LEOSTREAM™ | Gateway Guide

Leostream Gateway

Advanced Capacity and Connection Management for Hybrid Clouds

Version 9.0 – June 2018

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

The Leostream Gateway enables Leostream environments on isolated networks and provides remote access for users outside of your corporate network. It is the key component for a Leostream environment hosted on a public cloud or OpenStack cloud, as it allows you to isolate your desktops from the public internet.

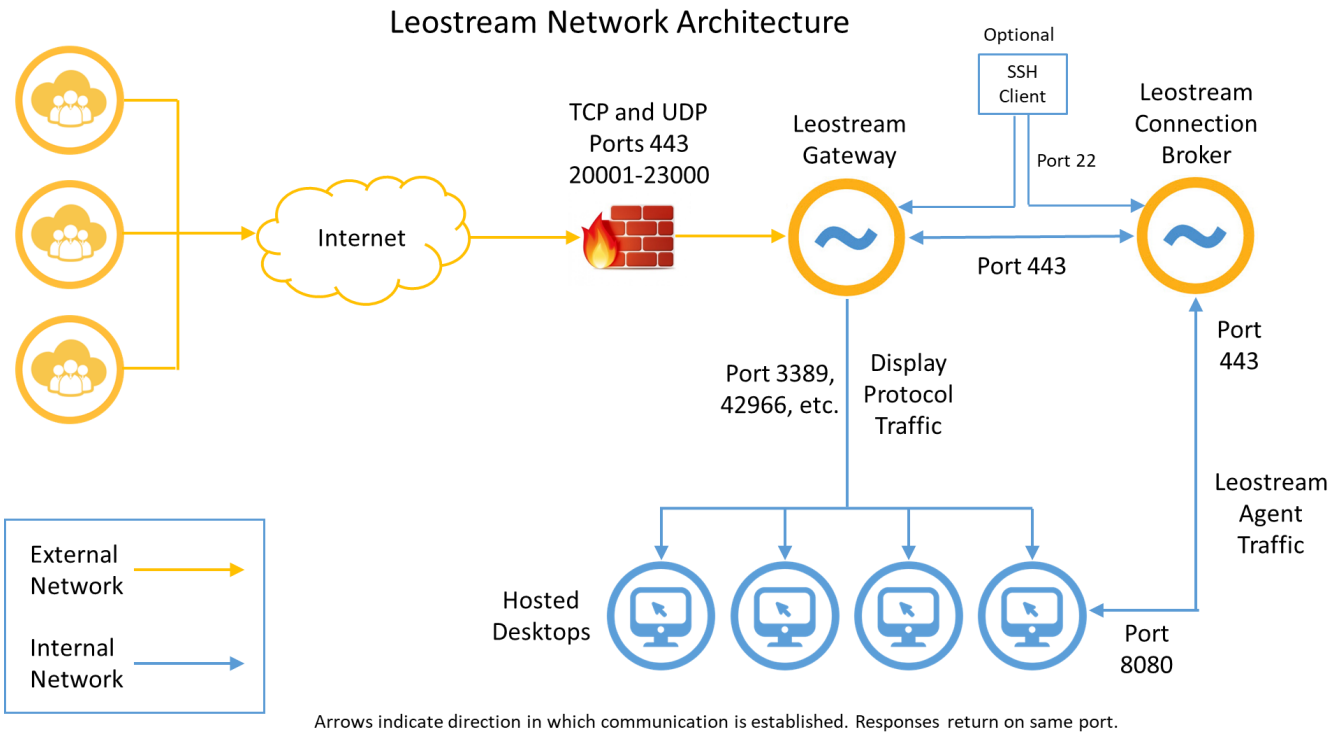
The Leostream Gateway supports HP RGS, Mechdyne TGX, RDP, and HTML5-based RDP, VNC, and SSH connections to desktops managed by the Leostream Connection Broker. HTML5-based display protocols allow users to connect to their desktop from any client device, without requiring additional installed software.

 The Leostream Gateway described in this document is for use with Leostream Connection Broker 9.0. You cannot upgrade any previously installed Leostream Gateway for Connection Broker 8.2 to the newest version.

This document covers topics related to installing the Leostream Gateway, configuring protocol plans to use the gateway, and using the HTML5 viewer. For complete instructions on configuring the Leostream Connection Broker, consult one of the Quick Start Guides or the Connection Broker Administrator's Guide, available on the Leostream Documentation page.

The Leostream Network Architecture

When building a Leostream environment, you must configure your network to open all ports required for communication between the different components. The following diagram illustrates a simple network topology for a Leostream environment.



When opening ports in your environment, keep in mind the following:

- The Leostream Gateway defaults to a port range of 20001 to 23000, for desktop connection traffic. This range is configurable using the Leostream Gateway CLI (see Setting the Desktop Connection Port Range).
- Port 8080 is the default Leostream Agent port. If you change the port during or after installation, ensure that your network opens the corresponding port.
- The display protocol port depends on which display protocol you use. For example, open port 3389 for RDP or 42966 for RGS. TGX requires a range of ports from 40001 to 40017.

How the Leostream Gateway Works

The network diagram included in the previous section becomes clearer in the context of an actual user login. In the diagram, your users are located outside of the network that hosts your desktops. Your virtual machines are isolated in a network that is not accessible to the user's client device, and your Leostream Connection Broker is co-located in the desktops' network. Sitting in between the two networks, with access to both, is the Leostream Gateway, which provides an access point for the Connection Broker to initiate user logins.

For example, for a user to log into their Leostream environment, they go to an HTTPS site that is the publicly exposed address of your Leostream Gateway. The Leostream Gateway redirects that URL to the Connection Broker **Sign in** page on port 443.

 The Leostream Gateway does not forward traffic from port 80 to port 443.

The user provides their login credentials and the Connection Broker uses those to identify the user and assign them to a Leostream policy, which determines which desktops the user may connect to.

When the user requests a connection to one of their offered desktop, the Connection Broker informs the Leostream Gateway about which desktop and what display protocol to use for the connection. All communication between the Leostream Gateway and Leostream Connection Broker is on port 443.

At that point, the Leostream Gateway opens a random port in its firewall to redirect the display protocol traffic. The user's client device connects to the Leostream Gateway on this random port, not on the default display protocol port, and receives the display protocol data from the Leostream Gateway.

The Leostream Gateway receives display protocol traffic from the remote desktop on the default display protocol port, for example, 3389 for RDP connections. You do not need to configure your remote desktops for use with the Leostream Gateway. From the remote desktop's perspective, it's transmitting the display protocol data to the Leostream Gateway along the default display protocol port. The Gateway then redirects the traffic to the randomly selected port to send to the user's client.

When the user logs out or disconnects from their remote desktop, the Leostream Gateway closes the port in its firewall, blocking access to that VM.

Installing the Leostream Gateway

The Leostream Gateway is packaged as an RPM-file that installs on a 64-bit CentOS or Red Hat Enterprise Linux operating system, version 7.4 or later. The Leostream Gateway can be installed on a virtual or physical system.

When running the Leostream Gateway on a machine with limited resources, the gateway may take several minutes to become fully functional. If initial connections through the Leostream Gateway timeout, wait for ten to fifteen minutes and try the connection again.

 Your Leostream license key must include Leostream Gateway support to integrate your Leostream Gateway with your Connection Broker.

Sizing the Leostream Gateway

The number of connections that can be handled by one Leostream Gateway is determined by the CPU available in the machine. When building the machine that will host your Leostream Gateway, allocate as much CPU as you can.

Regardless of the size of the machine, Leostream recommends a maximum of 100 simultaneous connections. To handle larger environments, install multiple Leostream Gateways and use a load balancer to distribute user connections between the gateways (see Using Load Balancers.)

The Leostream Gateway performs kernel-based port forwarding, which places very little load on the machine running the gateway. You can view the CPU being used by the Leostream Gateway while connections are being established by monitoring the output of the following command on the gateway.

```
top -d -1
```

As important as the CPU allocated to the Leostream Gateway is the bandwidth available on your network. To maximize the number of simultaneous connections that can be handled by your Leostream Gateway, ensure that your network includes sufficient bandwidth.

Online Installation and Upgrades

After building and updating your base operating system, run the following command to install your Leostream Gateway.

```
curl http://downloads.leostream.com/gateway.sh | bash
```

The installation script downloads and installs any dependencies required by the gateway.

Offline Installation and Upgrade

If your Leostream Gateway does not have internet access, or you prefer to perform a manual installation, you can download the Leostream Gateway RPM from the Leostream Website.

https://www.leostream.com/downloads/leostream-gateway

CentOS or Red Hat Enterprise Linux – Latest Version 7

After downloading the RPM, copy it to your Leostream Gateway machine and run the following three commands.

```
sudo yum -y install epel-release firewalld
sudo yum -y localinstall RPM_FILE_NAME
sudo /sbin/reboot
```

Where *RPM_FILE_NAME* is the name of the downloaded file you copied to the Leostream Gateway machine.

To upgrade an existing Leostream Gateway, run the following command.

```
sudo yum -y localinstall RPM_FILE_NAME
```

Ubuntu 16.04

After downloading the DEB, copy it to your Leostream Gateway machine and run the following three commands.

```
sudo apt -fy install firewalld
sudo apt -fy install ./DEB_FILE_NMAME
sudo /sbin/reboot
```

Where `DEB_FILE_NMAME` is the name of the downloaded file you copied to the Leostream Gateway machine.

To upgrade an existing Leostream Gateway, run the following command.

```
sudo apt -fy install ./DEB_FILE
```

Upgrading the Leostream Gateway

After installing the Leostream Gateway, all upgrades to the application are applied using the operating system `yum` or `apt-get` utility. You are responsible for applying any security or upgrade patches to the underlying operating system, separately.

- If your Leostream Gateway has internet access, performing a standard `yum upgrade` or `apt-get update` pulls down the latest version, for example:

```
sudo yum update -y leostream-gateway
sudo apt-get update -y leostream-gateway
```

- If your Leostream Gateway does not have internet access, download the latest Leostream Gateway RPM or DEB from the Leostream Website, copy the file to your gateway machine, and run the following command:

  ```
  sudo yum -y localinstall <RPM_FILE_NAME>

  sudo apt -fy install ./<DEB_FILE>
  ```

  Where `<RPM_FILE_NAME>` or `<DEB_FILE>` is the name of the downloaded file.

Configuring the Leostream Gateway

The Leostream Gateway provides a limited command line interface (CLI) that supports the tasks described in this chapter. The Leostream Gateway CLI may be run by the `root` user, or a user with `sudo` privileges, only.

When logged into the Leostream Gateway, you can use the following command to view the full list of supported options.

```
leostream-gateway --help
```

Applying SSL Certificates

The Leostream Gateway generates a default operating system SSL certificate during installation. This self-signed certificate produces warnings when users establish HTML5-based desktop connections.

For production usage, use the Leostream Gateway CLI to generate and install a signed SSL certificate, as follows.

1. Use the `--ssl-csr` option to generate an SSL CSR to use when obtaining a signed certificate.

   ```
   leostream-gateway --ssl-csr
   ```

   Step through the instructions to provide the information needed to generate the CSR. When finished, the CSR is stored in a file named `server.csr` in your current directory.

    Do not provide a passphrase when generating the CSR.

2. Use the generated CSR to obtain a signed certificate for an Apache server from your certificate authority.

3. Use the `--ssl-crt`, `--ssl-int`, and `--ssl-key` options to install your new signed certificate, intermediate certificates, and private key, respectively. For example:

   ```
   leostream-gateway --ssl-crt <certificate_filename> --ssl-int
   <intermediate_cert_filename> --ssl-key <private_key_file>
   ```

After installing the certificate, reboot your Leostream Gateway and wait for the web server to restart.

Forwarding Connection Broker Logins through the Gateway

The Leostream Gateway can be used to forward user login traffic from Leostream client devices to the Leostream Connection Broker. With Connection Broker forwarding enabled, you support the following setup.

- The Connection Broker does not need to be accessible from the user's network and, instead, can be isolated in the same private network as your desktops.
- Users can log into Leostream using Leostream Connect, a Leostream Web client, and any Dell Wyse thin client running ThinOS.

To enable Connection Broker forwarding, log into your Leostream Gateway and execute the following command.

```
leostream-gateway --broker <your-broker-address>
```

After forwarding is enabled, all calls to your Leostream Gateway are forwarded to the entered Connection Broker, with the exception of the URL used to check the status of the gateway and access the Leostream Gateway API.

⚠ The Leostream Gateway does not forward traffic from port 80 to port 443. After enabling Connection Broker forwarding, you must enter the URL for your Leostream Gateway using HTTPS. Calls to HTTP result in a warning that the site cannot be reached.

To disable Connection Broker forwarding, run the following command:

```
leostream-gateway --no-broker
```

Setting the Port Range for Desktop Connections

By default, the Leostream Gateway chooses a port between 20001 and 23000 for redirecting display protocol traffic from the client to the remote desktop. The Leostream Gateway dynamically manages the operating system firewall to open and close the ports associated with a particular connection, so you do not need to manage the operating system firewall.

If the Leostream Gateway is behind an external firewall, public cloud security group, etc., you must

ensure that it allows traffic from the internet to the Gateway on the port range, as well.

If needed, you can shrink the default port range using the `--ports` option to the Leostream Gateway CLI. Enter the port range in the format `minimumPort-maximumPort`, for example:

```
leostream-gateway --ports 25000-27000
```

The number of simultaneous connections a particular Leostream Gateway can proxy is limited by the number of ports the range. Ensure that you retain a large enough number of ports to support the number of connections you plan to proxy, realizing that TGX connections require multiple ports.

Unassociating a Leostream Gateway with a Connection Broker

Each Leostream Gateway can be associated with a single Connection Broker or Connection Broker cluster. The association is set in the Connection Broker Administrator web interface, on the **> Setup > Gateways** page.

Similarly, you can break the association by deleting the gateway's record on the **> Setup > Gateways** page.

If you decommission your Connection Broker before breaking the association with your Leostream Gateway, you can use the Leostream Gateway CLI to remove the association. Log into your Leostream Gateway and run the following command.

```
leostream-gateway --detach
```

You can then associate your gateway with a new Connection Broker.

Generating a Leostream Gateway Log Package

Leostream Gateway logs can be found in `/var/log/tomcat/guacamole.log`. If you need to provide logs to Leostream Technical Support, you can produce a log bundle using the following command.

```
leostream-gateway --logs
```

The log is generated in the current directory. Ensure that you deliver the entire log package to Leostream support when opening a ticket associated with your Leostream Gateway.

Finding your Leostream Gateway Version

When Connection Broker forwarding is disabled, you can find your Leostream Gateway version by going to the following URL:

```
https://<your-gateway-address>/
```

If Connection Broker forwarding is enabled, that URL brings you to the Connection Broker Sign in page. In this case, you can log into your Leostream Gateway and use the following command to find your operating system and Leostream Gateway version.

```
leostream-gateway --info
```

Checking the Leostream Gateway Status

If, at any time, you need to check the status of your Leostream Gateway, point a Web browser at the following URL.

```
https://<your-gateway-address>/app/system/ping
```

The URL returns a status of OK if the gateway application is running.

Integrating with the Connection Broker

After installing your Leostream Gateway, you use the Connection Broker Web interface to integrate it into your Leostream environment. The following procedure includes references to the sections in this document that describe each step.

1. Add the Leostream Gateway to your Connection Broker (see Registering the Leostream Gateway with a Connection Broker

2. Enable Connection Broker forwarding in the Leostream Gateway

3. Create protocol plans that use the Gateway for the desired display protocol (see Building Protocol Plans for the HTML5 Viewer and Building Protocol Plans for RDP, RGS, and TGX)

4. Configure pools and policies that assign these protocol plans to desktops, and desktops to users (see the Connection Broker Administrator's Guide for full instructions)

5. Log in to Leostream using Leostream Connect or the Leostream Web client, depending

Registering the Leostream Gateway with a Connection Broker

Each Leostream Gateway can be registered with a single Connection Broker, or Connection Broker cluster. You register your Leostream Gateway with your Connection Broker, as follows.

1. Log into the Connection Broker Administrator's Web interface.

2. Go to the **> Setup > Gateways** page.

3. Click the **Add Gateway** link.

4. In the **Add Gateway** form, enter a name for the Gateway in the **Name** edit field.

5. In the **Address** edit field, enter the publicly accessible IP address or hostname for your Leostream Gateway. This address must be accessible by the end users' client devices, and is the address used to log into Leostream and to forward desktop connections.

6. In the **Private address** field, enter the private address of your Leostream Gateway. This address is optional. If provided, the Connection Broker communicates with the Leostream Gateway using the private address.

7. If applicable, select the load balancer that manages this Leostream Gateway from the **Load balancer** drop-down menu (see Using Load Balancers).

8. Click **Save**.

After saving the form, the Connection Broker registers with the Leostream Gateway and it can now be used to create protocol plans.

You cannot save the form if the Leostream Gateway is already managed by another Connection Broker. If you receive an error indicating the Leostream Gateway is already managed by another Connection Broker, log into that Connection Broker and delete the Leostream Gateway (see Deregistering a Leostream Gateway in the Connection Broker). If the previously associated Connection Broker is no longer in service, you can manually detach the Connection Broker from the Leostream Gateway, as described in Manually Deregistering from a Connection Broker.

If the form displays a warning indicating the Connection Broker cannot contact the Leostream Gateway and the form fails to save, check that port 443 is open on the Leostream Gateway. You can test the Leostream Gateway connection by logging into the Connection Broker virtual machine console and executing one of the following commands at the Linux shell.

```
curl -k https://GATEWAY_ADDRESS/app/system/ping
```

```
wget --no-check-certificate -q -S -O - https://GATEWAY_ADDRESS/app/system/ping
```

Where *GATEWAY_ADDRESS* is the IP address or fully qualified hostname of your Leostream Gateway.

Configuring the Leostream Gateway to Handle User Logins

By default, users go to your Connection Broker address to log into your Leostream environment. Therefore, both the Connection Broker and Leostream Gateway must be network accessible to the user's client device.

If you prefer to have only the Leostream Gateway on the publicly facing network, as shown in the Leostream network architecture diagram, you can configure the Leostream Gateway to forward login traffic to you Connection Broker.

To enable Connection Broker forwarding

1. Log into the Leostream Gateway console so root, or as a user with sudo privileges.

2. Run the following command:

   ```
   sudo leostream-gateway --broker <broker-address>
   ```

   Where `<broker-address>` is your Connection Broker address.

After enabling forwarding, to log into your Leostream environment, users go to the following addresses.

- For Leostream Connect, enter the public IP or DNS name of the Leostream Gateway in the **Broker** tab of the **Options** dialog

- For Leostream Web clients, in a web browser, enter the HTTPS URL for the public IP or DNS name of the Leostream Gateway

- For Wyse ThinOS clients, enter the HTTPS URL for the public IP or DNS name of the Leostream Gateway

Logging into the Leostream Environment

The Leostream Gateway supports desktop connections from Leostream Connect, the Leostream Web client, and Dell Wyse ThinOS clients. The user logs into either the Connection Broker or the Leostream Gateway, depending on how your network is configured.

If the Connection Broker and the Leostream Gateway are both network accessible from the user's client device, use the Connection Broker address for user logins. For example, in the **Broker** tab of the **Options** dialog for Leostream Connect, enter the Connection Broker address.

If the Connection Broker is not network accessible from the user's client device, enable Connection Broker forwarding on the Leostream Gateway (see Enabling and Disabling Connection Broker Forwarding) and use the Leostream Gateway address for user logins. In this case:

- For Leostream Connect, enter the public IP or DNS name of the Leostream Gateway in the **Broker** tab of the **Options** dialog
- For Leostream Web clients, in a web browser, enter the HTTPS URL for the public IP address or DNS name of the Leostream Gateway
- For Wyse ThinOS clients, enter the HTTPS URL for the public IP or DNS name of the Leostream Gateway

Deregistering a Leostream Gateway in the Connection Broker

Each Leostream Gateway can be registered with a single Connection Broker, or Connection Broker cluster. If you want to switch a Leostream Gateway to a new Connection Broker or cluster, you must first deregister it from its original Leostream environment.

You can deregister the Leostream Gateway using the Connection Broker Administrator's Web interface, as follows. If you no longer have access to the Connection Broker that the Leostream Gateway is registered with, you can manually deregister the Leostream Gateway using the Gateway CLI (see Manually Deregistering from a Connection Broker).

1. Log into your Connection Broker Administrator's Web interface.

2. Go to the **> Setup > Gateways** page.

3. Edit the Leostream Gateway you want to remove. To the right of the **Edit Gateway** form, take note of any protocol plans that use this gateway.

4. Go to the **> Configuration > Protocol Plans** page.

5. For all the protocol plans found in step three, edit the protocol plan and remove this gateway from any **Gateway** drop-down menu. The gateway cannot be deleted if it is used in any protocol plans.

6. After removing the gateway from all protocol plans, return to the **> Setup > Gateways** page.

7. Edit the Leostream Gateway you want to remove. You should now see a **Delete** button

8. Click **Delete** to detach the gateway from this broker.

Building Protocol Plans for the HTML5 Viewer

The Leostream Gateway HTML5 viewer supports in-browser RDP, VNC, and SSH connections to Windows and Linux remote desktops. Your Leostream Gateway does not require any further configuration to support HTML5 connections.

You can use the following URL to test that the HTML5 viewer is working properly:

```
https://<your-gateway-address/guacamole/
```

A login page for the Apache Guacamole server displays at that URL. Neither you nor your users ever log directly into the Guacamole server.

Configuring Protocol Plans for HTML5 Connections

After you register a Leostream Gateway with your Connection Broker, you can configure a Protocol Plan to use the Leostream Gateway for HTML5 connections, as follows:

1. Go to the **> Configuration > Protocol Plans** page in your Connection Broker.

2. Edit an existing protocol plan, or click the **Create Protocol Plan** link to build a new plan.

3. In the **Web Browser** section of the protocol plan, switch the **Priority** menu of **RDP**, and any other protocol, to **Do not use**.

4. Also, in this section, select **1** from the **Priority** drop-down menu associated with the **Leostream HTML5 Viewer**.

5. From the **Gateway** drop-down menu, select the load balancer or specific Leostream Gateway to use for connections created from this protocol plan.

6. From the **Protocol** drop-down menu, indicate if this protocol plan launches RDP, VNC, or SSH.

7. Configure the protocol-specific parameters, as described in the following sections.

8. Click **Save**.

Ensure you select this protocol plan in the **Plan** sub-section of the **Desktop Assignment from Pool** section of the user's policy.

RDP Desktop Connections

The HTML5 RDP viewer provided by the Leostream Gateway can be used to connect to Windows or Linux desktops, if the Linux desktop supports xRDP. To launch in-browser RDP connection, select **RDP** from the Leostream HTML5 Viewer **Protocol** drop-down menu.

You can use the following options to configure the RDP session.

1. Select **Desktop composition and wallpaper** to display the desktop background, as well as the Windows desktop composition features.

2. Select the **High resolution** option to set the color depth to 24. If the **High resolution** option is off, the connection defaults to a value determined by the RDP server, typically 16.

3. Select the **Local printing** option to enable the virtual printer (see Local Printing).

4. Select the **File transfer** option to enable a virtual drive that users can leverage to move files between their client device and remote desktop (see File Transfer).

5. Use the **Keyboard** drop-down menu to set the server-side keyboard layout.

6. Use the **Security** drop-down to set the security mode for the RDP connection. If connecting to a Windows 10 desktop, typically select **Network Level Authentication**.

   ⚠ Ensure that the remote Windows 10 machine accepts connections from clients that do not use Network Level Authentication (uncheck the **Allow connections only from computers running Remote Desktop with Network Level Authentication** option.)

7. Use the **Client resize action** drop-down menu to indicate how the server should respond when the user resizes their browser window.

   - Select **No action** to leave the size of the RDP connection unchanged
   - If connecting to a Windows desktop with RDP 8.1 or later, select **Signal the server** to request the server change the display size.
   - Select **Reconnect to the server** to disconnect from the server and reconnect with the new size

For information on using the parameters related to launching RemoteApp sessions, see Launching RDP RemoteApp Sessions.

RemoteApp Sessions

By default, the Leostream Gateway connects users to the entire desktop. However, if you published applications in a Microsoft RemoteApp Server, you can instruct the Leostream Gateway to connect the user to one of those applications.

When using Leostream to manage connections to RemoteApp applications, configure your Connection Broker, as follows.

1. Create a **Remote Desktop Services/Multi-User** center and specify the total number of simultaneous connections supported by that server. The Connection Broker creates placeholder sessions that are displayed on the **> Resources > Desktops** page.

2. Create pools for each application you want to offer to users. Each pool should contain the maximum number of simultaneous connections you want to that application. Note that a particular session can be a member of multiple pools.

   For example, if your center allows a maximum of 40 connections, you can create two pools, each containing 30 sessions. The Connection Broker hands out the sessions on a first come-first served basis. Therefore, if 30 users connect to an application from one pool, only 10 users can connect to the application in the second pool.

3. Create a protocol plan that launches each of your published application. Instructions on creating the protocol plan are included later in this section.

4. Create a policy that offers your pools of RemoteApp applications, and assigns the appropriate protocol plan to each pool. The policy can also as many RemoteApp pools as needed, along with full desktop pools.

5. Assign the policy to your users. The RemoteApp server must be configured to allow users who are assigned to this policy to connect to the offered application.

You create a protocol plan that launches a RemoteApp session through the Leostream Gateway, as follows.

1. In the **Web Browser** section of the protocol plan, select **RDP** from the Leostream HTML5 Viewer **Protocol** drop-down menu.

2. Select the **Microsoft RemoteApp support** option.

3. In the **RemoteApp name** edit field, enter the name of the published application. The name must be prepended by two vertical bars, for example:

   ||wordpad

4. In the **RemoteApp directory** edit field, enter the working directory for the published application.

5. In the **RemoteApp arguments** edit field, enter any required command line parameters. Leave empty if the RemoteApp does not take command line parameters.

VNC Connections

HTML5 VNC connections are available for Windows and Linux desktops. When connecting to a Linux desktop, you can use the Leostream Agent to automatically start the VNC server process for the user. Multiple users can be connected to the same desktop on different VNC server ports.

For Windows desktops, the VNC server must be running prior to trying to establish the connection through the Leostream Gateway.

To launch in-browser VNC sessions, select **VNC** from the Leostream HTML5 Viewer **Protocol** drop-down menu. After selecting VNC, you must enter the password to use when launching the VNC server. The same password is used for each session. If different VNC servers or users have different VNC passwords, create a new Protocol Plan for each required password.

SSH Connections

When connecting to Linux desktops, you can launch in-browser SSH sessions by selecting **SSH** for the Leostream HTML5 Viewer **Protocol** drop-down menu. When selecting SSH connections, you can customize the connection using the **Color scheme** drop-down menu.

The SSH session is a simple terminal connection inside the browser. If you require a desktop environment connection, after an SSH session is established, you can launch VNC sessions to the desktop. Alternatively, you can use the HTML5 VNC viewer provided by the Leostream Agent (see Launching VNC Connections.)

Building Protocol Plans for RDP, RGS, and TGX

The Leostream Gateway can be used to forward Microsoft RDP, HP RGS, and Mechdyne TGX connections into a network that is not accessible from the user's client device. Using the Leostream Gateway, you can isolate virtual machines on private networks in OpenStack, Amazon Web Services, Microsoft Azure, or any other hosting platform, and provide users with connections from anywhere.

Users can log in using either Leostream Connect or the Leostream Web client, and establish RDP, RGS, and TGX connections through the Leostream Gateway.

 USB device passthrough is not currently supported through the Leostream Gateway.

Ensure that you install the Leostream Gateway in a location is network accessible from the user's client device and the hosted desktops, for example by placing the Gateway in the same private network and providing it with a publicly accessible IP address.

 The Leostream Gateway forwards traffic on ports 20,001 through 23,000. If you have a security group or firewall on the public network, ensure that it allows incoming traffic on that port range. You do not need to manage the firewall on the Leostream Gateway, itself.

Enabling the Leostream Gateway for RDP, RGS, and TGX

After you install your Leostream Gateway, configure a protocol plan to send the connection traffic through the gateway, as follows:

1. Go to the **> Configuration > Protocol Plans** page in your Connection Broker.
2. Either edit an existing protocol plan, or client the **Create Protocol Plan** link to build a new plan.
3. Depending on which client device users plan to use, go to the **Leostream Connect** or **Web Browser** section of the protocol plan.
4. Find the sub-section associated with the protocol you want to pass through the Leostream Gateway, for example, **HP RGS**. Set the **Priority** for this protocol to **1**.
5. From the **Gateway** drop-down menu in this sub-section, select the Leostream Gateway to use for connections.
6. Set the **Priority** menu for all other protocols to **Do not use**.
7. Save the protocol plan

Working with HP RGS

When establishing an RGS connection through the Leostream Gateway, the Connection Broker instructs the RGS Receiver on the client device to connect to the IP address of the Leostream Gateway appended by the port used to forward the traffic.

After connecting through the Leostream Gateway, if you launch the RGS Receiver and do not specifically reset the default RGS Receiver network port, RGS connections that are not established through the Leostream Gateway will fail.

To reset the default RGS Receiver Network port:

- For RGS connections established by Leostream, ensure that the HP RGS Configuration file in the protocol plan includes the following line:

  ```
  Rgreceiver.Network.Port=42966
  ```

- For RGS connections established by manually launching the RGS Receiver, edit the default `rgreceiverconfig` file in the RGS Receiver installation directory and uncomment the following line:

  ```
  Rgreceiver.Network.Port=42966
  ```

Working with Mechdyne TGX

Each Mechdyne TGX connection requires a range of five ports, instead of a single port. The Leostream Gateway, therefore, assigns a random range of five ports to each TGX connection.

Keep this in mind when determining the number of ports to configure for connections (see Setting the Desktop Connection Port Range) as the number of simultaneous TGX connections through a Leostream Gateway is less than for RGS or RDP.

Using Load Balancers

To support a large deployments and provide high availability, you can create a group of Leostream Gateways managed by a commercial load balancer. The load balancer should be configured to distribute load, as well as confirm that the Leostream Gateway is functional.

After configuring your load balancer, you must register it with your Connection Broker, and indicate which Leostream Gateways are associated with that load balancer, as follows.

1. Go to the **> Setup > Gateways** page.
2. Click the **Add Load balancer** link.
3. In the **Add Load balancer** form, enter a display name for your load balancer in the **Name** edit field.
4. Enter the load balancers IP address or resolvable hostname in the **Address** field.
5. Click **Save**.

After registering the load balancer, indicate which Leostream Gateways are behind it, as follows.

1. On the **> Setup > Gateways** page, click the **Edit** link for each of the appropriate gateways.
2. Use the **Load balancer** drop-down to indicate which load balancer manages this gateway.
3. Click **Save**.

To send user connections to the load balancer, ensure that you select the load balancer in the **Gateway** drop-down menus in your Protocol Plan.

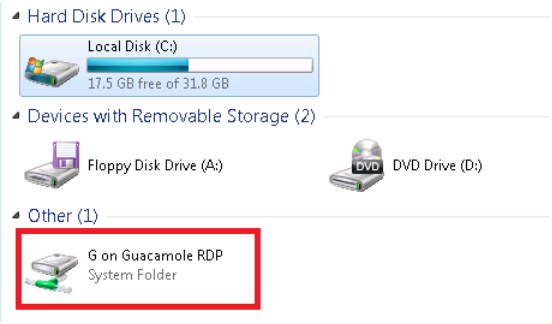
Working with the HTML5 RDP Viewer

Copy and Paste

Use the HTML5 clipboard to copy text to and from your HTML5 RDP connection. To access the clipboard, place the cursor on the desktop background of the HTML5 connection and press Ctrl-Alt-Shift. The sidebar menu that opens provides a clipboard that can be used to transfer text between the local client and remote desktop.

File Transfer

When file transfer is enabled, the HTML5 RDP session contains a virtual drive that can be used to transfer files between the client and remote desktop. The virtual drive appears in the file browser, for example:



To copy files from the remote desktop to your local client:

1. Copy the file into the shared drive on the remote desktop.
2. Open the sidebar menu by pressing Ctrl-Alt-Shift.
3. In the **Devices** section, click on the **Shared Drive** device.
4. Double-click on the file you want to download to your local client.
5. In the **File Transfer** dialog that opens at the bottom left, shown in the following figure, click the file name to download the file.

To copy files to the remote desktop from your local client:

1. In the HTML5 RDP session, open the sidebar menu by pressing Ctrl-Alt-Shift.
2. In the **Devices** section, click on the **Shared Drive** device.
3. Click the **Upload Files** button.
4. Browse for the file and click **Open**.

The file appears in the shared drive on the remote session.

Local Printing

If local printing is enabled, you can print files on the remote desktop to the redirected HTML5 printer, which saves the file to a PDF file that is then downloaded to your local client device.

When printing a file, select the Guacamole redirected printer from the **Print** dialog. To download the resulting PDF file, click on the link in the File Transfer dialog that opens at the bottom left of the windows, for example: