



# leostream<sup>®</sup>

Remote Desktop Access Platform

## **The Leostream Platform for HP Anyware**

Enterprise Management for Hybrid Hosted Desktops and PCoIP<sup>®</sup> Technology

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](mailto:features@leostream.com).

To request product information or inquire about our future directions, email [sales@leostream.com](mailto:sales@leostream.com).

## 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.

HP and the HP Logo are registered trademarks of HP Hewlett Packard Group LLC. The OpenStack Word Mark and OpenStack Logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. Leostream is not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community. Linux is the registered trademark of Linus Torvalds in the U.S. and 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

<b>CONTENTS .....</b>	<b>3</b>
<b>CHAPTER 1: OVERVIEW .....</b>	<b>4</b>
THE LEOSTREAM CONNECTION BROKER VERSUS THE HP ANYWARE MANAGER .....	4
HOSTING PLATFORM OPTIONS .....	5
HIGH-LEVEL ARCHITECTURE .....	6
HP ANYWARE COMPONENTS.....	6
USING HP ANYWARE PCOIP CLIENTS WITH THE LEOSTREAM PLATFORM.....	7
<b>CHAPTER 2: BUILDING A PROOF-OF-CONCEPT .....</b>	<b>9</b>
INSTALLING THE LEOSTREAM CONNECTION BROKER.....	9
INSTALLING THE PCOIP CONNECTION MANAGER AND SECURITY GATEWAY.....	9
<b>CHAPTER 3: PREPARING DESKTOPS AND IMAGES .....</b>	<b>10</b>
INSTALLING LEOSTREAM AGENTS.....	10
INSTALLING THE HP ANYWARE PCOIP AGENT .....	10
WORKING WITH MACOS DESKTOPS.....	10
<b>CHAPTER 4: CONFIGURING THE CONNECTION BROKER .....</b>	<b>11</b>
STEP 1: ADDING AUTHENTICATION SERVERS .....	11
<i>Defining an Authentication Server .....</i>	<i>11</i>
<i>Enabling PIV/CAC Cards for Leostream Logins .....</i>	<i>13</i>
<i>Multi-Factor Authentication Options.....</i>	<i>14</i>
STEP 2: ADDING DESKTOPS .....	15
<i>Connecting the Leostream Platform to an OpenStack Cloud .....</i>	<i>15</i>
<i>Connecting the Leostream Platform to Amazon Web Services .....</i>	<i>16</i>
<i>Connecting the Leostream Platform to Microsoft Azure .....</i>	<i>17</i>
STEP 3: DEFINING POOLS AND PROVISIONING INSTANCES.....	18
<i>Pooling by Center.....</i>	<i>18</i>
<i>Provisioning New Desktops .....</i>	<i>20</i>
STEP 4: DEFINING PLANS .....	21
<i>Protocol Plans.....</i>	<i>22</i>
<i>Power Control Plans.....</i>	<i>23</i>
<i>Release Plans .....</i>	<i>25</i>
STEP 5: DEFINING USER POLICIES.....	27
STEP 6: CREATING LOCATIONS THAT REQUIRE PIV/CAC LOGINS .....	29
STEP 7: ASSIGNING USER ROLES AND POLICIES.....	31
STEP 8: TESTING USER LOGIN .....	33
STEP 9: CONNECTING FROM A PCOIP CLIENT.....	35
<i>Displaying a Disclaimer before PCoIP Client Logins.....</i>	<i>35</i>

## Chapter 1: Overview

As a solution provider, you need to develop and evolve solutions that expand your portfolio and satisfy your customers' needs. You require tools that make it easier to manage the day-to-day operation of your solution, as well as provide the level of access and performance end users require. The combination of Leostream Platform and HP Anyware software is the ideal solution.

The Leostream Platform helps you automate the lifecycle of your environment - including provisioning and deleting desktops and applications - and provides access management, so end users have a seamless login to the correct resources. The HP Anyware software utilizes the industry-leading PCoIP® Technology, so your applications are delivered securely via a lossless display protocol, ensuring uncompromised user experience – regardless of network conditions.

Using the Leostream Platform with the HP Anyware software, you can host solutions that provide secure, policy-based access to desktops and applications from any client device, including PCoIP Zero Clients and PCoIP Soft Clients and Mobile Clients (iOS and Android), from any hosting platform, including VMware, Amazon Web Service, Microsoft Azure, Google Cloud Platform, and more.

This document describes how to integrate the Leostream Platform with HP Anyware software.

## The Leostream Connection Broker versus the HP Anyware Manager

HP Anyware software includes the Anyware Manager that you can use for small environments with basic requirements. When you need to go above and beyond simple assignments or need to model more complex business workflows, replace the Anyware Manager with the Leostream Connection Broker.

The following table summarizes some of the advanced functionality in the Leostream Connection Broker compared to the HP Anyware Manager

Functionality	Anyware Manager	Leostream Connection Broker
Supports dark sites with no network access	Yes – Anyware Manager is available as a hosted service or can be installed for on-premises	Yes – Leostream Connection Broker is installed in your environment
Authentication	Microsoft Active Directory	Active Directory, OpenLDAP, and local users
Smart card support	No	Supports PIV/CAC for PCoIP Zero Client logins
Multifactor authentication	Yes, with RADIUS	Yes, with RADIUS and SAML-based identity providers
Requires managed desktops be joined to an Active Directory domain	Yes	No

Functionality	Anyware Manager	Leostream Connection Broker
User assignment	One-to-one user-to-workstation	One-to-one or pool-assigned
Display protocol support	PCoIP technology	PCoIP, HP Remote Boost (RGS), Mechdyne TGX, NICE DCV, NoMachine, Microsoft RDP, Scyld Cloud Workstation, VNC
Provisioning	Manually create individual machines	Batch provisioning based on static limits or time-of-day – automatically increase and decrease pool size based on demand
Idle time monitoring	Managed via the Windows Registry or Linux .conf files	Easily configured via Release Plans in the Administrator Web interface
Power control	Automatically power down idle machines	Power Control plans can automate power down based on idle time, disconnects, logouts, or length of assignment
Audit level logging and tracking	No	Yes
macOS remote host support	Yes	Yes, using VNC, NoMachine, PCoIP, including Amulet Hotkey KVM Extenders, and Scyld Cloud Workstation

## Hosting Platform Options

The combination of the Leostream platform and HP Anyware Software allows you to manage high-performance connections to desktops hosted in a number of cloud and virtualization platforms, as well as to physical desktops and workstations. You can manage PCoIP connections to any virtual or physical machine, Windows, Linux, or macOS, with an installed Leostream Agent and PCoIP Agent.

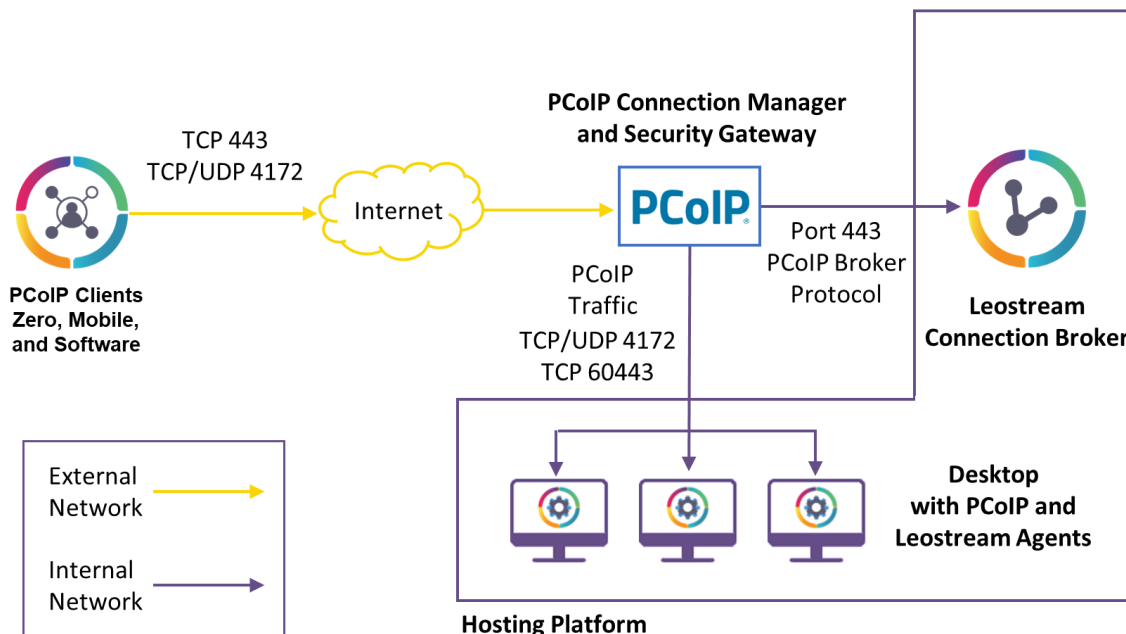
In addition, when using the Leostream platform you can build solutions that automate provisioning and power state for the following cloud and virtualization platforms.

- Amazon Web Services
- Microsoft Azure
- Google Cloud Platform
- OpenStack clouds, both public and hosted in your data center
- Nutanix AHV
- VMware vSphere and ESXi
- Red Hat Virtualization

## High-Level Architecture

A high-level Leostream Connection Broker and HP Anyware Software architecture is shown in the following figure. This architecture assumes users log in from a PCoIP client. If you wish to use a SAML-based Identity Provider to authenticate users into your Leostream environment, then launch the PCoIP connection from the Leostream Web client, please consult the Leostream guide [for Integrating with SAML-Based Identity Providers](#) for more information.

High-Level Leostream / HP Anyware Architecture



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

The following sections give an overview of the Leostream platform and HP components. For more information and documentation on the HP Anyware, visit the [HP Anyware Web site](#).

## HP Anyware Components

A solution that integrates Leostream and the HP Anyware Software includes the following HP components.

- PCoIP Connection Manager and Security Gateway:** The PCoIP Connection Manager creates a PCoIP session between the HP Anyware PCoIP client and remote desktop. The PCoIP Security Gateway allows WAN users to access their remote desktops from the Internet without having to set up a VPN connection. It is not required for LAN access. The Leostream Connection Broker communicates with the PCoIP Connection Manager using the PCoIP Broker Protocol, to offer the correct resources to the user based on their Leostream policy.



The PCoIP Connection Manager and Security Gateway is not the same as the HP Anyware Manager. If you already installed an HP Anyware server in your environment, replace it with the

PCoIP Connection Manager and Security Gateway.

- **License Server (optional):** If the PCoIP Agents on your desktops cannot register with the HP automatic cloud licensing server, you can install your own license server to track your session licenses.
- **PCoIP Agents:** The PCoIP Agent enables PCoIP connections to virtual and physical machines. HP offers two versions, a Standard Agent and Graphics Agent, to support different use cases. Desktops with installed PCoIP Agents appear on the > **Resources** > **Desktops** page of the Connection Broker.
- **HP Anyware PCoIP Clients:** The PCoIP client is a device or application for the user to connect to their remote desktop. PCoIP clients decode the PCoIP Session and present the results to the user. A number of client vendors, such as Amulet Hotkey and Dell Wyse®, have embedded PCoIP processors into their end-point, zero client hardware. In addition, users can connect to their desktop using PCoIP Soft Clients and Mobile Clients (iOS and Android). PCoIP client devices appear in the > **Resources** > **Clients** page of the Connection Broker.

## Using HP Anyware PCoIP Clients with the Leostream Platform

You can use any supported PCoIP software, mobile, or zero client to log into a Leostream environment. The type of client you use and whether the client communicates with the Leostream Connection Broker or the PCoIP Connection Manager determines what types of PCoIP-enabled resources the user can connect to.

The following table describes all combinations of resources users can connect to from different types of PCoIP client. The remainder of this guide focuses on connections with HP Anyware, only. For information on using the Leostream platform to manage connections to Remote Workstation Cards without HP Anyware, see the [Leostream Quick Start Guide using PCoIP Remote Workstation Cards](#).

Client Type	Client Points To	The client can connect to: Virtual Machines	The client can connect to: Physical Machines
PCoIP Software Client	PCoIP Connection Manager	Running the Cloud Access Software PCoIP Standard or Graphics Agent	With installed PCoIP Remote Workstation cards if the operating system has an installed PCoIP Agent for Remote Workstation Cards
PCoIP Mobile Client	Security Gateway <i>Disabled</i>		<b>And</b>
PCoIP Zero Client			Running the Cloud Access Software PCoIP Standard or Graphics Agent.

Client Type	Client Points To	The client can connect to: Virtual Machines	The client can connect to: Physical Machines
PCoIP Software Client  PCoIP Mobile Client  PCoIP Zero Client	PCoIP Connection Manager  Security Gateway <i>Enabled</i>	Running the Cloud Access Software PCoIP Standard or Graphics Agent	Running the Cloud Access Software PCoIP Standard or Graphics Agent
PCoIP Zero Client	Leostream Connection Broker	Running the VMware Horizon View Direct Connection Plug-In	With an installed PCoIP Remote Workstation Cards (no PCoIP RWC Agent installed)
PCoIP Zero Client  PCoIP Software Client - Windows	Leostream Gateway, forwarding to the Connection Broker	Not currently supported	With an installed PCoIP Remote Workstation Cards (no PCoIP RWC Agent installed)
Leostream Connect  and  PCoIP Software Client (Windows only)	Leostream Connection Broker  Or  Leostream Gateway, forwarding to the Connection Broker	Not currently supported	With an installed PCoIP Remote Workstation Cards (no PCoIP RWC Agent installed)
Leostream Web Client  (PCoIP Software Client installed)	Leostream Connection Broker  Or  Leostream Gateway, forwarding to the Connection Broker	Running the Cloud Access Software PCoIP Standard or Graphics Agent	With installed PCoIP Remote Workstation cards if the operating system has an installed PCoIP Agent for Remote Workstation Cards  <b>And</b>  Running the Cloud Access Software PCoIP Standard or Graphics Agent.



## Chapter 2: Building a Proof-of-Concept

### Installing the Leostream Connection Broker

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



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

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

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

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

For information regarding configuring an OpenStack, Amazon Web Services, or Microsoft Azure environment for use with the Leostream Connection Broker, please see the associated [Quick Start](#) guide for your platform.

### Installing the PCoIP Connection Manager and Security Gateway

The Connection Broker requires the PCoIP Connection Manager in order to communicate with the PCoIP clients. The PCoIP Connection Manager is installed on a separate Linux system. Please contact HP support for more information on downloading and installing the PCoIP Connection Manager.

For instructions on configuring the PCoIP Connection Manager to communicate with your Leostream Connection Broker, see the [Leostream Support Blog](#).

## Chapter 3: Preparing Desktops and Images

The Leostream Connection Broker can manage connections to remote desktops running Microsoft Windows, macOS, and Linux operating systems.

When using the Connection Broker to provision new desktops in AWS, Azure, Google Cloud Platform, or OpenStack, ensure that the master images include an installed and configured Leostream Agent and PCoIP Agent, as described in the following sections. You can also use the Connection Broker to provision new desktops in VMware vSphere and ESXi environments, as well as in Nutanix AHV. Again, ensure that appropriate agents are installed on the templates used for provisioning.

### Installing Leostream Agents

See the [Leostream Installation Guide](#) for instructions on installing the Leostream Agent. During the installation, do *not* select the **Enable single sign-on for PCoIP and VNC** task. This task is used only when establishing PCoIP connections to a workstation with a PCoIP Remote Workstation Card. For more information on the Leostream Agent, see the [Leostream Agent Administrator's Guide](#).

The Leostream Agent can locate the Connection Broker through the `_connection_broker` DNS SRV record. For large installations, Leostream recommends using this DNS SRV record. If you do not have, or do not want to use, a DNS SRV record for the Connection Broker, enter the Connection Broker IP address when you install the agent.

### Installing the HP Anyware PCoIP Agent

The Connection Broker can connect users to Windows, Linux, and macOS desktops that run either the Standard or Graphics PCoIP Agent. Contact HP for more information on obtaining and licensing the HP Anyware Software.

### Working with macOS Desktops

To use the Leostream platform options to log users out of their desktop, such as the Release Plan option to log the user out of the desktop when it is released, ensure that [automatic login](#) is off on the macOS device.

You can set Automatic login to Off by selecting **System Preferences** from the Apple menu and clicking **Users & Groups**. In **Users & Groups**, click the **Login Option** link at the lower-left corner and set the **Automatic login** drop-down menu to **Off**.

## Chapter 4: Configuring the Connection Broker

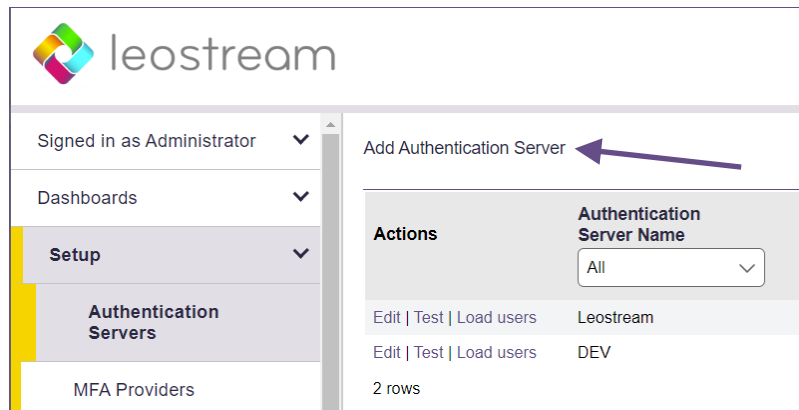
### Step 1: Adding Authentication Servers

The Connection Broker can authenticate users in standard LDAP systems, such as Active Directory, or OpenLDAP™, and with NIS authentication servers. In this example, we add an Active Directory authentication server, as follows. If you do not plan to use an authentication server, you can also define users locally in the Connection Broker. See “Locally Authenticated Users” in the [Connection Broker Administrator’s Guide](#) for more information.

#### Defining an Authentication Server

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

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



3. The **Add Authentication Server** form opens. In the **Authentication Server name** edit field, enter a name for this server in the Connection Broker.
4. In the **Domain** edit field, enter the domain name associated with this Active Directory server.
5. In the **Connection Settings** section, shown in the following figure, use the following procedure to integrate with your Active Directory authentication server.

**Connection Settings**

Specify address using

Hostnames or IP addresses

Hostname or IP address

Port

389

If using multiple addresses, separate each entry with spaces

Algorithm for selecting from multiple addresses

Random

The sequential algorithm uses the first working address in the list

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

AWS Directory ID

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

- a. Select **Active Directory** from the **Type** drop-down list.
  - b. From the **Specify address using** drop-down menu, select **Hostname or IP address**.
  - c. Enter the 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 on the **Encrypt connection to authentication server using SSL (LDAPS)** checkbox if you need a secure connection to the authentication server. The port number automatically changes to 636. Re-edit the **Port** edit field if you are not using port 636 for secure connections.
6. In the **Search Settings** section, shown in the following figure, enter the username and password for an account that has read access to the user records. 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

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

Password

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

For more detailed instructions, see the chapter “Authenticating Users” in the [Connection Broker](#)

Administrator's Guide.

## Enabling PIV/CAC Cards for Leostream Logins

When smart card logins are enabled, users that leverage a PCoIP Zero Client can authenticate into the Leostream environment using their smart card instead of their username and password.

**IMPORTANT NOTES:**

1. Smart card logins are not supported when using a PCoIP Software or Mobile Client.
2. When logging into the Connection Broker with a CAC or PIV card, you must enable the policy option to **Prompt user for alternate credentials before connecting to selected desktop (PCoIP only)**. The PCoIP Agent on the remote desktop is not able to authenticate the user with their smart card and, therefore, requires the username/password in order to connect the user to the remote desktop.
3. Before you begin the following procedure, obtain the Intermediate Certificate or CA Bundle file used to sign the certificates stored on the smart cards.

To enable PIV/CAC card logins:

1. Go to the **> Setup > Authentication Servers** page
2. Edit the Active Directory server used to issue the certificates on the smart card.
3. Scroll down to the **Smart/PIV Card Authentication** section shown in the following figure.

4. Use the **Choose File** button to upload the CA certificate or CA bundle file used to generate and sign the certificates on your smart cards.



You must upload the entire certificate chain, not just the root CA.

5. If you want to use OSCP to check for revoked certificates, select the **Check for certificate revocation using OSCP** option.



When checking certificate revocation, the issuing CA must appear first in the uploaded CA bundle. Also, the user's certificate on the PIV card must contain the OSCP URI.

6. In the **Account linking** drop-down menu, indicate which AD attribute the Connection Broker uses to link the certificate on the smartcard to the appropriate AD user record.
7. Click **Save**.

The Connection Broker validates the certificate when saving the form so you will know, at that time, if there is a problem with your certificate. If the certificate is valid, the Connection Broker displays the certificate's subject and issuer.

Use Leostream Locations to indicate which users require smart card authentication, as described [in Step 6: Creating Locations that Require PIV/CAC Logins](#).



Even though the Connection Broker can validate the certificate and identify the user based on the smart card certificate, the PCoIP Agent for Linux and macOS, installed as part of the Cloud Access Software, authenticates the user by their username and password. Use the **Prompt user for alternate credentials before connecting to selected desktop (PCoIP only)** option in the user's policy to allow the user to enter the username and password to send to the PCoIP Agent running on the remote operating system (see [Step 5: Defining User Policies](#).)

## Multi-Factor Authentication Options

PCoIP clients support multi-factor authentication for any Identity Provider that supports the RADIUS protocol. See the Leostream guide for [Using RADIUS Servers for MFA](#) for more information.

In addition, you can leverage SAML-based Identity Providers (IdP) to provide single sign-on to the Leostream web client with multi-factor authentication, and launch the PCoIP connection from the Leostream Web client. You can integrate the Leostream platform with any authentication service, such as Azure AD, Okta, Duo, and Ping Identity, that acts as a SAML 2.0 Identity Provider. See the Leostream guide for [Using SAML-based Identity Providers with the Leostream Platform](#).

## Step 2: Adding Desktops

To manage desktops, create centers that connect your Leostream Connect Broker to one or more hosting platforms.



*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. For a complete set of instructions for all center types, see “Chapter 6: Connecting to your Hosting Platforms” in the [Connection Broker Administrator’s Guide](#). The remainder of this step focuses on OpenStack clouds, and Microsoft Azure and Amazon Web Services environments.*

---



If you do not see a way to create a center for your hosting platform, please contact [sales@leostream.com](mailto:sales@leostream.com) to update your Leostream license key.

### Connecting the Leostream Platform to an OpenStack Cloud

The Connection Broker uses the OpenStack APIs to inventory the instances and images in your OpenStack cloud. Ensure that you have a user account that has the appropriate permissions for the OpenStack projects you plan to manage in your Connection Broker.

To create an OpenStack center:

1. Go to the > **Setup** > **Centers** page.
2. Click the **Add Center** link.
3. In the **Add Center** form, select **OpenStack** from the **Type** drop-down menu.
4. Enter a name for the center in the **Name** edit field.
5. In the **Auth URL** edit field, enter the public URL to the OpenStack Keystone identity service endpoint, for example:

```
http://external_openstack_ip:5000/v3.0
```

Where `external_openstack_ip` is an IP address to your identity service that is reachable by your Connection Broker.



*Leostream supports only version 3 of the Keystone API.*

---

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

7. Enter the OpenStack domain that contains your project and user in the **Project Domain** edit field.
8. Enter your project name into the **Project** edit field.
9. Enter an administrator domain, username, and password into the **User Domain**, **Username** and **Password** edit fields, respectively.
10. Click **Save** to create the center.

The instances in the center's OpenStack project appear in the **> Resources > Desktops** page. The Connection Broker inventories all images and displays them 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.

### Connecting the Leostream Platform to Amazon Web Services

The Connection Broker can inventory instances and images in your AWS account, and manage provisioning and terminating instances based on the pool, policy, and plan settings in your Connection Broker. To manage desktops hosted in AWS, you must install the Leostream Agent on your AWS instance and ensure that the Connection Broker has network access to the instances.

To create an AWS center:

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

Select **Use attached IAM role** if your Connection Broker EC2 instance has an attached IAM role with appropriate permissions. Otherwise, select **Enter IAM Access Key** and enter the following information. If your Connection Broker is not installed in EC2, the **Authentication** drop-down menu is not available and you must specify the **Access Key ID** and **Secret Access Key**, as follows.

- a. Enter your AWS access key into the **Access Key ID** edit field. You can create an IAM user to use in your Leostream environment. 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. 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.

If you are launching EC2 instances and creating new AMIs in the AWS Management Console, the Connection Broker finds these new items when the next refresh interval occurs.

8. Select the **Continuously apply any Auto-Tags** option to have the Connection Broker create Tags in AWS for the instances inventoried from this center. The Connection Broker creates tags in AWS for each Leostream Tag associated with the instance. See [Tagging AWS Instances and Volumes](#) for complete instructions.
9. Click **Save** to create the center.

The instances in the center's AWS region appear in the > **Resources** > **Desktops** page. The AMIs 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.

## Connecting the Leostream Platform to Microsoft Azure

In order to manage Azure instances, you need to create an Azure center in your Leostream Connection Broker. To create the Azure center, you must first acquire the necessary IDs for your Azure Subscription. See the [Leostream Quick Start Guide for Azure Clouds](#) for information on how to obtain the necessary IDs.

After you have your IDs, to create the 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 directory (tenant) ID into the **Directory (tenant) ID** edit field.
8. Enter your application (client) ID into the **Application (client) ID** edit field.
9. Enter the secret key associated with your Leostream application into the **Secret Access Key** field.

10. Select a time from the **Inventory scan interval** drop-down menu. This setting tells the Connection Broker how often to scan the desktops imported from this center. The scan interval is the length of time between when one scan completes and the next scan begins.
11. 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.



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

### Step 3: Defining Pools and Provisioning Instances

After you create your centers and the Connection Broker inventories all desktops, you can combine the desktops into logical groups, or **pools**. Use pools to create sets of desktops that have similar attribute or are used by a particular group of users.



---

*The Leostream Connection Broker defines a **pool** as any group of desktops. Pools also control provisioning in Leostream.*

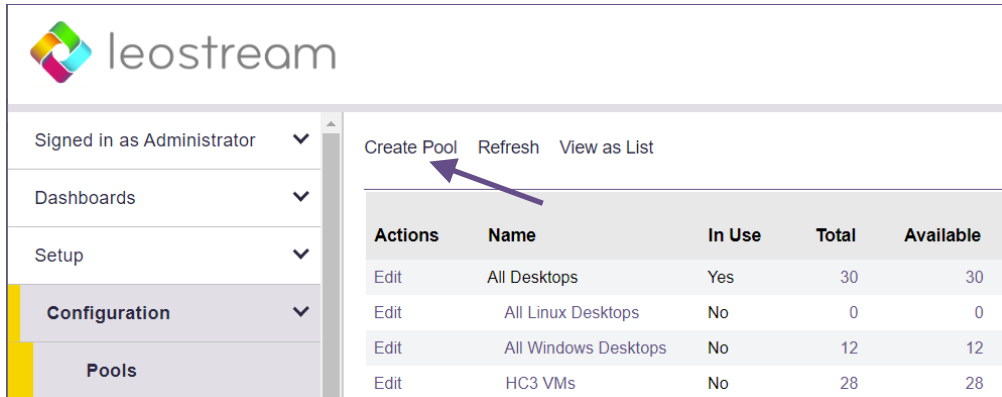
---

How you configure your pools depends on the services you plan to provide to end users and customers. You may pool desktops by customer, or by installed application. The Leostream platform provides a variety of way to configure you pools. For a complete description of pools, see the "Creating Desktop Pools" chapter in the Connection Broker Administrator's Guide.

#### Pooling by Center

If you want to group or provision desktops in a particular center, create your pool, as follows:

1. Go to the > **Configuration** > **Pools** page.
2. Click **Create Pool**, as shown in the following figure.



3. Enter a unique name for this pool in the **Name** edit field.
4. Select **Centers** from the **Define pool using** drop-down menu.

For information on creating pools using desktop attributes or any other method, see the “Creating Desktop Pools” chapter in the Connection Broker Administrator’s Guide.

5. In the **Center Selection** section, select the appropriate center from the **Available centers** list, for example:

The screenshot shows the 'Create Pool' form. It has a purple header with a question mark icon. The form contains several sections:

- Name**: A text input field.
- Display name**: A text input field.
- Pool Definition**: A section with a progress indicator.
- Subset of pool**: A dropdown menu with 'All Desktops' selected.
- Define pool using**: A dropdown menu with 'Centers' selected.
- Available centers**: A list of centers including AWS East, Azure, Enrolled Desktops, Google Cloud Platform, and vCenter Server 7. 'AWS East' is selected.
- Selected centers**: An empty list.
- Buttons**: 'Add item', 'Add all', 'Remove item', and 'Remove all'.
- Distribute new desktop assignments**: A dropdown menu with 'Evenly across all hosts' selected.
- Associate initial user login with assigned user**: A checkbox.

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

6. Click the **Add item** button to the right of the **Available centers** list.
7. Click **Save**.

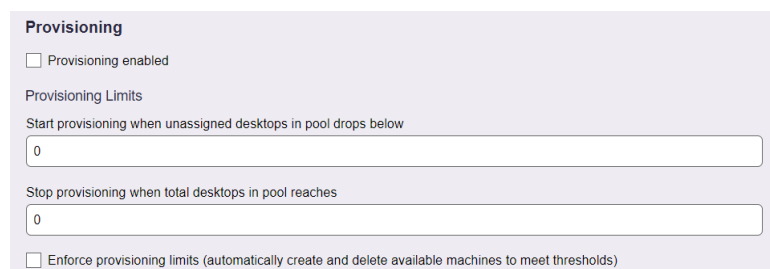
The pool created in this example contains all instances in the subscription associated with the selected Azure center. To instruct the Connection Broker to launch new instances, configure the **Provisioning Limits** and **Provisioning Parameters** sections in the **Edit Pool** page, as described in the next section.

### Provisioning New Desktops

Provisioning allows you to generate new OpenStack, AWS, Azure, Google Cloud Platform, Nutanix AHV, or VMware instances when the number of desktops in a pool reaches a specified lower threshold. Before provisioning instances, ensure that you do the following:

1. Create master images. In OpenStack, the images are displayed on the images page associated with the project. In AWS, the images are the AMIs in your account. For VMware, use the templates or snapshots in vCenter. In Azure, Managed Images can be created in the Azure Resource Manager or using the API. For Nutanix AHV clusters, you can provision new virtual machines from OVAs or free snapshots. For every platform you use, ensure that your master images contain an installed Leostream Agent and PColP Agent.
2. For OpenStack, Azure, and AWS deployments, configure the network where newly provisioned desktops will exist. Ensure that the network ID for this network is included in the **Network UUID** field of your OpenStack center. When provisioning desktops into Azure and AWS, the Leostream platform uses the network you select in the **Provisioning Parameters**.

The **Provisioning** section of the **Edit Pool** page allows you to configure when and how the Connection Broker creates new virtual machines. To begin, select the **Provisioning enabled** checkbox, as shown in the following figure.



The screenshot shows the 'Provisioning' section of the 'Edit Pool' page. It includes a checkbox for 'Provisioning enabled'. Below this is the 'Provisioning Limits' section, which contains two input fields: 'Start provisioning when unassigned desktops in pool drops below' and 'Stop provisioning when total desktops in pool reaches', both with the value '0'. At the bottom, there is a checkbox for 'Enforce provisioning limits (automatically create and delete available machines to meet thresholds)'.

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.

After defining provisioning limits, use the **Provisioning Parameters** section to configure provisioning. See “Chapter 9: Provisioning New Desktops” in the Connection Broker Administrator’s Guide for complete instructions on provisioning into the various platforms.

## Step 4: Defining Plans

After you separate your desktops into pools, define plans that determine how the Connection Broker manages the user’s session.



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

---

## Protocol Plans

### For PCoIP Clients

The Connection Broker always establishes a PCoIP connection when a user logs in using a PCoIP client. Use the **PCoIP Client Configuration** section of the Protocol Plan, shown in the following figure, to configure aspects of the connection.

**PCoIP Client Configuration**

Alternate port for remote viewer port check  
  
If policies use the remote viewer port check to invoke backup pools, enter the port to check for PCoIP connections

Desktop attribute to use for PCoIP connection  
  
If PCoIP Connection Manager or Client is unable to resolve the desktop's hostname, use a Dynamic Tag such as {IP\_PRIVATE} for the desktop hostname

Gateway  
  
Optional, requires PCoIP Remote Workstation Cards without using the PCoIP Connection Manager

1. In the **Alternate port for remote viewer port check** edit field, specify the port the Connection Broker should use when checking if the desktop is running and able to accept PCoIP connections.
2. By default, the Connection Broker sends the desktop's hostname to the PCoIP Connection Manager when establishing connections using HP Anyware Software. If the PCoIP Connection Manager is unable to resolve your desktop hostnames, use the **Desktop attribute to use for PCoIP connections** edit field to specify a different dynamic tag, such as `{IP_ADDRESS}` or `{IP_PRIVATE}`.



The option to specify a Leostream Gateway does not apply when using the HP Anyware Software. To provide access for remote users with HP Anyware Software, leverage the PCoIP Security Gateway.

### For Leostream Web Clients

For users logging in from the Leostream Web client, select **1** for the **Priority** of the **PCoIP Soft Client** in the **Web Browser** section of the protocol plan, as shown in the following figure.

**PCoIP Software Client** Priority:

Hostname or IP address of PCoIP Connection Manager

Send user domain as

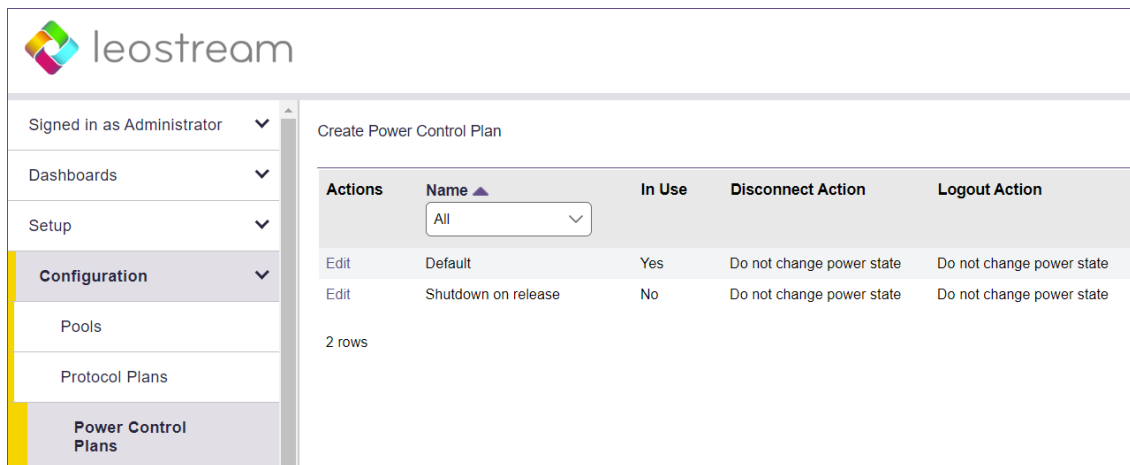
Send user login name as

Desktop attribute to use for PCoIP connection  
  
Use an IP address-based Dynamic Tag if the PCoIP Connection Manager or Client is unable to resolve the desktop's hostname

1. The PCoIP connection must be initiated by a PCoIP Connection Manager, therefore, enter the appropriate address in the **Hostname or IP address of PCoIP Connection Manager** edit field.
2. The Leostream Web client uses a URI to launch the PCoIP software client. In the URI, you can set default values to enter for the username and domain. Use the **Send user domain as** and **Send user login name as** edit fields to set these default values. The user must enter their password into the PCoIP software client to connect to their desktop.
3. By default, the Connection Broker sends the desktop's hostname to the PCoIP Connection Manager. If the PCoIP Connection Manager is unable to resolve your desktop hostnames, use the **Desktop attribute to use for PCoIP connections** edit field to specify a different dynamic tag, such as `{IP_ADDRESS}` or `{IP_PRIVATE}`.

## Power Control Plans

Power control plans define what power control action is taken on a desktop when the user disconnects or logs out of the desktop or when the desktop is released to its pool. Available power control plans are shown on the **> Configuration > Power Control Plans** page, shown in the following figure.



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

The screenshot shows the 'Create Power Control Plan' form. It has a title bar with a question mark icon. Below the title bar is a 'Plan name' text input field. There are four sections, each with a 'Wait' dropdown menu and a 'then' dropdown menu. The sections are: 'When User Disconnects from Desktop', 'When User Logs Out of Desktop', 'When Desktop is Released', and 'When Desktop is Idle'. Each 'Wait' dropdown is currently set to '0 minutes'. Each 'then' dropdown is currently set to 'Do not change power state'. There are four purple arrows pointing from text annotations to specific fields: the first arrow points to the 'Plan name' field; the second arrow points to the 'Wait' dropdown for 'When User Logs Out of Desktop'; the third arrow points to the 'then' dropdown for 'When User Logs Out of Desktop'; and the fourth arrow points to the 'then' dropdown for 'When Desktop is Idle'.


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 three remaining sections:
  - a. From the **Wait** drop-down menu, select a time period to wait before applying the power control action.
  - b. From the **then** drop-down menu, select the power control action to apply. Selecting **Do not change power state** renders the setting in the **Wait** drop-down menu irrelevant, as no action is ever taken.
4. Enter any optional **Notes**.
5. Click **Save** or **Cancel** to return to the **> Configuration > Power Control Plans** page without creating the plan.

---

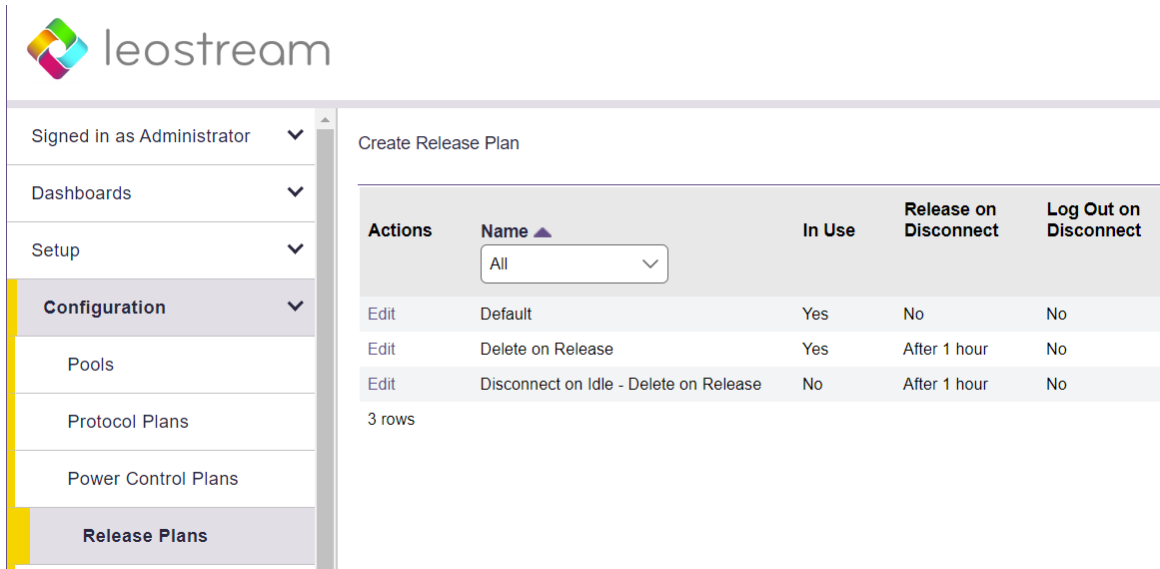
 *The desktop must have an installed and running Leostream Agent to allow the Connection Broker to distinguish between user logout and disconnect and to perform actions based on idle time.*

---



## Release Plans

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



The screenshot shows the Leostream web interface. The left sidebar has a navigation menu with the following items: Signed in as Administrator, Dashboards, Setup, Configuration (expanded), Pools, Protocol Plans, Power Control Plans, and Release Plans (selected). The main content area is titled 'Create Release Plan' and displays a table of existing release plans.

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

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

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

**Create Release Plan**

Plan name

When User Disconnects from Desktop

Release to pool: No

Log user out: 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.

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.

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


2. Enter a unique name for the plan in the **Plan name** edit field.
3. In the **When User Logs Out from Desktop** section, select **No** from the **Release to pool** drop-down menu to create a release plan for persistent desktops. Otherwise, use the **Release to pool** drop-down menu to indicate how long the user is assigned to the desktop.
4. In the **When Desktop is Released** section, select the **Delete virtual machine from disk** option to have the Connection Broker terminate the virtual workspace when the desktop is released back to its pool.

The desktop must be marked as deletable on the **Edit Desktop** page or the Connection Broker will not perform the terminate action.

5. Click **Save**.

## Step 5: Defining User Policies

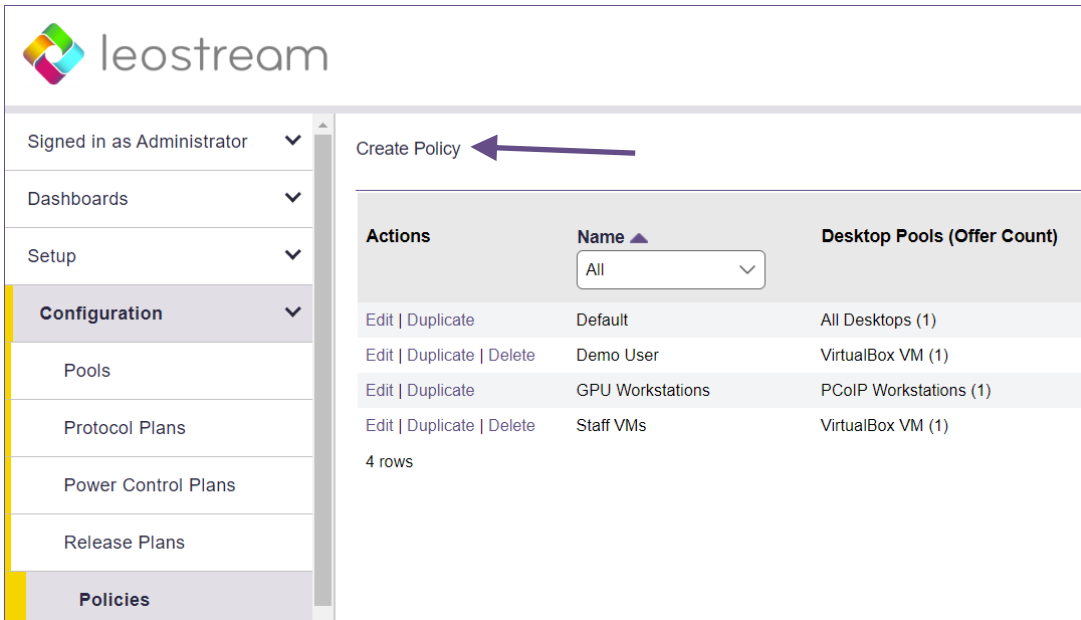
After you define pools and plans, build policies that assign the plans to desktops.

 *The Leostream Connection Broker defines a **policy** as a set of rules that determine how desktops are offered, connected, and managed for a user, including what specific desktops are offered, which Power Control and Release plans are applied to those desktops, what USB devices the user can access in their remote desktop, and more.*

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

You can create additional policies, as follows:

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



The screenshot shows the Leostream web interface. On the left is a navigation menu with the following items: Signed in as Administrator, Dashboards, Setup, Configuration (highlighted), Pools, Protocol Plans, Power Control Plans, Release Plans, and Policies. The main content area is titled 'Create Policy' with a purple arrow pointing to the button. Below this is a table with the following columns: Actions, Name, and Desktop Pools (Offer Count). The table contains four rows of data:

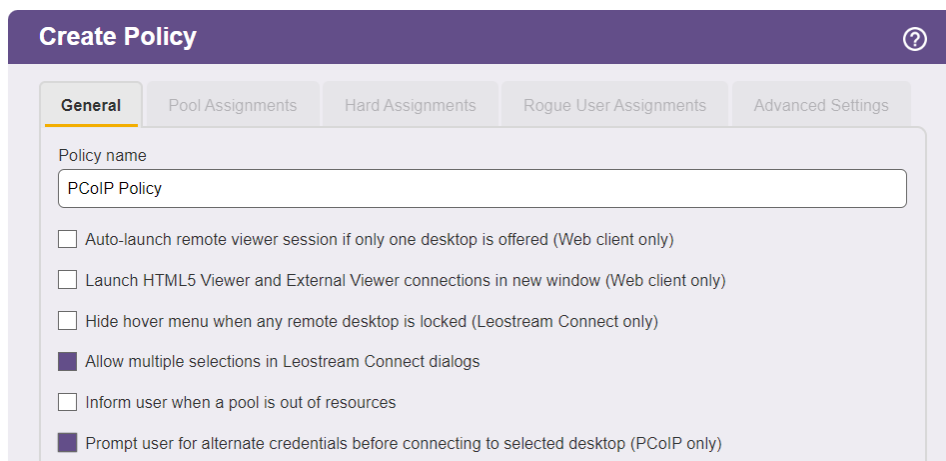
Actions	Name	Desktop Pools (Offer Count)
<a href="#">Edit</a>   <a href="#">Duplicate</a>	Default	All Desktops (1)
<a href="#">Edit</a>   <a href="#">Duplicate</a>   <a href="#">Delete</a>	Demo User	VirtualBox VM (1)
<a href="#">Edit</a>   <a href="#">Duplicate</a>	GPU Workstations	PCoIP Workstations (1)
<a href="#">Edit</a>   <a href="#">Duplicate</a>   <a href="#">Delete</a>	Staff VMs	VirtualBox VM (1)

Below the table, it indicates '4 rows'.

3. In the **Create Policy** form, enter a name for the policy in the **Policy name** edit field. For a discussion of the remaining general policy properties, see the [Connection Broker Administrator's Guide](#).
4. If you are using PIV/CAC cards for Leostream login or if you need to use different user credentials to

log into the remote operating system then used to log into Leostream, select the **Prompt user for alternate credentials before connecting to selected desktop** option in user's policy, as shown in the following figure.

This option allows you to, for example, log into the Connection Broker using Active Directory credentials while logging into the desktop as a local user.



The screenshot shows the 'Create Policy' interface with the following details:

- Title:** Create Policy
- Tabs:** General (selected), Pool Assignments, Hard Assignments, Rogue User Assignments, Advanced Settings
- Policy name:** PCoIP Policy
- Options:**
  - ☐ 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)

With this option selected the user enters their initial credentials (either a smart card or a username/password) to log into the Connection Broker and the Connection Broker assigns the user to a policy based on these credentials.

When displaying the list of desktops offered by the user's policy, the Connection Broker prompts the user to select their desktop and enter the alternate credentials to pass to the PCoIP Agent on the desktop.

5. Click **Save** to initialize the policy.
6. Go to the **Pool Assignments** tab.
7. Click the **Add Pool Assignments** link. The **Edit Pool Assignment** form opens.
8. 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.
9. 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



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.

---

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.

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

11. Click **Save**.



*You do not need to select the **Enable single-sign-on to desktop console** option when using the HP Anyware Software. The PCoIP Agent automatically performs single sign-on to the remote desktop.*

---

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.

## Step 6: Creating Locations that Require PIV/CAC Logins

The Leostream platform supports PIV/CAC card logins only for users logging in using PCoIP Zero clients. You indicate which Zero clients require PIV/CAC card logins using Leostream Locations.

1. Go to the > **Configuration** > **Locations** page.
2. Create a new location.
3. Select the **Require PIV smart card for login** option, as shown in the following figure.

PCoIP software or mobile clients that fall into this location will not require PIV card logins.

Create Location

Name

PCoIP

Subset of location

All

Attribute Selection

Client attribute	Conditional	Value
Device type	is equal to	PCoIP

[Add rows]

☐ The Clients must match any of the attribute rules (OR)
 ☒ The Clients must match all of the attribute rules (AND)

Plans

Protocol:

<Determined by policy>

PCoIP Zero Client Authentication

NOTE: A CA certificate or bundle file must also be uploaded to the Authentication Server(s)

☒ Require PIV smart card for login

When using smart card authentication, the user's policy must select the **Prompt user for alternate credentials before connecting to selected desktop** option. In this case, the workflow of a user login is as follows.

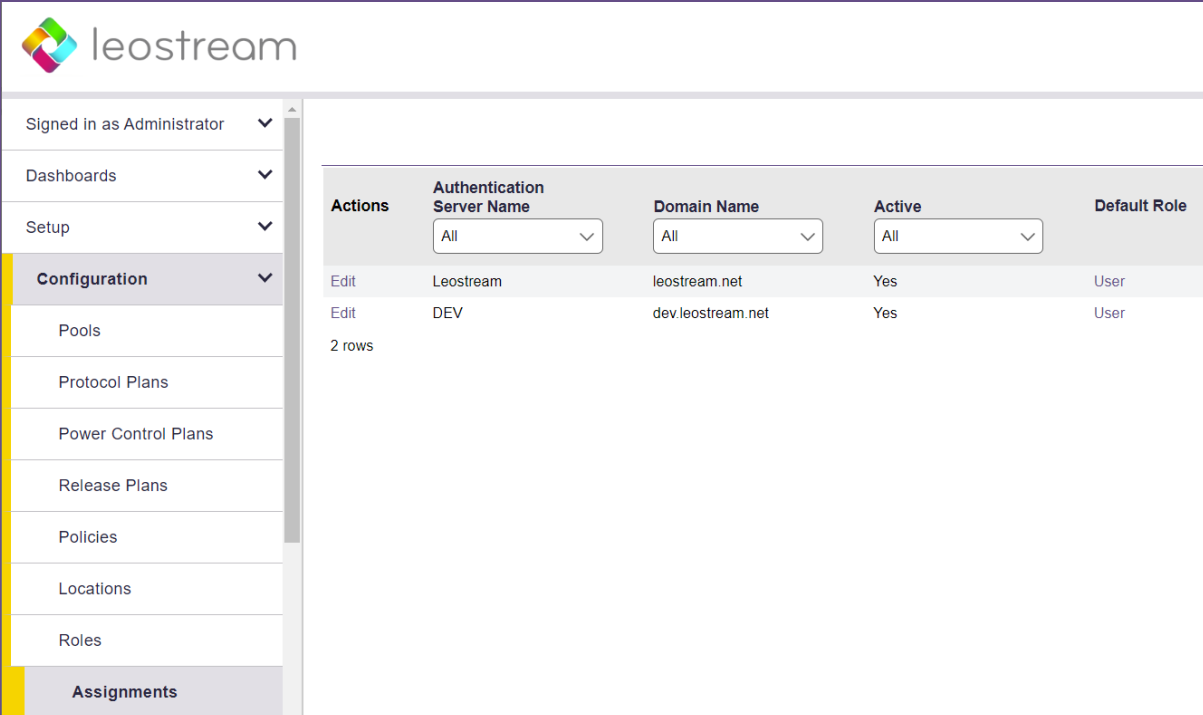
- The user points the Zero client at the PCoIP Connection Manager and Security Gateway and clicks **Connect**.
- The Leostream Connection Broker informs the PCoIP Connection Manager that PCoIP clients fall into a location that requires smart card logins.
- The Zero Client displays a prompt for the user's smart card or, if it's already inserted, asks for the PIN.
- The zero client uses the PIN to unlock the smart card. A validation process then takes place between the Zero client, the Leostream Connection Broker, and Active Directory to ensure that the smart card contains a valid certificate.

- If the certificate is valid, the Connection Broker uses the `userPrincipalName`, or email address if the `userPrincipalName` is not available, from the certificate to identify the user and determine their policy.
- a. The Connection Broker returns the user's list of offered desktop to the Zero client. With the **Prompt user for alternate credentials before connecting to selected desktop** option selected, the Zero client displays the list and prompts the user to select the desktop to connect to and enter the username and password for that desktop. The alternate credentials are passed to the PCoIP Agent on the remote workstation to use to establish the PCoIP connection and perform single sign-on to the remote operating system.

## Step 7: Assigning User Roles and Policies

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

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



Actions	Authentication Server Name	Domain Name	Active	Default Role
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

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

Users will be assigned the default role and policy if they don't match an assignment rule  
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. To require this group of users at this location to pass a multifactor authentication step, select the MFA provider from the drop-down menu. You must use a RADIUS MFA provider when logging in from a PCoIP Client. See the [Leostream Guide for Using RADIUS Servers for MFA](#) for more information.



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

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

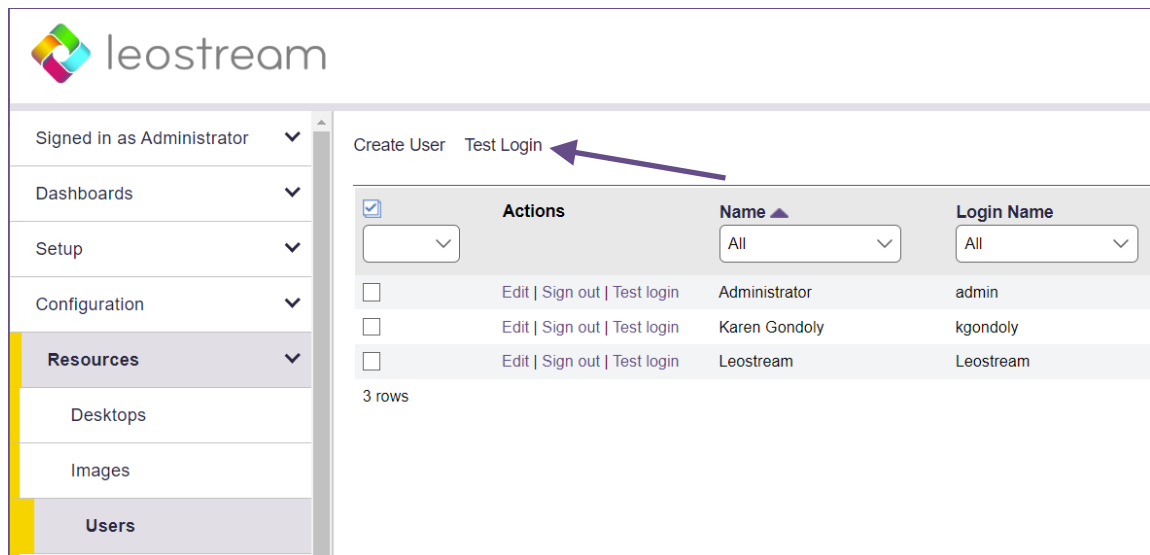
5. Assign a policy to this group and client location pair by selecting an item from the **User Policy** drop-down menu.

If you need to assign roles and policies based on a different user attribute, see “Assigning Roles and Policies Based on any Attribute” in Chapter 14 of the [Connection Broker Administrator's Guide](#).

## Step 8: Testing User Login

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

1. Navigate to the **> Resources > Users** page. As users log into your Leostream environment, their user information is added to this page. You do not need to load users before they can log in.
2. Click the **Test Login** link at the top of the page, shown in the following figure.



3. In the **Test Login** form that opens, enter the name of the user to test in the **User Name** edit field.
4. If you are allowing the user to specify their domain, select a domain from the **Domain** drop-down.

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

**Test Results**

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

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

Trying to match with Authentication Server Assignment rules: ([edit](#))

1: "memberOf" exactly matches "CN=Karen Test Sub Group,OU=Karen Test,OU=Karen Groups,DC=leostream,DC=net", location "All" ← no attribute match  
2: "memberOf" exactly matches "CN=Students,OU=Security Groups,DC=leostream,DC=net", location "All" ← **matched**

**User will have Role "User" and Policy "Default"**

User must first successfully authenticate with RADIUS server "Okta RADIUS Agent" ← **PIN+token not provided**  
User's role provides access to Web Client, only.

**Policy: Default** ([edit](#))

No hard-assigned desktops found

**Pool "All Desktops"** ([edit](#))

Including pool for all users  
Looking for two desktops  
Policy settings for this pool:

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

(389 total, 383 in service, 18 policy filtered, 18 pool filtered, 18 available, 8 running, 8 with an IP address)

kdg-debian9 ← **available**, running, Leostream Agent v5.1.22.0, will offer as: "kdg-debian9", will connect via RDP ([show](#)) ← will use protocol plan "Default" associated with policy [Default](#)  
kdg-1803 ← **available**, running, Leostream Agent v7.3.13.0, will offer as: "kdg-1803", will connect via RDP ([show](#)) ← will use protocol plan "Default" associated with policy [Default](#)

Offering two desktops with this policy.

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



*Please complete a login test before contacting Leostream Support.*

---

## Step 9: Connecting from a PCoIP Client

When using a PCoIP zero client with Leostream and the HP Anyware Software, ensure that you configure the client as follows.

1. Set the **Connection Type** to **PCoIP Connection Manager**
2. In the **Server URI** field, enter the `https` address of the PCoIP Connection Manager. Do not enter the Leostream Connection Broker address.

To connect to Leostream using a PCoIP soft or mobile client, enter the address of the PCoIP Connection Manager into the client. Do not enter the Leostream Connection Broker address.



If the client displays a 6609 error when you attempt to connect to your desktop, ensure that the **Hostname** field on the **Edit Desktop** page for that desktop contains a value that resolves. If the PCoIP Agent on the desktop cannot resolve the hostname, the connection fails. If this occurs replace the **Hostname** value with the IP address.

## Displaying a Disclaimer before PCoIP Client Logins

PCoIP connections typically result in single sign-on to the remote operating system. This may be incompatible with Microsoft GPOs used to display a disclaimer prior to the remote operating system login.

If you need your users to accept a disclaimer prior to connecting to their desktop, you can use Leostream to display a disclaimer before they log into your Leostream environment and connect to their desktops. Disclaimers display on PCoIP Zero clients, software clients, and mobile clients.

You enable disclaimers, as follows.

1. Scroll down to the **PCoIP Client Configuration** section on the **> System > Settings** page in your Connection Broker, shown in the following figure.

**PCoIP Client Configuration**

☒ Require users to accept disclaimer before authenticating

Disclaimer text

Enter your disclaimer text.

Rejection text

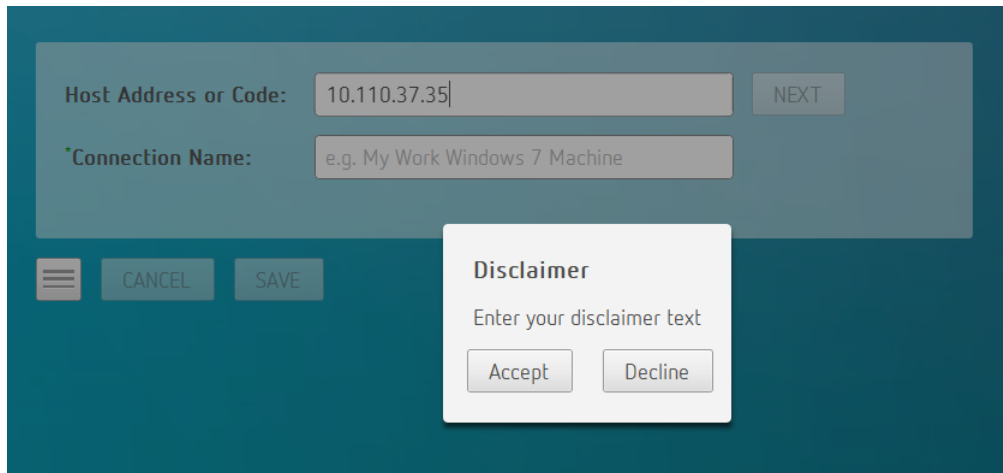
Enter text to display if the user rejects the disclaimer.

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

2. Select the **Require users to accept disclaimer before authenticating** option.
3. In the **Disclaimer text** edit field, enter your full disclaimer text. HTML formatting is not currently supported.

4. In the **Rejection text** edit field, enter the text to display if the user rejects the disclaimer. Note that not all PCoIP clients display this reply.

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



If the user clicks **Accept**, they are prompted for their credentials to log into the environment. If they click **Decline**, if possible, the rejection text displays, for example:

