



Connection Broker

Where Virtual Desktops Meet Real Business

Clients Guide

Versions 6.x, 7.x
February 8, 2012

Contacting Leostream

Leostream Corporation
411 Waverley Oaks Rd.
Suite 316
Waltham, MA 02452
USA

<http://www.leostream.com>

Telephone: +1 781 890 2019

Fax: +1 781 688 9338

To submit an enhancement request, email features@leostream.com.

To request product information or inquire about our future direction, email sales@leostream.com.

Copyright

© Copyright 2002-2012 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 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.

Sun, Sun Microsystems, Sun Ray, and Java are trademarks or registered trademarks of Oracle and/or its affiliates. Linux is the registered trademark of Linus Torvalds in the U.S. and other countries. UNIX is a registered trademark of The Open Group. OpenLDAP is a trademark of The OpenLDAP Foundation. Microsoft, Active Directory, SQL Server, Excel, ActiveX, Hyper-V, Windows, and the Windows logo 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 products are patent pending.

Contents

CONTENTS	3
OVERVIEW	4
USING LEOSTREAM CONNECT IN THE WINDOWS SHELL	4
10ZIG THIN CLIENTS	4
APPLE IPAD AND IPHONES AS CLIENT DEVICES	5
CRANBERRY THIN CLIENTS	6
PRAIM® BY COMPUMASTER THIN CLIENTS	6
DEVON IT DETOS THIN CLIENTS	7
IGEL® THIN CLIENTS	9
IGEL® LINUX® THIN CLIENTS	9
<i>Initial Setup</i>	9
<i>Smart Card Setup</i>	10
<i>Integrating the IGEL Thin Client with a Cisco® Firewall</i>	12
IGEL® MICROSOFT® WINDOWS® CE THIN CLIENTS	13
<i>Initial Setup</i>	13
HP® THIN CLIENTS	14
INSTALLING LEOSTREAM CONNECT	14
REMOTE PROTOCOL SELECTION FOR HP THIN CLIENTS.....	14
HP COMPAQ THINCONNECT THIN CLIENTS.....	15
HP SAM CLIENTS.....	15
HP/NEOWARE™ LINUX® THIN CLIENTS	17
ORACLE SUN RAY™ THIN CLIENTS	19
OVERVIEW.....	19
SUN RAY SERVER SETUP	20
CONNECTION BROKER SETTINGS.....	21
TERADICI® PC-OVER-IP® HARDWARE CLIENTS	23
VMWARE VIEW CLIENTS	24
WYSE® THIN CLIENTS	25
OVERVIEW.....	25
SPECIFYING WNOS.INI VARIABLES	25
PROTOCOL PLANS FOR WYSE WTOS THIN CLIENTS	26
USING SMART CARDS WITH THE WYSE® WTOS THIN CLIENT.....	27
ADDING THE LEOSTREAM SSL CERTIFICATE TO THE WYSE® WTOS THIN CLIENT.....	27
WYSE® WTOS PRINTER REDIRECTION	27
WYSE® XPE THIN CLIENTS.....	28
WYSE TCX SOFTWARE SUPPORT.....	28
WYSE VIRTUAL DESKTOP ACCELERATOR (VDA) SUPPORT.....	28

Overview

This document describes how to configure various client devices to communicate with the Leostream Connection Broker. Certain thin clients, such as those from 10ZiG, Praim/Compumaster, DevonIT, IGEL, IRIS, HP and Wyse, provide built-in integration with the Leostream Connection Broker.

If you have a thin client that does not provide built-in Leostream support and is running a Linux operating system, a full Microsoft® Windows® operating system, or a Windows XPe operating system, you can integrate with the Leostream Connection Broker by installing Leostream Connect on the thin client. See the [Leostream Installation Guide](#) for more information.



VMware View integration requires an installed VMware View Client *and* Leostream Connect client on the Windows client device.

Using Leostream Connect in the Windows Shell

On any client device running a Windows operating system, you can configure Leostream Connect to run in *shell mode*. In this mode Leostream Connect replaces `explorer.exe` as the system shell, and automatically launches its login dialog when the client device boots and the user logs in.

To install the Windows version of Leostream Connect in shell mode, or setup shell mode after installation, you must log into the client device using an administrator account with access to the client's registry keys. For the Java version of Leostream Connect, you can write a script that simulates shell mode.

Refer to the [Leostream Connect Administrator's Guide and End User's Manual](#) for instructions on configuring the client to run Leostream Connect as the shell.

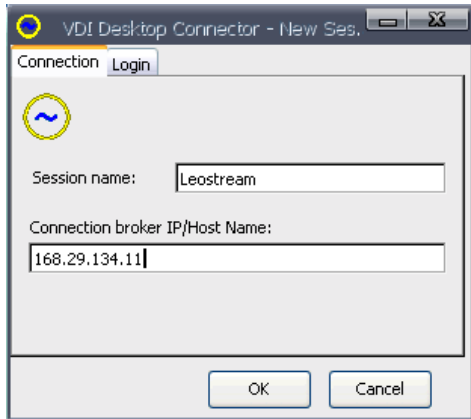
10ZiG Thin Clients

10ZiG Linux and Win CE thin clients provide built-in support for the Leostream Connection Broker. To obtain Connection Broker support for a 10ZiG XPe thin client, contact 10ZiG at info@10zig.com.

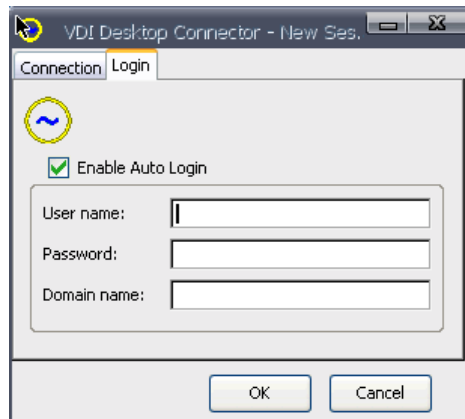
You must have a certificate installed in your Connection Broker if your 10ZiG clients use SSL to communicate with the Connection Broker. Use the Connection Broker > **System** > **Maintenance** page to generate and install a self-signed SSL certificate, if you do not have a third-party certificate.

Configure your 10ZiG thin client to establish Leostream connections, as follows:

1. Open the 10ZiG **Connections Manager** dialog.
2. Go to the **Configuration** tab.
3. Click the **Add** button. The **New Connection** dialog opens.
4. In the **New Connection** dialog, select **Leostream Connection Broker** in the **Choose new connection type** list.
5. Click **OK** to close the **New Connection** dialog.
6. In the **VDI- Desktop Connector - New Session** dialog, enter a name to display for the connection into the **Session name** edit field.
7. Enter the IP address or host name of your Connection Broker into the **Connection broker IP/Host Name** edit field. The following figure shows an example of the **New Session** dialog.



8. To configure the connection to automatically log into the Connection Broker when you open the connection, go to the **Login** tab.
 - a. In the **Login** tab, select the **Enable Auto Login** checkbox to enable the remaining controls on this tab, as shown in the following figure.



- b. Enter the **User name**, **Password**, and **Domain name** to use for the connection.
9. Click **OK**.

Please, see the [Configuration Guide](#) for your 10ZiG thin client for more information on setting the Leostream connection, such as configuring **Startup Options**.



If you are using a 10ZiG client running a Linux operating system to connect to Windows remote desktops, ensure that the protocol plan associated with the remote desktops assigns rdesktop a higher priority than RDP. See "Chapter 10: Building Pool-Based Plans" in the [Connection Broker Administrator's Guide](#) for more information on defining protocol plans.

Apple iPad and iPhones as Client Devices

Connection Broker 7.x allows users to access their Windows and Linux desktops from an Apple iPad and iPhone mobile device using the iTap RDP client and iTap VNC clients developed by HLW Software Development GmbH. To configure an iPad or iPhone to connect to Leostream, download and install the iTap RDP and/or iTap VNC clients from the Apple App store.

<http://itunes.apple.com/us/app/itap-rdp-client-remote-desktop/id317062064?mt=8>

<http://itunes.apple.com/us/app/itap-vnc-client-remote-desktop/id345580433?mt=8>



If a user requires RDP and VNC connections, they must install both iTap clients. Each client requires a separate Connection Broker login.

The Connection Broker uses the **iPhone and iPad Devices Connecting with iTap** section of the protocol plan, shown in the following figure, to configure connections through the iTap clients.

The screenshot shows a configuration window titled "iPhone and iPad Devices Connecting with iTap". It contains two main sections: "RDP" and "VNC". Each section has a "Priority" dropdown menu and a "Configuration file" text area. The RDP section has a priority of 1, and the VNC section has a priority of 2. The configuration file areas are currently empty.

For a description of the parameters supported in the iTap RDP and iTap VNC configuration files, see the iTap documentation:

- iTap RDP: <http://itap-mobile.com/itap-rdp/manual>
- iTap VNC: <http://itap-mobile.com/itap-vnc/manual>

By default, the user is allowed to connect from a mobile device. To prohibit users from connecting via mobile devices, change the **Priority** menus in this section to **Do not use**.

See the article "How do I access my desktops from an Apple iPad or iPhone?" on the [Leostream Knowledge Center](#) for a more detailed tutorial.

Cranberry Thin Clients

Please refer to the user's manual for your Cranberry thin client for information on configuring your client to work with the Leostream Connection Broker

Praim® by CompuMaster Thin Clients

Please refer to the user's manual for your Praim® thin client for information on configuring your client to work with the Leostream Connection Broker.

Devon IT DeTOS Thin Clients

Devon IT thin clients running the Devon Terminal Operating System (DeTOS) provide a built-in Leostream Connection Broker client. For more information on DeTOS, go to:

<http://www.devonit.com/software/detos/overview>

To setup the thin client to communicate with your Connection Broker:

1. On the thin client, select **System > Setup > Display**. The window shown in the following figure opens.

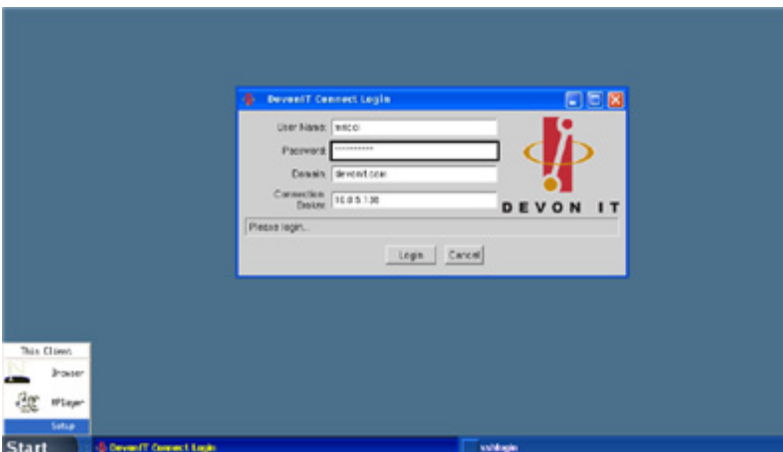


2. Set the color depth to the same setting as specified in the RDP configuration file used by the Connection Broker interface, typically 24-bit.
3. Click the checkbox **Don't Show Launcher**.
4. The **Save Settings**.
5. Add the Leostream option to the list of connections by going to the **Terminal** page on the **Setup** dialog.
6. Click **Add**.
7. In the dialog that opens, double-click on the **Leostream** entry. The dialog shown in the following figure opens.



8. In the **Session Name** edit field, enter a label for this connection.
9. Optionally, enter the default values for **Username**, **Password**, **Domain**, and **Connection Broker**.
10. Select the **Autostart** option. This option launches the **Login** window when the thin client boots up.
11. Optionally, select the **Restart** option. With this option enabled, the **Login** window automatically reopens if the user clicks **Cancel** or closes the **Login** window.
12. Click **OK**.
13. Click **Save Settings**.
14. Click **Quit Setup**.
15. Reboot the thin client.

Once the thin client has rebooted, you see the Leostream log-on screen, shown in the following figure.



When the user clicks **Login**, if the Connection Broker assigns the user a single desktop, it automatically launches that desktop. If the Connection Broker offers more than one desktop, a list of desktops is shown and the user can connect to one or more desktops.

IGEL® Thin Clients

The Leostream client runs as a session inside of IGEL thin clients running Linux and Windows operating systems. When the Leostream session is running, it takes full control of the IGEL session.

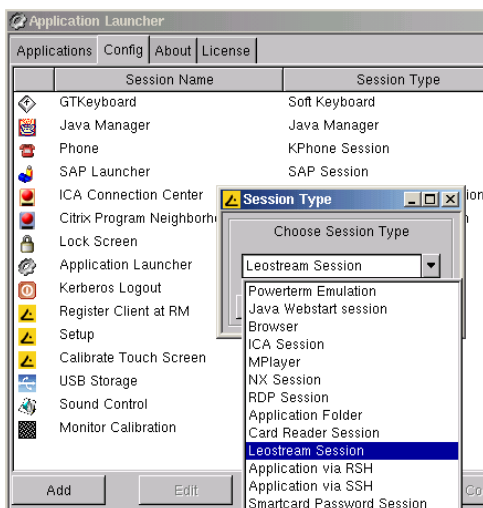
✓ Because the Leostream session takes full control of the IGEL session, dialogs for other sessions appear behind the Leostream session. For example, if you enable the **Request User Permission for Shadowing** feature on the IGEL thin client, the permission request appears behind the Leostream session. In these cases, you must disable the **Request User Permission** option for the particular session.

IGEL® Linux® Thin Clients

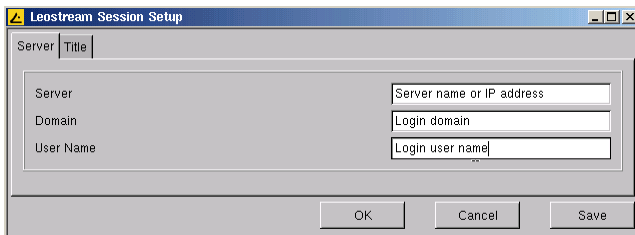
Initial Setup

To use IGEL thin clients with the Leostream Connection Broker, you must add a **Leostream Session** to each thin client. Add the session, as follows:

1. Boot the IGEL thin client. After the client boots, the **Application Launcher** opens.
2. Select the **Config** tab.
3. Press the **Add** button. The **Session Type** dialog opens.
4. Select **Leostream Session** from the **Choose Session Type** drop-down menu, as shown in the following figure.

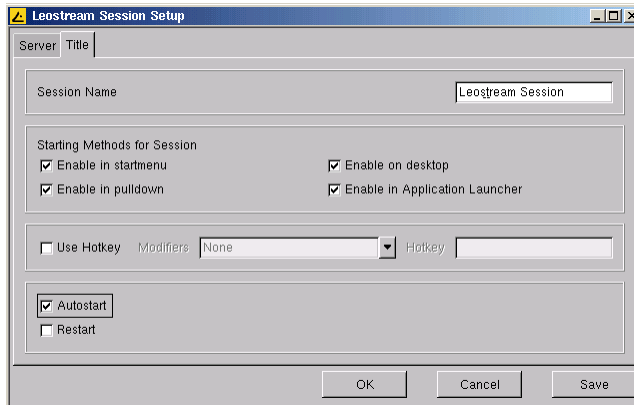


5. Click **Ok**. The **Leostream Session Setup**, shown in the following figure, opens.



6. In the **Server** tab, enter the IP address of the Connection Broker in the **Server** edit field.

7. Optionally, add the user's domain and user name in the **Domain** and **User Name** edit fields, respectively.
8. Click on the **Title** tab, shown in the following figure.



9. Enter a new name for the session in the **Session Name**, if necessary
10. Select options in the **Starting Methods for Session** section to add methods for starting Leostream Connect from:
 - The start menu
 - The menu that opens when you right-click on the desktop
 - A desktop icon
 - The **Applications** list in the **Application Launcher**
11. To automatically launch the Leostream session when the thin client starts, select the **Autostart** option.
12. To restart the session after the client is disconnected, select the **Restart** option.
13. Click **OK**.
14. In the warning dialog that opens, click **Yes** to add the session. This session overwrites any previous session with the same name.

See the **Service and Support** section of the IGEL Web site for complete set of manuals and guides for IGEL thin clients.

Smart Card Setup

After you add a Leostream Session to your IGEL client, you can setup the client to accept smart cards. The following figure shows an example smart card.



IGEL smart cards store the session variables within the user's smart card. When the user inserts the smart card into the smart card reader on the IGEL thin client, the thin client reads the session data from the card and launches the relevant session.

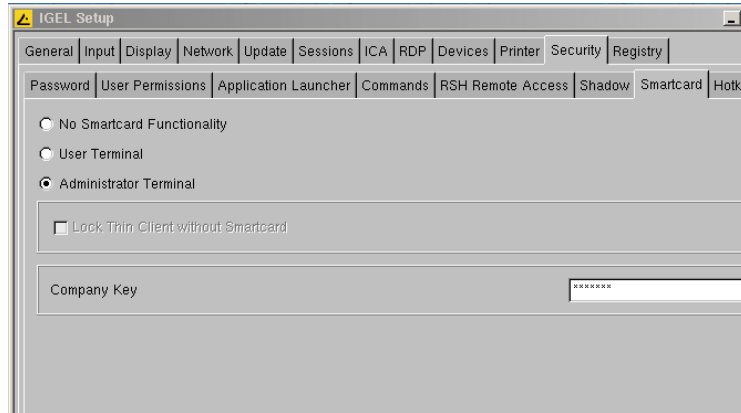
You can use IGEL thin clients with Java™ smart cards used in conjunction with AET **SafeSign Identity Client**® software. Use the following link for more information:

www.aeteurope.nl/aet/aet-europe/_www/files/pdf1/SOL200802IgeILEN01.pdf

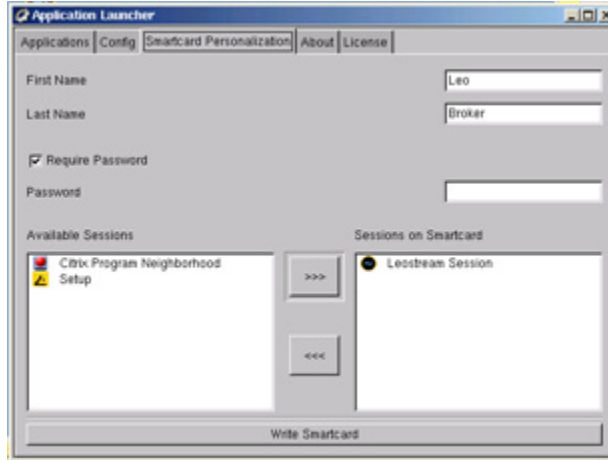
Writing Smart Cards

Write the Leostream Session to the smart card, as follows:

1. Put the thin client into Administrator mode:
 - a. Select **Setup** from the IGEL thin client's **Start** menu. The **IGEL Setup** dialog opens.
 - b. Select **Security** from the top level tabs.
 - c. Select **Smartcard** from the set of tabs inside the **Security** section, as shown in the following figure. Note that your client may not contain exactly the same set of tabs.



- d. Select the **Administrator Terminal** radio button.
 - e. Click **OK**. The client reboots.
2. After the thin client reboots, a **Smartcard Personalization** tab appears on the **Application Launcher**. Click the **Smartcard Personalization** tab.
3. Enter the first and last name of the user for this card, in the **First Name** and **Last Name** edit fields, respectively.
4. To require the user to enter a password when they insert their smart card, select **Require Password**.
5. Enter the user's password in the **Password** edit field.
6. Select the sessions to add to this smart card in the **Available Sessions** list.
7. Click the **>>>** button to add these sessions into the **Sessions on Smartcard** list. Your dialog now looks something like the following:



8. Click **Write Smartcard**.
9. Click **OK** in the warning dialog that appears.

The thin client writes the smart card and indicates any problems that occur. Contact IGEL for any issues with writing smart cards.

Enabling Smart Card Support

Once the smart card is written, place the thin client into User Terminal mode, as follows.

1. Select **Setup** from the IGEL thin client's **Start** menu. The **IGEL Setup** dialog opens.
2. Select **Security** from the top level tabs.
3. Select **Smartcard** from the set of tabs inside the **Security** section.
4. Select the **User Terminal** radio button.
5. Click **OK**. The client reboots.

Now, when the user inserts their smart card, the client automatically launches their sessions and prompts the user for their password. The client disconnects all sessions when the user removes the smart card. If the user inserts the smart card in a different thin client, the client reconnects to the user's sessions.

See the **Service and Support** section of the IGEL Web site for complete set of manuals and guides for IGEL thin clients.

Integrating the IGEL Thin Client with a Cisco® Firewall

The IGEL thin client can be setup to connect to a remote Cisco® firewall, authenticate, and connect to the corporate network. This enables home users to be sent home with just a thin client, and be able to connect securely to the corporate network by plugging the thin client into their broadband connection.

To setup this functionality:

1. Open the IGEL setup screen
2. Select the **Network** tab
3. Click on **Advanced Network Settings**
4. Select the **Cisco VPN** tab

You can then define a profile and select the authentication method. If you want to install a digital certificate on the thin client, you need to generate a CSR request file by going to the **Certificates** page, selecting the **Enrollment mode**, and clicking **Enroll**. You then must complete the CSR request and send the resulting document to the certificate authority.

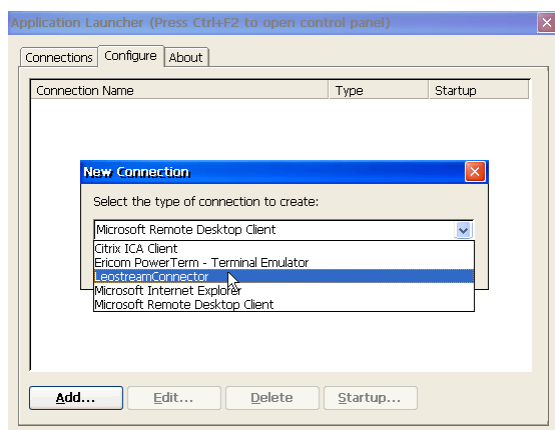
Once setup, the thin client automatically connects to the Cisco VPN and, once the user is authenticated, connects the user to the remote desktop session.

IGEL® Microsoft® Windows® CE Thin Clients

Initial Setup

To use IGEL thin clients with the Leostream Connection Broker, you must add a **Leostream Session** to each thin client. Add the session, as follows:

1. Boot the IGEL thin client. After the client boots, the **Application Launcher** opens.
2. Select the **Configure** tab.
3. Click the **Add** button. The **New Connection** dialog opens.
4. Select `LeostreamConnector` from the **drop-down** menu, as shown in the following figure.



5. Click **OK**. The **Leostream Configuration** dialog opens, shown in the following figure.



6. Enter a new name for the connection in the **Connection Name** edit field.
7. Enter the user name and password for the user connecting to this session, in the **User** and **Password** fields.
8. Enter the user's domain in the **Domain** edit field.
9. Enter the IP address or FQDN of your Connection Broker in the **Server Name** edit field.
10. To hard assign this client to a desktop, enter the desktop's name in the **Machine name** edit field. If this field is empty all available machines are displayed when the user runs the session.
11. Click **OK**.

IGEL Microsoft Windows CE thin clients do not currently support USB redirection or smart cards.

HP® Thin Clients

For information on installing the Java version of Leostream Connect on HP gt7725 thin client, see the article “How do I install Leostream Connect on an HP gt7725 Thin Client?” in the [Leostream Knowledge Center](#).

Installing Leostream Connect

Some HP thin clients include a native Leostream client. For thin clients that do not include a Leostream component, you can install the Leostream Connect software client.

- To access the Leostream Connection Broker from an HP client running Microsoft Windows XPe, install the windows version of the Leostream Connect client.
- To access the Leostream Connection Broker from an HP client running a version of a Linux operating system, install the Java version of the Leostream Connect client.

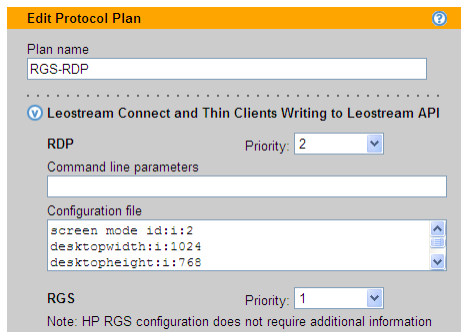
When you install the Java version of Leostream Connect, the client creates a client ID, which it sends to the Connection Broker when a user logs in from the thin client. The Connection Broker uses the client ID to uniquely identify different physical client devices.

If you clone your thin clients from a standard image that includes a Leostream Connect installation, you may create multiple unique physical devices with the same client UUID. The replicated client identifiers cause the Connection Broker to incorrectly inventory your client devices.

To avoid this problem, delete the `.clientuuid` file found inside the Leostream Connect installation directory on the image used to build your thin clients.

Remote Protocol Selection for HP Thin Clients

Many HP thin client support HP RGS and RDP connections to the remote desktop. Configure the protocol plan associated with the desktop to determine which of these protocols has the highest priority. For example, the protocol plan in the following figure assigns the highest priority to RGS.



When the user logs in to a desktop that is assigned the previous protocol plan, the Connection Broker first checks if the RGS port is open on the remote desktop. If the RGS port is open, the Connection Broker connects to the desktop using RGS. If the RGS port is not open, the Connection Broker next checks the RDP port and, if available, connects to the desktop using RDP.

Not all HP thin clients provide the functionality to encrypt passwords when establishing RDP connections. If you are using RDP to connect to a desktop from an HP thin client and are receiving errors, replace the following line in the RDP **Configuration file** field:

```
password 51:b:{RDP_PASSWORD}
```

With

```
password:s:{PLAIN_PASSWORD}
```

Typically, you must make this substitution on client devices that provide a custom Leostream client , instead of using Leostream Connect.

HP Compaq ThinConnect Thin Clients

Configure HP Compaq ThinConnect clients to communicate with the Leostream Connection Broker, as follows.

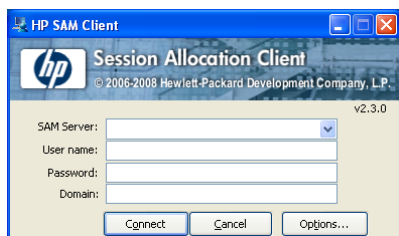
1. Ensure that you are running the device image S1ST0032, or higher.
2. Boot the thin client.
3. On the dialog that appears when the client finishes booting, click the **Settings** button.
4. Select the **Security** or **Thin Client** tab, depending on the device image you are running
5. Choose **Leostream** from the **Thin Client State** drop-down menu.
6. Click **Save**.

After you have saved the thin client state, restart the client. When the login prompt appears, enter the username, password, domain, and IP address of your Connection Broker.

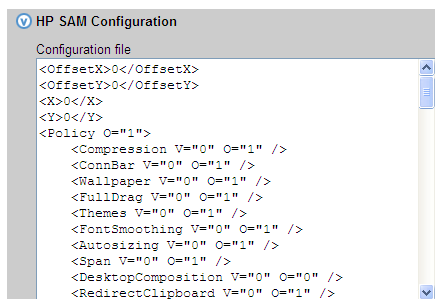
For more documentation on HP Compaq Thin Clients, see the [HP Web site](#).

HP SAM Clients

To connect to your Leostream Connection Broker from an HP SAM client device, enter your Connection Broker IP address or DNS name into the **SAM Server** field on the **HP SAM Client** dialog, shown in the following figure.



To configure the remote viewer session that is launched from the HP SAM client, edit the protocol plan associated with the desktops that are launched from the SAM client and scroll down to the **HP SAM Configuration** section, shown in the following figure.



Enter the **Configuration file** in XML-format. The parameters in this file map to individual controls on the SAM client's **Options** user interface.

Understanding the Configuration File

The configuration file allows you to customize the end user's experience when they log into the Connection Broker using an HP SAM client. The parameters set in this file are similar to those set in the Global Policy in the HP Session Allocation Manager Web interface.


The parameters within the `<Policy>` section pertain to RGS and RDP connections. The parameters inside the `<DynamicPolicy>` tags pertain specifically to RGS.

Use the following format to specify parameters in the `<Policy>` section:

```
<Span V="0" O="1" />
```

Where the string equated to `V` is the value to assign to that parameter. The string equated to `O` indicates if the end user can override the policy setting using the options on the SAM client.

- `O="1"` indicates that the setting on the SAM client overrides the policy setting.
- `O="0"` indicates that the SAM client cannot override the policy setting.

 By default, the HP SAM configuration file allows the user to override the policy settings. Ensure that you switch the override values to zero to hard-code the behavior.

Use the following format to specify RGS Receiver parameters in the `<DynamicPolicy>` tags.

```
<DynamicPolicy>Rgreceiver.IsMatchReceiverResolutionEnabled =value</DynamicPolicy>
```

Where `value` can be any of the following:

- No value: Leave the tag empty to not specify this parameter
- 1: To enable this setting
- 0: To disable this setting

By default, the RGS Receiver parameters can be modified by the client device. To hard-code the policy behavior, add an `isMutable` tag for each RGS Receiver property to hard-code. For example, to ensure the end user cannot turn off the RGS feature to match the client device resolutions, add the following line to the configuration file.

```
<DynamicPolicy>Rgreceiver.IsMatchReceiverResolutionEnabled.IsMutable=0</DynamicPolicy>
```

Configuring HP SAM for Multi-Monitor Support

The default HP SAM configuration file does not provide multi-monitor support. To provide multi-monitor support:

1. Modify the `Span` and `Display` settings in the `<Policy>` section, as follows:

```
<Span "V=1" O="0" />  
<Display FS="1" X="-1" Y="-1" Depth="-1" Stretch="0" O="0" />
```

2. Add the following lines to the `<DynamicPolicy>` section.

```
<DynamicPolicy>Rgreceiver.IsMatchReceiverResolutionEnabled.IsMutable=0</DynamicPolicy>  
<DynamicPolicy>Rgreceiver.IsMatchReceiverResolutionEnabled=1</DynamicPolicy>  
<DynamicPolicy>Rgreceiver.IsMatchReceiverPhysicalDisplaysEnabled.IsMutable=0</DynamicPolicy>  
<DynamicPolicy>Rgreceiver.IsMatchReceiverPhysicalDisplaysEnabled=1</DynamicPolicy>
```

3. If your RGS session opens with borders, ensure the `IsBordersEnabled` parameter is set to zero:

```
<DynamicPolicy>Rgreceiver.IsBordersEnabled=0</DynamicPolicy>
```

Policy Options for HP SAM

For users connecting to and from Windows machines, you can control the time zone of the remote desktop, using the **Adjust time zone on the destination to match client when user logs in** policy option. If the user's policy selects this option, the Connection Broker changes the time zone of the desktop the user logs into to the same time zone as on the client device they log in from.

HP/Neoware™ Linux® Thin Clients



Neoware thin client software and devices are now available and support by HP. Read the [announcement](#) for more information.

In order to communicate with the Leostream Connection Broker, you must install the Leostream snap-in into your Neoware Linux thin clients. To obtain the Leostream snap-in for Neoware thin clients, contact Leostream support.

To add the Leostream snap-in to a Neoware Linux thin client, first download the Neoware **ezRemote™ Manager** client software. Install and run the ezRemote Manager on a Microsoft Windows desktop machine that shares a subnet with the thin client devices. The ezRemote Manager discovers the Neoware thin clients, and displays a list.

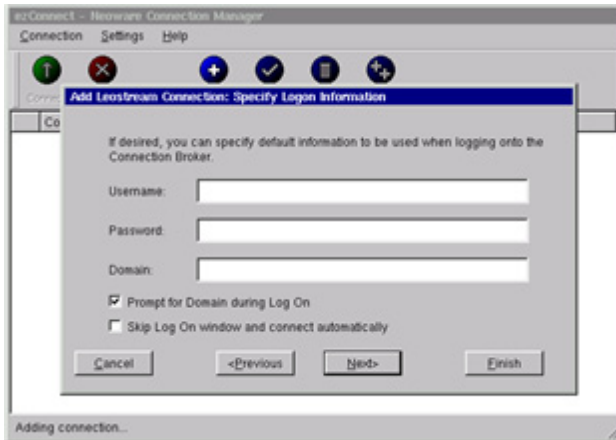
Select the relevant thin clients and choose > **Actions > Snap-in** option. When prompted, select the Leostream snap-in software and click **OK**.

To complete the configuration of each thin client:

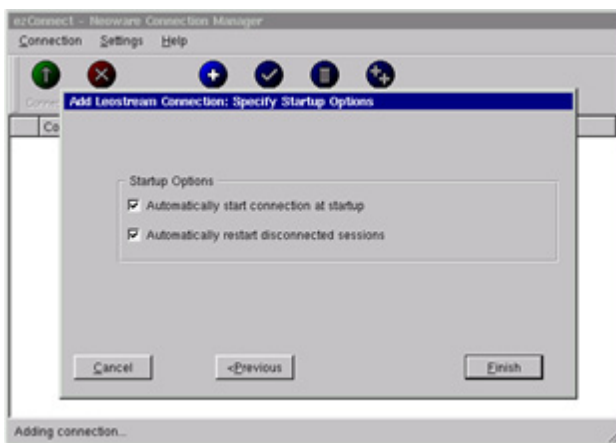
1. Enable shadowing using the desktop configuration > **Settings > Appliance Properties > Desktop Shadow** tab.
2. Connect to the thin client.
3. Click **Add Connection**.
4. Select the type of connection as **Leostream VDI Connection Broker**, as shown in the following figure.



5. Click **OK**.
6. On the dialog that opens, shown in the following figure, optionally enter any default information such as username, password, and domain.

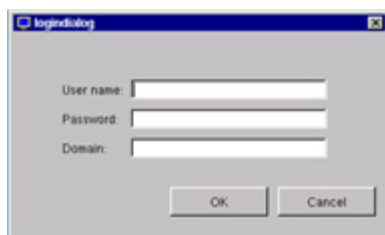


7. For **Startup Options**, select **Automatically start connection at startup**, as shown in the following figure.



8. Click **Finish**.

After the configuration is completed, the thin client displays a blue screen with the log on dialog shown in the following figure.



To subsequently change the configuration, connect to the thin client via the ezRemote Manager.

Once the thin client is working as desired, you can clone the configuration using the ezRemote Manager, as follows.

1. Select the configured appliance.
2. Go to the **> Actions > Properties** page.
3. Click the **Get properties from thin client appliance from list on the left** button, which imports the configurations into the Manager where they can be saved.

To propagate this configuration to other thin clients:

1. Go to the > **Actions** > **Properties** page.
2. Click **Get properties from file**.
3. Select the relevant file and propagate it using the **Update All** button.

Oracle Sun Ray™ Thin Clients

Overview

A typical Oracle Sun Ray™ architecture consists of Sun Ray thin clients, Solaris or Linux running the Sun Ray Server Software (SRSS), and virtual machines hosted on VMware® ESX servers managed by VMware vCenter Server. For an overview of the Sun Ray system, see the **Sun Ray** white papers provided by Oracle.

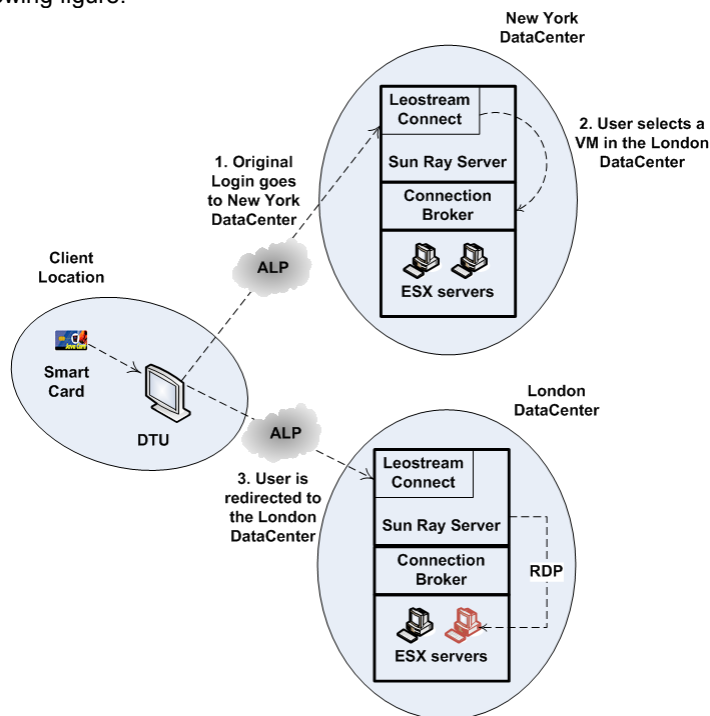
Typically, your system is set up in chassis of blades.

- Most of the blades run ESX Servers connected to the SAN, which host your virtual machines.

The virtual machines may or may not be located in one or more clusters in vCenter Server. A *cluster* is a set of two or more ESX servers coupled together so that the virtual machines can be moved between the hosts. A cluster can be divided into a number of *resource pools* that limit the amount of resources virtual machines can consume.

- Some of the blades run Sun Ray Servers. To reduce network latency, the Sun Ray Server needs to be as physically close as possible to the virtual machines.

The communication between the end user, the Sun Ray server, and their virtual machines occurs in stages, as depicted by the following figure.



The steps in the user's login process are as follows.

1. To log in, a user optionally inserts their smart card into the Sun Ray desk top unit (DTU). Each smart card has a unique token.
2. The DTU reads the card and sends the token to the SRSS. Leostream Connect stores the token in the Connection Broker database, however it does not use the token to identify or authenticate the user. The user must enter their authentication credentials (username and password) into Leostream Connect. The DTU and SRSS communicate using the highly efficient Oracle Appliance Link Protocol™ (ALP), which has higher performance than RDP for multi-media rich traffic. The SRSS establishes a non-root user X-session for each DTU that logs in. This X-session is a stepping stone for the final connection to the user's desktop. By minimizing the resources used by the X-session, you can maximize the number of logins per Sun Ray server.
3. Leostream Connect passes the user credentials to the Connection Broker, which looks up the user in the authentication server, determines which policy to apply, and offers desktops.
4. Using Leostream Connect, the user selects which desktop to log in to. Leostream Connect passes this information to the Connection Broker.
5. The Connection Broker sends Leostream Connect the list of Sun Ray hosts associated with the vCenter Server cluster in which the selected desktop resides. If the selected desktop is not part of a cluster, the Connection Broker sends the Sun Ray hosts associated with virtual machines not in a cluster. See step 3 in **Connection Broker Settings** for more information.
6. Leostream Connect determines if a switch is needed and, if so, picks a random Sun Ray server from the list and redirects the DTU to this host. If a switch is required, the user is automatically logged into the Leostream Connect on the new host and an RDP session to their selected desktop appears.

If the user selected the option to restart their desktops before connecting, Leostream Connect restarts all desktops before redirecting the user to the new Sun Ray server. See the [Leostream Connect Administrator's Guide and End User's Manual](#) for information on allowing users to restart their desktops.

The client launches one or more RDP sessions using the **Sun Ray Connector for Windows**. Using this setup, the high-latency link to the SRSS is traversed using ALP and the low latency link between the SRSS server and the desktop is crossed using RDP, with the SRSS server acting as a proxy. In the end, each user has their own DTU connected to a Sun Ray server, and the Sun Ray Connector for Windows connects them to a desktop using the RDP protocol.

To accomplish this, you associate the SRSS server with the desktop via clusters rather than with the particular DTU Sun Ray client. The Sun Ray Client uses the local SRSS server to boot and for its initial configuration, then relies on Leostream Connect to redirect to the SRSS physically closest to the desktop.



When the user removes their smart card, the Connection Broker disconnects them from their desktops. A new session starts when the user reinserts their card.

Sun Ray Server Setup

Before you begin, install your Connection Broker and note its IP address. Then, to set up your Sun Ray Server host:

1. Log into the Sun Ray Server host using the root account.
2. Ensure that a 32-bit Java Run Time Environment (JRE) version 1.6 or higher is installed. Although Leostream Connect requires only JRE version 1.5 or higher, the Leostream Agent requires version 1.6.
3. Install the Sun Ray Terminal Services client `uttsc` on the Sun Ray Server and ensure that your Sun Ray connections are working properly.
4. Install the java version of Leostream Connect on your Sun Ray servers (see "Leostream Connect - Installing on Linux® Operating Systems" in the [Leostream Installation Guide](#)). If you have a previous installation of Leostream Connect, ensure that you install the new version in the same directory as the existing installation.

Ensure that you select the **SunRayAgent** task when installing Leostream Connect.

5. Install the java version of the Leostream Agent on your Sun Ray servers (see “Leostream Agent - Installing on Linux® Operating Systems” in the [Leostream Installation Guide](#)).

If you previously installed Leostream Agent 1.1, you will need to stop the service before installing a new version. On a Solaris operating system, use the following command to stop the Leostream Agent service:

```
svcadm disable -t leostreamagentd
```

Install the Leostream Agent into a different directory than Leostream Connect. Leostream Connect and the Leostream Agent share some common Leostream libraries in the `lib` directory inside of their installation directories. If you do not install Leostream Connect and the Leostream Agent in different directories, you will not be able to upgrade one of the components without upgrading the other component. If you install the client and agent in different directories, you can safely upgrade one component without upgrading the other.

The installer automatically uninstalls the Leostream Sun Ray Script (`leostreamd`), if it was previously installed.

The Leostream Agent listens locally on port 7730. By default, Leostream Connect communicates with the SRSS using port 7007.



Leostream Connect 1.5 and higher are configured to work together with Leostream Agent 1.x on Sun Ray servers. Older versions of Leostream Connect are not compatible with Leostream Agent 1.x when used in a Sun Ray session. If you must use an older version of Leostream Connect, contact support@leostream.com for the previous version of the Leostream Sun Ray Session scripts.

If you upgrade an existing SRSS to use Leostream Connect 1.5 or higher, you do not need to replace your Leostream Sun Ray Session scripts with the Leostream Agent. Leostream Connect first tries to communicate with the Leostream Agent. If version 1.x of the Leostream Agent is not installed, Leostream Connect uses the deprecated Leostream Sun Ray Session scripts.

Connection Broker Settings

Once your Sun Ray servers are configured, you can configure your Connection Broker, as follows.

1. On the Connection Broker > **System** > **Settings** page, scroll down to the **Leostream Connect Configuration** section and ensure that the **Use Device UUID to uniquely identify clients** option is selected.
2. Add a VMware vCenter Server (VMware VirtualCenter 2) center, as described in the “Chapter 5: Understanding Connection Broker Centers” in the [Connection Broker Administrator’s Guide](#).
3. If you have virtual machines that are not in a cluster and you want to redirect the user’s session to a particular Sun Ray host when they connect to one of these virtual machines, expand the **Sun Ray Details** section of the **Create Center** form. This section appears as shown in the following figure.

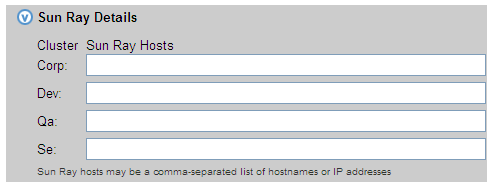



4. In the **Sun Ray hosts for virtual machines not in clusters** edit field, enter a comma separated list of host names or IP addresses for the Sun Ray servers physically closest to these virtual machines. If you enter multiple hosts, the Connection Broker randomly selects one host from the list.

If you leave this edit field blank, the Connection Broker does not do any redirection for virtual machines that are not in a cluster.

5. Save the center.


6. After the center finishes refreshing, if you have virtual machines in clusters, go to the **Edit Center** page for this vCenter Server center. Expand the **Sun Ray Details** section, an example of which is shown in the following figure. This section contains entries for each of your vCenter Server clusters.

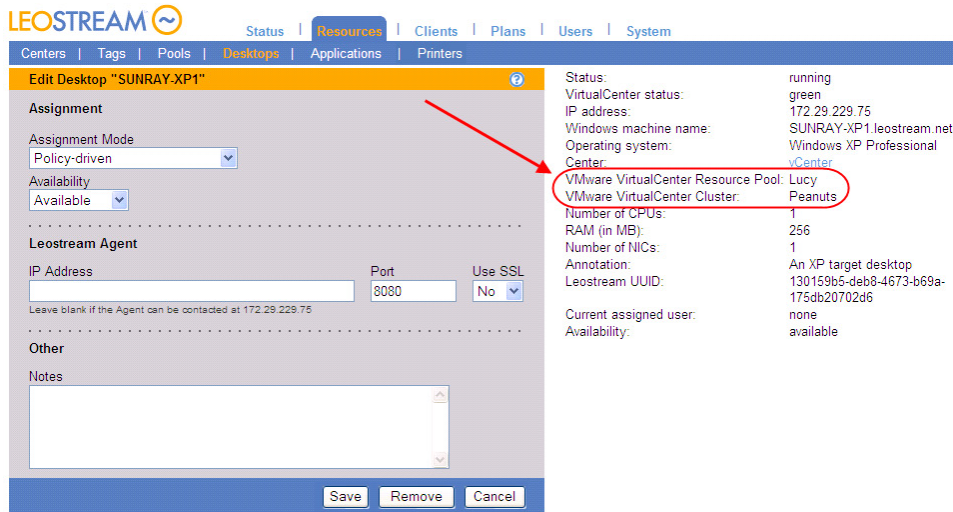


7. Enter the host name for the Sun Ray server physically closest to each vCenter Server cluster. You can enter multiple hosts as a comma separated list of either host names, IP addresses, or fully qualified domain names.
 If you are using the Sun High Availability system and SRSS failover groups, enter the IP address for the group, instead of for a single SRSS host.
 - If you leave an edit field blank, the Connection Broker does not do any redirection for virtual machines on this cluster.
 - If you enter multiple hosts, the Connection Broker randomly selects which host to redirect the user to.
8. Create a protocol plan for users logging in through Sun Ray DTUs.
9. In the **Leostream Connect and Thin Clients Writing to Leostream API** section of this protocol plan, select **Do not use** from the **Priority** drop-down menus for all protocols in this section.
10. In the **Leostream Connect and Thin Clients Writing to Leostream API** section, select **1** from the **Priority** drop-down menu in the **Sun Ray** sub-section.
11. Enter any changes in the **Command line parameters** field. The default command line parameters include the following:
 - `-u{USER}`: Specifies the user name.
 - `-i`: Indicates that the client must read the password from standard input, a requirement for single sign-on.
 - `-m`: Launches the remote desktop in full screen mode. This option is required when providing Leostream multi-monitor support to a user that logs into a desktop assigned to this protocol plan.
 - `-P port_number`: Indicates the port (*port_number*) to use for the RDP connection.
 - `-d`: The user's authentication domain. This is the name specified in the Connection Broker and must not contain any spaces. If your authentication server name contains any spaces, `uttsc` will not launch properly due to an unknown parameter.
 - `{IP}`: The IP address for machine.

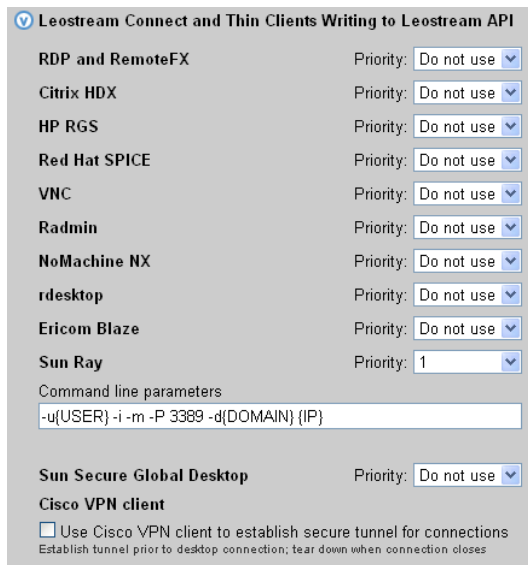
For a complete description of command line parameters for the `uttsc` command, refer to the `man` page. Typically, you can view the man page by invoking the following command.

```
man -M /opt/SUNuttsc/man uttsc
```

 You can use the right-hand side of the **> Resources > Desktops > Edit Desktop** page to view the vCenter Server resource pool and cluster associated with that desktop, as shown in the following figure.



The following figure shows an example of the **Leostream Connect and Thin Clients Writing to Leostream API** section of the protocol plan configured for use with Sun Ray environments.



Teradici® PC-over-IP® Hardware Clients

The Leostream Connection Broker provides native support for hardware-based PC-over-IP (PCoIP) client devices, such as those provided by Amulet Hotkey, DevonIT, and EVGA. For more information on configuring PCoIP clients, see “Chapter 17: PCoIP Setup and Configuration” in the Connection Broker Administrator’s Guide.

VMware View Clients

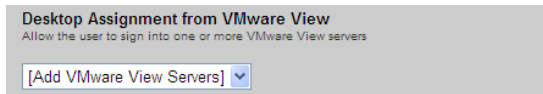
Connection Broker 7.0 allows you to offer VMware View sessions to users alongside other offered desktop and application from Leostream. Integrating VMware View with Leostream allows you to do the following.

- From a Leostream client, offer the user VMware View desktops and connect to these desktops using the software-based PCoIP protocol.
- Provide a single login portal for users with access to VMware View resources, as well as other resources such as virtual machines hosted in Microsoft Hyper-V or applications in a Citrix XenApp farm.
- Restrict a user's access to their VMware View resources, based on the location of the user's client.
- Seamlessly integrate the VMware View Client with the Cisco Systems VPN Client (see [Protocol Plans for Cisco Systems VPN Clients](#))

✓ The client device must have an installed VMware View client in order to launch the VMware View session. If you are using Leostream to manage USB devices, do not install the USB component of the VMware View client.

You can provide the user with login access to multiple VMware View Servers from a Leostream client. To configure the user's policy to provide VMware View access:

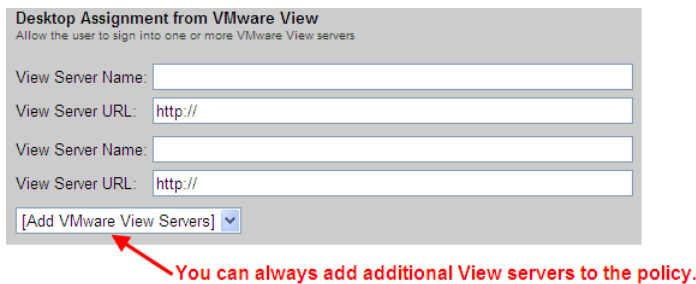
1. Go to the **Desktop Assignment from VMware View** section, shown in the following figure.



2. From the **Add VMware View Servers** drop-down menu, select the number of VMware View servers to allow the user to log in to using this policy. You can add an unlimited number of View servers to the policy, however you can add only three View servers, at a time, as shown in the following figure.

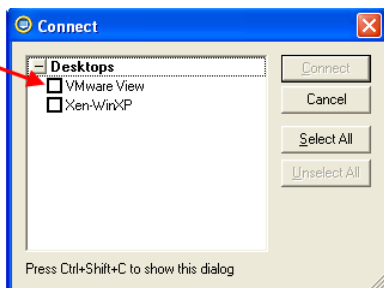


After adding the View servers, the **Desktop Assignment from VMware View** section appears as in the following figure. Use the **Add VMware View Servers** drop-down menu to add additional View servers.



3. In the **View Server Name** edit field, enter the name to display to the user for this VMware View connection server. For example, if `VMware View` is entered in the **View Server Name** edit field, Leostream Connect displays as follows.

Leostream Connect lists the View server using the string entered into the "View Server Name" edit field in the user's policy.



4. In the **View Server URL** edit field, enter the full URL to the View connection server.

When the user connects to a VMware View connection server, the Leostream Connection Broker signs the user into the View client using the same credentials used to log in to Leostream. After the user is logged in, the VMware View Manager controls which desktops are offered to the user and which display protocol is used to connect to those desktops.

See the [Leostream Connect Administrator's Manual and End User's Guide](#) for more information on using View in conjunction with Leostream.

Wyse® Thin Clients

Overview

The Wyse WTOS is a tied-down operating system that can run on a variety of Wyse Thin Clients. When the client boots, it accesses the Global and User configuration profile files from the Connection Broker by the `sysinit`, `signon`, `signoff`, and `shutdown` commands.

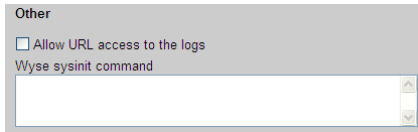
To setup the Connection Broker address on the Wyse thin client:

1. Click on the **Desktop** menu in the thin client task bar.
2. Select **System Setup**.
3. Select **Network**. The **Network Setup** dialog opens.
4. Select the **Server** tab.
5. In the **VDI Broker** edit field, enter your Connection Broker IP address.
6. Click **OK**.
7. To restart the client, click on the **Desktop** menu in the thin client task bar.
8. Select **Shutdown**.
9. In the dialog that opens, select **Shutdown and Restart the system**.
10. Click **OK**.

Specifying WNOS.INI Variables

When the thin client boots and successfully connects, the client sends the `sysinit` command to the Connection Broker. The Connection Broker responds by sending back the `wnos.ini` (global profile) file. If the file contains any variables, these variables over-ride any existing values.

Use the **> System > Settings** page to specify the `wnos.ini` variables that apply to all Wyse WTOS thin clients that connect to this Connection Broker. The following figure shows the **Wyse sysinit command** edit field, found at the bottom of the **> System > Settings** page.



If you plan to display desktops and applications to users using either the **Pool Name : Desktop Name** or **Pool Name : Windows Machine Name** policy option, ensure that you include the following parameter in the **Wyse sysinit command**:

```
LongApplicationName=yes
```

With `LongApplicationName` set to `yes`, the icons on the Wyse desktop display with 38 characters, instead of the default 19 characters.

After the thin client successfully receives the `wnos.ini` from the Connection Broker, a sign-on window prompts the user for username and password credentials.

The thin client then sends the `signon` command to the Connection Broker with the username and password as its parameter. If the sign on is successful, the Connection Broker sends back the `user.ini` (User profile) file, specified by the protocol plan assigned to the user's desktop by the user's policy.

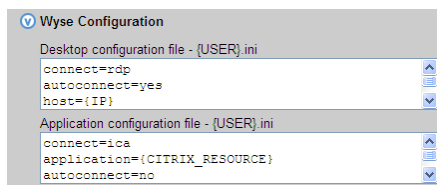
If the sign on is unsuccessful, the user is prompted again for username and password credentials.

The `signoff` command is sent when a user disconnects from the connection; and the `shutdown` command is sent when a user turns off the thin client power.

Use protocol plans to override the global `wnos.ini` variables when a user connects to a particular desktop, as described in the following section.

Protocol Plans for Wyse WTOS Thin Clients

Wyse configuration settings are set in the **Wyse Configuration** section of the protocol plan, shown in the following figure. You can configure separate configuration files to use when launching desktops with RDP and applications with ICA.



By default, the Connection Broker passes the user name and password down to the thin client so that the user is automatically logged into the session. When modifying Wyse configuration files:

- Ensure that each parameter name and value pair is on a single line
- Begin the line with the hash or pound (#) symbol to insert a comment
- Use the Leostream dynamic tags to set session specific variables

The Connection Broker automatically adds any required quotation marks around the values for the `application`, `username`, and `password` WTOS variables.

To use Wyse TCX or VDA, add the appropriate parameters to the desktop configure file (see [Wyse TCX Software Support](#) and [Wyse Virtual Desktop Accelerator \(VDA\) Support](#), respectively).

For a list of the WTOS variables and a detailed Wyse Thin Client setup guide, please refer to the Wyse Winterm 1 series

(Wyse Thin OS) Administrators Guide, available from the Wyse Web site.



If the user's policy offers more than one desktop, the Connection Broker changes the value of the `autoconnect` parameter to `no`. The Connection Broker never automatically launches connections if the user is offered multiple resources.

Using Smart Cards with the Wyse® WTOS Thin Client

To use a smart card with the Wyse WTOS thin client, add a USB-based smart card reader that is compatible with the Wyse thin client.

You must setup a certificate authority that is integrated with your authentication system and issue cards to users in a controlled way so that the user's fully qualified name is stored on the card, for example, `user@company.com`. This ensures that the Connection Broker can use the username it pulls from the smart card to identify that user in the authentication server.

Adding the Leostream SSL Certificate to the Wyse® WTOS Thin Client

If you want the Wyse WTOS thin client to connect using SSL to the Connection Broker when the Connection Broker does not have a certificate that is recognized by the thin client, you need to download the certificate from the Connection Broker interface using a web browser. Then use FTP to place the certificate in the `cacerts` subfolder under the `wnos` folder. Add a line `AddCertificate=filename` to the default `INI` file in the Wyse S10 and the certificate is copied into the S10 certificate cache.

Wyse® WTOS Printer Redirection

Local printing requires that the assigned virtual desktop is mapped to the relevant printer. The Connection Broker tracks the IP address of the client and applies a series of logic rules to determine which printer and fax to assign via the client configuration file.

The logic statements are included in the client configuration file but, rather than defining a variable such as `{IP}` which is always applied, the tag also includes a logic statement that has to be true for the embedded tag to be included when the configuration file is download to the client.

There are three parts to the logic statement. The parts can be together, or on different lines.

For example:

```
{NETWORK:10.0.0.0/255.255.255.0}printer=north{END_NETWORK}
```

The first part `{NETWORK:10.0.0.0/255.255.255.0}` defines a network IP address range. The client IP address has to fall within this range for the logic statement to be true.

The second part `printer=north` defines which printer is used if the logic statement is true. There can be multiple definitions spread across multiple lines.

The third part `{END_NETWORK}` closes the logic statement and has to be present.

There can be multiple logic statements. They are checked in order and as soon as one is true it is applied and all the following logic statements are ignored even if they are true.

For example:

```
{NETWORK:10.0.0.0/255.255.255.0}printer=north{END_NETWORK}
{NETWORK:192.168.10.0/255.255.255.128}printer=south{END_NETWORK}
{NETWORK:0.0.0.0/0.0.0.0}
printer=east
fax=hq
{END_NETWORK}
```

If the client's IP address is 10.0.0.*, they are assigned to the `north` printer; if it is between 192.168.10.1 and 192.168.10.127 they are assigned to the `south` printer; if it is anything else they are assigned to the `east` printer and the `hq` fax.

Wyse® XPe Thin Clients

To log into the Leostream Connection Broker from a Wyse thin clients running a Windows XPe operating system, including Wyse laptops, install Leostream Connect for Windows on the client. You can install Leostream Connect in shell mode, if the thin client should be used *only* to log into the Connection Broker.



To log into the Wyse thin client as the administrator, hold the `shift` key while logging out of the Wyse client.

Wyse TCX Software Support

The Connection Broker natively supports Wyse TCX. When a user logs into the Connection Broker from a Wyse thin client, the Connection Broker establishes an RDP connection between the client and remote desktop. Because TCX runs along the RDP channel, if the Wyse client and remote desktop are equipped with TCX components, the connection automatically switches to using TCX. The Connection Broker is not involved in this exchange.

Wyse Virtual Desktop Accelerator (VDA) Support

The Connection Broker natively supports the Wyse Virtual Desktop Accelerator (VDA) software. VDA software improves the end user experience by accelerating RDP and ICA connections.



The Wyse VDA software was introduced in Wyse ThinOS build 6.4.0 and later.

To instruct the Connection Broker to use the VDA software, add the following parameters to the **Desktop configuration file** and/or **Application configuration file** fields in the **Wyse Configuration** section of the desktop's protocol plan.

- **WyseVDA={no, yes}**: Set to **yes** to enable Wyse Virtual Desktop Accelerator for all ICA or RDP sessions.
- **WyseVDA_No_MMR={no, yes}**: Set to **yes** to disable acceleration for TCX multimedia (MMR). This parameter is applicable only when **WyseVDA** is set to **yes**.
- **WyseVDA_No_USB={no, yes}**: Set to **yes** to disable acceleration for TCX USB peripheral support. This parameter is applicable only when **WyseVDA** is set to **yes**.