



leostream

Remote Desktop Access Platform

The Leostream Agent Guide

Session Monitoring and End User Experience Features for Leostream Environments

Versions 2023.1 / 5.2
April 2023

Contacting Leostream

Leostream Corporation
77 Sleeper St.
PMB 02-123
Boston, MA 02210
USA

<http://www.leostream.com>
Telephone: +1 781 890 2019

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

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

Copyright

© Copyright 2002-2023 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.

HP is a trademark of Hewlett-Packard Development Company, L.P. in the U.S. and other countries. HPE is a trademark of Hewlett-Packard Enterprise Development, L.P. in the U.S. and other countries. Java is a registered trademark of Oracle and/or its affiliates. The OpenStack Word Mark and OpenStack Logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. Leostream is not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community. Linux is the registered trademark of Linus Torvalds in the U.S. and other countries. OpenLDAP is a trademark of The OpenLDAP Foundation. Microsoft, Active Directory, Azure, Hyper-V, Windows, and the Windows logo are trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Other brand and product names are trademarks or registered trademarks of their respective holders. Leostream claims no right to use of these marks.

Patents

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

Contents

CONTENTS	3
OVERVIEW	4
WHY DO I NEED THE LEOSTREAM AGENT?	5
<i>Controlling USB Device Passthrough</i>	5
<i>Registering Desktops with the Connection Broker</i>	6
<i>Single Sign-On to Remote Desktop Console</i>	6
INSTALLATION.....	7
UPGRADES.....	7
LEOSTREAM AGENT FOR WINDOWS OPERATING SYSTEMS	8
RELEASE PLANS FOR IDLE DESKTOPS.....	8
LOCATION-BASED PRINTING SUPPORT	8
USING REGISTRY PLANS	8
ADDING LOCAL USERS AND REMOTE DESKTOP USERS	8
CONFIGURING THE CONNECTION BROKER ADDRESS.....	11
USING SSL	11
<i>Incoming SSL Communication</i>	12
<i>Outgoing SSL Communications</i>	12
<i>Specifying Custom SSL Certificates</i>	12
WORKING WITH MICROSOFT® WINDOWS® FIREWALLS.....	13
LEOSTREAM AGENT CONTROL PANEL DIALOG.....	13
<i>Opening the Leostream Agent Control Panel Dialog</i>	13
<i>Status Tab</i>	13
<i>Options Tab</i>	14
<i>About Tab</i>	18
LEOSTREAM AGENT FOR LINUX AND MACOS DESKTOPS	19
WORKING WITH MACOS DESKTOPS.....	20
CONFIGURING THE CONNECTION BROKER ADDRESS.....	20
USING SSL	20
USING USB REDIRECTION	21
ADDING LOCAL USERS TO THE REMOTE DESKTOP.....	21
STARTING, RESTARTING, AND STOPPING THE LEOSTREAM AGENT.....	22
UNDERSTANDING THE LEOSTREAMAGENT.CONF FILE	23

Overview

The Leostream Agent provides the Connection Broker with insight into the connection status of remote users to their desktops. It is an essential part of the Connection Broker product. The Leostream Agent is required to use the following Leostream features.

- USB device management (Linux and Windows)
- Location-based printing (Windows, only)
- Registry plans (Windows, only)
- Idle-time options in Release Plans
- Joining Windows machines to an Active Directory domain
- Role option to create local or domain users on the remote desktop (Linux and Windows)
- Role option to add users to the Remote Desktop Group (Windows, only)
- Managing the power state and user connections to desktops that are not a member of support Leostream Center type

There are two versions of the Leostream Agent.

1. The Leostream Agent can be installed on any Microsoft Windows operating system version currently covered by Mainstream Support under the Microsoft Fixed Lifecycle Policy, or in service under the Microsoft Modern Lifecycle Policy.
2. The Java version of the Leostream Agent can be installed on the following operating systems:
 - CentOS
 - Debian
 - Fedora
 - SUSE Linux Enterprise
 - Red Hat Enterprise Linux
 - Ubuntu
 - macOS

The Leostream Agent requires a Java Runtime Environment version 1.8, or later.

Why Do I Need the Leostream Agent?

To have the most control over the user's session, Leostream recommends that you install the Leostream Agent on every desktop managed by your Connection Broker.

When installed on a desktop, the Leostream Agent provides the Connection Broker with additional information about the user's session, including:

- When the user logs into and logs out of the remote desktop
- When the user connects and disconnects from the remote session
- When the user locks or unlocks their remote desktop
- When the user's session is idle

In addition, the Connection Broker requires the Leostream Agent to enforce certain role and policy options, including:

- Adding local users and adding local and domain users to the Remote Desktop Users group
- Taking actions when the user disconnects from their remote session
- Managing USB devices
- Attaching network printers specified by Connection Broker printer plans
- Using registry plans to modify or create registry keys on the remote desktop
- Using release plan options to lock, disconnect, or log out the user after their session is idle
- Using release plans or manual actions to log users out of their remote desktop.
- Performing single sign-on for console connections to Windows and Linux remote desktops
- Automatically mapping PCoIP Remote Workstation Cards to the desktop on which they are installed
- Joining Windows desktops to an Active Directory domain

Controlling USB Device Passthrough

The Leostream Agent provides USB management when users log in using Leostream connect. You must select the **Enable USB over IP** task when you install the Leostream Agent on the remote desktop if you plan to use any of this feature.



Do not install the Leostream Agent's USB component if you have another vendor's USB over IP solution installed on the desktop, for example, the HP® ZCentral Remote Boost solution. If two USB

solutions are installed side-by-side, you may not be able to predict which solution is managing the USB devices.



The Leostream USB drivers are not guaranteed to be backwards compatible. Anytime you upgrade your Leostream Agents, ensure that you also upgrade your Leostream Connect clients to the latest version available at the time of the agent upgrade.

Registering Desktops with the Connection Broker

The Connection Broker natively manages remote desktops in a variety of virtualization and cloud platforms using the APIs provided by those platforms. If you need to manage a desktop that is hosted in an environment that is not controlled by a Center in your Connection Broker, you can use the Leostream Agent to manage the machine.

The Connection Broker inventories these virtual machines in the **Uncategorized Desktops** center. See the “Uncategorized Desktops” section of the [Connection Broker Administrator's Guide](#) for more information.

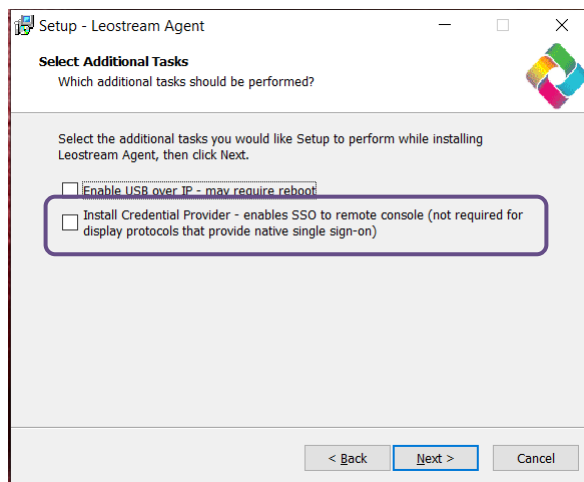


You can reboot and shutdown desktops with installed Leostream Agents. To start a powered off desktop in the Uncategorized Desktops center, use the Connection Broker to send Wake-on-LAN packets.

Single Sign-On to Remote Desktop Console

For display protocols that sign on directly to the machine's console, for example, NoMachine, you can use the Leostream Agent to provide single sign-on.

When installing the Leostream Agent on a Windows operating system, ensure that you select the **Install Credential Provider** task, shown in the following figure.



You do not need to install the Leostream Credential Provider when using the HP Anyware Software to establish PCoIP connections.

When installing the Java version of the Leostream Agent, ensure that you select the **Enable SSO** and the **Desktop Experience** tasks.



The Leostream Agent does not provide single sign-on for Apple macOS.



For Windows desktops, ensure that you enable the **Interactive logon: Do not require CTRL-ALT-DEL** group policy on your desktops. The Leostream Agent does not attempt single sign-on if CTRL-ALT-DEL is required to login.

See the [Leostream Installation Guide](#) for complete instructions.

Installation

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

Upgrades

The Connection Broker can automatically upgrade previously installed Leostream Agents to the version shown on the Connection Broker > **Dashboards** > **Downloads** page. For instructions on automatically upgrading the existing Leostream Agents, see “Upgrading Leostream Agents” in Chapter 17 of the [Connection Broker Administrator's Guide](#).

Leostream Agent for Windows Operating Systems

Release Plans for Idle Desktops

The Leostream Agent for Windows operating systems automatically installs the necessary components to monitor user idle time.



Idle-time monitoring is supported for Microsoft Windows Client operating systems, only. You cannot use the Leostream Agent to monitor idle time for Microsoft Remote Desktop Services sessions.

For Windows operating systems, the Leostream Agent uses the `Processor(_Total)\% Processor Time` performance counter to determine the percentage of CPU used. For multi-processor machines, this counter measures the utilization averaged over all processors.

Location-Based Printing Support

Leostream allows you to attach network printers to remote Windows desktops based on the location of the end user's client device. See "Attaching Network Printers" in the [Connection Broker Administrator's Guide](#) for information on configuring printers to attach to remote desktops.

Using Registry Plans

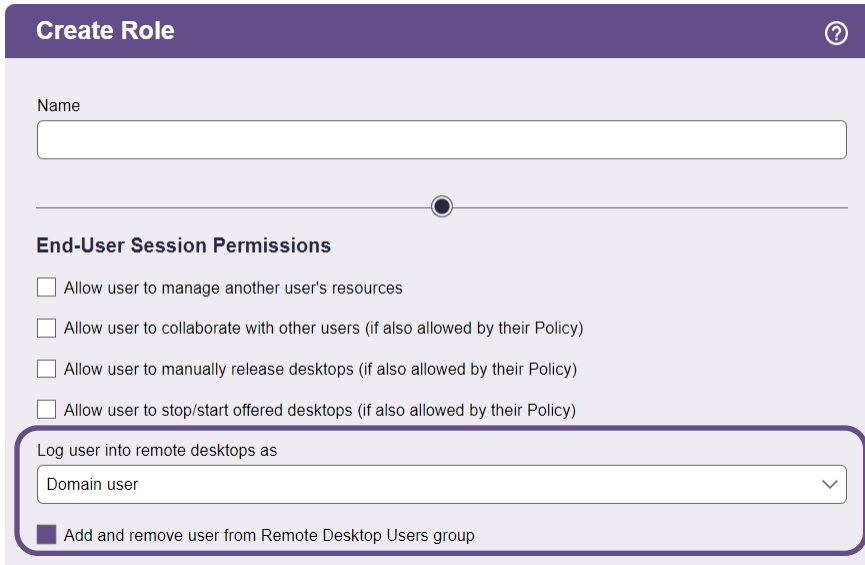
Leostream allows you to create and modify registry keys on the remote desktop based on the location of the end user's client device. To use the Leostream feature for setting registry keys, the remote desktop must have an installed Leostream Agent.

See "Manipulating Registry Keys" in the [Connection Broker Administrator's Guide](#) for information on configuring registry plans to create and modify registry keys on the remote desktop.

Adding Local Users and Remote Desktop Users

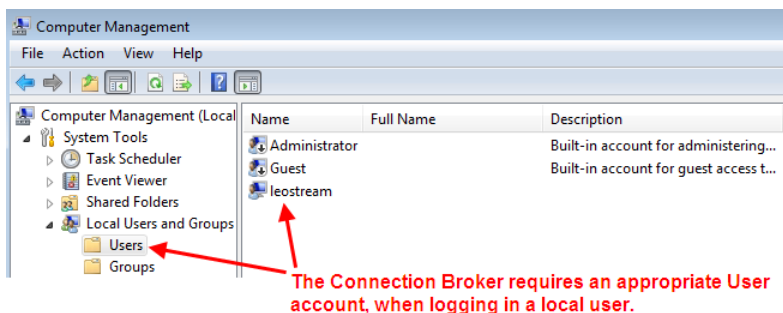
You can use the Leostream Agent to automatically add Local Users to the remote desktop and add these users or domain users to the desktop's Remote Desktop Users group. You do not need to select any additional tasks when installing the Leostream Agent to use the feature for adding Local Users or Remote Desktop Users.

The Leostream Agent adds the user to the Users group and/or Remote Desktop Users group, based on the user's Connection Broker role settings. The following figure shows the available role options.



Use the **Log user into remote desktop as** drop-down menu to 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, shown in the following figure.



To manage local user accounts, use one of the following 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.

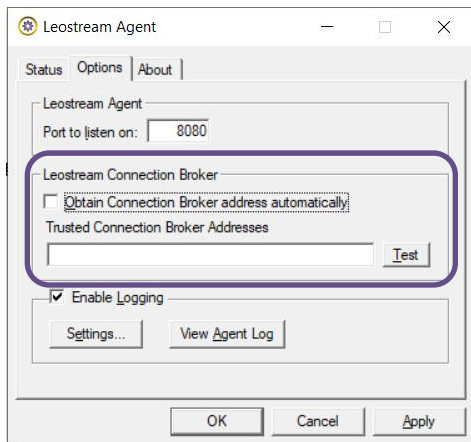
You can use the **Add and remove user from Remote Desktop Users group** option to automatically add the Leostream user to the Remote Desktop Users group on their offered Windows desktops. The Leostream Agent identifies the Remote Desktop Users group using a SID of S-1-5-32-555. You may rename or internationalize the Remote Desktop Users group name, as long as you retain this SID.

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.

 When this option is selected, the Connection Broker takes control of the Remote Desktop Users group. If a user is a member of the Remote Desktop Users group before they logged into the desktop, the Connection Broker still removes the user from that group when they log out of the desktop.

Configuring the Connection Broker Address

The Leostream Agent registers with the Connection Broker entered in the **Trusted Connection Broker Addresses** section on the Leostream Agent Control Panel dialog, shown in the following figure.



The Leostream Agent communicates only with the Connection Broker entered in this dialog. If the **Obtain Connection Broker address automatically** checkbox is selected, the Leostream Agent looks for the following DNS SRV record.

```
_connection_broker
```

See the guide for [Setting up Connection Broker DNS SRV Records](#) for instructions on setting up this DNS SRV record.

You can hard-code the Connection Broker address into the Leostream Agent, as follows:

1. Uncheck the **Obtain Connection Broker address automatically** checkbox.
2. Enter the Connection Broker IP address or fully qualified domain name into the **Address** edit field.
3. Click **Apply**.

To test if the DNS SRV record or entered Connection Broker address is valid, click the **Test** button. If the Leostream Agent successfully communicates with the Connection Broker, a dialog appears indicating that the Connection Broker is responding.

If the Agent cannot communicate with the broker, an error dialog appears.

Using SSL

All Leostream components communicate peer-to-peer. The Leostream Agent always expects SSL when receiving communications from the Connection Broker and uses SSL when sending outgoing communications to the Connection Broker.



Leostream Agent uses TLSv1.2.

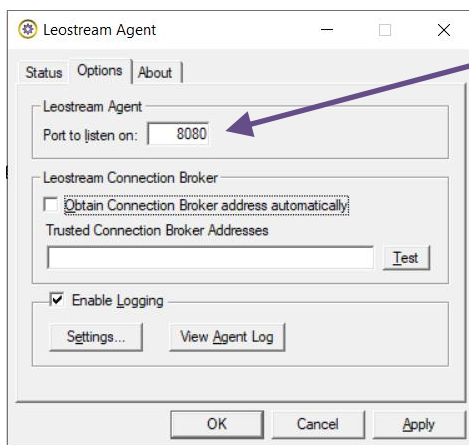


The Leostream Agent requires that MSVC runtime be installed in order to create an SSL certificate and key to use when communicating with the Connection Broker. If you do not have an MSVC runtime environment installed, the Leostream Agent will produce SSL errors.

Incoming SSL Communication

By default, the Leostream Agent listens for incoming SSL communications from the Connection Broker on port 8080. You can change the SSL port, as follows.

1. Open the Leostream Agent Control Panel dialog.
2. Go to the **Options** tab.
3. Enter a value for the **Port to listen on** edit field, as shown in the following figure.



Outgoing SSL Communications

For outgoing communications, the Leostream Agent always sends SSL communications to the Connection Broker on port 443.

Specifying Custom SSL Certificates

The Leostream Agent generates a new certificate every time the agent is started. If your organization prefers to use its certificates, you can place your valid certificate in the `tpc` directory in the Leostream Agent installation directory.

Please, note:

- The Leostream Agent supports certificate and RSA private keys in PEM format, only.
- Both the key and certificate should be stored in one PEM file.

- The PEM file must be located in the `<agent_install_directory>/tpc` directory.

Working with Microsoft® Windows® Firewalls

The Windows Firewall blocks incoming communication from the Connection Broker to the Leostream Agent. When the Connection Broker cannot communicate with the Leostream Agent, even though it is able to receive communications *from* the Leostream Agent, the Connection Broker marks the agent as **Unreachable**.

To avoid unreachable agents, when you install the Leostream Agent on a machine with an enabled Windows Firewall, the Leostream Agent automatically adds itself to the Windows Firewall exception list. When the Leostream Agent starts, it checks the **LeostreamAgent.exe** exception. Check that this exception was successfully added if you notice your Leostream Agents becoming unreachable by the Connection Broker.

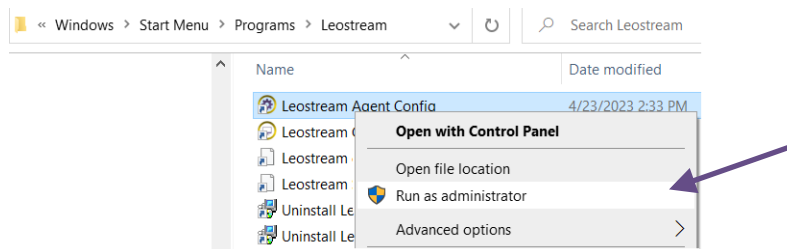
Leostream Agent Control Panel Dialog

Opening the Leostream Agent Control Panel Dialog

To open the Leostream Agent Control Panel dialog, double-click on the Leostream Agent icon in the Control Panel.

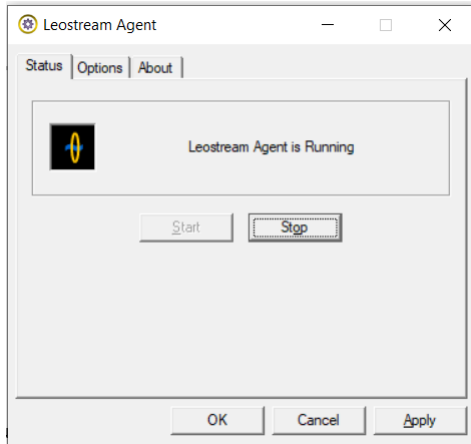


To modify the Leostream Agent options, you must be logged into the desktop as a user with administrator privileges, or run the Leostream Agent with administrator privileges. To run the Leostream Agent configuration with the necessary privileges, right-click on the Leostream Agent Config and select **Run as administrator**, as shown in the following figure.



Status Tab

The **Status** tab, shown in the following figure, indicates if the Leostream Agent is running or stopped, and allows you to toggle between these two states.

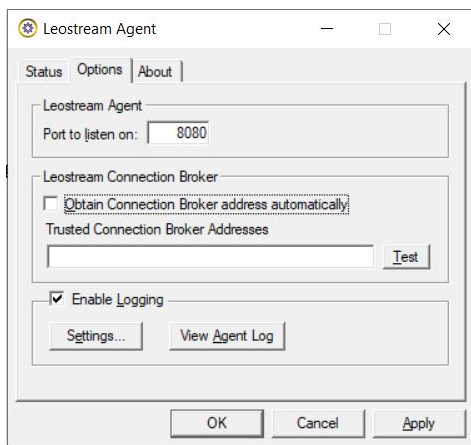


The Leostream Agent must be running in order for the Connection Broker to perform policy-based assignment control on this desktop. To toggle the running state of the Leostream Agent:

- Click **Stop** to stop the Leostream Agent. The Leostream Agent prompts you for a confirmation. When the Agent is stopped, the **Status** tab displays **Leostream Agent is Not Running**.
- Click **Start** to start the Leostream Agent. When the Leostream Agent is running, the **Status** tab displays **Leostream Agent is Running** and the Leostream icon rotates.

Options Tab

The **Options** tab, shown in the following figure, allows you to configure network and logging configurations.



Specifying the Listening Port

The **Leostream Agent** section allows you to specify the port used for communications coming from the Connection Broker. See [Using SSL](#) for more information.

Configuring the Connection Broker Address

The **Leostream Connection Broker** section allows you to enter the Connection Broker address and default port the Leostream Agent should use when initiating calls to the Connection Broker. See [Configuring the Connection Broker Address](#) for instructions on using this section.

By default, the Leostream Agent 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 Leostream Agent 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, the Leostream Agent queries the DNS SRV record.

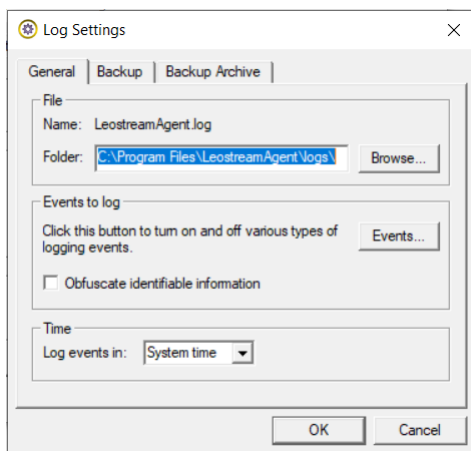
The Leostream Agent *initiates* calls to the Connection Broker indicated in the **Leostream Connection Broker** section. The Leostream Agent can *respond* to multiple Connection Brokers. When a Connection Broker initiates a call to the Leostream Agent, the Connection Broker provides the Leostream Agent with the address to use for any response. The Leostream Agent uses this address, instead of the value provided in the **Leostream Connection Broker** section when responding to that Connection Broker.

Logging

To enable Leostream Agent logging, select the **Enable Logging** checkbox. Ensure that you are maintaining logs before you contact Leostream Support with any issues that involve the Leostream Agent.

Configuring Log Settings

You can control logging options using the **Log Settings** dialog. To open this dialog, click the **Settings** button in the **Enable Logging** section. The following dialog opens.

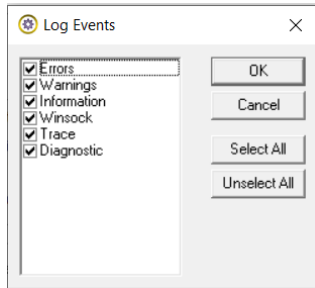


By default, the Leostream Agent stores logs in the `LeostreamAgent.log` file, which is written to the first writable directory from the following list.

- The location specified in the **Folder** edit field on the **General** tab
- The Leostream Agent installation directory

- A directory named `temp` inside of the Leostream Agent installation directory
- The `temp` directory inside the user folder for the currently logged in user
- The system `root` directory

The **Log Events** dialog, shown in the following figure, sets the level of information stored in the logs.



To open this dialog, click the **Set Events** button in the **General** tab of the **Log Settings** dialog. To modify the list of events, select the desired checkboxes and click **OK**.

Setting Log Time Stamps

The Leostream Agent can write logs in either the local system time of the machine on which it is installed, or in UTC. If your Connection Broker is in a different time zone from your desktops, logging in UTC may simplify correlating events in the Leostream Agent log with those in the Connection Broker.

By default, the Leostream Agent logs in the local system time. To switch to UTC:

1. On the Leostream Agent Control Panel Dialog, click the **Settings** button in the **Enable Logging** section on the **Options** tab.
2. In the **Time** section of the **Log Settings** dialog, select **UTC time** from the **Log events in** drop-down menu.
3. Click **OK** to close the **Log Settings** dialog.
4. Click **Apply** or **OK** on the Leostream Agent Control Panel Dialog.

Obfuscating User Information in Logs

The Leostream Agent never logs a user's password. However, usernames, domains, and desktop addresses are routinely added to the logs as the Leostream Agent manages the user's session. By default, these values are written to the logs in plain text.

If you prefer, you can tell the Leostream Agent to obfuscate personal information before writing to the logs. When the **Obfuscate identifiable information** option is selected on the **General** tab of the **Log Settings** dialog, the Leostream Agent obfuscates any personal information, including:

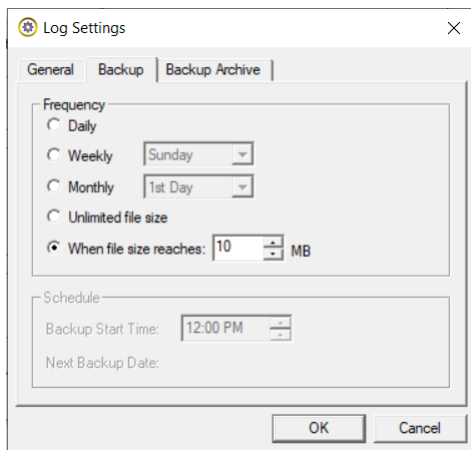
- User names

- Domain names
- Desktop addresses

The Leostream Agent is a multi-threaded process, and each process uniquely obfuscates the information. Therefore, the same username could appear in the logs with two different obfuscated values.

Backing up Logs

By default, the Leostream Agent maintains a single log file and continuously appends logs to that file. You can use the **Backup** tab, shown in the following figure, to break the log into multiple files, based on the date or file size.

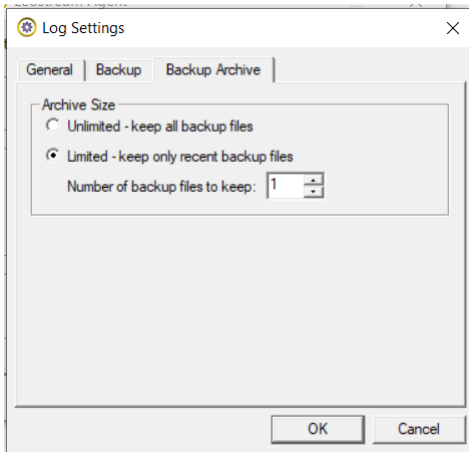


To change the backup schedule:

1. Select an option from the **Frequency** section.
2. Select a **Backup Start Time** in the **Schedule** section. The **Next Backup Date** text updates.
3. Click **OK**.

If you select any backup frequency except **Unlimited file size**, the **Backup Archive** tab enables. Use this tab, shown in the following figure, to indicate how many backup files to retain.

Backup files are stored with `.bak` extensions.



- **Unlimited – keep all backup files:** Retains all backup files.
- **Limited – keep only recent backup files:** Deletes all but the last n backup files, where n is the number you enter in the **Number of backup files to keep** field.

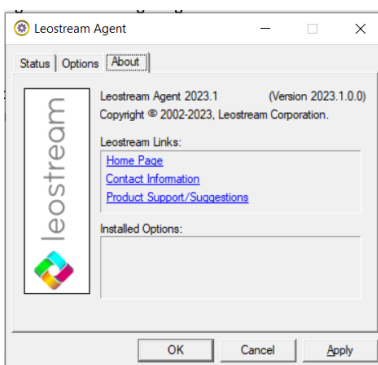
Viewing Logs

You can view the current Leostream Agent logs by clicking on one of the following two buttons.

- **View Agent Log:** Opens the `LeostreamAgent.log` file, containing the log information pertaining to Leostream Agent operations.
- **View Sign-On Log:** Opens the file that contains the current sign-on information. This button appears only if you installed the Leostream Agent with the single-sign on task selected.

About Tab

The **About** tab, shown in the following figure, provides information about your Leostream Agent installation, including what tasks were selected upon installation.



Click on any of the provided links to navigate to pages of the Leostream Web site.

Leostream Agent for Linux and macOS Desktops

The Java version of the Leostream Agent provides the Connection Broker with information about the connection status of remote users to their Linux and macOS desktops. In addition, the Leostream Agent allows you to automatically register any Linux and macOS desktop with the Connection Broker **Uncategorized Desktops** center.

The Leostream Agent allows you to:

- Discover Linux and macOS machines – If you have an **Uncategorized Desktops** center in your Connection Broker, machines that are not categorized in another center will register with the Connection Broker when you install the Leostream Agent.
- View desktop attributes for Linux and macOS machines listed on the > **Resources > Desktop** page.
- Obtain information about the desktop and active user sessions by using **Status** option on the > **Resources > Desktop** page.
- Perform actions when a user logs out of their remote session, providing additional policy control over the user's session (see **Working with macOS Desktops** for requirements when leveraging this functionality on Apple macOS devices).
- Perform actions when a user disconnects from their remote session.
- Perform actions when a user is idle on their remote session.
- Perform single sign-on for PCoIP sessions established to Red Hat or Ubuntu Linux desktops.
- Log out rogue users when a Connection Broker user connects to their remote desktop.
- Obtain session information for users logging into their remote desktops.
- Redirect USB devices from Leostream Connect clients to Linux machines, only.

This Java version of the Leostream Agent does not support the Leostream location-based printer assignment feature.

The Leostream Agent for Linux and macOS requires a JDK version 1.7 or higher.

Working with macOS Desktops

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

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

Configuring the Connection Broker Address

By default, the Leostream Agent contacts the Connection Broker at the address you provided during installation. If you do not provide an address during installation, the Leostream Agent can automatically discover the Connection Broker address from the following DNS SRV record.

```
_connection_broker
```

See the [Leostream Installation Guide](#) for instructions on setting up this DNS SRV record. If you do not want to use the DNS SRV record, set the `connection_broker_auto_discovery` parameter in the `leostreamagent.conf` file to `false`.

At any point, you can hard-code the Connection Broker address using the `connection_broker_address` parameter in the `leostreamagent.conf` (see [Understanding the leostreamagent.conf File](#)).

If the Leostream Agent is not detecting the DNS SRV record, ensure that the `resolve.conf` file on the desktop where the Leostream Agent is installed contains information for the correct domain. If the DNS SRV record exists in a different domain from that specified in the `resolve.conf` file, the Leostream Agent cannot discover the Connection Broker address.

Using SSL

The Leostream Agent always sends communications to the Connection Broker using SSL on port 443.

By default, the Leostream Agent listens for incoming SSL communications from the Connection Broker on port 8080. You can change this default port by setting the `agent_port` parameter in the `leostreamagent.conf` file.

The Leostream Agent communicates only using TLSv1.2.

Using USB Redirection

In order to use the Leostream Agent to accept USB devices redirected from Leostream Connect, the Leostream Agent installer must build USB drivers on the remote desktop. In order to build the drivers, the installer provides the following required header files:

- `hcd.h`
- `hub.h`

The Leostream Agent provides these header files for kernel versions 2.6.15 to 2.6.34. More recent kernel versions include these files in the kernel source.



USB redirection is not supported on macOS or for Linux kernel version higher than 4.5.

To determine which kernel version your Linux desktop is running, execute the following command.

```
uname -r
```

The Leostream Agent uses files in the kernel source directory to execute the `make` command that builds the drivers. These files are typically located in `/usr/src/kernels`. If your operating system does not provide the appropriate kernel files, you must download and install them, using the appropriate distribute method for your operating system.

For example, use the following commands for desktops running a CentOS operating system.

```
yum install kernel-devel
yum install gcc
```

If you installed the USB drivers, check that the daemon is live by running the following command:

```
cat /proc/modules |grep lsusb
```

If the daemon is not live, the remote desktop cannot accept USB devices. Contact supportsite@leostream.com for a resolution.

Adding Local Users to the Remote Desktop

You can use the Leostream Agent to automatically add local users to the remote desktop. Use the **Login user as** drop-down in the user's role to indicate if the Connection Broker should automatically add a local user to the remote desktop when this user logs in. For users logging in to a Linux remote desktop, use one of the following 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 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 user's home directory. Any information stored in their home directory can be recovered by the administrator.

- **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 home directory as soon as the user logs out of the desktop.



Because the user's home directory is deleted, the user loses all locally stored information.

Starting, Restarting, and Stopping the Leostream Agent

The Leostream Agent service automatically starts after installation. Should you need to restart the service, use the associated `service` command for the given operating system on which the Leostream Agent is installed. For example, on CentOS, use the `service` command, as follows.

- To start the Leostream Agent: `systemctl start leostreamagentd`
- To restart the Leostream Agent: `systemctl restart leostreamagentd`
- To stop the Leostream Agent: `systemctl stop leostreamagentd`

To view the status of the Leostream Agent process:

```
systemctl status leostreamagentd
```

When installed on a macOS desktop, use the `launchctl` command to start the Leostream Agent, for example:

```
sudo launchctl load /Library/LaunchDaemons/com.leostream.leostreamagentd.plist
```

To stop the Leostream Agent:

```
sudo launchctl unload /Library/LaunchDaemons/com.leostream.leostreamagentd.plist
```



If you update Java while the Leostream Agent is running, you must restart the Leostream Agent to switch to the new Java version.

Understanding the leostreamagent.conf File

To configure the Leostream Agent, edit the `leostreamagent.conf` file. During installation, this file is automatically created in the Leostream Agent installation directory, by default, `/opt/leostreamagent`.

- `agent_port` – The Leostream Agent port for incoming calls. The default port is 8080.
- `connection_broker_address` – The IP address or fully qualified domain name, if the system has DNS access, of your Connection Broker. The Leostream Agent always tries this Connection Broker address, first.

If the Leostream Agent fails to establish communications with the Connection Broker at this address, and the `connection_broker_auto_discovery` parameter is set to `true`, the Leostream Agent tries the address in the Connection Broker DNS SRV record.

If the `connection_broker_address` parameter is empty or not included in the `leostreamagent.conf` file, and the `connection_broker_auto_discovery` parameter is set to `true`, the Leostream Agent tries the address in the Connection Broker DNS SRV record.

- `connection_broker_auto_discovery` – Determines if the Leostream Agent will try to use the Connection Broker DNS SRV record to auto-detect the Connection Broker address.

To only use the DNS SRV record, remove the `connection_broker_address` parameter from the `leostreamagent.conf` file. The default is `true`. If `false`, the Leostream Agent will not try to use the Connection Broker DNS SRV record.

- `enable_sso` – Enables the single sign-on feature for PCoIP connections.
- `log_time_zone` – The time zone used for recording Leostream Agent log messages. By default, logs are recorded in system time, as specified by the `system` value. Change the parameter to `utc` to log Leostream Agent messages in the UTC time zone.
- `rgsender_path` – Provides the default path to the HP ZCentral Remote Boost (RGS) Sender. If not specified, the default path is `opt/hpremote/rgsender/rgsender.sh`.
- `registered_brokers` – A list of all Connection Brokers that have registered for notifications from this Leostream Agent.
- `ssl_ciphers` – A comma-separated list of the SSL ciphers that the Leostream Agent will use for Connection Broker communications, by default:

```
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA256
```

- `sso_desktop` – Determines the windows manager used to perform single sign-on to the operating system, either `lightdm` or `gdm`.

- `tgxsender_path` – Provides the default path to the Mechdyne TGX Sender. If not specified, the default path is `/opt/mechdyne/teleGraphix/bin64/TGXSender`.
- `trace_level` – Indicates the type of information to include in the Leostream Agent logs. Specify a comma-separated list including any of the following values: `error`, `warn`, `info`, `trace`, `diag`, `except`, `stack`, and `dump`.
- `vncsender_path` – Provides the default path to the VNC server. If not specified, the default path is `/usr/bin/vncserver`