



Connection Broker

Where Virtual Desktops Meet Real Business

Security Review

Version 7.x
February 8, 2012

Contacting Leostream

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

<http://www.leostream.com>

Telephone: +1 781 890 2019
Fax: +1 781 688 9338

To submit an enhancement request, email features@leostream.com.
To request product information or inquire about our future directions, email sales@leostream.com.

Copyright

© Copyright 2002-2012 by Leostream Corporation

This software program and documentation are copyrighted by Leostream. The software described in this document is provided under a license agreement and may be used or copied only under the terms of this agreement. No part of this manual may be copied or reproduced in any form without prior written consent from Leostream.

Trademarks

The following are trademarks of Leostream Corporation.

Leostream™
The Leostream graphical logo™

The absence of a product name or logo from this list does not constitute a waiver of the trademark or other intellectual property rights concerning that product, name, or logo by Leostream.

Sun, Sun Microsystems, Sun Ray, and Java are trademarks or registered trademarks of Oracle and/or its affiliates. Linux is the registered trademark of Linus Torvalds in the U.S. and other countries. UNIX is a registered trademark of The Open Group. OpenLDAP is a trademark of The OpenLDAP Foundation. Microsoft, Active Directory, SQL Server, Excel, ActiveX, Hyper-V, Windows, and the Windows logo are trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Other brand and product names are trademarks or registered trademarks of their respective holders. Leostream claims no right to use of these marks.

Patents

Leostream products are patent pending.

Contents

- CONTENTS..... 3**
- OVERVIEW 4**
- NETWORK LEVEL ACCESS 4**
- APPLICATION LEVEL ACCESS..... 5**
 - RESTRICTING USER ACCESS 5
 - LOGGING USER ACCESS..... 5
 - CLIENT APPLICATION ACCESS 5
 - VMWARE® vCENTER SERVER APPLICATION ACCESS..... 6
 - MICROSOFT® ACTIVE DIRECTORY® APPLICATION ACCESS..... 6
 - EVENT MONITORING..... 6
- CONNECTION BROKER MAINTENANCE..... 7**
 - PASSWORDS 7
 - Connection Broker Virtual Appliance Accounts*..... 7
 - The Local Connection Broker Administrator* 7
 - PATCH MANAGEMENT DETECTION AND DEPLOYMENT 8
 - BACKING UP THE CONNECTION BROKER 9
 - BACKING UP AN EXTERNAL DATABASE..... 9
 - CONNECTION BROKER INTERNAL DATABASE..... 9
- APPENDIX A: EXPORTING LOG CONTENTS 10**
- APPENDIX B: SECURITY AUDIT STATEMENT 12**

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 a virtual appliance that runs inside a virtual machine powered by a VMware®, Citrix®, or Microsoft® virtualization layer. As a virtual appliance, the Connection Broker contains both the application and the underlying operating system, made from the following components:

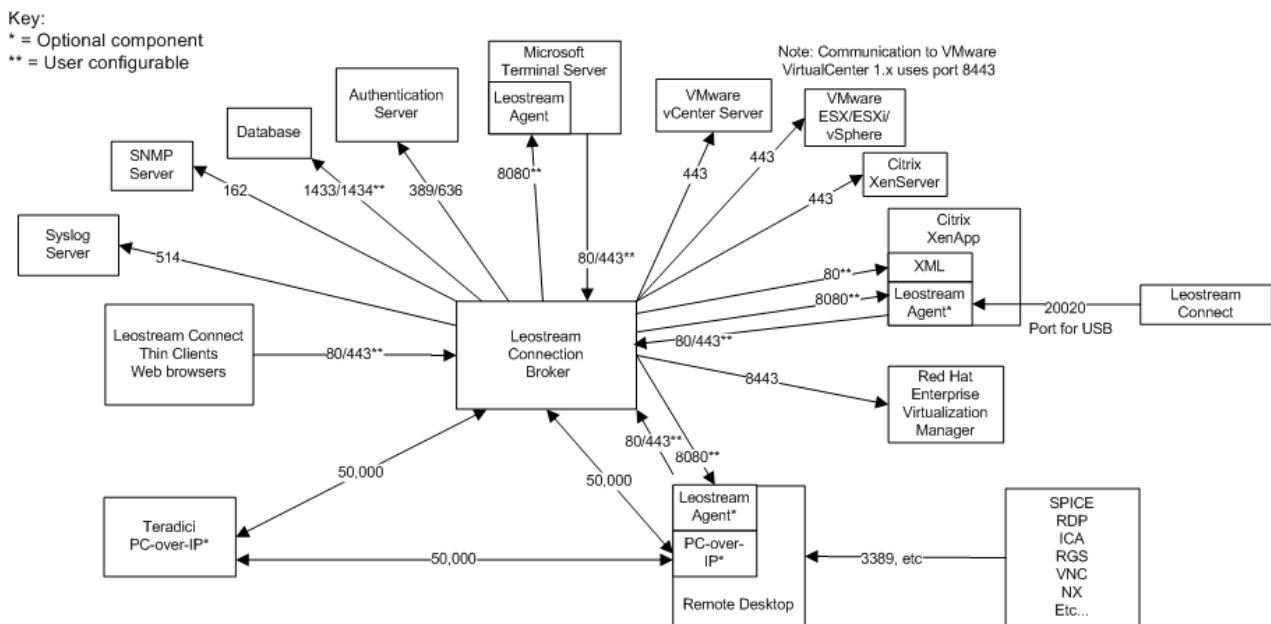
- CentOS Linux® 5.3
- Apache 1.3.41 Web Server
- OpenSSL version 0.9.8k

Network Level Access

By default, port 80 provides the only network level access to the Connection Broker when there is no SSL certificate installed. The Connection Broker uses port 443 when an SSL certificate is installed. If you turn on SLP discovery by enabling PCoIP, OpenSLP is enabled on port 50,000.

The following diagram summarizes the open ports used by the Connection Broker. All Leostream components communicate peer-to-peer. The “Database” depicted in the diagram is either a Microsoft® SQL Server® 2005 or SQL Server 2008 database. The Connection Broker sends TDS traffic to and from the SQL Server database using TCP/IP, instead of named pipes.

Leostream Connection Broker – Architecture Diagram
(Connections are initiated in direction of arrows)



Application Level Access

Restricting User Access

You can access the Connection Broker at the application level, using port 80 or port 443, 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:

- When the user logs into the Connection Broker
- 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 disconnected from a desktop
- When the user logged out of a 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](#).

Client Application Access

Different types of clients use the following communication protocols:

- Leostream clients, including the Leostream component for the iTap RDP client, use the Leostream XML-RPC based API to communicate with the Connection Broker.
- The Wyse® WTOS series thin clients use a URL based API.
- The Connection Broker Administrator Web interface uses standard HTML.

Normal communications use port 80 and are not encrypted. You can encrypt all communication protocols using SSL. To enable this feature, upload a signed or unsigned certificate into the Connection Broker (see “Generating and Installing Self-Signed SSL Certificates” or “Generating and Installing Third Party SSL Certificates” in the [Connection Broker Administrator’s Guide](#)). The Connection Broker automatically redirects communication to port 443.

VMware® vCenter Server Application Access

The Connection Broker currently reads and writes the following VMware vCenter Server commands, in order to have full functionality.

```
System.View
VirtualMachine.Interact.PowerOn
VirtualMachine.Interact.Suspend
VirtualMachine.Interact.PowerOff
VirtualMachine.Provisioning.DeployTemplate
VirtualMachine.State.RevertToSnapshot
VirtualMachine.State.CreateSnapshot
VirtualMachine.Provisioning.Customize
Resource.AssignVMToPool
```

If the Connection Broker does not have permission to these commands, an access fault occurs and the operation fails. See the Leostream [Knowledge Base](#) article “What privileges do I need to interact with VMware vCenter Server?” for more information on the required vCenter Server privileges.

All communications with vCenter Server are encrypted using SSL.

Microsoft® Active Directory® Application Access

The Connection Broker logs into the Active Directory service with an account that has Read access to all the user objects for the users managed by the Connection Broker.

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

The Connection Broker does not make any modifications to Active Directory records.

Event Monitoring

The Connection Broker has its own SNMP MIB and can signal a range of events to an external monitoring system, which, in turn 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 information, warnings, and errors that can trigger SNMP events.

Connection Broker Maintenance

Passwords

Connection Broker Virtual Appliance Accounts

The default administrator and root accounts can access and modify the Connection Broker through the VMware console.



This administrator account is different from an Administrator role/account in the Connection Broker Web interface.

By default, these accounts are setup as follows:

- administrator
 - User name: `leo`
 - Password: `leo`
- root
 - User name: `root`
 - Password: `leostream`

To secure the Connection Broker, change the passwords for these two accounts, as follows.

For the administrator account:

1. From the Connection Broker virtual machine console, press Ctrl-C.
2. Enter the username `leo` and password `leo`.
3. From the Leostream administrator **Main menu**, select **Exit** to go to the Linux shell.
4. Use the `passwd` command to change the password.

For the root account:

1. From the Connection Broker virtual machine console, press Ctrl-C.
2. Enter the username `root` and password `leostream`.
3. At the `#` prompt, use the `passwd` command to change the password.

After you have changed your passwords, you can enable SSH.



Do not enable SSH before changing your default passwords.

The Local Connection Broker Administrator

The local Connection Broker administrator is the account used when logging into the Connection Broker Administrator Web interface. By default, this user is listed in the **> Users > Users** page with the following 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 **> Users > 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 password. If you forget your password, you must change it through the Connection Broker console, as follows.

1. Login to the Connection Broker console in your virtualization management layer. Use either the administrator or root accounts described in **Connection Broker Virtual Appliance Accounts**.
2. In the **Administration Menu** that opens, select **Exit to the Linux shell**.
3. At the Linux shell prompt, enter the following command:

```
app/control.pl -change_password -user admin -new_password password
```

Where *admin* is the login name of the administrator account, which may not be *admin* if it was previously changed in the Connection Broker, and *password* is the new password to use for the administrator account.

If the Connection Broker is using the internal database, the password changes only in the internal database. If the Connection Broker is connected to an external database, the password changes only in the external database. When using an external database, include the `--internal_db` option to force the password to change in the internal database instead of the external database.

Patch Management Detection and Deployment

Use the Leostream update mechanism to update the Connection Broker, including the Connection Broker application and the underlying operating system. See the “Updating the Connection Broker” section in the **Connection Broker Administrator’s Guide** for information on getting Connection Broker updates.

The Connection Broker uses an indirect update mechanism, which requires internet access. If internet access is available, the update mechanism indicates if your Connection Broker is up to date. If your Connection Broker is not up-to-date, you have options to download and install an update file. The downloaded update file can be uploaded to any Connection Broker.

Offline updates are available by contacting Leostream support at **support@leostream.com**.

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 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 database, back up the database using the standard tools and techniques for Microsoft SQL Server 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 through the > **Users** > **Users** > **Create** 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 configuration** 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 “Downloading and Uploading Connection Broker Settings” and “Scheduling Remote Backup for the 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 three ways:

- Download a CSV-file
- Issue a Web query
- 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** link at the bottom-left 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.

Web Query

To extract the raw contents of the **> System > Log** table:

1. In a Web browser, enter the following URL to issue a Web query:

```
http://cb-address/qselect.iqy
```

Where *cb-address* is your Connection Broker IP address or hostname.

2. When the query prompts you for a username and password, enter in the credentials for the Connection Broker administrator.
3. When the query prompts you for the **Table to query**, enter `log`.

A Microsoft Excel spreadsheet opens, containing the contents of the **> System > Log** table. Users are referenced in the table by their user ID.

4. To see the mapping between users and user IDs, rerun the Web query and enter `user` for the **Table to query**.

See [Making Web Queries](#) for more information on using Web queries.

Download Technical Support Logs

When you click the **Download Leostream technical support logs** link at the bottom 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, go to the `logs` directory.
3. From the `logs` directory, extract the `sql-log.zip` file, into a directory called `sql-log`.
4. From the `sql-log` directory, go to the `logs` directory.

The `logs` 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.

- To see the mapping between users and user IDs, extract the `sql-user.zip` file.

You can also enable URL access to the logs by selecting the **Allow URL access to the logs** option at the bottom of the **> System > Maintenance** page. Once this feature is enabled, you can download the logs using the following URL:

```
http://cb-address/index.pl?action=pull_log;n=1000
```

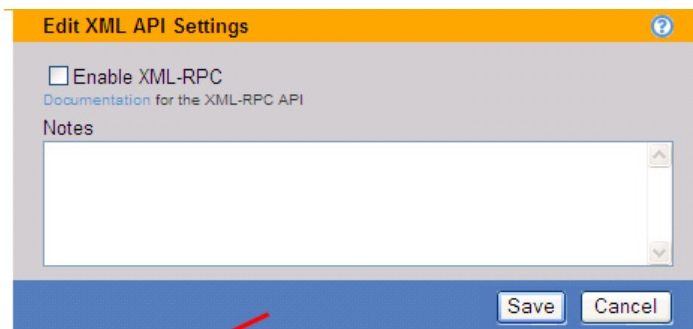
Where `cb-address` is your Connection Broker IP address. Change the value of `n` to change the number of lines downloaded from the logs.



The Connection Broker does not include any password information in the downloaded log files.

Making Web Queries

The Connection Broker Web query Interface allows you to create live data links between the Connection Broker and Microsoft Excel spreadsheets. To view the Web query documentation, click the **Web Query** link at the bottom of the **> System > XML API** page, shown in the following figure.



Using Web queries, you can import data from various Connection Broker tables into an Excel spreadsheet for reporting and graphing purposes.

Use the `qselect.iqy` command, to load a single table into an Excel spreadsheet, as follows:

```
http://cb-address/qselect.iqy
```

Where `cb-address` is your Connection Broker's IP address or hostname.

The query prompts you for your username and password, then asks for the name of the table to import. For example, to import the contents of the **> Users > Users** page, enter the table name `user`. The following Excel spreadsheet is created.

	A	B	C	D	E	F	G	H	I	J
1	last_login	links_as_dropdowns	status_refresh	remote_authentication_id	role_id	email	password	updated	id	name
2	6/30/2008 19:51		1	5	0	1	0f759dd1ea6c4c76cedc299039ca4f23	6/30/2008 19:51	1	Administrator

You can use the `select.iqy` command for more advanced queries. For information on this command, see the Web query documentation. For a list of available tables, refer to the Connection Broker data dictionary documentation, accessed through the Web query documentation.

Appendix B: Security Audit Statement

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

The Leostream Connection Broker is a virtual appliance. Leostream fully maintains the application and operating system software. Product updates are bundled into single, automatically installed packages, which include changes to the application and operating system elements of the Connection Broker virtual appliance. Updates are issued on a scheduled basis for major functionality additions, and as needed for defect vulnerability resolution. Major updates occur approximately four times a year. Minor updates are scheduled to meet customer requirements, or based on defect and vulnerability severity.

Customers are notified of updates through regular email newsletters. These newsletters are issued bi-monthly, 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 Connection Broker is typically updated via an update package obtained through the automatic check-for-updates process. This requires that the Web browser be able to connect to both the Connection Broker and the Internet. The Connection Broker can also be updated directly, without Internet access, using an update package obtained from the Leostream support team. In both cases, the update package manages the process of installing the necessary files and restarting Connection Broker services, as required.

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.