



leostream

Remote Desktop Access Platform

The Leostream Gateway Guide

Remote Access and In-Browser Connections for Leostream Environments

Leostream Gateway 202x
July 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

© Copyright 2002-2023 by Leostream Corporation

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

Trademarks

The following are trademarks of Leostream Corporation.

Leostream™

The Leostream graphical logo™

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

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, Hyper-V, Windows, and the Windows logo are trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Other brand and product names are trademarks or registered trademarks of their respective holders. Leostream claims no right to use of these marks.

Patents

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

Contents

Contents	3
Overview	5
The Two Functions of the Leostream Gateway	6
The Importance of firewall	6
An Example Leostream Login using the Leostream Gateway	7
The Leostream Network Architecture	9
Step 1: Logging into Leostream Environments	9
Step 2: Desktop Connections	11
Required Ports for Leostream Built-in HTML5 Viewer Connections	12
Required Ports when Forwarding Client-Based Display Protocols or Third-Party HTML5 Viewers using Random Ports	13
Required Ports when Forwarding Client-Based Display Protocols or Third-Party HTML5 Viewers using Random Ports Filtered by Client IP	14
Required Ports when Forwarding Client-Based Display Protocol or Third-Party HTML5 Viewers using the Display Protocol Ports Filtered by Client IP	15
Working with PCoIP Remote Workstation Cards	17
Installing the Leostream Gateway	18
Sizing the Leostream Gateway	18
Using Security-Enhanced Linux (SELinux)	19
Online Installation and Upgrades	19
Offline Installation and Upgrade	19
Changing the Default Leostream Gateway Port	21
Checking the Leostream Gateway Status	22
Permission Requirements	22
Listing Connections	22
Using the Leostream Gateway CLI	25
Applying SSL Certificates	25
Setting the Port Range for Desktop Connections	26
Manually Detaching a Leostream Gateway from a Connection Broker	27
Starting and Stopping the Leostream Gateway	27
Generating a Leostream Gateway Log Package	27
Finding your Leostream Gateway Version	28
Disabling and Enabling the Built-In HTML5 Viewer	28
Using the Leostream Gateway to Forward Azure API Calls	28
Integrating with the Connection Broker	30
Forwarding Connection Broker Logins through the Gateway	30
Attaching the Leostream Gateway to a Connection Broker	31
Removing a Leostream Gateway from a Connection Broker	33
Configuring Leostream Gateway Clusters	33
Configuring Clients to Log into your Leostream Environment	35
Building Protocol Plans for the Built-In HTML5 Viewer	35
HTML5 RDP Desktop Connections	36
HTML5 RemoteApp Sessions	38
HTML5 VNC Connections	39
SSH Connections	39
Building Protocol Plans for Client-Based Display Protocols	39

Enabling the Leostream Gateway for RDP, Remote Boost, NoMachine, DCV, and TGX	40
Enabling the Leostream Gateway for PCoIP	40
Working with HP ZCentral Remote Boost	41
Working with Mechdyne TGX	41
Working with NICE DCV	42
Building Protocol Plans for Third-Party HTML5 Viewers	42
Working with the HTML5 RDP Viewer	43
Copy and Paste	43
File Transfer	43
Local Printing	44

Overview

The Leostream Gateway provides remote access to Leostream environments without the need for costly and complicated VPN solutions. By incorporating the Leostream Gateway into your environment, you can model key business continuity workflows, such as:

- Supporting a work-from-home initiative by leveraging the Leostream Gateway to connect home-based users to on-premises resources
- Allowing end-users to leverage personal client devices, including Chromebooks, with in-browser connections to corporate resources
- Building a cloud or hybrid environment by leveraging the Leostream Gateway to connect anyone to cloud-based machines hosted in a private network
- Providing remote access to high-power workstations with a Teradici Remote Workstation Card or Amulet Hotkey KVM Extender

The Leostream Gateway includes a built-in HTML5-based RDP, VNC, and SSH client to provide in-browser connections to desktops managed by the Leostream Connection Broker. In addition, the Leostream Gateway supports in-browser connections using NoMachine, NICE DCV, and Scyld Cloud Workstation, using those products' HTML5 viewers. HTML5 viewers allow users to connect to their desktop from any client device, without requiring additional installed software.

The Leostream Gateway also supports client-based connections for the following display protocols.

- HP ZCentral Remote Boost (RGS)
- Mechdyne TGX
- Microsoft RDP
- NICE DCV
- NoMachine
- Teradici PCoIP, when connecting to PCoIP Remote Workstation Cards

This document covers topics related to installing the Leostream Gateway, configuring protocol plans to use the gateway and using the HTML5 viewers. 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 Gateway is not part of Leostream deployments with HP Anyware. For more information on architecting a solution to connect Leostream users with Cloud Access Software, see the [Leostream Quick Start Guide for Using Leostream with HP Anyware](#).

The Two Functions of the Leostream Gateway

The Leostream Gateway forwards network traffic from the user's client device to an internal system. That internal system could be your Leostream Connection Broker, it could be a racked workstation in your data center, or it could be a virtual machine isolated in a private network in a public cloud, to name a few.

That network traffic takes two forms:

1. Connection Broker HTTPS login traffic
2. Desktop connection traffic, for example RDP

These two functions of the Leostream Gateway, forwarding Connection Broker login traffic and forwarding desktop connection traffic, are completely decoupled. You may leverage one Leostream Gateway to forward Connection Broker logins, but use separate Leostream Gateways to handle desktop connections.



The Leostream Gateway does not perform any additional encryption on any of the traffic.

The Importance of firewalld

The Leostream Gateway forwards client-based desktop traffic by manipulating its internal firewall. In order for the Leostream Gateway to properly function, you must adhere to the following guidelines.

- a. Do not disable or modify the internal firewall (`firewalld`) on the Leostream Gateway machine. The `firewalld` service must be running in order for the Leostream Gateway to perform properly.
- b. Masquerading must be enabled on `firewalld`.
- c. The `https` service must be allowed through `firewalld`
- d. Optionally, the `ssh` service can be allowed through `firewalld` in order to access the Leostream Gateway console.



If your environment requires changes to `firewalld` or additional open ports in the Leostream Gateway firewall, please contact support@leostream.com to discuss your use case prior to making any changes. Disabling or modifying the firewall prevents normal operation of the Leostream Gateway and should not be done without the assistance of Leostream Support.

An Example Leostream Login using the Leostream Gateway

Consider a work-from-home scenario where your users' desktops are located in your corporate office while your users are home without a VPN connection to your corporate network. Your Leostream Connection Broker is installed in your data center on your desktops' network and your Leostream Gateway is installed in a DMZ where it can be accessed from the public internet and also has access to your desktops' network. The Leostream Gateway is configured to forward Connection Broker login traffic, as well as to connect the user to their desktop using RDP, as an example.

To log in, a user points their web browser at an HTTPS site that is the publicly exposed address of your Leostream Gateway or of a firewall or load balancer that redirects traffic to 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 enters their login credentials and the Connection Broker authenticates the user against your authentication servers, then assigns a Leostream policy to the user. The policy determines which desktops the user is offered.

When the user requests a connection to one of their offered desktops, the Connection Broker provides information about that desktop and what display protocol should be used to the Leostream Gateway. In the case of a client-based display protocol, the Connection Broker also indicates if the gateway should forward desktop connection traffic along a random port or on the display protocol port. Up until this point, all communication occurs on port 443.

At this point, the Leostream Gateway opens the appropriate port in its firewall to redirect the display protocol traffic from the hosted desktop to the user's client. The user's client device receives display protocol data from the Leostream Gateway on this port.

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 Leostream Gateway then redirects the traffic to the user's client.

When the user logs out or disconnects from their remote desktop, after receiving the instruction from the Connection Broker, the Leostream Gateway closes the port in its firewall, blocking access to the remote desktop.

The Connection Broker determines when to send the instruction to the Leostream Gateway based on the following settings.

- The Connection Broker always sends the instruction to close the forwarding port when a logout event is received from the Leostream Agent.
- When a disconnect notice is received from the Leostream Agent, the Connection Broker

waits for the length of time specified by the **Delay closing gateway forwarding ports on disconnect (seconds)** option on the > **System > Settings** page. If you leverage a display protocol that attempts to re-establish the desktop connection after a brief network outage, use this setting to preserve the port forwarding for a limited amount of time, to allow the display protocol to reconnect when the network is restored. See “Closing Leostream Gateway Ports for Disconnected Desktop Sessions” in the [Connection Broker Administrator’s Guide](#) for more information.

- For hard-assigned desktops, after the user requests a connection to their desktop, the Connection Broker waits for a login notification from the Leostream Agent. If the user does not log into their desktop after the length of time specified by the **Close Leostream Gateway port if user hasn't logged in after** option in the **Hard Assignments** tab of the user’s policy, the Connection Broker instructs the Leostream Gateway to close the forwarding port and the user must request a new connection to their desktop.

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 diagrams illustrate simple network topologies for a Leostream environment, based on the stage of the Leostream session and the method the Leostream Gateway uses to pass display protocol traffic.

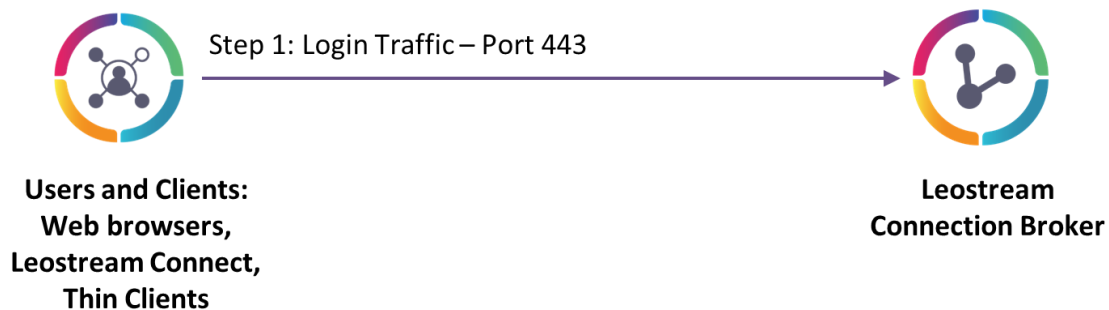
Step 1: Logging into Leostream Environments

The Leostream Connection Broker is responsible for authenticating users, assigning a policy to the user, and sending information to the client device about how to connect the user to their offered desktops. The Connection Broker determines if the user's connection leverages the Leostream Gateway, and instructs the Leostream Gateway on how to establish the connection.

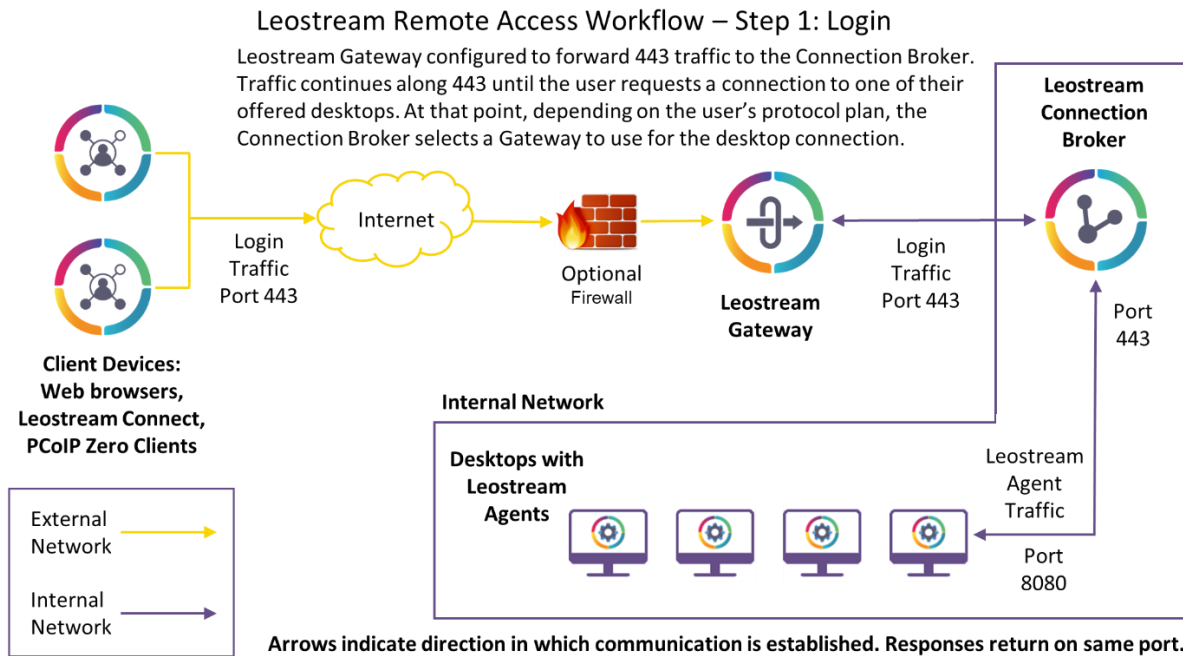
Because the Leostream Connection Broker is responsible for processing Leostream logins, all user client devices must be able to communicate with the Connection Broker. In some cases, the user's client device has network access to the Connection Broker, for example:

- When the users are located on the same network as the Connection Broker
- When the users have a VPN connection to the Connection Broker network
- If the Connection Broker is located in the DMZ with a public IP

In any of the previously mentioned cases, the client device can point directly to the Connection Broker, for example:



If the users' client devices do not have network access to the Leostream Connection Broker or you do not want to expose the Connection Broker to the internet, you can leverage the Leostream Gateway to forward login traffic to the Connection Broker, as shown in the following figure.




Note that, in this scenario, even though the client device points to the Leostream Gateway, the Connection Broker is responsible for processing the user login. The Leostream Gateway simply forwards traffic along TCP port 443 to the Connection Broker

To make the Leostream Gateway accessible to the client devices, you can either:

1. Leverage your corporate firewall to route traffic from the internet to the Leostream Gateway. In this case, the Leostream Gateway has a single NIC on the same network as the Connection Broker and hosted desktops. This scenario works particularly well if your users leverage the built-in HTML5 viewer and you can configure your firewall to route TCP port 443 traffic to your Leostream Gateway.

For client-based protocols, you will need to enable additional ports through your firewall to the Leostream Gateway, as described in the following section.

 Depending on your firewall, forwarding HTTPS traffic may not be sufficient. Instead, specifically route TCP port 443 to your Leostream Gateway.

2. Add a second NIC to your Leostream Gateway and place the gateway in your DMZ. In this case, one NIC should be internet facing while the second NIC is on the same network as the Connection Broker and hosted desktops.
3. For cloud environments, place the Leostream Gateway in the same private network as your Connection Broker and hosted desktops, and associate a public IP address with the gateway. Ensure that the security group associated with your Leostream Gateway instance allows the required traffic to pass to your gateway.

Step 2: Desktop Connections

After the user selects which desktop they want to connect to, the Connection Broker checks the user's protocol plan to see if that connection should be routed through the Leostream Gateway, either using the built-in HTML5 viewer, a third-party HTML5 viewer, or using a client-based display protocol.

If the connection uses a third-party HTML5 viewer or client-based display protocol, the Connection Broker checks how the Leostream Gateway record on the > **Setup** > **Gateways** page is configured to forward traffic. Leostream Gateways can forward desktop traffic using one of following three methods.

1. From a random Leostream Gateway port to the display-protocol-specific port on the hosted desktop – this scenario is useful if you have multiple client devices connecting from the same remote location
2. From the display-protocol-specific port on the Leostream Gateway to the display-protocol-specific port on the hosted desktop, filtered by the user's client IP address – this scenario is required when using the Leostream Gateway to forward PCoIP traffic to Teradici Remote Workstation Cards
3. From a random Leostream Gateway port to the display-protocol-specific port on the hosted desktop, filtered by the user's client IP address

The following sections describe the different ports that are used for these different scenarios.

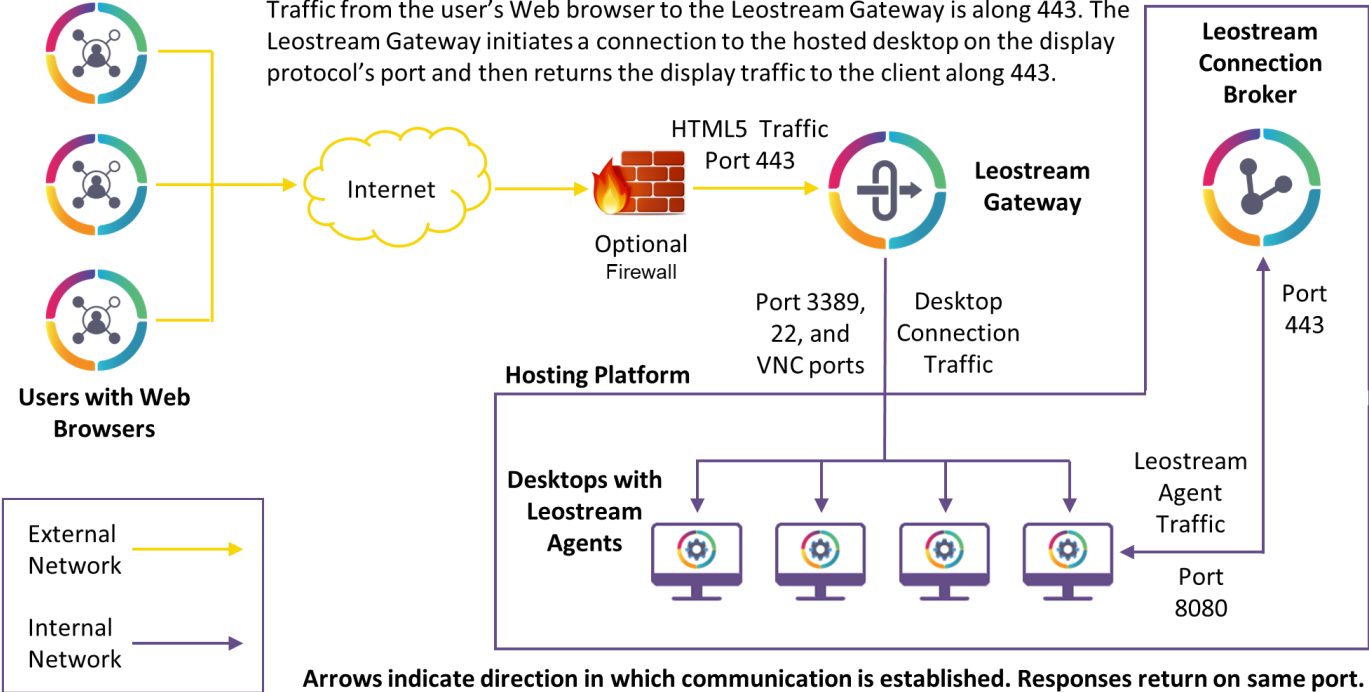
Required Ports for Leostream Built-in HTML5 Viewer Connections

When using the Leostream HTML5 client, traffic from the client device (a web browser) to the Leostream Gateway is always along TCP port 443. Traffic leaving the Leostream Gateway and going to the hosted desktop is along the port used by the display protocol, as follows.

- RDP – TCP and UDP 3389
- SSH – TCP 22
- VNC – TCP 5900, 5901, 5902, etc., depending on your VNC server configuration

Step 2: HTML5 Connections

Traffic from the user’s Web browser to the Leostream Gateway is along 443. The Leostream Gateway initiates a connection to the hosted desktop on the display protocol’s port and then returns the display traffic to the client along 443.



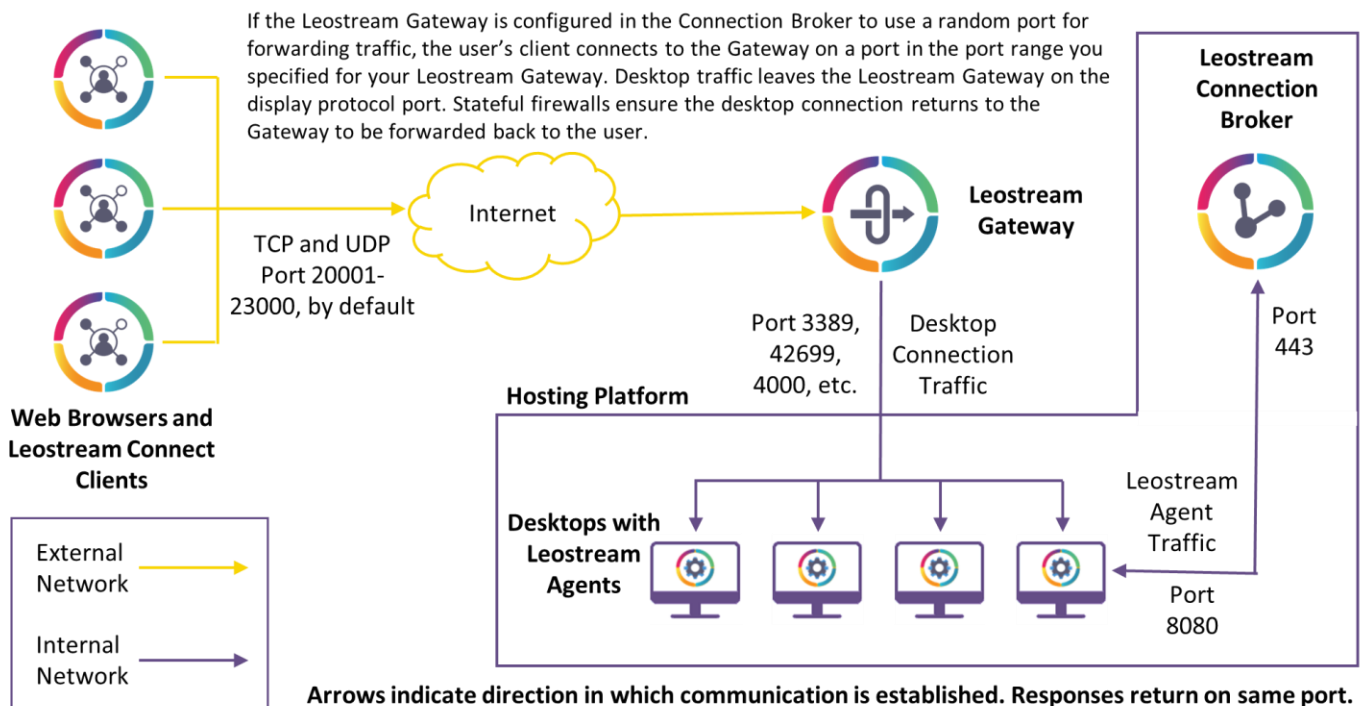
Required Ports when Forwarding Client-Based Display Protocols or Third-Party HTML5 Viewers using Random Ports

In a scenario using client-based display protocols or third-party HTML5 viewers, traffic from the client device to the Leostream Gateway can be routed along a random port selected by the gateway. This traffic may be TCP and UDP based, depending on the display protocol.

Traffic between the Leostream Gateway and the hosted desktop is along the port used by the display protocol, as follows.

- Microsoft RDP – TCP and UDP 3389
- HP ZCentral Remote Boost – TCP and UDP 42966
- NICE DCV client-based connections – TCP and UDP 8443, by default
- NICE DCV HTML5 connections – TCP 8443, by default
- NoMachine client-based connections – TCP and UDP 4000
- NoMachine HTML5 connections – TCP 4443
- Mechdyne TGX 1.10– TCP and UDP 40001-40017
- Mechdyne TGX 2.x – TCP and UDP 40001
- Scyld Cloud Workstation HTML5 connections – TCP 443

Step 2: Client-based RDP, TGX, etc., Connections Forwarded on a Random Port



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

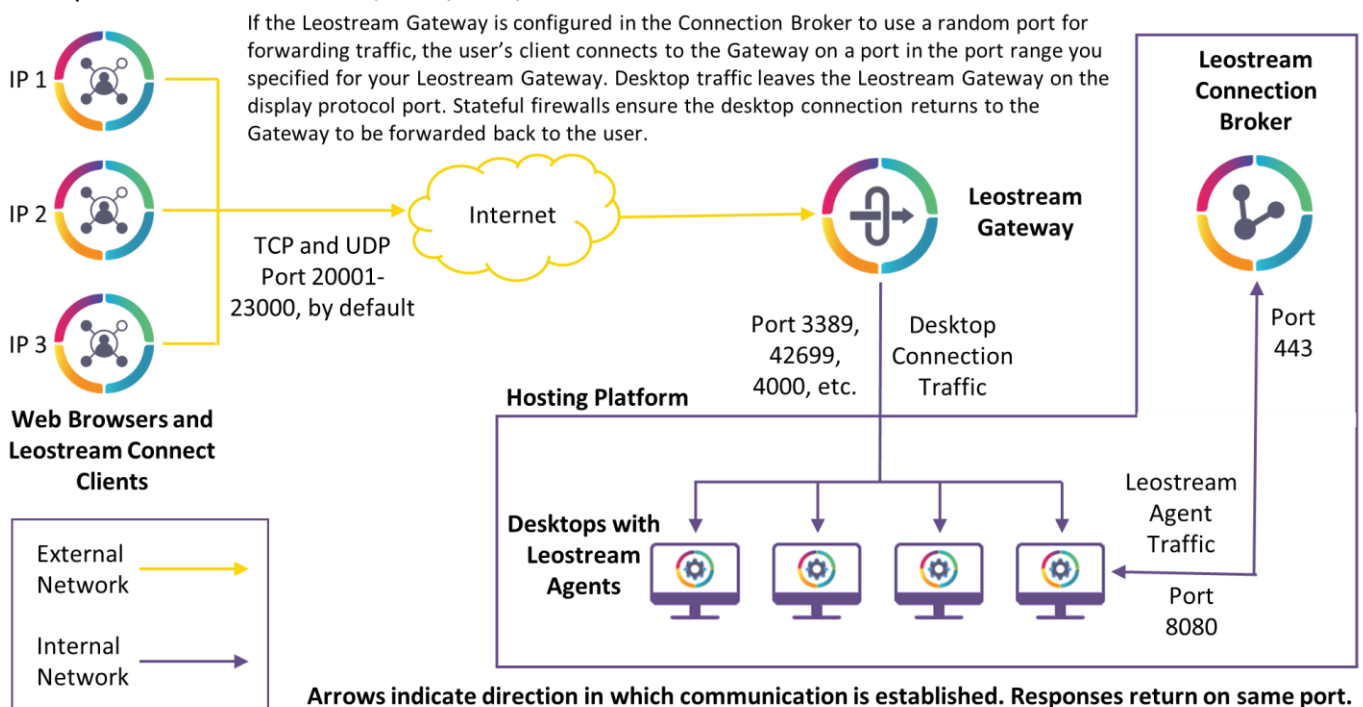
- Between the client and Leostream Gateway - The Leostream Gateway defaults to a port range of 20001 to 23000 for desktop connection traffic. This range is configurable using the Leostream Gateway CLI (see [Setting the Desktop Connection Port Range](#)).

- Between the Leostream Gateway and hosted desktop – The port depends on which display protocol you use, for example, TCP and UDP port 3389 for RDP or TCP and UDP 42966 for Remote Boost. Note that although TGX 2.0 requires only port 40001, Leostream opens the full range of ports from 40001 to 40017 that is required for TGX 1.10 connections.

Required Ports when Forwarding Client-Based Display Protocols or Third-Party HTML5 Viewers using Random Ports Filtered by Client IP

The ports required when filtering the forwarding rules by client IP are identical to the [previous scenario](#) where client IP addresses were not taken into account. In this scenario, however, the Leostream Gateway configures firewall rich rules that take into account the IP address of the user’s client.

Step 2: Client-based RDP, TGX, etc., Connections Forwarded on a Random Port



When configuring Leostream Gateways to filter connections based on Client IP addresses, if the Leostream Gateway is separated from the client device by a firewall or load balancer, ensure that it is set up to forward the original client IP address in the "X-Forwarded-For" HTTP header. Otherwise, the Leostream Gateway will see all client devices as the IP address of the firewall or load balancer.

Required Ports when Forwarding Client-Based Display Protocol or Third-Party HTML5 Viewers using the Display Protocol Ports Filtered by Client IP

If your Leostream Gateways are behind a load balancer or firewall, you may want to avoid opening a large port range. In this case, you can set the Leostream Gateway to forward display protocol traffic along the display protocol port, filtered by client IP address.



This configuration is required if forwarding PCoIP traffic to Teradici Remote Workstation Cards.

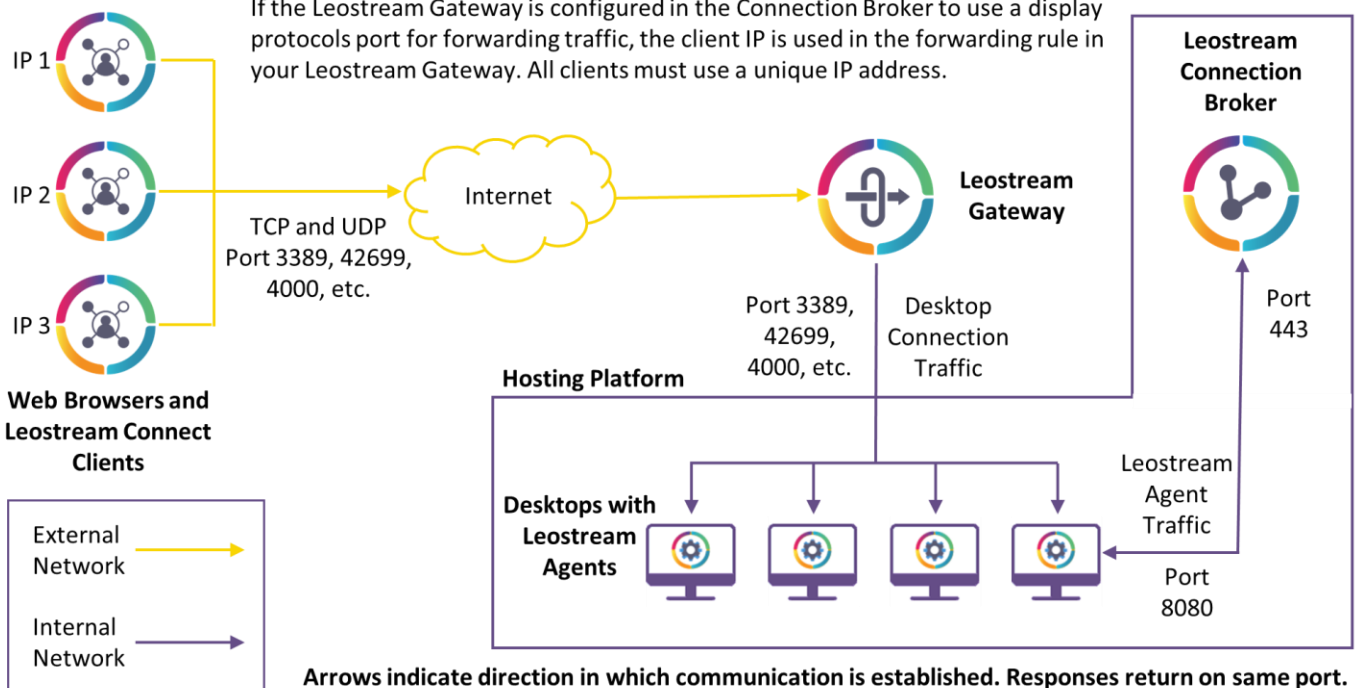
In this scenario, traffic from the client device to the Leostream Gateway is along the display protocol port. This traffic may be TCP and UDP based, depending on the display protocol.

Traffic leaving the Leostream Gateway and going to the hosted desktop is also along the display protocol port. For the currently supported display protocols, these ports are as follows.

- Microsoft RDP – TCP and UDP 3389
- HP ZCentral Remote Boost – TCP and UDP 42966
- NICE DCV client-based connections – TCP and UDP 8443
- NICE DCV HTML5 connections – TCP 8443
- NoMachine client-based connections – TCP and UDP 4000
- NoMachine HTML5 connections – TCP 4443
- Mechdyne TGX 1.10– TCP and UDP 40001-40017
- Mechdyne TGX 2.x – TCP and UDP 40001
- Scyld Cloud Workstation HTML5 connections – TCP 443
- Teradici PCoIP – TCP and UDP 4172, TCP 50001-50002

Step 2: RDP, TGX, etc., Connections – Forwarded on display protocol port

If the Leostream Gateway is configured in the Connection Broker to use a display protocols port for forwarding traffic, the client IP is used in the forwarding rule in your Leostream Gateway. All clients must use a unique IP address.



Because the Leostream Gateway uses the client IP address as part of the rich firewall rule that redirects the traffic, the user can connect to a single desktop at a time. They must disconnect from their first desktop before connecting to a second desktop using the same protocol. The user can connect to a second desktop using a different display protocol, for example connecting to one desktop using RDP and a second desktop using Remote Boost.

When using Scyld Cloud Workstation, because the Leostream Gateway forwards traffic for this protocol on port 443, the user is unable to log into Leostream to connect to other desktops until they disconnect from their Scyld Cloud Workstation.



In general, this Leostream Gateway forwarding method works best in cases where all users are logging in from unique client IP addresses. Two remote users logging in from the same location are not able to simultaneously connect to desktops when forwarding using the display protocol port filtered by client IP.

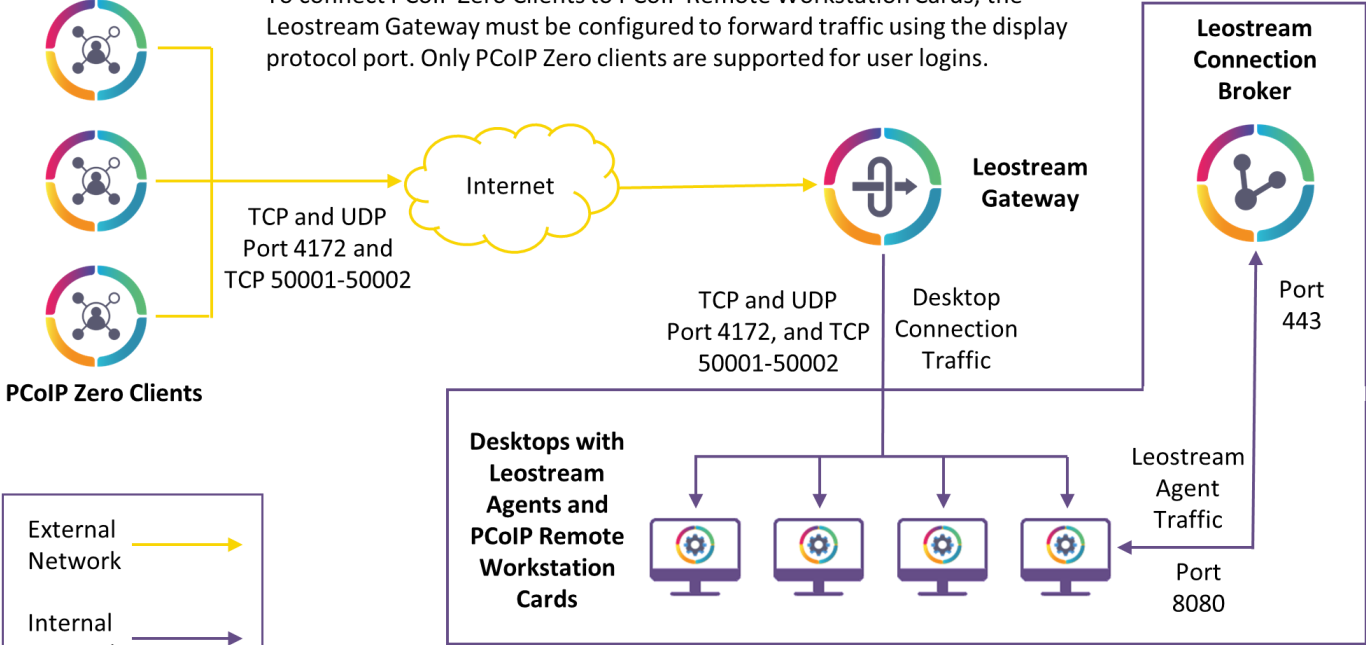
Working with PCoIP Remote Workstation Cards

Currently, the Leostream Gateway can forward PCoIP traffic for users with a PCoIP Zero client or PCoIP Software client (launched from a Leostream Connect login) to a PCoIP Remote Workstation Card, including the Amulet Hotkey KVM Extenders. This feature allows remote users to connect to high-performance workstations from home, without requiring hardware-based VPN solutions or Enterprise NAT configurations.

You must configure the Leostream Gateway to forward traffic along the display protocol port, filtered by client IP address. In this configuration, every PCoIP Zero client must report a unique IP address to the Connection Broker. Therefore, octal support for Amulet Hotkey devices is not currently supported through the Leostream Gateway.

Step 2: PCoIP Connections for PCoIP Remote Workstation Cards

To connect PCoIP Zero Clients to PCoIP Remote Workstation Cards, the Leostream Gateway must be configured to forward traffic using the display protocol port. Only PCoIP Zero clients are supported for user logins.



Installing the Leostream Gateway

Leostream Gateway 202x can be installed on any virtual or physical machine running the latest Red Hat Enterprise Linux 8.x operating system or one of its derivatives such as Rocky Linux and AlmaLinux OS.



The Leostream Gateway does not install on CentOS 8 or any other Linux distribution.

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.



You do not apply a license to the Leostream Gateway, itself. 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 and the bandwidth of the network.

When using the built-in HTML5 viewer, the Leostream Gateway utilizes CPU to translate the RDP, VNC, and SSH screens to HTML5. Therefore, if you are using the built-in HTML5 viewer, when provisioning the machine that will host your Leostream Gateway, allocate as much CPU as possible. Machines with higher CPU support more simultaneous connections.



The NoMachine, DCV, and Scyld Cloud Workstation HTML5 Viewers are treated as post-forwarded display protocols. The Leostream Gateway does not translate these protocols to HTML5.

For port-forwarded display protocol traffic, the CPU load on the Leostream Gateway is very low. In this case, the limiting factor for the number of simultaneous connections that can be handled by a single Leostream Gateway is a factor of the bandwidth of the network.

At a minimum, Leostream recommends:

- 2 or more CPUs or vCPUs at 2.5 GHz or higher
- 4 GB of RAM
- 4 GB of swap space
- 20 GB of free disk

Regardless of the size of the machine, Leostream recommends a maximum of 80 simultaneous connections. To handle larger environments, install multiple Leostream Gateways and use a load balancer to distribute user connections between gateways in a cluster (see [Configuring Leostream Gateway Clusters](#).)

When using the Leostream Gateway to port-forward client-based display protocols, the 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.

Using Security-Enhanced Linux (SELinux)

New installations of Leostream Gateway 2023.1.0.11 enable Security-Enhanced Linux (SELinux), by default.

When upgrading an existing Leostream Gateway to version 2023, perform the Leostream Gateway upgrade, manually enable SELinux on the Linux machine, and reboot the machine. After rebooting, run the following two commands to enable SELinux for the Leostream Gateway.

```
sudo leosteam-gateway --selinux  
sudo /sbin/reboot
```

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.



The Leostream Gateway uses the version of the Apache web server that is installed on the underlying operating system. Ensure that you keep your Linux operating system up-to-date to ensure you are using the latest Apache version. See [Permission Requirements](#) for important requirements related to the system `apache` user.

Upgrades can be applied to an existing Leostream Gateway by running the following command.

```
sudo dnf update leostream_gateway
```

Offline Installation and Upgrade

If you prefer to perform a manual installation, you can download the Leostream Gateway RPM from the Leostream downloads page.

<https://license.leostream.com/download.html>

When visiting the downloads page, the following login dialog appears.

Leostream downloads

Serial number

This is the serial number sent to you by Leostream sales or support

Email address


The email address associated with your Leostream license

Signing in constitutes continued acceptance of the [license agreement](#).

To view your permissible downloads:

1. Enter your Leostream Serial number.
2. Enter the Contact email address associated with your serial number. If you do not know your Contact email address, please contact sales@leostream.com.

After building your base operating system and applying all updates, copy the downloaded Leostream Gateway RPM into your user's home directory. You can then use the following commands to install your Leostream Gateway.

 This installation method requires access to local Red Hat repositories to pull all necessary Leostream Gateway dependencies.

```
sudo dnf -y install epel-release  
sudo dnf -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 dnf -y localinstall RPM_FILE_NAME
```

Changing the Default Leostream Gateway Port

By default, the Leostream Gateway web server uses port 443. In some situations, such as when using the built-in HTML5 viewer behind a load balancer or forwarding Scyld Cloud Workstation traffic along port 443, you may want to switch the Leostream Gateway to a non-standard HTTPS port.

To switch the Leostream Gateway port:


1. Log into the Leostream Gateway machine console as the `root` user or as a user with `sudo` permissions.

2. Edit the following file:

```
/etc/httpd/conf.d/ssl.conf
```

3. Near the top of the file, modify the `Listen 443 https` line to use your chosen port, for example:

```
Listen 9443 https
```


 When selecting a custom port, do not use port 8080 if you plan to use the Leostream HTML5 viewer.

4. Farther down in the file, locate the `<VirtualHost _default_:443>` line and set the port number to the same port you specified in step 3, for example:

```
<VirtualHost _default_:9443>
```

5. Save the `ssl.conf` file.
6. At a terminal prompt, add a new permanent firewall rule to the Leostream Gateway firewall, to allow traffic on your chosen port, for example:

```
sudo firewall-cmd --zone=public --add-port=9443/tcp --permanent
```

 Leostream does not recommend any other changes to the Leostream Gateway firewall.

7. Restart the Leostream Gateway

```
sudo /sbin/reboot
```

The Leostream Gateway continues to use HTTPS along the port you specify. When adding the Leostream Gateway to your Connection Broker, ensure that you specify the new port (see [Attaching the Leostream Gateway to a Connection Broker](#)).

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.

Permission Requirements

In order to function properly, the Leostream Gateway requires `sudo` privileges on the machine on which it is installed. After the installation completes, ensure that the following file exists.

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

 The Leostream Gateway will not function if the `leo` user does not have `sudo` privileges. The contents of the `leo` file must be as follows:

```
apache ALL=(ALL) !ALL
apache ALL=NOPASSWD: /usr/bin/firewall-
cmd,/usr/sbin/conntrack,/usr/bin/htpasswd,/usr/sbin/reboot,/usr/bin
/leostream-gateway
Defaults !requiretty
```

The Leostream Gateway leverages the default Apache installation on the RHEL machine on which it is installed. In order to manipulate `firewalld`, the `apache` user must have the required privileges. To test that the `apache` user has the appropriate privileges, run the following commands:

```
su - apache
sudo firewall-cmd --list-all
```

If `firewall-cmd` does not execute, the `apache` user does not have the required permissions.

Listing Connections

You can use connection tracking or the firewall to see what desktop connections are currently being sent through a particular Leostream Gateway. The firewall lists only client-based display protocols, such as NoMachine and Mechdyne TGX, while connection tracking shows all connections and indicates if an HTML5 connection is RDP, VNC, or SSH.

You can use the Leostream Gateway CLI to list all port-forwarded desktop connections, for example:

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

The output lists the IP address and port of the source and destination for the connection.

Alternatively, you can query the firewall to list all current client-based connections by executing the following command at the Linux prompt.

```
sudo firewall-cmd --list-all
```

For example:

```
[root@kdg-90gateway ~]# firewall-cmd --list-all
public (active)
target: default
icmp-block-inversion: no
interfaces: ens192
sources:
services: dhcpv6-client http https ssh
ports: 8080/tcp
protocols:
masquerade: yes
forward-ports:
source-ports:
icmp-blocks:
rich rules:
  rule family="ipv4" source address=<CLIENT_IP> forward-port port="4172" protocol="tcp" to-port="4172" to-addr=<DST_IP>
  rule family="ipv4" source address=<CLIENT_IP> forward-port port="4172" protocol="udp" to-port="4172" to-addr=<DST_IP>
```

The `source address` indicates the user's client IP address and the forwarded port indicates the display protocol they are using. In the previous figure, TCP and UDP ports 4172 are being forwarded, indicating a connection to a PCoIP Remote Workstation Card. The `to-addr`, in this case, is the address of the Remote Workstation Card, but for other display protocols indicates the address of the user's connected desktop.

The firewall list does not include any active connections using the HTML5 viewer. Use connection tracking to view a full list of connections, including the HTML5 connections by executing the following command at the Linux prompt

```
sudo conntrack -D
```

The output can take a number of formats, depending on how you configured your Leostream Gateway on the **> Setup > Gateways** page in your Connection Broker and what display protocol is used. Below are a few examples.

Example: HTML5 RDP Connection

```
ESTABLISHED src=gateway-ip dst=desktop-ip sport=47606 dport=3389
src=desktop-ip dst=gateway-ip sport=3389 dport=47606
```

In addition to the connection to the RDP port 3389 on the remote desktop, you'll find a corresponding Web browser connection from the user's client to the Leostream Gateway along port 443.

```
ESTABLISHED src=client-ip dst=gateway-ip sport=54126 dport=443
src=gateway-ip dst=client-ip sport=443 dport=54126
```

Example: Client-based RDP Connection – Gateway forwarding along random port

```
ESTABLISHED src=client-ip dst=gateway-ip sport=54021 dport=random-port  
src=desktop-ip dst=gateway-ip sport=3389 dport=54021
```

Where *random-port* is in the range you specified using the *leostream-gateway* CLI (see [Setting the Port Range for Desktop Connections](#)).


Example: HP ZCentral Remote Boost Connection – Leostream Gateway forwarding on protocol-specific port

```
ESTABLISHED src=client-ip dst=gateway-ip sport=53889 dport=42966  
src=desktop-ip dst=gateway-ip sport=42966 dport=53889
```

Where 42966 is the Remote port.

Using the Leostream Gateway CLI

The Leostream Gateway provides a limited command line interface (CLI) that supports the tasks described in this chapter and in the [Listing Connections](#) section.

 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.

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

Applying SSL Certificates

The Leostream Gateway uses the default Apache installation on the RHEL machine where it is installed. During installation, the Leostream Gateway generates a default operating system SSL certificate. This self-signed certificate produces warnings when users establish HTML5-based desktop connections.

To avoid these warnings, you can install your corporate SSL certificates or use the Leostream Gateway CLI to generate and install a signed SSL certificate. Expert users or more complicated setups should use the standard Apache SSL instructions available on the internet

If you have an existing SSL certificate chain, copy all certificates associated with the chain to your Leostream Gateway and edit the `/etc/httpd/conf.d/ssl.conf` file to point at the appropriate certificates and keys. After editing the file, restart Apache or the Leostream Gateway machine.

The SSL options of the `leostream-gateway` CLI help with standard setups, as described below.

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

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

Step through the instructions to provide the information needed to generate the CSR. The value you enter for the Site Name is used both for the Common Name (CN) and subjectAltName (SAN). When finished, the CSR is stored in a file named `server.csr` in your current directory.

The Leostream Gateway uses the private key generated when you originally installed the underlying operating system. It can be found in:

```
/etc/pki/tls/private/localhost.key
```

 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.


 The certificate must be a CRT-file. PEM-files are not supported.

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>
```

- The `--ssl-crt` option must be a `.crt` file
- The `--ssl-int` option must be a `.crt` file
- The `--ssl-key` option must be a `.key` file

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

 If the certificates are not installed correctly, Apache will not start and the Leostream Gateway cannot function. If Apache is not running on your Leostream Gateway, check that you installed the entire certificate chain and correct keys.

You can check the status of Apache by running the following command on the Leostream Gateway machine:

```
sudo systemctl status httpd
```

Setting the Port Range for Desktop Connections


If the Leostream Gateway is configured to route traffic from a random port on the client device to the display protocol port on the remote host, the Leostream Gateway defaults to choosing a port between 20001 and 23000. 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 firewall (see [The Importance of firewalld](#) for more information.)

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 Leostream Gateway on the port range, as well.

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

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

The number of simultaneous connections a particular Leostream Gateway can proxy is limited by the number of ports in the range. Ensure that you specify a large enough number of ports to support the number of connections you plan to proxy.

 In the case of TGX 1.10 connections, the Leostream Gateway chooses the starting port randomly, ensuring that 17 sequential ports are available. However, gaps in the port range that are smaller than 17 may appear. For TGX 1.10, you should over allocate the port range to ensure that desktop connections will succeed.

Manually Detaching a Leostream Gateway from a Connection Broker

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

You can break the attachment by deleting the Leostream Gateway record on the **> Setup > Gateways** page.

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

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

You can then attach your Leostream Gateway to a new Connection Broker.

Starting and Stopping the Leostream Gateway

You can use the `--stop` and `--start` options to stop, start, and restart the Leostream Gateway. To perform a restart, use the `--stop` option followed by the `--start` option.

Stopping the Leostream Gateway allows you to quickly drop all connections and close all forwarded ports without rebooting the entire operating system or manually manipulating the firewall.

Generating a Leostream Gateway Log Package

Leostream Gateway logs are located in `/var/log/tomcat/guacamole.log`. If you need to provide logs to Leostream Technical Support, use the following command to create the logs.

```
sudo 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.

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

Disabling and Enabling the Built-In HTML5 Viewer

By default, the Leostream Gateway enables the built-in HTML5 viewer for RDP, VNC, and SSH connections. If you do not plan to use the built-in HTML5 viewer, you can disable the service by executing the following commands:

```
sudo leostream-gateway --no-guac  
sudo /sbin/reboot
```

 When the HTML5 viewer is disabled, do not select the **Leostream HTML5 Viewer** option in any of your Leostream Protocol Plans. Users will receive an error if they are assigned to protocol plans that attempt to launch HTML5 connections.

To enable the HTML5 viewer, execute the following commands:

```
sudo leostream-gateway --guac  
sudo /sbin/reboot
```

Using the Leostream Gateway to Forward Azure API Calls

To create an Azure center in your Connection Broker, the Connection Broker must have internet access to access the following Azure URLs.

```
https://login.microsoftonline.com/...  
https://management.core.windows.net/  
https://management.azure.com/  
https://<storage-account-name>.blob.core.windows.net/  
https://<storage-account-name>.blob.core.windows.net:443/
```

If your Connection Broker cannot contact these URLs, you can use the Leostream Gateway to proxy the Azure URL calls. To enable Azure URL forwarding, log into the Leostream Gateway console and execute the following command:

```
sudo leostream-gateway --azure
```

After executing the command, you can run the following command to confirm that Azure Broker forwarding is ON.

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

Ensure that at least one of the Leostream Gateways attached to your Connection Broker enables Azure URL forwarding. The Leostream Gateways currently attached to your Connection Broker are listed on the > **Setup** > **Gateway** page.

When you create your Azure center in the Connection Broker, ensure that you select the **Use a Leostream Gateway to communicate with this Center** option. You do not need to specify which gateway to use for Azure URL forwarding. The Connection Broker will choose a Leostream Gateway from all its attached gateways that enable Azure URL forwarding. If multiple Leostream Gateways enable Azure URL forwarding, the Connection Broker automatically fails over between the gateways in the event an Azure URL call fails.

To stop forwarding Azure URL calls through the Leostream Gateway, run the following command.

```
sudo leostream-gateway --no-azure
```

Integrating with the Connection Broker

The following procedure describes how to configure your Leostream environment to leverage the Leostream Gateway for Connection Broker login and display protocol forwarding.

1. [Enable Connection Broker Login forwarding](#) in the Leostream Gateway
2. Attach the Leostream Gateway to your Connection Broker (see [Attaching the Leostream Gateway to a Connection Broker](#))
3. Create protocol plans that use the Leostream Gateway (see [Building Protocol Plans for the HTML5 Viewer](#) and [Building Protocol Plans for Client-Based Display Protocols](#))
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

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, the Connection Broker does not need to be accessible from the user's client device and, instead, can be isolated in the same network as your desktops.

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

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


If you have a Connection Broker cluster behind a load balancer, enter the address of your load balancer.

After forwarding is enabled, all URLs that point 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 to access the Leostream Gateway API.

 The Leostream Gateway leverages Apache, which imposes a character limit of 63 on the `ProxyAddress` directive. Amazon Elastic Load Balancers (ELB) may exceed this character limit. If the FQDN you are forwarding to is over 63 characters, configure a CNAME record in your DNS servers to map the FQDN to a shorter hostname



After Connection Broker forwarding is enabled on your Leostream Gateway, users enter the Leostream Gateway address into their client devices, not the Connection Broker. The gateway forwards the login to the Connection Broker, which is still responsible for authenticating the user, assigning a policy, and indicating which desktop to connect.

 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:

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

Attaching the Leostream Gateway to a Connection Broker

Each Leostream Gateway can be attached to a single Connection Broker or Connection Broker cluster. You attach your Leostream Gateway to 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. If this Leostream Gateway is part of a gateway cluster, use the **Add this Leostream Gateway to a Gateway Cluster** drop-down menu to add this gateway to the appropriate cluster. (see [Configuring Leostream Gateway Clusters](#))
6. The value you enter in the **Public IP address or FQDN for use in Protocol Plans** edit field depends on if this is a standalone Leostream Gateway or if it will be part of a Gateway Cluster.

- If this is a standalone Leostream Gateway, enter the publicly accessible IP address or hostname for your Leostream Gateway. If you are placing the Leostream Gateway behind your corporate firewall, enter the public address of your firewall.




This address must be accessible by the end users' client devices and is the address used to log into Leostream and for forwarded desktop connections.

If you have installed a corporate certificate onto the Leostream Gateway, enter the FQDN of the Leostream Gateway in the **Address** field, to ensure users do not receive certificate errors when connecting to their desktops.

- If this gateway will be part of a Gateway Cluster, enter your Leostream Gateways private address. You will specify the publicly accessible address in the Gateway Cluster.
7. In the **IP address or FQDN used for Connection Broker communications to this Gateway** 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. This address is never used for forwarding display protocol traffic.

If this Leostream Gateway is not part of a cluster and is behind your corporate firewall, enter the address that your firewall uses to NAT traffic to your Leostream Gateway.

 If you changed the default Leostream Gateway port (see [Changing the Default Leostream Gateway Port](#)) ensure that the address you enter in both the **Public IP address or FQDN for use in Protocol Plans** and **IP address or FQDN used for Connection Broker communications to this Gateway** fields includes the new port, for example:

```
my-gateway-name.my-company-name.com:9443
```

8. If this gateway is used to forward client-based display-protocol traffic, use the **Method for routing display protocol traffic through this Leostream Gateway** drop-down menu to indicate which method the gateway uses to configure the firewall rule for routing traffic.

You must configure the Leostream Gateway to forward traffic along the display protocol port, filtered by client IP address, if you plan to use this Leostream Gateway to forward PCoIP traffic to Remote Workstation Cards.



If this gateway is part of a cluster, this option is set on the cluster instead of on the individual gateway.


9. Click **Save**.

After saving the form, the Connection Broker registers with the Leostream Gateway and you can now use the gateway in your protocol plans.

The Connection Broker authenticates all calls it makes to the Leostream Gateway. To ensure that the Connection Broker communication is properly configured to authenticate, inspect the, `/var/www/auth` file in the Leostream Gateway and ensure that the `broker` user exists.



You may add as many Leostream Gateways as required in your Leostream environment. If your Leostream license is preventing you from adding Leostream Gateways, please contact sales@leostream.com to expand the number of supported gateways in your license.

 You cannot save the form if the Leostream Gateway is already attached to another Connection Broker. If you receive an error indicating that the Leostream Gateway is controlled by another Connection Broker, log into that Connection Broker and remove the Leostream Gateway (see [Removing a Leostream Gateway from a 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 Detaching a Leostream Gateway 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 FQDN of your Leostream Gateway.

Removing a Leostream Gateway from a Connection Broker

Each Leostream Gateway can be attached to 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 detach it from its original Leostream environment.

You can detach 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 detach the Leostream Gateway using the Gateway CLI (see [Manually Detaching a Leostream Gateway 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.

Configuring Leostream Gateway Clusters

To support a large deployment and provide high availability, you can create a cluster 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.



Load balancers used with Leostream must be configured to use sticky sessions.

After configuring your load balancer, build the Gateway Cluster in your Connection Broker, as follows.

1. Go to the > **Setup > Gateways** page.
2. Click the **Add Gateway Cluster** link.
3. In the **Add Gateway Cluster** form, enter a display name for your cluster in the **Name** edit field.
4. Indicate which Leostream Gateways should be configured to forward the display protocol traffic.
 - a. **All Gateways in this cluster** – In this case, the Connection Broker allows your load balancer to control which Leostream Gateway forwards the display protocol traffic. Because the Connection Broker cannot predict which Leostream Gateway that your load balancer will choose, the Connection Broker instructs all Leostream Gateways in the cluster to open an appropriate firewall rule.

When this option is selected, enter your load balancers IP address or resolvable hostname in the **Public IP address or FQDN of the external load balancer** field.

This address must be accessible by the end users' client devices, and is the address used in Protocol Plans for the desktop connection. If you already attached a Leostream Gateway with this address to your Connection Broker, you must first edit that gateway record on the > **Setup > Gateway** page and reset the **Address** field to its private address.

- b. **Only the Gateway that forwarded login traffic for this session** – If you enabled Connection Broker forwarding on your Leostream Gateways *and* your load balancer enforces sticky sessions, you can select this option to have the Connection Broker configure port forwarding only in the firewall of the Leostream Gateway that forwarded the user's login traffic.

When using this option, the users protocol plan includes the address in the **Public IP address or FQDN for use in Protocol Plans** field of the Leostream Gateway that is forwarded the user login so this address must be available to the user's client.

This option allows more connections through your cluster, as Leostream isn't opening redundant ports on all the Leostream Gateways in the cluster.

5. Use the **Method for routing display protocol traffic through this Leostream Gateway** drop-down menu to indicate which method the gateway uses to configure the firewall rule for routing traffic.

You must configure the Leostream Gateway to forward traffic along the display protocol port, filtered by client IP address, if you plan to use this Leostream Gateway to forward PCoIP traffic to Remote Workstation Cards.

This value overrides any settings previously made in Leostream Gateways that are added to this cluster.

6. Click **Save**.

After creating the Gateway Cluster, indicate which Leostream Gateways are included that cluster, as follows.

1. On the > **Setup > Gateways** page, click the **Edit** link for each of the appropriate gateways.
2. Use the **Add this Leostream Gateway to a Gateway cluster** drop-down to indicate which cluster this gateway belongs in.
3. Click **Save**.



When using a Gateway Cluster ensure that you select the Gateway Cluster in the **Gateway** drop-down menus in your Protocol Plan.

Configuring Clients to Log into your Leostream Environment

The Leostream Gateway supports desktop connections from Leostream Connect, the Leostream Web client, and PCoIP Zero 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 [Forwarding Connection Broker Logins through the Gateway](#)) and enter the Leostream Gateway address in the user's client. In this case:

- For Leostream Connect, enter the public IP or DNS name of the Leostream Gateway or gateway load balancer 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 or gateway load balancer
- For PCoIP Zero clients, select the **PCoIP Connection Manager** as the **Session** type and enter the public IP or FQDN of the Leostream Gateway or gateway load balancer.

Building Protocol Plans for the Built-In HTML5 Viewer

The Leostream Gateway HTML5 viewer supports in-browser RDP, VNC, and SSH connections to Windows, Linux, and macOS 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.

Leostream Gateway 2022 requires FreeRDP 2.2 to establish HTML5 RDP connections. You can check which version of FreeRDP is installed on your Leostream Gateway by logging into the gateway terminal and running the following command.

```
rpm -q freerdp
```

It should return a FreeRDP version 2, for example:

```
freerdp-2.2.0-7.el8_5.x86_64
```

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, select **1** from the **Priority** drop-down menu associated with the **Leostream HTML5 Viewer**.
4. From the **Gateway** drop-down menu, select the Gateway Cluster or specific Leostream Gateway to use for connections created from this protocol plan.
5. From the **Protocol** drop-down menu, indicate if this protocol plan launches RDP, VNC, or SSH.
6. Configure the protocol-specific parameters, as described in the following sections.
7. Click **Save**.

Ensure you select this protocol plan in the **Plan** sub-section of the appropriate section of the user's policy.

HTML5 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. Select **Audio input** to support audio in and out of the remote session. Note that audio in works only in cases where the client and remote host have the same operating system and the web browser supports your audio devices.
6. Select **Disable HTML5 remote desktop viewer menu** to prevent the user from opening the sidebar menu by pressing Ctrl-Alt-Shift.
7. Select **Disable single sign-on to desktop** if the user needs to sign into the remote desktop using different credentials that used to log into Leostream.
8. Select **Disable clipboard** to prohibit copy/paste out of the remote session.
9. See [RemoteApp Sessions](#) for information on using the RemoteApp options.
10. Use the **Keyboard** drop-down menu to set the server-side keyboard layout.
11. 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.)

12. 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

HTML5 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, 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.

To create a protocol plan that launches a RemoteApp session through the Leostream Gateway:

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.

HTML5 VNC Connections

HTML5 VNC connections are available for Windows, Linux, and macOS 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 and macOS 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.

The **VNC port** field indicates the port used for the VNC session. If the user is connecting to Linux and the Leostream Agent starts the VNC session for the user, use the {VNC_PORT} dynamic tag in this field. Otherwise, to connect the user to existing VNC sessions, enter the port number, for example 5900.

When connecting to Linux, you can send command line parameters for the Leostream Agent to use when starting the VNC session, as well as indicate if the Leostream Agent should check if the VNC password is set.

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 Gateway.

Building Protocol Plans for Client-Based Display Protocols

The Leostream Gateway can be used to forward Microsoft RDP, HP Remote Boost (RGS), Mechdyne TGX, NoMachine, NICE DCV, and Teradici PCoIP connections for Remote Workstation Cards. Users can log in using either Leostream Connect or the Leostream Web client, in addition to leveraging PCoIP Zero clients for PCoIP.

When using Leostream Connect with RDP, Remote Boost, and TGX, you can also pass USB devices through the Leostream Gateway.

Enabling the Leostream Gateway for RDP, Remote Boost, NoMachine, DCV, and TGX

To configure a protocol plan to send the connection traffic through the gateway:

1. Go to the > **Configuration > Protocol Plans** page in your Connection Broker.
2. Edit an existing protocol plan or click **Create Protocol Plan** 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 display protocol you want to pass through the Leostream Gateway, for example, **NoMachine**, and set the **Priority** for this protocol to **1**.
5. Use the **Configuration file** field to configure how the desktop connection is launched, such as setting the resolution. You do not need to make any changes to the configuration file to support the Leostream Gateway.
6. From the **Gateway** drop-down menu in this sub-section, select the Leostream Gateway or Gateway Cluster to use for desktop connections launched using this Protocol Plan.
7. Set the **Priority** menu for all other protocols to **Do not use**.
8. Save the protocol plan

Enabling the Leostream Gateway for PCoIP

You configure a protocol plan to send the PCoIP traffic through the Leostream Gateway, as follows:

1. Go to the > **Configuration > Protocol Plans** page in your Connection Broker.
2. Either edit an existing protocol plan or click the **Create Protocol Plan** link to build a new plan.
3. For users logging in using Leostream Connect and the PCoIP Software client:
 - a. Select **1** for the **Priority** of the **PCoIP Software Client** in the **Leostream Connect** section of the protocol plan.
 - b. From the **Gateway** drop-down menu, select the Leostream Gateway to use for connections.
4. For users logging in using a PCoIP Zero client:
 - a. Scroll down to the **PCoIP Client Configuration** section.
 - b. From the **Gateway** drop-down menu in this sub-section, select the Leostream Gateway to use for connections, for example:

▼ **PCoIP Client Configuration**

Alternate port for remote viewer port check

If policies use the remote viewer port check to invoke backup pools, enter the port to check for PCoIP connections

Desktop attribute to use for PCoIP connection

If PCoIP Connection Manager or Client is unable to resolve the desktop's hostname, use a Dynamic Tag such as {IP_PRIVATE} for the desktop hostname

5. Click **Save**.

After you build your protocol plans, use policies to assign these protocol plans to pools or hard-assigned desktops. Users are then assigned to policies on the **> Configuration > Assignments** page. Refer to the main section of this quick start guide for complete instructions.

Working with HP ZCentral Remote Boost

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

In order to enable Remote Boost Velocity, the Leostream Gateway forwards Remote Boost traffic on TCP and UDP port 42966.

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

To reset the default Remote Boost Receiver Network port:

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

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

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

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

Working with Mechdyne TGX


Each Mechdyne TGX 1.10 connection requires a range of ports, instead of a single port. The Leostream Gateway, therefore, assigns a random range of ports to each TGX connection, regardless of the TGX version.

Keep this in mind when determining the number of ports to configure for connections (see [Setting](#)

[the Port Range for Desktop Connections](#)) as the number of simultaneous TGX connections through a Leostream Gateway is less than for RGS or RDP.

Working with NICE DCV

The default configuration file passed to the NICE DCV client includes the user's credentials, including a plain text password. To avoid sending plain text passwords in the configuration file, you can select the **User DCV External authenticator with token** option.

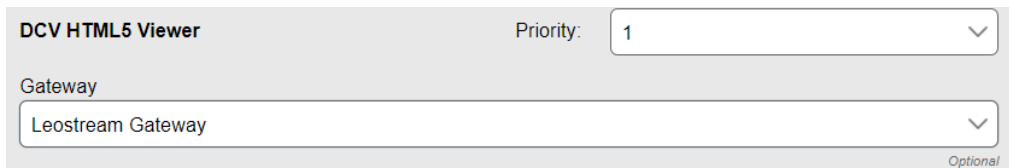
 When using the DCV External Authenticator, you must enable the REST API in the Connection Broker. See the [Connection Broker Application Guide](#) for instructions.

Building Protocol Plans for Third-Party HTML5 Viewers

When logging in using the Leostream Web client, users can connect to their desktops in-browser using NoMachine, NICE DCV, and Scyld Cloud Workstation protocols.

To configure a protocol plan to use one of these protocols:

1. Go to the > **Configuration > Protocol Plans** page in your Connection Broker.
2. Edit an existing protocol plan or click **Create Protocol Plan** to build a new plan.
3. Go to the **Web Browser** section of the protocol plan.
4. Find the sub-section associated with the HTML5 Viewer you want to use, for example, **DCV HTML5 Viewer**, and set the **Priority** for this protocol to **1**.
5. From the **Gateway** drop-down menu in this sub-section, select the Leostream Gateway or Gateway Cluster to use for desktop connections launched using this Protocol Plan, for example:



DCV HTML5 Viewer

Priority: 1

Gateway

Leostream Gateway

Optional

6. Click **Save**.



The Leostream Gateway treats all third-party HTML5 Viewers as port-forwarded display protocols.

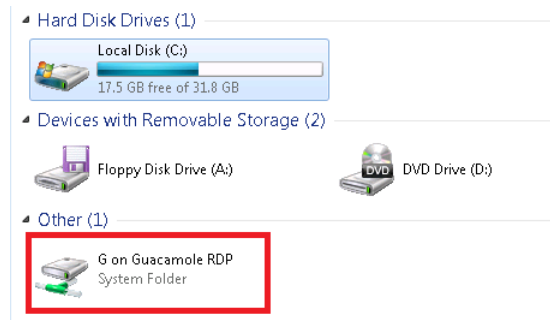
Working with the HTML5 RDP Viewer

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:

