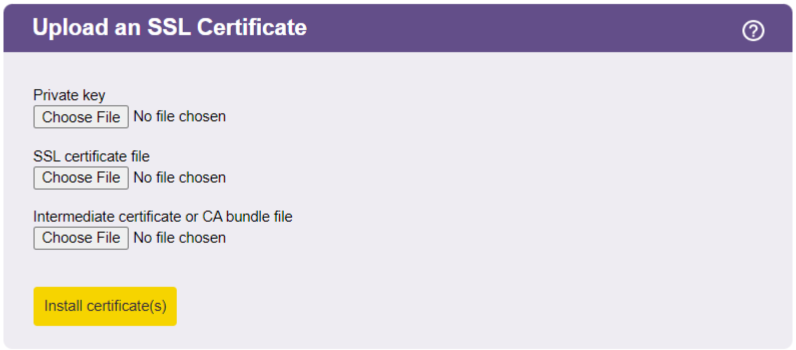
Installing a Signed SSL Certificate and Intermediate Certificate

After the signed SSL certificate arrives from the certificate signing authority, you can install it on the Connection Broker, as follows. This method can be used to upload the signed certificate, a new private key, and any intermediate certificates, as required.

1. Go to the **> System > Maintenance** page.

2. Select the **Install new SSL private key, certificate, or intermediate certificate** option.

3. Click **Next**. The following dialog opens.



Upload an SSL Certificate

Private key

Choose File No file chosen

SSL certificate file

Choose File No file chosen

Intermediate certificate or CA bundle file

Choose File No file chosen

Install certificate(s)

4. Browse for the private key, SSL certificate and intermediate certificate, as required.

5. Click **Install the certificate(s)**.

After the certificate is uploaded, the Connection Broker restarts in order to use the new certificate.

Sharing SSL Credentials between Connection Brokers

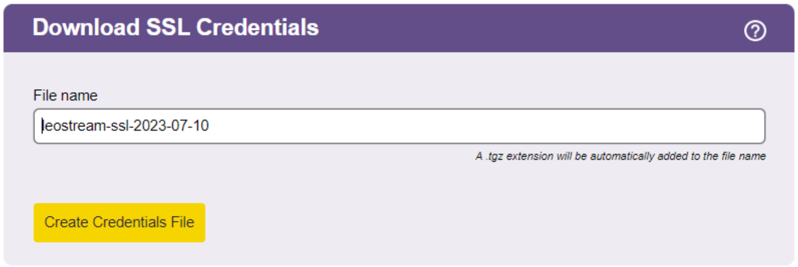
In deployments where you are clustering Connection Brokers, you want all brokers to use identical SSL credentials. To do this, setup the credentials on one Connection Broker and then share the credentials with other brokers, as follows.

To download the SSL credentials:

1. Go to the **> System > Maintenance** page

2. Select the **Download SSL credentials for installation on another Connection Broker** option.

3. Click **Next**. The following form opens



Download SSL Credentials

File name

leostream-ssl-2023-07-10

A .tgz extension will be automatically added to the file name

Create Credentials File

4. In the **File name** field, enter a file name for the downloaded SSL credentials.

5. Click **Create Credentials File**. The Connection Broker generates a `.tgz` file containing the SSL credentials and opens a Web page that allows you to download the credentials.

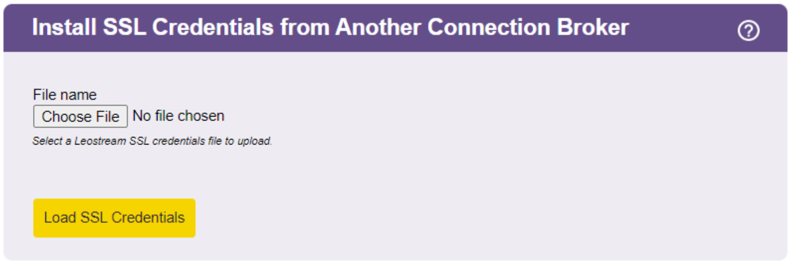
6. Click the **Click here** link in the Web page that opens and save the file locally on your machine.

To install these SSL credentials on another Connection Broker:

1. Go to the **> System > Maintenance** page

2. Select the **Install SSL credentials from another Connection Broker** option.

3. Click **Next**. The following form opens



Select a Leostream SSL credentials file to upload.

4. Enter or browse for the file name of the SSL credentials to install.

5. Click **Load SSL Credentials**.

Uninstalling an SSL Certificate

You can uninstall an SSL certificate as follows:

1. Go to the **> System > Maintenance** page.
2. Select the **Uninstall SSL certificate** option.

   This option only appears if you have installed a self-signed SSL certificate or a CSR. You cannot uninstall the default Leostream certificate.

3. Click **Next**. The **Uninstall the SSL certificate** page opens.
4. Click the **Uninstall** button to finish the process.

After the certificate is uninstalled, the Connection Broker restarts and uses the default Leostream certificate. The Connection Broker deletes the certificate's private key from the Connection Broker database when you uninstall the certificate.

Restarting the Connection Broker

This feature is available only when running your Connection Broker in debug mode.

You can restart the Connection Broker, as follows:

1. Select the **Reboot the Connection Broker** option on the **> System > Maintenance** page.
2. Click **Next**.

   The Connection Broker does not prompt you to confirm this action. The broker begins to reboot after five seconds. After the reboot completes, you must sign back into your Connection Broker.

Shutdown the Connection Broker Machine

This feature is available only when running your Connection Broker in debug mode.

You can shut down the Connection Broker, as follows:

1. Select the **Shutdown the Connection Broker** option on the **> System > Maintenance** page.
2. Click **Next**.

   The Connection Broker does not prompt you to confirm this action. The Connection Broker shuts down after 5 seconds.

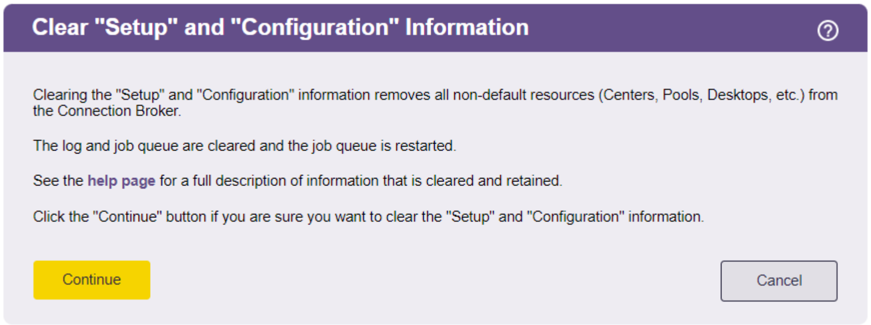
This option shuts down the operating system running the Connection Broker.

Purging Setup and Configuration in the Internal Database

You can clear all custom settings and configuration out your Connection Broker internal database, as follows:

1. Select the **Clear "Setup" and "Configuration" information** option in the **Database** Options section of the **> System > Maintenance** page.

2. Click **Next**. The following form opens.



Clear "Setup" and "Configuration" Information

Clearing the "Setup" and "Configuration" information removes all non-default resources (Centers, Pools, Desktops, etc.) from the Connection Broker.

The log and job queue are cleared and the job queue is restarted.

See the help page for a full description of information that is cleared and retained.

Click the "Continue" button if you are sure you want to clear the "Setup" and "Configuration" information.

3. To purge the database, click **Continue**. Click **Cancel** if you do not want to purge the internal database.

The Connection Broker cannot restore a purged database.

The Connection Broker purges the following items from the database:

- Authentication Servers
- Centers
- Clients
- Locations
- Logs
- Policies
- Plans
- Pools
- Desktops
- PCoIP Host Cards
- Users
- Roles
- Tags
- Message board
- Job queue

The Connection Broker does not purge the following items from the database:

- License key
- SSL certificate

- External database connection information
- Network setup
- General, SNMP, and log settings
- Remote backup settings and FTP site information
- Sign in terminology

Uploading Data from CSV Files

The Connection Broker allows you to create users and clients, as well as hard-assign users to desktops, by loading CSV formatted files into the Connection Broker database. To upload a file:

1. Select the radio button associated with the data you want to upload, either **Upload users**, **Upload desktops**, **Upload clients**, or **Upload PCoIP host devices**.

2. Click **Next**.

3. In the dialog that opens, enter or browse for the file to upload.

4. Click **Upload**.

Files must be formatted using comma separated values, where the first row contains the associated database field names. Do you use blank spaces before or after the commas.

Uploading Users

To upload users into the Connection Broker, the CSV-file must have the following format.

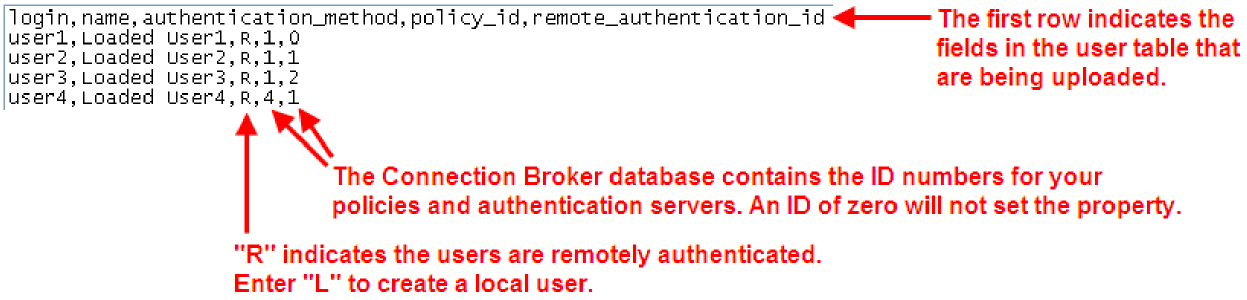
- The CSV-file must be comma delimited
- Quotes must be double quotes
- The first row must contain the field names, separated by commas with no additional blank spaces, and the data must be in the remaining rows
- The field names must match the field names in the user table in the data dictionary, including case
- The file must contain the `login` field, which is used to uniquely identify the user
- The *`xxx`*`_id` linkage fields (e.g., `role_id`) can contain either the numeric ID of the associated record or the name of the associated record
- The following fields cannot be edited:
  - `id`
  - `deleted`
  - `created`
  - `updated`
  - `last_login`

For a list of field names in the users table, go to:

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

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

For example, a file with the following contents loads four users into the Connection Broker.



```
login,name,authentication_method,policy_id,remote_authentication_id
user1,Loaded User1,R,1,0
user2,Loaded User2,R,1,1
user3,Loaded User3,R,1,2
user4,Loaded User4,R,4,1
```

The first row indicates the fields in the user table that are being uploaded.

The Connection Broker database contains the ID numbers for your policies and authentication servers. An ID of zero will not set the property.

"R" indicates the users are remotely authenticated. Enter "L" to create a local user.

If the value specified by `login` already exists in the Connection Broker and the user is remotely authenticated, the Connection Broker modifies the existing user record. If the value specified by `login` already exists in the Connection Broker as a remotely authenticated user and you are uploading a local user, a new user is created.

The **Uploaded** column on the **> Resources > Users** page displays **Yes** for users that were uploaded from a CSV-file.

If you do not specify the `authentication_method` field, the Connection Broker assumes the user is authenticated by one of the authentication servers defined on the **> Setup > Authentication Server** page. The first time the uploaded user logs into the Connection Broker, the **Authentication Server** column updates with the name of the authentication server used to authenticate the user and assign a policy.

Uploading Desktop Assignments

You can load a CSV-file to modify desktops already in the Connection Broker.

You cannot create new desktops using the bulk upload feature.

When uploading desktop 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 `vm` table in the data dictionary
- The modifiable fields are:
  - `display_name` – Text to enter into the desktop's **Display name** field.
  - `user_assignment_mode` – This case-sensitive field can take one of the following two values:
    - `H`: Indicates the desktop is hard assigned to the user
    - `P`: Indicates the desktop is policy assigned to the user
  - `user_id` – Either the numeric ID or name of the assigned user
- One of the following fields is required and must uniquely identify the desktop:
  - `id`
  - `name`

   - uuid

For a list of field names in the desktops table, go to:

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

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

Note: The bulk upload feature allows you to incorrectly policy-assign a desktop to a user via the CSV-file. If the CSV-file policy-assigns a desktop to a user, but the user's actual policy does *not* assign that desktop to the user, the user will not be presented with the desktop assigned by the CSV-file.

Uploading IPMI Settings for Desktops

The **Edit Desktop** page allows you to enable and configure IPMI settings for individual desktops. To simplify the setup for a large number of desktops, upload a CSV-file containing the IPMI information.

You cannot create new desktops using the bulk upload feature.

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

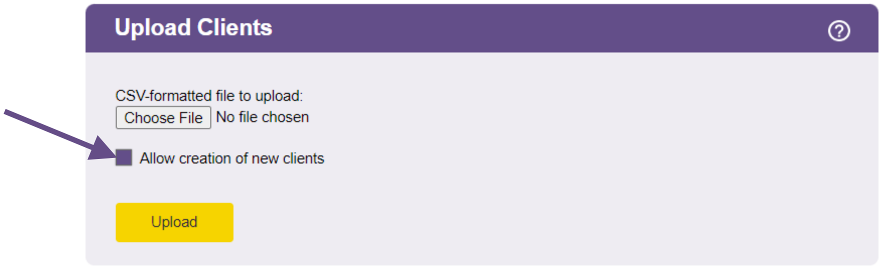
- The CSV-file must be comma delimited
- Quotes must be double quotes
- The first row must contain the field names, separated by commas with no additional blank spaces, and the data must be in the remaining rows
- The field names must match the field names in the `vm` table in the data dictionary
- The modifiable fields are:
   - `power_control_method` – set to a capital letter I to enable IPMI for this desktop
   - `ipmi_address` – enter the IPMI NIC IP address
   - `ipmi_username` – enter the IPMI username
   - `ipmi_password` – enter the IPMI password
- One of the following fields is required and must uniquely identify the desktop:
   - id
   - name
   - uuid

Physical desktops default to using Wake-on-LAN for power control so you must update the `power_control_method` field in order for the IPMI settings to take effect.

Ensure that the IPMI NIC is functioning properly before loading the file. The Connection Broker attempts to establish an IPMI v2 / RMCP+ session for each desktop when you upload the file.

Uploading Clients

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.



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
- The only modifiable fields are:
  - `client_assignment_mode`
  - `client_type`
  - `direct_to_host_policy_id` (for PCoIP clients, only)
  - `ip`
  - `vm_id`
- One of the following fields is required and must uniquely identify the client
  - `id` (for updating existing clients, only)
  - `ip` (for PCoIP clients, only)
  - `name`
  - `mac`
  - `serial_number`
- 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

To upload PCoIP clients, set the `client_type` to `blade`. Specifying a policy in the `direct_to_host_policy_id` field automatically selects the **Direct connect client to desktop** option for the client and sets the **Apply policy options from** drop-down menu to the entered policy. The `direct_to_host_policy_id` field does not apply to any other client type.

If the uploaded CSV-file contains PCoIP clients, the Connection Broker performs a scan of the PCoIP Devices center and updates the PCoIP client records with any additional information provided by the client.

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

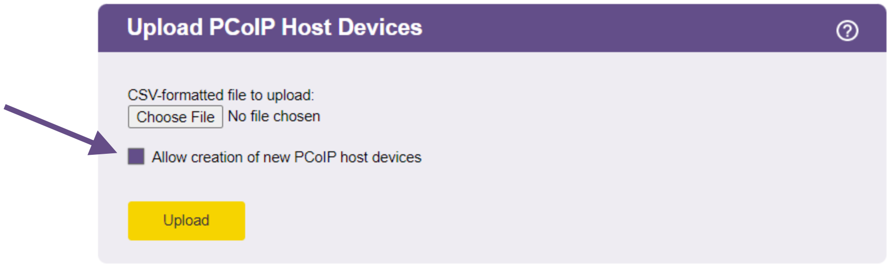
```
https://cb-address/download/account_db.html#client
```

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

Uploading PCoIP Remote Workstation Host Cards

If your Leostream license enables PCoIP support, the **> System > Maintenance** page contains an **Upload PCoIP host devices** option. Select this option to upload PCoIP Remote Workstation cards into the Connection Broker. In order for the Connection Broker to associated 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.

By default, the uploaded CSV-file modifies existing PCoIP host cards but 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. 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.



Upload PCoIP Host Devices
?
CSV-formatted file to upload:
Choose File
No file chosen
Allow creation of new PCoIP host devices
Upload

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)

After uploading a CSV-file of PCoIP host devices, the Connection Broker performs a scan of the PCoIP Devices center and updates the PCoIP host device records with any additional information provided by the host card.

For a list of field names and values in the PCoIP host card table, go to:

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

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

For more information, see the **Leostream Quick Start Guide for PCoIP Remote Workstation Cards**.

Checking Component Version Numbers

You can find version information for the Connection Broker, Leostream Connect, and Leostream Agent in the following locations:

- The Connection Broker version number appears at the bottom left of every page of your Connection Broker Web interface.
- For Leostream Connect:
  - If a user has logged into the Connection Broker via Leostream Connect, the Leostream Connect version number appears in the **Version** column of the **> Resources > Clients** page.
  - If Leostream Connect is running, select the **About** tab on the **Options** dialog, available from the Leostream Connect system tool tray menu.
- For the Leostream Agent:
  - If you installed the Leostream Agent on a desktop, the agent's version number appears in the **Leostream Agent Version** column on the **> Resources > Desktops** page.
  - On the remote desktop, the version is displayed in **About** tab of the Leostream Agent Control Panel dialog.