



Connection Broker

Where Virtual Desktops Meet Real Business

Leostream™ Connect Administrator's Guide and End User's Manual

Versions 2.8.x / 2.2.x
April 17, 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. Windows and the Windows logo are trademarks of the Microsoft group of companies. Active Directory is a registered trademark of Microsoft Corporation in the United States and 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
CHAPTER 1: OVERVIEW	5
WHAT'S NEW IN THIS RELEASE.....	6
<i>Leostream Connect for Windows</i>	6
<i>Leostream Connect for Linux</i>	7
INSTALLATION.....	8
CHAPTER 2: LEOSTREAM CONNECT SETTINGS	9
CUSTOMIZING THE LEOSTREAM CONNECT USER INTERFACE.....	9
UPGRADING LEOSTREAM CONNECT	11
SPECIFYING AUTHENTICATION METHODS.....	12
ADDING MESSAGE TEXT	12
CHAPTER 3: LEOSTREAM CONNECT ROLE SETTINGS	14
CHAPTER 4: LEOSTREAM CONNECT POLICY SETTINGS	17
HIDING THE HOVER MENU	17
LIMITING THE NUMBER OF ASSIGNED DESKTOPS.....	17
EXPIRING THE USER'S SESSION	18
LISTING DESKTOPS AND APPLICATIONS.....	19
ALLOWING USERS TO RESTART DESKTOPS.....	20
RESTRICTING USERS FROM RELEASING DESKTOPS	21
SETTING TIME ZONES ON REMOTE DESKTOPS.....	22
INTEGRATING WITH VMWARE VIEW CONNECTION SERVERS.....	23
BUILDING PROTOCOL PLANS FOR LEOSTREAM CONNECT	24
<i>Integrating with Cisco Systems VPN Clients</i>	25
<i>Protocol Plans for Sun Ray and Sun Secure Global Desktop</i>	28
USB DEVICE MANAGEMENT	28
<i>Installation Requirements</i>	28
<i>Global Connection Broker Settings</i>	28
<i>Policy Settings</i>	29
PRINTER REDIRECTION.....	30
<i>Redirecting USB Printers</i>	30
<i>Attaching Network Printers</i>	30
DRIVE REDIRECTION	30
CHAPTER 5: SMART CARD, BIOMETRIC AND PROXIMITY CARD SUPPORT	32
USING SMART CARDS WITH LEOSTREAM CONNECT.....	32
<i>Configuring the Connection Broker to Use Smart Cards</i>	32
<i>Using AET SafeSign Identity Client® Software</i>	33
<i>Using bit4id Card Manager Admin Software</i>	33
<i>Using CAC with ActivIdentity ActivClient Security Software</i>	33
<i>Using IAS Middleware</i>	33
<i>Using SafeNet® iKey 1000 USB Tokens</i>	34
<i>Using Smart Cards Containing Multiple Certificates</i>	34
<i>Trouble-Shooting Smart Card Connections</i>	34
USING DIGITALPERSONA® PRO WITH LEOSTREAM CONNECT	35
<i>Installation Requirements</i>	35
<i>Configuring DigitalPersona Pro for Active Directory Workstation Software</i>	35
<i>Unauthenticated Fingerprint Logins</i>	37

XYLOC PROXIMITY CARD AUTHENTICATION	37
HID PROXIMITY CARD AUTHENTICATION WITH RF IDEAS PCPROX© READERS	39
<i>Active Directory Setup</i>	39
<i>Enabling Proximity Card Logins in the Connection Broker</i>	39
<i>Logging in with Proximity Cards</i>	41
CHAPTER 6: USING THE MICROSOFT® WINDOWS® VERSION OF LEOSTREAM CONNECT	42
RUNNING LEOSTREAM CONNECT AND CONNECTING TO RESOURCES	42
<i>Logging into Leostream Connect</i>	42
<i>Connecting to Desktops and Applications</i>	43
USING SHELL MODE	44
<i>Using Quick-Key Options in Shell Mode</i>	44
<i>Using the Shell-Mode Hover Menu</i>	44
<i>Using Client-Side Idle Actions</i>	45
<i>Locking the Session</i>	45
<i>Changing the Connection Broker Address</i>	46
<i>Exiting Shell Mode</i>	46
CLIENT-SIDE CREDENTIAL PASSTHROUGH	46
<i>Example: Credential Passthrough with Shell Mode</i>	47
CONFIGURING OPTIONS ON MICROSOFT® WINDOWS® OPERATING SYSTEMS.....	47
<i>General Options</i>	47
<i>USB Options</i>	48
<i>Log Options</i>	51
<i>About Options</i>	52
USING THE LEOSTREAM CONNECT SYSTEM TRAY MENU	52
<i>Connecting to Desktops and Applications Using the System Tray Menu</i>	52
<i>Connecting to VMware View Connection Servers</i>	53
<i>Managing USB Devices Using the System Tray Menu</i>	54
<i>Managing Resources</i>	55
<i>Switching Users</i>	59
BRANDING LEOSTREAM CONNECT FOR WINDOWS.....	59
RUNNING LEOSTREAM CONNECT FOR WINDOWS FROM THE COMMAND LINE	59
LEOSTREAM CONNECT AND CONNECTION BROKER COMMUNICATION	60
CHAPTER 7: USING THE JAVA™ VERSION OF LEOSTREAM CONNECT	61
RUNNING LEOSTREAM CONNECT AND CONNECTING TO RESOURCES	61
<i>Logging into Leostream Connect</i>	61
<i>Connecting to Desktops and Applications</i>	62
<i>Using the Sidebar Menu</i>	63
<i>Alternate Login Button Configurations</i>	63
<i>Hiding the Domain Field</i>	64
MANAGING RESOURCES	65
SIMULATING SHELL MODE.....	67
CONFIGURING OPTIONS.....	67
<i>Entering the Connection Broker Address</i>	68
<i>Setting Log Levels</i>	68
<i>Viewing Logs</i>	69
<i>Using the Graphical Log Viewer</i>	69
<i>Specifying Remote Viewer Clients</i>	69
<i>Specifying USB Device Redirection Options</i>	71
<i>Writing lc.conf Files</i>	72
RUNNING LEOSTREAM CONNECT FOR LINUX® FROM THE COMMAND LINE	75
<i>Command Line Parameters</i>	76
<i>Command Line Options</i>	76
RUNNING LEOSTREAM CONNECT FOR LINUX® FROM A SHELL SCRIPT	76

Chapter 1: Overview

The Leostream™ Connect client allows users to log into the Connection Broker and access their resources from fat clients. There are two versions of Leostream Connect.

1. Leostream Connect for Microsoft® Windows® operating systems can be installed on the following operating systems:
 - Windows XP
 - Windows Server® 2003
 - Windows Vista®
 - Windows Server 2008
 - Windows 7
2. Leostream Connect for Linux operating systems can be installed on the following operating systems:
 - Apple Mac
 - CentOS
 - Debian
 - Fedora
 - Novell SUSE Linux Enterprise
 - Red Hat Enterprise Linux
 - Ubuntu
 - Solaris

Leostream Connect for Linux is a Java™ application, which requires the following additional software be installed on your Linux client

- An X Window System, such as X11 R6 or X.Org
- A Java Run Time Environment (JRE) version 1.5 or higher

This document describes configuring and using the Leostream Connect client.

- **Administrators:**
 - See **Chapter 2: Leostream Connect General Configuration** for information on general Leostream Connect options.
 - See **Chapter 3: Leostream Connect Role Settings** for information on how Connection Broker Role settings change the end user experience in Leostream Connect.
 - See **Chapter 4: Leostream Connect Policy-Specific Settings** for information on policy options found in the Connection Broker that pertain to Leostream Connect.
 - See **Chapter 5: Authentication Methods** for information about the different authentication methods supported by Leostream Connect for Windows.
 - For information on configuring different display protocols for use with Leostream Connect, see the Leostream Choosing and Using Display Protocols guide.
- **End users:**
 - See **Chapter 6: Using the Microsoft® Windows® version of Leostream Connect** if you are running the Windows version of Leostream Connect.
 - See **Chapter 7: Using the Java™ version of Leostream Connect** if you are running the Java version of Leostream Connect.

What's New in this Release

For features included in previously Leostream Connect client releases, see the complete Connection Broker Release Notes, available on the Leostream Web site [Downloads & Documentation](#) page.

Leostream Connect for Windows

Version 2.8.118 is the current version of Leostream Connect for Windows operating systems. This version contains the following enhancements.

- **USB drivers:** Leostream Connect 2.8 includes a new version of the USB drivers used for USB device redirection. These new drivers are compatible with the USB drivers in version 5.1 of the Leostream Agent for Windows desktops and version 1.4 of the Leostream Agent for Linux desktops, enabling USB device redirection from Windows clients to Linux remote desktops.




These new drivers are not backwards compatible. You must upgrade the Leostream Agents on all remote desktops, if you use Leostream USB redirection.

- **User-configurable NX parameters:** Leostream Connect supports the new Connection Broker feature to allow end users to configure a subset of NoMachine NX configuration parameters (see “NoMachine NX Client” in the Leostream Guide for [Choosing and Using Display Protocols](#))
- **RF IDEas proximity card authentication:** Users can now log in using proximity cards from RF IDEas (see [HID Proximity Card Authentication with RF IDEas pcProx® Readers](#))
- **Shell mode:**
 - Leostream Connect now allows users to lock their client workstation (see [Locking the Session](#))
 - The new registry key `HoverMenuDelay` specifies the amount of time (in milliseconds) to wait before displaying the Leostream Connect hover menu
 - The **About** tab no longer displays on the **Options** dialog
- **Command line parameters:**
 - The command line parameter `-address` to specify the Connection Broker address now honors the Connection Broker setting in the **> System > Settings** page to permit or deny users to specify the Connection Broker address
 - The new command line parameter `clearuser` forces the **Username** field to be empty when launching Leostream Connect, even if a username is specified
- Users can now specify their domain as part of their username, instead of selecting a domain from the **Domain** drop-down menu
- Leostream Connect now honors the TTL setting for the Connection Broker DNS SRV record when the **Obtain Connection Broker address automatically** option is selected (see [Configuring the Connection Broker Address](#))
- **Client-side credential passthrough:**
 - The installer option **Enable client-side credential passthrough** now always requires a reboot
 - Client-side credential passthrough is now supported on Windows Vista and Windows 7 clients
- New installation option `/CONNECTLOGIN` sets the default value for the **Connect to desktop after login**

option on the Leostream Connect **Options** dialog. Individual users can then over ride this default (see the [Leostream Installation Guide](#))

Leostream Connect for Linux

Version 2.2.59 is the current version of Leostream Connect for Linux operating systems.


 Starting with the 2.1.222 release, if a user is offered and connects to multiple resources, the user is no longer automatically logged out of Leostream Connect after they close their last connected desktop. The user must cancel the resource dialog to log out of Leostream Connect.

For example, if the user is offered three desktops and connects then disconnects from two of them, they still have access to the resource dialog and their list of offered desktops. In older versions of the client, as soon as the user disconnected the second desktop, they were automatically logged out of Leostream Connect.

To revert to the old behavior, add the `logout_ondisconnect` parameter to the `lc.conf` file (see [Writing lc.conf Files](#)).

Version 2.2.59 contains the following enhancements.

- **USB drivers:** Leostream Connect 2.2 includes a new version of the USB drivers used for USB device redirection. These new drivers are compatible with the USB drivers in version 1.4 of the Leostream Agent for Linux desktops and version 5.1 of the Leostream Agent for Windows desktops.

 These new drivers are not backwards compatible. You must upgrade the Leostream Agents on all remote desktops, if you use Leostream USB redirection.

- New `exit_ondisconnect lc.conf` parameter forces Leostream Connect to exit after the last resource connection is closed
- The **Password** field on the **Login** dialog now indicates if the Cap Lock key is on when the user begins typing their password
- The installer now displays the path to the Linux kernel.
- Installer no longer creates the `install.log` file. Instead, run the installer with the command line parameter `-DTRACE=true` to obtain an installation log.
- The `lc.conf` parameter `disable_options_tab` has been renamed to `hide_options_button`. The `disable_options_tab` parameter will be deprecated in a future release.
- If the `lc.conf` file does not include the `logout_ondisconnect` parameter, Leostream Connect behavior is set by the new **Log out user after last connection is closed** option on the Connection Broker > **System** > **Settings** page. The `lc.conf` parameter `logout_ondisconnect` will be deprecated in a future release.
- Support for the Connection Broker 7.5.40 feature to hide the Leostream Connect hover menu after the user locks one of their remote desktops.

Installation

See the [Leostream Installation Guide](#) for details on installing Leostream Connect.



Certain installation scenarios require extra privileges, for example:

- To install the Windows version of Leostream Connect with additional tasks, you must be logged into the client device as a user with Administrator privileges.
- To install the USB redirection feature for the Java version of Leostream Connect, you must run the installer as `root`.

Chapter 2: Leostream Connect Settings

This chapter describes the Leostream Connect options on the Connection Broker > **System** > **Settings** page that allow you to customize the appearance and behavior of the Leostream Connect clients communicating with that Connection Broker. These options apply to the Windows and Java versions of Leostream Connect, except where noted.

Customizing the Leostream Connect User Interface

This section describes Leostream Connect settings that are controlled globally via settings in the Connection Broker. You have additional control over the look-and-feel of each client instances, for example:

- You can use the `lc.conf` file to modify the appearance of the Java version of Leostream Connect to match your corporate standards. For a list of `lc.conf` parameters that control the appearance of the Java version of Leostream Connect, see [Common UI Controls](#) in “Writing lc.conf Files”.
- You can customize the icon displayed on the Windows version of Leostream Connect to match your corporate standard. For instructions, see [Branding Leostream Connect for Windows](#).

To open the **Leostream Connect Configuration** options:

- Go to the > **Systems** > **Settings** page in the Connection Broker.
- Scroll down to the **Leostream Connect Configuration** section, shown in the following figure.

The options in this section are as follows:

- Allow user to modify Connection Broker address:** Select this option to allow the user to modify the IP address of the Connection Broker associated with this Leostream Connect client.

This option applies to all users of the Java version of Leostream Connect. For the Windows version of Leostream Connect, this option applies only to users that are not defined as Administrators of the desktop on which Leostream Connect is installed. Users with administrative privileges can always modify the Connection Broker address.
- Allow user to modify domain name:** If you are running an environment with multiple domains, select this option to allow the user to enter or choose the domain to log into. This option applies only to users that are not defined as administrators of the desktop on which Leostream Connect is installed. Users with administrative privileges can always modify the domain.

Chapter 2: Leostream Connect Settings

The Java version of Leostream Connect allows you to remove the **Domain** field from the **Login** dialog. See [Hiding the Domain Field](#) for more information.

- **Allow user to modify user name:** Select this option to allow the user to specify their user name. This option applies only to users that are not defined as administrators of the desktop on which Leostream Connect is installed. Users with administrative privileges can always modify the user name.
- **Allow unauthenticated logins (hides password field):** Select this option to hide the password field on the Leostream Connect login page. With this option checked, if Leostream Connect was invoked from the command line with the user's password, the Connection Broker does not validate the user's password.
- **Allow user to select certificate for smart card login:** (*Applies to the Windows version of Leostream Connect, only.*) Select this option if your end users have smart cards that contain multiple certificates, and they must be able to select which certificate to use during login. With this option unchecked, the Connection Broker always uses the first valid certificate on the smart card.



Only Microsoft Vista and Windows 7 remote desktops honor the certificate selection. All other Microsoft platforms default to the first certificate on the card, regardless of what certificate the user selected in the Connection Broker.

- **Allow user to lock client workstation:** (*Applies to the Windows version of Leostream Connect, only.*) Select this option if users need to use Leostream Connect to lock their client workstation session. With this option selected, the Leostream Connect hover menu contains a **Lock Workstation** option. If Leostream Connect is running in the client device's shell, when the user selects this option, their remote sessions are hidden and Leostream Connect opens the **Unlock Workstation** dialog. If Leostream Connect is *not* running in the client device's shell, Leostream Connect uses the native Windows locking mechanism to lock the client device. The user enters their credentials to unlock their session. See [Locking the Session](#) for more information.
- **Provide client workstation idle time actions:** (*Beta*) Select this option to allow the user to automatically lock their client workstation or close all open desktop connections when the client device running Leostream Connect is idle for a specified length of time. See [Using Client-Side Idle Actions](#) for more information.
- **Log out user after last connection is closed (opens Login dialog):** (*Applies to the Windows version of Leostream Connect, only.*) Select this option to specify that Leostream Connect should automatically log out the user after the user closes, either by disconnecting or logging out, their last resource connection. After the user is logged out, the Leostream Connect **Login** dialog automatically opens.
- **Close connection when smart card is removed from reader:** (*Applies to the Windows version of Leostream Connect, only.*) Select this option to automatically disconnect all of the user's connections when they remove their smart card from the reader. This setting applies only when the **Smart card** authentication method is selected (see [Specifying Authentication Methods](#)).
- **Exit client after connection to resource is established:** Select this option to automatically exit the user's Leostream Connect session after the connection to their resources is established. Typically, select this option when users are logging in using Sun Secure Global Desktop software.

If the user is launching a connection to a resource they are managing for another user, Leostream Connect will not automatically exit after the connection is established. This option applies only when the user launches one of their resources.

- **Use Device UUID to uniquely identify clients:** Select this option to use the client's Device UUID to uniquely identify client devices on the **> Clients > Clients** page.



You must select this option if users log in from Sun Ray thin clients.


Client devices that register with the Connection Broker have the option to provide one or more of the following attributes.

- Device UUID – An ID unique to the client hardware
- Client UUID – An ID unique to the software client that handles the user login

- MAC address – The client device MAC address
- Serial number – The client device serial number


With this option selected, when a client device registers with the Connection Broker and that client device provides a device UUID, the Connection Broker searches the **Device UUID** column on the > **Clients** > **Clients** page for a client with the provided device UUID. If the Connection Broker finds the device UUID, the Connection Broker assumes a record for the registering client already exists. If the Connection Broker does not find the device UUID, the Connection Broker creates a new client record for the registering client.

When this option is not selected or if clients register without providing a device UUID, the Connection Broker searches the **Client UUID**, **MAC Address**, and **Serial Number** columns on the > **Clients** > **Clients** page, in order. When a client registers, if the Connection Broker finds a client on the > **Clients** > **Clients** page that matches the value for any of these attributes of the registering client, the Connection Broker assumes a record for the registering client already exists. If the Connection Broker does not find a match for any of these attributes, the Connection Broker creates a new client record for the registering client.

- **Show additional login button (Java client only):** *(Applies to the Java version of Leostream Connect, only.)* Select an option to show or hide an additional button on the Leostream Connect **Login** dialog. See [Alternate Login Button Configurations](#) for a description of the actions performed by the login options described in the following list.
 - **Do not display:** Never display an additional button on the **Login** dialog.
 - **Use client settings:** Show or hide the **Advanced Login** button based on the value set for the `hide_advanced_login` parameter in the `lc.conf` file stored in each client device.
 - **Advanced Login:** Display the **Advanced Login** button. Clicking the **Advanced Login** button opens the **Connect** dialog. On this dialog, end users with the appropriate policy and role settings can restart and connect to their desktop.
-  The **Advanced Login** button is required for users with a role that allows them to manage another user's desktops (see [Managing Resources](#)).
- **Restart:** Display the **Restart** button. The behavior of the **Restart** button differs based on the number of desktops the user is offered, and if they have permission to restart their desktops. See [Alternate Login Button Configurations](#) for a description of how the **Restart** button performs.

Upgrading Leostream Connect

After Leostream Connect is installed on a client device, the Windows and Java version can be upgraded to the latest version available on the Connection Broker > **Status** > **Downloads** page.

 Automatic upgrade support is new in version 2.0 of the Java version of Leostream Connect. You cannot automatically upgrade older versions of Leostream Connect to version 2.0. However, version 2.0 can automatically be upgraded to Leostream Connect version 2.1.

To push upgrades out to all the client devices that log into a particular Connection Broker, select one of the following options from the **Upgrade client to latest version** drop-down menu on the Connection Broker > **System** > **Settings** page.

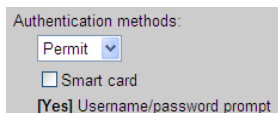
- **Never:** Do not update Leostream Connect. In this case, you must manually update end users' clients.
- **Always:** Always update Leostream Connect. In this case, when an end user runs Leostream Connect, they are warned that an update is in process. Leostream Connect restarts when the update is finished.
- **Prompt user:** Let the user decide if they want to update Leostream Connect. In this case, when the user launches Leostream Connect and an update is available, the client prompts the user to install the update.

Specifying Authentication Methods

 This section applies to the Windows version of Leostream Connect, only.

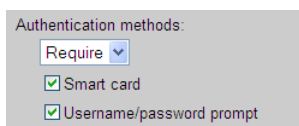
The **Leostream Connect Configuration** section on the **> Systems > General Configurations** page allows you to configure the type of identification a user can provide when authenticating with the Connection Broker.

When the **Authentication methods** drop-down menu is set to **Permit**, users are always allowed to authenticate using their user name and password. By default, the Connection Broker alternatively allows the user to authenticate via a smart card. If users should not be allowed to log in using a smart card, uncheck the **Smart card** checkbox, as shown by the following figure.



To require the user to provide their user name and password as well as a smart card:

1. Select **Require** from the drop-down menu in the **Authentication Methods** section.
2. Check the **Smart card** and **Username/password prompt** checkboxes, as shown in the following figure.



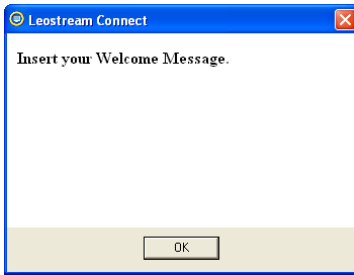
With the Connection Broker in the previous configuration, the Leostream Connect Login dialog appears as follows.



See **Chapter 5: Smart Card and Biometric Support** for information on integrating Leostream Connect with different types of smart cards and biometric readers.

Adding Message Text

To display a message to your users when they launch Leostream Connect, enter text in HTML format, including links, into the **Message text** field on the Connection Broker **> System > General Configuration** page. When the user runs Leostream Connect, the message text appears in a Welcome window prior to the user being asked for their credentials. For example:



After the user clicks **OK**, the **Login** page opens.

Chapter 3: Leostream Connect Role Settings

Beginning with Connection Broker version 6.3, Leostream Connect now adheres to the user's role settings when determining if the user is allowed to restart or release their desktop.

Roles are defined in the Connection Broker > **User** > **Roles** page. See “Chapter 13: Managing User Roles and Permissions” in the [Connection Broker Administrator's Guide](#) for a complete description of user roles.

The session permissions in each role, shown in the following figure, determine the actions that users with this role are allowed to perform.

The screenshot shows the 'Create Role' dialog box with the following fields and options:

- Name:** A text input field.
- End-User Session Permissions:** A section containing several checkboxes:
 - Allow user to manage another user's resources
 - Allow user to manually release desktops
 - Allow user to power desktops on or off
- Login user as:** A dropdown menu currently set to 'Domain user'.
- Add and remove user from Remote Desktop Users group

Explanatory text with arrows pointing to the dialog:

- Enter a display name for the role. Refer to this name when assigning this role to users. (points to Name field)
- Select this option if users should be able to manually release their desktop back to its pool. (points to 'Allow user to manually release desktops' checkbox)
- Select this option if users should be able to reboot their desktops. (points to 'Allow user to power desktops on or off' checkbox)
- Select this permission if a user with this role must be able to log into another user's desktop to perform administrative tasks on that desktop. (points to 'Allow user to manage another user's resources' checkbox)
- Use this option to indicate if the user logs into the remote desktop as a domain user or a local user. When using a local user, you can specify if the Connection Broker should automatically create and delete the local user on the remote desktop. (points to 'Login user as' dropdown)
- Use this option to allow users to connect to a remote desktop without requirement them to already be part of the Remote Desktop Users group. The Connection Broker can add the user as a local or domain user. The user is always removed from the group when they log out of the desktop. (points to 'Add and remove user from Remote Desktop Users group' checkbox)

The current session permissions are as follows:

- **Allow user to manage another user's resources:** Select this option if a user with this role should be able to view the desktops offered to another user, and then log into those desktops. Use this option for user's that are allowed to perform administrative tasks on another user's desktop, or for users that need to log into their own desktop using different credentials from those they provided when logging into the Connection Broker.
- **Allow user to manually release desktops:** (*This option applies to the Windows version of Leostream Connect, only.*) Select this option if a user with this role should be able to manually release their desktop back to its pool. By default, when a user connects to a desktop, the Connection Broker assigns that desktop to that user. When a desktop is assigned to a user, the Connection Broker will not offer that desktop to another user.

If a user manually releases one of their desktops back to its pool, the Connection Broker unassigns the desktop from that user. If the user is logged into that desktop when they release it, they remain logged in. However, because the user is no longer assigned to the desktop, the Connection Broker now considers them as a rogue user. In addition, because the desktop is back in its pool, the Connection Broker may offer that desktop to another user. If this new user tries to connect to the desktop, and their policy is set to log off rogue users, the new user will forcefully log out the original user.

If the **Allow user to manually release desktops** option is selected, the user is allowed to release any of their assigned desktops. The user's policy then indicates exactly which of their desktops the user can actually release. If the **Prevent user from manually releasing desktop** option is selected for a pool in the user's policy, the user will not be able to release desktops from this pool, even though their role gives them the permission.



The user can never release a desktop that is hard-assigned to them.

- **Allow user to power desktops on or off:** Select this option if a user with this role should be able to restart their desktop. If the **Allow user to power desktops on or off** option is selected, the user is allowed to restart any of their assigned desktops. The user's policy then indicates exactly which of their desktops the user can actually restart. If the **Allow user to reset offered desktop** option is set to Not allowed for a pool in the user's policy, the user can not restart the desktops in this pool, even though their role gives them the permission.
- **Login user as:** *(Requires a Leostream Agent on the remote desktop.)* Use this option indicate if the Connection Broker should log the user into the remote desktop using a domain account or local user account. Use local users to support, for example, LDAP or non-domain users that need to login to remote desktops. Options in the **Login user as** drop-down include.

- **Domain user:** When using an Active Directory domain user account, the Connection Broker uses the domain name specified by the authentication server on the **> Users > Authentication Servers** page that authenticated the user when they logged into the Connection Broker.
- **Local user:** When logging in as a local user, the Connection Broker requires an existing user account on the remote desktop. This user account must have the same login name as the user that logged into the Connection Broker. When using this option, you must manually create the appropriate account in the **Users** section of the **Local Users and Groups** node in the **Computer Management** dialog.

If you want the Connection Broker to manage the local user account, use one of the following two options.

- **Local user (create on login):** You can instruct the Connection Broker to automatically create local user accounts, to avoid having to manually create the accounts on each remote desktop. When this option is selected, the Connection Broker automatically creates an appropriate local user on the desktop the first time the user logs in. If an appropriate user account already exists, the Connection Broker uses that account.

If a user account exists on the remote desktop, the Connection Broker uses that account. If that user account has a different password from the password used to log into the Connection Broker, the Connection Broker changes the password for the local user on the remote desktop.

- **Local user (create on login; delete user on logout):** You can instruct the Connection Broker to automatically create and delete local user accounts, to avoid having to manage the accounts on each remote desktop. When this option is selected, the Connection Broker automatically creates an appropriate local user account on the desktop the first time the user logs in. The Connection Broker removes the user account as soon as the user logs out of the desktop.

The Connection Broker does not delete the profile folder associated with the user. Any information stored in the profile folder can be recovered by the desktop's administrator.



When the user subsequently logs into the desktop, the Connection Broker creates a new local user account. Because this is a new account, the Windows desktop does not associate this user with the profile created the last time the user logged in. If user's need persistent access to their profile, use the **Local user (create on login)** option.

- **Local user (create on login; delete user and profile on logout):** When this option is selected, the Connection Broker automatically creates an appropriate local user account on the desktop the first time the user logs in. The Connection Broker removes the user account and the user's profile folder as soon as the user logs out of the desktop.



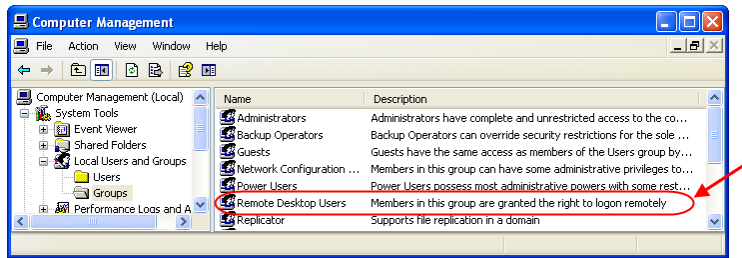
Because the user's profile folder is deleted, the user loses all information stored locally in their profile folder.

- **Add and remove user from Remote Desktop Users group:** *(Requires a Leostream Agent on the remote desktop.)* Use this option if your users are not already members of the Remote Desktop Users group on their offered Windows desktops.


By default, Windows desktops do not provide remote access. After you enable remote access for a particular desktop, you must indicate which users are allowed to remotely log into that desktop by placing those users

Chapter 3: Leostream Connect Role Settings

(one of their group memberships) in the Remote Desktop Users group, shown in the following figure.



When a user is part of the Remote Desktop Users group, they can remotely log into the desktop from any client. To restrict the user to log in only through the Connection Broker, do not manually add users to the Remote Desktop Group and, instead, select the **Add and remove user from Remote Desktop Users group** option. With this option selected, the Connection Broker automatically adds the user to the Remote Desktop Users group when the log into the desktop from the Connection Broker. When the user logs out, the Connection Broker automatically removes the user from the Remote Desktop Users group.

 The Connection Broker essentially takes control of the user's membership in the Remote Desktop Users group. If the user was already a member of the Remote Desktop Users group before they logged into the desktop, the Connection Broker removes the user from that group when they log out of the desktop. The Connection Broker adds the user back to the Remote Desktop Users group the next time they log into the Connection Broker.

Chapter 4: Leostream Connect Policy Settings

Connection Broker policy settings allow you to control the user's experience, including:

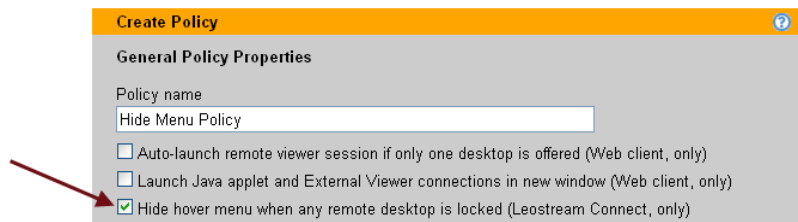
- The display names for the list of resources offered by Leostream Connect
- How many desktops the user can connect to, and how long they can continue to connect to new desktops
- If the user can restart or release their desktop
- The remote viewer protocol used to connect to each desktop
- What USB device the user can connect to their remote desktop
- And more!

Except where noted, policy settings apply to the Windows and Java versions of Leostream Connect. The following sections describe policy options that directly pertain to Leostream Connect. For a complete description of all Connection Broker policy options, see the [Connection Broker Administrator's Guide](#).

Hiding the Hover Menu

Connection Broker 7.5.40 allows you to hide the Leostream Connect hover menu on Linux operating systems after the user locks one of their connected desktops. By hiding the hover menu, you ensure that no other desktops can be launched after a connected desktop is locked.

To enable this feature, select the **Hide hover menu when any remote desktop is locked** option in the **General Policy Settings**, shown in the following figure.



The hover menu is hidden if *any* connected desktop is locked. The locked desktop does not need to be at the forefront or the current focus

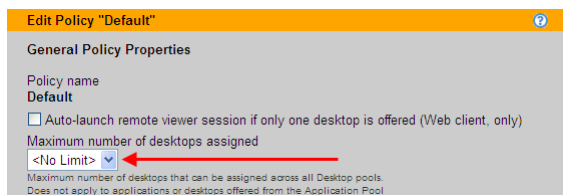


This feature requires version 2.2.59 of Leostream Connect for Linux.

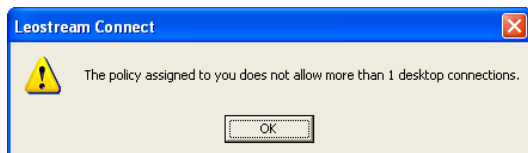
Limiting the Number of Assigned Desktops

By default, end users can be assigned and connected to all of the desktops offered to them by Leostream Connect. To conserve resources, you can limit the number of desktops assigned to a particular user, as follows.


1. Go to the **> Users > Policy** page.
2. Select the **Edit** action for the appropriate policy. The **Edit Policy** form opens.
3. Select the maximum number of desktops that can be simultaneously assigned to a particular use from the **Maximum number of desktops assigned** drop-down menu, shown in the following figure. The **<No Limit>** option allows the user to connect to all of their offered resources.




When the user logs into Leostream Connect, they can continue to connect to desktops until they reach the number selected in the **Maximum number of desktops assigned** drop-down menu. After that point, when the user tries to connect to another desktop, the client issues a warning, for example:



On the Windows version of Leostream Connect, the **Connect** options in the Leostream Connect system tray menu are disabled after the user reaches their maximum number of assigned desktops.

 Depending on the user's policy settings, a desktop may remain assigned to the user after they logout or disconnect from the desktop. Leostream Connect factors in that assignment when determining if the user can connect to a new desktop.

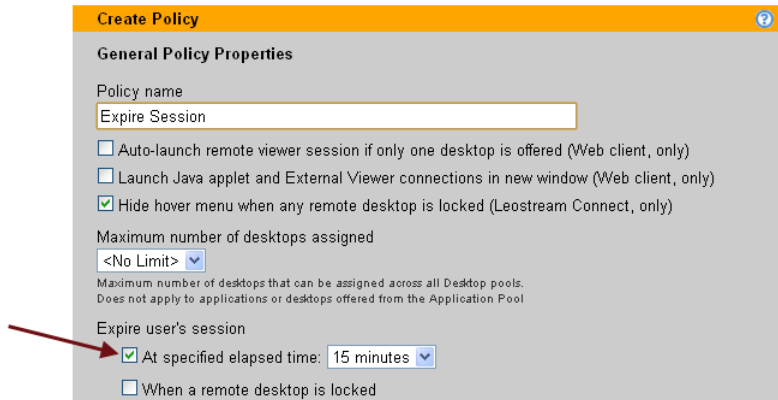
For example, consider a policy that offers two desktop, but limits the user to be assigned to one desktop. The policy also keeps the desktop assigned to the user when they disconnect from the desktop. The first time the user logs into Leostream Connect, they connect to one of their offered desktops. The user then disconnects from the desktop, and exits Leostream Connect. The next time they log into Leostream Connect, they are offered two desktops, but the only desktop Leostream Connect allows them to connect to is the desktop they are already assigned, i.e., the desktop the user disconnected from in their last Leostream Connect session.

 This option does not apply to applications and desktops published in a Citrix XenApp farm. The user can continue to launch these resources after their limit is reached.

Expiring the User's Session

By default, end users can connect to additional desktops and applications until they exit Leostream Connect. You may, for security purposes, want to limit how long the user can launch new connections. To do this, configure the user's session to expire after a specified elapsed time, as follows.


1. Go to the **> Users > Policy** page.
2. Select the **Edit** action for the appropriate policy. The **Edit Policy** form opens.
3. In the **Expire user's session** section, shown in the following figure, select the **At specified elapsed time** option.




4. From the drop-down menu, select the time after which the user can no longer connect to additional resources.

After a user's session expires, they can continue to use any desktops and applications they already launched. However, if the user is connected to desktops, they cannot attach additional USB devices.

If the user attempts to launch a new resource or attach a USB device to any connected desktop after their session expires, Leostream Connect automatically issues a warning and logs out the user. To launch additional resources, the user must log back into the Connection Broker.

 Leostream Connect 2.8 for Windows operating systems closes all of the user's open desktops when they log back in to Leostream Connect. Therefore, you should not select the **Log out user after last connection is closed** option on the Connection Broker > **System** > **Settings** page if you plan to expire the users session. If you do select this option, the user is required to log in twice after their session expires, once to unexpired the session and again after all their desktop connections are closed.

 Connection Broker 7.5.40 contains a beta feature to expire the user's session after they lock any of their open desktop connections. This feature requires the 2.9 beta version of Leostream Connect. The 2.9 beta release of Leostream Connect also keeps the user connected to their previously open desktops after they log back in to Leostream Connect. Contact support@leostream.com for more information on using this beta feature and release.

Listing Desktops and Applications

If an end user is offered multiple resources, you can define the format used to display the resource name, as follows:

1. Go to the > **Users** > **Policy** page.
2. Select the **Edit** action for the appropriate policy. The **Edit Policy** form opens.
3. For all desktop and application pools, as well as for hard-assigned desktops, select an option from the **Display to user as** drop-down menu, an example of which is shown in the following figure.

The screenshot shows the 'Edit Policy "Default"' interface. Under the 'Desktop Assignment from Pools' section, the 'Pool' is set to 'All Desktops'. In the 'When User Logs into Connection Broker' section, 'Number of desktops to offer' is 25, and 'Select desktops to offer based on' is 'User ("follow-me" mode)'. The 'Display to user as' dropdown is highlighted with a red circle and a red arrow pointing to it. The dropdown menu is open, showing options: 'Desktop name', 'Windows machine name', 'Pool name', 'Pool name - Desktop name', and 'Pool name - Windows machine name'. Below this, there are checkboxes for 'Allow users to reset offered desktops', 'Offer running desktops without a lock', and 'Offer stopped and suspended desktops'.

You can display desktops to users as any of the following:

- The desktop name, as shown in the **Name** column on the > **Resources > Desktops** page.
- The desktop's display name, as defined on the **Edit Desktop** page for the offered desktop.
- The desktop's Windows machine name
- The name of the desktop's pool
- The name of the desktop's pool followed by the desktop's name
- The name of the desktop's pool followed by the desktop's display name
- The name of the desktop's pool followed by the desktop's Windows machine name

You can display Citrix XenApp applications as any of the following:

- The application name
- The name of the application's pool
- The name of the application's pool followed by the application's name

Allowing Users to Restart Desktops

The Connection Broker allows end users to restart their remote desktops if the user is assigned a role and a policy that provide sufficient restart permissions. The user's role tells the Connection Broker if the user is allowed to restart any of their desktops. The user's policy then indicates which of the user's offered desktops they can restart, and how the Connection Broker should perform the restart.

To create a role that gives the user permission to restart their desktops:

1. Go to the > **Users > Roles** page.
2. Select **Create Role** to add a new role, or **Edit** to add this permission to an existing role.
3. In the **Session Permissions** section, select the **Allow user to power desktops on or off** option, shown in the following figure.

The screenshot shows the 'Create Role' interface. Under the 'End-User Session Permissions' section, there are three checkboxes: 'Allow user to manage another user's resources', 'Allow user to manually release desktops', and 'Allow user to power desktops on or off'. The 'Allow user to power desktops on or off' checkbox is checked and highlighted with a red circle and a red arrow pointing to it.

4. Click **Save**.

To configure how the Connection Broker performs any requested restarts:

1. Go to the **> Users > Policy** page.
2. Select the **Edit** action for the appropriate policy. The **Edit Policy** form opens.
3. Select an option from the **Allow users to reset offered desktops** drop-down menu, shown in the following figure.

The screenshot shows the 'Edit Policy "Default"' window. Under the 'When User Logs into Connection Broker' section, the 'Allow users to reset offered desktops' dropdown menu is highlighted with a red circle and currently shows 'Not allowed'. Other visible options include '25' for the number of desktops to offer, 'User ("follow-me" mode)' for selection, and 'Pool name : Desktop name' for display.

The **Shutdown and start** option attempts to gracefully shut down the user's desktop. If the user's desktop is a virtual machine, **Shutdown and start** first tries to reboot the VM's operating system. If a reboot cannot be done, **Shutdown and start** performs a guest shutdown and power up. The **Power off and start** option forcefully shuts down the desktop.



If the user's desktop is a physical machine, select the **Shutdown and start** option and ensure that the Leostream Agent is installed on the desktop.

Users access the restart action differently for the Windows and Java version of Leostream Connect.

- The Windows version of Leostream Connect provides a **Restart** option in the Leostream Connect system tray menu.
- The Java version of Leostream Connect provides a **Restart** button on the **Connect** dialog.

Restricting Users from Releasing Desktops



This option applies to the Windows version of Leostream Connect, only.

When the Connection Broker assigns a desktop to a particular user, that desktop is no longer part of any pool and, therefore, cannot be offered or assigned to another user. The Connection Broker assigns the desktop to a user as soon as the user requests a connection to that desktop. Release plans in Connection Broker policies determine when the desktop is released back to its pool.

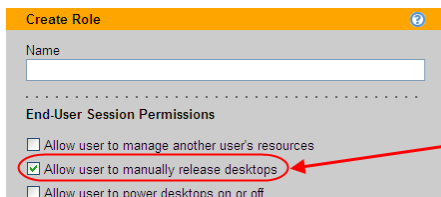
You can also allow the user to manually release their desktop back to its pool. After the user releases their desktop, the Connection Broker considers that user as a *rogue user* as long as they remained logged into the remote desktop connection established by Connection Broker.

The user's role tells the Connection Broker if the user is allowed to release any of their desktops.

Chapter 4: Leostream Connect Policy Settings

To create a role that gives the user permission to release their desktops:

1. Go to the **> Users > Roles** page.
2. Select **Create Role** to add a new role, or **Edit** to add this permission to an existing role.
3. In the **Session Permissions** section, select the **Allow user to manually release desktops** option, shown in the following figure.

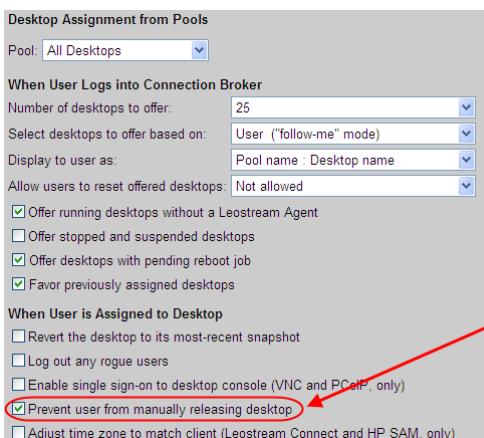


The screenshot shows a 'Create Role' dialog box with a 'Name' input field. Below it is the 'End-User Session Permissions' section, which contains three checkboxes: 'Allow user to manage another user's resources' (unchecked), 'Allow user to manually release desktops' (checked and circled in red), and 'Allow user to power desktops on or off' (unchecked). A red arrow points from the right side of the dialog to the checked checkbox.

4. Click **Save**.

By default, a user with this role can release all of their assigned desktops using the **Release** or **Disconnect and Release** options in the Leostream Connect system tray menu. See [The Leostream Connect System Tray Menu](#) for information on these options.

To prohibit users from releasing desktops from a particular pool, select the **Prevent user from manually releasing desktop** option in the **When User is Assigned to Desktop** section of the **Edit Policy** page, shown in the following figure.



The screenshot shows the 'Desktop Assignment from Pools' configuration page. The 'Pool' dropdown is set to 'All Desktops'. Under the 'When User Logs into Connection Broker' section, there are several dropdown menus and checkboxes. Under the 'When User is Assigned to Desktop' section, the checkbox 'Prevent user from manually releasing desktop' is checked and circled in red. A red arrow points from the right side of the page to this checkbox.

Leostream Connect removes the **Release** and **Disconnect and Release** options from the system tray menu for desktops assigned from this pool.


Setting Time Zones on Remote Desktops

For users connecting to Windows remote desktops – from either the Windows or Java version of Leostream Connect – you can set the time zone of the remote desktop to match that of the client device by selecting the **Adjust time zone to match client** check box shown in the following figure.

The screenshot shows the 'Desktop Assignment from Pools' configuration interface. It includes a dropdown for 'Pool' set to 'All Desktops'. Under 'When User Logs into Connection Broker', there are settings for 'Number of desktops to offer' (25), 'Select desktops to offer based on' (User ('follow-me' mode)), 'Display to user as' (Pool name : Desktop name), and 'Allow users to reset offered desktops' (Not allowed). There are four checked checkboxes: 'Offer running desktops without a Leostream Agent', 'Offer desktops with pending reboot job', 'Favor previously assigned desktops', and 'Prevent user from manually releasing desktop'. Under 'When User is Assigned to Desktop', there are four unchecked checkboxes: 'Revert the desktop to its most-recent snapshot', 'Log out any rogue users', 'Enable single sign-on to desktop console (VNC and PCoIP, only)', and 'Adjust time zone to match client (Leostream Connect and HP SAM, only)'. A red circle highlights the last checkbox, with a red arrow pointing to it from the right.

Selecting this option changes the time zone of the remote desktop to the same time zone as on the user's client.

The time zone is not reverted when the user logs out or disconnects. Therefore, if another user logs in to the same desktop with a policy that does not adjust the time zone, that user will see the time zone set for the previous user. To ensure that your end-users see the correct time zone, select this option for all policies that could assign a particular desktop.

 Adjusting the desktop's time zone may adversely affect scheduled tasks.

Integrating with VMware View Connection Servers

Leostream Connection Broker 7.0 and the Windows version of Leostream Connect provide single sign-on to the VMware View Client and the user's View desktops. You configure Leostream and View to work together, as follows.

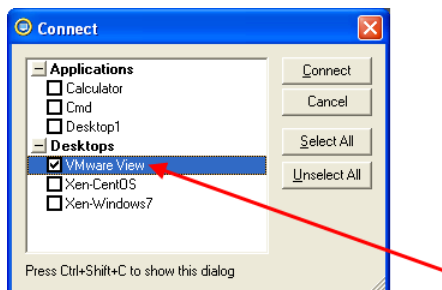
1. Install and configure the VMware View Manager to entitle your users to connect to the appropriate desktops using the desired protocol, including software PCoIP.
2. On the user's client device, install the VMware View Client. Consult your thin client vendor to determine if your thin client ships with an installed VMware View Client.
3. Also on the user's client device, install the Windows version of Leostream Connect. For installation instructions, see the [Leostream Installation Guide](#).
4. In the Leostream Connection Broker, in the **Desktop Assignment from VMware View** section of the user's policy, configure one or more VMware View Connection servers to offer to this user, in addition to any other desktops and applications the user needs to access.

To configure the **Desktop Assignment from VMware View** section, shown in the following figure, enter a display name for the View server and the VMware View Connection Server URL.

The screenshot shows the 'Desktop Assignment from VMware View' configuration interface. It includes a subtitle 'Allow the user to sign into one or more VMware View servers'. There are two text input fields: 'View Server Name' containing 'VMware View' and 'View Server URL' containing 'http://10.110.37.4'. Below these fields is a dropdown menu labeled '[Add VMware View Servers]'.

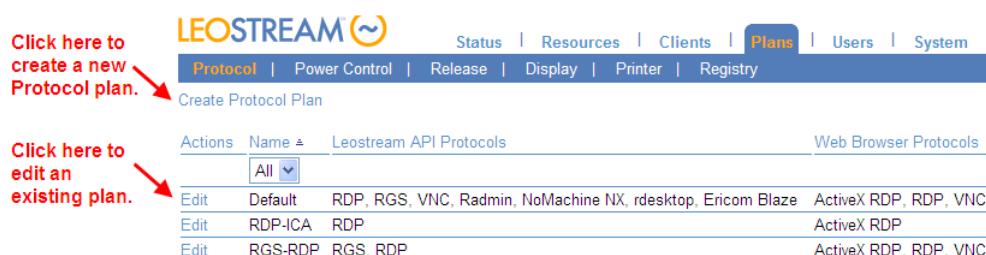
See "Configuring VMware View Policy Options" in the [Connection Broker Administrator's Guide](#) for more information.

When a user with this policy logs in to the Connection Broker, they are offered all the resources configured in their policy, including the VMware View server, as shown, for example, in the following figure.



Building Protocol Plans for Leostream Connect

Connection Broker protocol plans determine which display protocol is used when a user logs in through Leostream Connect. Available protocol plans are displayed on the > **Plans > Protocol** page, shown in the following figure.



You apply your protocol plans to the individual pools in each policy. The **Leostream Connect and Thin Clients Writing to Leostream API** section in the protocol plan defines which display protocols Leostream Connect can use to connect to a particular pool of desktops. This section contains subsections that define the configuration settings for each protocol, as follows:

- The **Priority** drop-down menu determines the order in which Leostream Connect tries to establish a connection using each protocol. Select Do not use to prohibit Leostream Connect from using a particular protocol.
- The **Command line parameters** and **Configuration file** fields define the settings used when establishing a connection with the selected protocol.

Create protocol plans that define the experience you want to provide for different groups of users. For example, if all users connect to their desktops using RDP, create a single protocol plan that gives RDP the highest priority. If another group of users connects using HP RGS, create a second protocol plan that gives RGS the highest priority, as shown in the following figure.

In the following example, Leostream Connect first tries to establish a connection to the remote desktop using HP RGS. If an RGS connection cannot be established, Leostream Connect then tries RDP, which has a priority of 2.

LEOSTREAM Status | Resources | Clients | Plans |

Protocol | Power Control | Release | Display | Printer | Registry

Edit Protocol Plan

Plan name
RGS before RDP

Leostream Connect and Thin Clients Writing to Leostream API

RDP Priority: 2

Command line parameters

Configuration file
screen mode id:i:2
desktopwidth:i:1024
desktopheight:i:768

RGS Priority: 1

Configuration file

VNC Priority: Do not use

Command line parameters

Configuration file
[connection]
host={IP}
port=5900

Use this section to specify which remote viewing protocols Leostream Connect should use.

The "Priority" determines the order in which Leostream Connect tries to connect to the desktop using this remote viewing protocol.

Set the "Priority" to "Do not use" to prohibit Leostream Connect from using this remote viewing protocol.

For complete information on using display protocols with Leostream Connect, see the Leostream guide for [Choosing and Using Display Protocols](#), available on the Leostream [Downloads and Documentation](#) Web site.

Integrating with Cisco Systems VPN Clients

The Windows version of Leostream Connect can automatically establish a secure tunnel using the Cisco Systems VPN Client, providing seamless and secure single sign-on for end users. Leostream Connect uses the `vpngui.exe` to launch the tunnel and then automatically connects the user to their remote desktop using the protocol defined in the **Leostream Connect and Thin Clients Writing to Leostream API** section of the protocol plan.

 Leostream Connect does not integrate with the Cisco Anywhere VPN client.

To enable this feature, check the **Use Cisco VPN client to establish secure tunnel for connections** option at the bottom of the **Leostream Connect and Thin Clients Writing to Leostream API** section of the protocol plan, shown in the following figure.

Cisco VPN client

Use Cisco VPN client to establish secure tunnel for connections
Establish tunnel prior to desktop connection; tear down when connection closes

Profile

With this option selected, Leostream Connect attempts to establish a secure tunnel before connecting to the desktop. You can use any of the display protocol defined in the **Leostream Connect and Thin Clients Writing to Leostream API** section to establish the connection to the desktop.

When the Cisco option is selected, as shown in the previous figure, the **Profiles** edit field appears. Enter a valid profile (the contents of a PCF-file) in the **Profiles** edit field, for example:

Chapter 4: Leostream Connect Policy Settings

```
[main]
Description=Authentication to your domain
Host=enter-cisco-vpn-ip
AuthType=1
GroupName=dev
GroupPwd=
enc_GroupPwd=enter-password
EnableISPConnect=0
ISPConnectType=0
ISPConnect=
ISPPhonebook=
ISPCommand=
Username=enter-username
SaveUserPassword=0
UserPassword=
enc_UserPassword=
NTDomain=
EnableBackup=0
BackupServer=
EnableMSLogon=1
MSLogonType=0
EnableNat=1
TunnelingMode=0
TcpTunnelingPort=10000
CertStore=0
CertName=
CertPath=
CertSubjectName=
CertSerialHash=
SendCertChain=0
PeerTimeout=90
EnableLocalLAN=0
```


After you define your protocol plan, assign it to pools of desktops used in each policy, as shown in the following figure.

Each pool in the policy is assigned a particular Protocol plan

Choose the appropriate plan from the "Protocol" drop-down menu.

The VPN client must be installed on the client device if the protocol plan enables login through the Cisco Systems VPN Client. After the user logs in, the Connection Broker sends Leostream Connect the PCF-file configured in the user's protocol plan. Leostream Connect copies this PCF-file to the Profiles directory on the user's client device, then uses the `vpngui.exe` command to establish the secure tunnel using this profile. If the PCF-file is not configured correctly in the protocol plan, the VPN client prompts the user for the information needed to establish the tunnel. As soon as the tunnel is established, Leostream Connect deletes the PCF-file from the client device.

The Cisco VPN supports a single tunnel. Therefore, if the user launches multiple desktops, Leostream Connect reuses the existing tunnel for all desktops, as long as all desktops use the same profile. If a desktop has a different profile, the existing tunnel is closed and a new tunnel is established. Closing the previous tunnel disconnects any connected desktops. To avoid inadvertently closing desktops, use the same protocol plan for add desktops connecting through the VPN.

 Create separate protocol plans for users that log in from clients that do not have an installed Cisco Systems VPN Client. Use these two protocol plans in different policies, and assign the policies to the user based on the user's location.

For example, in the following figure, the user is assigned the `RemotePolicy` when they login from home, but is assigned the `OfficePolicy` when they login at the office. The policy `RemotePolicy` uses a protocol plan that enables the Cisco Systems VPN Client feature, while the policy `OfficePolicy` disables Cisco VPN Client logins.

Order	Attribute Value	Client Location	User Role	User Policy
1	Development	InOffice	OfficeRole	OfficePolicy
2	Development	AtHome	RemoteRole	RemotePolicy

For information on creating locations and assigning policies to users, see Chapter 12 and 14 in the [Connection Broker Administrator's Guide](#).

Protocol Plans for Sun Ray and Sun Secure Global Desktop

The **Sun Ray** and **Sun Secure Global Desktop** sections of the protocol plan apply only to the Java version of Leostream Connect. When setting up a protocol plan for Oracle Sun Ray or Oracle Secure Global Desktop (SGD) environments, set the **Priority for Sun Ray** or **Sun Secure Global Desktop**, respectively, to 1. Set the Priority for *all* other protocols to **Do not use**.

The entry in the **Command line parameters** field configures the Sun ALP or AIP connection to the Sun server. The final connection to the remote desktop is accomplished using rdesktop.

- For more information on integrating Leostream with Oracle Secure Global Desktop Software, see “Oracle Secure Global Desktop Setup” in the [Connection Broker Administrator’s Guide](#).
- For more information on configuring Leostream to work with Sun Ray clients, see the Leostream [Thin Clients Guide](#).

USB Device Management

The Connection Broker allows you to manage the USB devices that different users are allowed to attach to their remote desktops. You must manually install any drivers required by your particular devices on the remote desktop. Leostream Connect does not control how the device and associated applications run or perform on the remote desktop.

Installation Requirements

The Leostream USB management feature requires functionality on the client device and remote desktop.

- On the client side, you must install Leostream Connect with the **Enable USB over IP** task is selected.
- On the desktop side, you must install the Leostream Agent, and the **Enable USB over IP** task must be selected during installation.



The USB drivers included in the current versions of Leostream Connect require the following versions of the Leostream Agent.

- Leostream Agent 5.1 – Windows version
- Leostream Agent 1.4 – Java version

The USB drivers on the current versions of Leostream Connect are *not* compatible with previous versions of the Leostream Agents. If you update your client devices and are using Leostream to manage USB devices, you must update your Leostream Agents.

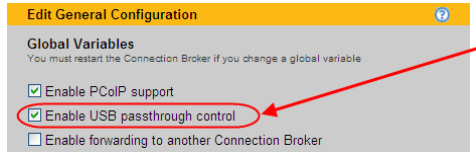


Leostream USB redirection is not supported for Linux operating systems running kernel version 2.6.35 or later.

Global Connection Broker Settings

To enable USB management in the Connection Broker:

1. Go to the **> System > General Configuration** page.
2. In the **Global Variables** section, select the **Enable USB passthrough control** option, shown in the following figure.



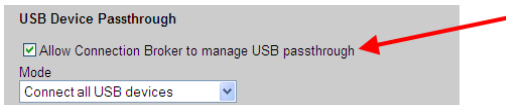
3. Click **Save**.

After you enable the global USB management feature, the following additional GUI elements are available:

- In the Connection Broker, the **USB Device Passthrough** section appears at the bottom of the **Edit Policy** page. These controls allow you to specify how to manage USB devices for users with this policy.
- In Leostream Connect, the **USB** tab appears in the **Options** dialog. In addition, options for attaching and detaching USB devices appear on the Leostream Connect system tray menu.

Policy Settings

By default, policies do not change the USB settings of the user's client. To override the client settings on a policy-by-policy basis, select the **Allow Connection Broker to manage USB passthrough** option, as shown in the following figure.



Use the **Mode** drop-down menu to constrain which USB devices end users can assign to desktops, as follows:

- **To pass through all USB devices to the desktop:** Select **Connect all USB devices**.
 Selecting this option redirects all USB devices with the exception of USB keyboards and USB mice, which are never redirected to the remote desktop.
- **To block all USB devices from being passed through to the desktop:** Select **Block all USB devices**.
 ⚠ Selecting this option blocks the keyboard and mouse from passing through to PCoIP devices. If you want to block all USB devices except the keyboard and mouse from passing through to a PCoIP device, select **Connect specific USB devices** from the **Mode** drop-down and select **Human Interface Devices** from the **Device Class** drop-down menu. Alternatively, enter the **Vendor ID** and **Product ID** of specific human interface devices.
- **To specify particular devices to pass through:** Select **Connect specific USB devices**. Specify the USB devices the Connection Broker can passthrough, as follows:
 - Select an item from the **Device Class** drop-down menu to pass through an entire class of devices.
 - Enter a **Vendor ID** and **Product ID** to pass through a specific type of device.

If you are upgrading from an old version of the Connection Broker, the device checkboxes convert to the new settings, as follows:

- **External Disk** = 08 - Mass Storage from the **Device Class** drop-downs
- **Camera** = 06 - Imaging or 0E - Video from the **Device Class** drop-down
- **Printer** = 07 - Printer from the **Device Class** drop-down
- **Security Device** = 0B - Smart Card from the **Device Class** drop-down

⚠ Leostream Connect uses port 20020 for USB traffic. Ensure that this port is open. On Windows client devices, the Leostream Connect installer automatically adds an exception for this port to the Windows Firewall. You must manually open USB port 20020 when running Norton Antivirus™ software from Symantec Corporation..

Printer Redirection

When using the Windows version of Leostream Connect, Microsoft RDP provides native printer redirection. To redirect all client printers, include the following line in the RDP configuration file found in the user's protocol plan.

```
redirectprinters:i:1
```

If you are using RDP to redirect printers, you do not need to enable printer redirection through Leostream Connect. For cases that do not use RDP or do not use RDP to redirect printers, the Connection Broker provides two methods for attaching printers to the remote desktop.

1. Redirect USB printers attached to the client
2. Assign network printers based on the client's location

Redirecting USB Printers

You can use the Windows version of Leostream Connect to redirect USB printers from the client to the remote desktop. When redirecting printers, ensure that the appropriate printer drivers are installed on the remote desktop. To enable USB printer redirection:

1. Enable Connection Broker USB device management, as described in [USB Device Management](#).
2. In the **USB Device Passthrough** section of the user's policy, select Connect specific USB devices from the **Mode** drop-down
3. Select 07 - Printer from the **Device Class** drop-down. Alternatively, you can redirect all USB devices, or specify a particular printer by vendor and product ID.

Attaching Network Printers

Connection Broker 6.2 and later allows you to attach network printers to the end user's Windows remote desktops based on the location of the client device. Using this *location-based printing* feature, you can:

- Register printers in Microsoft® Active Directory® servers with the Connection Broker
- Manually register a network printer with the Connection Broker
- Create printer plans, consisting of a group of printers with one default printer
- Assign printer plans to clients using locations defined in the Connection Broker
- Provide end-users with access to the network printers physically closest to their client device, no matter what type of client device and remote viewer protocol they are using

See "Attaching Network Printers" in the [Connection Broker Administrator's Guide](#) for complete instructions.

Drive Redirection

The Windows version of Leostream Connect supports dynamic tags for the `drivestoredirect` parameter in the Microsoft RDP file, allowing you to redirect specific drive types to the remote desktop. To use these tags:

1. Go to the protocol plan that contains the RDP configuration file that should redirect drives.
2. In the **Configuration file** edit field for RDP, remove the following line, which redirects all printers:

```
redirectprinters:i:1
```

3. Enter one of the following lines to the configuration file:

```
drivestoredirect:s:*: Redirects all drives, including any drives that are subsequently connected
```

`drivestoredirect:s:{DRIVE:CD}`: To redirect all CD drives

`drivestoredirect:s:{DRIVE:DVD}`: To redirect all DVD drives

`drivestoredirect:s:C;D;DynamicDrives`: Redirects the specified drives. In this example, the C and D drives are redirected. The `DynamicDrives` tag indicates RDP should redirect subsequently connected.

Chapter 5: Smart Card, Biometric and Proximity Card Support

Leostream Connect supports smart card, fingerprint, and proximity card authentication methods, including:

- Java™ smart cards used in conjunction with AET **SafeSign Identity Client®** software.
- ACOS5 smart cards used in conjunction with bit4id Card Manager Admin software and readers.
- Common Access Cards (CAC) used in conjunction with ActivIdentity® ActivClient™ security software.
- Smart cards compatible with the IAS (Identification, Authentication et Signature) middleware (Pilote Carte IAS), jointly developed by Dictao and Gemalto. This feature includes support for French CPS (health care professional's card) certificates.
- Fingerprint authentication when using the DigitalPersona® Pro for Active Directory® fingerprint identity solution from DigitalPersona, Inc.
- Proximity card authentication when using the XyLoc system from Ensure Technologies.

Using Smart Cards with Leostream Connect



Smart card authentication applies to the Windows version of Leostream Connect, only.

Leostream Connect supports single sign-on using a variety of smart cards and readers. When authenticating a smart card user, the Connection Broker identifies the user by matching the information on the smart card's certificate to a record in your authentication servers.

The Connection Broker attempts to identify the user based on one of the following attributes. In order:

1. Distinguished Name (DN)
2. NT Principal Name (UPN)
3. Email address

The Connection Broker begins searching for a user based on the first certificate on the card, and continues looking through the remaining certificates until it finds a match. You can alternatively allow the user to select which certificate to use for authentication by selecting the **Allow user to select certificate for smart card login** option in the **Leostream Connect Configuration** section on the **> System > General Configuration** page.

The Connection Broker assigns a policy and offers desktops based on the matched user's identity. The user is prompted for their smart card PIN when they log into their desktop.

Configuring the Connection Broker to Use Smart Cards

By default, Leostream Connect optionally allows users to authenticate via smart cards when a smart card reader is attached to the user's client. You can require or disallow smart card authentication using the **Leostream Connect Configuration** options on the **> System > General Configuration** page (see **Specifying Authentication Methods**).

Using AET SafeSign Identity Client® Software

To use Leostream Connect in conjunction with Java smart cards:

1. If necessary, install the drivers that come with your reader onto the client, to ensure that the operating system can communicate with the reader.
2. Install the client software, provided by AET, on each client and remote desktop. Leostream Connect requires this software in order to read the certificate from the card. Using the certificate, Leostream Connect identifies the user and passes that information to the Connection Broker, in order to retrieve the user's policy and desktop.
3. If you are using SSL, install the appropriate root certificate into the Connection Broker. The Connection Broker requires a certificate from an authority that recognizes the certificate on the smart card. Obtain an appropriate root certificate from your certificate authority and use your VMware virtualization layer console to load that certificate into the Connection Broker. (Do not use the > **System** > **Maintenance** page to load this certificate.)



If you are installing the AET client onto a 64-bit machine you must install the 64-bit version of the software.

Using bit4id Card Manager Admin Software

To use Leostream Connect in conjunction with ACOS5 smart cards:

1. Install the drivers that come with your reader onto each client, to ensure that the operating system can communicate with the reader.
2. Install the bit4id Card Manager Admin software onto each client and remote desktop. This software contains the SysGillo PKCS #11 software Leostream Connect requires in order to read the certificates from the card. Leostream Connect searches for this library in your client's system directory. If you do not install this library into the system directory, Leostream Connect attempts to locate the path for the library in the registry.

Using CAC with ActivIdentity ActivClient Security Software

Leostream Connect currently supports Common Access Cards (CAC) when used with the ActivIdentity ActivClient security software. To use CAC in conjunction with Leostream Connect:

1. Install the drivers that come with your smart card reader onto each client, to ensure that the operating system can communicate with the reader.
2. Install the ActivClient security software on the client and remote desktop. This software provides the DLLs required by Leostream Connect to read the x.509 certificates from the CAC.

Using IAS Middleware

To use Leostream Connect in conjunction with smart cards compatible with IAS middleware:

1. If necessary, install the drivers that come with your reader onto the client, to ensure that the operating system can communicate with the reader.
2. Install the Pilote Carte software on each client. Leostream Connect requires this software in order to read the certificate from the card. Using the certificate, Leostream Connect identifies the user and passes that information to the Connection Broker, in order to retrieve the user's policy and desktop.

Using SafeNet® iKey 1000 USB Tokens

To use Leostream Connect in conjunction with SafeNet iKey 1000 USB two-factor authentication tokens:

3. Install the drivers that come with your USB token onto the client, to ensure that the operating system can communicate with the device.
4. Install the iKey Component software on each client. Leostream Connect requires this software in order to read the certificate from the device. Using the certificate, Leostream Connect identifies the user and passes that information to the Connection Broker, in order to retrieve the user's policy and desktop.

Using Smart Cards Containing Multiple Certificates

When using Microsoft Vista® operating systems, users with a smart card containing multiple certificates can select which certificate to use for authentication. To invoke this behavior in Leostream Connect, enable the **Allow user to select certificate for smart card login** option on the > **System > General Configuration** page.

With this option enabled, when a user logs into Leostream Connect using a smart card containing multiple certificates, the following dialog opens.



Select one of the certificates and click **Login** to complete the login.

When the **Allow user to select certificate for smart card login** option is unchecked, Leostream Connect always authenticates using the first valid certificate on the smart card. Also,



If the remote desktop is not running a Vista operating system, the desktop ignores the smart card selection.

Trouble-Shooting Smart Card Connections

If smart card connections are not completing, consider the following.

- Does the smart card contain a valid certificate for the user? If the certificate does not match the domain, or the card simply does not contain a certificate, an error dialog appears.
- Is your smart card reader capable of reading all of the types of smart cards you are using?

Perform the following simple test prior to installing Leostream Connect. Insert a smart card into a reader and then establish an RDP connection to another desktop. If your reader is functioning properly, the RDP connection redirects the smart card to the destination machine. The remote desktop reads the card and prompts the user for their credentials.

Using DigitalPersona® Pro with Leostream Connect

The Connection Broker supports fingerprint authentication with Leostream Connect when using the DigitalPersona® Pro for Active Directory® fingerprint identity solution from DigitalPersona, Inc.



If using the Java version of Leostream Connect, you must use version 2.0 or higher.

When using fingerprint authentication with the Connection Broker:

1. The user enters their username and, optionally, password into Leostream Connect.
2. Leostream Connect sends the username to the Connection Broker.
3. The Connection Broker responds with the desktops to offer to that user.
4. When the user selects their remote desktops and clicks **Connect**, Leostream Connect opens a connection to that desktop. The DigitalPersona GINA opens on the remote desktop.
5. The user swipes their fingerprint, for example, using the DigitalPersona U.are.U® fingerprint reader.
6. The DigitalPersona Pro for Active Directory Workstation software redirects the fingerprint on the client to the remote desktop, and signs the user in.

If the user logs into multiple desktops, they must swipe their fingerprint on each remote desktop.

Installation Requirements

To use DigitalPersona Pro for Active Directory, install the following components:

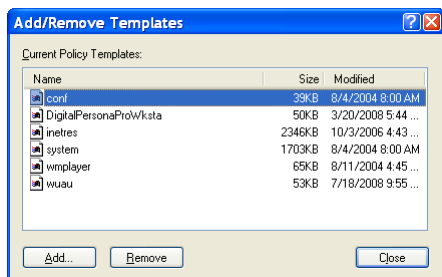
- DigitalPersona Pro for Active Directory Server 4.2.4 on your domain controller, where your Active Directory server is installed.
- DigitalPersona Pro for Active Directory Workstation 4.2.5 on your remote desktops.
- DigitalPersona Pro for Active Directory Workstation 4.2.5 on your client desktops, where Leostream Connect is installed and the fingerprint reader is connected.

Configuring DigitalPersona Pro for Active Directory Workstation Software

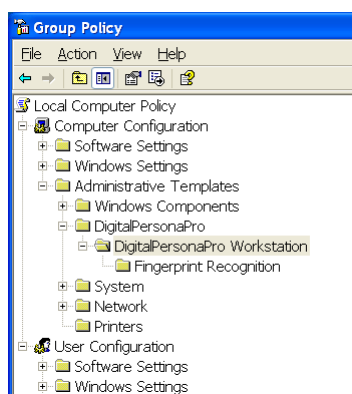
Fingerprint support with Leostream Connect requires that you allow the client desktop to redirect the fingerprint data to the remote desktop. To allow this behavior, configure the DigitalPersona Pro for Active Directory Workstation software on the client desktops, as follows:

1. Open the **Group Policy Object Editor** by running the following command:

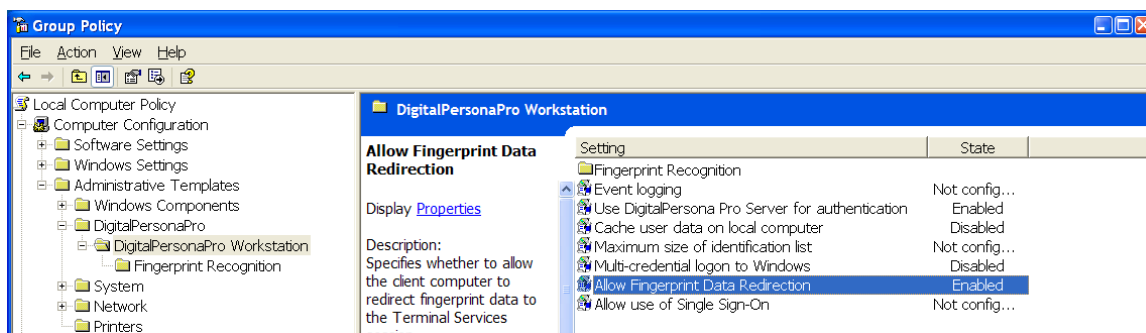
```
gpedit.msc
```
2. In the left-hand panel, open the **Computer Configuration** node, if it is not open by default.
3. Right-click on the **Administrative Templates** folder.
4. Select **Add/Remove Templates** from the right-click menu. The following dialog opens.



- In the **Current Policy Templates** list, select DigitalPersonaProWksta. This .adm file is located in C:/Windows/inf.
- Click **Add** to return to the **Group Policy Object Editor**
- In the **Group Policy Object Editor** navigate to **Computer Configuration > Administrative Templates > DigitalPersonaPro > DigitalPersonaPro Workstation**, as shown in the following figure.



- In the **Settings** list on the right-hand side, select Allow Fingerprint Data Redirection.
- Click the **Properties** link to the left of the list. The **Allow Fingerprint Data Redirection Properties** dialog opens.
- In the **Setting** tab, select the **Enabled** radio button.
- Click **OK** in the **Fingerprint Data Redirection Properties** dialog. Your **Group Policy Object Editor** appears, as follows:

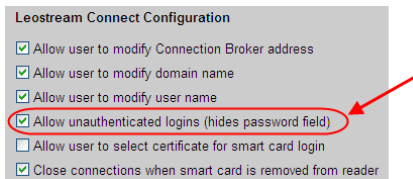


Leostream Connect does not require any specific setup to the DigitalPersona Pro for Active Directory Workstation software on the remote desktops.

Unauthenticated Fingerprint Logins

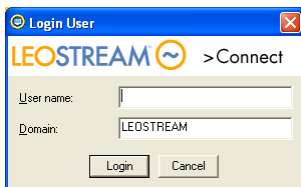
To allow a user to login using fingerprints without requiring an additional password, enable unauthenticated logins for Leostream Connect, as follows:

1. Go to the > **System > General Configuration** page. The **Edit General Configuration** page opens.
2. In the **Leostream Connect Configuration** section, select the **Allow unauthenticated logins (hides password field)** option, as shown in the following figure.



3. Click **Save** on the **Edit General Configuration** page.

In this mode, when a user opens Leostream Connect, the **Login User** dialog displays only the fields for entering their username and domain, if applicable, as shown in the following figure.



When the user clicks **Login**, the Connection Broker identifies the user based on the user name and domain, and offers the user their appropriate desktops. The remote desktop then prompts the user to swipe their fingerprint when they login.

XyLoc Proximity Card Authentication

Leostream and **Ensure Technologies** have partnered to provide an integrated proximity card solution for VDI using the Leostream Connection Broker with XyLoc proximity cards. Proximity card authentication provides ease-of-use and additional security for VDI environments. The healthcare industry, in particular, uses proximity card authentication to increase HIPAA compliance.

In the joint solution, the XyLoc software retrieves the user's information from their XyLoc proximity card and unlocks the client device. On unlock, Leostream Connect automatically grabs the user identity from the XyLoc software and logs the user into the Connection Broker. The Connection Broker then authenticates the user based on those credentials and offers the user their resources. If the user is offered a single resource, Leostream Connect automatically connects the user to their resource using single sign-on. From the user's perspective, they approach the client device and are automatically logged into their desktop.



Leostream Connect uses the personal name associated with the XyLoc card as the user login name.

To integrate the two products, first configure your XyLoc system independently of Leostream. When configuring your XyLoc users, you should select the **Must Enter Password** mode for each user. Other modes, such as the **Select User** mode can produce unexpected results under some conditions, for example, if the user manually disconnects from their desktop or if the user's password expires.

After the XyLoc software and sensors are installed on your client devices, you can add Leostream Connect, as follows.

1. Log into the client device as the XyLoc generic system user. This user should be different from any of the users that log in to Leostream.

Chapter 5: Smart Card, Biometric, and Proximity Card Support

2. Install Leostream Connect as described in the [Leostream Installation Guide](#). During the installation, ensure that you do not select any of the following extra tasks:
 - Enable Run as Shell mode
 - Enable client-side credential passthrough
 - Enable USB over IP – If your XyLoc device is attached to the client via a USB port. If XyLoc uses a different port, you may enable Leostream USB support.
3. Start Leostream Connect and configure your Connection Broker address in the **Options** dialog (see [Configuring the Connection Broker Address](#)).
4. Add Leostream Connect to the list of programs that run on logon.
5. Log out of the client device.

When a user approaches the client with an active XyLoc proximity card, the client device automatically unlocks and Leostream Connect automatically logs the user into their remote desktop, if the Connection Broker offers them a single desktop. By default, when the user with the XyLoc card moves away from the client device, the XyLoc software locks the client device and Leostream Connect automatically disconnects the user from their desktop.

The XyLoc sensor attached to the client device occasionally loses connection with the user's XyLoc proximity card even though the user remains near the client device. In these cases, the XyLoc system locks the screen and Leostream disconnects the user's desktop. As soon as the XyLoc sensor picks up the proximity card, the user reconnects to their desktop without losing work. However, the end-user experience suffers due to the delay in reconnecting to the session.

You can improve the end-user experience by instructing Leostream to keep the desktop connection open for a pre-defined period of time, as follows.

1. Open the Registry Editor on the client device
2. Navigate to the following key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Leostream\Leostream Connect
```
3. Inside of this key, add a new `DWORD` value
4. Name the value `DisconnectOnLockTimeout`
5. Set the value's data, in decimal, to the number of seconds to keep the user's connection open after the XyLoc system locks the users screen. You can delay the disconnect for up to one hour, or 3600 seconds.

For example, with the `DisconnectOnLockTimeout` value set to 20, when the user turns away from the client device and blocks their XyLoc card from the sensor, the XyLoc software locks the client device, but Leostream Connect keeps the user's desktop session open. If, within 20 seconds, the user turns back to the client device and re-establishes the connection between the proximity card and sensor, XyLoc unlocks the screen and the user instantly sees their desktop connection. If the user does not re-establish the connection between the proximity card and sensor in 20 seconds, Leostream Connect disconnects the user's desktop session.

By default, Leostream Connect operates in conjunction with XyLoc on any client device where both products are installed. You can uncouple the two products, as follows.

1. Open the Registry Editor on the client device
2. Navigate to the following key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Leostream\Leostream Connect
```
3. Inside of this key, add a new `DWORD` value
4. Name the value `XyLocSupportEnabled`

5. Set the value's data to zero.

HID Proximity Card Authentication with RF IDEas pcProx© Readers

Leostream Connect version 2.8 seamlessly integrates with the **RF IDEas pcProx© proximity card readers**, allowing users with existing HID proximity cards to connect easily to the Leostream Connection Broker and backend resources.



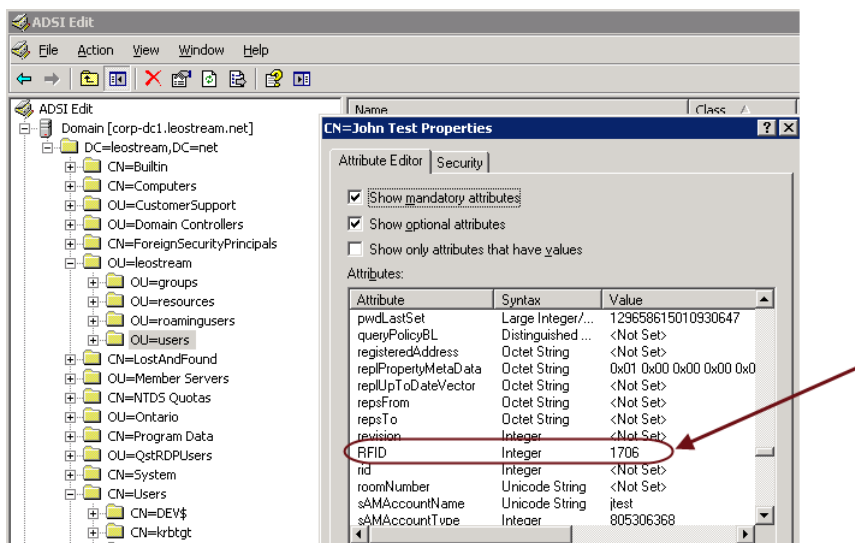
Leostream currently supports the USB model of the RF IDEas pcProx© readers. The serial versions of the pcProx Readers is not supported.

Active Directory Setup

In order for Leostream to associate a proximity card ID with a particular user, you must add a custom Active Directory attribute to your authentication server and register each user's ID in that attribute.

You can use the Active Directory Schema editor to add the attribute and assign it to the appropriate class. Please consult your Active Directory documentation for more information.

After adding the attribute, use the ASDI Edit snap-in to assign values to the new attribute for each user. For example, the following figure shows a value assigned to the new attribute **RFID** for the John Test user.



Enabling Proximity Card Logins in the Connection Broker

To allow users to log in using proximity cards, enable the feature, as follows.

1. Go to the > **System > Settings** page.
2. From the **Authentication Menu** in the **Leostream Connect Configuration** section, shown in the following figure:

Proximity card logins are considered username/password logins. The user is prompted for their password when they tap their proximity card.

Select this option to indicate the Connection Broker should determine the username based on the provided proximity card ID.

Leostream Connect Configuration

- Allow user to modify Connection Broker address
- Allow user to modify domain name
- Allow user to modify user name
- Allow unauthenticated logins (hides password field)
- Allow user to select certificate for smart card login
- Close connections when smart card is removed from reader
- Exit client after connection to resource is established
- Log out user after last connection is closed (opens Login dialog)

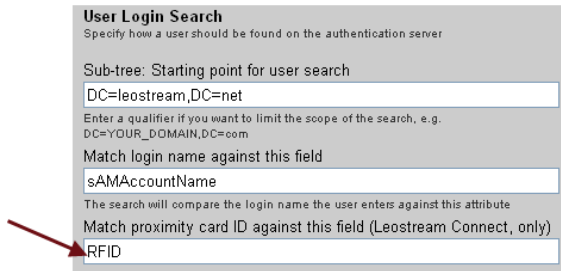
Show additional login button (Java client only):

Upgrade client to latest version:

Authentication methods:

- Smart card
- Username/password prompt
- Use proximity card ID to look up username
Setting this option hides the username field

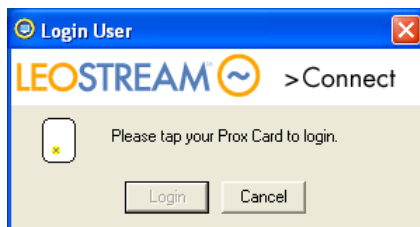
- a. Select **Require** from the drop-down menu
 - b. Select the **Username/password prompt** option
3. Select the **Use proximity card ID to look up username** option, as shown in the previous figure. By default, when the user taps their proximity card, Leostream Connect logs the user in and that user remains logged in until they manually log out of the client. If you want users to be able to log out by tapping their proximity card a second time, select the following options.
- a. **Close connections when smart card is removed from reader:** With this option selected, Leostream Connect interprets the second tap as a “smart card removal” and automatically disconnects the user from all their open desktops.
 - b. **Log out user after last connection is closed (opens Login dialog):** With this option selected, after the **Close connections when smart card is removed from reader** option disconnects from all desktops, Leostream Connect automatically logs out the user.
4. Click **Save** on the **Edit Settings** form.
5. For the Connection Broker to map proximity card IDs to usernames, you must tell the Connection Broker the name of the Active Directory attribute that contains the card IDs, as follows.
- a. Go to the **> Users > Authentication Servers** page.
 - b. Edit the Active Directory authentication server associated with your users.
 - c. In the **Edit Authentication Server** form, scroll down to the **User Login Search** section.
 - d. Enter the attribute name into the **Match proximity card ID against this field (Leostream Connect, only)** field, as shown in the following figure.



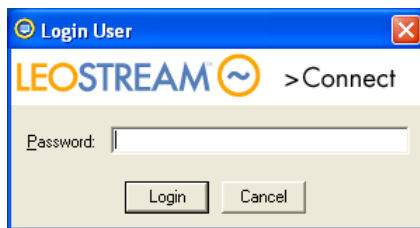
6. Click **Save** on the **Edit Authentication Server** form.

Logging in with Proximity Cards

Leostream Connect launches with the following prompt when your Connection Broker is configured to proximity cards.



After the user taps their proximity card, they are prompted for their Active Directory password, as shown in the following figure.



Leostream Connect passes the user's proximity card ID and password to the Connection Broker. The Connection Broker identifies the user by matching that ID against the IDs registered in your custom Active Directory attribute. After the Connection Broker finds a match, it authenticates the user using their username and password, and sends the username back to Leostream Connect.

After the user taps to log out of their desktop, Leostream Connect reopens the **Login User** dialog, if your Connection Broker settings are configured as described in step 3 in the previous section.

Chapter 6: Using the Microsoft® Windows® version of Leostream Connect

Running Leostream Connect and Connecting to Resources

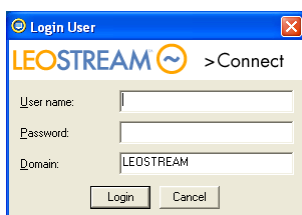
To run Leostream Connect, double-click on the Leostream Connect icon. For instructions on running Leostream Connect from the command line, see [Running Leostream Connect for Windows from the Command Line](#).

Logging into Leostream Connect

The appearance of the **Login User** dialog depends on the Connection Broker configuration.

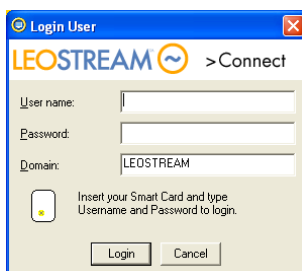
Authenticating with Username/Password

If you can authenticate with a username/password, the **Login User** dialog appears as shown in the following figure. The **Domain** field can be either an edit field or a drop-down menu containing the list of available domains.



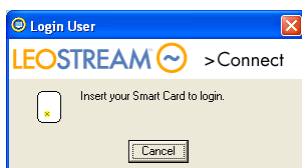
Authenticating with Username/Password and Smart Cards

If you must provide a username/password and enter a smart card, the following dialog opens.



Authenticating with Smart Cards

If you authenticate using only a smart card, the **Login User** dialog appears as shown in the following figure.



Insert your smart card into the smart card reader to log into Leostream Connect. If an invalid or unknown smart card is inserted into the reader, Leostream Connect issues a warning.

Authenticating with Fingerprints

If you can authenticate using a fingerprint reader, login to Leostream Connect as directed by the **Login User** dialog. After you log into Leostream Connect, a dialog on the remote desktop prompts you to swipe your fingerprint.

Accessing the Login Menu from the System Tray

You can use the Leostream Connect system tray menu to access the **Login User** dialog, as follows:

1. Right-click on the Leostream Connect icon in the system tray.
2. Select the **Login** option.

If a user is already logged into Leostream Connect, the system tray menu does not contain a **Login** option. Instead, select the **Switch User** option to open the **Switch User** dialog, which allows a new user to log into Leostream Connect.

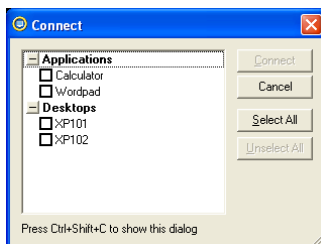
In the dialog that opens:

1. Enter any necessary credentials, such as username, password, domain, etc.
2. Click **Login**.

Connecting to Desktops and Applications

By default, if the Connection Broker offers you a single desktop or application, Leostream Connect automatically connects you to that resource when you log into the client. You can change this default by unchecking the **Connect to desktop after login** option on the Leostream Connect **Options** dialog (see [Setting Login Options](#)).

If you have more than one desktop or application, Leostream Connect opens the **Connect** dialog, listing your available connections, as shown in the following example.



To connect to one or more of your desktops and applications:

1. Check the box before each resource. Alternately, click **Select All** to select all items.
2. Click **Connect**.

Leostream Connect opens a remote viewer session to each selected desktop and application.

If you click **Cancel** on the **Connect** dialog, Leostream Connect continues to run and you remain logged into the Connection Broker, but you will not connect to any resources. Select **Connect Multiple** from the system tray menu or press Ctrl-Shift-C to reopen the **Connect** dialog and connect to your resources.



Leostream Connect performance may be slow when connecting to VMs with very low memory.

Using Shell Mode

You can install Leostream Connect in shell mode by selecting the **Enable Run as Shell mode** task in the Installation Wizard. In this mode, `LeostreamConnect.exe` replaces `explorer.exe` in the `winlogon Shell` registry key. After a user logs into their physical client device, the Leostream Connect **Login User** dialog automatically opens. When the user logs out of their last desktop, the login dialog automatically reopens.

When the user boots a client device that has Leostream Connect installed in shell mode, Leostream Connect waits for the network to be available before opening the **Login** dialog. If the client device is experiencing networking problems, Leostream Connect opens an appropriate warning.



In shell mode, Leostream Connect must be able to communicate with the Connection Broker. If Leostream Connect cannot communicate with the Connection Broker and you are defined as an administrator on the client device, Leostream Connect prompts you for a new Connection Broker address. Otherwise, you must manually open the **Options** dialog and configure the Connection Broker address (see [Changing the Connection Broker Address](#)).

- If your Connection Broker uses a static IP address, enter this address into Leostream Connect as described in [Configuring the Connection Broker Address](#).
- Otherwise, ensure that you have a DNS SRV record for your Connection Broker and check the **Obtain Connection Broker address automatically** option on the **General** tab of the Leostream Connect **Options** dialog.

Using Quick-Key Options in Shell Mode

When Leostream Connect is running in shell mode, you cannot access the Leostream Connect System tray menu. Instead, use the hover menu or the following key combinations to access Leostream Connect dialogs.

- `Ctrl-Shift-C`: Opens the **Connect** dialog, where you can launch additional desktops and applications.
- `Ctrl-Shift-L`: Locks the client workstation running Leostream Connect, if the **Allow user to lock client workstation** option is selected on the Connection Broker > **System** > **Settings** page.
- `Ctrl-Shift-M`: Opens the **Manage** dialog, where you can manage another user's resources.
- `Ctrl-Shift-O`: Opens the **Options** dialog, where you can modify the Connection Broker address and USB options.
- `Ctrl-Shift-X`: Exits shell mode.

Using the Shell-Mode Hover Menu

The Leostream Connect System Tray menu provides options for connecting to and disconnecting from desktops, as well as attaching and detaching USB devices and managing Leostream Connect options. When running in shell mode, end users do not have access to the System Tray. Instead, they can use the Leostream Connect hover menu.

To access the hover menu, move and hold the cursor at the left-most edge of the primary display for two seconds. You can change the 2 second delay by modifying the following registry key. The registry key values are in milliseconds.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Leostream\Leostream Connect\HoverMenuEnabled
```

The content of the hover menu is identical to that of the System Tray menu. See [Using the Leostream Connect System Tray Menu](#) for information on using this menu.



The **Exit** menu closes all desktop connections and logs the user out of the client device.

If users do not need access to the Leostream Connect menu, set the `DWORD` value of the following registry key to zero.

`HKEY_LOCAL_MACHINE\SOFTWARE\Leostream\Leostream Connect\HoverMenuEnabled`

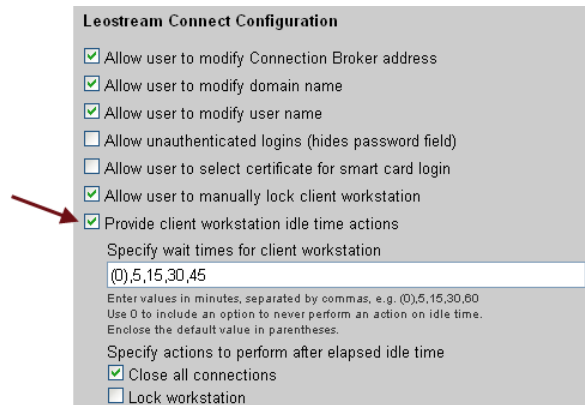
Using Client-Side Idle Actions

Connection Broker 7.5.40 includes beta functionality to provide users with actions they can automatically invoke after their client is idle for a specified length of time.



This feature requires the 2.9 beta version of Leostream Connect for Windows. Please, contact support@leostream.com for information on this client.

To enable client-side idle time actions, select the **Provide client workstation idle time actions** option on the Connection Broker > **System** > **Settings** page, shown in the following figure.



After selecting this option, additional settings appear that allow you to configure the default behavior for the user's client, as follows:

1. In the **Specify wait times for client workstation** field, enter all the possible wait times the user can select from. Use a zero (0) to indicate the user has the option to never perform an action no matter how long the client is idle. All wait times are entered in minutes.

Enclose the default value in braces, for example {0}.
2. In the **Specify actions to perform after elapsed idle time**, indicate the default actions Leostream Connect takes after the client passes its specified idle time.
 - The **Close all connections** option automatically closes all open desktop connections without prompting the user.
 - The **Lock workstation** option automatically locks the client workstation. If Leostream Connect is not installed in shell mode, the native Windows locking mechanism is used. If Leostream Connect is running in the Windows shell, Leostream Connect uses its own locking mechanism.

Locking the Session

When running in shell mode, a generic (or *kiosk*) user typically logs into the client workstation. Individual users, not kiosk user, then log into Leostream Connect. If the user who logged into Leostream Connect uses the Windows lock feature to lock the client workstation, that user must know the kiosk user's password in order to unlock the client.

To solve the problem of sharing the kiosk user's password with all users, you can enable client-side locking on

Chapter 6: Using the Microsoft Windows version of Leostream Connect

Leostream Connect. Client-side locking allows the user who is logged into Leostream Connect to lock the client workstation using the Leostream lock feature. The user then enters their own password to unlock the client.

To enable client-side locking, select the **Allow user to lock client workstation** option on the Connection Broker > **System** > **Settings** page.

With the previous option selected, when a user logs into Leostream Connect, the Leostream system tray menu contains a **Lock Workstation** option. Selecting this option, or using the hot-key combination `Ctrl-Shift-L` locks the client workstation and opens the Leostream Connect **Unlock** dialog. The user must enter their password into the **Unlock** dialog to unlock the client workstation.



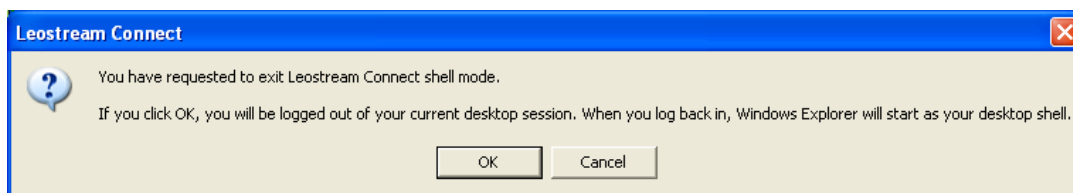
Only the user that locked the client workstation can unlock Leostream Connect.

Changing the Connection Broker Address

To point Leostream Connect at a different Connection Broker, press `Ctrl-Shift-O` to open the **Options** dialog. Use the settings on the **General** tab to change the Connection Broker address (see [Configuring the Connection Broker Address](#)).

Exiting Shell Mode

To exit shell mode, press `Ctrl-Shift-X`. Leostream Connect prompts you to confirm that you want to exit shell mode, as shown in the following figure.



Click **OK** to exit shell mode. Leostream Connect automatically logs out the current session. You must log back in to access the `explore.exe` shell.

When you log back in, Leostream Connect no longer runs in shell mode. Ensure that your Connection Broker is properly running; start Leostream Connect; and confirm that the IP address used by Leostream Connect is correct before returning to shell mode.

Client-Side Credential Passthrough

When repurposing desktops and laptops as VDI clients, end users must provide their credentials in two places:

1. When logging into their physical client device.
2. When logging into their VDI client.

Leostream Connect credential passthrough shrinks the two step process into a single login, allowing end users to seamlessly launch their remote desktops directly after logging into their physical client device.

Credential passthrough is most effective when used in conjunction with Leostream Connect in shell mode. With these two features working together, you can lock down your fat desktops and laptop, turning them into repurposed thin clients.

To enable credential passthrough, install Leostream Connect with the **Enable client-side credential passthrough** task selected in the Installation Wizard (see the [Leostream Installation Guide](#)).

Example: Credential Passthrough with Shell Mode

If you install Leostream Connect in shell mode and with credential passthrough, end users experience the following behavior.


1. The user boots up their desktop/laptop and see the normal Windows login prompt.
2. The user enters their credentials into the Windows login prompt.
3. Because Leostream Connect is in shell mode and using credential passthrough, after the user logs in, Leostream Connect automatically starts up (without presenting a login dialog), grabs the user's Windows logon credentials, and passes those credentials to the Connection Broker.
4. If the user's policy offers them a single desktop, Leostream Connect automatically launches the remote session. If the user's policy offers them multiple resources, Leostream Connect offers the list of resources.
5. When a remote session is launched, Leostream Connect automatically signs the user into the remote session. From an end user's perspective, it's as if their original Windows login, logged them directly into the remote session.
6. When the user logs out of the remote session, they are logged out of Leostream Connect and the physical client device, going back to the original Windows login screen.

If credential passthrough is on but Leostream Connect is not in shell mode, after the user logs into their client device, they must manually launch Leostream Connect. At this point, Leostream Connect automatically starts up (without presenting a login dialog), grabs the user's Windows logon credentials, and passes those credentials to the Connection Broker. For security reasons, after the first login, end user's must re-enter their credentials to log into Leostream Connect.

Configuring Options on Microsoft® Windows® Operating Systems

Use the Leostream Connect **Options** dialog to set logging, USB, and Connection Broker options. You must start Leostream Connect to access the **Options** dialog.

To configure Leostream Connect options:

1. Right-click on the Leostream Connect icon  running in the system tray.
2. Select **Options....** The **Options** dialog opens.

The remaining sections describe the different Leostream Connect options available on Windows operating systems.

General Options

Setting Login Options

The **Leostream Connect Startup** section on the **General** tab contains options that control Leostream Connect behavior when the user logs in. In general, leave these options selected to provide the smoothest end-user experience.

- **Login to Connection Broker:** Indicates if Leostream Connect opens the **Login User** dialog when they start Leostream Connect. If you do not select this option, after the user starts Leostream Connect they must select the **Login** option from the Leostream Connect system tray menu to log in.
- **Login automatically when Smart Card is inserted:** If checked, when the user starts Leostream Connect, the client automatically logs in the user if a smart card reader is attached and a valid smart card is inserted in the reader. This option appears only if the **Smart card** authentication method is selected in the **Leostream Connect Configuration** section of the **> System > General Configuration** page.
- **Connect to desktop after login:** Indicates if the remote viewer session starts immediately after a successful

login. When enabled, if the Connection Broker assigns one desktop to the user, Leostream Connect immediately launches a remote session to that desktop. If the Connection Broker assigns multiple resources, Leostream Connect always opens the **Connect** dialog regardless of how this option is set. If this option is disabled, the user must use the system tray menu to connect to their resources.

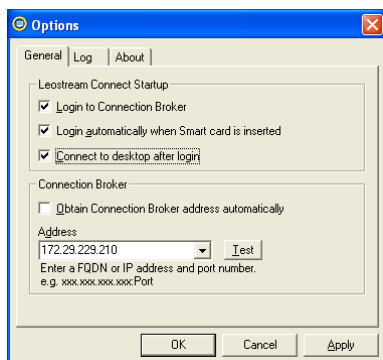
 Do not disable the **Connect to desktop after login** option if Leostream Connect runs in shell mode.

Configuring the Connection Broker Address


By default, Leostream Connect searches for a DNS SRV record associated with your Connection Broker. See the Leostream **DNS Setup Guide**, available on the Leostream Downloads and Documentation Web site, for instructions on creating an appropriate DNS entry for your Connection Broker. After the client starts and locates the record, it retains the record's information for the length of the TTL associated with the record. After the TTL expires, Leostream Connect requeries the DNS SRV record.

If a DNS SRV record does not exist, or the Leostream Connect cannot communicate with the Connection Broker, the client displays a warning message. In this case, you must either configure a DNS SRV for your Connection Broker, or hard-code the Connection Broker address into each Leostream Connect installation. To enter a specific Connection Broker address:

1. Select the **General** tab, shown in the following figure.



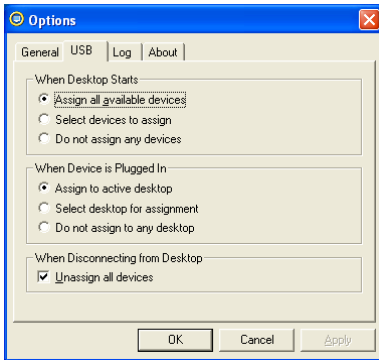
2. Uncheck the **Obtain Connection Broker address automatically** option.
3. Enter the Connection Broker's fully qualified domain name (FQDN) or IP address in the **Address** edit field.
3. To test the Connection Broker address, click **Test**. A message opens, indicating if Leostream Connect was able to communicate with the Connection Broker.
4. Click **Apply** to store the changes and continue working with the **Options** dialog, or click **OK** to apply the changes and close the dialog.

 Only administrators can save changes to the Connection Broker address. Other users can modify the address for their current session, however, Leostream Connect does not store the address for future sessions. Windows 7 requires elevated privileges to run Leostream Connect as an administrator. See the Leostream Knowledge Center article "How do I change the Connection Broker address in Leostream Connect when the client is installed on Windows 7?" for more information.

USB Options

The **Options** dialog contains a **USB** tab only for users who log in with a policy that allows the Connection Broker to manage USB devices.

For Leostream Connect Version 2.1 and higher, the **USB** tab, shown in the following figure, allows you to control how USB devices are assigned to your desktops.



Assigning USB Devices When You Connect to Your Desktop

Options in the **When Desktop Starts** section allow you to configure what happens to existing USB devices when you connect to a desktop. You can choose from the following three options.

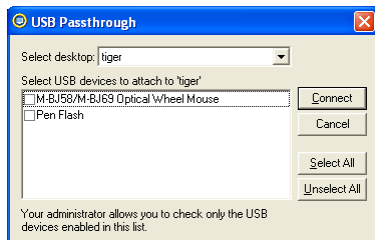
Option 1: Assign all available devices: Select this option to associate all USB devices with one desktop. If you connect to multiple desktops, the Connection Broker attaches the USB devices to the first connected desktop.

Option 2: Select devices to assign: Select this option if you want to select particular USB devices to associate with one of your desktops.



Ensure that you select option 2 if you are allowed to connect all USB devices to your remote desktop *and* you use a USB mouse or USB keyboard. Otherwise, Leostream Connect automatically redirects the mouse and keyboard to the remote machine.

With this option selected, after you select the desktop to connect, the following dialog opens:



To select USB devices:

1. Select the desktop to connect USB devices to from the **Select desktop** drop-down menu.
2. Check the boxes before the USB devices to assign to your desktop. If a device is disabled in the list, your administrator does not allow you to pass through this type of device to your connected desktops.

Mouse over any USB devices to learn more about this particular device.

3. Click **Connect** to launch a remote viewer to your connected desktops and assign USB devices. Click **Cancel** to stop connecting to desktops.

Option 3: Do not assign any devices: Select this option if you do not want to assign any USB devices to any of your desktops.

Assigning New USB Devices

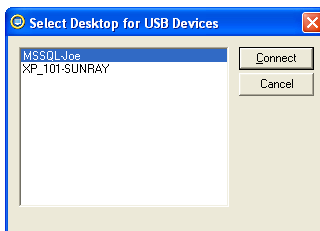
Options in the **When Device is Plugged In** section allow you to configure what happens when you connect another USB device to your client after you are connected to a desktop. You can choose from the following three options.

Option 1: Assign to active desktop: Select this option to associate new USB devices with the desktop you are currently working with, i.e., the desktop whose remote viewer session is currently maximized.

✓ When you use this option, a remote viewer session must be open on your screen. Leostream Connect will not assign new USB devices to any desktop if you minimize all your remote viewer sessions.

Option 2: Select desktop for assignment: Use this option to select which desktop to associate new USB device with, as follows:

- If you are connected to a single desktop, Leostream Connect assigns the new USB device to this desktop.
- If you are connected to multiple desktops, Leostream Connect opens the following dialog, where you can select the desktop for attached USB devices.



Option 3: Do not assign to any desktop: Select this option if you do not want to passthrough a new USB device to any of your connected desktops.

Unassigning USB Devices

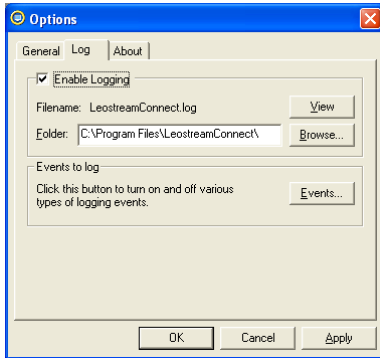
Leave the **Unassign all devices** option checked to ensure that USB devices can be reassigned to new desktops when you disconnect from its currently assigned desktop.

Leostream Connect automatically unassigns all USB devices when you exit Leostream Connect.

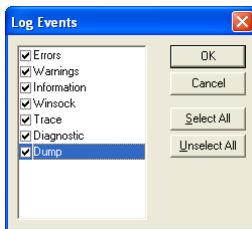
Log Options

To log Leostream Connect operations for debugging purposes:

1. Select the **Log** tab, shown in the following figure.



2. Ensure that the **Enable Logging** option is selected, the default.
3. Enter a destination folder for the logs in the **Folder** edit field. Leostream Connect stores log files in this directory in a file named LeostreamConnect.log.
4. Click the **Events** button to configure the type of information to store in the Leostream Connect logs. The **Log Events** dialog, shown in the following figure, opens.



- a. Select the events to log. Use the **Select All** button to check all options, and the **Unselect All** option to remove all selections
- b. Click **OK** to store any changes, or **Cancel** to exit the dialog without saving your new selections



Ensure that the **Diagnostic** events are selected when creating logs to send to Leostream Support.

5. To view the log file, at any time, click **View**.
6. Click **Apply** to store the changes and continue working with the **Options** dialog, or click **OK** to apply the changes and close the dialog.


Leostream Connect first attempts to write the log in the directory entered in the **Folder** edit field. If it cannot write to this directory, Leostream Connect attempts to write the log into one of the following directories, in order:

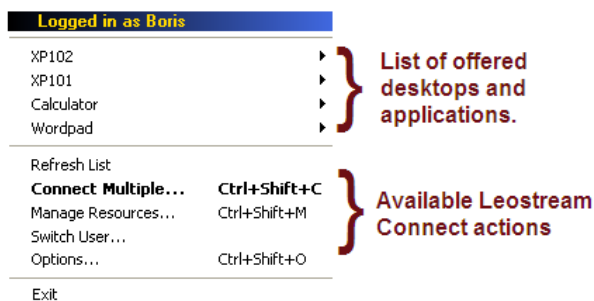
1. The Leostream Connect installation folder
2. A folder named `temp` inside the Leostream Connect installation folder
3. The user's `temp` folder
4. The `root` folder

About Options

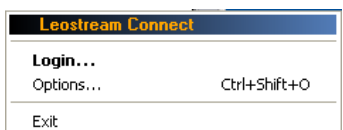
The **About** tab contains information about your Leostream Connect installation, including version number, installed options, and links to relevant Leostream Web pages.

Using the Leostream Connect System Tray Menu

Leostream Connect appears as an icon in your system tray whenever the client is running. Right-click on the Leostream Connect  icon to access the Leostream Connect system tray menu. If you are currently logged into Leostream Connect, the menu lists your available desktops and applications, followed by a list of actions, for example:



If you are not logged in, the system tray menu contains a **Login** option, as shown in the following figure.

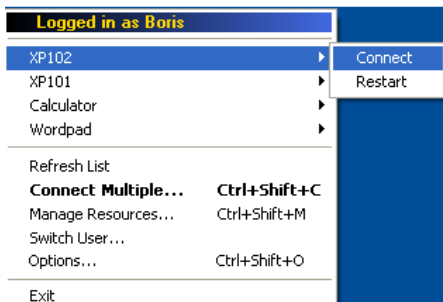


Use the **Login** option to log into the Connection Broker so that you can connect to your desktops.

Connecting to Desktops and Applications Using the System Tray Menu

After you log in to Leostream Connect, you can use the system tray menu to access the desktops and applications offered to you by the Connection Broker, as follows:

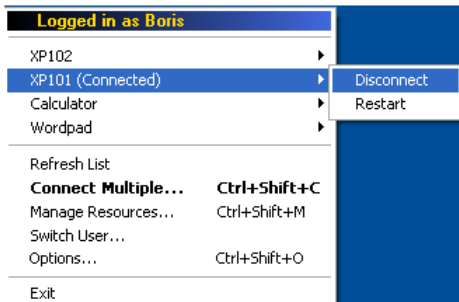
- To connect to a particular desktop, select the name of the desktop and select **Connect**, as shown in the following figure.



If the **Connect** menu is disabled, you are already assigned to the maximum number of desktop allowed by the Connection Broker. To launch another desktop, you must first release one of your existing desktops.

- To restart a desktop, select the **Restart** option, shown in the previous figure.

- To update your list of offered resources, select the **Refresh List** menu item.
- To simultaneously connect to a number of desktops and applications, select **Connect Multiple** to open the **Connect** dialog.
- To disconnect from a connected desktop, select the **Disconnect** or **Disconnect and Release** option associated with that desktop. Depending on the settings in your assigned Connection Broker policy, your system tray menu may not contain the **Disconnect and Release** option, as shown in the following figure.



You cannot use Leostream Connect to disconnect from applications. Use the application's native **Exit** feature.

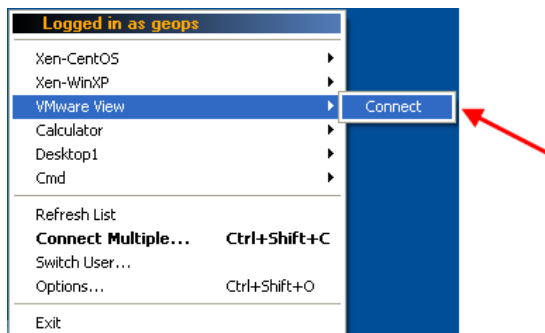


When running Leostream Connect in shell mode, the **Exit** menu closes all desktop connections and logs the user out of the client device.

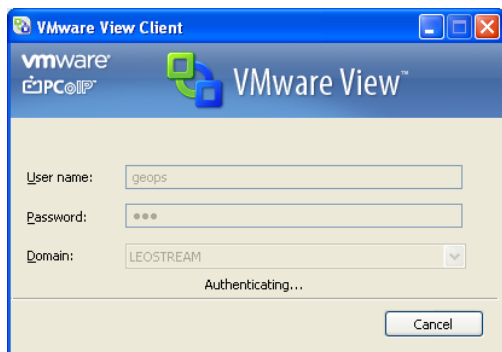
Connecting to VMware View Connection Servers

To connect to a VMware View server, the client device must have an installed VMware View client. If you are using Leostream to manage USB devices, do not install the USB component of the VMware View client.

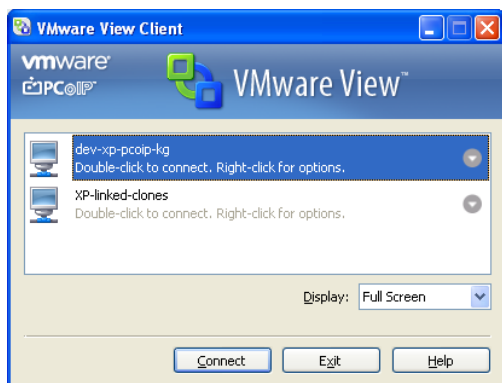
If your policy is configured to offer VMware View Servers, the Leostream system tray menu contains an entry for View, as shown in the following figure.



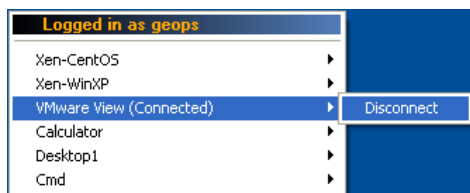
Select the **Connect** option associated with View to log in to the VMware View Client. The VMware View Client displays the authentication process, as shown in the following figure.



After the authentication succeeds, the View Client displays the desktop pools that you are entitled to use, as configured in the View Manager, for example.




The VMware View Manager completely configures and controls all desktop connections started from the View Client. After logging in to the VMware View Client, the Leostream System Tray menu displays a **Disconnect** menu, as shown in the following figure.



Selecting **Disconnect** logs out of the View Client and disconnects any desktop connections that were launched from the View Client. Leostream power control and release plans are not invoked on desktops launched from VMware View.

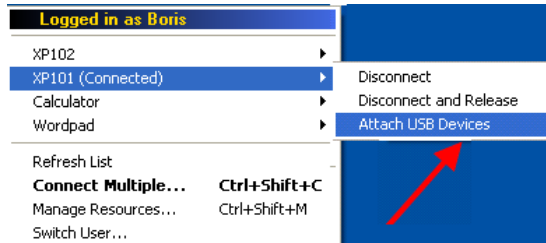
Managing USB Devices Using the System Tray Menu

After you are connected to a remote desktop, you can use the system tray menu to attach and detach USB devices.

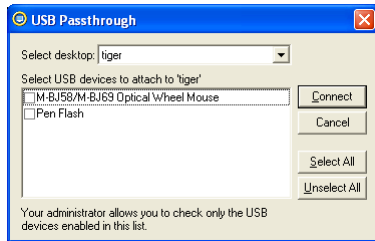
 Leostream Connect does not control how the devices or any associated applications run or perform on the remote desktop.

To attach a USB device:

1. Right-click on the Leostream Connect icon in the system tray.
2. Select the name of a connected desktop to attach the USB device to.
3. Select **Attach USB Devices**, as shown in the following figure.



The **USB Passthrough** dialog, shown in the following figure, opens.



✓ If a USB device is missing from the USB Passthrough list, the device was likely grabbed by another application running on the client device. For example, Skype may grab a Webcam, making the camera invisible to Leostream Connect. Unplug and replug in the device while Leostream Connect **USB Passthrough** list is displayed, to allow Leostream Connect to see the device.

4. To select the USB devices to attach.
 1. Check the box before the desired USB devices to assign to your desktop.
 2. Mouse over any USB devices to learn more about this particular device.
 3. Click **Connect**.

If you previously attached the selected USB device to another desktop, Leostream Connect prompts you to confirm that you want to move this USB device to the new desktop.

To detach a USB device from a desktop:

1. Right-click on the Leostream Connect icon in the system tray.
2. Select the name of the desktop to detach the USB device from.
3. Select **Detach USB Devices**.
4. In the dialog that opens, select the USB devices to detach.
5. Click **OK**.

Managing Resources

If you log into the Connection Broker with a role that has the **Allow user to manage another user's resources** option selected, the Leostream Connect system tray menu contains a **Manage Resource** option. This feature allows you to log into desktops using credentials other than those you provided to the Connection Broker.

Managing resources allows you to perform administrative tasks on desktops, including:

- Reviewing the list of desktops that the Connection Broker offers to another user.

- Logging into a desktop that is offered to another user, to perform administrative tasks on that desktop.
- Logging into one of your own desktops using different credentials from what you provided to the Connection Broker.

How the Connection Broker Determines the Offered Resource List

When you manage a user's resources, the Connection Broker offers you resources based on that user's policy. Which policy the Connection Broker assigns to that user is determined by the **Assigning User Role and Policy** section found in each authentication server in the Connection Broker, an example of which is shown in the following figure.

Order	Group	Client Location	User Role	User Policy
1	Sales	LSC	User	Default
2	Operations	All	User	Blade and VM

As the previous figure shows, the policy selected in the **User Policy** drop-down menu, is assigned to the managed user based on their membership in a particular group in the authentication server (the selection in the **Group** drop-down menu), and the location of their client (the selection in the **Client Location** drop-down menu).

After the Connection Broker knows the managed user's policy, it looks only at the following sections of this policy. All other aspects of the managed user's policy are ignored.

- The **Filters** section for constraining which desktops to pull from all desktop pools.
- The **When User Logs into the Connection Broker** section for all pools in the **Desktop Assignment from Pools** section, with the exception of the **Allow users to reset offered desktops** option. You cannot use Leostream Connect to restart a managed desktop.
- The selection in the **Protocol** plan drop-down menu for each pool.
- The **Application Assignment from Pools** section.
- In the **Desktop Hard Assignments** section, the **Display to user as** and **Protocol** plans drop-down menus.

Based on these sections, the Connection Broker offers you the following resources to manage.

- All desktops hard-assigned to the managed user.
- Any Citrix XenApp applications contained in the application pool selected in the **Application Assignment from Pools** section of the managed user's policy.
- For each pool in the **Desktop Assignment from Pools** section of the managed user's policy, the desktops determined by the **When User Logs into the Connection Broker** section, shown in the following figure, after any constraints in the **Filters** section have been applied.

In the previous figure, the Connection Broker offers three desktops from the pool named Xen. These desktops must be running, but are not required to have an installed, running Leostream Agent. The desktops are offered by name.

When determining which three desktops to offer from the pool, the Connection Broker always offers any desktops that

are already assigned to the managed user. The Connection Broker then picks the remaining desktops based on the availability of desktops in the pool. Because the Connection Broker can choose any unassigned desktop from the pool, you may not see exactly the same list of desktops as would be offered to the user.

Connecting to a Managed Resource

The Connection Broker connects you to the managed desktop using the protocol determined by the protocol plan in the managed user's policy. If the managed user typically connects to their desktops using HP RGS, you must log into their desktop from a client that supports RGS.

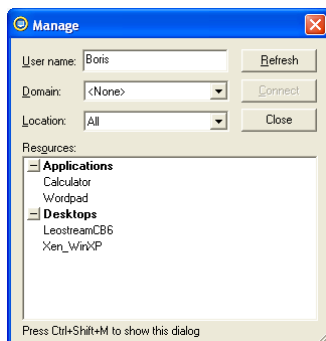
When you log into a managed resource, the Connection Broker does *not* assign that resource over to you. Because you are not assigned to the desktop:

- The Connection Broker does not honor any settings in the **When User is Assigned to Desktop** section of the managed user's policy.
- The Connection Broker does not use the selections in the **Power control** or **Release** plan drop-down menus in the managed user's policy.
- You do not appear in the **User** column for that desktop in the Connection Broker > **Resources** > **Desktops** page.
- You will not appear in any resource usage reports run from the Connection Broker > **Status** > **Reports** page.

Managing Your Own Resources


Managing your own resources allows you to log into your offered desktops using different credentials from what you provided the Connection Broker. If your Connection Broker account does not have administrative privileges for your desktop, you can use the manage resource feature to, for example, log into your desktop using administrator credentials. To manage your own resources:

1. After you log into Leostream Connect, select the **Manage Resources** menu from the system tray menu. The **Manage** dialog, shown in the following figure opens.



By default, the **Resources** list shows your offered applications and desktops.

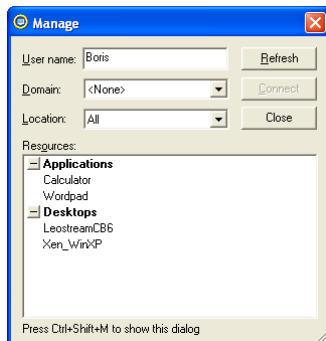
2. To manage one of your desktops:
 - a. Select the appropriate desktop from the **Resources** list. You can connect to one desktop at a time.
 - b. Click **Connect**. Leostream Connect launches a remote session to that desktop, but does not sign you in. Instead, the Login dialog appears for that desktop.
 - c. Enter credentials to log into the desktop. These can be the credentials for any user that has rights to log into this desktop.
3. To manage another desktop, repeat step 2.

 You can reopen the **Manage** dialog at any time by pressing `Ctrl-Shift-M`.

Managing another User's Resources

Managing another user's resources allows you to perform administrative tasks on the user's desktop. The user's policy determines which resources are offered to them by the Connection Broker. The policy the Connection Broker chooses to assign to the user depends on the domain the user logs into, and the location the user logs in from. To accurately obtain a list of resources offered to a particular user, you must enter this information, as follows.

1. After you log into Leostream Connect, select the **Manage Resources** menu from the system tray menu. The **Manage** dialog, shown in the following figure opens.



2. To get the list of desktops offered to a particular user, simulate that user logging into the Connection Broker:
 - a. Enter the user's login name in the **User name** edit field.
 - b. Select the domain to log the user into from the **Domain** drop-down menu.

The user must be in a domain defined by one of your Authentication Servers. You cannot manage resources for a user that is defined locally in your Connection Broker.
 - c. Select the user's location from the **Location** drop-down menu. This menu contains all the locations defined in the Connection Broker > **Clients** > **Locations** page.
 - d. Click **Refresh**.

The **Resources** list updates to show the applications and desktops that would be offered to that user, if they logged in from that location. See [How the Connection Broker Determines the Resource List](#) for a description of how the Connection Broker determined this list.

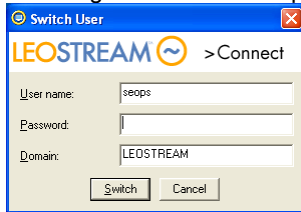
3. Select the desktop you want to log into from the **Resources** list. You can connect to one desktop at a time
4. Click **Connect**. Leostream Connect launches a remote session to that desktop, but does not sign you in. Instead, the Login dialog appears for that desktop.
5. Enter credential to log into the desktop. These can be the credentials for any user that has rights to log into this desktop.

If the user is still logged into their desktop, and you are logging in with non-administrator credentials, you will not automatically log the user out. Only administrators are allowed to automatically log another user out of their desktop.

Similarly, because the Connection Broker does not assign you to the desktop you are managing, you are technically a rogue user on that desktop. The Connection Broker may offer that desktop to another user. If you are not logged into the desktop as an administrator and the Connection Broker offers that desktop to a user with a policy that logs out rogue users, the Connection Broker will automatically log you out to accommodate the new user.

Switching Users

The **Switch User** option allows you to change your user credentials after you are already logged into Leostream Connect. Selecting the **Switch User** option opens the following dialog.



Enter your new credentials and click **Switch**.

Leostream Connect warns you that switching users closes any existing desktop and applications. Click **Yes** to continue, or **No** to remain logged in as the current user.

Branding Leostream Connect for Windows

You can replace the Leostream Connect logo at the top of the **Login** dialog to brand the client with your corporate image, as follows.

1. Create a bitmap file with your corporate brand. This file should be 294 pixels wide and 40 pixels high.
2. Name your bitmap file `LeostreamConnect.bmp`.
3. On each client device, replace the `LeostreamConnect.bmp` file in the Leostream Connect installation directory with your bitmap file.

When you run Leostream Connect, your image appears on the **Login** dialog.

Running Leostream Connect for Windows from the Command Line

You can run the Leostream Connect client from the command line, using the following syntax:

```
LeostreamConnect.exe -address ip address:port options
```

Available options include the following:

- `-domain` or `-d`: The domain name to log the user into.
- `-user` or `-u`: The name of the user to login.
- `-pwd` or `-p`: The user's password.
- `-machine`: The name of the desktop to launch, for users that are offered multiple desktops. Use `*` to launch all connections.
- `-address`: The Connection Broker address and, optionally, port. Leostream Connect honors this setting for users who are not administrators on the client device *only* if the **Allow user to modify Connection Broker address** option is selected on the Connection Broker > **System** > **Settings** page.
- `-login`: Use with the `-user`, `-pwd`, and, optionally, `-domain`, command line options to switch users without opening a confirmation dialog. Leostream Connect forcefully logs out any user that is already logged into the Connection Broker.
- `-logout`: Forcefully log out the user that is currently logged into Leostream Connect. Leostream Connect continues to run.

Chapter 6: Using the Microsoft Windows version of Leostream Connect

- `-closeall` or `-ca`: Closes all desktops that have been connected to via Leostream Connect.
- `-clearuser`: Forces the **Username** field to be empty when launching Leostream Connect, even if a username is specified.
- `-noprompt` or `-np`: Use in conjunction with command line arguments that finish with the **Login** or **Switch User** dialog opening, to suppress that dialog when the command finishes. For example, use with `-closeall` to prevent the **Switch User** dialog from opening after all connections are closed.
- `-exit` or `-e`: Exits Leostream Connect. If `-exit` is used in the same command as `-login` or `-logout`, the `-login` and `-logout` are ignored.
- `-help` or `?` - Display a message box describing the available command line options.



You can use a forward slash (/) instead of a dash (-) in front of each option.

You can encode these command line options into a desktop icon, to open Leostream Connect in a particular configuration. For example, use the following command to encode a username and password into the command:

```
"C:\Program Files\LeostreamConnect\LeostreamConnect.exe" -user myUser -pwd theirPassword
```

Where *myUser* is the user's user name and *theirPassword* is their password.



If you encode your username and password into the shortcut, Leostream Connect skips the **Login** dialog if no other form of authentication is required and automatically logs you into the Connection Broker.

Leostream Connect and Connection Broker Communication

When specifying the Connection Broker address, you have the option of specifying the port to use when communicating with the Connection Broker. Regardless of the port you specify, Leostream Connect first attempts to communicate with the Connection Broker using SSL on port 443. If SSL fails and you specified port 443, Leostream Connect fails over to non-SSL communication on port 80. Otherwise the client fails over to non-SSL communication on the specified port.



Leostream Connect cannot communicate with the Connection Broker using SSL if you are running version 1.6.12 of the Java Runtime Environment. If you try to use SSL with this version of the Runtime Environment, the following error occurs.

```
5452-27    01/10/12 14:53:56:603 ERR: Unable to validate broker(broker_address) with SSL
Cause:
java.net.SocketException: Unconnected sockets not implemented
```

To resolve this issue, upgrade your Java Runtime Environment to version 1.6.25.

Chapter 7: Using the Java™ version of Leostream Connect


For information on configuring Leostream Connect in Sun™ Sun Ray™ server environments, see the Leostream Connection Broker [Thin Client Guide](#).

Running Leostream Connect and Connecting to Resources

To run the Java™ version of Leostream Connect, issue the following command:

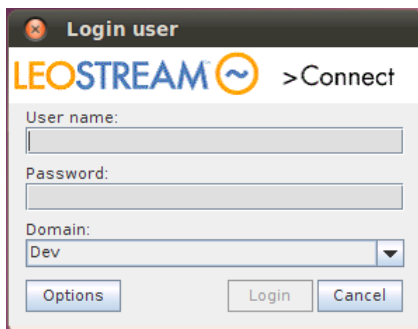
```
java [options] -jar LeostreamConnect.jar
```

Where `java` is the full path to the Java executable. For a description of available options, see [Running Leostream Connect for Linux® from the Command Line](#).

 Version 2.x of Leostream Connect obsoletes the tabbed dialog format. Any existing tabbed dialog deployments automatically switch to the new standard dialog format.


Logging into Leostream Connect

The following figure shows the **Login** dialog for the Java version of Leostream Connect. The buttons provided on your **Login** dialog may differ, based on the setting of the **Show additional login button** option on the Connection Broker > **System > General Configuration** page (see [Customizing the Leostream Connect User Interface](#)). For a description of the functionality of these additional buttons, see [Alternate Login Button Configurations](#).



To log into Leostream Connect:

1. Enter your username and password in the **User name** and **Password** edit fields, respectively.

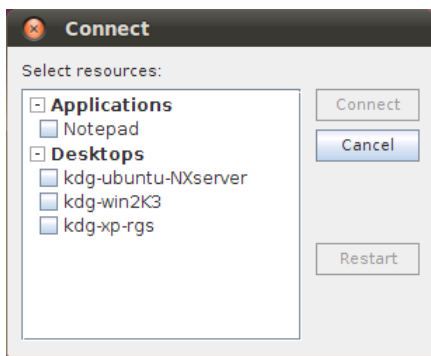
 The Java version of Leostream Connect does not accept smart card or biometric logins.


2. Enter or select a domain from the **Domain** field, if this field is shown.
3. Click **Login**.

If the Connection Broker offers you a single desktop, a connection to that desktop automatically launches. Otherwise, the **Connect** dialog opens, allowing you to select which resources to launch.

Connecting to Desktops and Applications

By default, the Java version of Leostream Connect allows you to launch multiple resources. If you are offered multiple resources, the **Connect** dialog lists the available applications and desktops preceded by check boxes, as shown in the following figure.



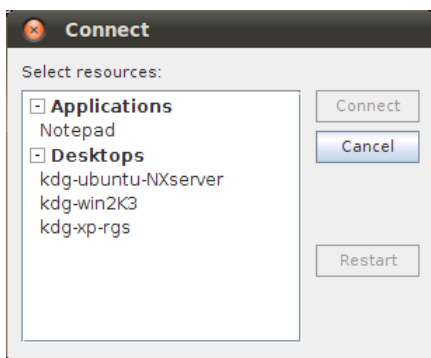
 The **Restart** button appears only if you are logged in as a user with a Connection Broker role and policy that allows you to restart one or more of your offered desktops (see [Allowing Users to Restart Desktops](#)).

To connect to one or more resources, select the checkbox associated with the resources you want to connect to.

- Click **Connect** to launch these resources
- If available, click **Restart** to restart the desktops before connecting. If you select multiple desktops, Leostream Connect restarts all selected desktops before opening any remote viewer. Restarting multiple desktops could take a significant amount of time.

If you do not have permission to restart all of the selected desktops, Leostream Connect indicates which desktops will not be restarted before establishing the connection.

If you are restricted to launch a single resource, the **Connect** dialog lists the available resources in a single-selection list, as shown in the following figure.



To connect to a resource, select the resource you want to connect to.

- Click **Connect** to launch this resource
- If available, click **Restart** to restart the desktop before connecting.

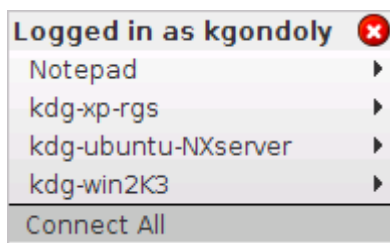
Using the Sidebar Menu

The Leostream Connect sidebar allows you to connect to and disconnect from your offered resources without having to return to the **Connect** dialog, as well as attach USB devices to your remote desktop, if applicable.

To enable the Leostream Connect sidebar, add the following lines to the `lc.conf` file.

- `sidebar_enabled = true` – Enables the sidebar. Set this value to `false` to disable the sidebar. If not specified, the default value is `false`.
- `sidebar_show_delay = seconds` – An integer value indicating the amount of time, in seconds, the user must keep their mouse at the left-most side of the screen before the sidebar opens. If not specified, this value defaults to 2.
- `sidebar_hide_timeout = seconds` – An integer value indicating the length of time, in seconds, that the sidebar remains open after the mouse leaves the sidebar. If not specified, this value defaults to 1.

To open the sidebar, hold the mouse anywhere along the edge of the client's display. If you are connected to a remote desktop that is not in full screen mode, place the mouse at the edge of the physical display, not at the edge of the remote session. The following figure shows an example of the sidebar.



In this menu:

- The top row displays the name of the current user. Click the red X in this row to close the sidebar.
- The middle rows display your offered resources. Each item has a **Connect** or **Disconnect** submenu. Select these items to establish a connection to the resource, or disconnect from an existing connection.

When using HP RGS to manage USB device on the remote desktops, the Leostream Connect sidebar menu contains additional menus that allow you to select which remote desktop should have access to all USB devices. See [USB Passthrough with HP RGS](#) for more information.

- Any resource that is already connected is preceded by a green dot.
- Use the **Connect All** option to launch a connection to all resources.
- Use the **Disconnect All** option to disconnect from any existing resource connections.

Alternate Login Button Configurations

Depending on the setting for the **Show additional login button** option on the Connection Broker > **System** > **Settings** page, your **Login** dialog may have one of the following button configurations.

1. The **Login** button, only:
 - If the Connection Broker offers you a single resource and you do not have permission to restart that desktop, clicking the **Login** button connects the desktop.

- If the Connection Broker offers you a single resource and you do have permission to restart that desktop, clicking the **Login** button opens the **Connect** dialog. Use the **Restart** button on the **Connect** dialog to restart and connect to the desktop. Use the **Connect** button to connect to the desktop without restarting.
- If the Connection Broker offers you multiple resources, clicking **Login** always opens the **Connect** dialog.

2. The **Login** and **Advanced Login** buttons:

- If the Connection Broker offers you a single desktop, click the **Login** button to connect to the desktop without restarting the desktop, regardless of if you have permission to restart the desktop.
- If the Connection Broker offers you a single desktop and you want to restart that desktop before connecting to it, click the **Advanced Login** button to open the **Connect** dialog. Use the **Restart** button on the **Connect** dialog to restart and connect to the desktop. Use the **Connect** button to connect to the desktop without restarting.
- If the Connection Broker offers you multiple desktops, and you do not want to restart any of the desktops before connecting, click the **Login** button to open the **Connect** dialog. Use the **Connect** button on the **Connect** dialog to connect to the desktop without restarting.
- If the Connection Broker offers you multiple desktops and you want to restart one or more of them, click the **Advanced Login** button to open the **Connect** dialog. Use the **Restart** button on the **Connect** dialog to restart and connect to the desktop. Use the **Connect** button to connect to the desktop without restarting.

3. The **Login** and **Restart** buttons:

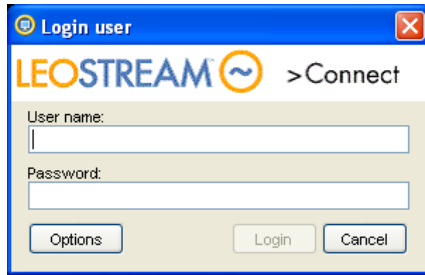
- If the Connection Broker offers you a single desktop, click the **Login** button to connect to the desktop without restarting, regardless of if you have permission to restart the desktop.
- If the Connection Broker offers you a single desktop and you want to restart that desktop before connecting to it, use the **Restart** button to automatically restart and connect to that desktop.

The **Restart** button differs from the **Advanced Login** button in that clicking **Restart** instantly restarts the desktop while clicking **Advanced Login** opens the **Connect** dialog, where you have the option to restart your desktop.

- If the Connection Broker offers you multiple desktops, and you do not want to restart any of the desktops before connecting, use the **Login** button to open the **Connect** dialog. Use the **Connect** button on the **Connect** dialog to connect to the desktop without restarting.
- If the Connection Broker offers you multiple desktops and you need to restart one of them, use the **Restart** button to open the **Connect** dialog. Use the **Restart** button on the **Connect** dialog to restart and connect to the desktop. Use the **Connect** button to connect to the desktop without restarting.

Hiding the Domain Field

You can use the `remove_domain` option in the `lc.conf` file to hide the **Domain** field on the Leostream Connect **Login** dialog. With the **Domain** field removed, the Login dialog appears as shown in the following figure.

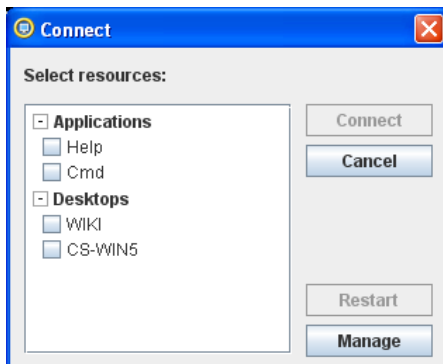


With the **Domain** field hidden, the user is unable to select which domain to log into. You may want to hide the **Domain** field, for example, if you specified authentication server names that are different from your domain names and may not be recognized by your users.

If your Connection Broker includes more than one authentication server, ensure that the **Include domain in drop-down** menu in all **Edit Authentication Server** forms is *not* set to **Yes, as default**. If you do specify a default authentication server, users in other authentication servers cannot log into the Connection Broker using Leostream Connect. In this case, although the **Domain** field is not shown, Leostream Connect tries to use only the default authentication server to log the user in.

Managing Resources

If you log into the Connection Broker with a role that has the **Allow user to manage another user's resources** option selected, the **Connect** dialog contains a **Manage** button, shown in the following figure. This feature allows you to log into desktops using credentials other than those you provided to the Connection Broker.



You must access the **Connect** dialog by clicking either the **Advanced Login** or **Restart** button. The **Connect** dialog does not contain the **Manage** button when launched from the **Login** button.

Managing resources allows you to perform administrative tasks on desktops, including:

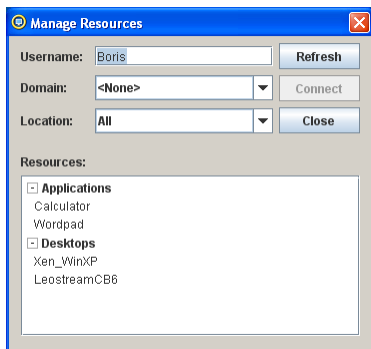
- Reviewing the list of desktops that the Connection Broker offers to another user.
- Logging into a desktop that is offered to another user, to perform administrative tasks on that desktop.
- Logging into one of your own desktops using different credentials from what you provided to the Connection Broker.

See the **Managing Resources** section for the Windows version of Leostream Connect for information on how the Connection Broker determines which resources you can manage, and what happens when you connect to a managed resource.

Managing Your Own Resources

Managing your own resources allows you to log into your offered desktops using different credentials from what you provided the Connection Broker. If your Connection Broker account does not have administrative privileges for your desktop, you can use the manage resource feature to, for example, log into your desktop using administrator credentials. To manage your own resources:

1. On the Connect dialog, click the **Manage** button to open the **Manage Resources** dialog, shown in the following figure.



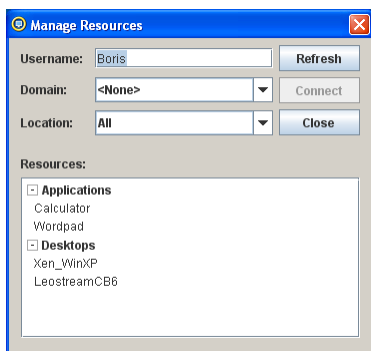
By default, the **Resources** list shows your offered applications and desktops.

2. To manage one of your desktops:
 - a. Select the appropriate desktop from the **Resources** list. You can connect to one desktop at a time.
 - b. Click **Connect**. Leostream Connect launches a remote session to that desktop, but does not sign you in. Instead, the Login dialog appears for that desktop.
 - c. Enter credential to log into the desktop. These can be the credentials for any user that has rights to log into this desktop.
3. To manage another desktop, repeat step 2.

Managing another User's Resources

Managing another user's resources allows you to perform administrative tasks on the user's desktop. The user's policy determines which resources are offered to them by the Connection Broker. The policy the Connection Broker chooses to assign to the user depends on the domain the user logs into, and the location the user logs in from. Therefore, to accurately obtain a list of resources offered to a particular user, you must enter this information, as follows.

1. On the **Connect** dialog, click **Manage** to open the **Manage Resources** dialog, shown in the following figure opens.



2. To get the list of desktops offered to a particular user, simulate that user logging into the Connection Broker:

- a. Enter the user's login name in the **Username** edit field.
- b. Select the domain to log the user into from the **Domain** drop-down menu.
- c. Select the user's location from the **Location** drop-down menu. This menu contains all the locations defined in the Connection Broker > **Clients** > **Locations** page.
- d. Click **Refresh**.

The **Resources** list updates to show the applications and desktops that would be offered to that user, if they logged in from that location. See [How the Connection Broker Determines the Resource List](#) for a description of how the Connection Broker determined this list.

3. Select the desktop you want to log into from the **Resources** list. You can connect to one desktop at a time
4. Click **Connect**. Leostream Connect launches a remote session to that desktop, but does not sign you in. Instead, the Login dialog appears for that desktop.
5. Enter credential to log into the desktop. These can be the credentials for any user that has rights to log into this desktop.

If the user is still logged into their desktop, and you are logging in with non-administrator credentials, you will not automatically log the user out. Only administrators are allowed to automatically log another user out of their desktop.

Similarly, because the Connection Broker does not assign you to the desktop you are managing, you are technically a rogue user on that desktop. The Connection Broker may offer that desktop to another user. If you are not logged into the desktop as an administrator and the Connection Broker offers that desktop to a user with a policy that logs out rogue users, the Connection Broker will automatically log you out to accommodate the new user.


Simulating Shell Mode

The Windows version of Leostream Connect can be used in the `shell` registry key to create a shell-mode installation. However, the Java version of Leostream Connect requires that you simulate shell mode using a script.

The script automatically launches Leostream Connect when the user logs in to the Linux desktops, and effectively disables the **Cancel** button by placing the call to launch Leostream Connect in a `while` loop. For example:

```
if [ -f /opt/leostreamconnect/LeostreamConnect.jar ] ; then
  echo "Launching LSCj.... "
  while :
  do
    java -jar /opt/leostreamconnect/LeostreamConnect.jar
  done
  echo "exiting LSCj ...."
fi
```

Place this script in `/etc/X11/xinit/initrc.d`.

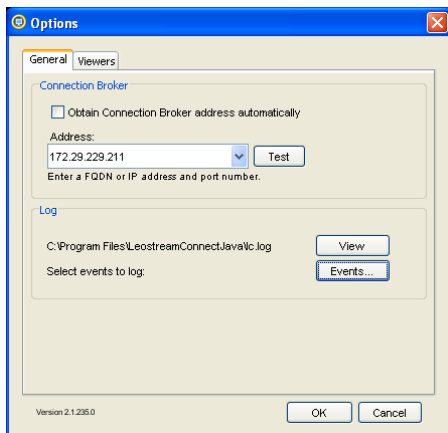
 Ensure that the command `java -jar /opt/leostreamconnect/LeostreamConnect.jar` functions properly before placing it in the `initrc.d` directory as this will affect all users that using KDE. Also, ensure that you have an alternate method for logging in to the Linux desktop, such as SSH.

Configuring Options

You can use the Leostream Connect **Options** dialog to specify the Connection Broker address and remote viewer locations. Alternately, you can configure Leostream Connect options using the `lc.conf` file (see [Writing lc.conf Files](#)).

Click the **Options** button to open the **Options** dialog, shown in the following figure.

✓ You can access the **Options** dialog by pressing `Ctrl+Shift+O`, even if the **Options** button does not appear on the **Login** dialog.



Entering the Connection Broker Address

By default, Leostream Connect uses the Connection Broker address stored in the `lc.conf` file (see [Writing lc.conf Files](#)). To change the Connection Broker used in this session of Leostream Connect, enter the Connection Broker hostname or IP address in the **Address** combo-box on the **General** tab, or select an existing address from the drop-down menu. To instruct Leostream Connect to discover the Connection Broker address using the appropriate DNS SRV record, select the **Obtain Connection Broker address automatically** option.

Clicking **OK** attempts to save the new address in the `lc.conf` file.

If you do not have write privileges to the `lc.conf` file, the new Connection Broker address is used only during the current Leostream Connect session. Closing and restarting Leostream Connect reverts to the Connection Broker address contained in the `lc.conf` file.

If you do have write privileges to the `lc.conf` file, the new Connection Broker address is stored in the file and used for all subsequent Leostream Connect sessions.

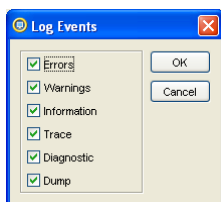
Setting Log Levels

The **Log** section on the **General** tab allows you to specify the type of events to include in the Leostream Connect logs, and view the resultant logs. If you are gathering logs to send to Leostream support, ensure that all event types are being logged.

To view the current logs, click the **View** button. The text to the left of the **View** button indicates the full path to the log file.

To set the logging levels:

1. Click the **Events** button.
2. In the **Log Events** dialog, shown in the following figure, check the box before each type of event to log.



3. Click **OK** on the **Log Events** dialog.

Viewing Logs

Leostream Connect writes all log information in the `lc.log` file. If you do not specify a directory for the log file, Leostream Connect places the log file in one of the following two locations, depending on the permissions allotted to the user that is running Leostream Connect.

- The Leostream Connection installation directory, if the user has permission to write to that directory and any `lc.log` file already in that directory.
- The user's directory, if the user cannot write to the installation directory.

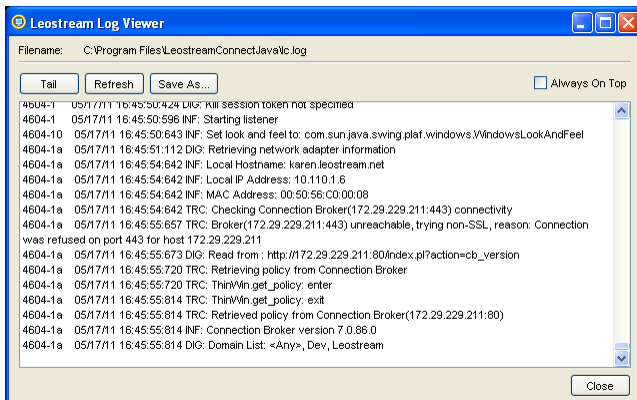
To place the log file in a specific directory, run Leostream Connect with the `LeostreamLogDir` option (see **Running Leostream Connect for Linux® from the Command Line**). The user running Leostream Connect must have write permission for the specified directory. Otherwise, Leostream Connect places the log file into the user's directory.



If logging in from a Sun Ray thin client, ensure that the logs directory is writable for all users.

Using the Graphical Log Viewer

You can access the **Log Viewer** by clicking the **View** button on the **General** tab of the **Options** dialog. Alternatively, you can open the **Log Viewer** at any time by pressing `Ctrl+Shift+L`. The following figure shows the default **Log Viewer**.



The logs display in the text field with the most recent log messages at the bottom. To use the **Log Viewer**:

- Click **Tail** or **Pause** to turn off or on, respectively, the real-time display of new log information in the **Log Viewer**. If you turn off the real-time display of the logs, Leostream Connect continues to store log information in the `lc.log` file.
- If you have stopped the real-time display of log information, click **Refresh** to update the Log Viewer with the current contents of the `lc.log` file.
- Click **Save As...** to store the log information to a file.

Specifying Remote Viewer Clients

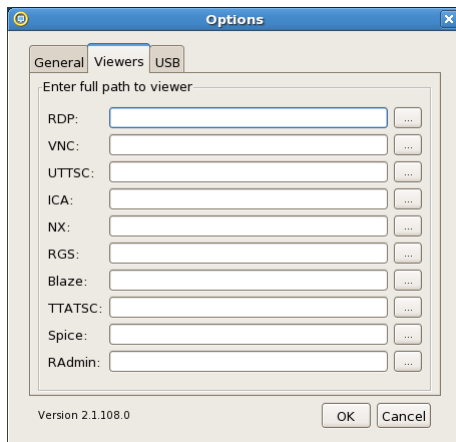
You can use any of the following remote viewer clients with the Java version of Leostream Connect.

- **RDP**: To connect to a Windows desktop. Leostream Connect looks for the `rdesktop` executable when installed on a Linux desktop, and looks for the Microsoft RDP executable when installed on a Windows desktop.

- VNC: To connect to a Linux or Windows desktop
- Citrix ICA: To connect to a Citrix XenApp application or desktop
- NoMachine NX: To connect to a Linux or Windows desktop
- HP RGS: To connect to a Linux or Windows desktop
- Ericom Blaze: To connect to a Windows desktop
- Red Hat Enterprise Virtualization SPICE: To connect to a Linux or Windows desktop
- Sun™ Sun Ray™ `uttsc`: To connect from a Sun Ray DTU
- Sun Secure Global Desktop (SGD) `ttatsc`: To run Leostream Connect in a Sun SGD environment.
- Famatech Radmin: To connect to a Windows desktop

On the **Viewers** tab, shown in the following figure, in the edit field associated with each remote viewer, enter the full path to the file name for the associated executable file. You can browse for the remote viewer binary file in the following two ways.

- Click the **Browse** button next to the remote viewer to locate.
- Place the cursor in the edit field for the remote viewer and press `Ctrl-O`.



The command line parameters and configuration file for these remote viewers are determined by the protocol plans in the Connection Broker. See the Leostream [Choosing and Using Display Protocols](#) guide for information on specifying configuration files and command line parameters for the different display protocols.

Specifying USB Device Redirection Options

If Leostream Connect is communicating with a Connection Broker that has the **USB passthrough control** feature selected on the > **System > Settings** page, the **Options** dialog contains the **USB** tab, shown in the following figure.



By default, Leostream Connect does not prompt the user to attach any USB devices to the remote desktop. You can specify different behavior based on if the user is offered a single or multiple desktops, as follows.

For users with a single offered desktop:

- Select **Do not attached USB devices** (the default) to restrict Leostream Connect from redirecting a USB device connected to the client over to the remote desktop.
- Select **Prompt to select devices to attach** to indicate that Leostream Connect should prompt the user to redirect a USB device connected to the client over to the remote desktop. The user is prompted to redirect the USB device when they connect to their remote desktop and when a new USB device is attached to the client.
- Select **Automatically attach all devices** to indicate that Leostream Connect should automatically redirect all USB devices as soon as the user connects to their remote desktop. Leostream Connect redirects all USB devices as soon as the user connects to their remote desktop, and whenever a new device is attached to the client.

For users with a multiple offered desktop:

- Select **Do not attached USB devices** (the default) to restrict Leostream Connect from redirecting a USB device connected to the client over to the remote desktop.
- Select **Prompt to select devices to attach** to indicate that Leostream Connect should prompt the user if they want to redirect a USB device connected to the client over to the remote desktop. The user is prompted to redirect the USB device when they connect to their remote desktop and when a new USB device is attached to the client.

When **Prompt to select devices to attach** is selected and the user connects to a remote desktop, Leostream Connect opens the following dialog.



To attach a USB device to the remote desktop:

1. Select the checkbox in front of the USB devices to redirect to the remote desktop. If you do not want to redirect any USB devices, leave all checkboxes unchecked.
2. Click **Connect** to connect to the remote desktop, regardless of if you are redirecting USB devices, or not.
Click **Cancel** *only* if you do not want to connect to the remote desktop.

Writing lc.conf Files

Leostream Connect stores a set of configuration parameters in a properties file called `lc.conf`. You can write or modify the `lc.conf` file to customize certain aspects of Leostream Connect, such as the colors and logo used on the **Login** dialog.

By default, Leostream Connect looks for the `lc.conf` file in the Leostream Connect installation directory. If an `lc.conf` file does not exist in the installation directory, Leostream Connect looks for the file in the following directories. In order:

1. A `.leostream` directory within the Leostream Connect installation directory
2. A `.leostream` directory inside the user's home directory

Alternatively, you can store the `lc.conf` file in a user-defined directory and use the `LeostreamConfFile` option to specify the absolute or relative path to the file when you run Leostream Connect. See [Running Leostream Connect for Linux® from the Command Line](#) for more information.

In general, if you are running Leostream Connect in a kiosk-like mode where multiple users can access the `lc.conf` file, setup the `lc.conf` file with your default values and then mark this file as read-only for all users.

The `lc.conf` file takes the following form

```
option1 = value1
option2 = value2
etc...
```

The following options are available.

Connection Options

- **connection_broker_ip**: IP address or hostname of the Connection Broker.
- **connection_broker_port**: Connection Broker port.
- **domain**: The default authentication server shown to the user in the **Domain** field.
- **logout_ondisconnect**: Set to `true` (1) to return to the legacy Leostream Connect logout behavior. In legacy versions of the client, users that connected to multiple resources were automatically logged out of Leostream Connect when they closed their last desktop connection. Setting `logout_ondisconnect` to `false` (0), the default, leaves the user logged into Leostream Connect after they close their last desktop connection.

- **read_username_from_smartcard:** Set to `true` (1) to read the username from a Sun Ray DTU Java smartcard, and automatically filled in to the **User name** field on the Leostream Connect login dialog. The default value is `false`; the username is not automatically populated.
- **recent_brokers:** A comma separated list of Connection Broker addresses that this Leostream Connect client has contacted. These addresses appear in the **Address** combo-box on the **Options** dialog (see [Entering the Connection Broker Address](#)). Delete this entry or individual addresses from the `lc.conf` file to clear out the contents of the **Address** combo-box.
- **enable_window_tracking:** When establishing HP RGS connections from a client with multiple monitors, indicates if Leostream Connect should track and remember the movement of RGS windows across displays. When tracking window location, Leostream Connect automatically reopens a disconnect RGS session in the display that last contained the session. Set to `true` (1) to enable window tracking; `false` (0) to disable tracking. Please see the Leostream Guide to [Choosing and Using Display Protocols](#) for more information.
- **caps_lock_warning:** Set to `true` (1) to warn users when their `Caps Lock` key is on and they are entering their password.

External Programs

- **ica_path:** Path to the ICA client
- **ifconfig_bin:** Path to `ifconfig` (for Unix, only)
- **nx_path:** Path to NX client
- **radmin_path:** Path to the Radmin binary
- **rdp_path:** Path to the Terminal Services Client (`rdesktop`) binary
- **rgs_path:** Path to the HP Remote Graphics Software receiver binary
- **ttatsc_path:** Path to the `ttatsc` binary for Sun Global Desktop
- **uttsc_path:** Path to the `uttsc` binary
- **vnc_path:** Path to the `vncviewer` binary
- **blaze_path:** Path to the Ericom Blaze Client binary
- **prompt_for_path:** If set to `true` (1), displays a prompt to browse for the remote viewer binary file if a file is not specified in the **Options** dialog.



Leostream Connect/Java version 1.2.19 and higher no longer accepts the `username` and `password` fields.

Common UI Controls

All colors are specified as RGB triplets, using the format (R, G, B) , where R, G and B are decimal values between 0-255. You can use either ones and zeros or the strings `true` and `false` for the values of parameters that accept Boolean values.

- **border_color:** Specify the color of the border around the **Login** dialog. Expects a value in the form (R,G,B), where R, G and B are decimal values between 0-255. For example, to make the border all red, use `border_color=(255,0,0)`
- **border_width:** Width in pixels of the border along the left, bottom and right of the panels. Use the `border_color` option to specify a color for the border.
- **button_face_color:** Color of the face of all buttons. The default color is based on the configured Look-and-Feel.
- **button_select_color:** Color of the background on selected buttons. The default color is based on the configured Look-and-Feel.
- **button_text_color:** Color of the text on all buttons. The default color is based on the configured Look-and-Feel.
- **decorate_window:** Show or hide default window decorations such as title bar and border. By default the value is set to 1 to show the decorations. Set to 0 to hide the decorations. Note that some windows managers do not support hiding window decorations.

- **dialog_background**: Color of the background of text fields on the **Login** and **Connect** dialogs. Default is (255,255,255).
- **disable_options_tab**: *Deprecated*. See `hide_options_button`.
- **exit_ondisconnect**: Set to 1 to indicate that Leostream Connect should exit after the user closes, either by disconnecting or logging out, their last resource connection. Default is 0.
- **geometry**: Specify the initial location of the login dialog. Default is 0,0, which is the top-left corner of the screen.
- **header_background**: Background color for top panel containing the logo. If not specified, the header background color is set by the `panel_background` parameter.
- **hide_advanced_login**: When using Leostream Connect version 1.5 with Connection Broker version 6.2 or earlier, or when using a Leostream Connect version earlier than 1.5 with any Connection Broker version, set this parameter to 1 to prevent the **Advanced Login** button from appearing in the Standard interface. For Leostream Connect 1.5 and later, Connection Broker version 6.3 and later may ignore this parameter based on the value set by the **Show additional login button** option on the Connection Broker > **System** > **General Configuration** page.
- **hide_exit_button**: If set to 1, will prevent the **Cancel** button on the credentials form from appearing.
- **hide_options_button**: Set to 1 to hide the **Options** button on the **Connect** dialog. Default is 0, which displays the button. See [Configuring Options on Linux® Operating Systems](#) for information on available options.
- **keyboard_country**: Enter the two-letter uppercase country code for the keyboard attached to the client, for example `US` or `GB`. Must be used in conjunction with `keyboard_language`.
- **keyboard_language**: Enter a two-letter lowercase language code for the keyboard attached to the client, for example `en`, `jp`, or `fr`. Must be used in conjunction with `keyboard_country`, Leostream Connect attempts to force the keyboard locale used for inputting data into text fields.
- **laf**: Specifies the look-and-feel for the Leostream Connect dialogs. When not specified, Leostream Connect defaults to the system look-and-feel. Possible values include, the following, when supported by the client device.
 - `windows` – Default Windows look-and-feel
 - `windows classic` – Windows classic look-and-feel
 - `motif` – Motif
 - `gtk` – gtk
 - `metal` – Java cross platform look-and-feel
 - `system (default)` – Default system look-and-feel
- **login_url**: Specify a full URL to include as a link on the bottom right side of the **Login** dialog.
- **login_url_label**: Specify a label for the link to display on the bottom right side of the **Login** dialog. Must be used in conjunction with `login_url`. If 9 is specified by no `login_url_label` is given, a potentially truncated version of the URL is displayed on the **Login** dialog.
- **login_url_tooltip**: Specify a tooltip to display when the user hovers the cursor over the URL displayed on the **Login** dialog. If left blank, or not included in the `lc.conf` file, no tooltip is displayed.
- **logo_path**: Specify the path to a GIF-file to replace the Leostream banner on the login dialog. The file must be sized to 294 x 40.
- **logout_ondisconnect**: Specify if users that connect to multiple resources are automatically logged out of Leostream Connect after they close their last desktop connection. If the `lc.conf` file does not contain this

parameter, the default behavior is determined by the **Log out user after last connection is closed** option on the Connection Broker > **System** > **Settings** page.

- **panel_background**: Color of the background of the entire panel. Default is (212,208,200).
- **remove_domain**: Set to 1 to remove the domain field from the login screen.
- **resource_dlg_size**: The width and height, in pixels, of the resource selection dialog, entered as (width, height).
- **selected_background**: RGB value indicating the color of the background of selected options in the **Resource Selection** dialog.
- **selected_text_color**: RGB value indicating the color of the text of selected options in the **Resource Selection** dialog.
- **sidebar_edge**: Indicates the edges of the screen where the user can access the Leostream Connect sidebar menu. Possible values include `left`, `right`, `top`, `bottom`, and `all`.
- **sidebar_enabled**: If set to 1 (`true`), enables the Leostream Connect sidebar for connecting and disconnecting from remote sessions. The default value of 0 (`false`) hides the sidebar.
- **sidebar_show_delay**: An integer value indicating the amount of time, in seconds, the user must keep their mouse at the left-most side of the screen before the sidebar opens. If not specified, this value defaults to 2.
- **sidebar_hide_timeout**: An integer value indicating the length of time, in seconds, that the sidebar remains open after the mouse leaves the sidebar. If not specified, this value defaults to 1.
- **single_desktop_only**: Set to 1 to restrict the user to connect to a single desktop. When set to one, if the user is offered multiple desktops, the desktops are displayed with radio buttons instead of check boxes. See [Connecting to a Single Offered Desktop](#) for an example dialog.
- **window_title**: Set the window title. The default window title is Leostream Connect.

Other UI Controls

- **check_port_timeout**: (*Deprecated*) Specify the length of time, in milliseconds, before interrupting a port check. Default is 2000 (2 seconds). Leostream Connect 1.5 and later hard-code this value to 8000 (8 seconds).
- **log_viewer_visibility**: (*Deprecated*) Set to `disabled`, `enabled`, or `always`. When `disabled`, the graphical log viewer can never be opened. When set to `enabled`, the log viewer can be opened by pressing `Ctrl+Shift+L`. Set to `always` to force the log viewer to always be visible.
- **serial_number**: An optional setting that will be automatically generated if not manually configured.
- **sr_alive_port**: Enter the port to check on the Sun Ray host before redirection. The default port is 7007.
- **TraceLevel**: Specify the level of information to keep in the Leostream Connect logs. Valid trace levels include: `ERROR`, `WARN`, `INFO`, `TRACE`, `DIAG`, `DUMP`, and `STDOUT`. With the exception of `STDOUT`, all trace levels correspond to the associated checkbox on the **Log Events** dialog. The `STDOUT` trace level instructs Leostream Connect to print the logs to standard out, as they occur.

Running Leostream Connect for Linux® from the Command Line

To invoke Leostream Connect from the installation directory, enter the following command.

```
java -jar LeostreamConnect.jar
```

The following sections describe the supported command line parameters and options.

Command Line Parameters

The following command line parameters are supported by Leostream Connect version 1.5 and later.

- `-user <username>`: Specifies the username to automatically use when the client starts up. (Replaces the obsolete `form.username` command line option.)
- `-password <password>`: Specifies the password to automatically use when the client is authenticating with the Connection Broker. (Replaces the obsolete `form.password` command line option.)
- `-readpassword`: Causes the client to wait for up to 2 seconds for the password to be written to the standard input of Leostream Connect to facilitate more secure credential passing.
- `-domain <domain>`: Specifies the domain to automatically use when the client is authenticating with the Connection Broker using the credentials provided by `-user` and `-password`. (Replaces the obsolete `form.domain` command line option.)

To use the command line parameters, append the options after `LeostreamConnect.jar`, for example:

```
java -jar LeostreamConnect.jar -user Example -readpassword -domain leostream
```

Command Line Options

You can customize Leostream Connect by invoking the command with any of the following options:

- **LeostreamConfFile**: Full path to the Leostream Connect configuration file. This directory name overrides any other possible location for the `lc.conf` file.
- **LeostreamLogDir**: Full path to the directory for storing the Leostream Connect logs. Overrides other settings.
- **LeostreamLogFileSuffix**: An additional identifier for log file names. The default log file name is `lc.log`. If this option is used, the log filename is changed to `lc- $\$$ ID.log`.
- **LeostreamLogStdOut**: Write log to standard out in addition to a file.
- **geometry**: Sets the position of the window (e.g. `-Dgeometry=100,100`).

To invoke Leostream Connect for Linux with any of the options, prepend the option with `-D` and add it to the command just before the `-jar`, for example, the following command sets the directory for the `lc.conf` file.

```
java -DLeostreamConfFile=/etc/leostream/lc.conf -jar LeostreamConnect.jar
```

Running Leostream Connect for Linux® from a Shell Script

You can create shell scripts that launch Leostream Connect/Java so users do not have to use the command line interface. For example:

```
#!/bin/sh
JAVA_HOME=/path/to/jre
LSC_HOME=/path/to/leostream
cd $LSC_HOME
$JAVA_HOME/bin/java -jar LeostreamConnect.jar
```

Where `/path/to/jre` and `/path/to/leostream` are the full path name to your Java Run-Time Environment and Leostream Connect, respectively.