

---

## Getting Started Guide

- [Getting Started Guide](#)
  - [LineRate Overview](#)
    - [About This Guide](#)
    - [Technical Support](#)
    - [System Requirements](#)
  - [Installing LineRate](#)
    - [Installing to a Local Disk on a Dedicated Server](#)
    - [Diskless Software Deployment](#)
    - [Installing on VMWare vSphere](#)
  - [Accessing the the LineRate CLI](#)
  - [Configuring Licensing](#)
  - [Using the Command Line Interface](#)
  - [Working with Bases](#)
  - [Configuring Management Interfaces](#)
  - [Configuring a Forward Proxy](#)
    - [Configuring Data Interfaces](#)
    - [Configuring the Virtual IP](#)
    - [Configuring the Forward Proxy](#)
  - [Configuring a Reverse Proxy](#)
    - [Configuring Data Interfaces](#)
    - [Configuring Load Balancing](#)
      - [Monitoring and Troubleshooting Load Balancing](#)
    - [Configuring SSL](#)
    - [Complete Example Show Run Output](#)

---

## LineRate Overview

1. [Overview](#)
2. [Reverse Proxy](#)
3. [Forward Proxy](#)
4. [LineRate Security](#)
5. [IP-based Protocols](#)
  - 5.1. [UDP](#)
  - 5.2. [TCP](#)
  - 5.3. [CARP](#)
  - 5.4. [ICMP](#)
  - 5.5. [Other](#)
6. [Non-IP-based Protocols](#)
  - 6.1. [ARP, LACP, and VLAN](#)
  - 6.2. [Other](#)
7. [What's Next](#)

LineRate® from F5® is the industry's first purely software-defined network appliance delivering advanced performance, availability, and scale to web and secure web services. You install LineRate natively on a server platform or as a virtual appliance on a hypervisor to create a highly scalable network appliance.

---

## Reverse Proxy

The LineRate reverse proxy capability provides a full-proxy front-end to the web and secure web services on back-end servers of the application. To successfully manage load, health, and availability of the application, LineRate constantly monitors the traffic flows from the client to the back-end servers to ensure the delivery of the application services. LineRate provides several discrete services including health monitoring, transaction statistics, and traffic management to ensure balanced usage of back-end servers and rapid client service.

---

## Forward Proxy

The LineRate forward proxy capability provides a proxy function from one network to another. A common use case for a forward proxy is for connections from your private network to the Internet.

A forward proxy lets you insert custom logic created with scripts. Scripts can perform a variety of functions, including gathering usage statistics, redirecting requests to your own cache, blocking of access to specific sites, managing cookies, and much more.

To use a forward proxy effectively, be sure to create and attach a virtual IP that includes the range of Internet IP addresses you want to go through the forward proxy.

---



When attaching a virtual IP to a forward proxy, the virtual IP must not include any of the system's own IP addresses. For a virtual IP with a single IP address, do not set the virtual IP's IP address to one of the system's own IP addresses. For a virtual IP with a range of addresses, you must ensure that the IP address range does not contain any of the system's own IP addresses. This may mean you need to break the virtual IP into multiple virtual IPs. See [Configuring a range for a virtual IP with forward proxy](#) for more detail and an example.

---

---

## LineRate Security

LineRate uses several security measures to mitigate Denial of Service (DoS) attacks. These measures greatly reduce the system's vulnerability to DoS attacks. In general, the system ignores ("black-holes") requests to IP addresses and ports that are not configured on an interface or virtual IP.

The sections below provide additional details.

---

## IP-based Protocols

The sections below describe how the system handles IP-based protocols.

---

### UDP

The system discards most UDP requests, with the exception of DNS request responses. The system accepts the following traffic:

- MOUNT (dynamic port number)
- NFS (port 2049)
- RPCBIND (port 111)
- STAT (dynamic port number)

Aside from the RPCBIND service, these Sun RPC services have dynamically assigned port numbers which are then discovered by the client via RPCBIND. Client traffic returning on ephemeral ports will also be accepted and processed.

All other traffic on ports without bound sockets in the LISTEN state is discarded without processing or ICMP generation.

These services are all NFS-related. These ports will be open and active only when using the PXE boot feature in LineRate.

---

## TCP

The system accepts TCP traffic only on IPs and ports configured on virtual IPs, for the REST server, for the SSH server, and for active TCP connections initiated by the LineRate, such as those to real servers. TCP traffic directed to other IPs and ports on the system not in those categories will be dropped without acknowledgement or ICMP generation.

---

## CARP

The system accepts and processes all inbound CARP traffic.

---

## ICMP

The system accepts ICMPv4 messages with the following [Type, Code] pairs:

- [0x00, 0x00] - Echo Reply
- [0x08, 0x00] - Echo Request\*
- [0x03, 0x03] - Destination Port Unreachable
- [0x03, 0x04] - Destination Requires Fragmentation
- [0x0B, 0x00] - Time Exceeded

The system accepts ICMPv6 messages with the following [Type, Code] pairs:

- [0x81, 0x00] - Echo Reply
- [0x80, 0x00] - Echo Request\*
- [0x01, 0x04] - Destination Port Unreachable
- [0x02, 0x00] - Packet Too Big
- [0x03, 0x00] - Time Exceeded
- [0x87, 0x00] - Neighbor Solicitation
- [0x88, 0x00] - Neighbor Advertisement

\* - When not in gateway (IP forwarding) mode, the following criteria must be met:

- Destination IP address for the incoming request must be an address assigned to the ingress interface, or a CARP IP address on the ingress interface or an IP address on a loopback interface.
- The ICMP response must route out the ingress interface (reverse path filtering).
- The source IP address must be within the same IP subnet as the destination. This means that ICMP "pings" are only responded to when initiated from a host local to one of the LineRate system's interfaces.

All other ICMP traffic is ignored without processing.

---

## Other

Any inbound IP traffic not explicitly referenced above is dropped without any processing.

---

## Non-IP-based Protocols

The sections below describe how the system handles non-IP-based protocols.

---

## ARP, LACP, and VLAN

The system accepts and processes all ARP, LACP, and VLAN traffic normally and responds appropriately.

---

## Other

The system drops, without processing, any non-IP traffic not explicitly mentioned above.

---

## What's Next

The rest of this *Getting Started Guide* describes how to install LineRate and takes you through an example configuration.

---

## About This Guide

1. [Audience](#)
2. [Conventions](#)
3. [Example IP Addresses](#)
4. [Searching the Guide](#)
  - 4.1. [Relevance Level](#)
  - 4.2. [Limiting a Search to Specific Tree](#)
  - 4.3. [Term Modifiers](#)
    - 4.3.1. [Wildcard Searches](#)
    - 4.3.2. [Fuzzy Searches](#)
    - 4.3.3. [Proximity Searches](#)
    - 4.3.4. [Boosting a Term](#)
  - 4.4. [Boolean Operators](#)
    - 4.4.1. [OR](#)
    - 4.4.2. [AND](#)
    - 4.4.3. [±](#)
    - 4.4.4. [NOT](#)
  - 4.5. [Grouping](#)
  - 4.6. [Escaping Special Characters](#)
5. [Legal Notices](#)
  - 5.1. [Copyright](#)
  - 5.2. [Trademarks](#)

---

## Audience

This guide is intended for experienced network administrators and network architects who understand your organization's existing TCP/IP network and who need to set up basic load balancing and SSL services using LineRate.

---

## Conventions

This guide uses the following symbols and typographic conventions.

Convention	Definition
<b>Monospaced bold</b>	Text in a monospaced bold font represents commands or other text that you type exactly as you see it.
<b>&lt;angle brackets&gt;</b>	Text in a monospaced bold font inside angle brackets represents a placeholder that describes what you must type.
<b>[square brackets]</b>	Text in a monospaced bold font inside angle brackets represents a an optional command or option.
Monospaced	Text in a monospaced font represents output or results the system displays.
<b>Bold</b>	Text in bold shows keys to press and items to select or click, such as menu items or buttons.
	Shows the beginning of a procedure.
 <b>Caution</b>	Cautions contain critical information about configuring your system or data.
 <b>Note</b>	Notes contain important information that may affect how you install or configure your system.
 <b>Tip</b>	Tips contain best practices or useful information to help you when configuring your system.
	Shows that the content is for advanced users.

---

## Example IP Addresses

Throughout this guide, we use example IP addresses for both internal (private) and external (public) uses.

For private addresses, we use the IP addresses designated in [RFC 1918](#):

- 10.0.0.0 - 10.255.255.255 (10/8 prefix)
- 172.16.0.0 - 172.31.255.255 (172.16/12 prefix)
- 192.168.0.0 - 192.168.255.255 (192.168/16 prefix)

For public addresses, we use the IP addresses designated for documentation in [RFC 5737](#):

- 192.0.2.0/24 (TEST-NET-1)
- 198.51.100.0/24 (TEST-NET-2)
- 203.0.113.0/24 (TEST-NET-3)

---

## Searching the Guide

The search box at the top-right of each page lets you enter a term or phrase to search for. By default, the system searches all pages in the LineRate content. Searches are not case sensitive. By default, searches find plurals and other matches from word stems, such as tests, testing, tested, and tester if you search for test.

You can search for a single term such as:

`interface`

Or

`certificate`

You can also search for an exact phrase surrounded by double quotes such as:

`"real server"`

Or

`"IP address"`

---

## Relevance Level

By default, the system sorts the search results by relevance. The relevance is determined by a weighting algorithm that takes into consideration the pages title, content, tags, and attachments. The relevance is also affected by the page rating (thumb up or down) and by how often other users select a page to view from similar searches.

You may find a large number of hits for these types of searches. You can narrow your searches a number of ways by:

- Limiting your search to a specific tree
- Using term modifiers
- Using Boolean operators

---

## Limiting a Search to Specific Tree

If you only want to search one area or tree of a guide, you can limit your search to that tree. For example, if you only want to search the Configure Command tree of the 2.2 Release of the CLI Reference Guide for the term "interface," you can enter your search like this:

```
+(path:300Release_2.2/200CLI_Reference_Guide/Configure_Commands/*) AND interface
```

You can further narrow the search using the term modifiers and Boolean operators (described below):

```
+(path:300Release_2.2/200CLI_Reference_Guide/Configure_Commands/*) AND interface  
AND CARP
```

```
+(path:300Release_2.2/*) AND load AND balancer
```



For a tree-specific search, words in quotes are not treated as a specific phrase. The search does an OR search for any words in quotes, so you may not want to use quotes and use AND instead, as shown in the example above.

---

A few steps to help with this type of search:

1. Navigate to the tree you want to search.
2. In your browser's address bar, copy the address of the page.
  - You only need the part after the "https://docs.lineratesystems.com/".
3. Using the syntax example above, type in your search and paste in the path of the page you want to search.

---

## Term Modifiers

The search supports modifying query terms to provide a wide range of searching options.

---

## Wildcard Searches

The guides support single- and multiple-character wildcard searches with single terms (not within phrase queries).

To perform a single-character wildcard search, use the ? symbol.

To perform a multiple-character wildcard search, use the \* symbol.

The single-character wildcard search looks for terms that match that with the single character replaced. For example, to search for "text" or "test" you can use the search:

```
te?t
```

Multiple character wildcard searches looks for 0 or more characters. For example, to search for test, tests or tester, you can use the search:

```
test*
```

You can also use the wildcard searches in the middle of a term.

```
te*t
```



You cannot use a \* or ? symbol as the first character of a search.

---

## Fuzzy Searches

The guide supports fuzzy searches based on the Levenshtein Distance or Edit Distance algorithm. To do a fuzzy, search use the tilde ~ symbol at the end of a single word. Fuzzy searches work for multiple characters. For example, to search for a term similar in spelling to "roam" use the fuzzy search:

```
roam~
```

This search will find terms like foam and roams.

You can add an optional parameter to specify the required similarity. The value is between 0 and 1. With a value closer to 1, only terms with a higher similarity will be matched. For example:

```
roam~0.6
```

The default is 0.5.

---

## Proximity Searches

The guide supports finding words that are within a specific distance from each other. To do a proximity search, use the tilde ~ symbol at the end of a phrase. For example, to search for a "feature" and "standard" within 10 words of each other in a document use the search:

```
"feature standard"~10
```

---

## Boosting a Term

The guide provides the relevance level of matching documents based on the terms found. To boost a term, use the caret ^ symbol with a boost factor (a number) at the end of the term you are searching. The higher the boost factor, the more relevant the term will be.

Boosting allows you to control the relevance of a document by boosting its term. For example, if you are searching for:

```
mindtouch search
```

and you want the term "mindtouch" to be more relevant boost it using the ^ symbol along with the boost factor next to the term. You would type:

```
mindtouch^4 search
```

This will make documents with the term mindtouch appear more relevant. You can also boost phrases as in the example:

```
"mindtouch search"^4 "Apache"
```

By default, the boost factor is 1. Although the boost factor must be positive, it can be less than 1 (e.g. 0.2)

---

## Boolean Operators

Boolean operators allow terms to be combined through logic operators. MindTouch supports AND, +, OR, NOT, and - as Boolean operators.



Boolean operators must be ALL CAPS.

---

### OR

The OR operator is the default conjunction operator. This means that if there is no Boolean operator between two terms, the OR operator is used. The OR operator links two terms and finds a matching document if either of the terms exist in a document. This is equivalent to a union using sets. The symbol || can be used in place of the word OR.

To search for documents that contain either "mindtouch search" or just "mindtouch" use the query:

```
"mindtouch search" mindtouch
```

or

```
"mindtouch search" OR mindtouch
```

---

### AND

The AND operator matches documents where both terms exist anywhere in the text of a single document. This is equivalent to an intersection using sets. You can use the symbol && in place of the word AND.

To search for documents that contain "mindtouch search" and "Advanced" use the query:

```
"mindtouch search" AND "Advanced"
```

---

## +

The + (required operator) requires that the term after the + symbol exist somewhere in a document.

To search for documents that must contain "search" and may contain "advanced," use the query:

```
+search advanced
```

---

## NOT

The NOT operator excludes documents that contain the term after NOT. This is equivalent to a difference using sets. You can use the symbol ! in place of the word NOT.

To search for documents that contain "mindtouch search" but not "Advanced" use the query:

```
"mindtouch search" NOT "Advanced"
```

---



The NOT operator cannot be used with just one term. For example, the following search will return no results:

```
NOT "mindtouch search"
```

---

---

## Grouping

The guide supports using parentheses to group clauses to form sub queries. This can be very useful if you want to control the Boolean logic for a query.

To search for either "mindtouch" or "search" and "advanced" use the query:

```
(mindtouch OR search) AND advanced
```

This eliminates any confusion and makes sure you that website must exist and either term mindtouch or search may exist.

---

## Escaping Special Characters

The Guide supports escaping special characters that are part of the query syntax. The current list of special characters is:

```
+ - && || ! ( ) { } [ ] ^ " ~ * ? : \
```

To escape these character use the \ before the character. For example, to search for (1+1):2 use the query:

```
\(1\+1\)\:2
```

---

# Legal Notices

---

## Copyright

Copyright © 2013, F5 Networks, Inc. All rights reserved.

F5 Networks, Inc. (F5) believes the information it furnishes to be accurate and reliable. However, F5 assumes no responsibility for the use of this information, nor any infringement of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent, copyright, or other intellectual property right of F5 except as specifically described by applicable user licenses. F5 reserves the right to change specifications at any time without notice.

---

## Trademarks

AAM, Access Policy Manager, Advanced Client Authentication, Advanced Firewall Manager, Advanced Routing, AFM, APM, Application Acceleration Manager, Application Security Manager, ARX, AskF5, ASM, BIG-IP, BIG-IQ, Cloud Extender, CloudFucious, Cloud Manager, Clustered Multiprocessing, CMP, COHESION, Data Manager, DevCentral, DevCentral [DESIGN], DNS Express, DSC, DSI, Edge Client, Edge Gateway, Edge Portal, ELEVATE, EM, Enterprise Manager, ENGAGE, F5, F5 [DESIGN], F5 Certified [DESIGN], F5 Networks, F5 SalesXchange [DESIGN], F5 Synthesis, f5 Synthesis, F5 Synthesis [DESIGN], F5 TechXchange [DESIGN], Fast Application Proxy, Fast Cache, FirePass, Global Traffic Manager, GTM, GUARDIAN, iApps, IBR, Intelligent Browser Referencing, Intelligent Compression, IPv6 Gateway, iControl, iHealth, iQuery, iRules, iRules OnDemand, iSession, L7 Rate Shaping, LC, Link Controller, Local Traffic Manager, LTM, LineRate, LineRate Systems [DESIGN], LROS, LTM, Message Security Manager, MSM, OneConnect, Packet Velocity, PEM, Policy Enforcement Manager, Protocol Security Manager, PSM, Real Traffic Policy Builder, SalesXchange, ScaleN, Signalling Delivery Controller, SDC, SSL Acceleration, software designed applications services, SDAC (except in Japan), StrongBox, SuperVIP, SYN Check, TCP Express, TDR, TechXchange, TMOS, TotALL, Traffic Management Operating System, Traffix Systems, Traffix Systems (DESIGN), Transparent Data Reduction, UNITY, VAULT, vCMP, VE F5 [DESIGN], Versafe, Versafe [DESIGN], VIPRION, Virtual Clustered Multiprocessing, WebSafe, and ZoneRunner, are trademarks or service marks of F5 Networks, Inc., in the U.S. and other countries, and may not be used without F5's express written consent.

All other product and company names herein may be trademarks of their respective owners.

---

## Technical Support

Support tools are available to help you answer your questions whenever and wherever you need help. From the documentation to the global technical community you can collaborate with on DevCentral, LineRate self-service tools help you solve issues quickly and proactively.

The [LineRate Support page](#) can help you find the resources you need.

## System Requirements

- [Overview](#)

- [Hardware Requirements for the VMWare vSphere Environment](#)

- [What's Next](#)

## Overview

The LineRate software does not require any specific software for installation. LineRate software includes the LineRate OS (LROS) and installs directly on a server as the primary operating system.

Below are the hardware requirements.

Minimum hardware requirements	Recommended hardware requirements
Intel® Westmere Class Processor, 2 sockets x 4 cores	Intel® Westmere Class Processor, 2 sockets x 6 cores
<p><b>1 Gigabit (functional, low performance):</b></p> <p>Intel 82576 NIC</p> <p>Intel 82574L NIC</p> <p>Broadcom 5716 NIC</p> <p><b>10 Gigabit (high performance):</b></p> <p>10 Gb Intel® 82599 NIC or 10 Gb Emulex BE3 NIC</p>	2 x 10 Gb Intel® 82599 NIC
<p>8 GB RAM (performance configuration)</p> <p>4+ GB available RAM (testing configuration. Memory usage depends on configuration and load.)</p>	24 GB RAM
64 GB locally attached hard disk	Locally attached hard disk, at least 40 GB larger than installed system RAM

---

## Hardware Requirements for the VMWare vSphere Environment

Below are the minimum required virtual resources.

<b>Disk space</b>	22 GB (The .ova file contains a sparse virtual disk image that can grow to 22 GB. The datastore should have 22 GB of available space.)
<b>Virtual CPUs</b>	Four
<b>Virtual RAM</b>	8 GB
<b>Interfaces</b>	Three

---

## What's Next

After making sure your hardware meets the requirements, you are ready to install the LineRate software. See [Installing LineRate](#).

---

## Installing LineRate

1. [Overview](#)
2. [Downloads](#)
3. [Installation Methods](#)

---

## Overview

This section provides a link to the LineRate download page and describes the methods available for installing LineRate software.

---

## Downloads

You can access downloads for the free LineRate trial with your DevCentral account. If you do not have a DevCentral account, you can create one when you go to the download page.



**Note:** For purchased licenses, you will receive a download link in an email.



### To download the software:

1. Go to <https://linerate.f5.com/downloads>.
2. Follow the steps on the page to create a DevCentral account or log in with an existing DevCentral account.
3. Download the file you need, based on your installation method.

---

## Installation Methods

You can install LineRate using any of the following methods. Continue the installation process by clicking the link for the method you want.

Installation type	Method	Click to continue
Bare metal	Local disk on dedicated server—Use dedicated hardware and install directly on the server.	<a href="#">Installing to a Local Disk on a Dedicated Server</a>
Bare metal	Diskless software deployment—Use Preboot eXecution Environment (PXE>) boot on one or more LineRate systems over your network.	<a href="#">Diskless Software Deployment</a>
VMWare vSphere	Use the vSphere Client to install on a virtual machine.	<a href="#">Installing on VMWare VSphere</a>

After you install, you are ready to [configure licensing](#).

---

## Installing to a Local Disk on a Dedicated Server

1. [Overview](#)
2. [Installation Options and Process Overview](#)
3. [Creating Installation Media](#)
4. [Configuring the Server's BIOS Settings](#)
5. [Configuring the Server to Boot from the Installation Drive](#)
6. [Installing the LineRate Software](#)
7. [What's Next?](#)

---

### Overview

This section walks you through the steps of installing LineRate software onto a commercial off-the-shelf server using the [downloaded](#) file. For the system requirements, see [System Requirements](#).

---

### Installation Options and Process Overview

You can install the LineRate software using one of two methods:

- DVD—Use this method with an internal or external DVD drive connected to the server. USB-connected and virtual DVD drives also use this method. The software image needed for this method is a ".iso.gz" file. Example: LROS-2.2.0-RC4-R-x64.iso.gz
- USB—Use with a hard drive or flash drive connected to a USB port or with a virtual USB. Be sure that your server supports using a USB drive as the system boot device. The software image needed for this method is a ".usb.gz" file. Example: LROS-2.2.0-RC4-R-x64.usb.gz



**Note:** During the installation process, you must select the drive to use for the software installation. The list of drives displayed may not give enough information to help you uniquely identify a drive. To ensure the software is installed on the disk you intend, you may want to remove all hard drives from the server, leaving just the one you want to use for the LineRate installation. Be sure that you know the size of the remaining hard drive, so you can distinguish it from any USB drives, which will also display in the list.

---



**Caution:** The LineRate software installation removes the operating system and all data from the hard drive where you install the software. Be sure that any data you need is backed up to another location.

---



**You must complete the following tasks to install the LineRate software:**

Create installation media

- Configure the server's BIOS settings.
- Configure the server to boot from the installation drive.
- Install the LineRate software.
  - Continue with [Configuring the Server's BIOS Settings](#).

---

## Creating Installation Media



**To create a DVD for installation:**

1. Unzip the [downloaded](#) .iso.gz file using **zip**, **gunzip**, or a similar utility, based on the operating system that you are using.
  - The zip file contains one large .iso file.
2. Use blank DVD media and DVD creation or "burning" software to put the unzipped .iso file onto the blank DVD.
  - For Mac users, you can use the built-in Disk Utility.
  - For Windows users, you can use a free utility like [ISO Recorder](#) or [Free ISO Burner](#). Note that the .iso file is a full disc image, so be certain to select the option in your DVD creation software to put a full disc image onto the DVD. Do not use the option to create a data disc.



**To create a USB drive for installation:**



**Caution:** The process of creating a bootable USB drive erases all data on the USB drive. Be sure that any important data on the USB drive is saved elsewhere before performing the steps below.

---

1. Unzip the [downloaded](#) .usb.gz file using **zip**, **gunzip**, or a similar utility based on the operating system that you are using.
  - The zip file contains one large .usb file.
2. Connect the USB drive to the PC.
  - The USB drive must have a capacity of at least 2 GB.
3. Select a disk utility that can copy the .usb file to the raw disk.

- The .usb file is a full disk image, including file system format and must be copied to the raw disk, replacing any filesystem that was previously on the USB disk.
  - For a PC running Apple MacOS or Linux, you can use the **dd** utility from the terminal command line.
  - For a PC running Microsoft Windows, you will need to find third party software to perform the copy of the .usb file to the raw disk.
4. Copy the .usb file from the PC onto the USB drive, using the disk utility such as **dd**.
- Continue with [Configuring the Server's BIOS Settings](#).

---

## Configuring the Server's BIOS Settings

The LineRate software requires specific BIOS settings on the server before you install the software. The names and locations of the BIOS settings may vary, but look for something similar to those described below.



### To configure the server's BIOS settings:

Connect a monitor and keyboard to the server.

- Power on the server and access the server's BIOS settings.
- If you see an option to optimize defaults, select that option.
- Enable simultaneous multithreading.
  - This may also be called hyperthreading. You may find it under **Advanced > Processor** settings.
- Disable nonuniform memory architecture (NUMA).
  - You may find it under **Advanced > ACPI Configuration** settings.
- Enable Intel AES-NI.
  - You may find it under **Advanced > Processor** settings.
- Enable Intel Turbo Mode technology.
  - This may also be called Turbo Boost Technology. You may find it under **Advanced > Processor** settings.
- Save the BIOS settings.
  - Stay in the BIOS and continue with [Configuring the Server to Boot from the Installation Drive](#).

---

## Configuring the Server to Boot from the Installation Drive

For the installation process, you must set your server to boot from the drive where you will place the installation image. You will change this option later.



### To configure the server to boot from the installation drive:

Insert the DVD into the DVD drive or attach the USB device to a USB port on the server.

- (Continuing from the previous section) From the server's BIOS, find and select the boot order option.
  - The boot order option may be in a boot-related menu or in an advanced options or other options menu.
- Change the boot order to put the installation drive type first.
  - Your installation drive will be either an internal DVD drive, a USB hard drive, or a USB flash drive.
- Save your changes.
- Exit the BIOS.
  - Continue with [Installing the LineRate Software](#).

---

## Installing the LineRate Software

After you configure the server's BIOS, you are ready to install the LineRate software.



**Caution:** The LineRate software installation removes the operating system and any data from the hard drive where you install the LineRate software. Be sure that any data you need is backed up to another location.



### To install the LineRate software:

1. Power on or reboot the server.
  - As the system restarts, the status of the initial setup displays until the installation options display.
2. From the Select an Option screen, select the **install** option and press **Enter**.
  - A list of all storage devices connected to the server displays in the Install on Device screen. The name of each device is based on the controller installed in the server.
3. Select the device where you want to install the LineRate software and press **Enter**.
4. From the Dumpdev size screen, enter the amount of disk space to use for the dump device and press **Enter**.
  - The dumpdev is a partition on the hard disk used to create a snapshot of the system in the event of a catastrophic system error. This snapshot can be used to diagnose the cause of the system error. The size of the dumpdev needs to be at least as large as the system memory. After installation, you cannot resize the dumpdev without reinstalling the system.
  - You can edit the default now, if needed. The default amount of disk space is the same as the amount of RAM currently installed in the server, which is typically the ideal setting. If you might increase the amount of RAM in this system in the future, you can increase the dumpdev size to be equal to the greatest amount of RAM that this server might have.
  - You should ensure that you have least 20 GB of remaining disk space available after subtracting the size of the dumpdev from the available disk space. Although you may lower the size of the dumpdev to less than the amount of system RAM, this is strongly discouraged. Lowering the size of the dumpdev too much may make diagnosing catastrophic system errors difficult, if one should occur.
  - Use M for MB and G for GB.

5. When prompted to commit the configuration, select **Yes** and press **Enter**.
  - The process takes about five minutes and displays progress information.
6. When you see the prompt to reboot, press **Enter**.
7. While the system reboots, remove the installation media.
8. Enter the system BIOS and set the server to boot first from the drive where you installed LineRate.
9. Save your BIOS changes.
10. Reboot the server.
  - When you see the login prompt, the installation is complete and successful.
  - If the server does not restart automatically, you may need to manually restart it.
  - If the restart fails, be sure to capture the information on the screen and [contact LineRate support](#).

---

## What's Next?

After you install, you are ready to [configure licensing](#).

---

## Diskless Software Deployment

1. [Overview](#)
2. [Required for Diskless Software Deployment](#)
3. [Configuring the Server's BIOS Settings](#)
4. [NFS Share](#)
5. [TFTP Service](#)
6. [DHCP Server Configuration](#)
7. [How LineRate Works When Using Diskless Software Deployment](#)
8. [What's Next?](#)

---

### Overview

Diskless software deployment lets you boot one or more LineRate systems over your network using the Preboot eXecution Environment (PXE), also called net boot.

The sections that follow describe the general process for configuring diskless software deployment for LineRate using the [downloaded](#) file. You must determine the implementation specifics based on your environment.

For the system requirements, see [System Requirements](#).

---

### Required for Diskless Software Deployment

The following are required for using diskless software deployment:

- Network interface on the server where you want to run LineRate that supports PXE booting
- LineRate diskless media, which is a tarball containing all of the files needed. Do not use the .iso or .usb installation files.
- BIO configuration
- Network File System (NFS) share
- Trivial File Transfer Protocol (TFTP) service
- DHCP server

The following sections describe environment setup requirements in more detail.

---

# Configuring the Server's BIOS Settings

The LineRate software requires specific BIOS settings on the server before you install the software. The names and locations of the BIOS settings may vary, but look for something similar to those described below.



## To configure the server's BIOS settings:

Connect a monitor and keyboard to the server.

- Power on the server and access the server's BIOS settings.
- If you see an option to optimize defaults, select that option.
- Enable simultaneous multithreading.
  - This may also be called hyperthreading. You may find it under **Advanced > Processor** settings.
- Disable nonuniform memory architecture (NUMA).
  - You may find it under **Advanced > ACPI Configuration** settings.
- Enable Intel AES-NI.
  - You may find it under **Advanced > Processor** settings.
- Enable Intel Turbo Mode technology.
  - This may also be called Turbo Boost Technology. You may find it under **Advanced > Processor** settings.
- Set the BIOS to only boot from the network.
- Save the BIOS settings.

---

## NFS Share

An NFS share provides the PXE client with both the operating system kernel program and a root file system, which makes up the rest of LineRate system. The system uses NFS version 2.0 and does not require a writable export point.

The exact configuration of the NFS service is unique to your environment. The only requirement is that the root of the installation tree be an export point. This can have implications, because some NFS implementations require all export points be explicitly exported and prevent subtrees of an export point from being mounted by a client. In these scenarios, each version of LineRate will need an explicitly configured export point, rather than a parent tree being exported alone. Refer to your NFS vendor documentation to see if this applies to your NFS service implementation.

Extract the LineRate distribution file (tarball) using your favorite archive tool into a location that you will be serving it from. After extraction, you can move or rename the top-level directory. Be sure to retain the file mode bits during extraction.

After the extraction is complete, make the top-level directory an export point within the NFS configuration. Use the resulting path in the Root Path DHCP option described in the previous section. For example, if your NFS server has an IP address of 10.0.1.100, and the LineRate distribution was extracted and exported to `/srv/nfs/lros_v2.0`, your DHCP redirection service would be configured to set the DHCP Root Path option to:

```
10.0.1.100:/srv/nfs/lros_v2.0
```

The export point configuration using Linux's kernel based NFS server might look like something:

```
# /etc/exports  
  
#  
  
/srv/nfs/lros_v2.0    *(ro,all_squash)
```

Notice that the export point does not need to be writable or have any UID/GID mapping configured for LineRate to operate correctly.

---

## TFTP Service

The diskless deployment requires a TFTP service running on the standard TFTP port (UDP port 69). The IP address of this service must be in the PXE-specific DHCP options provided by the DHCP redirection service and can reside alongside any combination of the other services or an entirely independent machine. However, unlike the NFS service, it must not require access via a gateway (router) and be must present on the same subnet as the client itself.

The exact configuration of the TFTP service is dependent on your environment. Refer to your TFTP vendor documentation. You can use any standards-compliant (RFC 1350) TFTP service for the diskless software deployment.

After configuring the NFS service, copy the file called `lros.pxe` (found in the extracted `boot` subdirectory) to the root of your TFTP server. We recommend giving the file a new name that includes the LineRate version, for example, `lros_v2.0.pxe`. This is the boot file that you configure in the DHCP settings.

---

## DHCP Server Configuration

Booting a LineRate system over a network requires a DHCP server that can provide PXE-specific options to a PXE-enabled client system. You can configure the DHCP server using one of the following methods:

- Combined DHCP/redirection service—Replace or configure existing DHCP services to provide both the standard DHCP OFFER with client IP address for all clients and PXE extension tags for clients that are PXE enabled.

- Separate DHCP/redirection services—Add PXE-enabled DHCP services to the existing DHCP infrastructure. These services, known as DHCP Proxies, only respond to PXE-enabled clients and only provide redirection extensions in the DHCP message.
  - You can use either separate servers or reuse the servers running the standard DHCP services. The latter requires the Proxy service to listen on port 4011, because the existing DHCP service is already bound to the standard DHCP port (UDP port 67). The standard DHCP service needs to reply to PXE-enabled clients with option 60 set to a value of `PXEClient` to indicate to the client to follow up with an interrogation on port 4011.
  - The IP-granting DHCP service need only provide the Class Identifier option with the `SIAddr` field set to the redirection server. The DHCP redirection service can use of the UUID to distinguish between clients and to conditionally provide different PXE options.

How you configure the DHCP service depends on both the method and the DHCP service implementation. Since there is no single standard configuration format between DHCP service vendors, refer to the documentation for your DHCP service for configuration specifics.

Unless otherwise stated, all DHCP options, header fields, and protocol states conform to the standard DHCP specifications.

The DHCP OFFER from the redirection service is expected to set the header fields accordingly and contain the following PXE-specific tags:

Setting (option number, if applicable)	Description
SIAddr	<ul style="list-style-type: none"> <li>• SIAddr (proxy DHCP server)—If using a DHCP proxy server, it should respond with this field set to the IP address of the boot server.</li> <li>• SIAddr (Boot DHCP server)—The boot DHCP server should respond with the IP address of the NFS server in this field, if it will not be included in the Root Path value.</li> </ul>
SName or TFTP Server (66)	IP address or host name of the TFTP server. <ul style="list-style-type: none"> <li>• SName—Use this field if <i>not</i> using Option Overloading.</li> <li>• TFTP Server—Use this field if using Option Overloading.</li> </ul>
Bootfile or Bootfile Name (67)	Path from the TFTP root to the boot file on the TFTP server. <ul style="list-style-type: none"> <li>• Bootfile—Use this field if <i>not</i> using Option Overloading.</li> <li>• Bootfile Name—Use this field if using Option Overloading.</li> </ul>

Setting (option number, if applicable)	Description
Root Path (17)	<p>Path to the top-level directory of the NFS share, in the format:  <code>ip_address:/top-level_directory_of_NFS_share</code></p> <p>For example:</p> <p><code>10.0.1.100:/srv/nfs/lros_v2.0</code></p> <p>If the IP address of the NFS server is given in SIAddr, then use only the path.  For example:</p> <p><code>/srv/nfs/lros_v2.0</code></p>
Class Identifier (60)	<p>Boot DHCP server should return this exact string:  PXEClient</p>
Router (3)	<p>Optional. Use only if the NFS server is on a different subnet from the LineRate and TFTP servers.</p>

---

## How LineRate Works When Using Diskless Software Deployment

For most functions, LineRate works the same when using diskless software deployment as it does for regular disk installations. A few functions operate differently:

- If you make configuration changes, you can save them using the `write` command. However, the changes will not be retained when you next reboot the system.
- When backing up the system, you must send the backup to a network location, not a local directory.
- You can use the `copy` command to copy files. However, the files will not be retained in the new location when you next reboot the system.
- The `upgrade` command is not available. To upgrade to a new version, you must extract a new tarball with the upgraded version to the NFS server and make any required DHCP configuration changes.
- When you use the `show version` command, the system includes the PXE boot information:

```
PXE Boot Info:
Root Path: nfs://10.1.1.2/boot/bootsystem
PXE Path: tftp://10.1.1.2/pxebooters/bootsystem
```

---

## What's Next?

After you install, you are ready to [configure licensing](#).

---

## Installing on VMWare vSphere

1. [Overview](#)
2. [Default Settings](#)
3. [Installing on vSphere](#)
4. [Assigning a Static IP Address to the Management Interface](#)
5. [Configuring vSwitches and Hosts to Permit CARP and Failover](#)
6. [Editing the VM Settings](#)
7. [What's Next?](#)

---

## Overview

You can install LineRate as a guest your VMWare vSphere environment using the [downloaded](#) .ova file. For the minimum required virtual resources, see [System Requirements](#).

---

## Default Settings

The default settings configured in the .ova file are:

- Virtual CPUs - Four
- Virtual RAM - 8 GB
- Interfaces - Three (one for management and two for the data path)
  - The management interface (em0) is configured to acquire an IP address from a DHCP server.

You can change these settings, but these are the minimum supported requirements for a production system. For functional testing, 2 Virtual CPUs and 4 GB RAM may suffice, but performance will suffer at higher traffic loads.

---

## Installing on vSphere

After downloading the .ova file, you can install from the vSphere Client. For more detailed installation information, see the [VMWare documentation](#).

The .ova file has three networks defined:

- Management—Bound to interface em0.
- Network A—Bound to interface em1.
- Network B—Bound to interface em2.

During installation, you must attach each of these interfaces to a network. Networks A and B are interfaces dedicated to the data path. For example, in the case of configuring a proxy, the Network A might correspond to the external network and Network B to an internal network, or vice versa.



### To install on vSphere:

1. From the vSphere Client, select **File > Deploy OVF Template**.
2. Enter a URL to download the .ova file or click **Browse** to select the downloaded file and click **Next**.
3. Verify the template details and click **Next**.
4. Enter a name for the deployment, select a location, and click **Next**.
5. Select the host or cluster for the deployment and click **Next**.
6. Select a datastore for the virtual machine files and click **Next**.
  - The .ova file contains a sparse virtual disk image that can grow to 22 GB. The datastore should have 22 GB of available space.
7. Select the type of provisioning and click **Next**.
8. For the three network interfaces listed in Source Networks, assign the Destination Networks to use and click **Next**.
  - We recommend assigning your management network to the Management interface and assigning one of the other interfaces to your external network and the other to your internal network.
9. Verify the options and click **Finish**.
10. Power on the virtual machine.

---

## Assigning a Static IP Address to the Management Interface

The network interface designated as the Management interface (em0) is configured to acquire its IP address from a DHCP server. If this is the configuration you want, you do not need to do anything else. You can ssh to the VM instance on the network you assigned to the interface and log in using the default credentials. See [Logging In](#).

If there is no DHCP server on the network assigned to the Management interface, you must assign a static IP.



### To assign a static IP address to em0:

1. Select the VM where LineRate is installed.
2. Click the **Console** tab.
3. Log in as admin.
  - See [Logging In](#).
4. Use the following commands to set the static IP address:

```
config
interface em0
ip address <ip_address> <netmask>
no ip address <DHCP_assigned_addr> <netmask>
```

5. Write the configuration:

```
write
```

Continue with the rest of the configuration either in the vSphere Client console or by using ssh to access the Management interface.

Keep in mind that until you assign a Static IP address and write the configuration, the management interface may switch to different IP addresses, for instance if you move the host machine to a different network or restart the VM.

---

## Configuring vSwitches and Hosts to Permit CARP and Failover

If you plan to use [CARP](#), you must change the vSwitch and host settings in the vSphere Client:

- For each vSwitch that your LineRate installation is attached to, you must change the vSwitch security settings (edit vSwitch properties) to accept Promiscuous Mode, MAC Address Changes, and Forged Transmits.
- For each vSphere host where LineRate is installed, you must set the Net.ReversePathFwdCheckPromisc (Advanced Settings > Net) to 1.

---

## Editing the VM Settings

If needed, you can edit the default settings (right-click the virtual machine and select **Edit Settings**) to increase the CPUs, RAM, or network interfaces, depending on the resources available in vSphere.

The default settings are the minimum requirements.

---

## What's Next?

After you install, you are ready to [configure licensing](#).

---

## Accessing the the LineRate CLI

1. [Overview](#)
2. [Accessing the CLI](#)
  - 2.1. [Using a Serial Connection](#)
3. [Logging in to the CLI](#)

---

### Overview

You can access the LineRate CLI to configure and manage the system several ways. You can also use the REST API to configure and manage the system. For more information about using the REST API, see [Accessing the REST Server](#).

---

### Accessing the CLI

You can access the CLI in the following ways:

- Using SSH. See [Configuring Management Interfaces](#).
- Using a serial connection. See [Using a Serial Connection](#).
- Directly using a monitor and keyboard connected to the system.

---

### Using a Serial Connection

You can access the system to use the CLI using two COM ports: COM1 and COM2. The specific procedure for connecting to the serial interfaces depends on the mechanism you use (for example, terminal server, IPMI Serial Over LAN, usb-to-serial, etc.).

By default, the system sends boot messages to COM1.

Use the following settings from the remote system to access the COM ports.

<b>Baud rate</b>	115200
<b>Data bits</b>	8
<b>Parity bit</b>	None
<b>Stop bit</b>	1

<b>Flow control</b>	None
---------------------	------

---

## Logging in to the CLI

You must log in to the LineRate software to configure and manage your server.

Use the default settings the first time:

- Login—admin
- Password—changeme

We highly recommend that you change the password for the admin login, after you have logged in.



### To change the admin password:

1. Enter configuration mode by typing:  
`configure`
2. Type:  
`username admin secret "<password>"`
  - Use the double quotes if the password contains non-alphanumeric characters.
3. Save your changes by typing:  
`write`

---

## Configuring Licensing

1. [Overview](#)
2. [Enabling a Free Trial License](#)
3. [Enabling a Purchased License](#)
4. [Confirming the License](#)
5. [What's Next](#)

---

### Overview

This section describes how to configure licensing. After you install LineRate, you can configure the system. To run traffic on the system, you must enable licensing.

---

### Enabling a Free Trial License

A free trial license permits up to the following limits:

- 180 HTTP requests per minute sustained, 360 per minute burst
- 60 TCP connections per minute sustained, 120 per minute burst
- 5 Mb per second (bandwidth)

For information about how the limits work, see [Licensing Mode Commands](#).

To acquire a free trial license, the system must be connected to the Internet and will use the phone home feature to send usage and configuration data to F5.

You must configure the following:

- IP address on an interface
- Default route to reach the Internet
- Phone home configuration with a DevCentral username and password

You should not need to configure DNS, because the system defaults will work in most cases. For information about configuring DNS, see [IP Mode Commands](#).

If you have already configured the free trial license, but something is not working properly, see [Troubleshooting Licensing](#).



**To enable a free trial license:**

1. If you created an account on devcentral.F5.com to download LineRate, you can go to the next step. If you don't have an account, go to this site and register for an account: <https://devcentral.f5.com/> and click **Sign Up**.

2. Log in to LineRate.

3. To see the names of the interfaces, type:  
**show interfaces**

- A list of all interfaces on the system displays. It is possible for the system to have an interface that LineRate cannot detect.
- The first line is the interface name and its status. The interface name is based on the driver for the interface type. The remaining lines list the information available about the interface (typically, manufacturer, model, MAC address, speed in kilobits, and more).
- Below are the names used for some common interfaces:
  - em—Intel 1Gb interface
  - igb—Intel 1Gb interface
  - bce—Broadcom 1Gb interface
  - ix—Intel 10 Gb interface
  - oce—Emulex 10 Gb interface
  - lo—Loopback interface (internal interface)
  - po—Port channel interface

4. Use the following commands:

```
config
ip route 0.0.0.0/0 <default_gateway_IP>
```

```
interface <interface_name>
  ip address <ip_address>
```

```
phone-home
userid "<F5_username>" secret "<password>"
```

- Once configured, the system accesses the phone home server using your DevCentral credentials and automatically installs the license. If you need help with your DevCentral credentials, go to <https://devcentral.f5.com/login> to retrieve your username or password. For more information about what phone home does, see [Phone Home Mode Commands](#).
- We recommend that you check network connectivity after configuring your default route and IP address to ensure that phone home works properly. Using bash mode, you can use ping or telnet to make sure you can both resolve and reach ihealth.f5.com and askf5.com before configuring phone home. See [Bash Mode Commands](#) for instructions on using system tools available in the bash shell.

---

## Enabling a Purchased License

To purchase a license, send an email to [linerate-sales@f5.com](mailto:linerate-sales@f5.com) or call 1.855.LINERATE (1.855.546.3728).

If you purchased a license for LineRate, you must provide information to identify the hardware, then you will receive the license file and the X.509 signing certificate in an email. You must install both files.

The rate limits for HTTP requests, TCP connections, and Mb per second are based on the license you purchased.

Currently, the only feature you can license is called base. For information about how the limits work, see [Licensing Mode Commands](#).



### To enable a purchased license:

1. Log in to LineRate and use the following command to get the information needed for the license:

```
show licensing host-id
```

- The output will look similar to the following:

```
31273436-3033-5955-4631-34254B39584C
```

2. Send the host ID to [sales@linratesystems.com](mailto:sales@linratesystems.com).
  - You will receive an email with the download link for the license and installations files.
3. Log in to LineRate.
4. Use `scp` to copy the license file to the LineRate system.
5. Use the following command to install the license.

```
license install base <uri>
```

- URI of the JSON-formatted license file to install. System supports `file://` protocol. If the protocol prefix is not given, start the URI with a `/` for an absolute path and start without a `/` for a relative path from `/home/linerate`. A maximum file size of 100 kB is enforced. Protect URIs with quotes (for example, `"file:///home/linerate/license"`, or just `"license"`)

---

## Confirming the License

To confirm that the license is enabled, use the `show licensing brief` command. This command shows your license and status or a warning if the license was not enabled. It also shows the expiration date and the applicable limits.

---

## What's Next

You are now ready to [configure the management access to the system](#). You may want to review [Using the Command Line Interface](#) to become familiar with the LineRate command line interface (CLI) and [Working with Bases](#).

---

## Using the Command Line Interface

1. [Overview](#)
2. [Getting CLI Help](#)
3. [Command Completion](#)
4. [Running Config and Startup Config](#)
  - 4.1. [Comparing Running Config and Startup Config](#)
  - 4.2. [Saving to the Startup Config](#)
5. [Command Line Modes](#)
6. [Command History](#)
7. [Single-value vs. Multiple-value Commands](#)
8. [Using the Pager](#)
9. [What's Next](#)

---

## Overview

The following sections describe the basics of using the LineRate command line interface (CLI). If you are an experienced user of other networking device CLIs, such as Cisco IOS<sup>®</sup>, you should find that the LineRate CLI works very similarly to those devices.

---

## Getting CLI Help

At any point in the CLI, you can display help for the available commands by typing the question mark (?) or the **Tab** key. The table below explains how to use these two keys.

Help example	Result
?	List of available commands.
s?	List of available commands that start with the letter s.
c <b>Tab</b>	System either completes the command that begins with the letter c (if there is only one) or lists all available commands that start with c.
<command> ?	List of available options for the command.

Some commands have options that are less frequently used and are considered advanced options. The advanced options do not display in the help when you first type the question mark. But if advanced options are available, typing question mark will display the non-advanced options along with the message, "Advanced options are also available. Press ? again for list." Typing question mark again will display all options, including the advanced options.

---

## Command Completion

The individual words that make up a command do not have to be typed out fully. The system will accept partial words as long as each word has enough characters to be uniquely identified. So the commands `show running-config brief` and `sh run b` will both be accepted by the system and produce the same result. Note that newer versions of the LineRate software will often add more commands, options, and keywords and will occasionally deprecate commands or options. So it is possible that a command with partial keywords may be unique on one version of the LineRate software, but ambiguous on a different version.

In addition to accepting partial commands, the system also accepts partial object names. For example, if you have just one real server and its name is `rsweb1`, you can go into configuration mode for that real server using `real-server rTab`. The system autocompletes the `rTab` as `rsweb1`.

If you have multiple real servers configured with the names `rsweb1`, `rsweb2`, and `rsweb3`, typing `real-server rTab` results in a list of the existing real servers with names that start with the letter `r`.

---

## Running Config and Startup Config

Changes you make to the configuration of the LineRate software take effect immediately. The LineRate software has two configurations:

- Running config—The configuration you are currently running, including changes you have made since you last saved the configuration. The system has a default running config that it runs if it cannot find a startup config. The current running config can be displayed with the command `show running-config`.
- Startup config—The saved configuration that the system will use when you next restart the LineRate software. The startup config can be displayed with the command `show startup-config`.

---

## Comparing Running Config and Startup Config

As you make changes to your configuration, you may want to compare the current running config to the saved startup config to determine what has changed since you last saved the configuration.



**To compare the running config and the startup config:**

- Type:  
`show running-config diffs`
  - Lines with a - show they were removed from the startup config.
  - Lines with a + show they were added to the running config.
  - Lines with no - or + show the context of the changed lines.

---

## Saving to the Startup Config

When you have made configuration changes that you want in the startup config, you must save them.



### To save the startup config:

- Type:  
`write`

This saves all changes currently in the running config to the startup config.

---

## Command Line Modes

The CLI has multiple modes. The mode you are currently in is always reflected in the prompt. When you first log in to the system, you are in exec mode. Commands available in exec mode do not change the running configuration, but do take effect immediately. The prompt for exec mode is simply the hostname followed by a hash sign:

```
LROS#
```

Exec mode commands are always available, regardless of what mode you are in. For example, you can use the show or write commands, shown in the sections above, at any time.



### To change from exec mode to config mode:

- Type:  
`configure`

As you enter commands to change the configuration, the mode changes based on the command you last entered. Each mode has a specific set of commands available. The modes stack, and the prompt changes to show the mode you are in.

For example, the prompt below shows that you are in configure real-server mode for the real-server called rs1:

```
LROS(config-rserver:rs1)#
```



### To change from any config mode to exec mode:

- Do one of the following:
  - Type:  
`end`
  - Press **Ctrl+z**.

If you are further down the config mode stack, you can move one level up the mode stack.



### To change from the current config mode to the mode one level up:

- Type:  
`exit`

## Command History

You can access the history of commands you have entered in the following ways.

History example	Result
Up or down arrow key	Scrolls through the list of previously used commands.
<b>Ctrl+r</b> <phrase>	Searches backwards for and lists any used command that contains with the sequence of characters <phrase>. Pressing Ctrl-r again continues the search backward, finding the next command that contains <phrase>.

## Single-value vs. Multiple-value Commands

CLI command are generally one of the following types:

- Single-value—The command accepts only one value and replaces the existing value with the last value set. For example, when setting the base for any object, the object can have only one direct base. If you set the base again, the new base **replaces** the previous one.

The following commands first create the real server called rs1, then set it to use the base called base1.

```
real-server rs1
base base1
```

The following command, when already in real server config mode for rs1, replaces the base that rs1 uses to be base2. The previous base (base1) is no longer applicable to rs1.

```
base base2
```

- Multiple-value—The command accepts multiple values and either creates a new object with the value or puts you into configuration mode for an existing value. For example, when creating real servers, you can create and name as many real servers as you need. Each time you use the **real-server** command and follow it with a word, the system **creates** a real server with the word as its name. If a real-server with the name exists, the system puts you into **configuration mode** for that real server.

The following command creates a real server named rs1.

```
real-server rs1
```

The following command creates a real server named rs2

```
real-server rs2
```

The following command puts you into configuration mode for the existing real server called rs1.

```
real-server rs1
```

---

## Using the Pager

Some CLI commands cause the system to respond with more output than fits on a single terminal screen. When this happens, the system will only output a single page of text, then pause and display the prompt **--More--**. From this prompt, you can perform the following actions:

Command	Result
<space>	Outputs the next page of text. If the full output has been displayed, returns to the normal system prompt.
b	Goes back one page of text, outputting the previous page.
Up arrow key	Scrolls backward one line at a time.
Down arrow key	Scrolls forward one line at a time.
q	Quits displaying output and returns you to the normal prompt.
/ <b>&lt;searchphrase&gt;</b>	Searches forward through the output. To search forward through the output, enter a slash character, followed by the phrase you want to search for, then press <b>Enter</b> .

Command	Result
?<searchphrase>	Search backward through the output.
n	Repeats the last search.
h	Displays additional help on the pager. Press <b>q</b> when done viewing the help message.

---

## What's Next

For information about configuring interfaces, see [Working with Base](#)

---

## Working with Bases

1. [Overview](#)
2. [Using Bases \(Templates\)](#)
  - 2.1. [Inheritance](#)
  - 2.2. [Finding the Where a Parameter's Value Is Set](#)
3. [What's Next](#)

---

### Overview

A "base" in LineRate is a type of template that allows you to reuse common portions of configuration across multiple objects. Each base can inherit from another base, overriding properties from that base. This lets you create basic configurations that you can reuse and build upon.

---

### Using Bases (Templates)

You can create a base for the following objects:

- Real server
- Virtual IP
- SSL profile



**Best Practice:** A best practice is to create the most basic base for each object type that includes all settings common to an object. You may also want to create a second tier of bases that inherit settings from the basic base and then add settings for variations you need.

Throughout this guide, when we create an object that can have a base, we go through creating an example base. For an example of how to create a base, see [Creating a Real Server Base](#).

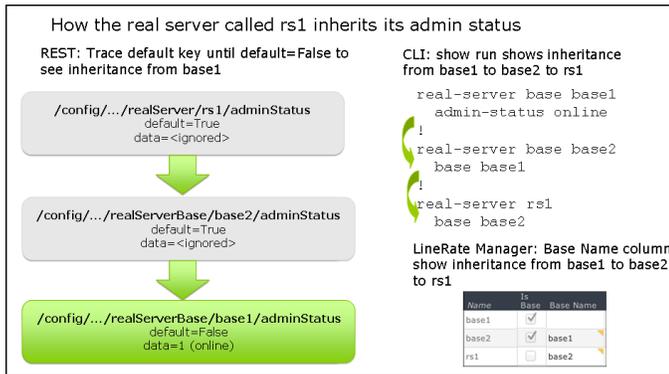
---

### Inheritance

Bases can inherit properties from another base. The object takes its values from the most specific configuration. For example, an object looks for its settings as follows:

1. Its own settings
2. The base it is configured to inherit from
3. The base that its base is configured to inherit from

The diagram below shows how a real server inherits its admin status in the REST API, the CLI, and LineRate Manager. Here, we use the /config tree in REST.

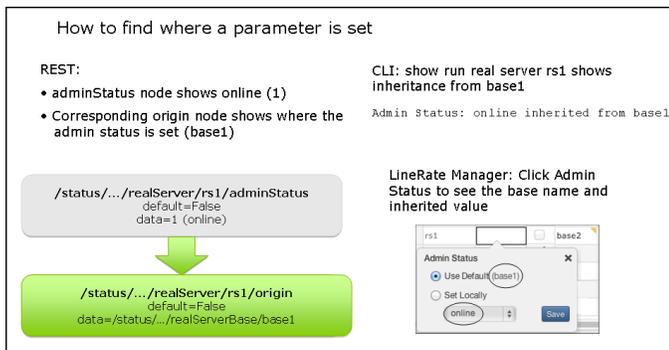


For information about how to temporarily override the base for a setting, then return to inheriting from the base, see

- CLI— [no command usage for objects with a base](#)
- REST— [Changing Configurations Locally, Then Back to the Base](#)

## Finding the Where a Parameter's Value Is Set

You can see where an object is getting its configuration using the CLI show command or the the REST origin node associated with an object, as shown in the diagram below. Here, we use the /status tree in REST.



**To see where a real server is getting its configuration:**

- In the CLI, type:  
**show real-server <real server name>**

```

example_host# show real-server rs1
show real-server rs1
  Configuration
  Address:                               10.1.2.101:80 set locally
  
```

Admin Status:	online	inherited from base1
Max. Connections:	0	default
TCP Options:	<none>	default
...		

---

## What's Next

For information about configuring interfaces, see [Configuring Management Interfaces](#).

---

## Configuring Management Interfaces

1. [Overview](#)
2. [Configuring the Host Name](#)
3. [Configuring the Management Interface](#)
4. [Configuring SSH](#)
5. [Management Access Example](#)
6. [What's Next](#)

---

### Overview

An initial, basic configuration includes the following key functions:

- Configuring the host name
- Configuring the management interface
- Configuring SSH

---

### Configuring the Host Name

You should first configure a host name for the system. The default host name is LROS.

For this example, we are naming the host `example_host`.



**To configure the host name:**

1. Type:  
`configure`
2. Type:  
`hostname example-host`
  - The prompt will change to reflect the new host name.
3. To check the host name setting, type:  
`show run`  
`hostname example-host`
4. Type:  
`write`

---

### Configuring the Management Interface

You must assign an IP address to an interface to use for management.

LineRate supports both IPv4 and IPv6. You can specify the IP address and subnet mask in any of the following formats:

- `192.0.2.1/24`— example of an IPv4 address with a 24-bit subnet mask using CIDR notation.
- `192.0.2.1 255.255.255.0`—equivalent to above using net mask notation.
- `2001:DB8::/64`—example of an IPv6 address with a 64 bit subnet mask using CIDR notation.

If you need more information about IP addresses and subnet masks, see these sites for more information:

- [http://en.wikipedia.org/wiki/IP\\_address](http://en.wikipedia.org/wiki/IP_address)
- [http://en.wikipedia.org/wiki/CIDR\\_notation](http://en.wikipedia.org/wiki/CIDR_notation)

In this example, we are configuring one management interface as shown in the diagram in [Configuring Load Balancing](#):

- Management (on em0)—`10.200.0.1/24`



**Note:** If you installed using VMWare and have [configured the management interface to use a static IP address](#), you can skip this section. Your management interface is already configured.

---



### To configure the management interface:

1. Type:  
`show interfaces`
  - A list of all interfaces on the system displays. It is possible for the system to have an interface that LineRate cannot detect.
  - The first line is the interface name and its status. The interface name is based on the driver for the interface type. The remaining lines list the information available about the interface (typically, manufacturer, model, MAC address, speed in kilobits, and more).
  - Below are the names used for some common interfaces:
    - em—Intel 1Gb interface
    - igb—Intel 1Gb interface
    - bce—Broadcom 1Gb interface
    - ix—Intel 10 Gb interface
    - oce—Emulex 10 Gb interface
    - lo—Loopback interface (internal interface)
    - po—Port channel interface
2. Type:  
`configure`
3. Type:  
`interface em0`
4. Type:  
`ip address 10.200.0.1/24`

5. To check the interface settings, type:  
**show interfaces**  
em0 is up, line protocol is up  
Hardware is Intel82540EM, address is 0800.279e.0b3a  
Internet address is 10.200.0.1/24, broadcast is 10.200.0.255  
...
6. Type:  
**write**

---

## Configuring SSH

You should also configure secure shell (SSH) to permit access to the system using SSH.

By default, when the LineRate is first installed, SSH is automatically configured to allow incoming connections from any SSH client and to allow incoming connections to any IP address configured on the system on TCP port 22. Although this is convenient for first connecting to and configuring the system, best security practices are to limit SSH connections to only those networks and IP addresses where access is required. So you should remove the automatic settings and replace them with settings that limit access. Typically, you want to allow access only from your management network. You can allow from more than one management network, if needed.



**Caution:** If you are currently logged into the system via SSH, you may disconnect yourself by changing the allow to or allow from settings if your current connection would no longer be allowed under the new settings. In order to avoid this, you may need to first add additional allow to or allow from lines, possibly make a new connection to the system, using a connection that will be allowed with the new settings, then remove any unwanted allow to or allow from lines.

---

In this example, we first add the setting for allowing incoming connections from hosts on the 10.200.0.0/24 management subnet and also add the setting to allow incoming connections to only the management IP address. We then remove both of the "any" settings that were added automatically.



### To configure SSH:

1. Type:  
**configure**
2. Type:  
**ssh**
3. Type:  
**allow from 10.200.0.0/24**
4. Type:  
**no allow from any**

5. Type:  
`allow to 10.200.0.1 22`
6. Type:  
`no allow to any`
7. To check the SSH settings, type:  
`show run`

```
...
ssh
  allow from 10.200.0.0/24
  allow to 10.200.0.1 22
...
```

7. Type:  
`write`

---

## Management Access Example

After configuring management access as described above, you can use the `show run` command to see the configuration. We have annotated the example command output below. Comment lines start with an exclamation mark (!).

```
LROS(config)# show run
Building configuration...

!
! Hostname setting.
!
hostname example-host
!
! Default user name and encrypted password.
!
username admin secret encrypted "$2a$04$7TYufYOKVQ8i8bblVtZ1ierxZXzcH5mR/
QeaZH8WnWRzVEkPt0MgS" uid 2000
!
! IP address configured on the interface called em0 for management access.
!
interface em0
  ip address 10.200.0.1 255.255.255.0
!
! IP address configured on the interface called em1 for data.
!
! Default SSL configuration. See Configuring SSL.
!
ssl profile self-signed
  attach primary-certificate self-signed
```

```

attach private-key self-signed
!
! SSH configuration to limit access to the LineRate system.
!
ssh
  allow from 10.200.0.0/24
  allow to 10.200.0.1 22
!
! Default REST server configuration.
!
rest-server
  allow from any
  allow to any 8443
  attach ssl profile self-signed
!
! Default certificate and key called self-signed. For information about
certificates, see Configuring SSL.
!
certificate self-signed
  pem-format
  -----BEGIN CERTIFICATE-----
MIIDOjCCAiKgAwIBAgIJAPm1YLOdNan3MA0GCSqGSIB3DQEBBQUAMBwxGjAYBgNV
BAMTEWxyb3MtZGVmYXVsdClOb3N0MCAXDTEyMDMyNzEwMDczN1oYDzIyODYwMTEw
MTAwNzM3WjAcMRowGAYDVQQDExFscm9zLWRLZmFlbHQtaG9zdDCCASIWdQYJKoZI
hvcNAQEBAQADggEPAADCCAQoCggEBAL4QCxbazhzBnPW4GHBQebKWRVax9khfPpWp
+YbJztXolweTcXHvRuhEsmTkvdDdTtkgoWgdOvGBPblrYiBXivkNo9eC6oBkzuW0T
gY6XjR6p4AFSMkRDh3RCIfxC2s7lSANjYe15BkcibMeak6/4BxFIF12XNQxjR64Z
pJ5NM8ygc4SM8dkB7kUe5FTg4xEi+DR9/TZqZ1y/3lTa+atW/On7nLcgB7z/mlhk
mp8NCdw4xzNCbIJdX5WG1dbIbFD8uOsPoHyoGUtdYJ9exDCuAgX3xRU5L187fT3x
WUz5xw13zZ7NrrAaCG8h6ugfLNKPkxi28tL+TNZHzDPFbyeNiMUCAwEAAAn9MHsw
HQYDVR0OBBYEFO61P0Y4qwK3WC20wP2kDNbZ8X18MEwGA1UdIwRFMEoAFO61P0Y4
qwK3WC20wP2kDNbZ8X18oSCkhjAcMRowGAYDVQQDExFscm9zLWRLZmFlbHQtaG9z
dIIJAPm1YLOdNan3MAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEFBQADggEBAHUm
y8HavCdrjabf2Ajs1TX87zeZmR0RYkezL/feZ+xri+DDHal+uJMu0DUppPoR0YyI
jorz6t79uq1DT8jGCalLjjiCvr6E2Sz0cXJ2aKE45eu4GMuMz/ohczm0LyexP01J
gqfp8Q5cvr/xQik8eLpxgCIjZ0188e8OQRNetwgzbi579bjkKglLCJfjQZE9ot14
0Pmz5DG1QtCC1OA0Ppdz7y+P1PLNwpRxKN0cjl6fH1P9qeZvBoDPp6X72nMEOkn1
eT2JxS0Vofyp9rDlGVusuP1EFzM/BCh/dHq4SMmHuQqgc/dzCJruLrztj/hgGXKk
PK7/nxRt+C72hde2OaU=
  -----END CERTIFICATE-----
quit
!
key self-signed
  pem-format
  -----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAvhALFtrOHMGc9bgYcFB5spZFVrH2SF8+lan5hsn01ejXB5Nx
ce9G6ESyZOS8N0lOSChaB068YE9uWtiIFeK+Q2j14LqgGT05bROBjpeNHqngAVIy
REOHdEih/ELazuVIA2Nh7XkGRyJxs5qTr/gHEUgXXZc1DGNHrhmkknk0zzKBzhIzx

```

```
2QHURR7kVODjESL4NH39NmpnXL/eVNr5q1b86fuctyAHvP+bWGSanw0J3DjHM0Js
gl1flYbV1shsUPy46w+gfKgZS11gn17EMK4CBffFFTkuXzt9PfFZTPnHDXfNns2u
sBoIbyHq6B8s0o+TGLby0v5M1kfMM8VvJ42IxQIDAQABAoIBAGXakSbJUWWFuIjS
BH7EEcPL1hLUwggcypxH/8nlAmwOIJYVxNjrAtPcZMG+9sKmDUaMIVsDLd5rEteq
bJtV7OKRMBsjyEJZPsieiHKS8vR40uvCUd/VVJTQEAhxB3OS2dm++67Yia27XBJH
21eVEqyHNsZYDvy5g6NgaKDQ/K5ubCfPkXji9OKfT8AGFR6kKPraloG1w+YUR8qh
F7H4o9yo+Adr0un2QZOKowG7mwmTE7L4a4nIfS09sFeNKYDW0hohp2qrX6HY/HJd
2iy1SuUUzfWGuqYVwAUQKz9UvuqezK2H3xnP/S//gDUWJZ+lXmMKx38j+gFxbld
RxRcxs0CgYEA9xXNtlvEqg17vfm+vh841oV3MTypYpCq3RRND+yqwyZdAdzaie4Z
nEt1H7V/ry5HmaH4XTXKer3X3SWJIdbZeNXmcZnatZi2XqVmhhmCMR0rHXuwa4GA
qMlCwOwZS1N2tJxGwmkHC51Gy6J21TL68PQIafeAYrBl3zW330W+I78CgYEAxOuN
gODEx4/8pHvgjlq+w1gbA5oXDCGTD1Y0Kt9RcPgwjnkQtW7KY3slGDrfPdIWfSRj
tNNTsqUA4cfxF9yWykFC+aiFufn6lutHrq5SUAc/heoatvL7XAMlVQnHltqYinZL
rDOat7wkby2WIQPzbXK0ojWcVLf5DND/E0y0pHsCgYAgjyL4cMdNkVFJC2vzKbIP
Q68dMd0w09gIIfc1tH4cESYYZL33hwSg7+CTORuGPhb5S7qqrbszK9xWMz1RKaL
ocQoHBoR6/m8JxeHfD0Hs8xGqlHbZG1L1JmTSolav7jYu+8nFyfyg1Qs6U+3cGxY
7A9fx1mHp68E5tM//LS9iQKBgQCEWtJcKjb47wVfRMfUxpdqpq9Zh2swQyzFORmN
K1Zg+OaiEqsxv0r+/FkdZQyBT8C/0gKWGmgqLY9fMfURFbngLWcnyLd08PEGGR0w
DAjVM1n11zineL+Lw62G77DP6xMWFZadIn4+Ol2+wEQk4qJ0VsgZrLDrnE/v1lVr
kmXkGwKBgHUodQ38HGIdAw+XUDksvvs+TGVHkGXj4B2r4Y1WUEIYV/kEEH1VxDX
+KR//WjiMrt1o3cmILMrQLOEX4NFTh0kmzYGTc+4BiE1Y2krxEqxyVYyou+iDITCz
2oA1A+w/eMlx4CwZr8HeV6U2kdtx/nEvWpadImNLvKx6GXdRT3e/
-----END RSA PRIVATE KEY-----
quit
```

```
example-host (config) #
```

---

## What's Next

After configuring management access, you are ready to configure a reverse proxy or a forward proxy. See [Configuring a Reverse proxy](#) or [Configuring a Forward Proxy](#).

---

## Configuring a Forward Proxy

1. [Overview](#)
2. [More about Forward Proxies](#)
3. [Example Configuration](#)
4. [What's Next](#)

---

### Overview

The LineRate forward proxy capability provides a proxy function from one network to another. A common use case for a forward proxy is for connections from your private network to the Internet.

---

### More about Forward Proxies

A forward proxy lets you insert custom logic created with scripts. Scripts can perform a variety of functions, including gathering usage statistics, redirecting requests to your own cache, blocking of access to specific sites, managing cookies, and much more.

To use a forward proxy effectively, be sure to create and attach a virtual IP that includes the range of Internet IP addresses you want to go through the forward proxy.



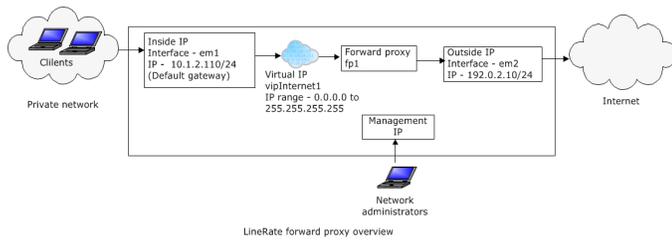
When attaching a virtual IP to a forward proxy, the virtual IP must not include any of the system's own IP addresses. For a virtual IP with a single IP address, do not set the virtual IP's IP address to one of the system's own IP addresses. For a virtual IP with a range of addresses, you must ensure that the IP address range does not contain any of the system's own IP addresses. This may mean you need to break the virtual IP into multiple virtual IPs. See [Configuring a range for a virtual IP with forward proxy](#) for more detail and an example.

---

### Example Configuration

The diagram below shows the configuration for a forward proxy from a private network to the Internet. Requests from clients in the private network go to the default gateway, which is a LineRate interface configured with the inside IP address (for example, 10.1.2.110). The virtual IP configured with a range of IP addresses listens for requests on the configured TCP port. This example shows the forward proxy configured to intercept TCP port 80, the typical port for HTTP traffic. The virtual IP passes the request to

the forward proxy, where a script may intercept the request and perform specific functions, then passes the request to the outside interface and on to the Internet.



---

## What's Next

After determining that you want to configure a forward proxy, you are ready to configure the data interfaces. See [Configuring Data Interfaces](#).

---

## Configuring Data Interfaces

1. [Overview](#)
2. [Configuring the Data Interfaces](#)
3. [Configuring the Default IP Route \(Gateway\) on LineRate](#)
4. [Configuring the Default IP Route on Clients](#)
5. [What's Next](#)

---

### Overview

An initial, basic configuration for a forward proxy includes the following key functions:

- Configuring the data interfaces
- Configuring the default IP route (gateway) on LineRate
- Configuring the default IP route on clients

---

### Configuring the Data Interfaces

You must assign an IP address to at least two interfaces to use for data. The LineRate software supports both IPv4 and IPv6.

For general information about the IP addresses and formats, see [Configuring Management Interfaces](#).

In this example, we are configuring two interfaces as shown in the diagram in [Configuring a Forward Proxy](#):

- Inside to the virtual IP (on em1)—10.1.2.110/24
- Outside to the Internet (on em2)—192.0.2.10/24



#### To configure the data interfaces:

1. Type:  
**show interfaces**
  - A list of all interfaces on the system displays. It is possible for the system to have an interface that LineRate cannot detect.
  - The first line is the interface name and its status. The interface name is based on the driver for the interface type. The remaining lines list the information available about the interface (typically, manufacturer, model, MAC address, speed in kilobits, and more).
  - Below are the names used for some common interfaces:
    - em—Intel 1Gb interface

- igb—Intel 1Gb interface
  - bce—Broadcom 1Gb interface
  - ix—Intel 10 Gb interface
  - oce—Emulex 10 Gb interface
  - lo—Loopback interface (internal interface)
2. Type:  
`configure`
  3. Type:  
`interface em1`
  4. Type:  
`ip address 10.1.2.110/24`
  5. Type:  
`interface em2`
  6. Type:  
`ip address 192.0.2.10/24`
  7. To check the interface settings, type:  
`show interfaces`  
em0 is up, line protocol is up  
Hardware is Intel82540EM, address is 0800.279e.0b3a  
Internet address is 10.200.0.1/24, broadcast is 10.200.0.255  
...  
em1 is up, line protocol is up  
Hardware is Intel82540EM, address is 0800.27bc.5b47  
Internet address is 10.1.2.110/24, broadcast is 10.1.2.255  
...  
em2 is up, line protocol is up  
Hardware is Intel82540EM, address is 0800.2738.ce7e  
Internet address is 192.0.2.10/24, broadcast is 192.0.2.255  
...
  8. Type:  
`write`

---

## Configuring the Default IP Route (Gateway) on LineRate

You should also configure the default IP route (gateway). For this forward proxy example, the inside IP address is the default gateway for all clients to the Internet.

For general information about the IP addresses and formats, see [Configuring Management Interfaces](#).



### To configure the default IP route:

1. Type:  
`configure`

2. Type:

```
ip route 0.0.0.0/0 192.0.2.2
```

- You can specify the destination IP subnet in any of the following formats:

```
192.0.2.2 255.255.255.255
```

- `192.0.2.2/24`—for a 24-bit subnet mask

3. To check the default route setting, type:

```
show ip route
```

- If you configured IPv6, use this command: `show ipv6 route`

Codes: C - connected, S - static

```
Gateway of last resort is 192.0.2.10 to network 0.0.0.0
```

```
S    0.0.0.0/0 via 192.0.2.2, em0, MTU 1500
```

```
C    10.0.2.0/24 is directly connected, em0, MTU 1500
```

```
C    10.0.3.0/24 is directly connected, em1, MTU 1500
```

```
C    10.0.4.0/24 is directly connected, em2, MTU 1500
```

```
C    10.1.2.0/24 is directly connected, em2, MTU 1500
```

```
C    192.0.2.10/24 is directly connected, em1, MTU 1500
```

```
C    10.200.0.1/24 is directly connected, em0, MTU 1500
```

4. Type:

```
write
```

---

## Configuring the Default IP Route on Clients

You should also configure the default IP route on clients to work with the forward proxy. In this example, each client's default IP route should point to the inside IP address of LineRate (10.1.2.110).

---

## What's Next

After configuring the data interfaces, you are ready to configure the virtual IP. See [Configuring the Virtual IP](#).

---

## Configuring the Virtual IP

1. [Overview](#)
2. [Creating a Virtual IP Base](#)
3. [Creating a Virtual IP](#)
4. [What's Next](#)

---

### Overview

In this forward proxy example, you want the virtual IP to listen for requests from all possible Internet IP addresses on port 80. Therefore, you want to configure the virtual IP with an address range from 0.0.0.0 to 255.255.255.255.

You can attach a virtual IP to only one forward proxy. You cannot use the same virtual IP for both a reverse proxy and forward proxy.



**To configure a virtual IP address, complete the following tasks:**

1. [Create a virtual IP base.](#)
2. [Create a virtual IP.](#)

---

### Creating a Virtual IP Base

We recommend creating one or more virtual IP bases. For general information about bases in LineRate, see [Working with Bases](#). A base lets you configure the most common settings that you want for your virtual IPs. You can also create more than one virtual IP base for settings that you need to be different or more specific for some virtual IPs.

In this example, we are creating a single virtual IP base called `vipbase_web1`. We recommend giving each virtual IP base a meaningful name that helps identify the base. For example, you might use the application type (such as serving similar web content) or security settings (such as SSL) in the name.



**To create an example virtual IP base:**

Step	Command	Description
1	<code>configure</code>	Puts LineRate into configure mode.
2	<code>virtual-ip base vipbase_web1</code>	Names the base vipbase_web1.
3	<code>admin-status online</code>	Brings the virtual IP online, so it is ready for use.
4	<code>service http</code>	Sets the service type to HTTP for layer 7 web traffic.
5	<code>keepalive- timeout 5</code>	Sets the keepalive timeout to 5 seconds. This is the time the system waits for a specific client to send a request before closing the connection, reclaiming connection resources. For most use cases, this setting will affect the number of simultaneous connections that the system will have open. A lower setting will usually result in fewer simultaneous open connections. A good rule of thumb is to set this number no higher than 500,000 divided by the number of expected connections per second at peak load. For example, if the system is expected to process up to 100,000 connections per second, 500,000 divided by 100,000 is 5. So the setting should be 5 seconds in this example.

## Creating a Virtual IP

After creating the virtual IP base, you can create a virtual IP. We recommend giving each virtual IP a meaningful name that helps identify the virtual IP. For example, you might use the application or service type (such as serving similar web content) or security settings (such as SSL) in the name.

For this example, we are configuring a range of IP address that cover the entire range of IP addresses on port 80 (HTTP).



### To create a virtual IP:

- Type:  
`configure`
- Type:  
`virtual-ip vipInternet1`
- Type:  
`base vipbase_web1`
- Type:  
`ip range 0.0.0.0 255.255.255.255 80`
- Type:  
`show run brief`

```
...
virtual-ip base vipbase_web1
admin-status online
keepalive-timeout 5
service http
!
virtual-ip vipInternet1
ip range 0.0.0.0 255.255.255.255 80
...
```

5. Type:  
**write**

---

## What's Next

After configuring the virtual IP, you are ready to configure the forward proxy itself. See [Configuring the Forward Proxy](#).

## Configuring the Forward Proxy

For this example, you now need to configure the forward proxy itself. You must give the forward proxy a name, attach the virtual IP to it, and put the forward proxy online. In addition, it is a best practice to always set the response timeout and the keepalive timeout.



**To create an example forward proxy:**

Step	Command	Description
1	<code>configure</code>	Puts LineRate into configure mode.
2	<code>forward-proxy fp1</code>	Names the forward proxy fp1.
3	<code>admin-status online</code>	Brings the forward proxy online, so it is ready for use.
4	<code>service http</code>	Sets the service type to HTTP for layer 7 web traffic.
5	<code>response-timeout 5</code>	<p>Sets the response timeout to 5 seconds. This is the time the system waits for the HTTP server to respond to a request. If the server does not respond in this time, the system sends an HTTP 504 error to the client and closes the connection. This ensures that connections are closed and system resources are reclaimed if the server does not respond.</p> <p>Consider the amount of time you're willing to wait for a target web server to respond to any request. The response-timeout must always be configured to be higher than the amount of time it takes for any of the web servers to respond to a request.</p>
6	<code>keepalive-timeout 10</code>	Sets the keepalive timeout to 10 seconds. This is the time the system waits for a new HTTP request from a client to a server. If there are no active HTTP transactions (that is, no active requests or responses) to a server for the specified time (in seconds), the system closes the TCP connection to the server, reclaiming resources. This also helps avoid problems that some HTTP servers have when connections are kept open indefinitely.

Step	Command	Description
7	<code>attach virtual-ip vipbase_web1</code>	Attaches the virtual IP we created earlier.

---

## Complete Forward Proxy Example

After configuring the forward proxy, as described above, you can use the `show run brief` command to see the complete forward proxy configuration.

```
example-host# show run brief
Building configuration...

!
hostname example-host
!
username admin secret encrypted "$2a$04$7TYufYOKVQ8i8bblVtZ1ierxZXzch5mR/
QeaZH8WnWRzVEkPt0MgS" uid 2000
!
interface em0
 ip address 10.200.0.1 255.255.255.0
!
interface em1
 ip address 10.1.2.110 255.255.255.0
!
interface em2
 ip address 192.0.2.10 255.255.255.0
!
ip route 0.0.0.0/0 192.0.2.2
!
ssl profile self-signed
 attach primary-certificate self-signed
 attach private-key self-signed
!
forward-proxy fp1
 attach virtual-ip vipbase_web1
 service http
 response-timeout 5

keepalive-timeout 10
admin-status online
```

```
!  
virtual-ip base vipbase_web1  
  service http  
    keepalive-timeout 5  
    admin-status online  
!  
virtual-ip vipInternet1  
  ip range 0.0.0.0 255.255.255.255 80  
!  
ssh  
  allow from 10.200.0.0/24  
  allow to 10.200.0.1 22  
!  
rest-server  
  allow from any  
  allow to any 8443  
  attach ssl profile self-signed  
!  
certificate self-signed  
! Cert data not shown in brief output  
!  
key self-signed  
! Key data not shown in brief output
```

---

## Configuring a Reverse Proxy

1. [Overview](#)
2. [More about Reverse Proxies](#)
3. [What's Next](#)

---

### Overview

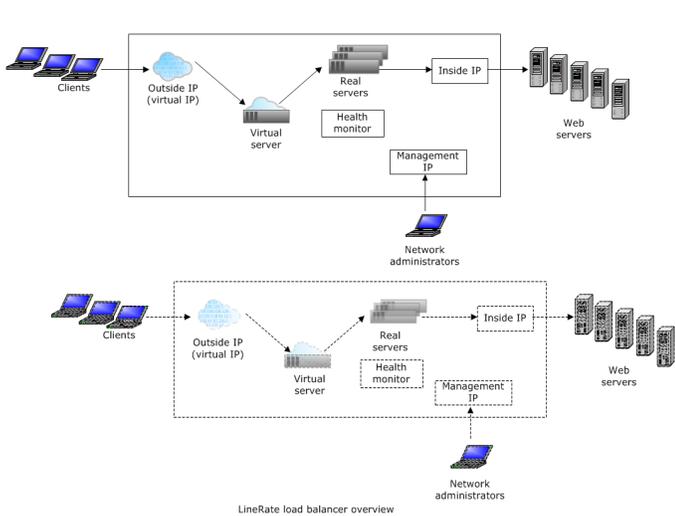
The LineRate system provides a full-proxy front-end to the web and secure web services on back-end servers of the application. As a full proxy, LineRate provides a logical front-end to the client's connection to the web and secure web services of the application.

---

### More about Reverse Proxies

To successfully manage load, health, and availability of the application, LineRate constantly monitors the traffic flows from the client to the back-end servers to ensure the delivery of the application services. LineRate provides several discrete services including health monitoring, transaction statistics, and traffic management to ensure balanced usage of back-end servers and rapid clients service.

The diagram below shows a basic LineRate configuration for a load balancing use case. You can have multiple load balancer configurations in the LineRate software, as shown by the second configuration in the diagram. Clients access the virtual IP, which goes through a virtual server. Based on the load balancing algorithm set in the virtual server, it passes client requests through the real servers and the inside IP address to the web servers.



## What's Next

After determining that you want to configure a reverse proxy, you are ready to configure the data interfaces. See [Configuring Data Interfaces](#).

---

## Configuring Data Interfaces

1. [Overview](#)
2. [Configuring the Data Interfaces](#)
3. [Configuring the Default IP Route \(Gateway\)](#)
4. [Data Interfaces Example](#)
5. [What's Next](#)

---

### Overview

An initial, basic configuration includes the following key functions:

- Configuring the data interfaces
- Configuring the default route (gateway)

---

### Configuring the Data Interfaces

The LineRate software supports both IPv4 and IPv6.

The recommended configuration for performance and security reasons is to configure IP addresses on at least two interfaces.

For general information about the IP addresses and formats, see [Configuring the Management Interface](#).

In this example, we are configuring two data interfaces as shown in the diagram in [Configuring Load Balancing](#):

- Outside for the virtual IP (on em1)—192.0.2.1/24
- Inside to web servers (on em2)—10.1.2.1/24



#### To configure the data interfaces:

1. Type:  
**show interfaces**
  - A list of all interfaces on the system displays. It is possible for the system to have an interface that LineRate cannot detect.
  - The first line is the interface name and its status. The interface name is based on the driver for the interface type. The remaining lines list the information available about the interface (typically, manufacturer, model, MAC address, speed in kilobits, and more).
  - Below are the names used for some common interfaces:
    - em—Intel 1Gb interface

- igb—Intel 1Gb interface
  - bce—Broadcom 1Gb interface
  - ix—Intel 10 Gb interface
  - oce—Emulex 10 Gb interface
  - lo—Loopback interface (internal interface)
2. Type:  
`configure`
  3. Type:  
`interface em1`
  4. Type:  
`ip address 192.0.2.1/24`
  5. Type:  
`interface em2`
  6. Type:  
`ip address 10.1.2.1/24`
  7. To check the interface settings, type:  
`show interfaces`  
em0 is up, line protocol is up  
Hardware is Intel82540EM, address is 0800.279e.0b3a  
Internet address is 10.200.0.1/24, broadcast is 10.200.0.255  
...  
em1 is up, line protocol is up  
Hardware is Intel82540EM, address is 0800.27bc.5b47  
Internet address is 192.0.2.1/24, broadcast is 192.0.2.255  
...  
em2 is up, line protocol is up  
Hardware is Intel82540EM, address is 0800.2738.ce7e  
Internet address is 10.1.2.1/24, broadcast is 10.1.2.255  
...
  8. Type:  
`write`

---

## Configuring the Default IP Route (Gateway)

You should also configure the default IP route (gateway). You can configure additional static IP routes, as needed, to permit access to your networks.

For general information about the IP addresses and formats, see [Configuring the Management Interface](#).



### To configure the default IP route:

1. Type:  
`configure`
2. Type:  
`ip route 0.0.0.0/0 192.0.2.2`

- You can specify the <gateway IP address> in any of the following formats:
  - 192.0.2.2/24—for a 24-bit subnet mask
  - 192.0.2.2 255.255.255.255

3. To check the default route setting, type:

```
show ip route
```

4. If you configured IPv6, use this command:

```
show ipv6 route
```

```
Codes: C - connected, S - static
```

```
Gateway of last resort is 192.0.2.2 to network 0.0.0.0
```

```
S    0.0.0.0/0 via 192.0.2.2, em0, MTU 1500
C    10.0.2.0/24 is directly connected, em0, MTU 1500
C    10.0.3.0/24 is directly connected, em1, MTU 1500
C    10.0.4.0/24 is directly connected, em2, MTU 1500
C    10.1.2.0/24 is directly connected, em2, MTU 1500
C    192.0.2.1/24 is directly connected, em1, MTU 1500
C    10.200.0.1/24 is directly connected, em0, MTU 1500
```

5. Type:

```
write
```

---

## Data Interfaces Example

After configuring the data interfaces as described above, you can use the **show run** command to see the configuration. We have annotated the example command output below. Comment lines start with an exclamation mark (!).

```
LROS(config)# show run
Building configuration...

!
! Hostname setting.
!
hostname example-host
!
! Default user name and encrypted password.
!
username admin secret encrypted "$2a$04$7TYufYOKVQ8i8bb1VtZ1ierxZXzcH5mR/
  QeaZH8WnWRzVEkPt0MgS" uid 2000
!
interface em0
  ip address 10.200.0.1 255.255.255.0
!
! IP address configured on the interface called em1 for data.
!
```



```

PK7/nxRt+C72hde2OaU=
-----END CERTIFICATE-----
quit
!
key self-signed
  pem-format
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAvhALFtrOHMGc9bgYcFB5spZFVrH2SF8+lan5hsnOlejXB5Nx
ce9G6ESyZOS8N0lOSChaB068YE9uWtiIFeK+Q2j14LqgGT05bROBjpeNHqngAVIy
REOHdEiH/ELazuVIA2Nh7XkGRyJsx5qTr/gHEUgXXZc1DGNHrhmkknk0zzKBzhIzx
2QHURR7kVODjESL4NH39NmpnXL/eVNr5q1b86fuctyAHvP+bWGSanw0J3DjHM0Js
gl1flYbV1shsUPy46w+gfKgZS11gn17EMK4CBffFTkuXzt9PfFZTPnHDXfNns2u
sBoIbyHq6B8s0o+TGLby0v5M1kfMM8VvJ42IxQIDAQABAoIBAGXakSbJUWWFuIjS
BH7EEcPL1hLUwggcypxH/8n1AmwOIJYVxNjrAtPcZMG+9sKmDUaMIVsDLd5rEteq
bJtV7OKRMBsjyEJZPsieihKS8vR40uvCuD/VVJTQEAhxB3OS2dm++67Yia27XBJH
21eVEqyHNsZYDvy5g6NgaKDQ/K5ubCfPkXji9OKfT8AGFR6kKPra1oG1w+YUR8qh
F7H4o9yo+Adr0un2QZOKowG7mwmTE7L4a4nIfs09sFeNKYDW0hohp2qrX6HY/HJd
2iy1SuUUzfWGuqYVwAUQKz9UvuqezK2H3xnp/S//gDUWJZ+1XmMKx38j+gFxbld
RxCxs0CgYEA9xXNt1vEqgl7vfm+vh84loV3MTypYpCq3RRND+yqwyZdAdzaie4Z
nEt1H7V/ry5HmaH4XTXKer3X3SWJIdbZeNXmcZnatzi2XqVmhhmCMR0rHXuWA4GA
qMlCwOwZs1N2tJxGwmkHC5lGy6J21TL68PQIafeAYrBl3zW330W+I78CgYEAxOuN
gODEx4/8pHvgj1q+w1gbA5oXDCGTD1Y0Kt9RcPgWjnkQtW7KY3slGDrfPdIWfSRj
tNNTsqUA4cfx9yWykFC+aifUfn6lutHrq5SUAc/heoatvL7XAM1VQnH1tqYinZL
rDOat7wkby2WIQPZbXKOojWcVLf5DND/E0y0pHsCgYAgjyL4cMdnkVFJC2vzKbIP
Q68dMd0w09gIIfc1tH4cESYYZL33hwSg7+CTORuGPhb5S7qqrbszK9xWMz1RkaL
ocQoHBoR6/m8JxeHfD0Hs8xGq1HbZG1L1JmTSolav7jYu+8nFyfyg1Qs6U+3cGxY
7A9fx1mHp68E5tM//LS9iQKBgQCEWtJcKjB47wVfRMfUxpdppq9Zh2swQyzFORmN
K1Zg+OaiEqsxV0r+/FkdZQyBT8C/0gKWGmgqLY9fMfURFbngLWcnyLd08PEGGRoW
DAjVM1n11zineL+Lw62G77DP6xMWFZadIn4+Ol2+wEQk4qJ0VsgZrLDrne/v11Vr
kmXkGwKBgHUodQ38HGIdAw+XUDksvvs+TGVHkGXj4B2r4Y1WUEIYV/kEEH1VxDX
+KR//WjiMrt1o3cmILMrQLOEX4NFTh0kmzYGTC+4BiE1Y2krxEqxyVYou+iDITCz
2oA1A+w/eMlx4CwZr8HeV6U2kdtX/nEvWpadImNLvKx6GXdRT3e/
-----END RSA PRIVATE KEY-----
quit

example-host (config) #

```

---

## What's Next

After configuring the data interfaces, you are ready to configure [load balancing](#). See [Configuring Load Balancing](#).

# Configuring Load Balancing

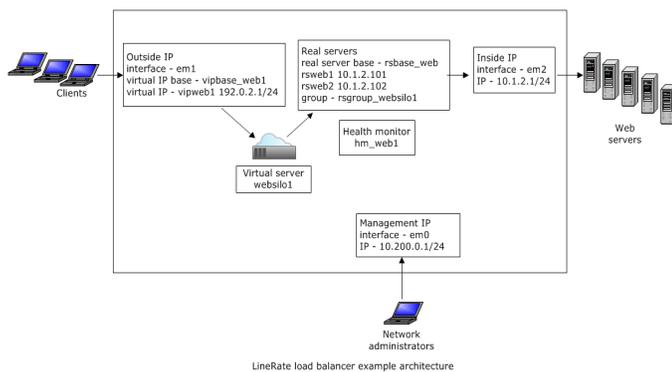
1. [Overview](#)
2. [Configuring a Virtual IP Address](#)
  - 2.1. [Creating a Virtual IP Base](#)
  - 2.2. [Creating a Virtual IP](#)
3. [Configuring a Health Monitor](#)
4. [Configuring Real Servers](#)
  - 4.1. [Creating a Real Server Base](#)
  - 4.2. [Creating Real Servers](#)
  - 4.3. [Creating a Real Server Group](#)
5. [Configuring a Virtual Server](#)
6. [Load Balancing Example](#)
7. [What's Next](#)

## Overview

The figure below shows a very simple example load balancing architecture, with all of the basic elements you need. It includes the specific names and IP addresses that we use throughout the rest of this *Getting Started Guide*.

This example architecture assumes the following:

- The system has three physical interfaces.
- The architecture uses two real servers.
- You have two web servers.



The remainder of this *Getting Started Guide* walks through how to create this architecture with the LineRate software.

---

## Configuring a Virtual IP Address

The load balancer requires at least one virtual IP address. The virtual IP address is a configuration object that represents the outside interface that clients connect to. In this example, we will configure one virtual IP, but you can configure more, depending on your needs.



**To configure a virtual IP address, complete the following tasks:**

- Create a virtual IP base.
- Create a virtual IP.

---

## Creating a Virtual IP Base

We recommend creating one or more virtual IP bases. For general information about bases in LineRate, see [Working with Bases](#). A base lets you configure the most common settings that you want for your virtual IPs. You can also create more than one virtual IP base for settings that you need to be different or more specific for some virtual IPs.

In this example, we are creating a single virtual IP base called `vipbase_web1`. We recommend giving each virtual IP base a meaningful name that helps identify the base. For example, you might use the application type (such as serving similar web content) or security settings (such as SSL) in the name.



**To create an example virtual IP base:**

Step	Command	Description
1	<code>configure</code>	Puts LineRate into configure mode.
2	<code>virtual-ip base vipbase_web1</code>	Names the base <code>vipbase_web1</code> .
3	<code>admin-status online</code>	Brings the virtual IP online, so it is ready for use.
4	<code>service http</code>	Sets the service type to HTTP for layer 7 load balancing of web traffic.
5	<code>keepalive-timeout 5</code>	Sets the keepalive timeout to 5 seconds. This is the time the system waits for a specific client to send a request before closing the connection, reclaiming connection resources. For most use cases, this setting will affect the number of simultaneous connections that the system will have open. A lower setting will

Step	Command	Description
		usually result in fewer simultaneous open connections. A good rule of thumb is to set this number no higher than 500,000 divided by the number of expected connections per second at peak load. For example, if the load balancer is expected to process up to 100,000 connections per second, 500,000 divided by 100,000 is 5. So the setting should be 5 seconds in this example.

## Creating a Virtual IP

After creating the virtual IP base, you can create a virtual IP. We recommend giving each virtual IP a meaningful name that helps identify the virtual IP. For example, you might use the application or service type (such as serving similar web content) or security settings (such as SSL) in the name.

For this example, we are using the IP address of the outside interface (em1) that we configured already ([Configuring Data Interfaces](#)) to create the virtual IP, and we are using the virtual IP base we already created. You must also include the TCP port number on which the clients will contact the load balancer.



### To create a virtual IP:

- Type:  
`configure`
- Type:  
`virtual-ip vipweb1`
- Type:  
`base vipbase_web1`
- Type:  
`ip address 192.0.2.1 443`
- Type:  
`show run brief`

```

...
virtual-ip base vipbase_web1
  admin-status online
  keepalive-timeout 5
  service http
!
virtual-ip vipweb1 ip 192.0.2.1 443 base vipbaip_web1
...

```



Notice how with having set just the base and IP address (and port), the show run brief output lists the virtual-ip on just one line. This lets you review a long list of virtual-ips to find differences or patterns in names and IP addresses.

5. Type:  
`write`

## Configuring a Health Monitor

A health monitor can monitor multiple real servers. The health monitor for web servers (HTTP) opens a connection to the web server, sends an HTTP request to the web server for something (possibly a specific web page), looks at the response, and determines if the response is correct. The configuration settings on the health monitor object determine what to request from the web server and what the response should be.

In this example, we are creating a single health monitor called `hm_web1`. We recommend giving each health monitor a meaningful name that helps identify the health monitor. For example, you might use the application or service (such as serving similar web content) or how you are monitoring in the name.



**To create an example of the health monitor:**

Step	Command	Description
1	<code>configure</code>	Puts LineRate into configure mode.
2	<code>health-monitor hm_web1</code>	Names the health monitor <code>hm_web1</code> .
3	<code>interval 5</code>	Sets the health monitor to start a health check every 5 seconds.
4	<code>timeout 1</code>	Sets the timeout to 1 second. The health monitor will determine an individual health probe to fail if it does not respond within this time. One use of this setting is to test the server's response time.
5	<code>server-down "8/10"</code>	Sets the threshold for marking the server DOWN to the failure of 8 out the last 10 health probes. If the health probe fails 8 out of the last 10 times, the system takes the server offline.
6	<code>server-up "9/10"</code>	Sets the threshold for marking the server UP to the success of 9 out the last 10 health probes. If the health

Step	Command	Description
		probe succeeds 9 out of the last 10 times, the system puts the server back online.
7	<code>type http</code>	Sets the health monitor type to HTTP for web use.
8	<code>request-method GET</code>	Sets the type of request the health monitor will send to a GET request.
9	<code>request-target "/health.html"</code>	Sets the specific web page that the health monitor will request. If the health monitor is able to retrieve the page, receiving a 200 OK response from the server, the server's health probe is deemed successful.
10	<code>admin-status online</code>	Brings the health monitor online, so it is ready for use.

---

## Configuring Real Servers

Real servers are another required configuration object of the LineRate load balancer. Real servers represent and point to actual web servers that the load balancer is distributing client requests to.



**To configure real servers, complete the following tasks:**

- Create a real server base.
- Create a real server.

---

## Creating a Real Server Base

We recommend creating one or more real server bases. For general information about bases in LineRate, see [Working with Bases](#). A base lets you configure common settings that you want for your real servers. You can also create more than one real server base for settings that you need to be different for some real servers.

In this example, we are creating a single real server base called `rsbase_web`. We recommend giving each real server base a meaningful name that helps identify how the base will be used. For example, you might use the application type (such as serving similar web content), hardware capabilities (such as CPU or memory), or security settings (such as SSL) in the name.



**To create an example of the real server base:**

Step	Command	Description
1	<code>configure</code>	Puts LineRate into configure mode.
2	<code>real-server base rsbase_web</code>	Names the base rsbase_web.
3	<code>max-connections 1000</code>	Sets the maximum connections to the real server at 1000. LineRate will not open more than 1000 connections to any server.
4	<code>admin-status online</code>	Brings the real server online, so it is ready for use.
5	<code>attach health-monitor hm_web1</code>	Attaches a health monitor called hm_web1. See <a href="#">Configuring a Health Monitor</a> .
7	<code>service http</code>	Sets the service type to HTTP, which sets this real server to be compatible with layer 7 load balancing, for web use. The service setting on a real server must match the service setting on any virtual server to which the real server is attached.
8	<code>keepalive-timeout 10</code>	Sets the keepalive timeout of the HTTP service to 10 seconds. If there are no requests that get sent to a connection for 10 seconds, the load balancer closes the connection to the server, reclaiming resources. This can help avoid problems that some web servers have when connections are kept open indefinitely.
9	<code>response-timeout 60</code>	Sets the response-timeout of the HTTP service to 60 seconds. The load balancer closes the connection if the HTTP server takes longer than 60 seconds to respond to a request. Consider the amount of time the web server takes to respond to any request. The response-timeout on the load balancer must always be configured to be higher than the amount of time it takes for any of the web servers to respond to a request.
10	<code>response-idle-timeout 60</code>	Sets the response-idle-timeout of the HTTP service to 60 seconds. The load balancer closes the connection if it takes longer than 60 seconds either to receive any part of the response from the HTTP server or to transmit any part of the response to the client. Consider the size of a typical response for your application as well as the user environment to set this value. For example, an application where users download HD videos using mobile devices would need longer timeout than simple web pages due to mobile bandwidth and device processing limitations.

---

## Creating Real Servers

After creating the real server base, you can create a real server. We recommend giving each real server a meaningful name that helps identify the real server. For example, you might use the application type (such as serving similar web content), hardware capabilities (such as CPU or memory), or security settings (such as SSL) in the name.

In this example, we are creating two real servers (rsweb1 and rsweb2) that inherit properties from our real server base and assigning them the IP addresses of two actual web servers. You must also include the TCP port number on which the load balancer will contact the server.



### To create real servers:

1. Type:  
`configure`
2. Type:  
`real-server rsweb1`
3. Type:  
`base rsbase_web`
4. Type:  
`ip address 10.1.2.101 8080`
5. Type:  
`real-server rsweb2`
6. Type:  
`base rsbase_web`
7. Type:  
`ip address 10.1.2.102 8080`
8. Type:  
`show run brief`

```
real-server base rsbase_web
  admin-status online
  max-connections 1000
  service http
    response-timeout 60
    response-idle-timeout 60
    keepalive-timeout 10
  attach health-monitor hm_web1
!
real-server rsweb1 ip 10.1.2.101 8080 base rsbase_web
real-server rsweb2 ip 10.1.2.102 8080 base rsbase_web
...
```



Notice how with having set just the base and IP address (and port), the show run brief output lists the real-servers on just one line. This lets you review a long list of real-servers to find differences or patterns in names and IP addresses.

---

9. Type:  
`write`

---

## Creating a Real Server Group

You can use real server groups create logical groups of real servers. A real server can be a member of multiple groups. You can use the groups to show information about the real servers or to attach the group to a virtual server for load balancing.

We recommend giving each real server group a meaningful name that helps identify the group use. For example, you might set up a real server group based on the application, floor location (all servers in a specific rack), or data center (all servers in data center).

In this example, we are creating a real server group (rsgroup\_websilo1) and are adding the two real servers we already created, using a regular expression. We will then attach this real server group to a virtual server.



### To create a real server group:

1. Type:  
`configure`
2. Type:  
`real-server group rsgroup_websilo1`
3. Type:  
`members by regex "rsweb.*"`
4. Type:  
`write`

---

## Configuring a Virtual Server

Each load balancing (reverse proxy) configuration requires at least one virtual server. The virtual server is a configuration object that acts as a reverse proxy and ties together one or more virtual IPs and real servers. You also set the load balancing algorithm on the virtual server.

We recommend giving each virtual server a meaningful name that helps identify the server use. For example, you might name a virtual server based on the application and the resources that the virtual server is load balancing traffic to (real servers).

In this example, we are creating a virtual server and are attaching the virtual IP and real server group to it. We will also set the load balancing algorithm.



### To create a virtual server:

1. Type:  
`configure`
2. Type:  
`virtual-server websilol`
3. Type:  
`attach virtual-ip vipweb1 default`
4. Type:  
`attach real-server group rsgroup_websilol`
5. Type:  
`lb-algorithm round-robin-free`
6. Type:  
`service http`
7. Type:  
`show run brief`  
  
`...`  
`virtual-server websilol`  
`lb-algorithm round-robin-free`  
`service http`  
`attach virtual-ip vipweb1 default`  
`attach real-server group rsgroup_websilol`  
`...`
8. Type:  
`write`

---

## Load Balancing Example

After configuring load balancing, as described above, you can use the **show run brief** command to see the configuration. We have annotated the load balancing configuration in the example command output below. Comment lines start with an exclamation mark (!).

```
example-host(config)# show run brief
Building configuration...

!
hostname example-host
!
username admin secret encrypted "$2a$04$7TYufYOKVQ8i8bb1VtZ1ierxZXzch5mR/
  QeaZH8WnWRzVEkPt0MgS" uid 2000
!
```

```

interface em0
 ip address 10.200.0.1 255.255.255.0
!
interface em1
 ip address 192.0.2.1 255.255.255.0
!
interface em2
 ip address 10.1.2.1 255.255.255.0
!
ip route 0.0.0.0/0 192.0.2.2
!
! Health monitor and its configuration.
!
health-monitor hm_web1
 interval 5
 timeout 1
 server-down "8/10"
 server-up "9/10"
 type http
  request-method GET
  request-target "/health.html"
 admin-status online
!
! Default SSL configuration. See Configuring SSL.
!
ssl profile self-signed
 attach primary-certificate self-signed
 attach private-key self-signed
!
! Real server base and its configuration.
!
real-server base rsbase_web
 admin-status online
 max-connections 1000
 service http
  response-timeout 60
  response-idle-timeout 60
  keepalive-timeout 10
 attach health-monitor hm_web1
!
! Real servers showing their names, IP addresses, and base in a single line.
!
real-server rsweb1 ip 10.1.2.101 8080 base rsbase_web
real-server rsweb2 ip 10.1.2.102 8080 base rsbase_web
!
! Virtual IP base and its configuration.
!
virtual-ip base vipbase_web1
 admin-status online
 service http
  keepalive-timeout 5
!
! Virtual IP showing its name, IP address, and base in a single line.
!

```

```
virtual-ip vipweb1 ip 192.0.2.1 443 base vipbaip_web1
!
! Real server group showing the regular expression used for group members.
!
real-server group rsgroup_websilol
members by regex "rweb.*"
!
! Virtual server and its configuration.
!
virtual-server websilol
lb-algorithm round-robin-free
service http
attach virtual-ip vipweb1 default
attach real-server group rsgroup_websilol
!
ssh
allow from 10.200.0.0/24
allow to 10.200.0.1 22
!
rest-server
allow from any
allow to any 8443
attach ssl profile self-signed
!
certificate self-signed
! Cert data not shown in brief output
!
key self-signed
! Key data not shown in brief output

example-host(config-vserver-http:websilol)#
```

---

## What's Next

After you configure the load balancer, you can test the load balancer ([Monitoring and Troubleshooting Load Balancing](#)) or add security by configuring SSL ([Configuring SSL](#)).

---

# Monitoring and Troubleshooting Load Balancing

1. [Overview](#)
2. [Solutions](#)
  - 2.1. [Seeing "404 Not Found" errors when attempting to access a new virtual server, but real-server logs do not show any error\\_log messages that match](#)
  - 2.2. [Seeing "502 Bad Gateway" error messages when attempting to access a virtual server](#)
  - 2.3. [Seeing "couldn't connect to host" error messages when attempting to access a virtual server](#)
  - 2.4. [Some of my real servers may be more heavily loaded than others. How can I see this?](#)

---

## Overview

This section provides a few possible errors you might encounter while setting up a load balancing or SSL offload use case and how to resolve those issues.

---

## Solutions

---

### Seeing "404 Not Found" errors when attempting to access a new virtual server, but real-server logs do not show any error\_log messages that match

The most common issue surrounding 404 errors, especially with a new virtual server, is a missing "default" virtual IP for the virtual server.

When the virtual server is using the service type HTTP, the virtual server parses the HTTP request headers and looks for a hostname match to a given virtual server. If no hostname match is found, the proxy will respond to the client with a 404 error and not pass the request to the real server. This will also happen with requests that request the URL with the IP address of the virtual IP and not using an FQDN.

For example, the following virtual server has a hostname set and no default virtual IP for requests.

```
!  
virtual-server vs1  
  service http  
    tcp-multiplex  
    hostname www.lineratesystems.com  
  attach virtual-ip v1p1  
  attach real-server group reals  
!
```

When a request is made to the IP address of the virtual-ip we receive a "404 Not Found" message:

```
curl 201.0.50.1:8080/  
<html><head><title>Status 404 Not Found</title></head><body><h1>Status 404 Not  
Found</h1></body></html>
```

If we append the Host: header to the request using our defined hostname, the error goes away:

```
curl 201.0.50.1:8080/ -H "Host: www.lineratesystems.com"  
<html>  
<head>  
<title>Welcome to the virtual-server!</title>  
</head>  
<body bgcolor="white" text="black">  
<center><h1>Welcome to the virtual-server!</h1></center>  
</body>  
</html>
```

Similarly, if we use a Host: header name that is not defined for the virtual server, we will get a 404 error:

```
curl 201.0.50.1:8080/ -H "Host: www.lineratesomething.com"  
<html><head><title>Status 404 Not Found</title></head><body><h1>Status 404 Not  
Found</h1></body></html>
```

Attaching the virtual IP with the "default" setting will allow all of these unmatched requests to be proxied to the back-end real servers.

```
!  
virtual-server vs1  
service http  
tcp-multiplex  
hostname www.lineratesystems.com  
attach virtual-ip vipl default  
attach real-server group reals  
!
```

These 404 response codes can be monitored on the system with SNMP or viewed from the CLI. The load-balancer statistics are where we can find the current count of HTTP internal response codes, as none of these will match a defined virtual server:

```
lrs01# show load-balancer statistics detailed  
<output omitted>  
httpInternalResp404: 6
```

---

## Seeing "502 Bad Gateway" error messages when attempting to access a virtual server

The most common issue surrounding 502 errors, especially with a new virtual server, is when the real servers are either marked down with a failed health monitor or their admin status is set to offline. The default setting for a new real server base is admin status offline.

Check the real servers to make sure they are all in admin status online.

```
lrs01# show real group reals
reals Group Members
Name Address      Port  Svc   Admin   Health  Conns  Rx Mbps  Tx Mbps
-----
rs1   201.0.51.1     8080  http  offline up       0       0.0     0.0
rs2   201.0.51.2     8080  http  offline up       0       0.0     0.0
rs3   201.0.51.3     8080  http  offline up       0       0.0     0.0
rs4   201.0.51.4     8080  http  offline up       0       0.0     0.0
rs5   201.0.51.5     8080  http  offline up       0       0.0     0.0
```

If the real servers are offline, change their real server base to admin status online or edit each real server individually to set the admin status online.

Check the real servers to make sure they are all passing their health monitor checks and are marked as "up."

```
lrs01# show real group reals
reals Group Members
Name Address      Port  Svc   Admin   Health  Conns  Rx Mbps  Tx Mbps
-----
rs1   201.0.51.1     8080  http  online  down    0       0.0     0.0
rs2   201.0.51.2     8080  http  online  down    0       0.0     0.0
rs3   201.0.51.3     8080  http  online  down    0       0.0     0.0
rs4   201.0.51.4     8080  http  online  down    0       0.0     0.0
rs5   201.0.51.5     8080  http  online  down    0       0.0     0.0
```

Check the health monitor settings to make sure that the configuration is correct and that the request target is available on each of the real servers.

```
lrs01# show real group reals
reals Group Members
Name Address      Port  Svc   Admin   Health  Conns  Rx Mbps  Tx Mbps
-----
rs1   201.0.51.1     8080  http  online  up       0       0.0     0.0
rs2   201.0.51.2     8080  http  online  up       0       0.0     0.0
```

---

## Seeing "couldn't connect to host" error messages when attempting to access a virtual server

The most common issue surrounding "couldn't connect to host" error messages is when the virtual IP is admin status offline. The default setting for a virtual IP base is admin status offline.

Check your virtual IP or virtual server to make the virtual IP is online:

```
lrs01# show virtual-server vs1
Configuration
  LB Algorithm:          round-robin
  Service Type:         http
  Real Server Groups:
    Name                Weight
    reals               1 (default)
  Real Servers:
    <none>
  Virtual IPs:
    Name                Address      Port Svc  Admin
    vip1               201.0.50.1  8080 http offline
```

Make sure your virtual IP base or virtual IP is set to admin status online:

```
!
virtual-ip vip1
  ip address 201.0.50.1 8080
  admin-status offline
!
```

---

## Some of my real servers may be more heavily loaded than others. How can I see this?

Use a real server group and **show real group <name>** to get all of the traffic and connection distribution counts for each real server.

```
!
real-server rs1 ip 201.0.51.1 8080 base rsb
real-server rs2 ip 201.0.51.2 8080 base rsb
real-server rs3 ip 201.0.51.3 8080 base rsb
real-server rs4 ip 201.0.51.4 8080 base rsb
real-server rs5 ip 201.0.51.5 8080 base rsb
!
real-server group reals
  members by regex "rs.*"
!
```

```
lrs01# show real group reals
```

```
reals Group Members
```

Name	Address	Port	Svc	Admin	Health	Conns	Rx Mbps	Tx Mbps
rs1	201.0.51.1	8080	http	online	up	2	87.0	0.2
rs2	201.0.51.2	8080	http	online	up	2	87.0	0.2
rs3	201.0.51.3	8080	http	online	up	2	87.1	0.2
rs4	201.0.51.4	8080	http	online	up	2	87.0	0.2
rs5	201.0.51.5	8080	http	online	up	2	86.9	0.2

## Configuring SSL

1. [SSL Types Supported in the LineRate Software](#)
2. [SSL Termination](#)
3. [Setting Up the Private Key for SSL termination](#)
4. [Setting Up Certificates for SSL Termination](#)
5. [Configuring SSL Termination](#)
6. [Configuring SSL Initiation](#)
7. [SSL Example](#)
8. [What's Next](#)

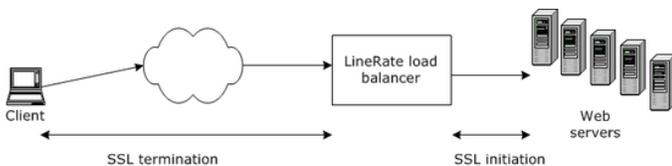
Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are closely related technologies that provide communication security over an insecure network, such as the Internet. TLS is a standardized protocol, defined by IETF RFCs, and is the successor to the non-standardized SSL protocol. The LineRate software supports both TLS and SSL, but the system and documentation refers to both protocols collectively as "SSL," following the most common industry terminology.

## SSL Types Supported in the LineRate Software

The LineRate software supports two types of SSL connections:

- SSL termination—SSL connection from the client to the LineRate load balancer.
- SSL initiation—SSL connection from the LineRate load balancer to the web server.

The diagram below shows the two types of SSL.



SSL configuration in LineRate

By using the SSL termination feature in LineRate, you can move the computationally intensive SSL processing off your web servers and onto the LineRate, allowing your web servers to concentrate on performing application tasks. Or, if your application requires greater security on your internal network, you can use SSL initiation together with SSL termination to provide end-to-end SSL security, while still allowing the LineRate to do full layer 7 load balancing.

---

## SSL Termination

Before beginning to set up SSL termination, you will need the following:

- Primary certificate file that identifies the website you wish to set up on the LineRate system
- Private key file that corresponds to the primary certificate
- Chain certificate files (also called intermediate certificates) that correspond to the primary certificate are only required if their primary certificate uses them.

To set up SSL termination, you must complete the following tasks:

1. Set up the private key.
2. Set up certificates.
3. Configure SSL on the virtual IP.

---

## Setting Up the Private Key for SSL termination

You set up a private key object to correspond to each primary certificate you need. The system supports using one private key to generate more than one primary certificate and the use of separate private keys for individual primary certificates.

You need access to your private key file. The LineRate software supports keys in PEM format.

We recommend giving each key a meaningful name that helps identify the key. For example, you might use the domain name or security settings in the name.

In this example, we will create a key object in the configuration, give it a name (key\_secure.example.com), and paste the key text into it.



### To set up the private key for SSL termination:

1. Open the private key file in a text editor and copy the text.
2. In another window, log in to LineRate using SSH.
3. Type:  
**configure**
4. Type:  
**key key\_secure.example.com**
5. Type:  
**pem-format**
6. Paste the text from the private key file and press **Enter**.
7. Type:  
**quit**
8. Type:  
**write**



**Note:** When installing an SSL certificate on the LineRate, you must remove any passphrases from the certificate file.

When the system first starts the SSL web service, it cannot wait for user input to enter a passphrase before the services will start.



#### To remove a passphrase using openssl:

1. Make a copy of your SSL key file keeping the original intact.
2. Use openssl to enter the passphrase and output a new key file:  
`openssl rsa -in key.pem -out newkey.pem`
3. Use this new file newkey.pem as your SSL private key for upload into LineRate.

## Setting Up Certificates for SSL Termination

To set up certificates, you must have access to your certificate files. The LineRate software supports PEM format certificates. You must configure the primary certificate that identifies the virtual IP on LineRate and the chain of certificates that lead to the root certificate that a client will trust.

We recommend giving each certificate a meaningful name that helps identify the certificate. For example, you might use the domain name or security settings in the name.

In this example, we will assume that your primary certificate only requires a single chain certificate. So we will create two certificate objects in the configuration, give them names (cert\_prim\_secure.example.com and cert\_chain\_secure.example.com1, as shown below), and paste the certificate text into them.



#### To set up certificates for SSL termination:

1. Open the primary certificate file in a text editor and copy the text.
2. Type:  
`configure`
3. Type:  
`certificate cert_prim_secure.example.com`
4. Type:  
`pem-format`
5. Paste the text from the certificate file and press Enter.
6. Type:  
`quit`
7. Open the second certificate file in a text editor and copy the text.
8. Type:  
`certificate cert_chain_secure.example.com1`

9. Type:  
**pem-format**
10. Paste the text from the certificate file and press Enter.
11. Type:  
**quit**
12. Type:  
**show cert brief**  
Certificate Subject Common Name (CN)  
-----  
cert\_chain\_secure.example.com1 Example Corp Intermediate CA  
cert\_prim\_secure.example.com secure.example.com  
self-signed lros-default-host  
Certificate Bundle  
-----
13. Type:  
**write**

---

## Configuring SSL Termination

After you set up the private key and certificates you can create an SSL profile and attach it to a virtual IP.

In this example, `cert_prim_secure.example.com` is the certificate that identifies the website "secure.example.com" and `cert_chain_secure.example.com1` is the chain certificate required for that primary certificate. We have to create an SSL profile (`ssl_prof_secure.example.com`) and attach the private key, and the certificates to it. We then attach the SSL profile to the virtual IP. We recommend giving each profile a meaningful name that helps identify it. For example, you might use the domain name or security settings in the name.

Attaching an SSL profile to a virtual IP configures that virtual IP to always use SSL. It will no longer accept connections from clients unless they perform SSL negotiation.



### To configure SSL termination:

1. Type:  
**configure**
2. Type:  
**ssl profile ssl\_prof\_secure.example.com**
3. Type:  
**attach private-key key\_secure.example.com**
4. Type:  
**attach primary-certificate cert\_prim\_secure.example.com**
5. Type:  
**attach chain-certificate cert\_chain\_secure.example.com1**

6. Type:  
**virtual-ip vipweb1**
7. Type:  
**attach ssl profile ssl\_prof\_secure.example.com**
8. Type:  
**show virtual-ip vipweb1**  
Configuration  
Address: 192.0.2.1:443 set locally  
Admin Status: offline default  
SSL Profile: ssl\_prof\_secure.example.com set locally  
...
9. Type:  
**show run brief**  
...  
ssl profile ssl\_prof\_secure.example.com  
attach primary-certificate cert\_prim\_secure.example.com  
attach private-key key\_secure.example.com  
attach chain-certificate cert\_chain\_secure.example.com1  
...  
certificate cert\_chain\_secure.example.com1  
! Cert data not shown in brief output  
!  
certificate cert\_prim\_secure.example.com  
! Cert data not shown in brief output  
!  
certificate self-signed  
! Cert data not shown in brief output  
!  
key key\_secure.example.com  
! Key data not shown in brief output  
!  
key self-signed  
! Key data not shown in brief output  
...
10. Type:  
**write**

---

## Configuring SSL Initiation

In many cases, the default settings for SSL initiation work well.

In this example, we will set up the SSL initiation profile (ssl\_prof\_init1), using the defaults, and attach it to the real server base (rsbase\_web). We recommend giving each profile a meaningful name that helps identify it. For example, you might use the security settings in the name.

Attaching an SSL profile to a real server configures that real server to always use SSL. If the web server is not configured to accept an SSL connection from the LineRate system, the system will not be able to send traffic to that web server.



### To configure SSL initiation:

1. Type:  
`configure`
2. Type:  
`ssl profile ssl_prof_init1`
3. Type:  
`real-server base rsbase_web`
4. Type:  
`attach ssl profile ssl_prof_init1`
5. Type:  
`show run brief`  
...  
real-server base rsbase\_web  
admin-status online  
max-connections 100  
idle-timeout 10  
service http  
response-timeout 60  
response-idle-timeout 60  
keepalive-timeout 10  
attach ssl profile ssl\_prof\_init1  
attach health-monitor hmweb  
...
6. Type:  
`write`

---

## SSL Example

After configuring SSL, as described above, you can use the `show run brief` command to see the configuration. We have annotated the SSL configuration in the example command output below. Comment lines start with an exclamation mark (!).

```
example-host(config)# show run brief
```

```
Building configuration...
```

```
!  
hostname example-host  
!  
username admin secret encrypted "$2a$04$7TYufYOKVQ8i8bblVtZ1ierxZXzcH5mR/  
QeaZH8WnWRzVEkPt0MgS" uid 2000
```

```

!
interface em0
ip address 10.200.0.1 255.255.255.0
!
interface em1
ip address 192.0.2.1 255.255.255.0
!
interface em2
ip address 10.1.2.1 255.255.255.0
!
ip route 0.0.0.0/0 192.0.2.2
!
health-monitor hm_web1
interval 5
timeout 1
server-down "8/10"
server-up "9/10"
type http
request-method GET
request-target "/health.html"
admin-status online
!
! Default certificate configuration remains unchanged.
!
ssl profile self-signed
attach primary-certificate self-signed
attach private-key self-signed
!
! Name of the SSL initiation profile we created.
!
ssl profile ssl_prof_init1
!
! Name of the SSL termination profile we created and the certificates and key
  configured.
!
ssl profile ssl_prof_secure.example.com
attach primary-certificate cert_prim_secure.example.com
attach private-key key_secure.example.com
attach chain-certificate cert_chain_secure.example.com1
!
! The real server shows the attached SSL initiation profile.
!
real-server base rsbase_web
admin-status online
max-connections 1000
service http
response-timeout 60
response-idle-timeout 60
keepalive-timeout 10
attach ssl profile ssl_prof_init1
attach health-monitor hm_web1
!
real-server rsweb1 ip 10.1.2.101 8080 base rsbase_web
real-server rsweb2 ip 10.1.2.102 8080 base rsbase_web

```

```

!
virtual-ip base vipbase_web1
admin-status online
service http
keepalive-timeout 5
!
! The virtual IP shows the attached SSL termination profile.
!
virtual-ip vipweb1
ip address 192.0.2.1 443
base vipbase_web1
attach ssl profile ssl_prof_secure.example.com
!
real-server group rsgroup_websilol
members by regex "rsw.*"
!
virtual-server websilol
lb-algorithm round-robin-free
service http
attach virtual-ip vipweb1 default
attach real-server group rsgroup_websilol
!
ssh
allow from 10.200.0.0/24
allow to 10.200.0.1 22
!
rest-server
allow from any
allow to any 8443
attach ssl profile self-signed
!
! The certificates and key we set up are listed, but the details do not display in the
  brief show output.
! The default certificate and key (self-signed) remain unchanged.
!
certificate cert_chain_secure.example.com1
! Cert data not shown in brief output
!
certificate cert_prim_secure.example.com
! Cert data not shown in brief output
!
certificate self-signed
! Cert data not shown in brief output
!
key key_secure.example.com
! Key data not shown in brief output
!
key self-signed
! Key data not shown in brief output

```

---

## What's Next

After you have completed all the sections of *Configuring a Reverse Proxy*, you have a basic load balancing setup that uses SSL, as shown in [Configuring Load Balancing](#).

For the complete configuration, see [Complete Example Show Run Output](#).

---

## Complete Example Show Run Output

1. [Overview](#)
2. [Show Run Brief of Example Configuration](#)
3. [What's Next](#)

---

### Overview

This section provides a complete, annotated **show run brief** output of the whole configuration example in this guide. Lines starting with ! are annotations added to help explain the output.

---

### Show Run Brief of Example Configuration

```
example_host(config)# show run brief
```

```
Building configuration...
!
! Hostname setting.
!
hostname example_host
!
! Default user name and encrypted password.
!
username admin secret encrypted "$2a$04$7TYufYOKVQ8i8bb1VtZ1ierxZXzcH5mR/
  QeaZH8WnWRzVEkPt0MgS" uid 2000
!
! IP address configured on the interface called em0 for management access.
!
interface em0
  ip address 10.200.0.1 255.255.255.0
!
! IP address configured on the interface called em1 for data.
!
interface em1
  ip address 192.0.2.1 255.255.255.0
!
! IP address configured on the interface called em2 for data.
!
interface em2
  ip address 10.1.2.1 255.255.255.0
!
! Default route configured for a router at 192.0.2.2.
!
```

```

ip route 0.0.0.0/0 192.0.2.2
!
! Health monitor and its configuration.
!
health-monitor hm_web1
  interval 5
  timeout 1
  server-down "8/10"
  server-up "9/10"
  type http
    request-method GET
    request-target "/health.html"
  admin-status online
!
! Default certificate configuration remains unchanged.
!
ssl profile self-signed
  attach primary-certificate self-signed
  attach private-key self-signed
!
! Name of the SSL initiation profile we created.
!
ssl profile ssl_prof_init1
!
! Name of the SSL termination profile we created and the certificates and key
  configured.
!
ssl profile ssl_prof_secure.example.com
  attach primary-certificate cert_prim_secure.example.com
  attach private-key key_secure.example.com
  attach chain-certificate cert_chain_secure.example.com1
!
! Real server base and its configuration.
!
real-server base rsbase_web
  admin-status online
  max-connections 1000
  service http
    response-timeout 60
    response-idle-timeout 60
    keepalive-timeout 10
  attach ssl profile ssl_prof_init1
  attach health-monitor hm_web1
!
! Real servers showing their names, IP addresses, and base in a single line for each.
!
real-server rsweb1 ip 10.1.2.101 8080 base rsbase_web
real-server rsweb2 ip 10.1.2.102 8080 base rsbase_web
!
! Virtual IP base and its configuration.
!
virtual-ip base vipbase_web1
  admin-status online
  service http

```

```

    keepalive-timeout 5
!
! Virtual IP and its configuration.
!
virtual-ip vipweb1
    ip address 192.0.2.1 443
    base vipbase_web1
    attach ssl profile ssl_prof_secure.example.com
!
! Real server group showing the regular expression used for group members.
!
real-server group rsgroup_websilol
    members by regex "rsw.*"
!
! Virtual server and its configuration.
!
virtual-server websilol
    lb-algorithm round-robin-free
    service http
    attach virtual-ip vipweb1 default
    attach real-server group rsgroup_websilol
!
! SSH configuration to limit access to the LineRate system.
!
ssh
    allow from 10.200.0.0/24
    allow to 10.200.0.1 22
!
! Default REST server configuration.
!
rest-server
    allow from any
    allow to any 8443
    attach ssl profile self-signed
!
! The certificates and key we set up are listed, but the details do not display in the
    brief show output.
! The default certificate and key (self-signed) remain unchanged.
!
certificate cert_chain_secure.example.com1
    ! Cert data not shown in brief output
!
certificate cert_prim_secure.example.com
    ! Cert data not shown in brief output
!
certificate self-signed
    ! Cert data not shown in brief output
!
key key_secure.example.com
    ! Key data not shown in brief output
!
key self-signed
    ! Key data not shown in brief output

```

---

## What's Next

Use the other sections of the [Getting Started Guide](#) to walk through this example configuration. Refer to the [CLI Reference Guide](#) for information about individual commands.