leostream

Remote Desktop Access Platform

Using Leostream with Nutanix AHV

Version 202x
July 2023

Contacting Leostream

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

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

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

Copyright

Trademarks

The following are trademarks of Leostream Corporation.

Leostream™
The Leostream graphical logo™

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

Microsoft, Active Directory and Windows are trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Other brand and product names are trademarks or registered trademarks of their respective holders. Leostream claims no right to use of these marks.

Patents

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

Contents

Chapter 1: Introduction and Architecture

Why use Leostream to Manage Your Nutanix VDI Environment

The Leostream Connection Broker now delivers the ability to manage virtual machines hosted on the Nutanix Acropolis Hypervisor (AHV). Leostream with Nutanix provides a complete VDI solution to satisfy a wide range of use cases.

This document describes how to configure the Leostream Connection Broker to manage capacity and user connections to virtual machines hosted on AHV.

For an introduction to Leostream, including a description of key concepts and components, please reference the Getting Started with Leostream Concepts guide available on the Leostream web site.

For complete details on using the Leostream Connection Broker, download the Connection Broker Administrator's Guide.

High-Level Architecture Diagrams

Leostream provides remote access to virtual machines hosted on AHV for both on-premises and remote users. How you architect your environment varies slightly based on which types of users you plan to support.

The diagrams in the following sections show where the Leostream platform components are located when working with AHV. For a complete architecture diagram, including external databases, authentication servers, and public clouds, see the section on "Network Level Access" in the Connection Broker Security Review document.

On-Premises Environments

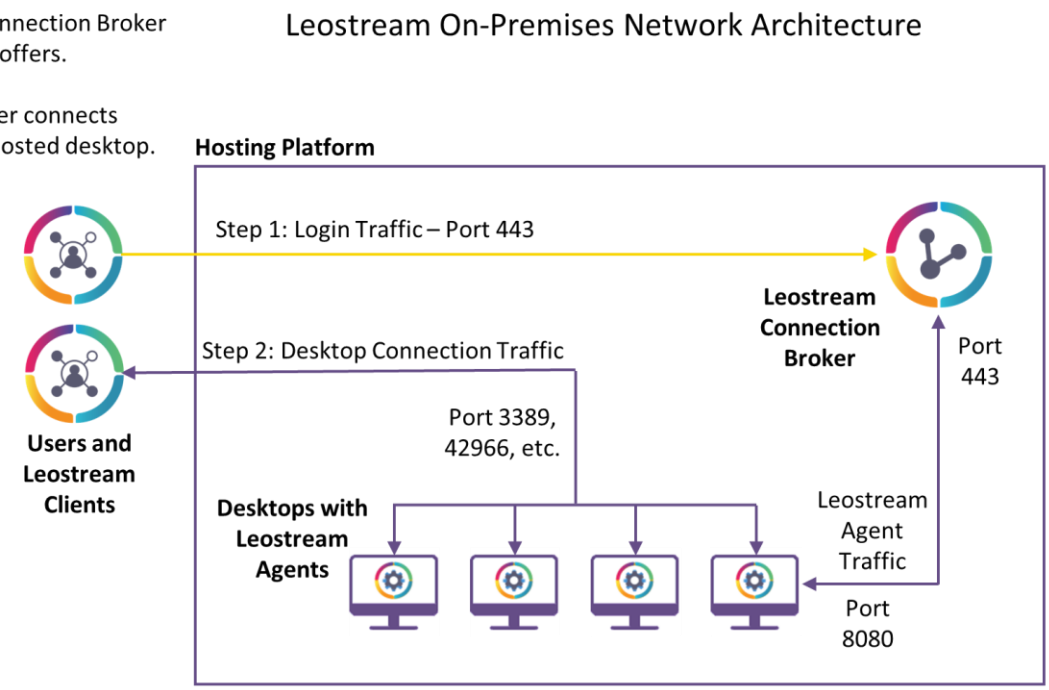
The simplest Leostream environments manage logins for users on the same network as your Nutanix infrastructure. This configuration requires a Connection Broker that is reachable by the user's client device and by the virtual machines hosted on Nutanix.

The desktops have installed Leostream Agents that communicate information about the user's desktop connection to the Connection Broker. The user's client may be running the Leostream Connect software client, but users can also log into Leostream from a Web browser or from a number of thin and zero clients.

The following diagram shows a high-level architecture, including the ports required for login, Leostream Agent, and desktop connection traffic.

Step 1. User logs into Connection Broker to receive their desktop offers.

Step 2. Connection Broker connects user's client directly to hosted desktop.



Arrows indicate direction in which communication is established. Responses return on same port.

Remote User Access

If you need to connect users that are outside your corporate network to desktops hosted on your Nutanix infrastructure, you can introduce the Leostream Gateway into your architecture. The Leostream Gateway provides three key pieces of functionality.

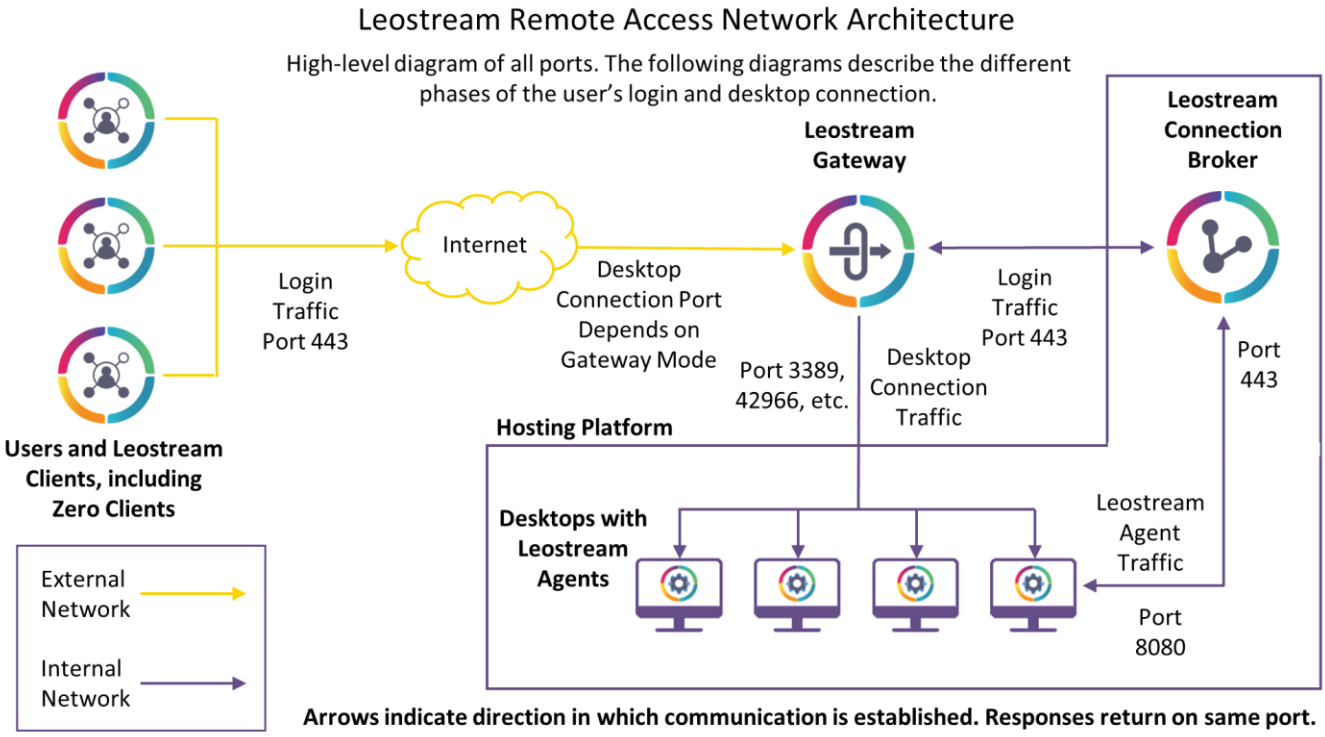
1. The Leostream Gateway forwards user login traffic to the Connection Broker, so the Connection Broker can authenticate the user and offer them the appropriate desktops.

2. The Leostream Gateway includes a built-in HTML5 RDP, VNC, and SSH viewer, allowing users to connect to their desktops inside of a Web browser without installing additional client software.

3. The Leostream Gateway forwards client-based display protocol traffic from the user's client outside

the network to the Nutanix hosted desktops.

The following diagram includes the Leostream Gateway in the high-level architecture. In the case of client-based display protocol traffic, the Leostream Gateway manages its firewall to redirect the traffic, opening and closing ports only when required by desktop connections. If you place the Leostream Gateway in a DMZ that includes additional firewalls, ensure that you open the appropriate ports.



Note that this Quick Start guide does not cover using the Leostream Gateway. For more information on configuring your Leostream environment to use the Leostream Gateway, see the Leostream Gateway Guide.

Chapter 2: Installing Leostream

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, on any operating system based on Fedora, or any other Linux distribution.

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

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

Prior to installing your Connection Broker, install the latest updates to the operating system. See the Leostream Installation Guide for full Connection Broker installation instructions and the procedure for applying your Leostream license.

Obtaining Your Leostream License

After installing your Connection Broker, you must obtain your Leostream license key. Your Connection Broker license key is derived from the serial number you received from Leostream Sales. If you did not receive your Leostream serial number, please contact sales@leostream.com.

You can generate the license key by logging into your Connection Broker Administrator web interface from any web browser with internet access, as follows.

1. Enter your Connection Broker address in your Web browser's URL edit field. The Connection Broker **Sign In** page opens.

2. Sign into the Connection Broker Web interface using the following default credentials:

   - **User name**: admin
   - **Password**: leo

3. Click **Sign In**. The **Leostream license** page opens.

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

5. 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.

   The installation code for your Connection Broker is automatically populated. If your Connection Broker does not have internet access, note the **Installation code** to the right of the form and navigate to the Leostream license server from a device with internet access.

6. In the **Leostream license key generator**, enter the Serial number you received from Leostream. If you do not have a Leostream Serial number, contact sales@leostream.com.

7. If the **Installation code** is not automatically populated, enter the Installation code listed on your Connection Broker.

8. In the **Email address** form, enter your email address.

9. Click **Generate a license**.

10. If you navigated to the Leostream license generator from your Connection Broker, click **Apply to the broker** to copy the new license key into your Connection Broker. Otherwise, copy the key into a text file.

11. Back on your Connection Broker **Leostream License** form, enter the license key you obtained from the Leostream license generator. Ensure that you include the BEGIN and END lines.

12. Click on the **License Agreement** link to view the end user license agreement. Select the **I have read and accept the License Agreement** option if you agree to the terms of the Leostream end user license agreement.

13. Click **Save**. The **Welcome** page opens, giving you the option to check for any Connection Broker updates.

Chapter 3: Preparing Master Images

Leostream can manage connections to existing Windows and Linux virtual machines, and can provision new virtual machines from OVAs or snapshots in your Nutanix platform. All VMs managed by Leostream should have an installed Leostream Agent configured to communicate with your Connection Broker.

Leostream Agents are available on the Leostream Product Downloads page. The Leostream Installation Guide contains complete instructions for installing the Leostream Agent.

When installing the Leostream Agent, ensure that you enter your Connection Broker address and that the agent registers with the Connection Broker.

You can use the **Test** button on the Leostream Agent Control Panel dialog to ensure that the Leostream Agent can contact the Connection Broker. To test if the Connection Broker can contact the Leostream Agent, go to the **> Resources > Desktops** page in the Connection Broker Administrator Web interface and click the **Status** link associated with the instance's record in the Connection Broker. Communication must work in both directions to use all Leostream functionality.

After you create your base virtual machine, either take a snapshot or export the VM as an OVA file to use for Leostream provisioning in pools.

- To create a snapshot, locate the master VM in Prism Element. Right-click on the VM and select **Take Snapshot**.
- To create an OVA, locate the VM in Prism Central. Right-click on the VM and select **Export to OVA.**


Nutanix recommends preparing master images with the Nutanix Guest Tools (NGT) or with the Nutanix VirtIO drivers. Leostream successfully provisions virtual machines from images that include NGT, however you will need to reinstall NGT on each VM after provisioning completes.

Chapter 4: Integrating with Your Nutanix Platform and Authentication Servers

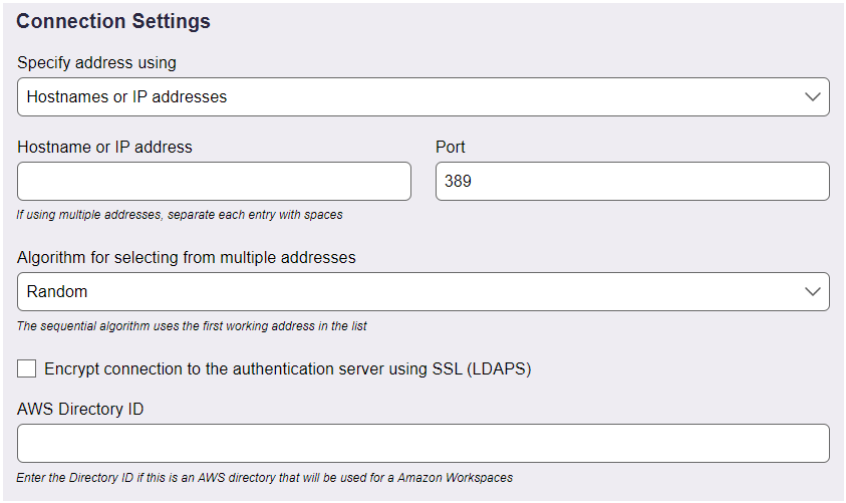
In the **Setup** section of the Connection Broker Administrator Web Interface, you integrate Leostream with the other components of your hosted desktop environment, such as your Nutanix cluster and your authentication servers.

The **Setup** section is also used to integrate your Connection Broker with the Leostream Gateway. Note that this Quick Start guide does not cover using the Leostream Gateway. For more information on configuring your Connection Broker to work with the Leostream Gateway, see the Leostream Gateway Guide.

Connecting to Your Authentication Servers

The Connection Broker can authenticate users against Microsoft Active Directory, OpenLDAP, and NIS authentication servers. To authenticate users, you first register your domain with your Connection Broker. For example, the following procedure shows how to integrate with Microsoft Active Directory.

1. Go to the **> Setup > Authentication Servers** menu.
2. Click the **Add Authentication Server** link.
3. In the **Add Authentication Server** form, enter a name for this server in the Connection Broker in the **Authentication Server name** edit field.
4. In the **Domain** edit field, enter the domain name associated with this Active Directory server.
5. In the **Connection Settings** section, shown in the following figure, use the following procedure to integrate with your Active Directory authentication server.



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

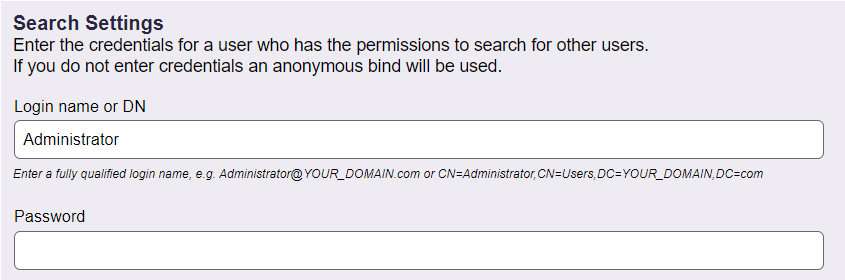
b. From the **Specify address using** drop-down menu, select **Hostname or IP address**.

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

d. Enter the port number in the **Port** edit field.

e. Check the **Encrypt connection to authentication server using SSL (LDAPS)** checkbox if you need a secure connection to the authentication server. The port number automatically changes to 636. Re-edit the **Port** edit field if you are not using port 636 for secure connections.

6. In the **Search Settings** section, shown in the following figure, enter the username and password for an account that has read access to the user records. Leostream does not need full administrator rights to your Active Directory authentication server.



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

8. Click **Save**.

Connecting to your Nutanix AHV Cluster

In order to manage existing virtual machines on your Nutanix cluster and to create and delete VMs, you need to create a Nutanix Acropolis center in your Leostream Connection Broker. The Connection Broker requires both the Prism Element and Prism Central APIs in order to be fully functional.

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

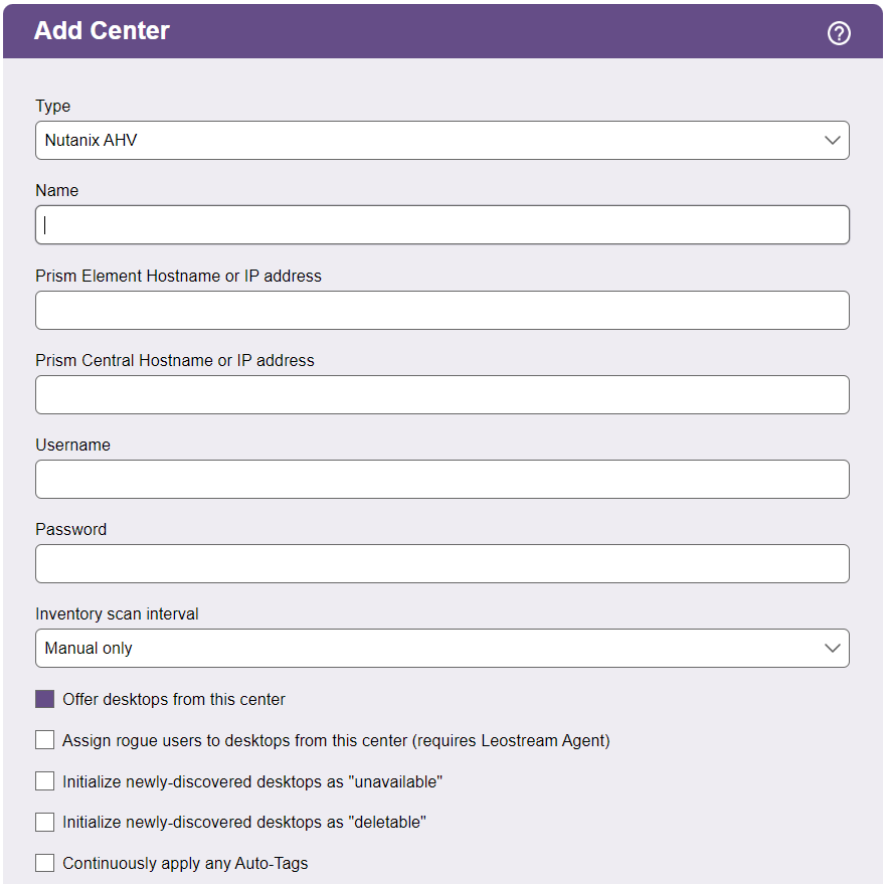
If your Nutanix environment uses a VMware hypervisor or includes OpenStack software, use the VMware or OpenStack center to manage your Nutanix cluster. Nutanix centers in Leostream apply only to virtual machines hosted on the AHV.

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.



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 images in your Connection Broker. Desktops are listed on the **> Resources > Desktops** page. Any 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.

Chapter 5: Pooling and Provisioning

After you create your centers and the Connection Broker inventories your desktops and images, the next step is to group the desktops into ***pools***. The Leostream Connection Broker defines a pool as any group of desktops. Pools can be nested within one another, to create sub-pools. These pools and sub-pools have three distinct functions in Leostream:

1. Organizing desktops on the **> Resources > Desktops** page
2. Provisioning new virtual machines in your Nutanix AHV cluster
3. Indicating the desktops that a user may connect to and how the Connection Broker manages the user's connection to those desktops

Creating Pools

When using Leostream to provision new instances on Nutanix, the key is to construct your pool in a way that ensures that newly provisioned desktops become members of that pool. One method to ensure this is to define your pool based on the instance name, which you set as one of your provisioning parameters, for example:

1. Go to the **> Configuration > Pools** page.
2. Click the **Create Pool** link. The **Create Pool** form opens.
3. Enter a name for the pool in the **Name** edit field.
4. In the first row of the **Desktop Attribute Selection** section:
    a. Select **Name** from the **Desktop attribute** drop-down menu.
    b. Select **begins with** from the **Conditional** drop-down menu.
    c. In the **Text value** field, enter the beginning of the name you will use for all the instances in this pool.
5. Click **Save** to save the pool.

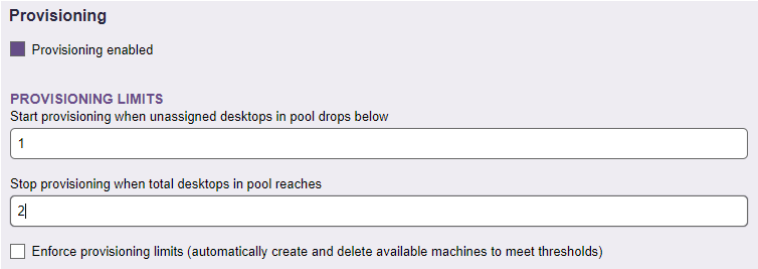
For a complete description of creating pools, including how to create a pool of all the desktops in your Nutanix center, see the "Creating Desktop Pools" chapter in the Connection Broker Administrator's Guide.

⚠ When using pools for provisioning, do not define the pool based on the desktop's operating system version or type. The Connection Broker does not know the operating system of the desktop at the time the desktop is provisioned, and therefore the desktop will not appear in the pool.

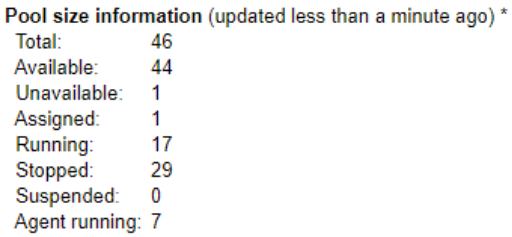
Provisioning New Instances

Your Leostream license determines if provisioning is enabled in your Connection Broker. If you do not see the options described in this section, contact sales@leostream.com to update your license key.

The **Provisioning** section of the **Edit Pool** page, partially shown in the following figure, allows you to configure when and how the Connection Broker creates new virtual machines in your Nutanix AHV cluster.



The Connection Broker determines when to create new VMs by comparing the thresholds specified in the **Provisioning Limits** section to the current metrics of the pool. If you edit an existing pool, the Connection Broker displays the current metrics of the pool to the right of the **Edit Pool** form, for example:



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 the provisioning limits and creates new instances at the following times

- When the pool is saved
- When a user is assigned to a desktop in this pool
- When any `pool_stats` or `pool_history_stats` job runs

The Connection Broker continues to provision new desktops whenever the lower threshold is crossed and 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.

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.

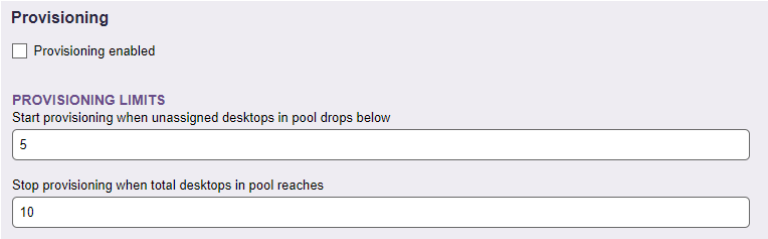
5. From the **Provisioning method** drop-down menu, select the appropriate option to indicate if you want to deploy new virtual machines from an OVA or from a snapshot.

6. In the **Deploy from image** or **Parent virtual machine and snapshot image** drop-down menu, select your master OVA or snapshot, respectively.

7. 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.

Disabling Provisioning

If you've set non-zero provisioning limits in your pool and need to temporarily disable provisioning, uncheck the **Provisioning enabled** check box, shown in the following figure.



The Connection Broker automatically disables provisioning in some cases when provisioning fails due to configuration errors in your pool. If this occurs, please check and correct your provisioning parameters before enabling provisioning.

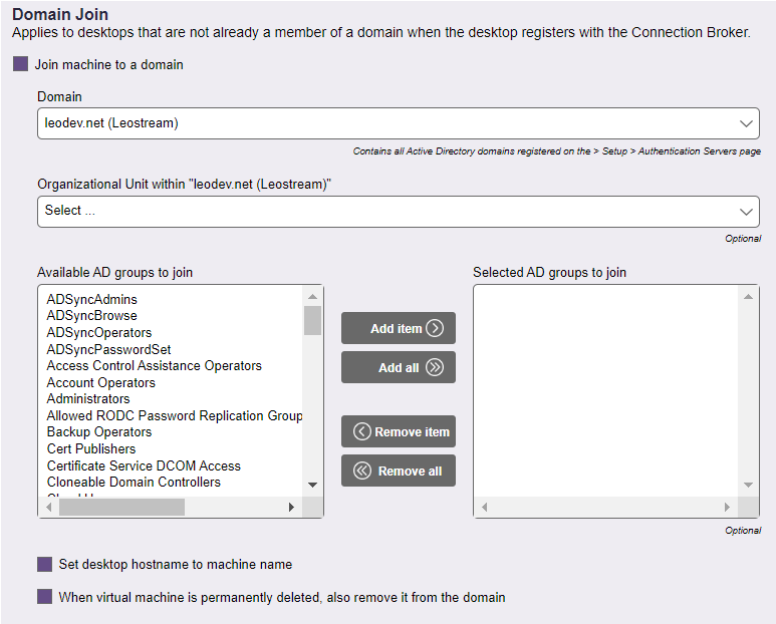
Joining Instances to a Domain

You can use Leostream to join desktops to any Active Directory domain you registered with your Connection Broker in Chapter 4. When enabled, the Connection Broker attempts to join a desktop to the domain as soon as the Leostream Agent on the desktop registers with the Connection Broker, for example, when a desktop is provisioned or when you reboot the desktop.

The desktop must have an installed and running Leostream Agent that is properly registered with your Connection Broker in order to be joined to a domain.

To enable domain joining for a pool:

1. Select the **Join virtual machine to a domain** option in the **Domain Join** section, shown in the following figure.



2. Select the domain from the **Domain** drop-down menu.

3. Optionally, from the **Organizational Unit** drop-down menu, select an OU for the desktops.

4. To add the desktop to one or more AD groups, select and move the groups from the **Available AD groups to join** to the **Selected AD groups to join** list.

5. To reset the desktops hostname when joining it to the domain, select the **Set desktop hostname to virtual 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.

   If the pool provisions new desktops, this is the name created by the value of the **Virtual machine name** field.

The **Name** field must contain a valid hostname, restricted by the following rules.

- 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.

6. If you are provisioning non-persistent desktops, select the **When virtual machine is permanently deleted, also remove it from the domain** to instruct the Connection Broker to delete the Computer record from your Active Directory server. If you do not select this option, the Computer record remains in AD after the VM is deleted

 Leostream performs the domain join for any desktop in the pool that is not already joined to a domain. Leostream does not have to provision the desktop to perform the domain join.

Chapter 6: Offering Desktops to Users

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

Defining Pool-Based Plans

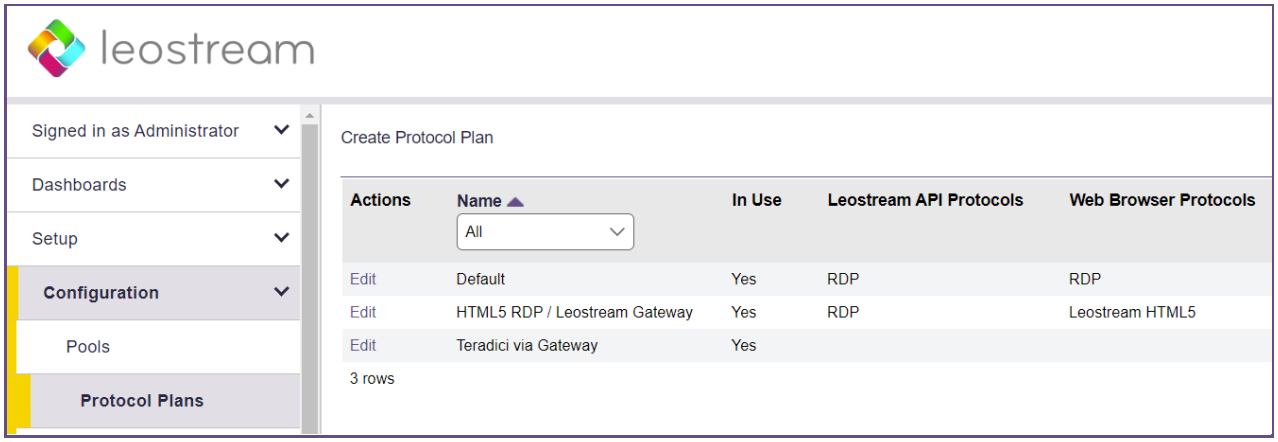
After you separate your desktops into pools, define the rules that control how the Connection Broker manages the user's connection to the desktops in those pools. To perform this step, ask yourself the following questions.

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

*The Leostream Connection Broker defines a **pool-based plan** as a set of rules that determine how the Connection Broker manages the connection to a desktop in a pool. This step describes three types of pool-based plans. 1) Protocol, 2) Power Control, and 3) Release. The Connection Broker also provides **location-based plans** for setting registry keys and attaching network printers to the remote desktop. See the Connection Broker Administrator's Guide for information on using location-based plans.*

Protocol Plans

Protocol plans determine the display protocol the Connection Broker uses to connect a user to their desktop. The Connection Broker contains one default protocol plan on the **> Configuration > Protocol Plans** page, shown in the following figure.



The default Protocol Plan instructs the Connection Broker to connect to the remote desktops using Microsoft RDP.

To create a new Protocol Plan, click the **Create Protocol Plan** link. The **Create Protocol Plan** form is divided into sections based on the type of client device used to log into Leostream, for example, Leostream Connect or the Leostream Web client.

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

In each section, indicate which protocol the Connection Broker should use to connect users to their desktops by selecting **1** from that protocol's **Priority** drop-down menu. Then, use the **Configuration file** and **Command line parameters** to determine how that connection is launched. For example, the RDP configuration file is a list of RDP-file parameters used to launch the RDP client.

See the Leostream Guide for Working with Display Protocols for more information on defining command line parameters and configuration files for each supported display protocol.

For a complete description of protocol plans, see "Building Pool-Based Plans" in the Connection Broker Administrator's Guide.

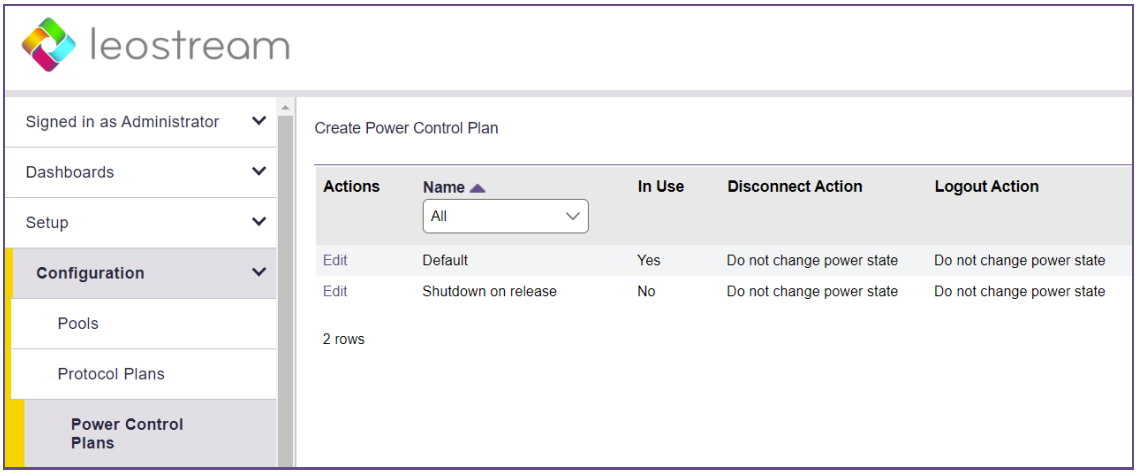
Power Control Plans

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

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

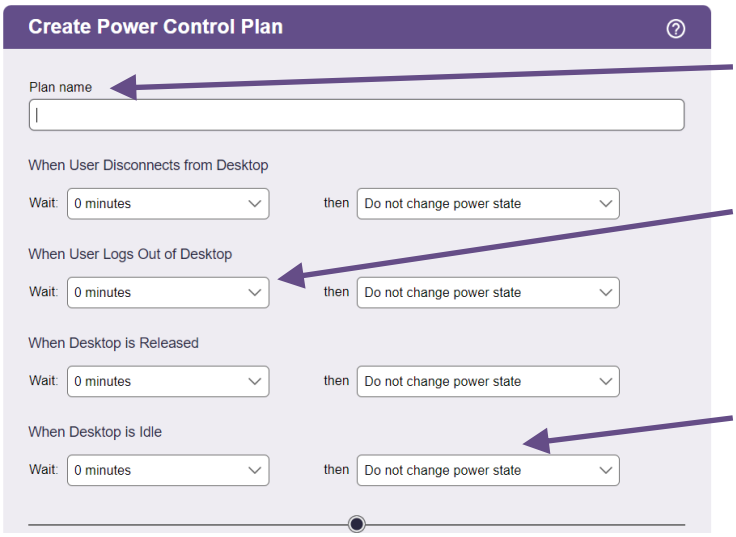
The remote desktop must have an installed and running Leostream Agent to allow the Connection Broker to distinguish between user logout and disconnect and to perform actions based on idle time.

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



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

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



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

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

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

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

3. For each of the remaining sections:

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

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

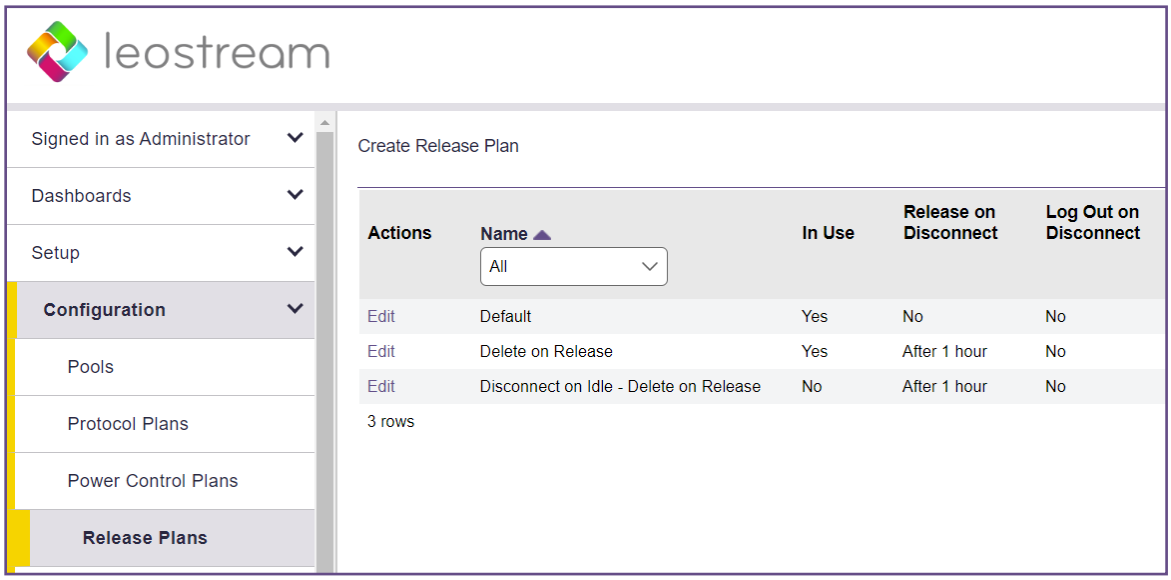
4. Click **Save** to store the changes or **Cancel** to return to the **> Configuration > Power Control Plans** page without creating the plan.

Release Plans

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

---

*When a desktop is **assigned** to a user, the Connection Broker always offers that desktop to that user, regardless of where the user logs in, and to no other users. Desktops can be policy-assigned or hard-assigned. For a description of hard-assigned desktops, see the Connection Broker Administrator's Guide.*



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

For example, to build a release plan that schedules a logout one hour after the user disconnects from their desktop and deletes the virtual machine when it is released from the user:

1. Click the **Create Release 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.

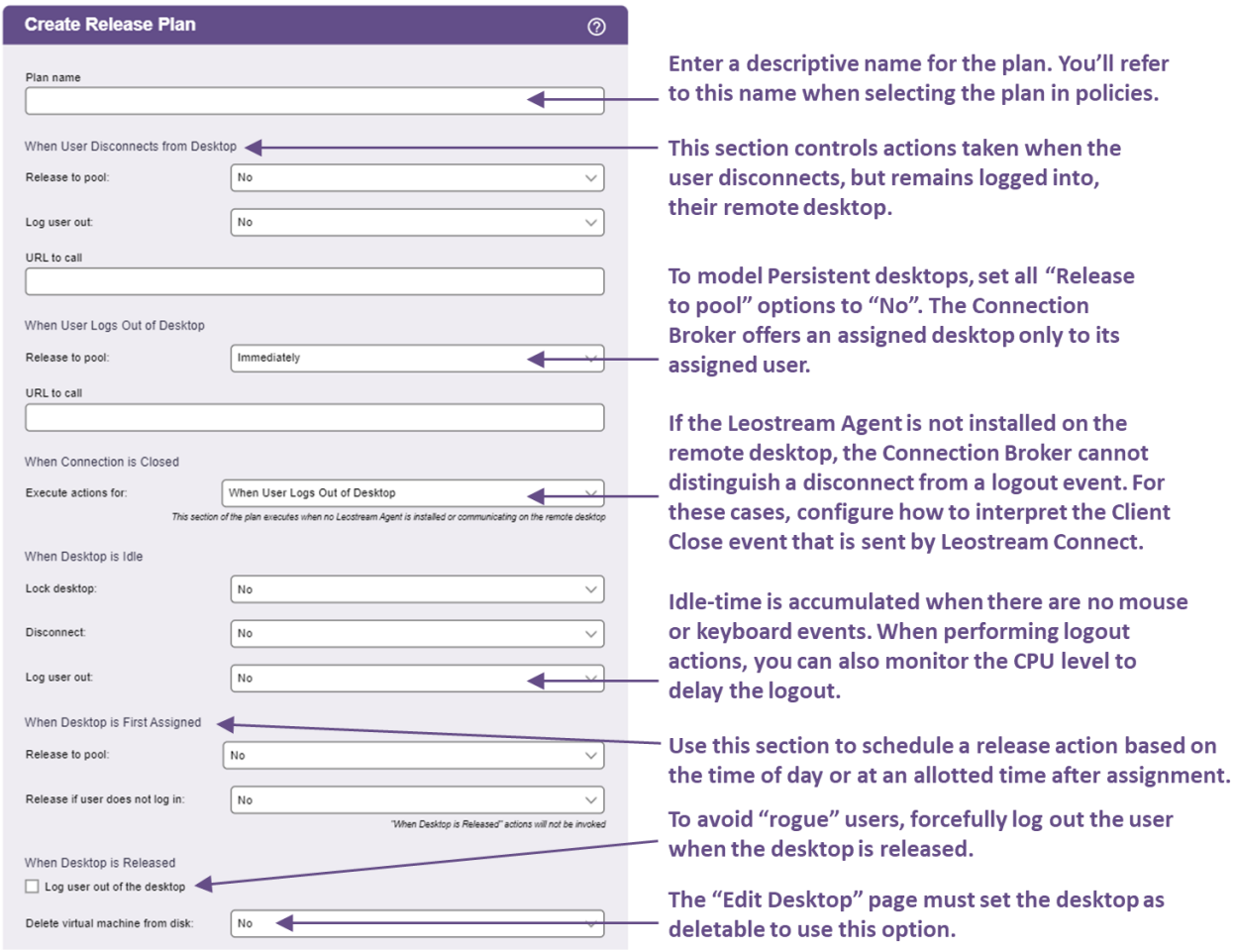
3. To build the Release Plan for our example, in the **When User Disconnects from Desktop** section, select **after 1 hour** from the **Log user out** drop-down menu.

4. In the **When Desktop is Released** section, select **Immediately** from the **Delete virtual machine from disk** drop-down menu.

5. Click **Save**.

When using this release plan, the Connection Broker forcefully logs the user out an hour after they disconnect from their desktop. The logout event then triggers the **When User Logs Out of Desktop** section of the release plan, which releases the desktop back to its pool and removes the user's assignment to the desktop. The *release* event triggers the **When Desktop is Released** part of the plan, which then deletes the virtual machine from your Nutanix AHV cluster.

The following figure shows the full form for creating Release Plans. For more details on creating and using release plans, see the "Release Plans" section in Chapter 11 of the Connection Broker Administrator's Guide.



Building User Policies

After you define your pools and plans, build policies.

*The Leostream Connection Broker defines a **policy** as a set of rules that determine which pools to offer desktops from, which display protocol to use to connect to those desktops, which power control and release plans to apply to those desktops, which USB devices the user can access in their remote desktop, and more.*

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

1. Navigate to the **> Configuration > Policies** menu.
2. Click the **Create Policy** link.
3. In the **Create Policy** form, enter a name for the policy in the **Policy name** edit field. For a discussion

on the remaining general policy properties, see the Connection Broker Administrator's Guide.

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

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

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

7. In the **When User Logs into Connection Broker** section use the **Number of desktops to offer** drop-down menu to indicate the number of desktops to offer to a user of this policy.

8. Also, in this section, use the **Pool** menu to select the pool to offer desktops from. When a user is offered this policy, the Connection Broker sorts the desktops in the selected pool based on the other Pool Assignment settings, then offers the user the top *n* desktops from the pool, where *n* is the number selected in the **Number of desktops to offer** drop-down menu.

9. Scroll down to the **Plans** section to select the protocol, power control, and release plans to apply to desktops offered from this pool.

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

10. Click **Save**.

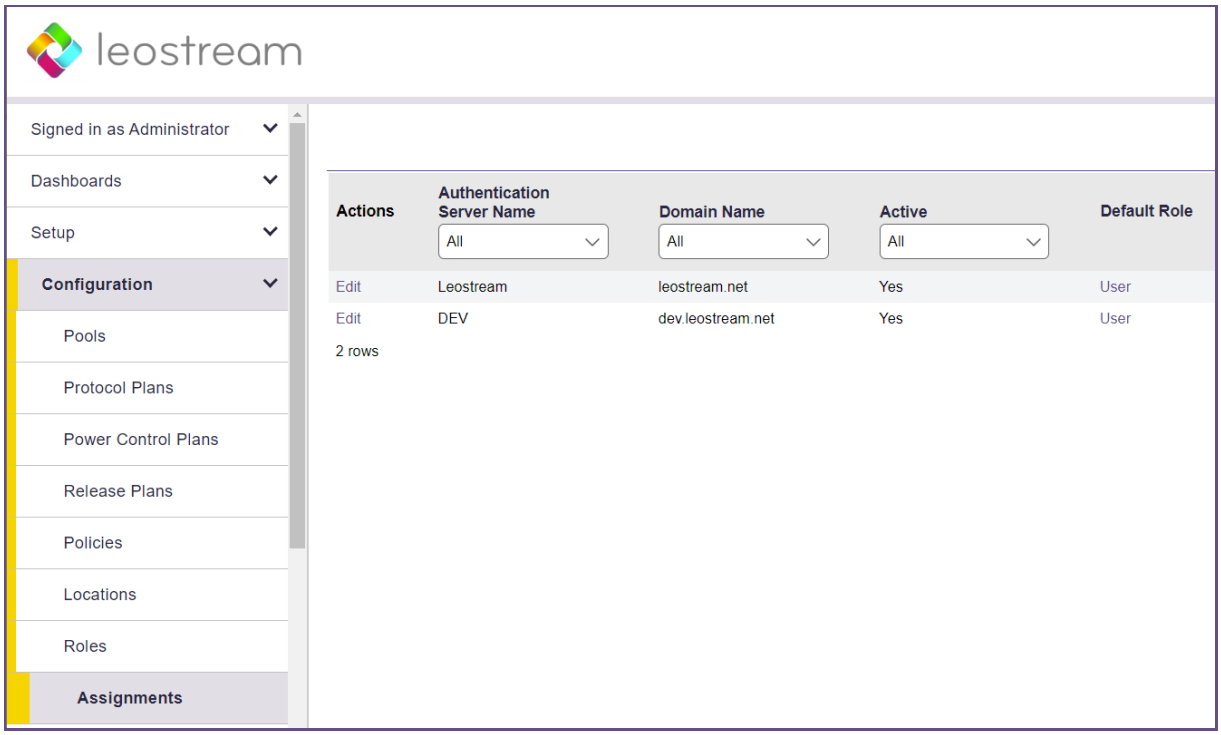
 *A policy can offer desktops from multiple pools. Click the **Add Pool Assignment** link to add a new pool, or use the kebab menu to clone an existing Pool Assignment to simplify initializing the options for an additional pool.*

See the "Configuring User Experience by Policy" chapter of the Connection Broker Administrator's Guide for information on using the additional options in the **Create Policy** form.

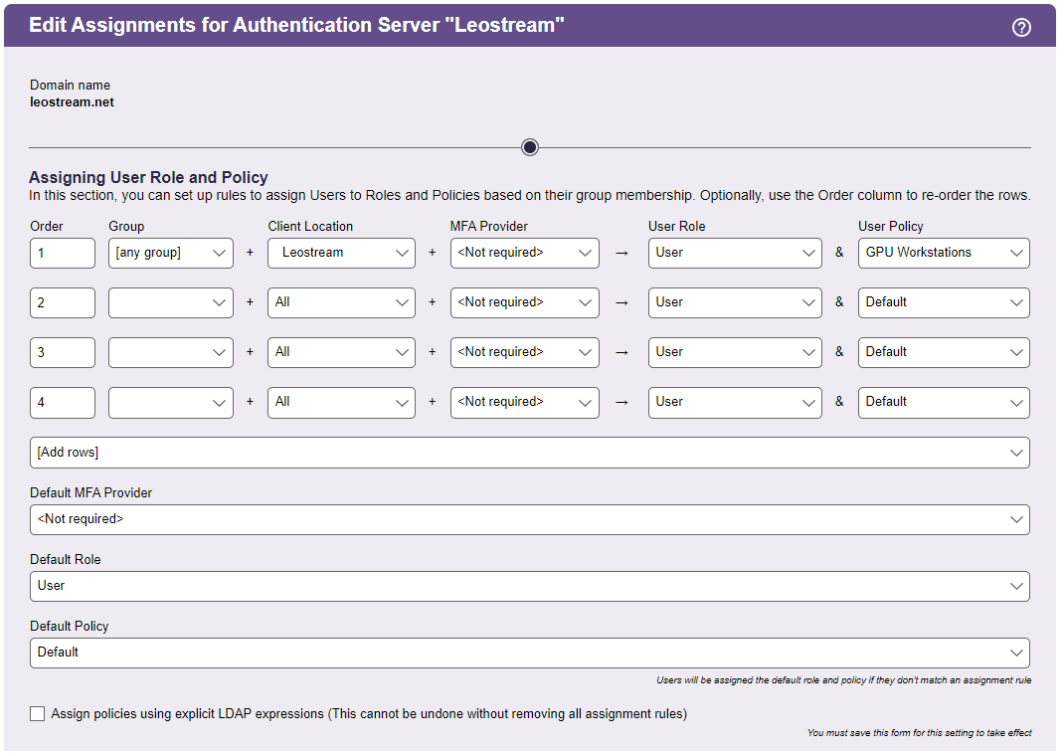
Assigning Policies to Users

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

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



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



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

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

To assign policies based on the user's `memberOf` attribute:

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

*In Leostream, **roles** are permissions that control the actions an end user can take on their desktop and the level of access the user has to the Connection Broker Administrator Web interface. A **location** is a group of clients defined by attributes such as manufacturer, device type, OS version, IP address, etc. For more information on building roles and locations, see Chapters 10 and 13 in the Connection Broker Administrator's Guide.*

4. Assign a policy to this group and client location pair by selecting an item from the **User Policy** drop-down menu.

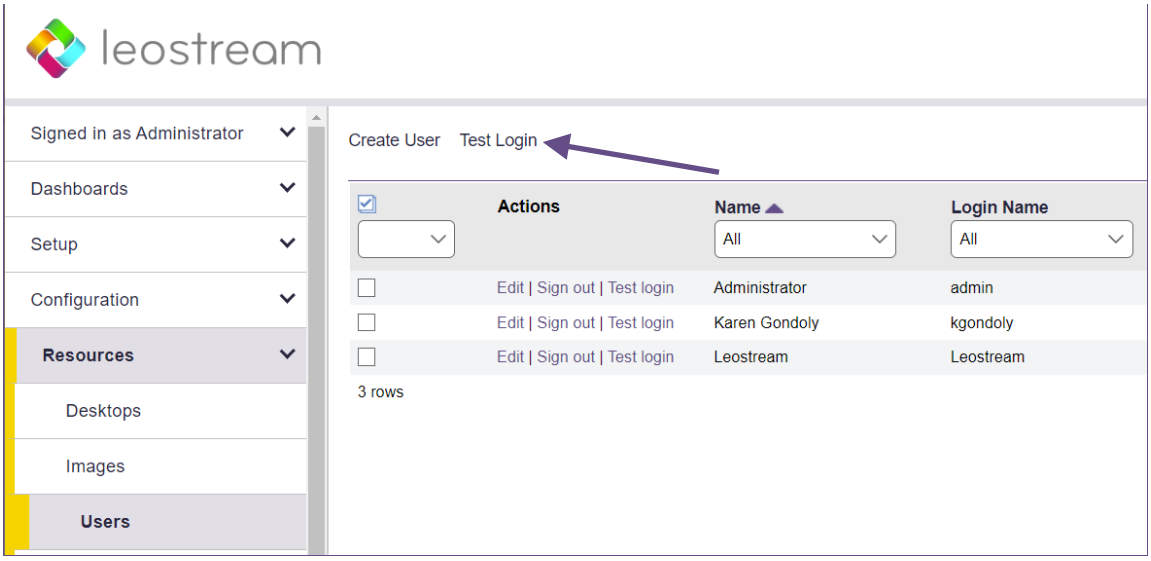
If you need to assign roles and policies based on a different user attribute, see "Assigning Roles and Policies Based on any Attribute" in Chapter 14 of the Connection Broker Administrator's Guide. To learn about options for enforcing MFA for policy assignments see the Leostream guides for Using RADIUS Servers for MFA, Using SAML-Based Identity Providers, and Using Duo MFA with Leostream.

Testing Your Connection Broker Configuration

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

1. Navigate to the **> Resources > Users** menu. As users log into your Leostream environment, their user information is added to this page. You do not need to load users before they can log in.

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



3. In the **Test Login** form that opens, enter the name of the user to test in the **User Name** edit field.

4. If you are allowing the user to specify their domain, select a domain from the **Domain** drop-down.

5. Click **Run Test**. The Connection Broker searches the authentication server for your user, and then presents a report, for example:

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

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

Trying to match with Authentication Server Assignment rules: (edit)
1: "memberOf" exactly matches "CN=Karen Test Sub Group,OU=Karen Test,OU=Karen Groups,DC=leostream,DC=net", location "All" ← no attribute match
2: "memberOf" exactly matches "CN=Students,OU=Security Groups,DC=leostream,DC=net", location "All" ← **matched**
User will have Role "User" and Policy "Default"
User must first successfully authenticate with RADIUS server "Okta RADIUS Agent" ← **PIN+token not provided**
User's role provides access to Web Client, only.

Policy: Default (edit)

No hard-assigned desktops found

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

(389 total, 383 in service, 18 policy filtered, 18 pool filtered, 18 available, 8 running, 8 with an IP address)
kdg-debian9 ← **available**, running, Leostream Agent v5.1.22.0, will offer as: "kdg-debian9", will connect via RDP (show) ← will use protocol plan "Default" associated with policy Default
kdg-1803 ← **available**, running, Leostream Agent v7.3.13.0, will offer as: "kdg-1803", will connect via RDP (show) ← will use protocol plan "Default" associated with policy Default

Offering two desktops with this policy.

See “Testing User Role and Policy Assignment” in the Connection Broker Administrator’s Guide for information on interpreting test login results.

Please complete a login test before contacting Leostream Support.