leostream

Remote Desktop Access Platform

Leostream Connection Broker Security Review

Overview of Connection Broker Network and Application-Level Access

Version 2023
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 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.

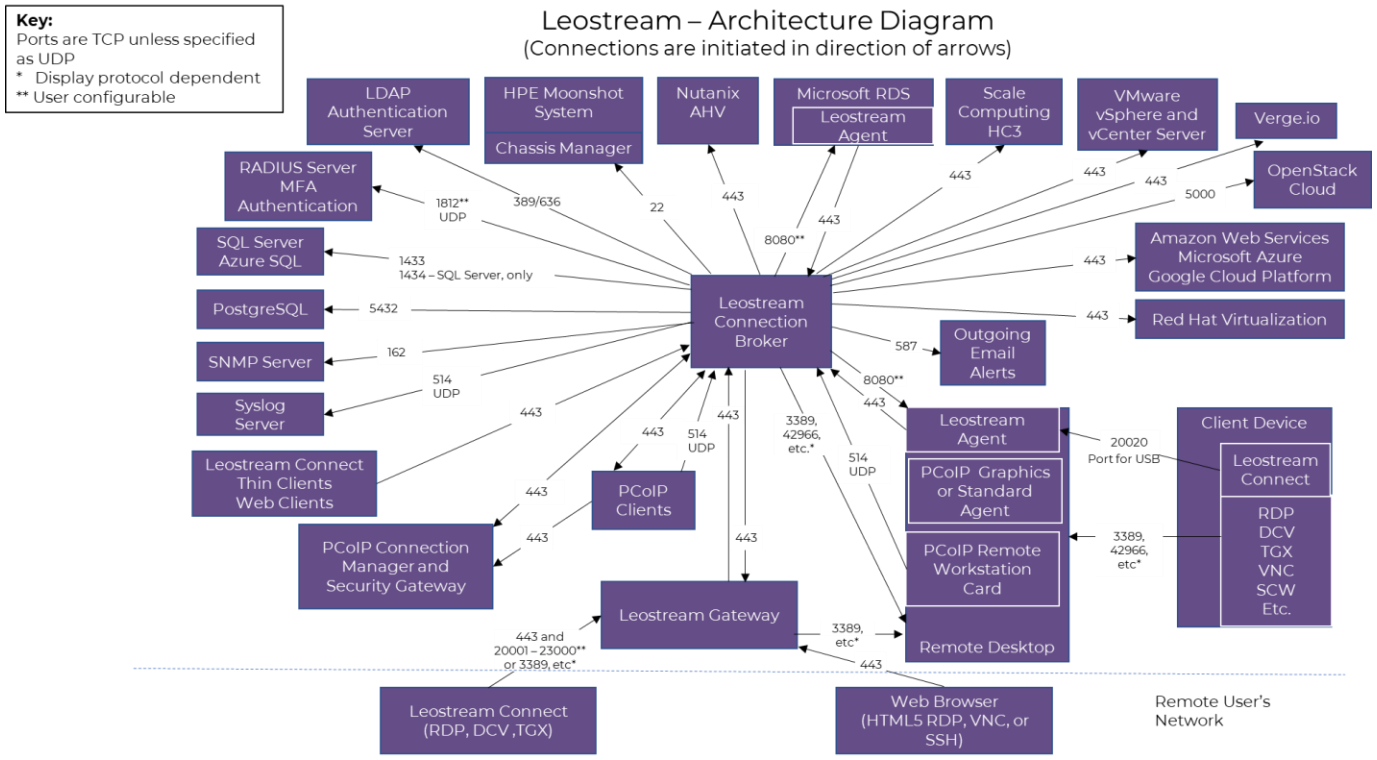
The Connection Broker is packaged for installation on any virtual or physical machine running the latest Red Hat® Enterprise Linux® 8.x operating system and its derivatives, such as Rocky and Alma Linux.

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 2.4.57.

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.

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.



Connection Broker Application-Level Access

The Connection Broker Web Administrator Account

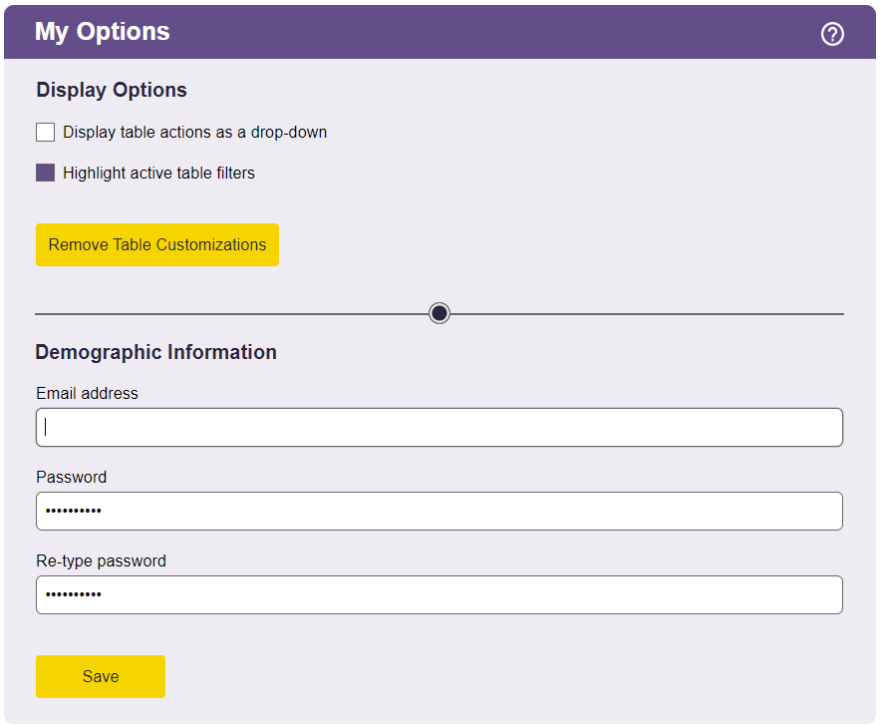
The Connection Broker includes a default administrator account that you can use to log into Connection Broker Administrator Web interface. This user is listed in the **> Resources > Users** page with the following default attributes.

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

⚠ Leostream recommends changing this password to a more secure password that adheres to your corporate security guidelines as soon as you license your Connection Broker.

Changing the Default `admin` User's Password on the "My Options" Page

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**

Changing the Default `admin` User's Login Name and Password on the "Users" Page

The default `admin` user is defined locally in the Connection Broker database. As with any local user, you can edit the user's record on the **> Resources > Users** page of your Connection Broker. Editing the user allows you to change the login name, enter an email address, change the password, and enable MFA.

To edit the `admin` user:

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

2. Click or select the **Edit** action for the default `admin` user.

3. Use the **Display Name** field to change the default name of `Administrator`. This is the value that appears in the **Name** column of the **> Resources > Users** page.

4. Enter an optional **Email address** for the default local administrator.

5. Use the **Login name** field to change the default local administrator from `admin` to your name of choice. The Connection Broker does not treat login names as case sensitive.

6. Enter an initial password for the local administrator in the **Password** and **Re-type password** edit fields. Passwords are case sensitive.

7. Indicate if the local administrator requires multifactor authentication by selecting one of the available identify providers in the **MFA Providers** drop-down menu.

8. Click **Save**.

Resetting the Default `admin` Password

 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:

   ```
   /var/lib/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.

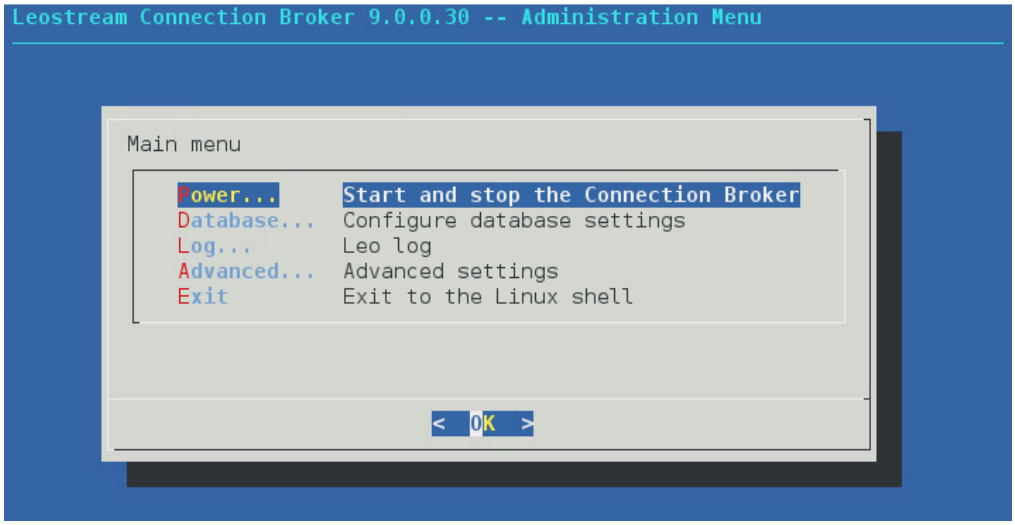
The password is changed in the current Connection Broker database. For example, if the Connection Broker is connected to an external database, the password changes only in the external database and not in the internal database. Therefore, if you switch back to the internal database, or to another existing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

Disabling Logins for the Default admin User

You can disable the default `admin` user using the Connection Broker Administrator Menu found in the Connection Broker machine console. To access the Connection Broker Administrator Menu, log into the machine running your Connection Broker as the `root` user and issue the following command.

```
su - leo
```

The **Administration Menu**, shown in the following figure, opens.



1. Select **Advanced** from the **Main menu** to open the **Advanced settings** page.
2. Select the **Admin** option.
3. Select **OK**.

Repeat the procedure to enable admin logins.

Connection Broker Settings for Securing Communications

The **> System > Settings** page contains a set of options that allow you to tune the security settings for Connection Broker communications.

Restricting HTTP Access

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 in the **Connection Broker Security Options** section.

After selecting this option and clicking **Save**, reboot the Connection Broker to close port 80.

When port 80 is blocked, you cannot access the Connection Broker Administrator Web interface or Leostream Web client using HTTP. You must enter an HTTPS address to sign into the Connection Broker.

If you do not block port 80 and are using the default Leostream certificate, you can select the **Redirect http traffic to https** option to redirect the **Sign in** page from HTTP to HTTPS. The Connection Broker automatically redirects HTTP to HTTPS after you install a custom SSL certificate.

Configuring TLS Versions and SSL Cipher Suites

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.

 The Leostream Agent require the TSLv1.2 SSL protocol. Therefore, you cannot disable TLSv1.2 in your Connection Broker.

The **Enable Strict-Transport-Security header (HSTS)** option on the **> System > Settings** page allows you to instruct the Connection Broker to enforce strict transport security and sets the expiration time for when the Connection Broker can be accessed using only HTTPS. Enter the expiration time in seconds. The default value is one year.

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.

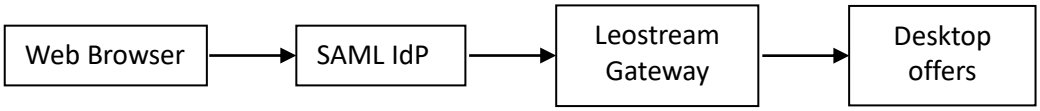
 The TLS versions accepted by the Connection Broker and the SSLCipherSuite settings are not changed

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, check that the new default Cipher Suites are shown in the the **Web server "SSLCipherSuite" directive** edit field, and restart your Connection Broker to obtain the up-to-date default values.

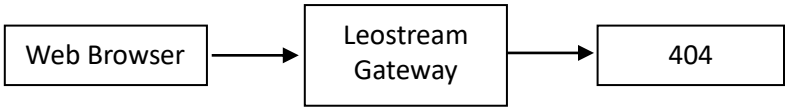
Blocking External Access to the Login Page

If your Leostream environment includes Leostream Gateways that forward login traffic to your Connection Broker *and* you leverage a SAML-based Identity Provider (IdP) for authentication, you can block access to the Leostream Login page by selecting the **Block web browser login dialog when accessing Connection Broker via a Leostream Gateway** option on the **> System > Settings** page. Enabling this option keeps bad actors from accessing the Login form for your Leostream environment.

Regardless of if the **Block web browser login dialog when accessing Connection Broker via a Leostream Gateway** option is selected or not, the following workflow is always supported.



With this option selected, however, pointing a web browser directly at the Leostream Gateway displays a 404 Not Found page.



Setting the Content Security Policy

The **Content Security Policy** (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. You can view and edit the Connection Broker Content Security Policy HTTP header using the **Web server "Content-Security-Policy" HTTP header** field on the **> System > Settings** page.

By default, the Connection Broker CSP uses the `frame-ancestors` directive to block the Connection Broker **Sign in** page from being embedded in an iframe. If you want to include the Leostream Sign in page in an iframe in your corporate portal, ensure that you add the appropriate site to the list of `frame-ancestors`.

Because the `frame-ancestors` directive obsoletes the `X-Frame-Options` header, the Connection Broker no longer includes the `X-Frame-Options` HTTP response header. Some security scanning software may flag the missing `X-Frame-Options` header.

Setting HTTP Security Headers

- Use the **Web server "Cross-Origin-Embedder-Policy" HTTP** header to prevent a document from loading any cross-origin resources that don't explicitly grant the document permission.

   If you use Duo for MFA and set this value to `require_corp` then you must configure Duo to return a value of `cross-origin` to ensure that Leostream has permission to use the Duo resource.

- Use the **Web server "Cross-Origin-Opener-Policy" HTTP header** to ensure a top-level document does not share a browsing context group with cross-origin documents.

- Use the **Web server "Cross-Origin-Resource-Policy" HTTP header** to convey a desire that the browser blocks no-cors cross-origin/cross-site requests to the given resource.

Closing Leostream Gateway Ports for Disconnected Desktop Sessions

In many circumstances, for optimal security, the Connection Broker should instruct the Leostream Gateway to close forwarded ports as soon as the user disconnects or logs out from their remote desktop. However, the Connection Broker may receive disconnect notices from the Leostream Agent when desktop connections are dropped due to temporary network outages.

Some display protocols, such as Mechdyne TGX and HP ZCentral Remote Boost, attempt to re-establish the desktop connection after a loss of network. If the Leostream Gateway forwarded port is dropped, however, the desktop connection is unavailable even after the network is restored.

If you are using a display protocol that automatically attempts to re-establish lost desktop connections, you can use the **Delay closing gateway forwarding ports on disconnect** option to hold the forwarded port open for the specified length of time, to allow the display protocol client to reconnect to the desktop when the network is restored using the original forwarded port.

If the **Delay closing gateway forwarding ports on disconnect** option is set to zero or to a value shorter than the length of time the display protocol client attempts to reconnect to the desktop, the user must return to their Leostream session to request the desktop connection and open a new Leostream Gateway port.

Throttling User Login Attempts

In the event your Connection Broker is exposed to the internet, you can leverage the Connection Broker's built-in rate limiting to mitigate a denial-of-service attack due to login attempts for domain and local Connection Broker users. Configure the **Throttle login attempts** drop-down menu to indicate the throttling method to use.

If three failed login attempts originate from the source indicated by the selection in the **Throttle login attempts** drop-down menu, the Connection Broker waits for a pre-determined period of time before resuming checks against your LDAP server for submitted credentials from that source.

Working with SSL Certificates

The Connection Broker includes a default Leostream certificate that is used to encrypt communication between the Connection Broker and the Leostream Agents and Leostream Connect clients. Each Connection Broker generates a unique certificate during installation.

In a production environment, replace the default Leostream certificate with your organization's signed certificate. You can upload your SSL private key, certificate, and any required intermediate certificates into your Connection Broker using options on the **> System > Maintenance** page.

Each Connection Broker stores the certificate information in its internal database, in the `httpd` table. Connection Brokers in a cluster do not share a common certificate. You must install the certificate on each Connection Broker in the cluster.

When the Connection Broker boots, it copies the certificate information from its internal database to the `/var/lib/leo/conf` directory, and alters the Apache configuration file `/var/lib/leo/conf/httpd.conf` to reference the appropriate certificate information, as follows.

- If you are using the default Leostream certificate, `httpd.conf` references:
  - /var/lib/leo/conf/leostream_default.crt
  - /var/lib/leo/conf/leostream_default.key

- If you uploaded a certificate, `httpd.conf` references:
  - /var/lib/leo/conf/server.crt
  - /var/lib/leo/conf/server.key
  - /var/lib/leo/conf/server.int_crt

Any manual changes you make to the Apache configuration file are lost during a Connection Broker reboot.

Connection Broker Configuration Files

The Connection Broker stores the default application configuration files in the `/var/lib/leo/conf` directory, including configuration files for the internal PostgreSQL database and Redis.

The `/var/lib/leo/conf/postgresql.conf` file is copied into `/var/lib/leo/postgres/postgresql.conf` each time the Connection Broker boots, and the copy is modified with the local system's current time zone.

For information on the files related to SSL certificates, see **Working with SSL Certificates**.

Restricting User Access

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

- The Connection Broker Web interface

- The XML-RPC API
- The RESTful API

Roles restrict how much of the Connection Broker functionality users can access, via either the Web interface or one of the APIs. You can create different user roles to restrict access to the various elements of the Connection Broker including the API and the different pages in the Administrator Web interface (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 (see **The Connection Broker Web Administrator Account**). 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 personally identifiable information (PII) for your users, such as usernames, full names, email address, etc. When exporting Technical Support Packages, take appropriate measures to protect your users' information and share logs only with trusted third-parties.

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 **Restricting HTTP Access** for instructions on closing port 80.

VMware® vCenter Server Application Access

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

Leostream Action	VMware Privileges	vCenter Role Terminology
Inventory	System.Anonymous System.Read System.View	
Power On	VirtualMachine.Interact.PowerOn	> Virtual Machine > Interaction > Power on
Power Off	VirtualMachine.Interact.PowerOff	> Virtual Machine > Interaction > Power off
Shutdown	VirtualMachine.Interact.PowerOff	> Virtual Machine > Interaction > Power off
Suspend	VirtualMachine.Interact.Suspend	> Virtual Machine > Interaction > Suspend
Resume	VirtualMachine.Interact.PowerOn	> Virtual Machine > Interaction > Power on
Reboot	VirtualMachine.Interact.PowerOn VirtualMachine.Interact.PowerOff VirtualMachine.Interact.Reset	> Virtual Machine > Interaction > Power on > Virtual Machine > Interaction > Power off > Virtual Machine > Interaction > Reset
Revert to snapshot	VirtualMachine.State.RevertToSnapshot	> Virtual Machine > Snapshot management > Revert to snapshot
Create snapshot	VirtualMachine.State.CreateSnapshot	> Virtual Machine > Snapshot management > Create snapshot
Provisioning	Datastore.AllocateSpace Host.Inventory.EditCluster Resource.AssignVMToPool VirtualMachine.Inventory.CreateFromExisting VirtualMachine.Provisining.Clone VirtualMachine.Provisioning.Customize VirtualMachine.Provisioning.DeployTemplate VirtualMachine.Provisioning.ReadCustSpecs	> Datastore > Allocate space > Host > Inventory > Modify cluster > Resource > Assign virtual machine to resource pool > Virtual Machine > Edit inventory > Create new > Virtual Machine > Clone virtual machine > Virtual Machine > Provisioning > Customize guest > Virtual Machine > Provisioning > Deploy template > Virtual Machine > Provisioning > Read customization specification
Delete VM	VirtualMachine.Inventory.Delete	> Virtual Machine > Edit inventory > Remove
Cold migration	Resource.AssignVMToPool Resource.ColdMigrate	> Resource > Assign virtual machine to resource pool > Resource > Migrate powered off virtual machine

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 support@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`, assigns the required permissions to that user, and installs the Connection Broker in the `/var/lib/leo` directory. By default, the `leo` user does not have an assigned password.

 To view the list of commands the `leo` user executes as `sudo`, log into the Connection Broker machine console and execute the folowing command.

```
cat /etc/sudoers.d/leo
```

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
```

Patch Management Detection and Deployment

Use the Leostream update mechanism to update the Connection Broker. See the "Updating the Connection Broker" section in the Leostream Connection Broker Application 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 than 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, Azure SQL, 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.

Leostream Gateway Considerations

The Leostream Gateway provides remote access to your Leostream environment, both for logging into your Connection Broker and for the user's desktop connection. All traffic from the user's client device to the Leostream Gateway and on to the Connection Broker occurs on port 443. When using the Leostream Gateway HTML5 viewer, connections from the client device to the Leostream Gateway occur on 443, then continue along the display protocol port from the Leostream Gateway to the remote desktop.

When using the Leostream Gateway to forward client-based display protocol traffic, the Leostream Gateway manipulates its firewall based on instructions from the Connection Broker, to allow traffic to pass to your hosted desktops. You can configure your Leostream Gateway in one of three modes.

- **From random gateway port to protocol-specific port**: In this mode, the Leostream Gateway forwards the user's client on a random port to the protocol-specific port on the desktop they requested a connection to. You can modify the default random port range of 20001-23000 using the Leostream Gateway CLI. Note that, in this mode, the Leostream Gateway is not taking the client device into account when establishing the connection. This mode is useful when multiple users log in from the same apparent client IP, such as multiple users working from the same remote office. However, this mode could open up the connection to attackers that are scanning for open ports.

- **Use protocol-specific port on both gateway and desktop, filtered by client source IP address**: In this mode, the Leostream Gateway forwards the user's client IP traffic on the display protocol port (e.g., 3389 for RDP) to the same protocol-specific port on the desktop they requested a connection, but now a rich firewall rule is created that takes the client IP address into account. This mode must be used when connecting remote users to PCoIP Remote Workstation Cards. In this mode, you do not need to open the random port range on any external firewall that sits in front of your Leostream Gateway. However, you do need to open the protocol-specific port on any external firewall, because the Leostream Gateway uses that port to connect remote users. In the case of RDP, that means opening port 3389, which may conflict with corporate security guidelines.

- **From random gateway port to protocol-specific port, filtered by client source IP address:** In this mode, the Leostream Gateway forwards the user's client on a random port to the protocol-specific port on the desktop they requested a connection to, using a rich firewall rule that takes the client IP address into account. This method allows you to avoid opening known display protocol ports through your external firewall, while also limiting connections to known client IP addresses.

No matter what forward method you select, ensure that you monitor the firewall on your Leostream Gateways for evidence of brute force attacks. Also, periodically check the list of open firewall rules on each of your Leostream Gateways to ensure that no rules have been orphaned due to network outages that resulted in missed instructions from your Connection Broker to your Leostream Gateways. You can check the list of current ports using the following Leostream Gateway CLI:

```
sudo leostream-gateway --conn
```

When filtering destkop connections based on source IPs, ensure that network devices such load balancers and firewalls preserve the client's IP. For load balancers, this typically require enabling IP transparency.

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 Technical Support Package** 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 user 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 the latest 64-bit version of Red Hat® Enterprise Linux® 8 operating system. Leostream fully maintains the application software. Updates are issued on a scheduled basis when major features are available, 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 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 to supported Connection Broker versions are available without additional charge to any customer with an active support or subscription 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.