Transitioning to Leostream from HP SAM

Overview

This document aims to ease your transition from HP SAM to the Leostream Connection Broker. We want to assure you that the path is *not* fraught with peril.

As you read this document, or if you're a skimmer, look out for any  symbols. These symbols indicate important facts about Leostream that you, as an HP SAM user, should pay particular attention to.

Also, look out for  symbols, which indicate definitions of important Leostream terms.

By the time you're done with this document, you should have answers to all of the following questions.

1. **What components does a Leostream deployment include** and, how are those pieces licensed?
2. Are my favorite **HP SAM features in Leostream**?
3. **What new things can I do** with Leostream in an HP Blade and RGS environment?
4. If I have a **choice between using HP RGS or Leostream for a particular feature**, which do I choose?
5. How does the **terminology** used in SAM and Leostream compare?
6. How do I **configure my Leostream Connection Broker to mimic my SAM** environment?

Need a reference? Please contact sales@leostream.com and they can get you in touch with other customers who have switched from HP SAM to Leostream.

Leostream Components and Licensing

First, understand that there are *four* components to a Leostream solution. Some of the components are required; some are nice-to-haves.

The four components are:

- **The Connection Broker**: The Connection Broker is the central management layer for configuring your deployment, including inventorying desktops, assigning these desktops to users, and defining the end-user experience.

   The Connection Broker is a *virtual appliance*. You *must* have a virtualization platform in which you can install the Connection Broker. Most likely, the server-side of your organization already has a virtualization platform that you can leverage for your Connection Broker installation.

  Ultimately, you'll want to install your Connection Broker in your production virtualization environment. However, you can design your proof-of-concept by installing the Connection Broker into the free and easy-to-install VMware Player. But, again, *don't* use Player for production!

- **Leostream Agent**: The Leostream Agent is installed on your blades. The Agent optional, but highly recommended. The Leostream Agent provides the Connection Broker with insight into the connection status of remote users. Plus, in an HP Blade environment, the Leostream Agent communications blade location information to the Connection Broker.

- **Leostream Connect:** Leostream Connect is a software client provided by Leostream. You may or may not need it, depending on what client devices your users log in from. If you have HP thin clients running the HP Thin OS, you'll want to install the Java version of Leostream Connect onto those clients. If, however, your users are used to logging into the HP SAM client, you can continue to use the SAM client.

  If you do choose to use the HP SAM client, we still recommend that you transition to the Leostream Connect client over time, so you can benefit from software that is fully supported and under development

- **Database:** The Connection Broker stores all information in a database. When building a POC, you'll likely use the Connection Broker's internal Postgres database. However, when you go to production, you need to cluster a number of Connection Brokers around a common Microsoft SQL Server® 2005 or 2008 database. That external database represents the one non-Leostream component that is not covered by our license agreement.


A Leostream license is perptual and per user. A particular user consumes one license, no matter how many blades they log into. Also, that user continues to consume a license when they are not logged in to a blade, as long as Leostream maintains connection and blade assignment information for that user.


In addition to the perpetual user license, you need to purchase a Leostream support subscription. An active Leostream support subscription entitles you to download and install as many instances and updates for the Connection Broker, Leostream Agent, and Leostream Connect clients as you need.

What HP SAM Features does Leostream Provide?

Most HP SAM features are provided in Leostream, albeit under different names (see our description on **terminology**). With Leostream, you can do all of the following and more:

- Use RDP/rdesktop and RGS for desktop connections, as well as a variety of additional protocols such as VNC, NoMachine NX, and Citrix HDX
- Support Windows and Linux operating systems on the client-side and blade/desktop-side
- Manage multiple-monitors, including spanning one session across multiple displays and positioning different sessions on different displays
- Perform dynamic and static assignment of blades to users and clients (i.e., access devices)
- Assign one or more blades from a group of blades to a user based on that user's Active Directory attributes
- Allow users to connect simultaneously to multiple blades
- Forcefully logout users who disconnect from their blades
- Forcefully disconnect or logout users after their sessions are idle for a specified length of time, including suspending the disconnect/logout until the desktop's CPU activity falls below a threshold (policy-assigned desktops, only)
- Provide USB passthrough support
- Use RGS and RDP protocols
- Define levels of administrator access to different resources (users, blades, clients, etc.)
- Smart card support for Windows clients, including support for CAC cards
- Disaster recovery and failover using Leostream Connection Broker clusters

There are, unfortunately, a few SAM features that are *not* supported by Leostream, including:

- You cannot limit access to devices based on time-of-day, as currently provided in SAM Roles
- You cannot power on a stopped blade using HP Integrated Lights-Out (iLO)
- Users cannot use smart cards to authenticate against the Leostream Web client

Leostream has planned some of these features, and more, into our Roadmap. For questions about our roadmap, contact **sales@leostream.com**.

How does Leostream add to an HP SAM & RGS Environment?

While switching to Leostream may seem like a daunting task, after you switch, you'll have access to the multitude of features that Leostream provides above and beyond HP SAM. In particular, you may consider taking advantage of the following Leostream features.

- Access the Administrator Web interface from all Web browsers, including all versions of Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, and Safari
- Single management console for blades, terminal services, and virtual desktop infrastructures
- Deliver Citrix XenApp applications and desktops in conjunction with blades and VDI
- Advanced policy assignment that maximizes resource utilization and eases administration
- Failover functionality for blades, to ensure that users remain productive when their primary blades becomes unavailable
- Advanced location awareness to tailor user access and experience based on the user's physical location
- Additional display protocol support to use the best display protocol based on the user's identity and location
- Ability to set registry keys on the remote blade workstation
- Ability to attach network printers to the remote blade workstation
- When using the Java version of Leostream Connect, allow users to reassign USB devices to different active sessions
- Audit level reporting
- User authentication against multiple, untrusted domains
- User authentication against Novell eDirectory or OpenLDAP authentication servers, in addition to Microsoft Active Directory
- Full support for remote users via third-party SSL VPN solutions, such as Juniper Networks and Cisco

Where do HP RGS and Leostream Features Overlap?

Leostream provides a few features that already exist in HP RGS. Why do you need the Leostream features? If you are using RDP 6 or some other display protocols, the Leostream features are critical for enhancing the user experience.

If you are using HP RGS, you should use the native RGS features to provide the following capabilities. Leostream allows you to use and configure these RGS features inside the Leostream Connection Broker.

- USB device redirection
- Multi-monitor support
- Single sign-on

Ensure that you *do not* install the Leostream equivalents of these features when you install your Leostream Connect clients and Leostream Agents.

How Does the Terminology in Leostream and SAM Compare?

Functionality	HP SAM Terminology	Leostream Terminology
A set or RGS Receiver and RDP client parameters	Policy	Protocol Plan
Clients	Access devices	Clients
A collection of blades	Asset group	Pool
A collection of clients	Asset group	Location
Assign blades from an asset group to a user	Role	Policy
Define permission levels for administrative access to asset groups	Administrator Groups (Permissions)	Roles

Procedure

In general, SAM customers get started by hard-assigning blades to users in Leostream. After your hard-assigned environment is running and you are more familiar with Leostream, you can switch to the full power and flexibility of policy-assignment.

Step 1: Installing the Connection Broker

The Connection Broker is a virtual appliance that installs into most VMware, Citrix, Microsoft, and Red Hat virtualization layers. To download the Connection Broker:

1. Go to:

   http://www.leostream.com/cb

2. Click on the Connection Broker link for your virtualization platform.
3. Unpack the Connection Broker archive.
4. Install the Connection Broker virtual appliance. See the Leostream Installation Guide for complete details on installing the Connection Broker.

After you install the Connection Broker, start the virtual machine. The Connection Broker IP address appears in the virtual machine's console, for example:

If the console cannot obtain an IP address from DHCP, you can manually configure the network. See “Manually Configuring the Connection Broker Address” section in the Leostream Installation Guide for more information.

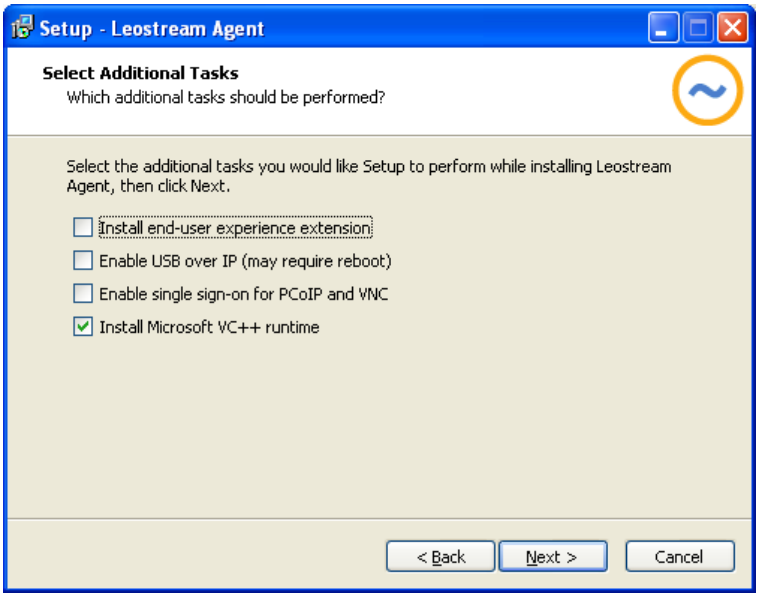
Step 2: Installing Leostream Agents

Leostream recommends that you install the Leostream Agent on all of your blades. The Leostream Agent provides additional control over the user’s session, specifically allowing you to forcefully log out users that disconnect from their sessions. The Agent is also required to display the physical location of HP ProLiant Blades within an HP BladeSystem enclosure,

You can download the latest version of the Leostream Agent from the Leostream **Downloads & Documentation** Web page. During the installation, do *not* select the following two options.

- **Enable USB over IP (may require reboot):** Instead, use the RGS USB redirection feature
- **Enable single sign-on for PCoIP VNC:** Instead, use the RGS Easy Logon or Single Sign-On features

For example:



Consult the Leostream Installation Guide for complete instructions on installing the Leostream Agent.

Step 3: Installing Leostream Connect

When using an HP thin client, you can login to your Leostream Connection Broker using the HP SAM client that is natively installed on the thin client. If, instead, you want to use the Leostream Connect client, you must manually install the Java version of Leostream Connect and a Java run-time environment on the thin client.

For instructions on installing Leostream Connect onto an HP GT7725 thin client, download the following document from the Leostream Knowledge Center.

http://www.leostream.com/resources/documentation/sections/installing-Leostream-Connect-on-HP-7725.pdf

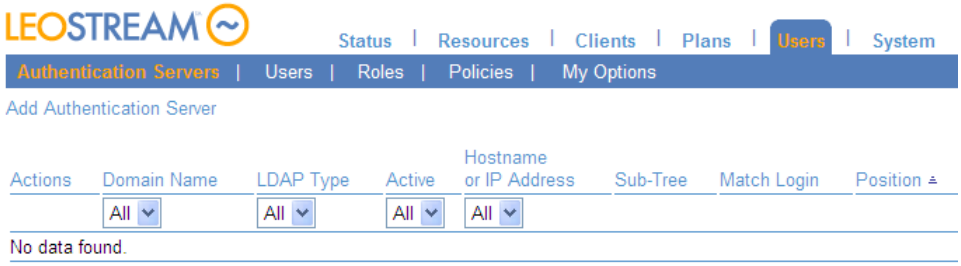
You can also use the Windows version of Leostream Connect to repurpose laptops or other clients running a Windows operating system. Consult the Leostream Installation Guide for complete instructions on installing Leostream Connect.

Step 4: Registering Blades with the Connection Broker

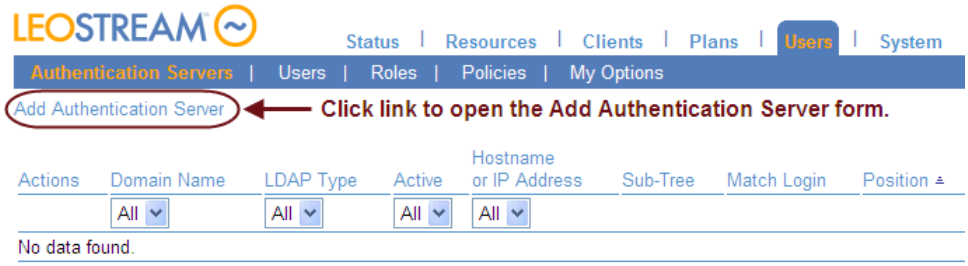
If your blades have associated Computer records in your Active Directory, the Connection Broker can use Active Directory to inventory and assign your blades to users. Doing so is a two step process. First, create an Active Directory authentication server then create an Active Directory center from the authentication server.

Leostream does not automatically connect to your Active Directory server. You must manually create the server record, as described in the following steps.

1. Go to the **> Users > Authentication Servers** page, shown in the following figure.



2. Click the **Add Authentication Server** link, shown in the following figure.



3. The **Add Authentication Server** form opens. Fill in the form with the appropriate information for your Active Directory authentication server. For complete instructions, see "Adding Microsoft® Active Directory® Authentication Servers" in the Leostream Connection Broker Administrator's Guide.

4. Now, to add the Active Directory center, go to the **> Resources > Centers** page.

   Leostream defines ***centers*** as the external systems that inform the Connection Broker about desktops and other resources (such as applications, printers, and Teradici PC-over-IP host devices) that are available for assignment to end users.

5. Click the **Add Center** link.

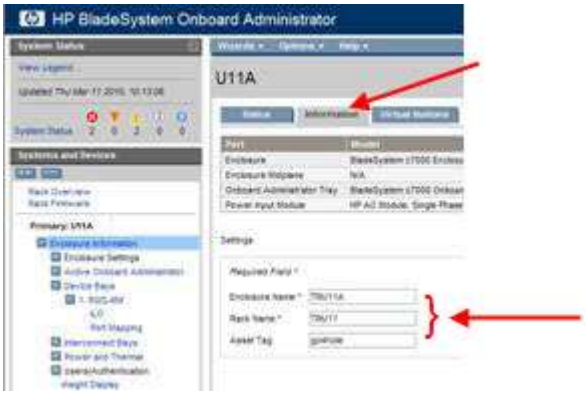
6. Configure the **Add Center** form to create an Active Directory center, as shown in the following figure.

7. Click **Save**.

After the Connection Broker completes its scan of the center, the **> Resources > Desktops** page lists all blades and other desktops that are inventoried in Active Directory. If your blade have a running Leostream Agent, you can display blade location information on the **> Resources > Desktops** page.

Displaying Blade Location

To correctly display blade location, you must enter the blade location, enclosure name, and rack name in the BladeSystem Onboard Administrator, shown in the following figure. In order for the Leostream Agent to correctly pick up the location information, after entering the information, you must reboot the blade.



You can find the blade location information displayed in two places in the Connection Broker. Click **Edit** for any blade on the **> Resources > Desktops** page to display the location information on the right side of the **Edit Desktop** page, for example:

You can also display this information directly on the **> Resources > Desktops** page by adding the **HP Blade Location** column. See **Customizing Tables** in the Leostream Connection Broker Administrator's Guide for information on adding this column to the **> Resources > Desktops** page.

After you add the **HP Blade Location** column, any HP blade that provides location information includes a partial display of this information, as shown in the following figure.

The blade location in the **HP Blade Location** column is displayed in the following format.

```
Rack: Enclosure: Blade location
```

Where `Rack`, `Enclosure`, and `Blade location` are replaced with the values for the rack name, enclosure name, and blade location you entered in the BladeSystem Onboard Administrator.

Step 5: Grouping desktops into pools

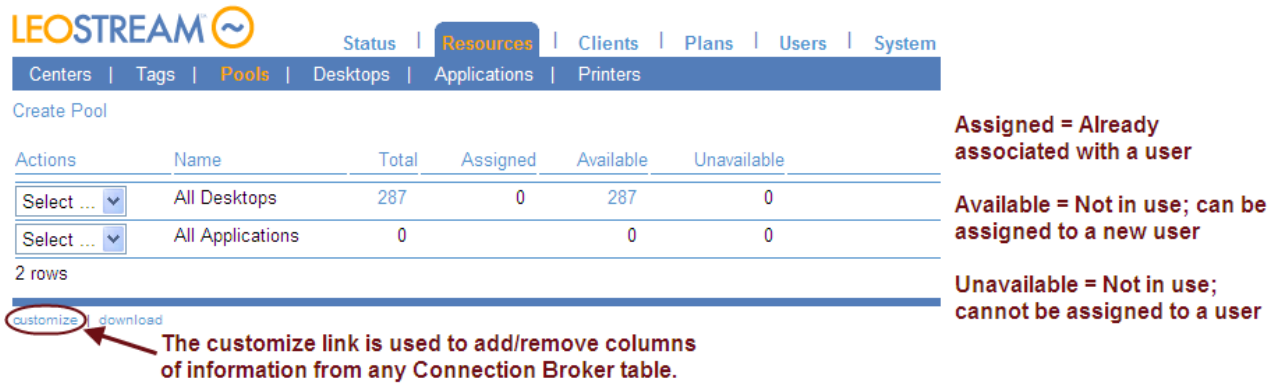
After you create your centers and the Connection Broker registers all your blades, you can combine the blades into logical groups, or ***pools***. Use pools to create sets of desktops that have similar attributes. Creating pools is optional, but provides convenience and flexibility when configuring your Connection Broker.

The Leostream Connection Broker defines a ***pool*** as any group of desktops or applications.

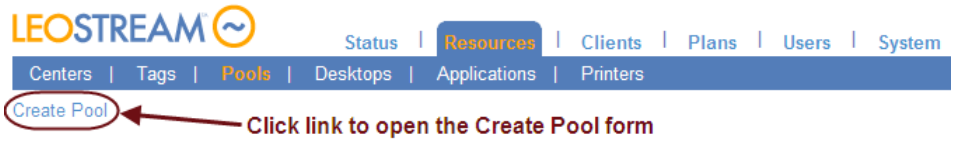
As you transition to Leostream from SAM, you'll probably start by hard-assigning blades to users. In that scenario, Leostream pools are used mostly for inventorying and monitoring purposes. As you move forward, you'll use pools when performing policy assignments.

To create a desktop pool:

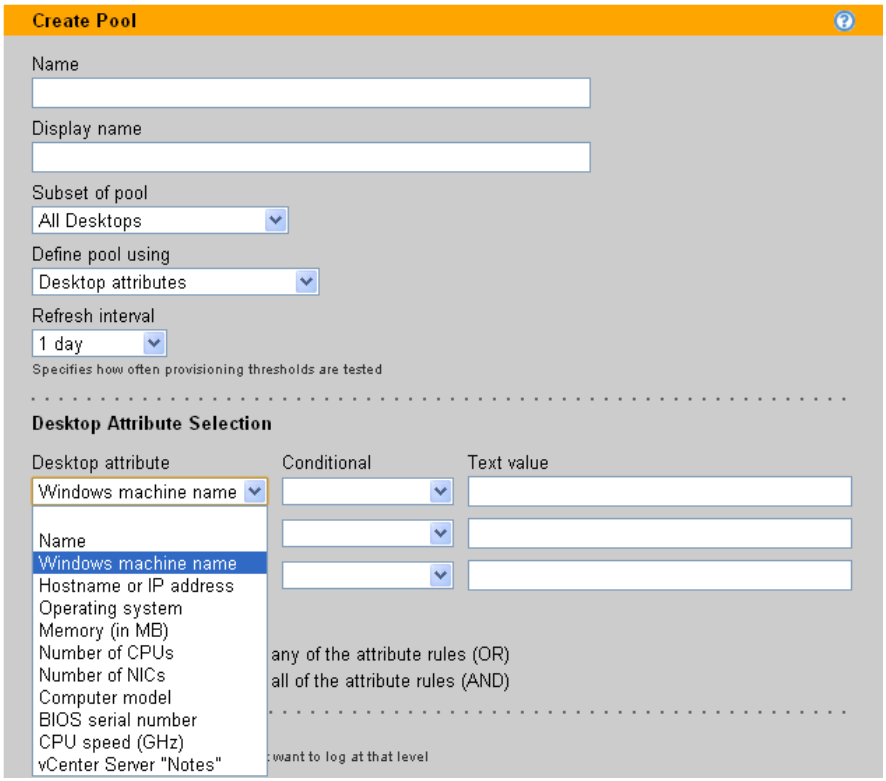
1. Go to the **> Resources > Pools** page, show in the following figure.



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



3. The **Create Pool** form opens. When working with blades, often you want to create pools of blades with similar attributes. Leostream allows you to create pools using the desktop attributes shown in the following figure.



4. Click **Save**. The **> Resources > Pools** page shows the new pool, indented under its parent pool.

Leostream dynamically determines pool membership. As new blades enter your environment, Leostream automatically places these desktops into the appropriate pools.

Step 6: Creating plans

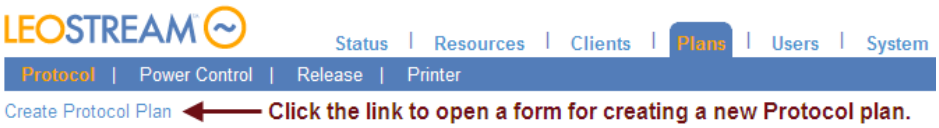
The Leostream Connection Broker defines a ***plan*** as a set of behaviors that can be applied to any number of desktops and pools. This step describes two types of plans: Protocol and Release.

Creating Protocol Plans

Protocol plans configure the RGS Receiver parameters used to launch the RGS connection and, therefore, are analogous to Policies in HP SAM. The following procedure assumes your end users log in through the Leostream Connect client. If they are using an HP SAM client, please consult the "HP SAM Clients" section of the Leostream **Thin Clients Guide** for instructions on configuring the protocol plan.

Correctly configuring the protocol plan is critical for providing your end users with the best experience. For RGS connections, the protocol plan controls multi-monitor configurations, USB redirection, and much more. To create a Protocol plan for RGS:

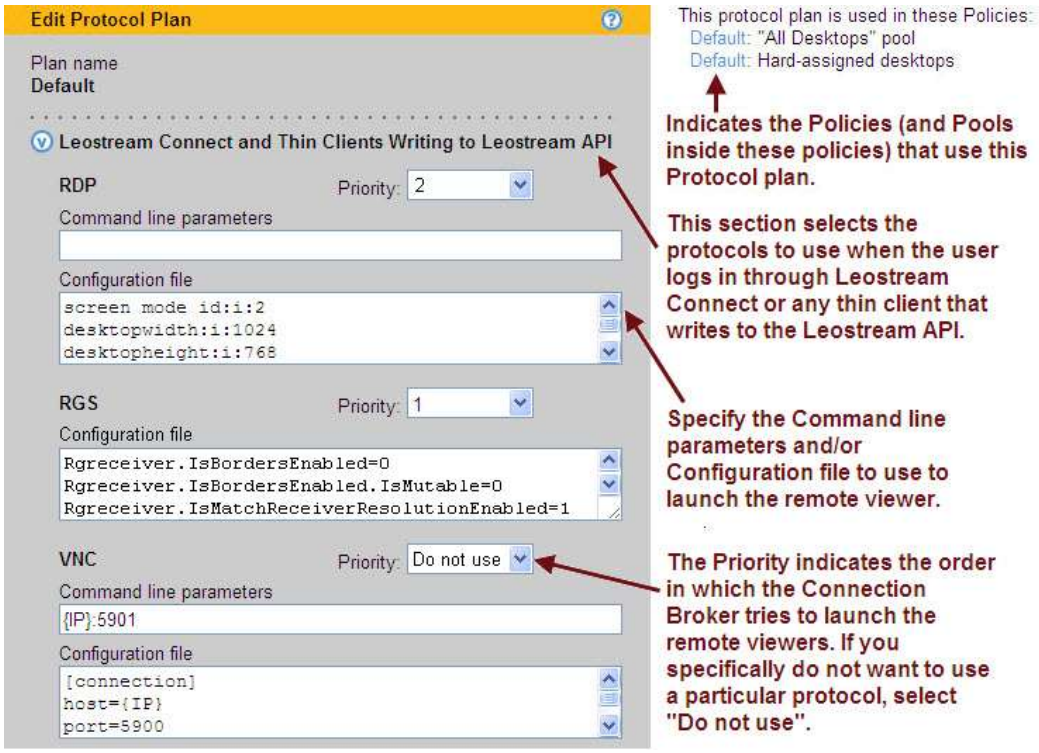
1. Go to the **> Plans > Protocol** page.
2. Click the **Create Protocol Plan** link.



3. In the **Leostream connect and Thin Clients Writing to Leostream API** section of the **Create Protocol Plan** form, Select **1** from the **Priority** menu associated with RGS, as shown in the following figure.

   The setting in the **Priority** drop-down menu determines the order in which the Connection Broker tries to establish desktop connections using the different remote viewing protocols.

   You can give RDP a priority of 2 to have the Connection Broker fail over to RDP if the client cannot contact the RGS sender on the blade. If you do not want to failover to RDP, set the priority for RDP to **Do not use**.



3. The text you enter into the **Configuration file** field is analogous to the `rgreceiverconfig` file that sets RGS Receiver parameters on the client computer when making native HP RGS connections to a remote desktop. See Chapter 8 “RGS properties” in the HP Remote Graphics Software User Guide for a complete description of the available RGS Receiver properties.

   Every RGS Receiver installation provides a documented example `rgreceiverconfig` file in the installation directory.

The following sections describe some important features of protocol plans when used with RGS.

Multi-Monitor and Borderless Connections

By default, the configuration file for RGS enables multi-monitor support and disables the borders. These features are enabled by entering the following text into the **Configuration file** edit field:

```
Rgreceiver.IsBordersEnabled=0
Rgreceiver.IsBordersEnabled.IsMutable =0
Rgreceiver.IsMatchReceiverPhysicalDisplaysEnabled=1
Rgreceiver.IsMatchReceiverPhysicalDisplaysEnabled.IsMutable=0
Rgreceiver.IsMatchReceiverResolutionEnabled=1
Rgreceiver.IsMatchReceiverResolutionEnabled.IsMutable=0
```

The display parameters relate to the **Match receiver display resolution** and **Match receiver display layout** options on the RGS client, which in turn relate to the **Span** and **Match Sender to Client Displays** option in HP SAM Policies.

Set the `IsMutable` parameter off for each RGreceiver parameter. Otherwise, the local settings on the RGS client will over-ride the values set in the protocol plan.

Mimicking Monitor Layouts in Leostream

If you use monitor layouts in HP SAM, you can choose to create analogous hard-coded monitor layouts in

Leostream or allow Leostream to adaptive learn a user's preferred monitor layout.

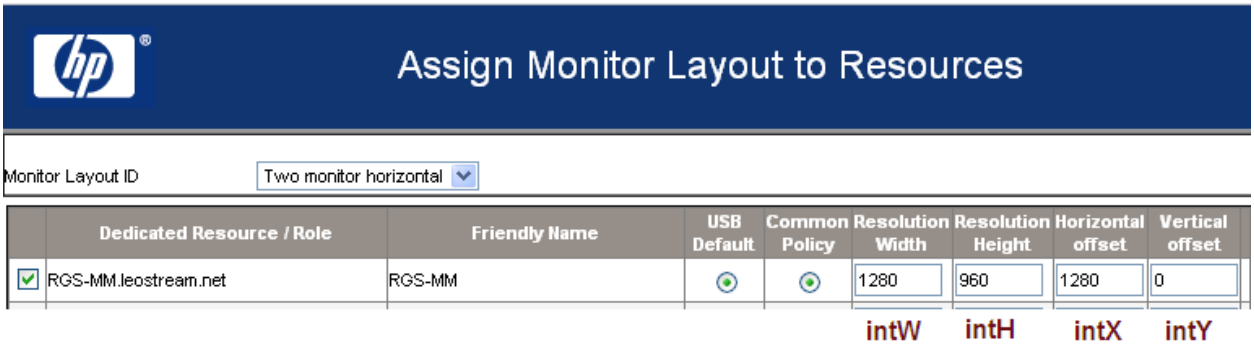
To hard-code a monitor layout, you must create a unique protocol plan for every monitor layout you support in HP SAM. Each protocol plan must include the following parameters into the configuration file.

```
Rgreceiver.Session.<N>.RemoteDisplayWindow.X=intX
Rgreceiver.Session.<N>.RemoteDisplayWindow.Y=intY
Rgreceiver.Session.<N>.VirtualDisplay.IsPreferredResolutionEnabled=1
Rgreceiver.Session.<N>.VirtualDisplay.IsPreferredResolutionEnabled.IsMutable=0
Rgreceiver.Session.<N>.VirtualDisplay.PreferredResolutionHeight=intH
Rgreceiver.Session.<N>.VirtualDisplay.PreferredResolutionHeight.IsMutable=0
Rgreceiver.Session.<N>.VirtualDisplay.PreferredResolutionWidth=intW
Rgreceiver.Session.<N>.VirtualDisplay.PreferredResolution.IsMutable=0
```

Where *<N>*, in each line, is replaced by the RGS session number.

In HP SAM, a monitor layout is associated with a particular blade. In Leostream, you must map the blades to session numbers. Session numbers start at 0 and increase numerically, where 0 is the first session that is launched. Therefore, the previously described parameters are repeated for each blade.

The values for each parameter correspond to the values set in the HP SAM monitor layout definition, as described in the following figure.



Alternatively, instead of hard-coding the monitor layout, if you use the Java version of Leostream Connect, you can enable session position tracking. To do so, add the following line to the `lc.conf` file on the client.

```
enable_window_tracking = true
```

Then, enter the following three lines in the **Configuration file** field.

```
Rgreceiver.Session.{SESSION}.VirtualDisplay.IsPreferredResolutionEnabled=1
Rgreceiver.Session.{SESSION}.RemoteDisplayWindow.X={VALUE:x}
Rgreceiver.Session.{SESSION}.RemoteDisplayWindow.Y={VALUE:y}
```

`{SESSION}` is a Leostream dynamic tag. Leostream Connect automatically adjusts the value for `{SESSION}` when the user connects to multiple desktops using HP RGS. `{VALUE:x}` and `{VALUE:y}` are additional dynamic tags that Leostream Connect uses to label and store the X and Y position of the remote session window for the desktop with session ID `{SESSION}`.

USB Passthrough with HP RGS

If using Java version of Leostream Connect, you can use the Leostream Connect sidebar to switch USB devices between sessions.

Leostream Connect for Windows operating systems does not support the following functionality.

To turn on the sidebar for USB access:

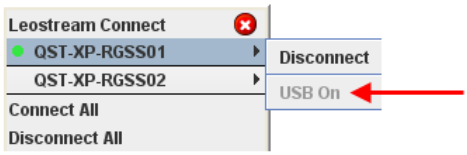
1. Enable the sidebar by adding the following line to the `lc.conf` file on the client device.

   ```
   sidebar_enabled = true
   ```

2. In the protocol plan assigned to users that connect to desktops using HP RGS, add the following line to the **Configuration file** field for HP RGS.

   ```
   Rgreceiver.Usb.ActiveSession={USB_SESSION}
   ```

When a user logs in through Leostream Connect, by default, the first desktop they connect to using HP RGS has access to all USB devices. The sidebar menu for this desktop, shown in the following figure, displays a **USB On** menu item.



When you attach a USB device to your client device, the USB device appears in the remote desktop that indicates **USB On**. You can switch all USB devices to another desktop by selecting the **Turn USB On** menu associated with that desktop, as shown in the following figure.

You must be connected to the desktop using RGS before you can connect USB devices. Leostream Connect prompts you to confirm that all USB devices should be switched to the new desktop. Click **Yes** in the confirmation dialog, shown in the following figure to move USB devices to the new desktop. Click **No** to keep the USB devices attached to the current desktop.

If you disconnect from the RGS session that has access to USB devices, Leostream Connect automatically switches all USB devices to the next active RGS session.

Creating Release Plans

Release plan options allow you to mimic the HP SAM behavior to logout disconnected sessions. However, Leostream does not provide CPU monitoring. If the Leostream is set to logout a disconnect session, the logout occurs regardless of if the user is running any processes.

Release plans relate to policy-assigned desktops. When using hard-assignments, instead of using Release Plans you use policy options to control the user's session, as described in the step 7, building Connection Broker Policies.

Creating Power Control Plans

This example does not configure a power control plan. You can, however, opt to use power control plans to restart or shutdown your blades *if* your blades have a running Leostream Agent.

Leostream does not integrate with HP iLO to provide power control. Therefore, you cannot use iLO to power on stopped blades in Leostream. If you choose to shut down your blades, use wake-on-LAN to automatically power the blades back on when the user tries to connect. See “Using Wake-on-LAN for Power Control” in the Leostream Connection Broker Administrator’s Guide for complete instructions.

Step 7: Building Connection Broker Policies

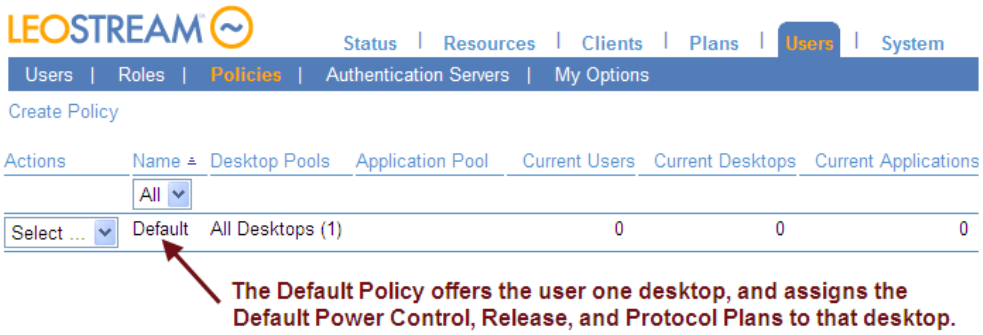
After you define your pools and plans, you can combine them into policies

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

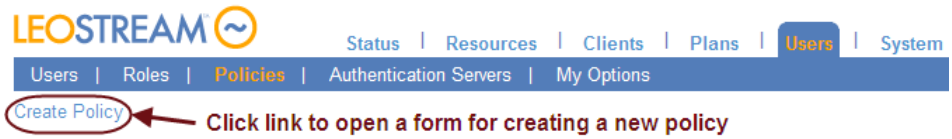
This example assumes you have hard-assigned blades to users

To create a policy:

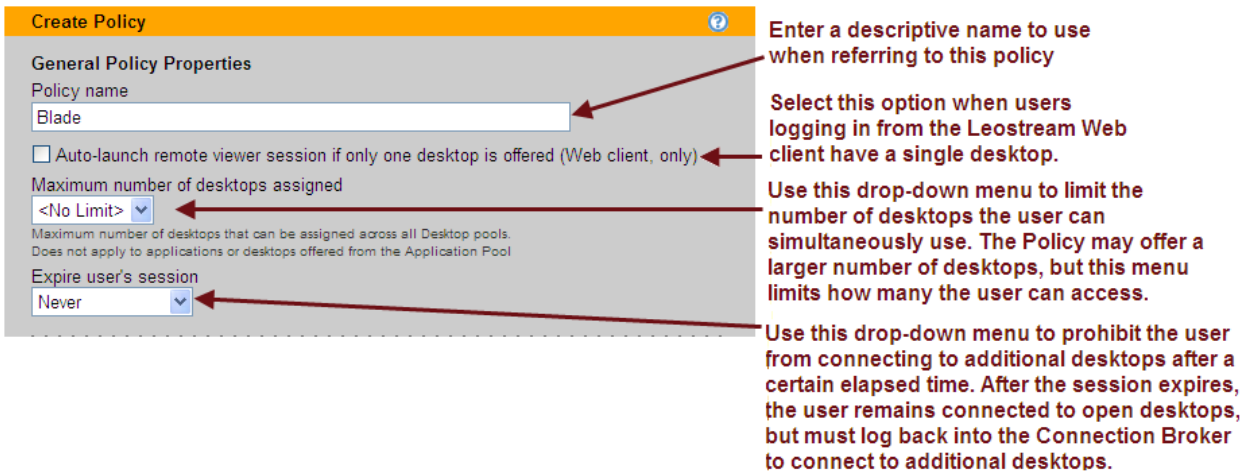
1. Go to the **> Users > Policies** page, shown in the following figure.



2. To create a new policy, click the **Create Policy** link, shown in the following figure.

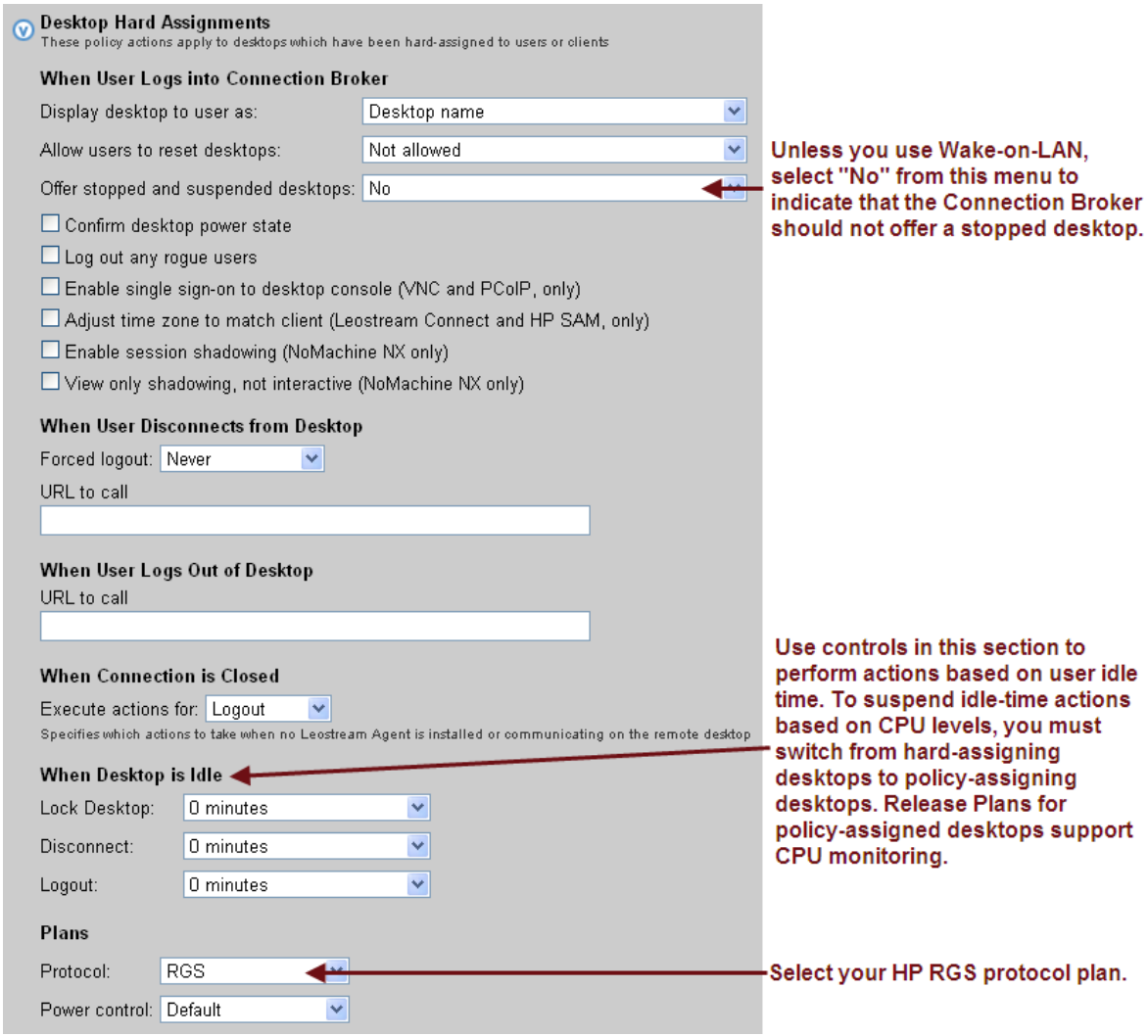


3. The **Create Policy** form opens. Fill in the form with the appropriate information, shown in the following figures.



4. For this example, scroll down to the **Desktop Hard Assignment** section and expand this section.

5. Configure the options in the **Desktop Hard Assignment** section as described in the following figure.



6. Click **Save**.

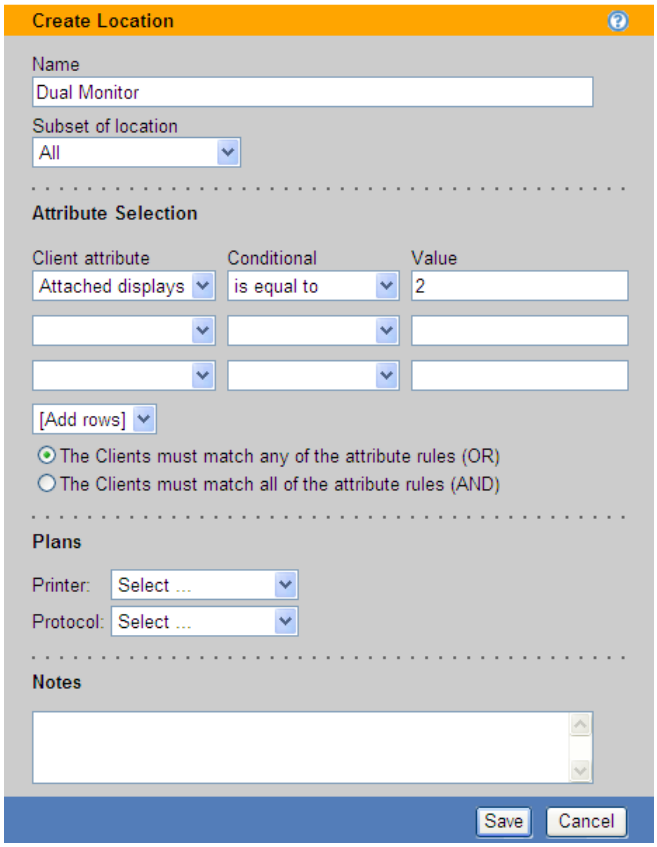
Step 8: Creating Locations

If you hard-coded monitor layouts in protocol plans for clients with a different number of attached displays, you can use client locations to correctly apply the protocol plans based on the user's client.

A *location* is a group of clients with similar attributes. Locations are similar to asset groups that consist of access devices.

To build a location:

1. Go to the **> Clients > Locations** page.
2. Click the **Create Location** link.
3. In the **Create Location** form, construct a location to hold the clients with the desired number of attached displays. For example, the following figure creates a dual monitor location.



4. Click **Save**

You can create locations based on other client attributes, such as IP address, operating system, device type, etc.

Step 9: Assigning Policies to Users

The Connection Broker assigns policies to users based on the user's location and the attributes associated with their Active Directory account. By default, the Connection Broker uses the `memberOf` attribute. However, you can specify any other valid attribute.

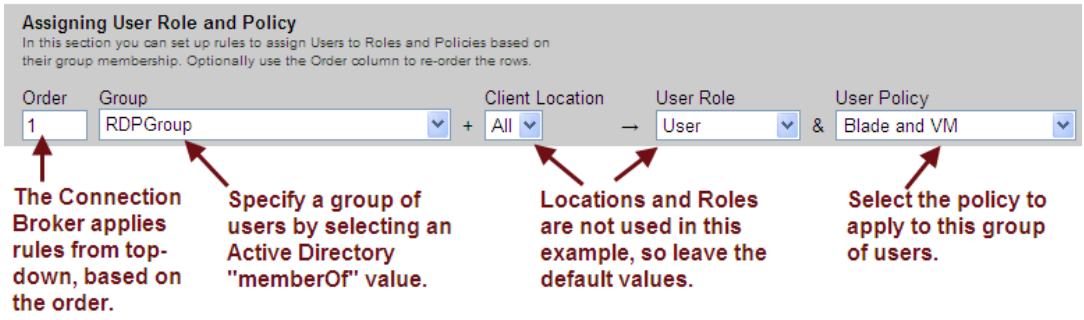
To assign policies to users

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

2. Use the **Assigning User Role and Policy** section, shown in the following figure, to assign policies to users based on the user's Active Directory membership.

The "Assigning User Role and Policy" section defines rules that determine how policies are assigned and, therefore, desktops are offered, to groups of users.

The format of the section is different depending on if you selected the "Query for group information" option when creating the authentication server. The format shown below assumes this option was selected.



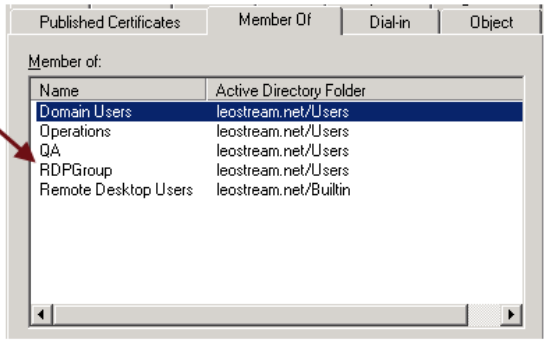
The Connection Broker applies rules from top-down, based on the order.

Specify a group of users by selecting an Active Directory "memberOf" value.

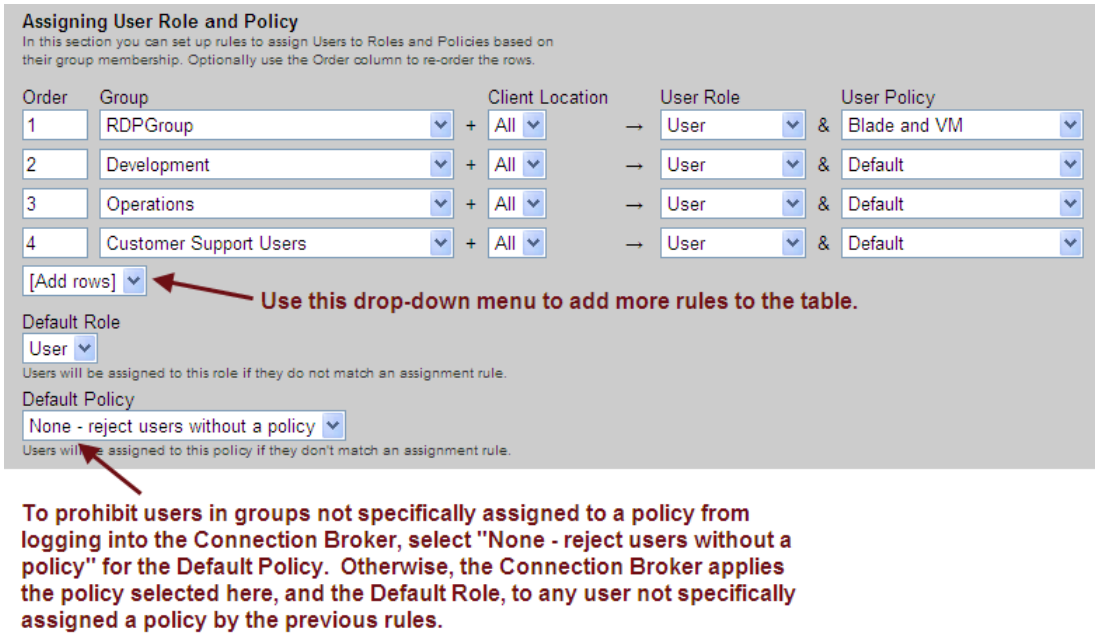
Locations and Roles are not used in this example, so leave the default values.

Select the policy to apply to this group of users.

The Connection Broker checks the user's memberOf attribute to determine if a particular policy should be assiged to that user. For example, this user is a member of the RDPGroup, so would be assigned the "Blade and VM" policy.



3. After all the rules are configured, set a default role and policy to apply to users that are not assigned a policy by one of the rules, as shown in the following figure.



4. Click **Save** to save any changes to the authentication server.

Step 10: Uploading Users

Note: If you are using policy to assign blades to users, skip step 10 and 11. These two steps show how to hard-assign desktops to users.

The Connection Broker automatically loads a user the first time that user signs into the broker. For hard-assignments, however, you must upload your end-users into the Connection Broker and indicate their hard-assigned blade

You can use the **Load user** option for your authentication server to load users, as follows.

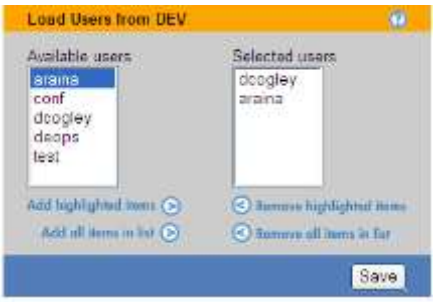
1. Select the **Load users** action for the appropriate authentication server on the **> Users > Authentication Servers** page, as shown in the following figure.

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

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.
- **Select from recently created users**: Enter a number indicating a number of 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**: Select the group to load users from. The Connection Broker displays only users in this group. This option appears only if the authentication server has the **Query for group information** option selected.
- **Select from all the users**: Select this option to select from all users in the authentication server.

3. Click **Next >**.
4. In the dialog that opens, shown in the following figure, select which users in this group to import from the **Available users** list at the left.



5. Click the **Add highlighted items** link to add the users to the **Selected users** list.
6. Click **Save**.

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

Step 11: Hard-Assigning Desktops

If you have a small number of blades, you can hard-assign those blades to users by going to the **Edit Desktop** page for each blade and manually switching the **Assignment mode** to **Hard-assigned to specific user**. After switching the mode, you then enter the user's login name into the **Assigned user** field.

If you have a large number of blades, it is easier to create a CSV file that describes your hard-assignments, and upload that file into the Connection Broker, as follows.

1. After the users are loaded, in Internet Explorer, use the following Web Query command to retrieve the Connection Broker `id` for your users.

   `http://cb_address/qselect.iqy`

   Where *`cb_address`* is your Connection Broker address.

2. When the query runs, enter your Connection Broker Administrator username and password, and query for the `user` table.

3. Using the results of the query, create a CSV-file that contains the following columns:

   `name,user_assignment_mode,user_id`

   Where:
   - `name` is the desktop name shown in the **Name** column of the **> Resources > Desktops** page
   - `user_assignment_mode` is `H`
   - `user_id` is the user's ID returned from the Web query.

   Each row in the CSV-file should contain the name of one of the blades and the user ID of the user to assign to that blade. The H indicates the assignment is hard-based. For example:

   ```
   name,user_assignment_mode,user_id
   win7-rgs,H,3
   xp-rgs,H,4
   ```

   Ensure that there are no spaces between entries.

4. After creating the file, go to the **> System > Maintenance** page.

5. Select the **Upload desktops** option near the bottom of the form.

6. Click **Next**.

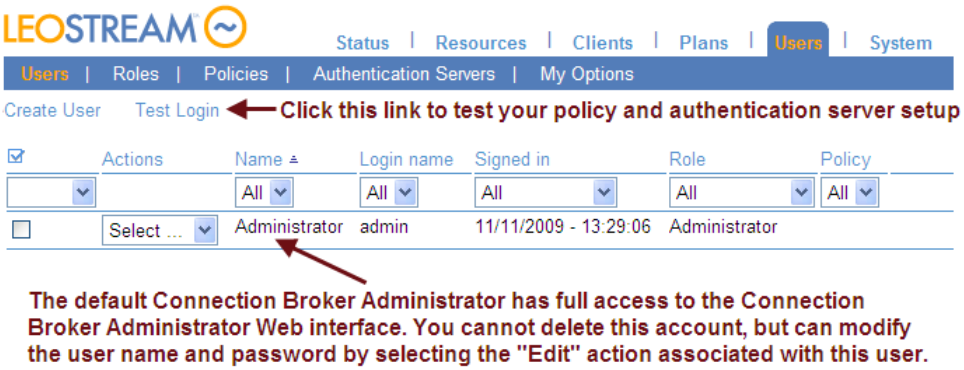
7. Enter the full path to your CSV file and click **Upload**.

The Connection Broker displays the progress of the file upload. After the upload completes, check the **Edit Desktop** page for a few of your blades to ensure that the upload ran to successfully.

Step 12: Testing a User Login

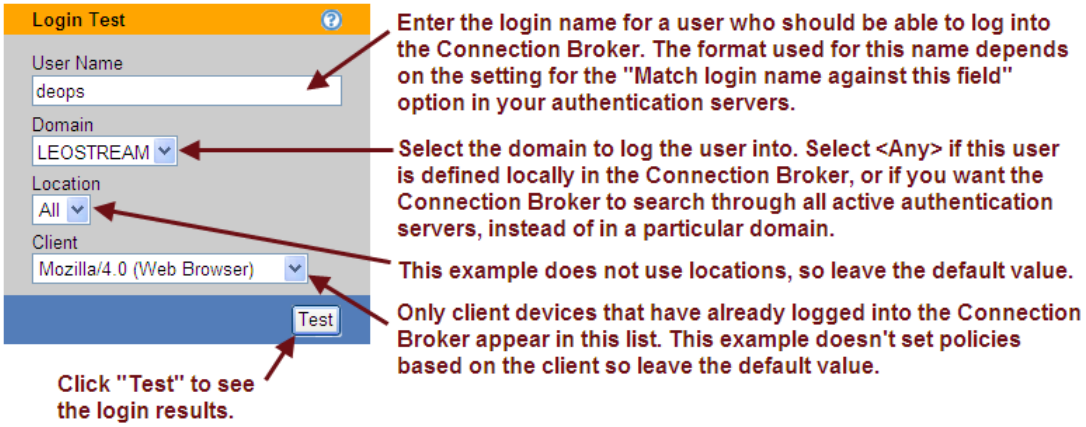
The following procedure allows you to test if your policies and authentication servers are correctly configured.

1. Go to the **> Users > Users** page, shown in the following figure.



2. Click the **Test Login** link, shown in the previous figure. The **Login Test** dialog opens.

3. Specify the test parameters, as shown in the following figure.



4. Click **Test** to display the results.