LEOSTREAM™ | Security Guide

Connection Broker

Advanced Connection and Capacity Management for Hybrid Clouds

Version 9.0 – March 2019

Contacting Leostream

Leostream Corporation
271 Waverley Oaks Rd.
Suite 206
Waltham, MA 02452
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 directions, email **sales@leostream.com**.

Copyright

Trademarks

Patents

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

Contents

Overview

This section describes the different pieces of the Connection Broker that are relevant to a security audit. Three key areas for analysis include:

- Network level access
- Application level access
- Maintenance.

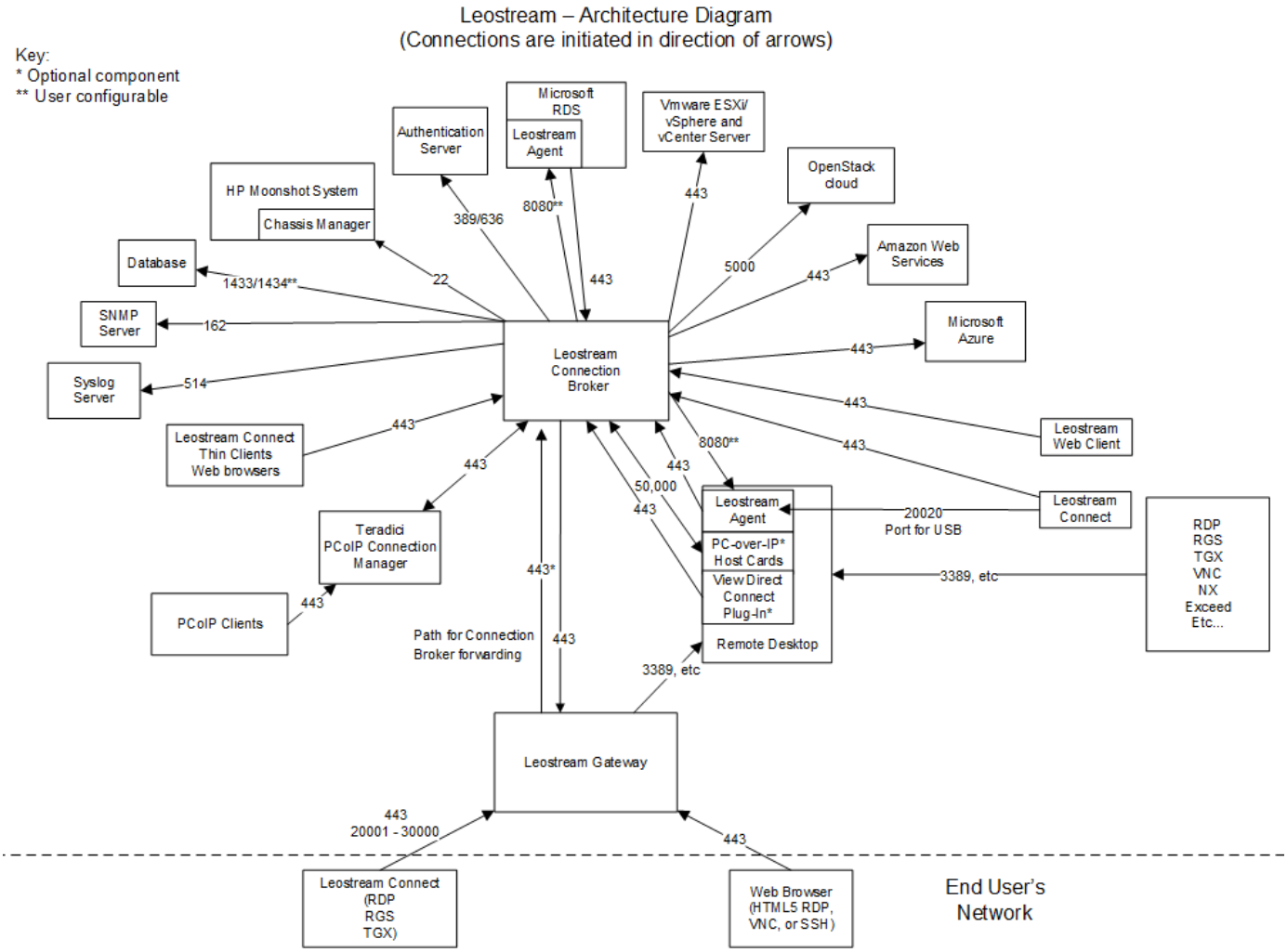
The Leostream Connection Broker installer is packaged as an RPM or DEB file for installation on a 64-bit CentOS or Red Hat Enterprise Linux operating system, latest version 7, Ubuntu 16.04, or SUSE Linux Enterprise Server 12 SP3 operating system.

The Connection Broker uses the operating system libraries, such as OpenSSL, whenever possible, with one exception. The Connection Broker application installs and uses Apache Web Server version 2.4.38.

Network Level Access

By default, the Connection Broker uses port 443 for SSL communications. Port 80 is open, but not used for communication with the Leostream Agent or Leostream Connect clients. You can block port 80 using the **Block all traffic on port 80** option on the **> System > Settings** page. Port 50,000 is open if you enable PCoIP and is used by the Connection Broker to communicate with PCoIP devices using the Connection Management Interface.

The following diagram summarizes the ports used by the Connection Broker. All Leostream components communicate peer-to-peer. The Connection Broker sends TDS traffic to and from the SQL Server database using TCP/IP, instead of named pipes.

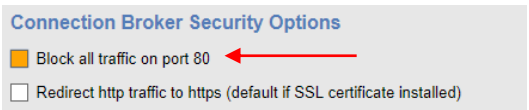


Application Level Access

Configuring Secure Connection Broker Communication

The Connection Broker includes a default Leostream certificate, which is used to encrypt traffic between the Connection Broker, Leostream Agents, and Leostream Connect clients. Although traffic between these components uses port 443, by default, port 80 remains open.

If you have security guidelines that restrict the use of port 80, select the **Block all traffic on port 80** option available in the **Connection Broker Security Options** section of the **> System > Settings** page, shown in the following figure.



After selecting this option, click **Save** on the **> System > Settings** page. You must reboot the Connection Broker to block port 80.

 HTTP addresses are not redirected to HTTPS, even if the **Redirect http traffic to https** option is selected on the **> System > Settings** page. If you block all traffic to port 80 and try to use an HTTP address to access the Connection Broker, the Web browser cannot contact the Connection Broker.

The Connection Broker allows you to indicate which protocols to use for secure communications with Leostream Connect clients and Leostream Agents. Use the options on the **> System > Settings** page to indicate if the Connection Broker uses TLSv1, TLSv1.1, or TLSv1.2. You cannot disable TLSv1.2 as that is the only SSL protocol accepted by Leostream Agents.

The **Connection Broker Security Options** section of the **> System > Settings** page includes an additional option that allows you to configure the Cipher Suite used for SSL. In the **Web server "SSLCipherSuite" directive** edit field, enter a colon-separated cipher-spec string consisting of OpenSSL cipher specifications to configure the Cipher Suite. For more information on the syntax entered in this field, see the **Apache Module mod_ssl** documentation.

 The TLS versions accepted by the Connection Broker and the SSLCipherSuite settings are not changed when you upgrade your Connection Broker. If you use the default SSLCipherSuite and want to upgrade to the latest default settings after upgrading your Connection Broker, go to the **> Sytem > Settings** page, choose the TLS versions you want to allow, and delete all text in the **Web server "SSLCipherSuite" directive** edit field. Save the **> System > Settings** form and restart your Connection Broker to obtain the up-to-date default values.

Restricting User Access

You can access the Connection Broker at the application level via either:

- The Connection Broker Web interface
- The XML-RPC API

Roles restrict how much of the Connection Broker functionality users can access, via either the Web interface or XML-RPC API. You can create different user roles to restrict access to the various elements of the Connection Broker including the XML API, maintenance, network, and general configuration (see "Managing User Roles and Permissions" in the Connection Broker Administrator's Guide).

The Connection Broker provides a default Administrator account with locally stored user credentials. The Administrator password is stored encrypted.

Logging User Access

The Connection Broker logs all user access, including:

- Which desktops the user was offered

- Which desktops the user selected
- What protocol configuration was used to connect the user to their desktop
- Which desktops the user logged into
- When the user's session became idle
- When the user logged into, logged out of or disconnected from a desktop
- When the user locked and unlocked the desktop

From the Connection Broker Web interface, you can manually log users out of any desktop or the Connection Broker (see "Logging Users Out" in the Connection Broker Administrator's Guide).

You can view the logs on the **> System > Logs** page. For information on extracting the log information for use in a Microsoft® Excel® spreadsheet or a SQL Server database, see **Appendix A: Exporting Log Contents**.

 The Connection Broker logs contain personal information for your users, such as usernames, full names, email address, etc. When exporting logs, take appropriate measures to protect your users' information.

Client Application Access

Different types of clients use the following communication protocols:

- Leostream clients, including Leostream Connect, use the Leostream XML-RPC based API to communicate with the Connection Broker.
- The Dell Wyse® WTOS series thin clients use a URL based API.
- The Connection Broker Administrator Web interface uses standard HTML.
- PCoIP Zero clients use the PCoIP Broker Protocol

Communications use port 443 and are encrypted using the default Leostream certificate. You can optionally upload a custom signed or unsigned certificate into the Connection Broker (see "Generating and Installing Self-Signed SSL Certificates" or "Installing a Signed SSL Certificate and Intermediate Certificate" in the Connection Broker Administrator's Guide).

By default, port 80 remains open and the Connection Broker does not automatically redirect communications on port 80 to port 443. See Configuring Secure Connection Broker Communication for instructions on closing port 80.

VMware® vCenter Server Application Access

The user associated with a VMware centers in the Connection Broker must have the following VMware vCenter Server permissions, in order to use all Leostream functionality.

Action	VMware Privilege
Power On / Resume	VirtualMachine.Interact.PowerOn
Power Off / Shutdown	VirtualMachine.Interact.PowerOff
Provisioning	Resource.AssignVMToPool VirtualMachine.Inventory.Create VirtualMachine.Provisioning.Customize VirtualMachine.Provisioning.DeployTemplate VirtualMachine.Provisioning.ReadCustSpecs
Cold Migration	Resource.AssignVMToPool Resource.ColdMigrate
Reboot	VirtualMachine.Interact.PowerOff VirtualMachine.Interact.PowerOn VirtualMachine.Interact.Reset
Revert to Snapshot	VirtualMachine.State.RevertToSnapshot
Suspend	VirtualMachine.Interact.Suspend
Delete	VirtualMachine.Inventory.Delete

If the user does not have the permission to perform a requested action, such as deleting a virtual machine, the Connection Broker logs an error.

All communications with vCenter Server are encrypted using SSL.

Microsoft® Active Directory® Access

The Connection Broker logs into the Active Directory service with the account specified on the **Edit Authentication Server** page. If you use the Leostream feature to join desktops to the domain, the Leostream Agent on the desktop uses this account to perform the domain join

The credentials for this account are stored in the Connection Broker in an encrypted form.

Event Monitoring

The Connection Broker provides two versions of an SNMP MIB and can signal a range of events to an external monitoring system, which can signal events using pagers, emails, etc. Supported events include, but are not limited to, pool thresholds and Connection Broker metric thresholds. Contact supportsite@leostream.com for a complete list of events that can trigger SNMP events.

You can also send Connection Broker log messages to a syslog server.

Connection Broker Maintenance

Connection Broker Virtual Application Account

The Connection Broker installation process automatically creates a user named `leo` and installs the Connection Broker in the `/home/leo` directory. By default, the `leo` user does not have an assigned password.

If you need to log in as the `leo` user, log in as `root` and assign a password to the `leo` user using the following command.

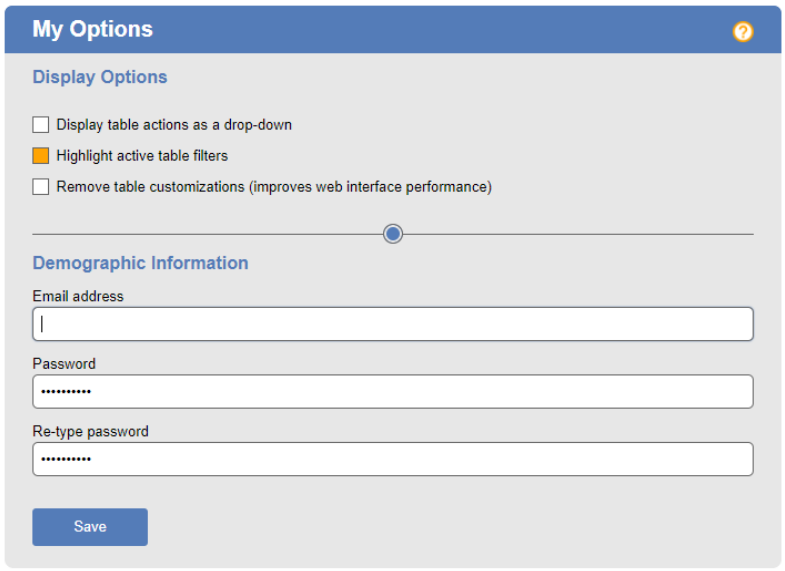
```
passwd leo
```

The Connection Broker Web Administrator Account

The Connection Broker includes a default administrator account that you can use to log into Connection Broker Administrator Web interface. This user is listed in the **> Resources > Users** page with the following default attributes.

- Name: Administrator
- Role: Administrator
- Login: admin
- Password: leo

To change the administrator password, log into the Connection Broker as the administrator, and go to the **> Signed in as > My Options** page, shown in the following figure.



1. Enter a new password in the **Password** edit field
2. Reenter the new password in the **Re-type password** edit field
3. Click **Save**

 The Connection Broker cannot remind you of the Administrator's password, or of the password of any locally defined user. If you forget your password, you must change it at the Linux shell of the Connection Broker machine, as follows.

1. Log in to the Linux shell of the Connection Broker machine, as either the `root` or `leo` user.
2. At the Linux shell prompt, enter the following command:

   ```
   /home/leo/app/control.pl –change_password –user username –
   new_password password
   ```

   Where *username* is the login name of the account you want to modify and *password* is the new password to use for this account.

The password is changed in the current Connection Broker database. For example, if the Connection Broker is connected to an external database, the password changes only in the external database and not in the internal database. Therefore, if you switch back to the internal database, or to another existing external database, you must run the `control.pl` command, again, to change the password in that database.

Patch Management Detection and Deployment

Use the Leostream update mechanism to update the Connection Broker. See the "Updating the Connection Broker" section in the **Using the Leostream Connection Broker Console Guide** for information on getting Connection Broker updates.

If internet access is available, the update mechanism indicates if your Connection Broker is up to date. If you need to perform an offline update, please contact **support@leostream.com** for an update file.

Backing Up the Connection Broker

You can back up the Connection Broker using any backup system intended for virtual machines.

You can also backup the Connection Broker internal database and its settings using the **> System > Backup** page. This backup method is more efficient then backing up the entire appliance, however does not backup the Microsoft SQL Server or PostgreSQL database, if used. See the "Scheduling Remote Backup for the Connection Broker" section in the Connection Broker Administrator's Guide for information on using this feature.

Backing Up an External Database

If you are using an external SQL Server or PostgreSQL database, back up the database using the standard tools and techniques for those databases.

Connection Broker Internal Database

The Connection Broker maintains an inventory of the following information.

- Users: The Connection Broker stores passwords for users only if the users are created locally on the **> Resources > Users** page.
- Clients
- Desktops and their environments
- Microsoft Active Directory user credentials: Encrypted.
- Machine centers: Access credentials are encrypted.
- Locations, roles, and all other operational parameters

If you are using an internal Connection Broker database, you can backup this information by selecting the **Backup internal database** option on the **> System > Maintenance** page. The downloaded `.tgz` file stores additional configuration files, including the Connection Broker ID and external database settings. See the "Backing Up and Restoring an Internal Connection Broker Database" and "Backing Up Your Connection Broker" sections in the Connection Broker Administrator's Guide for more information on generating the `.tgz` file.

Appendix A: Exporting Log Contents

You can extract the contents of the Connection Broker log in two ways:

- Download a CSV-file
- Click the **Download Leostream technical support logs** link

CSV-File

To download a CSV:

1. Go to the **> System > Log** page
2. Click the **Export list** link near the top-right of the page.
3. When prompted, save the CSV-file

The CSV-file contains the entire contents of the **> System > Log**, not just the information on the currently displayed page.

Download Technical Support Logs

When you click the **Download Technical Support Package** link at the bottom-left of any Connection Broker Web interface page, the Connection Broker downloads a ZIP-file containing all the information stored in the broker.

To extract the log information from the `.zip` file:

1. Extract the downloaded `.zip` file.
2. In the directory you unzipped the downloaded logs into, extract the `sql-log.zip` file, into a directory called `sql-log`.

   The `sql-log` directory contains a file called `sql-log.txt`, which is a tab delimited file containing the contents of the **> System > Log** table. You can then import this table into an Excel spreadsheet for analysis.

   Users are referenced in the table by their user ID.
3. To see the mapping between users and user IDs, extract the `sql-user.zip` file.

 Connection Broker logs contain personal information for your users, such as usernames, full names, email address, etc. The logs do not include passwords.

Appendix B: Security Audit Statement

The following statement is provided for inclusion in your security audit.

> The Leostream Connection Broker is an application that installs on a 64-bit CentOS or Red Hat Enterprise Linux operating system, version 7.3 or later, or Ubuntu 16.04 operating system. Leostream fully maintains the application software. Updates are issued on a scheduled basis for major functionality additions, and as needed for defect vulnerability resolution. Major updates occur approximately once a year. Minor updates are scheduled to meet customer requirements or based on defect and vulnerability severity.
>
> Connection Broker updates are bundled into single, automatically installed package. This requires that the Web browser be able to connect to both the Linux machine running the Connection Broker and the Internet. The Connection Broker can also be updated without Internet access, using an update package obtained from the Leostream support team.
>
> The Connection Broker application utilizes operating system libraries, with the exception of the Apache Web Server. Updates to the Apache Web Server are bundled into the Connection Broker update package. Updates to the operating system libraries are the responsibility of the customer and can be performed using standard Linux update mechanisms.
>
> Customers are notified of Leostream updates through regular email newsletters. These newsletters are issued quarterly, but are released on an as-needed basis for urgent issues. Release notes provide details of the changes in each update that reference any relevant security updates. The availability of product updates can also be found from within the Connection Broker, using the **> System > Maintenance** page. Updates are available without additional charge to any customer with an active support contract.
>
> The Connection Broker reports on the version numbers of connecting clients and Leostream Agents. Leostream Agents can be centrally updated from within the Connection Broker.
>
> The Leostream product suite is frequently reviewed internally as part of the Quality Assurance process, and also validated via regular assessments by our strategic partners. We actively monitor both CERT and SANS for pertinent severity information and updates.