leostream®

Remote Desktop Access Platform

Using the Leostream® Platform to Manage VDI in Microsoft Azure Clouds

Provide Remote Access to Hybrid Cloud Environment

Version 202x
August 2024

Contacting Leostream

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

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

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

Copyright

Trademarks

Patents

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

Contents

CONTENTS **3**

CHAPTER 1: INTRODUCTION **4**

CHAPTER 2: INSTALLING THE LEOSTREAM PLATFORM IN MICROSOFT AZURE **5**

LAUNCHING A CONNECTION BROKER VIRTUAL MACHINE 5
INSTALLING THE CONNECTION BROKER 5
OBTAINING YOUR LEOSTREAM PLATFORM LICENSE 6

CHAPTER 3: PREREQUISITES FOR INTEGRATING WITH MICROSOFT AZURE **7**

STEP 1 OF 5: OBTAINING YOUR SUBSCRIPTION ID 7
STEP 2 OF 5: CREATING AN APPLICATION (CLIENT) ID 7
STEP 3 OF 5: FINDING THE DIRECTORY (TENANT) ID 8
STEP 4 OF 5: GENERATING A SECRET KEY VALUE 8
STEP 5 OF 5: ASSIGNING YOUR LEOSTREAM APPLICATION TO A ROLE 9

CHAPTER 4: PREPARING AZURE INSTANCES AND IMAGES **10**

CHAPTER 5: INTEGRATING THE LEOSTREAM PLATFORM WITH AZURE **11**

CONNECTING TO YOUR MICROSOFT ACTIVE DIRECTORY SERVER 11
CONNECTING TO YOUR AZURE SUBSCRIPTION 12

CHAPTER 6: POOLING AND PROVISIONING IN AZURE **14**

CREATING POOLS 14
PROVISIONING NEW INSTANCES 14
DISABLING PROVISIONING 17
JOINING INSTANCES TO A DOMAIN 18

CHAPTER 7: OFFERING DESKTOPS TO USERS **20**

DEFINING POOL-BASED PLANS 20
Protocol Plans *20*
Power Control Plans *21*
Release Plans *23*
BUILDING USER POLICIES 25
ASSIGNING POLICIES TO USERS 26
TESTING YOUR CONNECTION BROKER CONFIGURATION 28

Chapter 1: Introduction

The Leostream Connection Broker makes it possible to manage capacity and connections to virtual workspaces in Microsoft® Azure® clouds. The Leostream platform provides the tools necessary to satisfy a wide range of use cases and maximize the utility of desktops and applications hosted in the public cloud. With the combination of the Leostream platform and Azure, you can:

1. Provide desktops on-demand – provision virtual workspaces in minutes, preconfigured from customized images created in your Azure account.

2. Support multi-tenancy – separate departments, customers, etc., using Azure subscriptions, to provide isolated networks and manage resources independently.

3. Improve security – keep data off of the end user's client device, to ensure that sensitive data never leaves the cloud.

4. Lower costs – avoid licensing fees associated with commercial VDI or DaaS stacks and pay low hourly usage fees for Azure compute and storage.

This document describes important aspects to consider when configuring Azure for use with the Leostream platform. For an introduction to the Leostream platform, including a description of key concepts and components, please reference the Introduction to the Leostream Platform guide available on the Leostream web site.

Chapter 2: Installing the Leostream Platform in Microsoft Azure

Launching a Connection Broker Virtual Machine

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 Leostream Connection Broker requires, at least, the following resources:

- 2 vCPU
- At least 8 Gbytes of RAM
- At least 20 Gbytes of hard drive space
- One NIC, ideally with Internet connectivity

When installing into a cloud environment, note that the cloud hosting provider may reserve some of the instance CPU. To avoid triggering health check errors in your Connection Broker, select an instance size with more than 8GB of RAM.

Ensure that the Connection Broker Network Security Group allows inbound traffic on port 443 and port 80 to provide access to the Administrator Web interface, and on port 22 to provide SSH access to the virtual machine. Leostream Agents contact the Connection Broker on port 443.

Installing the Connection Broker

Prior to installing your Connection Broker, install the latest updates to the operating system. Before you can access Leostream Platform 202x, you must have a valid Leostream license that enables access to Leostream Platform 202x. If you are unsure if you have access, please contact sales@leostream.com.

You can download the Connection Broker installation file from the following page.

https://license.leostream.com/download.html

See the Leostream Installation Guide for instructions on how to complete the installation.

Obtaining Your Leostream Platform License

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

You can generate the license key from the Connection Broker Administrator web interface if your Connection Broker has internet access, as follows.

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

3. If your Connection Broker has internet access, click the link to go to https://license.leostream.com.

   The installation code for your Connection Broker is automatically populated.

4. In the **Leostream license key generator**, enter the serial number you obtained from the Leostream Sales team.

5. In the **Leostream license key generator**, 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**.

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

Chapter 3: Prerequisites for Integrating with Microsoft Azure

This chapter discusses the key requirements when setting up your Azure account to use with the Leostream platform.

The Connection Broker must authenticate with your Azure account in order to access the Azure Management API used to manage the VDI environment. Before you can connect your Leostream platform to your Microsoft Azure account, you must do the following:

1. Obtain your subscription ID
2. Register the Connection Broker application and get the application ID
3. Find the tenant ID for the application
4. Generate a secret key
5. Assign the Connection Broker application to an appropriate role

You need the three IDs and secret key to create your Azure center in your Leostream Connection Broker. As you step through this procedure, copy this information into a document for future use.

Step 1 of 5: Obtaining your Subscription ID

You can use the Leostream platform to manage VDI in any Microsoft Azure subscription, including the free subscription. Determine the subscription you will use for your Leostream environment, then find its subscription ID, as follows.

1. Log into the Microsoft Azure portal.

2. Click on the **All services** item in the left menu and then click on **Subscriptions** in the list of General services.

3. Select the subscription you want to use from the list of subscriptions.

4. Locate and copy the **Subscription ID** from the **Overview** of the subscription. Save this value to a location where you can access it from your Connection Broker.

Step 2 of 5: Creating an Application (Client) ID

Register your Connection Broker application with your Microsoft Entra ID.

1. In the Azure portal, select **Microsoft Entra ID** from the left-hand navigation pane.

2. From the list of actions below the **Manage** header, select **App registrations**.

3. At the top of the list of application registrations, click the **New registration** button.

4. In the **Register an application** pane, enter the following information.

    a. Enter a **Name** for your Leostream application.

    b. Specify that this application is used in this organizational directory only.

    c. Click **Register**.

5. After creating the application, copy the **Application (client) ID** and **Directory (tenant) ID** and save these values along with your subscription ID from step 1. The Application ID is the Client ID you'll use to create your Azure center in your Leostream Connection Broker.

Step 3 of 5: Finding the Directory (Tenant) ID

If you did not copy your Directory ID during Step 2, you can obtain your Directory (tenant) ID from the endpoints associated with your Leostream application, as follows.

1. If you navigated away from the App registrations list, follow steps 1 and 2 in the previous section to return to the list.

2. Click the **Endpoints** icon above the application list.

3. Click the copy icon to the right of the first endpoints in the **Endpoints** pane.

4. Your tenant ID is the UUID after the domain name, for example:

    `https://login.windows.net/`***`<your-tenant-id-is-here>`***`/saml2`

    Save this value along with your subscription ID and Application ID from steps 1 and 2.

Step 4 of 5: Generating a Secret Key Value

Next, generate a secret key value for your Leostream application, as follows.

1. If you navigated away from the App registrations list, follow steps 1 and 2 in the section on creating an Application ID to return to the list.

2. Select your Leostream application.

3. Below the **Manage** heading, select **Certificates & secrets**.

4. In the **Client secrets** pane, click **New client secret**.

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

    a. Enter a **Key description**, such as "Leostream key."

    b. Select an appropriate duration time.

c. Click the **Add** button at the top of the pane.

d. After the key is created, copy the key value displayed in the **Value** column. Save this value along with the three IDs you created in the previous steps.

   NOTE: You must copy the key at this point in the process. The key will be hidden the next time you navigate to this page.

Step 5 of 5: Assigning your Leostream Application to a Role

You must assign the Leostream application to a role in order to grant it permissions to perform actions in your Azure subscription or resource group, as follows.

1. Click on the **All services** item in the left menu and then click on **Subscriptions** in the list of General services. Alternatively, you can follow through this procedure for a particular Resource Group.
2. From the list of subscriptions, select the subscription you are using with your Leostream platform.
3. In the subscription, select **Access control (IAM)**.
4. At the top of the **Access control** pane, click **Add** and select **Add role assignment**.
5. In the **Role** step of the **Add role assignment** pane, go to the **Privileged administrator** roles tab.
6. Select **Contributor** from the list of roles and click **Next**.
7. In the **Members** tab, leave **User, group, or service principal** selected and click the **Select members** link.
8. Type the name of your Leostream registered application in the **Select** edit field and hit your **Enter** key. Your Leostream registered app should be displayed below the edit field.
9. Select your Leostream application and click **Select**.
10. Click **Review + assign**.
11. Click **Review + assign** a second time to add the role.

Chapter 4: Preparing Azure Instances and Images

The Leostream platform can manage connections to existing Windows and Linux Azure instances, and can provision new Azure instances from existing Azure images. All instances managed by the Leostream platform must have an installed Leostream Agent that can communicate with the Connection Broker. The Leostream Agents are available on the Leostream Product Downloads page. The Leostream Installation Guide contains complete instructions for installing the Leostream Agent.

During installation, you can specify the address of the Connection Broker that manages the instance. If the Connection Broker and instance are in the same private network, you can point the Leostream Agent at the Connection Broker's private IP address. Otherwise, to ensure proper communication between the Connection Broker and Leostream Agents, use the Connection Broker public IP.

After the Leostream Agent is installed, 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 platform functionality.

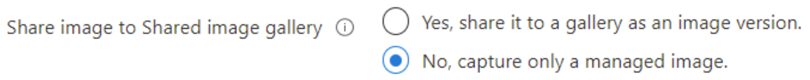
If you plan to use the Leostream platform to provision new instances in Azure, and to have the Connection Broker join the new instances to your Active Directory domain, please adhere to the following guidelines.

- The instance used to create the image must not be joined to the domain. The Connection Broker only joins instances to a domain if they are currently part of a Workgroup.

- The instance must have an installed Leostream Agent that is registered with your Connection Broker. If the Leostream Agent cannot communicate with the Connection Broker, new instances will not be joined to the domain.

- Run `sysprep` on the master VM prior to taking the image.

- When capturing an image of your virtual machine in Azure, ensure that you capture a managed image, for example:



Share image to Shared image gallery ⓘ ○ Yes, share it to a gallery as an image version.
● No, capture only a managed image.

⚠ Do not share the image to a gallery as an image version. You cannot currently use images in a Shared Images Gallery for provisioning within the Leostream platform.

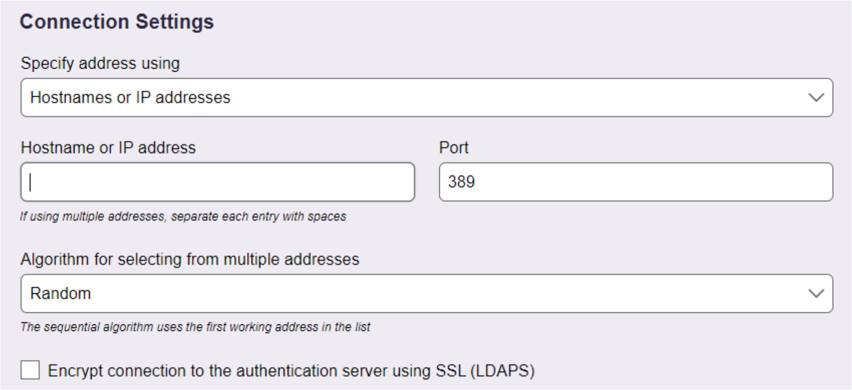
After you create an image from an instance following the previous guidelines, you can configure Leostream pools that automatically provision new capacity in Azure.

Chapter 5: Integrating the Leostream Platform with Azure

Connecting to Your Microsoft Active Directory Server

To authenticate users with a Microsoft Active Directory server, you must first register that domain with your Connection Broker, as follows. Note that you cannot connect to Microsoft Entra ID using the following procedure. Instead, treat Entra ID as a SAML-based identity provider, as described in the Leostream guide for Using Microsoft Entra ID and Azure MFA with the Leostream Platform.

1. Go to the **> Setup > Authentication Servers** menu.
2. Click the **Add Authentication Server** link.
3. In the **Add Authentication Server** form, select **Active Directory** from the **Type** drop-down list.
4. Enter a name for this server's record in the **Authentication Server name** edit field.
5. In the **Domain** edit field, enter the domain name associated with this Active Directory server.
6. In the **Connection Settings** section, shown in the following figure, use the following procedure to integrate with your Active Directory authentication server.



Connection Settings

Specify address using: Hostnames or IP addresses

Hostname or IP address: |

Port: 389

If using multiple addresses, separate each entry with spaces

Algorithm for selecting from multiple addresses: Random

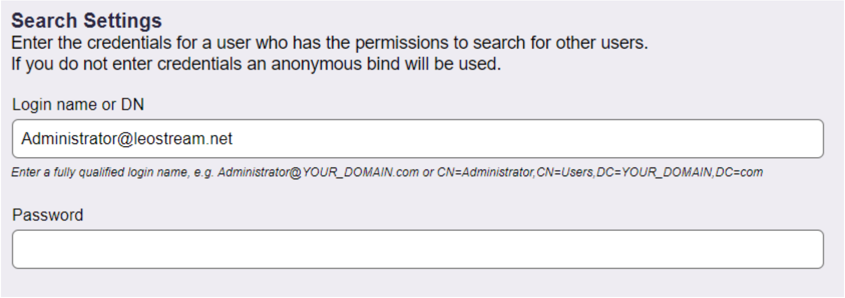
The sequential algorithm uses the first working address in the list

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

   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** 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.

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



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

Login name or DN

Administrator@leostream.net

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

Password

8. 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 your Leostream environment.

9. Click **Save**.

Connecting to Your Azure Subscription

In order to manage Azure instances, you need to create an Azure 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.*

Your Connection Broker must be able to access the following internet addresses in order to connect to your Microsoft Azure account:

login.microsoftonline.com, port 443
management.azure.com, port 443
xxxx.blob.core.windows.net, port 443, where *xxxxx* can be any Azure storage account name

Note that these hostnames typically resolve to different IP addresses with each call.

If your Connection Broker cannot access these addresses, you leverage the Leostream Gateway to perform Azure API forwarding to the above addresses. See the Leostream Gateway guide for information on enabling Azure API forwarding.

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 application ID into the **Application (client) ID** edit field.

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

10. 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 completes and the next refresh action begins.

11. Select the **Use a Leostream Gateway to communicate with this Center** option if you need to leverage a Leostream Gateway to connect to the required internet addresses.

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

The instances in the center's Azure region appear on the **> Resources** > **Desktops** page. The images available for provisioning appear on the **> Resources > Images** page. See the "Working with Desktops" section of the Connection Broker Administrator's Guide for information on viewing, editing, and controlling desktops from within the Connection Broker.

Chapter 6: Pooling and Provisioning in Azure

The Leostream Connection Broker defines a ***pool*** as any group of desktops. Pools can be nested within one another, to create sub-pools. Pools and sub-pools have three distinct functions in Leostream:

1. Organizing desktops on the **> Resources > Desktops** page
2. Provisioning new virtual machines in Azure
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 the Leostream platform to provision new instances in Azure, the key is to construct your pool in a way that ensures that newly provisioned desktops become members of that pool. One method is to set the pool to contain all instances in the Azure region associated with the center you created in the previous chapter.

If that pool definition is too broad, another easy way to ensure that new desktops become part of a pool is to define the pool based on the instance name, which you set during provisioning, 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 name you will use for all the instances in this pool.

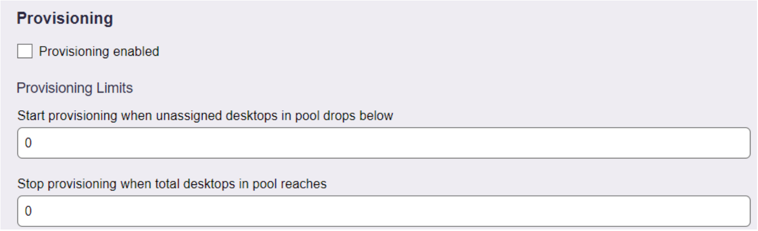
5. Click **Save** to save the pool.

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

Provisioning New Instances

Your Connection Broker 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 allows you to configure when and how the Connection Broker creates new instances in your Azure cloud. To begin, check the **Provisioning enabled** checkbox, as shown in the following figure.



Provisioning

□ Provisioning enabled

Provisioning Limits

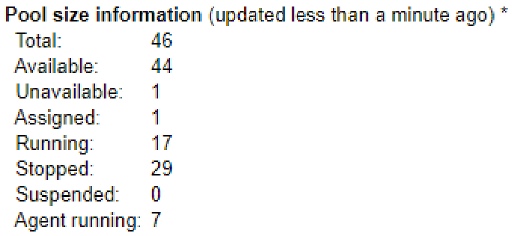
Start provisioning when unassigned desktops in pool drops below

0

Stop provisioning when total desktops in pool reaches

0

The Connection Broker 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 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, 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 the Leostream platform provisions new instances 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, the Connection Broker 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. The Leostream platform 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.

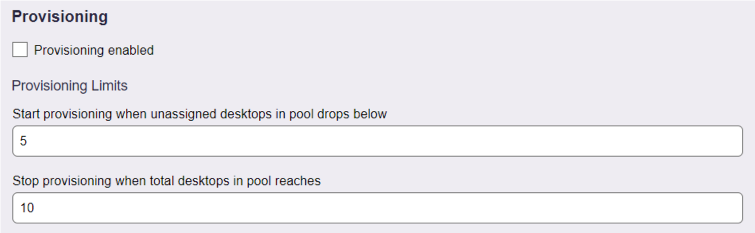
19. Select the **Mark newly provisioned desktops as deletable** option to indicate that the Connection Broker is allowed to delete this VM from disk. When this option selected, the **Edit Desktop** page for the newly provisioned VM has the **Allow this desktop to be deleted from disk** option selected, by default. Use release plans to schedule VM deletion.

    For more information on using release plans to terminate Azure instances, see the example on deleting virtual machines in the "Release Plans" section of Chapter 11 of the Connection Broker Administrator's Guide.

20. Click **Save**.

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.



Provisioning

□ Provisioning enabled

Provisioning Limits

Start provisioning when unassigned desktops in pool drops below

5

Stop provisioning when total desktops in pool reaches

10

The Connection Broker may automatically disable provisioning in cases where provisioning fails due to configuration errors in your pool. If this occurs, please check and correct your provisioning parameters before enabling provisioning. Typical errors to look for include:

- Your Azure account has reached its quota for the selected instance type
- The instance type is not available in your Azure region

If provisioning fails due to an issue with the Azure API that the Connection Broker is using, the Connection Broker does not disable provisioning. In these cases, the Connection Broker retries the provisioning command, until the Azure APIs become responsive.

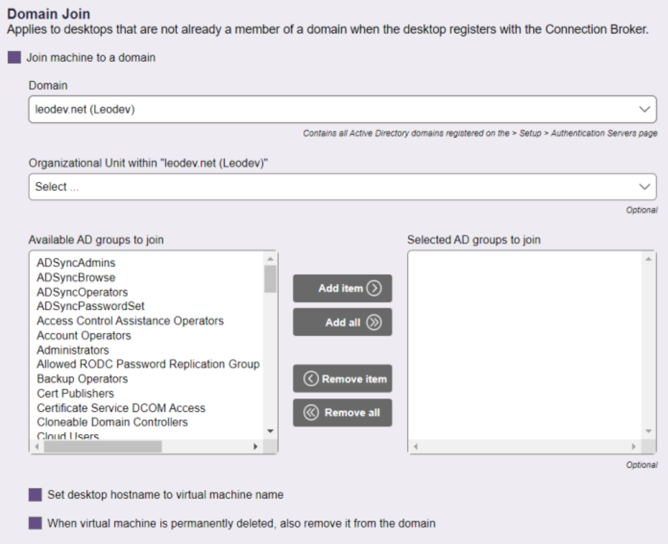
Joining Instances to a Domain

You can use the Connection Broker to join Azure instance to a domain. When enabled, 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 a desktop is provisioned or when you reboot the desktop.

*Before configuring a pool to join desktops to a domain, you must define the Active Directory domain on the **> Setup > Authentication Servers** page. For information on creating an authentication server in your Connection Broker, see "Chapter 13: Authenticating Users" in the* Connection Broker Administrator's Guide.

You enable domain joining for a pool:

1. 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: leodev.net (Leodev)

Contains all Active Directory domains registered on the > Setup > Authentication Servers page

Organizational Unit within "leodev.net (Leodev)": 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
Cloud Users

Selected AD groups to join:

Optional

■ Set desktop hostname to virtual machine name

■ When virtual machine is permanently deleted, also remove it from the domain

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 of more AD groups, move those groups from the **Available AD groups to join** to **Selected AD groups to join** list by selecting the groups and clicking the **Add item** button.

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 found in the **Virtual machine name** edit field.

   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.

6. If you are provisioning non-persistent desktops, select the **When virtual machine is permanently deleted, also remove it from the domain** option to remove the desktop record from AD after the Connection Broker deletes the VM.

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 7: 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

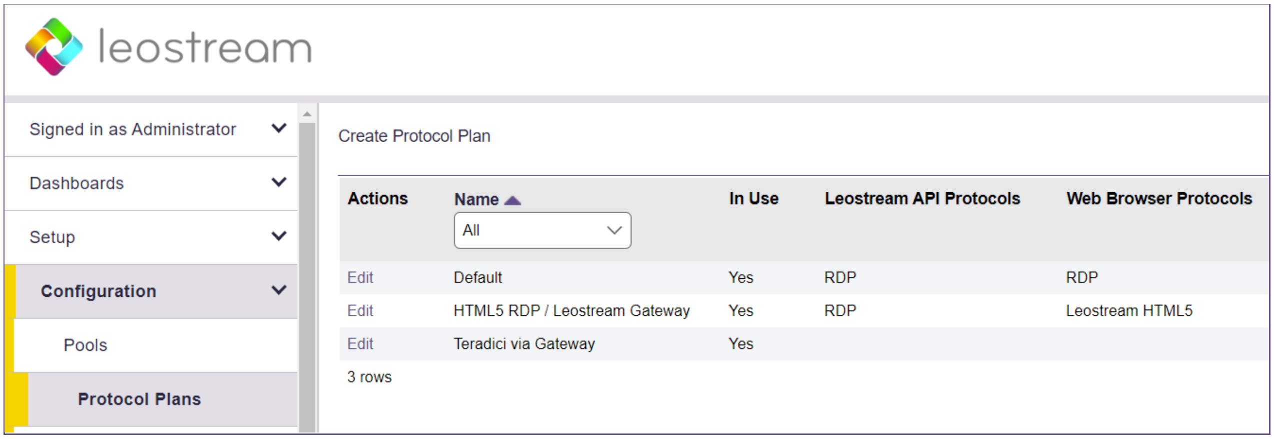
After you separate your desktops into pools, define the rules that control how the Connection Broker manages the user's connection to the desktops in those pools. To perform this step, ask yourself the following questions.

- 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 provides one default protocol plan, which is shown on the **> Configuration > Protocol Plans** page, shown in the following figure.



Actions	Name ▲ All	In Use	Leostream API Protocols	Web Browser Protocols
Edit	Default	Yes	RDP	RDP
Edit	HTML5 RDP / Leostream Gateway	Yes	RDP	Leostream HTML5
Edit	Teradici via Gateway	Yes		

3 rows

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, for RDP, the **Configuration file** is a list of RDP-file parameters that determine if, for example, the connection is launched in full screen.

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.

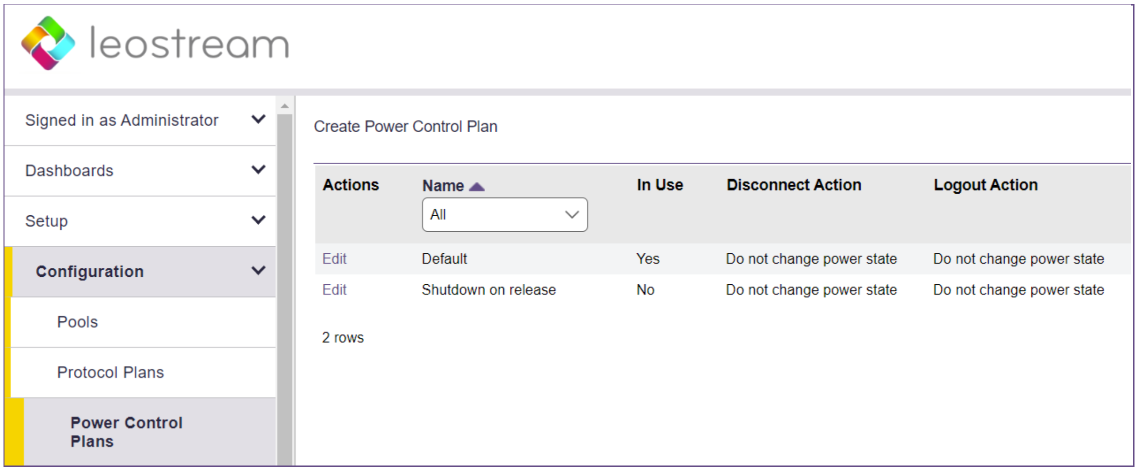
Power Control Plans

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.



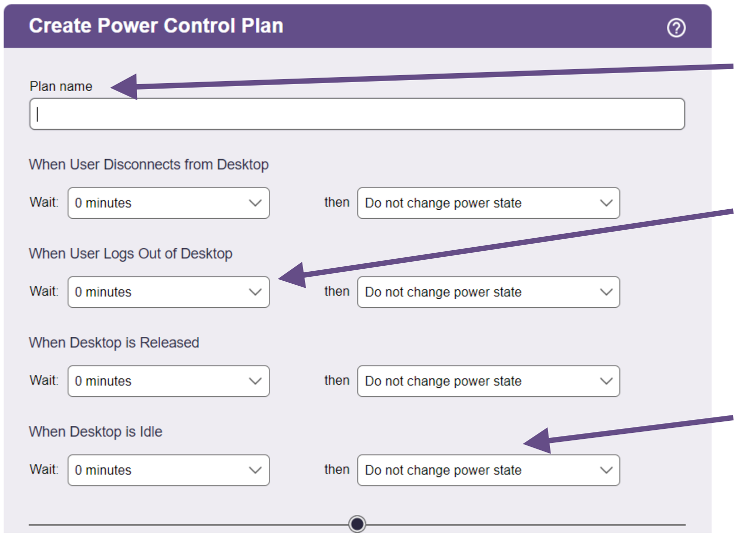
Create Power Control Plan

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

2 rows

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

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



Create Power Control Plan

Plan name

When User Disconnects from Desktop

Wait: 0 minutes then Do not change power state

When User Logs Out of Desktop

Wait: 0 minutes then Do not change power state

When Desktop is Released

Wait: 0 minutes then Do not change power state

When Desktop is Idle

Wait: 0 minutes then Do not change power state

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

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

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

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

3. For each of the remaining sections:

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

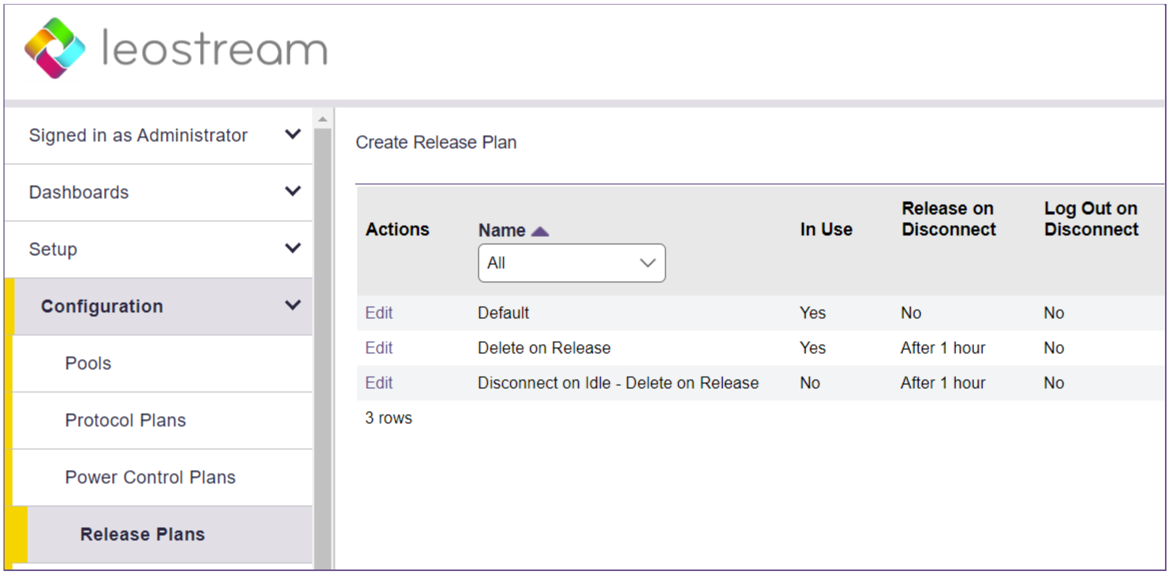
    b. From the **then** drop-down menu, select the power control action to apply. Selecting **Do not change power state** renders the setting in the **Wait** drop-down menu irrelevant, as no action is ever taken.

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

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.*



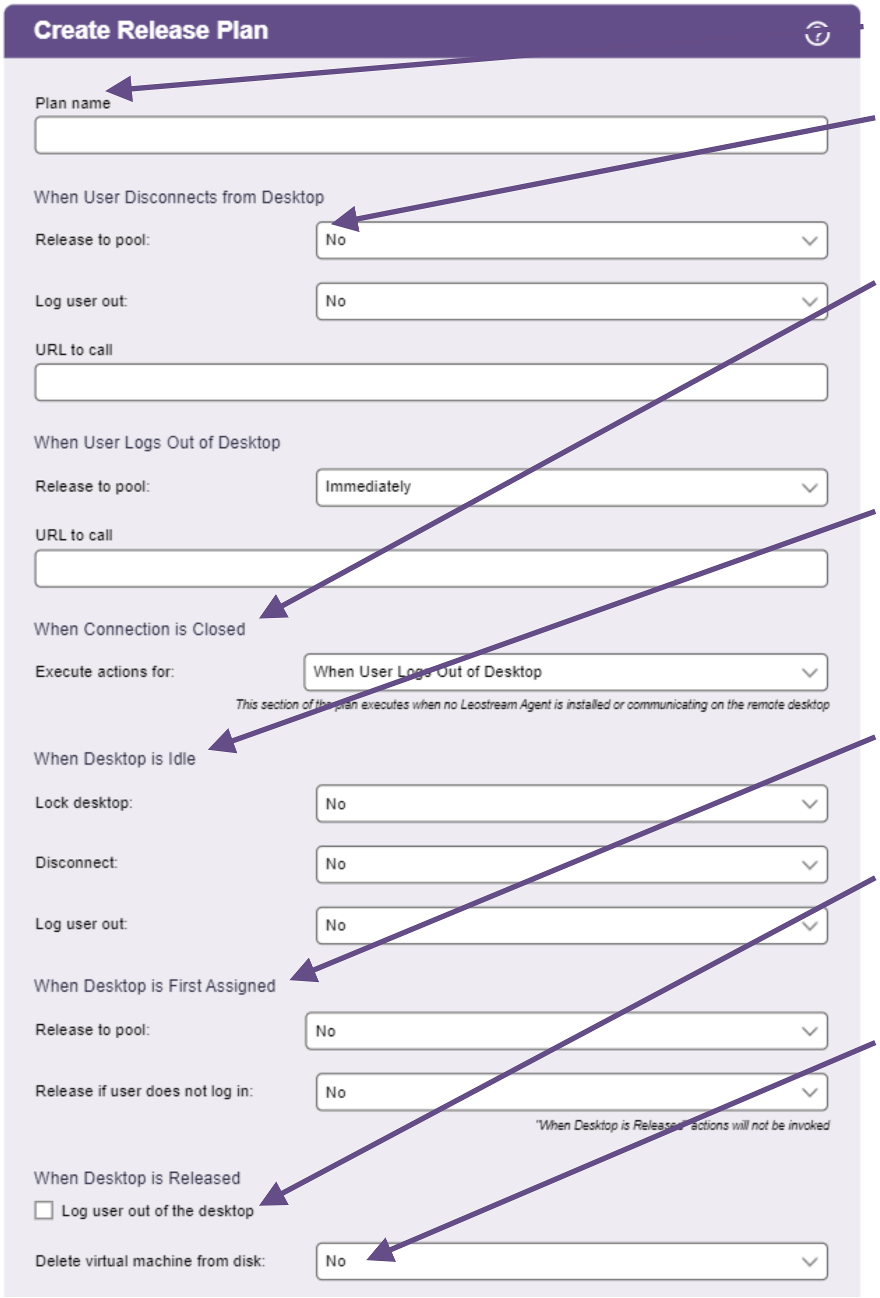
Actions	Name All	In Use	Release on Disconnect	Log Out on Disconnect
Edit	Default	Yes	No	No
Edit	Delete on Release	Yes	After 1 hour	No
Edit	Disconnect on Idle - Delete on Release	No	After 1 hour	No

3 rows

New Connection Broker installations contain one default release plan. 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:

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



Create Release Plan

Plan name

When User Disconnects from Desktop

Release to pool: No

Log user out: No

URL to call

When User Logs Out of Desktop

Release to pool: Immediately

URL to call

When Connection is Closed

Execute actions for: When User Logs Out of Desktop

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

When Desktop is Idle

Lock desktop: No

Disconnect: No

Log user out: No

When Desktop is First Assigned

Release to pool: No

Release if user does not log in: No

"When Desktop is Released" actions will not be invoked

When Desktop is Released

□ Log user out of the desktop

Delete virtual machine from disk: No

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

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

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

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

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

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

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

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

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

4. Click **Save**.

In 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.

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

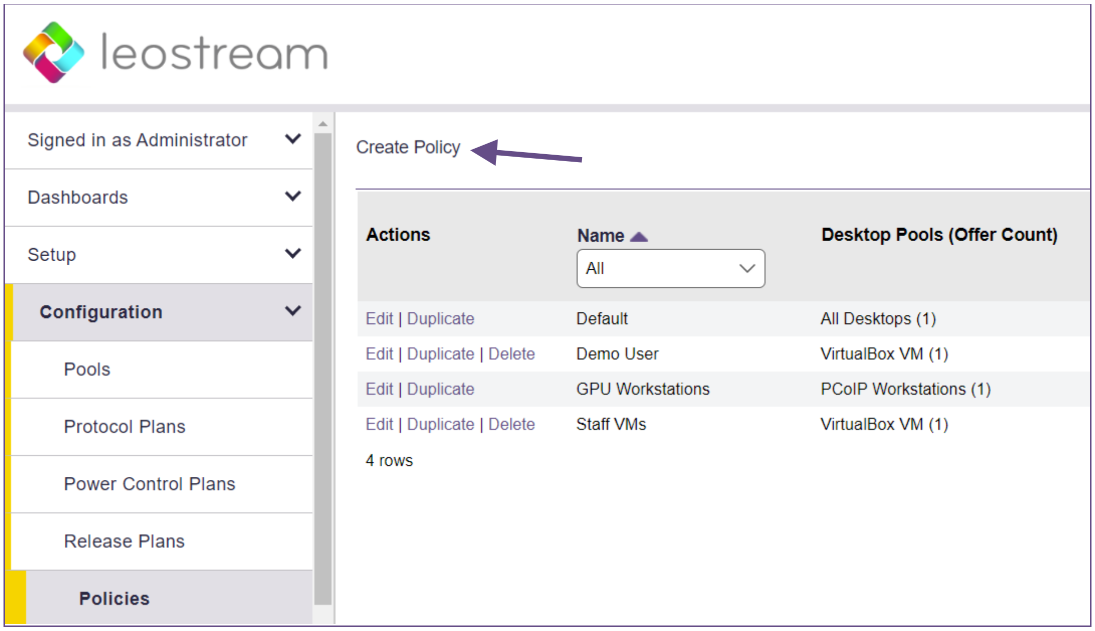
After you define your pools and plans, build policies.

> 💡 *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. You can create additional policies, as follows:

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

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



Actions	Name ▲ (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

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**.

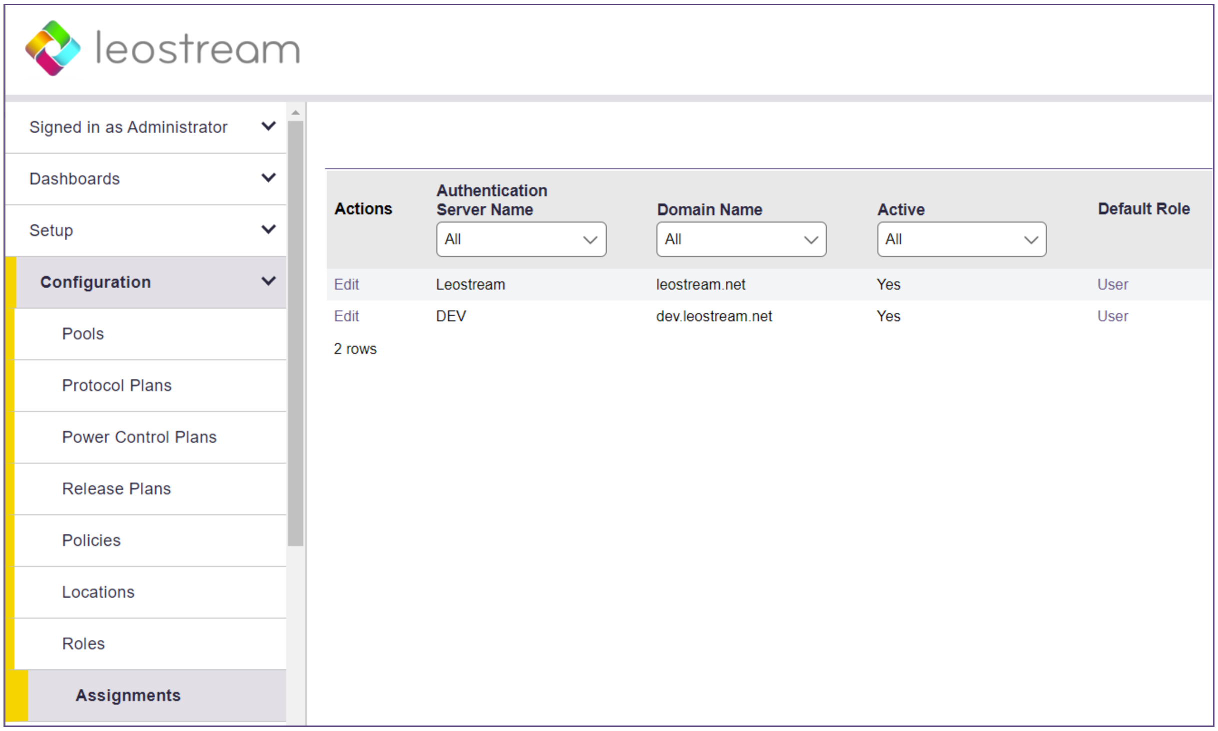
*A policy can offer desktops from multiple pools. Click the **Add Pool Assignment** link to add a new pool, or use the kebab menu to clone an existing Pool Assignment to simplify initializing the options for an additional pool.*

11. 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.

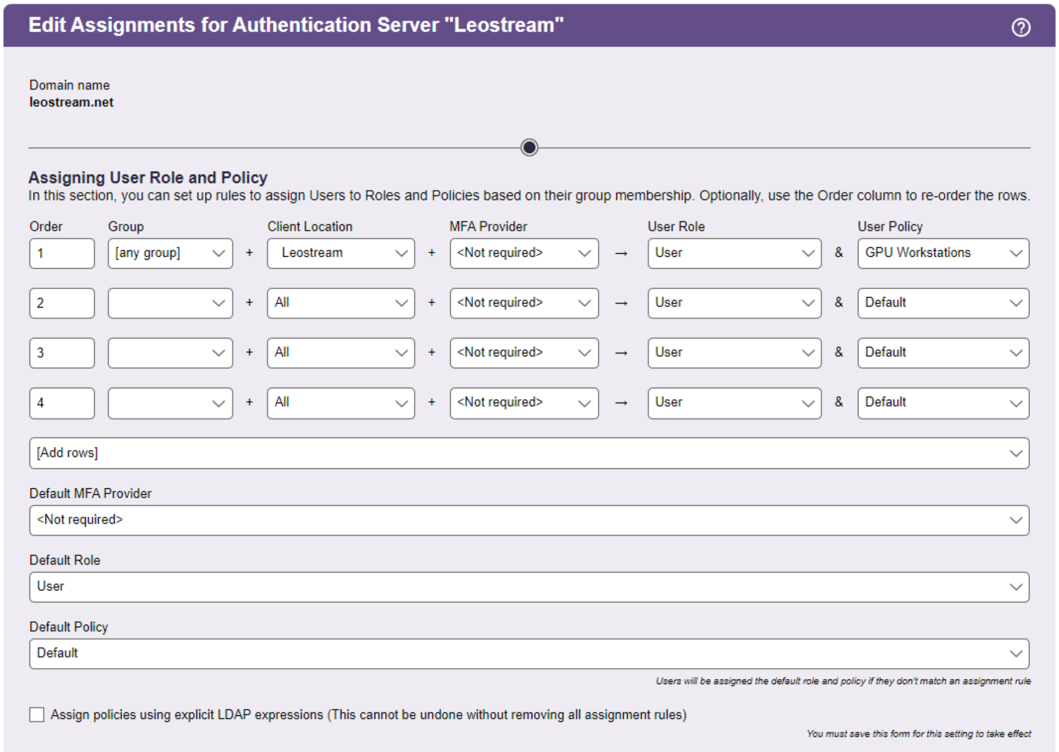
The Connection Broker then looks on the **> Configuration > Assignments** page, shown in the following figure, for the assignment rules associated with the user's authentication server. For example, if the Connection Broker authenticated the user in the `LEOSTREAM` domain defined on the **> Setup > Authentication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



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

2 rows

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



Edit Assignments for Authentication Server "Leostream"

Domain name
leostream.net

Assigning User Role and Policy

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

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

[Add rows]

Default MFA Provider
<Not required>

Default Role
User

Default Policy
Default

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

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

You must save this form for this setting to take effect

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

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

To assign 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 9 and 12 in the Connection Broker Administrator's Guide.*

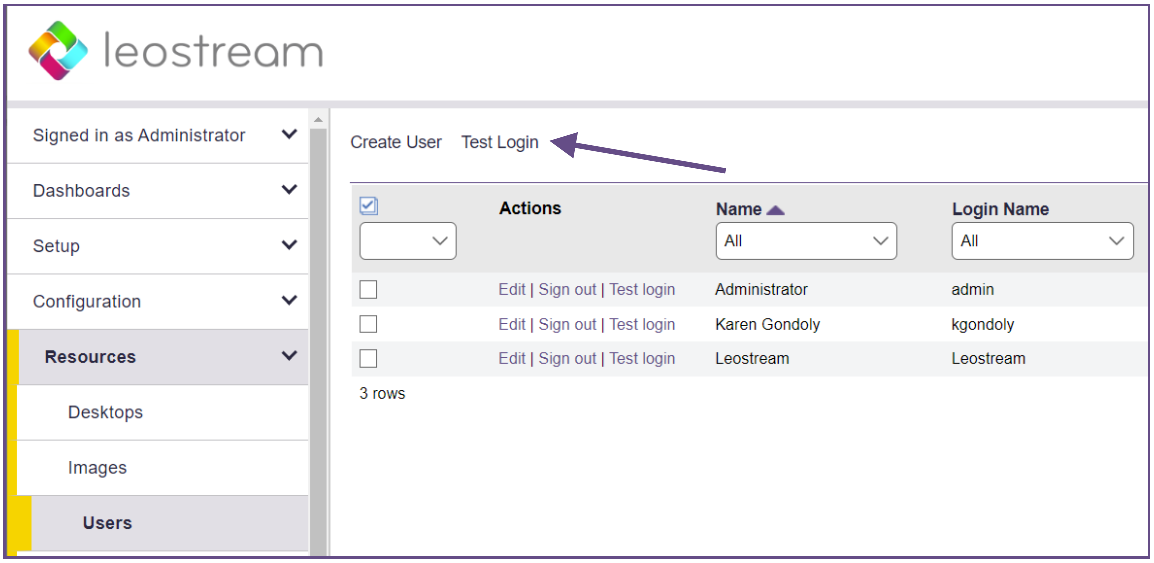
4. Assign a policy to this group and client location pair by selecting an item from the **User Policy** drop-down menu.

If you need to assign roles and policies based on a different user attribute, see "Assigning Roles and Policies Based on any Attribute" in the Connection Broker Administrator's Guide.

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.



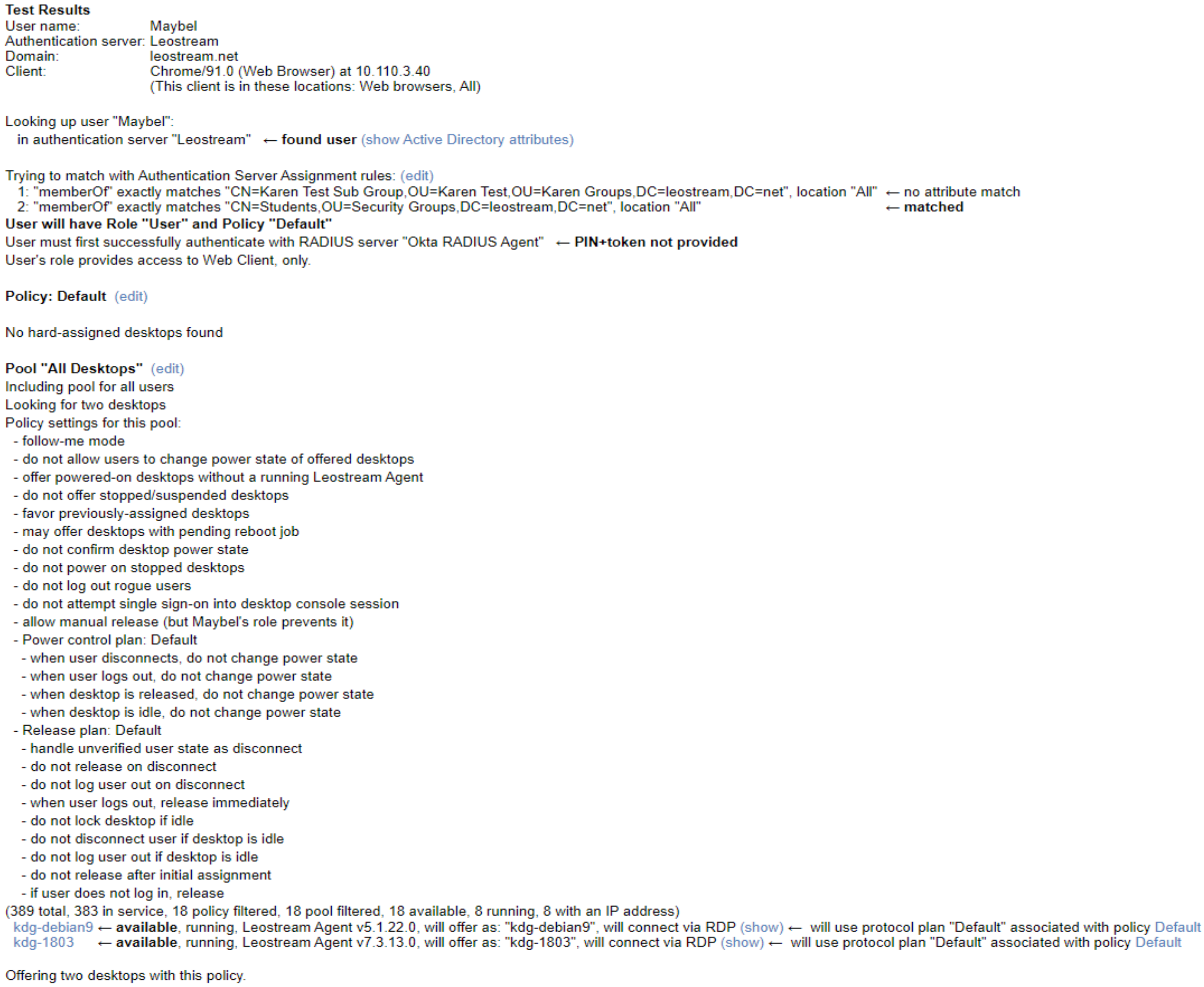
☑	Actions	Name ▲	Login Name
		All	All
□	Edit | Sign out | Test login	Administrator	admin
□	Edit | Sign out | Test login	Karen Gondoly	kgondoly
□	Edit | Sign out | Test login	Leostream	Leostream

3 rows

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

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

5. Click **Run Test**. The Connection Broker searches the authentication server for your user, and then presents a report, as shown in the following figure.



```
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.