



leostream[®]

Remote Desktop Access Platform

Using the Leostream[®] Platform to Manage Amazon WorkSpaces Core

Remote Access and Desktop Connection Management with Leostream

Version 202x
March 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.

For support, contact support@leostream.com. (See the [Leostream Support Policy](#).)

Copyright

© Copyright 2002-2024 by Leostream Corporation

This software program and documentation are copyrighted by Leostream. The software described in this document is provided under a license agreement and may be used or copied only under the terms of this agreement. No part of this manual may be copied or reproduced in any form without prior written consent from Leostream.

Trademarks

The following are trademarks or registered 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.

Amazon Web Services, the “Powered by AWS” logo, Amazon EC2, EC2, Amazon Relational Database, Amazon RDS, Amazon S3, Amazon Route 53, Amazon Virtual Private Cloud, Amazon VPC, AWS Marketplace, and AWS are trademarks of Amazon.com, Inc. or its affiliates in the United States and/or other countries. OpenLDAP is a trademark of The OpenLDAP Foundation. Microsoft, Active Directory and Windows are trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Other brand and product names are trademarks or registered trademarks of their respective holders. Leostream claims no right to use of these marks.

Patents

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

Contents

CONTENTS	3
CHAPTER 1: INTRODUCTION	4
CHAPTER 2: GETTING STARTED	7
OVERVIEW	7
SETTING UP SECURITY GROUPS	8
CONFIGURING THE DIRECTORY SERVICES SECURITY GROUP	8
CONFIGURING THE VPC	9
CHAPTER 3: INSTALLING THE LEOSTREAM PLATFORM IN AWS EC2	11
REQUIRED AWS PERMISSIONS	11
LAUNCHING A CONNECTION BROKER INSTANCE	12
UPGRADING THE LEOSTREAM CONNECTION BROKER	13
LAUNCHING A LEOSTREAM GATEWAY INSTANCE	14
OBTAINING YOUR LEOSTREAM LICENSE	16
CHAPTER 4: PREPARING WORKSPACES CORE IMAGES	18
CHAPTER 5: INTEGRATING WITH YOUR AWS INFRASTRUCTURE	20
CONNECTING TO YOUR AMAZON DIRECTORY SERVICES	20
CONNECTING TO YOUR AMAZON WORKSPACES ACCOUNT	21
ATTACHING THE LEOSTREAM GATEWAY TO A CONNECTION BROKER	22
CHAPTER 6: LAUNCHING NEW AMAZON WORKSPACES	23
LOADING USERS	23
DEPLOYING NEW WORKSPACES	24
CHAPTER 7: CONNECTING USERS TO WORKSPACES	26
AMAZON WORKSPACES POOLS	26
PROTOCOL PLANS	27
POWER CONTROL PLANS	28
RELEASE PLANS	31
BUILDING USER POLICIES	32
ASSIGNING POLICIES TO USERS	34
TESTING YOUR CONNECTION BROKER CONFIGURATION	36
CONNECTING TO WORKSPACES	37

Chapter 1: Introduction

The Leostream Platform leverages AWS WorkSpaces Core to allow organizations to launch and assign WorkSpaces instances to users in hybrid environments managed by the Leostream platform. The Leostream platform provides the tools necessary to satisfy a wide range of use cases and maximize the utility of desktops and applications hosted on WorkSpaces Core instances, and allows organizations to manage WorkSpaces Core instances from the same VDI management portal as an infrastructure built using Amazon EC2 and on-premises virtualization. With the combination of the Leostream platform and Amazon WorkSpaces Core, you can:

1. Lower costs – Save 20% on WorkSpaces fees by leveraging the WorkSpaces Core feature to “Bring your own license” (BYOL) and “Bring your own Protocol” (BYOP)
2. Provide desktops on-demand – provision WorkSpaces Core instances, preconfigured from customized images created in AWS, within the Leostream platform to quickly create and assign desktops to new users
3. Support multi-tenancy – manage WorkSpaces Core instances across AWS Regions from a single pane-of-glass
4. Improve security – keep data off of the end user’s client device, to ensure that sensitive data never leaves the cloud; leverage multifactor authentication for secure access; use the Leostream Gateway to connect users to WorkSpaces Core instances

A virtual desktop infrastructure leveraging the Leostream platform can utilize a range of AWS services, as described below, allowing you to build a complete VDI solution in the cloud. This guide focuses on Amazon WorkSpaces Core and indicates the services required to work through this Quick Start guide. For more information on using the Leostream platform with AWS EC2 or Amazon DCV, see the [Leostream Quick Start for AWS EC2](#) or the [Leostream Guide for Using Display Protocols](#), respectively.

- [Amazon WorkSpaces Core](#) (required) provides a managed virtual desktop infrastructure hosted on AWS. Using the Leostream platform with Amazon WorkSpaces Core, you can easily build and manage hybrid cloud VDI across AWS and on-premises environments. Contact your AWS representative to ensure that WorkSpaces Core is enabled in your AWS account.
- [AWS EC2 \(required\)](#) provides compute for a “build-your-own” virtual desktop infrastructure. The Leostream platform launches, terminates, power controls, and connects users to instances in EC2. You host your Leostream Connection Broker and Leostream Gateway on EC2 instances, and use EC2 to build your custom image to use for provisioning WorkSpaces Core instances.
- [Amazon DCV](#) securely connects users to WorkSpaces Core and EC2 instances from any device over varying network conditions, with the ability to deliver graphics-intense applications and HPC workloads. Amazon DCV is available at no extra charge when used on Amazon Web Services.
- [AWS Relational Database Service \(RDS\)](#) provides the database required to build a cluster of Leostream Connection Brokers for high availability. The Leostream Connection Broker includes a

built-in PostgreSQL database for small environments and proof-of-concepts. In a production environment, or to support a large number of users, create a cluster of Connection Brokers that use a common database hosted in RDS.

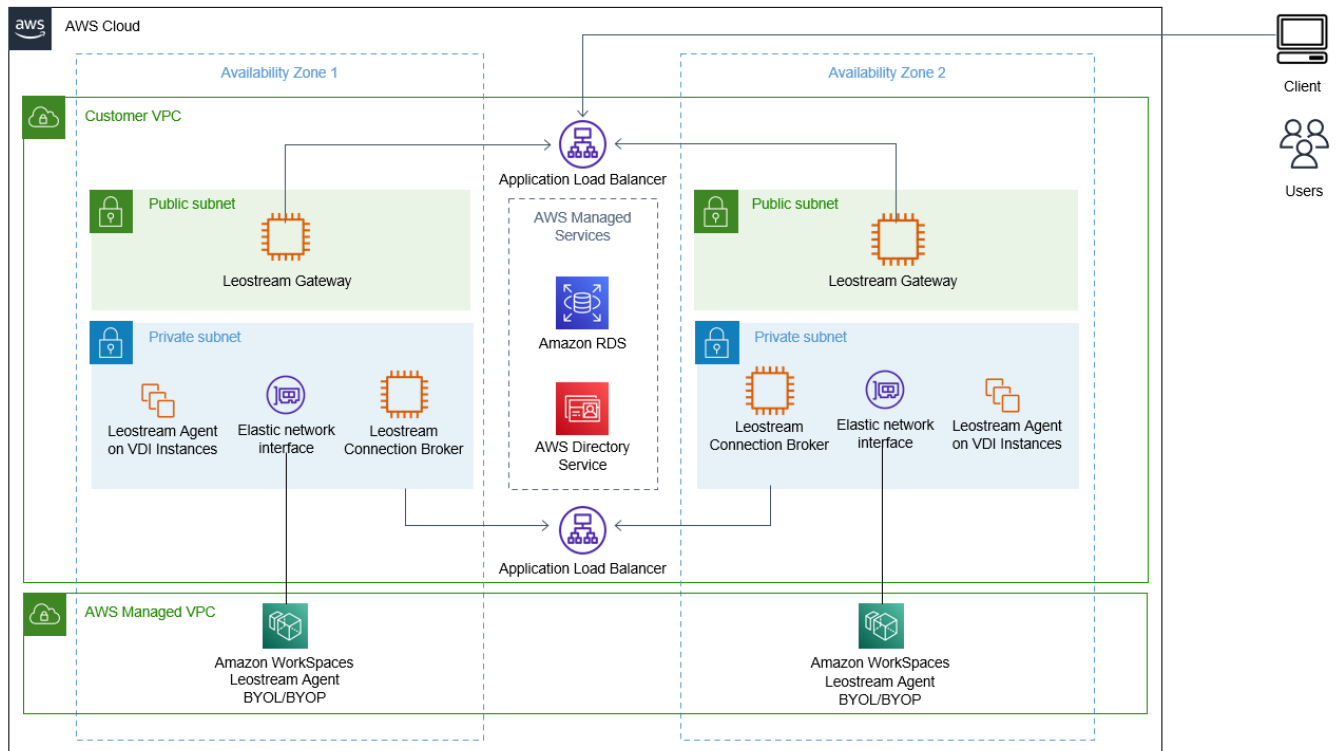


The Connection Broker database stores all of your Leostream configuration information and user login history. The Leostream platform has no access to your sensitive information. All passwords and secret keys which are saved when creating Centers, Authentication Servers, etc. are stored encrypted in your Connection Broker database.

- [AWS Elastic Load Balancing](#) distributes user logins to different Connection Brokers in a cluster, to provide high availability and failover. Connection Brokers can be load balanced like any other application that uses HTTPS traffic.
- [Amazon Virtual Private Cloud](#) (VPC) (required) isolates WorkSpaces Core an EC2 instances in a private network. The Leostream Gateway can then be used in conjunction with the Connection Broker to provide secure access into the private network.
- [Amazon Directory Services](#) (required) manages domain users and computers. The Leostream platform can authenticate users and launch new WorkSpaces Core instances in your Directory Services domain.
- [Amazon Route 53](#) provides DNS load balancing and routes users to your Leostream login page.

This document describes important aspects to consider when configuring your Amazon Web Services account for use with the Leostream platform and describes how to configure the Leostream Connection Broker to manage capacity and user connections to Amazon WorkSpaces Core. The document assumes a basic familiarity with AWS EC2, Amazon WorkSpaces, Amazon Virtual Private Cloud, and Amazon Directory Services concepts and use.

The following figure depicts the basic architecture when using the Leostream platform with Amazon WorkSpaces Core.



For an introduction to the Leostream platform, 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](#).

Chapter 2: Getting Started

Overview

To use the Leostream platform to manage Amazon WorkSpaces Core, you complete the following steps.

1. In the AWS VPC console, create a [VPC for Amazon WorkSpaces and create a Security Group in that VPC](#). The Security Group should allow communication between your Connection Broker and the Leostream Agents that will be installed on your Amazon WorkSpaces instances. It should also allow any other ports required by your selected display protocol, etc. (see [Setting up Security Groups](#)). Note that you will need to connect to your initial WorkSpaces instance using RDP to install the Leostream Agent, so ensure the RDP port is open in your Security Group.
2. In the Amazon WorkSpaces console, create an AWS Directory Service for deploying your WorkSpaces in this VPC. When creating the Directory Service, ensure that you select the Security Group created in step one, to allow communication between your Connection Broker and Leostream Agents installed on your WorkSpaces instances, as well as to support your chosen display protocol.

After the service is created, note the Directory ID for your Directory Service.

The remainder of this Quick Start uses a [Simple AD directory](#).

3. In the Amazon WorkSpaces console, register this [Directory Service](#) with your Amazon WorkSpaces.
4. In the AWS IAM console, [create an IAM](#) user with permission to manage Amazon WorkSpaces (see [Required AWS Permissions](#)).
5. Using the AWS EC2 console, install your Leostream Connection Broker and Leostream Gateway in your VPC (see [Chapter 3: Installing Leostream in AWS EC2](#)).
6. Create a custom bundle to use for provisioning WorkSpaces with the Leostream platform (see [Chapter 4: Preparing WorkSpaces Core Images](#)).
7. In your Leostream Connection Broker Administrator web interface, connect your Connection Broker to your AWS Directory Services and Amazon WorkSpaces account (see [Chapter 5: Integrating with Your AWS Infrastructure](#)).
8. Use your Leostream Connection Broker Administrator web interface to launch new Amazon WorkSpaces Core instances (see [Chapter 6: Launching new Amazon WorkSpaces](#)).
9. Configure your Connection Broker to offer and connect users to WorkSpaces (see [Chapter 7: Connecting Users to WorkSpaces](#)).

Setting up Security Groups

EC2 and WorkSpaces instances block all incoming traffic, by default. To ensure that the Connection Broker and WorkSpaces instances can communicate, you must create one or more security groups that open the required ports for incoming traffic. You can create a single security group to use for all components in your environment or create separate security groups for the Leostream Connection Broker, Leostream Gateway, and WorkSpaces instances.

Port	Type	Security Group Used By	Purpose
22	TCP	Connection Broker, Leostream Gateway	For SSH access to the Connection Broker and Leostream Gateway
80	TCP	Connection Broker	(Optional) For access to the Connection Broker web interface. If you close port 80 on your Connection Broker, you may omit that port from the security group.
443	TCP	Connection Broker, Leostream Gateway	For access to the Connection Broker web interface, and communication with the Leostream Agents and Leostream Connect.
20001-30000		Leostream Gateway	The Leostream Gateway uses this default port range to forward display protocol traffic from the user's client device to an instance isolated in a private OpenStack network. You may optionally change this port range using the Leostream Gateway CLI.
8080*	TCP	WorkSpaces Instances	Port for communications from the Connection Broker to the Leostream Agent. * The Leostream Agent port may be changed using the Leostream Agent Control Panel dialog. If you change the default Leostream Agent port, ensure that you open the associated port in the security group
3389*	TCP	WorkSpaces Instances	For RDP access to the AWS VDI/DaaS instances ** If you use a display protocol other than RDP, ensure that you open any ports required by that display protocol.

Configuring the Directory Services Security Group

In order to ensure that your Connection Broker can communicate with the Leostream Agent installed on newly provisioned WorkSpaces and to ensure that users can connect to these WorkSpaces, ensure that you set an appropriate default Security Group for your WorkSpaces Directory Services.

1. Go to the **Directories** page in the Amazon WorkSpaces console.
2. Click on the name for the WorkSpaces Directory Services you will use with your Leostream platform.

3. In the Directory Details, scroll down to the **Security group** section.
4. If the selected security group does not open the appropriate ports, use the **Edit** button to assign a new security group.

For example, to support Leostream Agent communication and RDP connections through the Leostream Gateway, the security group must open port 8080 and 3389. Port 8080 can be limited to the Connection Broker private IP, while port 3389 can be limited to the Leostream Gateway private IP.

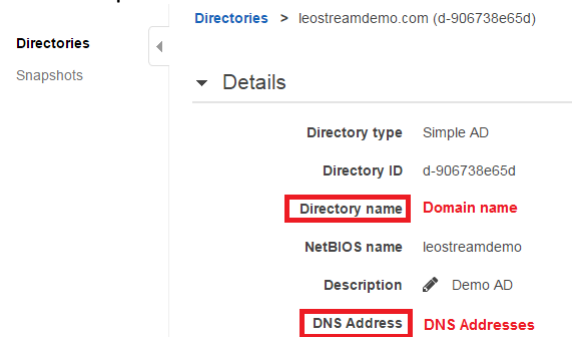
Configuring the VPC

An Amazon Virtual Private Cloud (VPC) isolates WorkSpaces Core instances on a virtual network within the AWS cloud, allowing you to secure and separate instances for different customers, use cases, etc. All VPC configuration must be done within the AWS Management Console. After you configure your VPCs, the Leostream platform can launch and manage WorkSpaces Core instances in those VPCs.

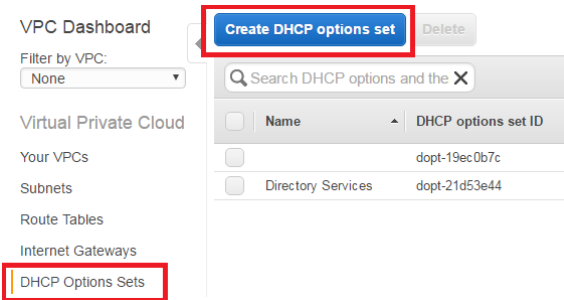


If your VPC uses AWS Directory Services, you must create a DHCP option set that associates the **Domain name** and **Domain name servers** to the domain name and DNS addresses of your Directory Services. Any Leostream Connection Broker launched within the VPC uses the DNS information in the DHCP options set to resolve hostnames within the VPC.

To find the DNS addresses used by your Directory Services, open the Directory Services console in the AWS Management Console and click on the Directory ID for your Directory Services. The **Directory name** and **DNS Address** fields displays the domain name and DNS addresses you should use in your DHCP options set, for example:



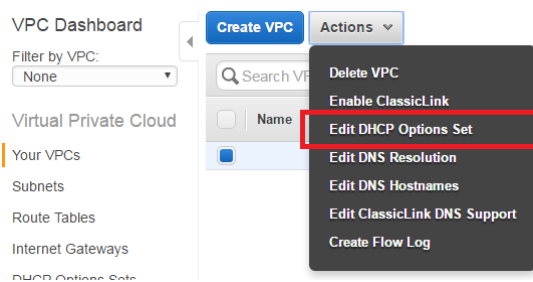
To create a new DHCP option set, go to the **DHCP Options Set** page in the VPC service and click the **Create DHCP options set** button, highlighted in the following figure.



In the **Create DHCP options set** form, ensure that you complete the **Domain name** and **Domain name servers** information.

After creating the DHCP option set, you can associate it with your VPC, as follows.

1. On the **Your VPCs** page, select your VPC.
2. Select **Edit DHCP Options Set** from the **Actions** drop-down menu, for example:



3. In the **Edit DHCP Options Set** dialog, select the DHCP options set associated with your Directory Services.
4. Click **Save**.

Chapter 3: Installing the Leostream Platform in AWS EC2

You can quickly and easily install the Leostream Connection Broker using the Leostream Platform AMIs in the [AWS Marketplace](#).



Leostream currently provides AMIs based on Rocky Linux 8. For environments that require Red Hat Enterprise Linux 8, please see the [Leostream Installation Guide](#) for instructions on installing the Leostream components on AWS instances launched with that operating system.

To run properly, the Connection Broker requires, at least, the following resources.

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

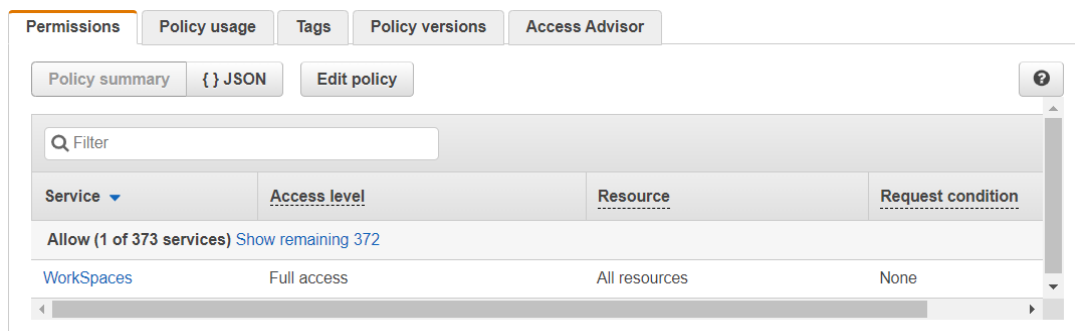


Leostream recommends launching the Connection Broker on a `t2.large` or `t3.large` instance type in order to adhere to the RAM requirement guidelines. The instance type used when launching the Leostream Gateway depends on your environment's requirements.

You can run the Connection Broker and Leostream Gateway on any virtual or physical machine with the required resources. If you are managing a hybrid cloud and need to install the Connection Broker on a platform outside of AWS, please consult the [Leostream Installation Guide](#) for complete instructions. The remainder of this guide covers installing the Connection Broker in your AWS account.

Required AWS Permissions

This Quick Start guide uses an IAM Policy that provides full access to the WorkSpaces service, for example:



After you create your policy, create an IAM user with this policy or assign the user to an IAM Group with this policy. Note down the Access Key ID and Secret Access Key for this user to later provide to your

Connection Broker.



IAM Roles will be supported in a future version of the Connection Broker.

Launching a Connection Broker Instance

When launching a Connection Broker instance from the Leostream Connection Broker AMI in the AWS Marketplace, please adhere to the following guidelines:

1. Configure the instance name and tags according to your environment's requirements.
2. Search for an **Application and OS Images** that contains the name **Leostream**. Click the **Select** button for the Leostream Connection Broker AMI in the AWS Marketplace AMIs, shown in the following figure, then click **Continue** on the Leostream Connection Broker description dialog that opens.

Choose an Amazon Machine Image (AMI)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

leostream

Quickstart AMIs (0)
Commonly used AMIs

My AMIs (21)
Created by me

AWS Marketplace AMIs (2)
AWS & trusted third-party AMIs

Community AMIs (2)
Published by anyone

Refine results

Categories

- Infrastructure
- Software (2)
- Business Applications (2)

▼ Publisher

- ☐ Leostream (2)

▼ Pricing model

- ☐ Bring Your Own License (2)

Operating system

- ☐ All Linux/Unix

leostream (2 results) showing 1 - 2

Sort By: Relevance

Leostream Gateway
By Leostream | Ver 2022.1.0.6
1 external review

The Leostream Gateway is a key component of the Leostream platform - consisting of the Leostream Connection Broker, Leostream Gateway, Leostream Agent, and Leostream Connect. Using Leostream, organizations and service providers can build a hosted desktop or application environment (VDI or DaaS) in...

Leostream Connection Broker
By Leostream | Ver 2022.1.0.9
1 external review

The Leostream platform - consisting of the Leostream Connection Broker, Leostream Gateway, Leostream Agent, and Leostream Connect clients - allows organizations and service providers to build a hosted desktop and application (VDI or DaaS) environment

3. For the **Instance type**, select a t2.large instance, or larger. Consider using a T2 Unlimited instance type to avoid CPU throttling.
4. In the **Key pair name** drop-down menu, select a key pair to use for the instance. You will need this key pair to SSH into the Connection Broker instance.



Ensure that you rotate the SSH key used for your Connection Broker in accordance with your corporate standards for rotating SSH key pairs.



The Linux user for SSH access to the instance console is `leostream`.

5. When configuring the **Network settings**:

- a. To use the Connection Broker with an AWS Directory Services and Amazon WorkSpaces, use the **Network** drop-down menu to place the Connection Broker in the same VPC as the WorkSpaces.



The Connection Broker must be in the same VPC to communicate with the Directory Services and Leostream Agents on the WorkSpaces instances. Also, ensure that the VPC's DHCP option set is configured to use the domain and DNS servers associated with the Directory Services (see [Configuring a VPC.](#))

- b. You must be able to access the Connection Broker Administrator Web interface to configure your Leostream environment, but you do not need to assign a public IP address to your Connection Broker to do so. The Leostream Gateway provides access to Connection Brokers that are isolated in a private network. See “Forwarding Connection Broker Logins through the Gateway” in the [Leostream Gateway Guide](#) for complete instructions.

- a. The Leostream AMI suggests a security group with the following rules.

Description	Inbound	Outbound	Tags
<div>Edit</div>			
Type ⓘ	Protocol ⓘ	Port Range ⓘ	Source ⓘ
HTTPS	TCP	443	0.0.0.0/0
HTTP	TCP	80	0.0.0.0/0
SSH	TCP	22	0.0.0.0/0

These rules provide SSH, HTTP, and HTTPS access to the Connection Broker instance. If you want to restrict the Connection Broker to only HTTPS, remove the inbound rule for port 80. To limit SSH access, you can restrict the source to the IP address range of your clients.

6. In **Configure storage**, allocate at least 20 GB of storage to the Connection Broker.
7. Configure any **Advanced details** as required by your environment then click **Launch instance**.

Upgrading the Leostream Connection Broker

After launching your Connection Broker instance, update the underlying operating system and Connection Broker to the latest version.

To upgrade your Connection Broker, download the latest RPM file from the Leostream Downloads page, found at:

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

Ensure that you have your Leostream Serial Number and the email addresses associated with it, in order to log into the Leostream Downloads page.



Do not uninstall or stop your existing Connection Broker before performing the upgrade.

After downloading the latest RPM from the Leostream Downloads page, copy the file to your Connection Broker instance and run the following commands from the instance's terminal.

```
sudo dnf update
sudo dnf -y install RPM-FILE-NAME
sudo /sbin/reboot
```

Subsequent upgrades may be performed using the upgrade options on the Connection Broker > **System** > **Maintenance** page.

If, at any time, you need to check the status of your Leostream Connection Broker, point a Web browser at the following URL, which will reply with `CB_IS_OKAY` if your Connection Broker is functioning nominally.

```
https://CB_ADDRESS/index.pl?action=is_alive
```

Launching a Leostream Gateway Instance

When launching a Leostream Gateway instance using the Leostream Gateway AMI in the AWS Marketplace, please adhere to the following guidelines:

1. Configure the instance name and tags according to your environment's requirements.
2. Search for an **Application and OS Images** that contains the name **Leostream**. Click the **Select** button for the Leostream Gateway AMI in the AWS Marketplace AMIs, shown in the following figure, then click **Continue** on the Leostream Gateway description dialog that opens.

Choose an Amazon Machine Image (AMI)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

Search: leostream

Quickstart AMIs (0) Commonly used AMIs | My AMIs (21) Created by me | **AWS Marketplace AMIs (2)** AWS & trusted third-party AMIs | Community AMIs (2) Published by anyone

Refine results

Categories: Infrastructure, Software (2), Business Applications (2)

Publisher: ☐ Leostream (2)

Pricing model: ☐ Bring Your Own License (2)

Operating system: ☐ All Linux/Unix

leostream (2 results) showing 1 - 2

Sort By: Relevance

Leostream Gateway
By Leostream | Ver 2022.1.0.6
1 external review
The Leostream Gateway is a key component of the Leostream platform - consisting of the Leostream Connection Broker, Leostream Gateway, Leostream Agent, and Leostream Connect. Using Leostream, organizations and service providers can build a hosted desktop or application environment (VDI or DaaS) in...

Leostream Connection Broker
By Leostream | Ver 2022.1.0.9
1 external review
The Leostream platform - consisting of the Leostream Connection Broker, Leostream Gateway, Leostream Agent, and Leostream Connect clients - allows organizations and service providers to build a hosted desktop and application (VDI or DaaS) environment

- For the **Instance type**, ensure you choose the appropriate instance type based on the size of your environment. Leostream recommends at least 4GB of RAM and 2 or more CPUs.

The number of user connections that can be handled by the Leostream Gateway is determined by two key factors, the number of available ports for forwarding display protocol traffic and the amount of CPU. Ensure that you choose an instance type with adequate CPU, particularly if you are connecting users to their desktops with a high-performance protocol such as Mechdyne TGX.

- In the **Key pair name** drop-down menu, select a key pair to use for the instance. You will need this key pair to SSH into the Leostream Gateway instance.



Ensure that you rotate the SSH key used for your Leostream Gateway in accordance with your corporate standards for rotating SSH key pairs.



The Linux user for SSH access to the instance console is `leostream`.

- When configuring the **Network settings**:
 - The Leostream Gateway must have network access to your AWS instances and must be reachable by the end user's client. Typically, that means locating the Leostream Gateway in the public network of the VPC that contains your instances and assigning an Elastic IP address to the gateway instance.
 - The Leostream Gateway AMI suggests a security group with the following rules.

Security group recommendations

Visible to buyers as a recommendation for optimal product configuration

Protocol	Range start port	Range end port	Comma separated list of CIDR IPs
tcp	443	443	0.0.0.0/0
tcp	22	22	0.0.0.0/0
tcp	20001	23000	0.0.0.0/0
udp	20001	23000	0.0.0.0/0

These rules provide SSH and HTTPS access to the Leostream Gateway instance, and open the default random port range required to forward client-based display protocol traffic. Add or modify the security group rules related to display protocol traffic based on the types of display protocols you plan to use and the forwarding rules you configure in your Leostream Connection Broker.

6. In **Configure storage**, allocate at least 20 GB of storage to the Leostream Gateway.
7. Configure any **Advanced details** as required by your environment then click **Launch instance**.

After launching your Leostream Gateway instance, update the underlying operating system and Leostream Gateway by running the following commands from the instance's terminal.

```
sudo dnf update
sudo dnf update leostream_gateway
```

If you need to use the Leostream Gateway to access your Connection Broker login page, SSH into the Leostream Gateway instance as a user with `sudo` privileges and execute the following command:

```
sudo leostream-gateway --broker <your-broker-private-IPaddress>
```

If, at any time, you need to check the status of your Leostream Gateway, point a Web browser at the following URL.

```
https://<your-gateway-address>/app/system/ping
```

Obtaining Your Leostream License

After installing your Connection Broker, you must obtain your Leostream license key. Your Connection Broker license 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 from the Connection Broker Administrator web interface if your Connection Broker has internet access, as follows.

1. Enter <https://<broker-or-gateway-address>> in your Web browser's URL edit field, depending on if

you can access your Connection Broker or if you are using the Leostream Gateway to forward traffic. 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. Select **Enter manually** from the **How do you want to enter your license key** drop-down menu.

5. 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. 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 4: Preparing WorkSpaces Core Images

Amazon WorkSpaces Core images require you to bring your own Windows license (BYOL) and bring your own display protocol (BYOP). Currently, you can run Windows 10 or Windows 11 desktop images if they meet Microsoft's licensing requirements.

Use the follow procedure to create a WorkSpaces Core bundle for use with Leostream.

1. Complete steps 1 through 5 of the BYOL process in the [AWS documentation](#). Take special note of the [requirements](#), for example, note that no additional software can be installed on the Windows VM before you create the image. You install your Leostream Agent and any additional software on the Windows operating system after importing the image into WorkSpaces.



Windows 10 images must be configured with BIOS set as the boot mode. Windows 11 images may use the default UEFI. When importing the Windows image, ensure that you specify the proper boot-mode:

- For Windows 10 images, use `boot-mode legacy-bios`
- For Windows 11 images, use `boot-mode uefi`

2. Use the [CLI to import the WorkSpaces](#) image.

You must use `BYOL_REGULAR_BYOP` or `BYOL_GRAPHICS_G4DN_BYOP` for the `IngestionProcess` to support WorkSpaces Core. For example:

```
aws workspaces import-workspace-image --ec2-image-id ami-ID --ingestion-process  
BYOL_REGULAR_BYOP --image-name my-image --image-description base-image-  
description
```

Where *ami-ID* is the EC2 AMI ID associated with the image you imported in step 5 of the BYOL process, *my-image* is an image name that is displayed on the **Images** page in the Amazon WorkSpaces console and *base-image-description* is the description shown when you view the summary for an image.



Leostream cannot distinguish between WorkSpaces and WorkSpaces Core images and bundles. Therefore, Leostream suggests using a naming convention for your images and bundles that makes it easy for you to distinguish the image types based on their names.

3. After importing your base image, create a base bundle using the **Create bundle** action on the **Images** page in the WorkSpaces console.
4. Use the WorkSpaces console to create a base WorkSpaces instance from your base bundle and assign it to one of the users in the Directory Services associated with your WorkSpaces environment.
5. Use an RDP client [Amazon WorkSpaces client](#) to connect to your WorkSpaces instance.

6. After you are logged into the base WorkSpaces operating system, [install the Leostream Agent](#). Follow through the installation wizard. When prompted, uncheck the **Obtain Connection Broker address automatically using DNS** option and set the **Connection Broker address** to the private IP address of your Connection Broker instance. You do not need to install additional tasks or change any other installation parameters.

After the Leostream Agent is installed, use the **Test** button on the Leostream Agent Control Panel dialog to ensure that the Leostream Agent can contact the Connection Broker. Do not proceed if the test does not succeed.

7. Install any additional software, including display protocol software, that is required. If you plan to use RDP or the Leostream Gateway HTML5 viewer to connect users to their WorkSpaces, you do not need to install additional display protocol software.

When finished, log out of the Windows operating system and close the connection to your base WorkSpaces instance. Do not stop the WorkSpaces instance.

8. With your base WorkSpaces instance in the **Available** state, create a custom image from your base WorkSpaces instance by clicking its name on the **WorkSpaces** page in the WorkSpaces console and clicking the **Create image** button on the WorkSpaces Summary page.
9. After the image is created, go to the **Images** page in the WorkSpaces console, select your custom image, and use the **Create bundle** action to create a custom bundle from that image. This is the customer bundle that you will use in Leostream to provision and assign additional WorkSpaces.

Chapter 5: Integrating with Your AWS Infrastructure

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 Amazon Directory Services and your Amazon WorkSpaces account.

Connecting to Your Amazon Directory Services

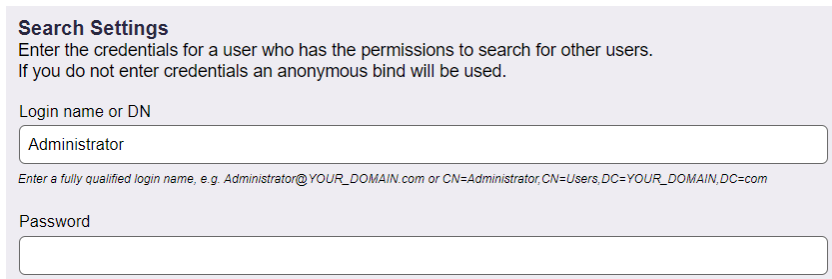
To authenticate users with Amazon Directory Services, or other Microsoft Active Directory server, you must first register that domain with your Connection Broker, as follows.

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.

The screenshot shows the 'Connection Settings' section of a web form. It includes a dropdown menu for 'Specify address using' with 'Hostnames or IP addresses' selected. Below this are two input fields: 'Hostname or IP address' and 'Port', with '389' entered in the port field. A note states: 'If using multiple addresses, separate each entry with spaces'. There is another dropdown for 'Algorithm for selecting from multiple addresses' with 'Random' selected, and a note: 'The sequential algorithm uses the first working address in the list'. A checkbox for 'Encrypt connection to the authentication server using SSL (LDAPS)' is unchecked. At the bottom is an 'AWS Directory ID' input field with a note: 'Enter the Directory ID if this is an AWS directory that will be used for a Amazon Workspaces'.

- a. Select **Active Directory** from the **Type** drop-down list.
- b. From the **Specify address using** drop-down menu, select **Hostname or IP address**.
- c. Enter the authentication server hostname or IP address 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.
 - f. Enter the Directory ID into the **AWS Directory ID** edit field.
6. In the **Search Settings** section, shown in the following figure, enter the username and password for an account that has read access to the user records. Leostream does not need full administrator rights to your Active Directory authentication server.



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

Login name or DN

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

Password

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

Connecting to Your Amazon WorkSpaces Account

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



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

1. Go to the **> Setup > Centers** page.
2. Click the **Add Center** link.
3. In the **Add Center** form, select **Amazon WorkSpaces** from the **Type** drop-down menu.
4. Enter a name for the center in the **Name** edit field.
5. Select the AWS Directory Services associated with this WorkSpaces account from the **Authentication Server** drop-down menu. Create separate centers for each region and Directory Services that you want to manage in Leostream.
6. If your Connection Broker is installed on an AWS EC2 instance, you can use the **Authentication**

drop-down menu to indicate how the Connection Broker authenticates against the AWS API. Currently, to manage Amazon WorkSpaces, you must select **Enter IAM Access Key** and enter the following information.

- a. Enter your AWS access key into the **Access Key ID** edit field. You can create an IAM user to use with Leostream. Ensure that user has sufficient privileges to access EC2.
 - b. Enter the secret key associated with your access key into the **Secret Access Key** field.
7. Click **Save** to create the center.

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

Attaching the Leostream Gateway to a Connection Broker

To associated the Leostream Gateway you installed in your VPC with your Connection Broker:

1. Go to the **> Setup > Gateways** page.
2. Click the **Add Gateway** link.
3. In the **Add Gateway** form, enter a name for the Gateway in the **Name** edit field.
4. Enter your Leostream Gateway instance's public IP address in the **Public IP address or FQDN for use in Protocol Plans**.
5. In the **IP address or FQDN used for Connection Broker communications to this Gateway** field, enter the private address of your Leostream Gateway. This address is optional. If provided, the Connection Broker communicates with the Leostream Gateway using the private address. This address is never used for forwarding display protocol traffic.
6. Click **Save**.

After saving the form, the Connection Broker registers with the Leostream Gateway.

Chapter 6: Launching new Amazon WorkSpaces

Loading Users

Because WorkSpaces are assigned to individual users, you must load users from your Directory Services prior to launching new WorkSpaces in Leostream. To load users:

1. Go to the > **Setup > Authentication Servers** page.
2. Click the **Load users** action for your Directory Services.
3. In the **Load Users from** form that opens, shown in the following figure, select one of the radio buttons to define the scope to choose from when selecting users to load.

Load Users from Demo ⓘ

☐ Select a specific user

Enter the name of the user to select

☐ Select from recently created users

hour(s)

Users created within the specified number of hours will be selected

☐ Select from users that match an expression

Enter an LDAP expression

☐ Select users from a group

☐ Select from all the users

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

Next > **Cancel**

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

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

for user records that were created anywhere in the range from the present time back to the indicated number of hours ago.

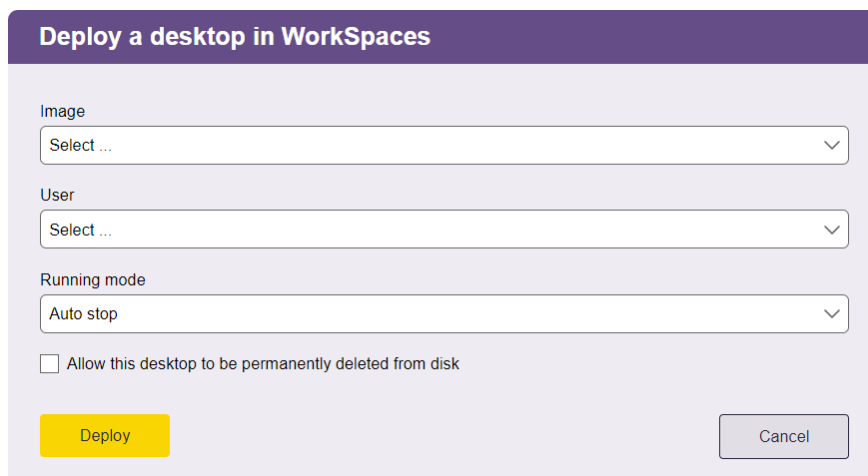
- **Select from users that match an expression:** Enter an LDAP expression. The Connection Broker looks for user records that satisfy the LDAP expression.
 - **Select users from a group:** If the authentication server has the **Query for group information** option selected, select the group to load users from. The Connection Broker displays only users in this group.
 - **Select from all the users:** Select this option to select from all users in the authentication server.
4. Click **Next >**.
 5. In the dialog that opens select the users to import from the **Available users** list at the left.
 6. Click the **Add item** link to add the users to the **Selected users** list.
 7. Click **Save**.

Users are listed on the **> Resources > Users** page.

Deploying New WorkSpaces

To provision a new WorkSpaces instance from your custom bundle:

1. Go to the **> Setup > Centers** page
2. Click the **Deploy** option for your Amazon WorkSpaces center



The screenshot shows a dialog box titled "Deploy a desktop in WorkSpaces". It contains three dropdown menus: "Image" with "Select ..." text, "User" with "Select ..." text, and "Running mode" with "Auto stop" text. Below these is a checkbox labeled "Allow this desktop to be permanently deleted from disk". At the bottom are two buttons: a yellow "Deploy" button and a grey "Cancel" button.

3. From the **Images** drop-down menu, select the bundle to use for the new WorkSpaces instance.



Ensure that you select a WorkSpaces Core bundle. These bundles are labeled with a BYOP Client protocol in the Amazon WorkSpaces console. Leostream cannot currently distinguish WorkSpaces from WorkSpaces Core bundles.

4. From the **User** drop-down menu, select the user to assign to the new WorkSpaces instance.



Amazon WorkSpaces limits users to a single WorkSpaces instance per Directory Services.

5. Select the **Running mode** to use for the WorkSpaces instance.

- Auto stop: Not supported for WorkSpaces Core bundles
- Always on: The WorkSpaces Core Instance is billed monthly
- Manual: The WorkSpaces Core Instance is billed hourly

The Connection Broker controls the power state of your new WorkSpaces Instances based on the settings in your Leostream Policies. Depending on the usage patterns of your users, you may want to configure those policies to leave the WorkSpaces running instead of automatically powering them down. To determine which option works best for you, consult the [WorkSpaces Core Pricing](#) page.

6. Check the **Allow this desktop to be permanently deleted from disk** option if you want to use Leostream to delete Workspaces instances. You can delete instances manually on the **> Resources > Desktops** page or automatically by configuring Release Plans to delete the WorkSpaces instance when it is released from the user.

7. Click **Deploy**.

When the WorkSpaces instance is launched, the selected user is associated with the WorkSpaces instance and appears in the **Assigned Users** column on the **> Resources > Desktops** page. This assignment is initialized as a policy-assignment instead of a hard-assignment, so you can leverage Leostream Release Plan options to terminate the WorkSpaces, if required.

The example Leostream configuration in Chapter 7 indicates how to configure Leostream pools and policies to ensure users are offered and successfully connected to their WorkSpaces, and to manage the WorkSpaces power state.



If the WorkSpaces instances takes a long time to deploy, the `wait_for_start` job associated with that new instance may complete prior to the WorkSpaces instance reaching an **Available** state. If that occurs, the Connection Broker releases the user assignment and marks the Workspace as Stopped on the **> Resources > Desktops** page. If this occurs, monitor the Amazon WorkSpaces console for the Workspace to reach an **Available** state and then return to the **> Setup > Centers** page in the Connection Broker and click the **Scan** option for the Amazon WorkSpaces center.

Chapter 7: Connecting Users to WorkSpaces

Amazon WorkSpaces Pools

Because Amazon WorkSpaces are considered policy-assigned in Leostream, to start, create a pool of the WorkSpaces that you want to manage in Leostream. You can pool by center, as shown in this example, if all WorkSpaces in your Directory Services are managed by Leostream, or you can create sub-pools to manage a subset of WorkSpaces.

To create a pool of desktops from a center, in the **Create Pool** form:

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. If your policies are configured to display a user-friendly pool name to end-users, enter that name in the **Display name** field. Otherwise, leave the **Display name** field empty.
5. Select **Centers** from the **Define pool using** drop-down menu. The form updates to display the Center selection fields, shown in the following figure.

Create Pool ?

Name

Display name

Pool Definition

Subset of pool

Define pool using

Available centers

Selected centers

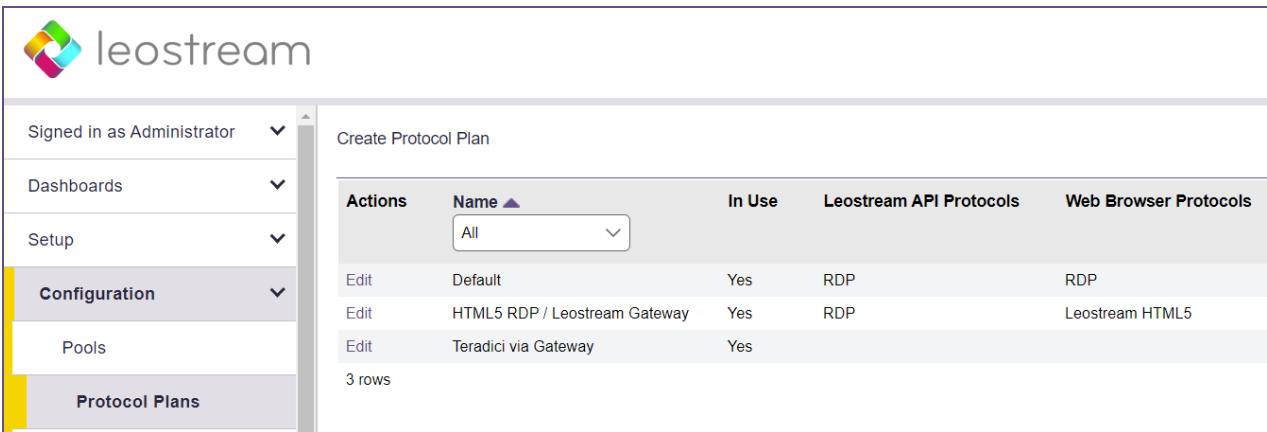
Distribute new desktop assignments

☐ Associate initial user login with assigned user
Executes assigned user's Power Control and Release Plans for the first user who logs into desktops in this pool

6. Select your Amazon WorkSpaces center from the **Available centers** list.
7. Move the center to the **Selected centers** list by clicking the **Add item** button.
8. Click **Save**.

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	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

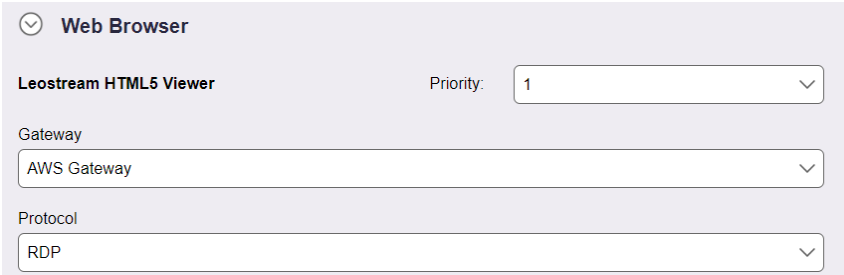
The default Protocol Plan instructs the Connection Broker to connect to the remote desktops using Microsoft RDP.

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.

For this example, edit the **Default** protocol plan use the Leostream Gateway HTML5 RDP viewer for desktop connections, for example.



Web Browser

Leostream HTML5 Viewer

Priority: 1

Gateway

AWS Gateway

Protocol

RDP


For a complete description of protocol plans, see “Building Pool-Based Plans” in the [Connection Broker Administrator’s Guide](#).

 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.

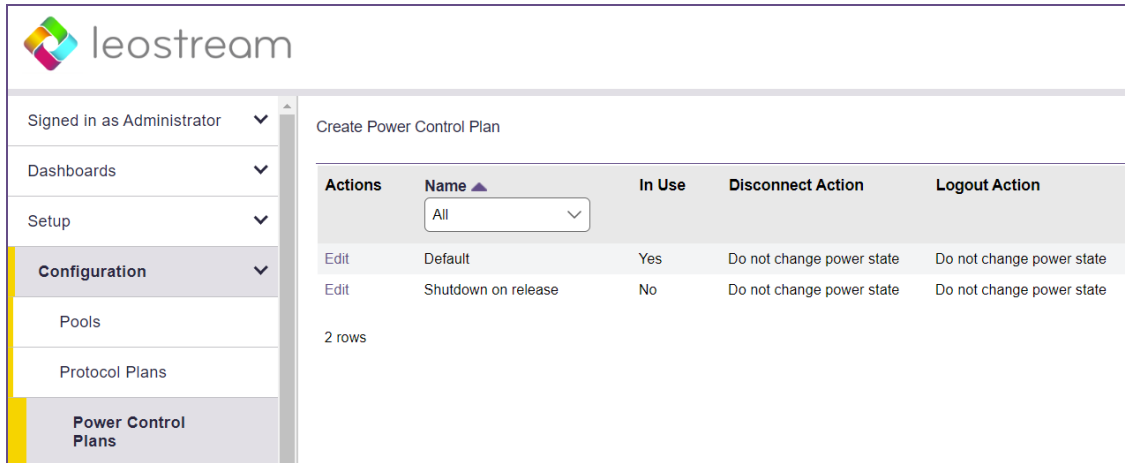
Power Control Plans

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.

Create Power Control Plan

Plan name:

When User Disconnects from Desktop
Wait: then:

When User Logs Out of Desktop
Wait: then:

When Desktop is Released
Wait: then:

When Desktop is Idle
Wait: then:

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.

When deploying WorkSpaces Core instances with a **Manual** running mode, ensure that you configure the Power Control plan to shut down the WorkSpaces instance after the user logs off by selecting **Shutdown** from the **then** drop-down menu in the **When User Logs Out of Desktop** section of the Power Control Plan, as shown in the following figure.

Create Power Control Plan ⓘ

Plan name
Shutdown on logout

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

When User Logs Out of Desktop
Wait: 0 minutes ▾ then **Shutdown** ▾

☐ and Shelve (OpenStack only)

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 ▾

Notes

Save Cancel

Note that if you attempt to shut down or power off an **Always On** WorkSpaces instance, AWS automatically powers the instance back on. The WorkSpaces instance will appear as Stopped in Leostream after the Leostream Agent shuts down, then return to Running after the WorkSpaces instances completes its reboot.

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.

Actions	Name	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

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.

WorkSpaces instance provisioned by Leostream are initially considered policy-assigned to their associated user. To retain the association, create a Release Plan that persists the assignment, as described in the following procedure.

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, for example, "Persistent WorkSpaces Assignment".
3. To model a persistent assignment, ensure that the WorkSpaces instance is never released to its pool. In the **When User Logs Out from Desktop** section, select **No** from the **Release to pool** drop-

down menu, as shown in the following figure.

Edit Release Plan ⓘ

Plan name
Persistent WorkSpaces Assignment

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: No

URL to call

4. Click **Save**.

For more details on creating and using release plans, see the “Release Plans” section in Chapter 10 of the [Connection Broker Administrator’s Guide](#).

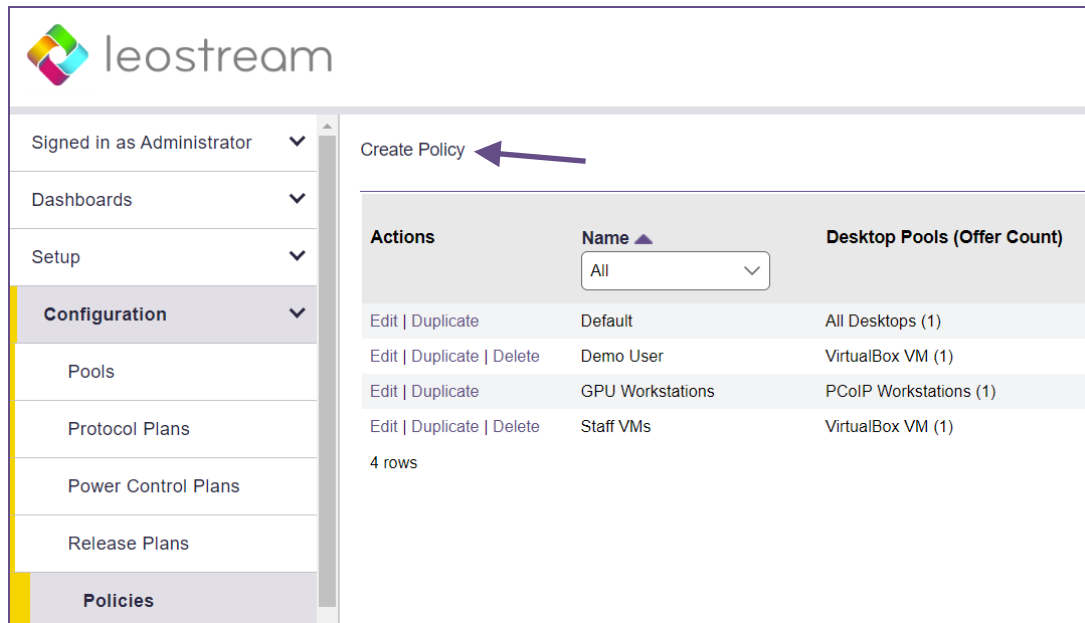
Building User Policies

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 a new policy that offers WorkSpaces instances to users:

1. Go to the **> Configuration > Policies** page.
2. Click the **Create Policy** link, shown in the following figure.



The **Create Policy** form, shown in the following figure, opens.

The screenshot shows the 'Create Policy' form in the Leostream platform. The form has tabs for General, Pool Assignments, Hard Assignments, Rogue User Assignments, and Advanced Settings. The General tab is active, showing fields for Policy name, checkboxes for various settings, a dropdown for protocol parameters, and a dropdown for maximum number of desktops.

Create Policy

General | Pool Assignments | Hard Assignments | Rogue User Assignments | Advanced Settings

Policy name

☐ Auto-launch remote viewer session if only one desktop is offered (Web client only)

☐ Launch HTML5 Viewer and External Viewer connections in new window (Web client only)

☐ Hide hover menu when any remote desktop is locked (Leostream Connect only)

☒ Allow multiple selections in Leostream Connect dialogs

☐ Inform user when a pool is out of resources

☐ Prompt user for alternate credentials before connecting to selected desktop (PCoIP only)

Store user-configured protocol parameters

Individually for each connection/client pair

Maximum number of desktops that can be assigned across all pools

<No Limit>

Expire user's resource offers and Connection Broker session after specified elapsed time

2 days

☐ Expire user's session as soon as a remote desktop is locked

☐ Send HTTP GET request at start of session

Notes

Save Cancel

3. In the **General** tab, 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 continue building the policy.
5. Go to the **Pool Assignments** tab.

Click the **Add Pool Assignments** link. In the **Edit Pool Assignment** form:

- a. In the **When User Logs into Connection Broker** section, select **1** from the **Number of desktops to offer** drop-down menu.
- b. Select your Amazon WorkSpaces pool from the **Pool** menu to select the pool to offer desktops from.
- c. From the **Display desktop to user as** drop-down menu, select **Desktop display name**.
- d. If you are using WorkSpaces Core instances with a **Manual** running mode, from the **Offer stopped and suspended desktops** drop-down menu, select **Yes, only if Leostream gent is installed**.
- e. Scroll down to the **Plans** section and select the protocol, power control, and release plans edited or created in this example, to apply them to the WorkSpaces instances offered from this pool.

Protocol Plan: Default

Power Control Plan: Shutdown on logout

Release Plan: Persistent WorkSpaces Assignment



In a proof-of-concept environment, the remaining settings can be left at their default values.

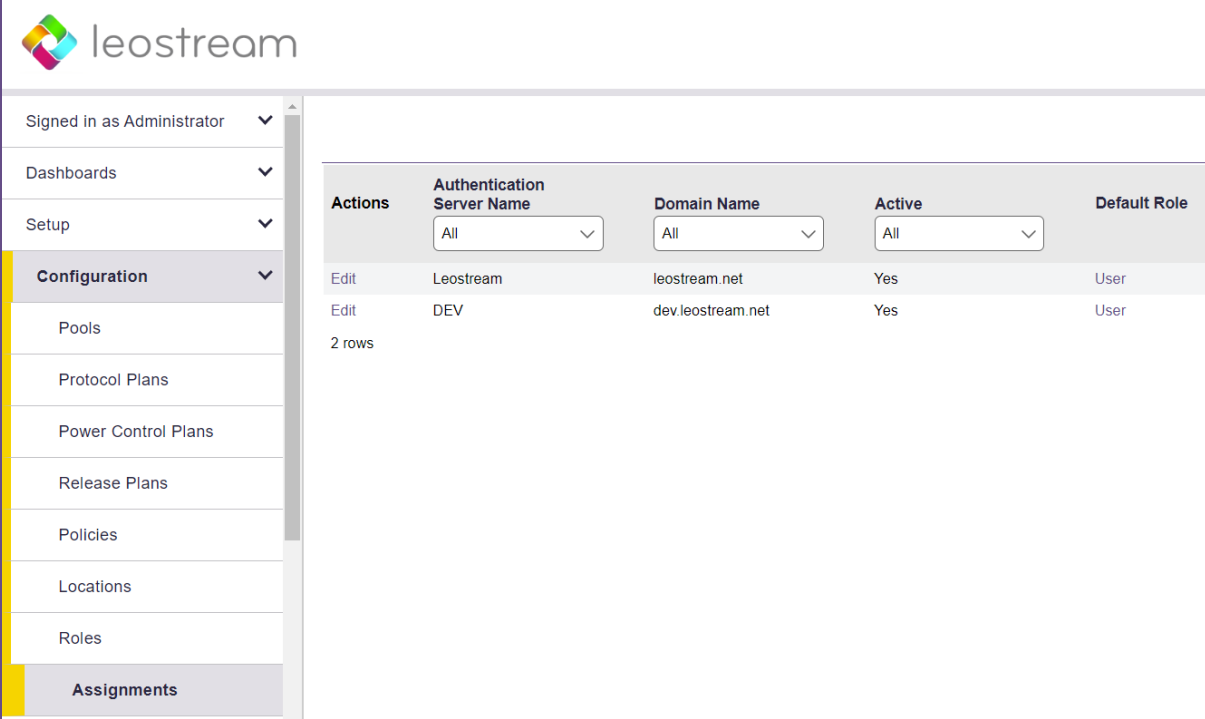
- f. Click **Save**.

For a complete description of setting up policies, see “Configuring User Experience by Policy” in the [Connection Broker Administrator’s Guide](#).

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
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. 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. For simplicity in this proof-of-concept, you can select **[any group]**.
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 your Amazon WorkSpaces policy to this group and client location pair by selecting it from the **User Policy** drop-down menu, as shown, for example, in the following figure.

Assigning User Role and Policy
 In this section, you can set up rules to assign Users to Roles and Policies based on their group membership. Optionally, use the Order column to re-order the rows.
 NOTE: MFA Providers can be created on the >Setup >MFA Providers page

Order	Group	Client Location	MFA Provider	User Role	User Policy
1	[any group]	All	[None available]	User	WorkSpaces Poli

If you need to assign roles and policies based on a different user attributes, see Step 12 under “Adding Microsoft Active Directory Authentication Servers” in Chapter 13 of 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.

The screenshot shows the Leostream web interface. On the left is a sidebar with a menu: Signed in as Administrator, Dashboards, Setup, Configuration, Resources (highlighted), Desktops, Images, and Users. The main content area shows the 'Users' section. At the top, there are links for 'Create User' and 'Test Login', with a purple arrow pointing to 'Test Login'. Below these links is a table with columns: Actions, Name, and Login Name. The table contains three rows of user data. At the bottom of the table, it says '3 rows'.

Actions	Name	Login Name
<input checked="" type="checkbox"/>	All	All
<input type="checkbox"/> Edit Sign out Test login	Administrator	admin
<input type="checkbox"/> Edit Sign out Test login	Karen Gondoly	kgondoly
<input type="checkbox"/> 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.

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

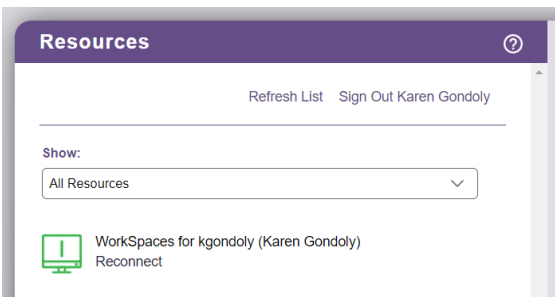


Please complete a login test before contacting Leostream Support.

Connecting to WorkSpaces

In this example, users log in using the Leostream Web client by pointing a web browser at the public IP of your Leostream environment. After the user logs in, they are presented with their WorkSpaces instance.

Because the user is already assigned to the instance, they are presented with an option to **Reconnect**, as shown in the following figure.



Clicking **Reconnect**, in this example, launches an in-browser RDP connection via the Leostream Gateway.