FORCEPOINT
POWERED BY Raytheon

V-Series Appliance Manager Help

TRITON AP-WEB, TRITON AP-EMAIL, Web Filter & Security

Models: V10000, V5000

v8.2.x

10900-A Stonelake Blvd, Quarry Oaks 1, Suite 350, Austin, TX 78759, USA

R042616820

Published 2016
Printed in the United States and Ireland

Every effort has been made to ensure the accuracy of this manual. However, Forcepoint, makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. Forcepoint LLC, shall not be liable for any error or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or the examples herein. The information in this documentation is subject to change without notice.

Trademarks

Forcepoint and TRITON are registered trademarks of Forcepoint LLC, in the United States and certain international markets. Forcepoint has numerous other unregistered trademarks in the United States and internationally. All other trademarks are the property of their respective owners.

Microsoft, Windows, Windows Server, and Active Directory are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Mozilla and Firefox are registered trademarks of the Mozilla Foundation in the United States and/or other countries.

Adobe, Acrobat, and Acrobat Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Red Hat is a registered trademark of Red Hat, Inc., in the United States and other countries. Linux is a trademark of Linus Torvalds, in the United States and other countries.

This product includes software distributed by the Apache Software Foundation (http://www.apache.org).

Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are the sole property of their respective manufacturers.

Contents

1 V-Series Overview

Help | V-Series Appliance | v8.2.x

Related topics:

- *Accessing the Appliance manager and other consoles*, page 5
- *V-Series appliance general system status*, page 9
- *V-Series appliance system configuration*, page 15
- *V-Series Appliance Administration*, page 43

The V-Series™ appliance hosts software that analyzes web traffic, email traffic, or both in real-time and applies security policies.

Modules available on the appliance

Regardless of whether the appliance hosts web protection software, email protection software, or both, it always includes an Appliance Controller module. This module includes:

- The Appliance manager, used to configure appliance settings, monitor system performance, manage services, perform system backups, apply hotfixes and upgrade patches, and perform diagnostic tasks.
- The Appliance command line (CLI) and command line utility (CLU), which offer command-line access to diagnostic utilities and configuration options.

See *V-Series Appliance Configuration* and *V-Series Appliance Administration* for more information about managing the appliance via the management console, CLI, and CLU.

When TRITON® AP-WEB resides on the appliance, the following additional modules are enabled:

TRITON AP-WEB	Categorizes sites, identifies users, and uses the appropriate administrator-configured policy to manage users' Internet requests.
Network Agent	Internet traffic sniffer. Enforces security for protocols other than HTTP, HTTPS, and FTP.
Content Gateway	● Instantly categorizes new sites and dynamic content, proactively discovering security risks, and blocking unwanted content and malware per administrator configured policy. ● Provides advanced analytics—including rules, signatures, heuristics, and application behaviors—to detect and block proxy avoidance, hacking sites, adult content, botnets, keyloggers, phishing attacks, spyware, and many other types of unsafe content. ● Closes a common security gap: decrypting and scanning SSL traffic before it enters the network.

When the TRITON AP-EMAIL module is enabled, it:

- Scans and manages incoming email messages to block spam or virus content per administrator configured policy.
- Integrates with TRITON AP-DATA solutions to help you monitor and restrict transmission of sensitive or inappropriate information via email.

Appliance security best practices

- Lock the appliance in an IT closet or data center and enable a BIOS password. Physical access to the appliance can be a security risk for your network.

  Using physical access to the appliance via serial console (KVM) to access the command line interface is protected by the administrator credentials after you finish running the **firstboot** script.
- Ensure that administrator credentials are restricted to a select few persons to help prevent unauthorized access to the system.
- Enable troubleshooting ports and permit remote access only when requested to do so by Technical Support. Return these settings to the disabled state immediately after the Technical Support specialist logs off.

TRITON management consoles

Help | V-Series Appliance | v8.2.x

Related topics:

- *Accessing the Appliance manager and other consoles*, page 5
- *Two-factor authentication and V-Series appliances*, page 6
- *Disabling and enabling Appliance manager password logon*, page 7

TRITON solutions include a combination of software that runs on-appliance and software that runs off-appliance. This is true both for security components and management components.

Management consoles that reside on the V-Series appliance

- The **Appliance manager** is used for system configuration and monitoring. Use this console to:
  - Monitor the status of software modules and appliance resources.
  - Establish assignments and routes for network interfaces.
  - Apply patches and hotfixes.
  - Run diagnostics, configure alerting, and perform other system troubleshooting.
- The **Content Gateway manager** is used to configure and manage the Content Gateway proxy used for TRITON AP-WEB real-time security analysis.

Management consoles that reside on a Windows server

The **TRITON Manager** runs off the appliance. It is the unified management console for TRITON on-premises web, data, and email protection solutions. Depending on which solutions you have installed, it may include the following modules:

Management module	Description	Used by (appliance modules)
TRITON Settings	Used to configure administrator accounts and other settings common to all other modules.	TRITON AP-WEB Web Filter & Security TRITON AP-EMAIL
Web module	Used to: ● Configure security policies ● Enable usage alerting ● Configure policy enforcement behavior ● Report on threats and user activity	TRITON AP-WEB Web Filter & Security Network Agent Content Gateway (analysis settings)
Email module	Used to: ● Configure email policies ● Enable usage alerting ● Report on email activity	TRITON AP-EMAIL
Data module	Used to: ● Configure data security policies ● Report on DLP incidents	None (TRITON AP-DATA components do not reside on the appliance.)

The TRITON Manager can be configured to provide single sign-on access to the V-Series Appliance manager and the Content Gateway manager.

- Appliances that are part of your TRITON installation are registered automatically on the TRITON console **Appliances** > **Manage Appliances** page. Information for each appliance includes:
  - C interface IP address
  - Hostname
  - Security Mode (Web, Email, or both Web and Email)
  - If Web is enabled, policy source mode (Full, Limited, or Filtering Only)
  - Software version (for example 8.1.0)
  - Hardware platform (for example V5000 G2R2, V10000 G3)
  - Appliance description
- Content Gateway instances are typically registered automatically on the **Settings** > **General** > **Content Gateway Access** page in the Web module of the TRITON console. This page includes:
  - The status of Content Gateway clustering

- Whether Policy Server can connect to Content Gateway
- The IP address of Content Gateway manager

  Click the Log On button to open Content Gateway manager in another tab or browser window.

You can also use this page to create a unique description for each Content Gateway instance for ease of management, or to delete obsolete Content Gateway entries after a server has been relocated or removed.

Accessing the Appliance manager and other consoles

Help | V-Series Appliance | v8.2.x

All TRITON management consoles support the following browsers:

- Microsoft Internet Explorer 9 (non-compatibility mode)
- Microsoft Internet Explorer 10 – 11 (standard mode)
- Microsoft Edge 15, 20, and 25
- Mozilla Firefox versions 4.4 – 44
- Google Chrome 13 – 49

✓ **Note**

If you are using Internet Explorer, ensure that Enhanced Security Configuration (IE ESC) is switched off.

Compatibility View is not supported.

Use any of the following methods to access the Appliance manager from a supported browser.

The user name is **admin**, and the password was set either when the **firstboot** script was run, or subsequently by an administrator. (To change the console password, see *Account management*.)

- **Direct access**

  If two-factor authentication is not configured, do one of the following:

  - Launch a Logon Portal to access the Appliance manager, Content Gateway manager, and the TRITON console from a single page:

    `https://<IP-address-of-interface-C>:9447/`

    Click the button for the management console you want to open.

  - Navigate directly to the Appliance manager using the following URL:

    `https://<IP-address-of-interface-C>:9447/appmng/`

  Note that direct access via the C interface IP address is disabled when two-factor authentication is configured.

- **Through the TRITON Manager** (not using two-factor authentication)
  1. Log on to the TRITON Manager:

     ```
     https://<IP-address-of-TRITON-machine>:9443/triton/
     ```

  2. Go to the **Appliances > Manage Appliances** page.
  3. If single sign-on is enabled, click the **Single Sign-On** button. The Appliance manager opens and you are logged on automatically.
  4. If no single sign-on option appears, click the C interface IP address. The Appliance manager logon screen is displayed. Enter your admin password to log on.
- **Using two-factor (certificate) authentication** via the TRITON Manager
  1. Log on to the TRITON Manager:

     ```
     https://<IP-address-of-TRITON-machine>:9443/triton/
     ```

  2. Go to the **Appliances > Manage Appliances** page in the TRITON Manager.
  3. Click the **Single Sign-On** button. The Appliance manager opens and you are logged on automatically.

  When two-factor authentication is enabled, appliance single sign-on must also be enabled to allow access to the Appliance manager from the TRITON console.

  - For information about configuring single sign-on, see Configuring an existing appliance for single sign-on in the TRITON Manager Help.
  - Direct access via the C interface IP address is disabled when two-factor authentication is configured. See *Two-factor authentication and V-Series appliances*.

Two-factor authentication and V-Series appliances

Help | V-Series Appliance | v8.2.x

Two-factor authentication:

- Is configured for and applies to TRITON console logon.
- Requires administrators to perform certificate authentication to log on.
- Can be made to apply to the Appliance manager and Content Gateway manager by forcing administrators to log on to the TRITON console before accessing other consoles.
- Requires single sign-on to be configured for administrators allowed access to the Appliance manager console and Content Gateway manager.
- Requires that the password logon capability be **disabled** with an appliance Command Line Interface command. This prevents administrators not configured for single sign-on from accessing the Appliance manager and Content Gateway manager.

Configuration is described in detail in Configuring two-factor authentication in the TRITON Manager Help.

Disabling and enabling Appliance manager password logon

Help | V-Series Appliance | v8.2.x

Appliance manager password logon can be disabled to allow only two-factor authentication or single sign-on access from the TRITON Manager.

To disable appliance password logon:

1. Use the **Appliances > Manager Appliances** page in the TRITON console to set up single sign-on.
2. If two-factor authentication will be used, configure it on the **TRITON Settings > Two-Factor Auth** page in the TRITON console.
3. Access the appliance Command Line Interface and log on with **admin** credentials.
4. At the command line, enter:

   ```
   password-logon disable
   ```
5. Log off and verify that direct logon is disabled by entering the IP address of the Logon Portal in your browser. The Logon Portal should not include links to the V-Series console or Content Gateway manager.

To re-enable password logon for all administrators:

1. Access the appliance Command Line Interface and log on with the admin credentials.
2. At the command line, enter:

   ```
   password-logon enable
   ```

Note

✓ If for some reason the appliance loses its registration with the TRITON console, password logon is automatically re-enabled.

Databases used on V-Series appliances

Help | V-Series Appliance | v8.2.x

TRITON software handles Internet and email activity based on your active policies **and** information stored in databases that must be updated at regular intervals.

- Residing in the TRITON AP-WEB or Web Filter & Security module of the appliance, the **Master Database** contains URL category information and protocol definitions. It is managed by Filtering Service. Administrators can control how often the database is updated, and whether or not partial, real-time updates are applied between full updates. (See The Master Database for details.)

  A limited, initial version of the Master Database is pre-installed on the appliance. Download the full Master Database as soon as possible to enable comprehensive

Internet security capabilities. See the V-Series Getting Started Guide after you complete initial setup of the appliance.

When TRITON AP-EMAIL is deployed with a web protection solution, the Email module can query the **Master Database** to get the category of URLs embedded in email content.

- Content Gateway analytic and categorization options rely on a set of databases installed with software. The software checks for updates to these databases at a regular interval. Updates to these databases occur independently of all Master URL Database updates.

  Every time you restart the appliance or the Content Gateway module, a download of these small databases is initiated. If that download fails, a new download is attempted every 15 minutes until a successful download occurs.
- TRITON AP-EMAIL uses a configurable set of antispam and antivirus databases. The software checks for updates to these databases at a regular interval. You can initiate updates manually from within the Email console.

Navigating in the Appliance manager

Help | V-Series Appliance | v8.2.x

The Appliance manager opens showing the **Status > General** page in the content pane (see *V-Series appliance general system status* for more information).

The banner at the top of the page displays the appliance platform and hostname, icons that indicate the security mode, and a Log Off button.

- To navigate to another page, select any entry in the left navigation pane.
- To get a detailed explanation of the options on any page, go to **Help > Explain This Page**.

The Appliance manager offers access to the following functionality:

- Status
  - *V-Series appliance general system status*
  - *V-Series appliance CPU and memory status*
  - *V-Series appliance disk use by module*
  - *V-Series appliance network bandwidth*
- Configuration
  - *V-Series appliance system configuration*
  - *V-Series appliance network interface configuration*
  - *V-Series appliance routing configuration*
  - *V-Series appliance alerting*
  - *Configuring V-Series appliance Web components*

- Administration
  - *V-Series appliance patch management*
  - *V-Series appliance hotfix management*
  - *Using the V-Series appliance backup utility*
  - *V-Series appliance log files*
  - *V-Series appliance tools*
  - *Account management*

V-Series appliance general system status

Help | V-Series Appliance | v8.2.x

The **Status** > **General** page displays first when you log on to the Appliance manager. It presents the current status of each software module on the appliance.

Use this page to:

- Check for system alerts, including information about new patches.
- Gauge resource use by each module, including:
  - How many CPUs are dedicated to the module.
  - How much memory (RAM) is allocated.
  - Which appliance interfaces are used by the module (for example, C, P1).
  - Which services (daemons), if any, are included in the module.
- Stop and start software services, or restart or disable an entire software module.
- Restart or shut down the appliance itself.

Important

For security purposes, a logon session ends after 30 minutes of inactivity.

However, you can choose to monitor the **Status** pages even after the 30-minute timeout is reached. To do this, in the **Appliance Controller** section, mark the box labeled **Monitor status without timing out**. You are prompted to confirm your selection. Information on all **Status** pages then continues to update normally until you close the browser.

Modules on the V-Series may include:

- The **Appliance Controller** software operates behind the scenes. It manages appliance configuration, downloads and applies patches, accesses the backup utility, requests module restarts, initiates shutdowns, and handles other appliance management tasks.

- **Content Gateway** is the web proxy component. It also performs web content scanning and analysis. Several services (daemons) comprise this software.
- **TRITON AP-WEB** is the software that handles web analysis. Several services (daemons) comprise this software.
- **Network Agent** is the Web component that monitors Internet traffic and manages non-HTTP protocols such as instant messaging.
- **TRITON AP-EMAIL** is the software that handles email security. Several services (daemons) comprise this software.

The links and buttons on the page allow you to perform the following tasks:

Button or Link	Description
View Patch	Appears when an alert indicates that a new patch is available. Click the button to go to the **Administration** > **Patches / Hotfixes** page, where you can view a list of available patches.
Restart Appliance	Reboot the appliance. All enabled modules are stopped, then restarted.
Shutdown Appliance	Shut down this appliance and all of its software modules in an orderly fashion.
Restart (Content Gateway)	Stop and restart all services in the Content Gateway module on this appliance.
Launch (Content Gateway manager)	Launch the Content Gateway manager in a new browser tab or window. See *TRITON management consoles*.
Stop Services Start Services (Content Gateway)	Stop or start all proxy services and content analysis in the Content Gateway module on this appliance.
Restart (TRITON AP-WEB)	Stop and restart all services in use within the TRITON AP-WEB module on this appliance.
Stop Services Start Services (TRITON AP-WEB)	Stop or start all TRITON AP-WEB services running on this appliance. **Note:** If this appliance is not designated to be the Full policy source for your network, some services may not be in use.
Restart (Network Agent)	Stop and then restart the Network Agent service on this appliance.

Button or Link	Description
Disable Enable (Network Agent)	Not all deployments use Network Agent. Disabling it redistributes system resources (CPU and memory) to other modules on the appliance. The Disable option displays only when Network Agent is running on a TRITON AP-WEB appliance. Network Agent cannot be disabled on a Web Filter & Security appliance. It is a good idea to perform a full system backup (including the policy source machine) before you temporarily or permanently disable Network Agent, in case you need to re-enable the component in the future. When you click Disable, you are given two options: ● Permanently disable the module When Network Agent is permanently disabled, the appliance must be **re-imaged** in order to regain the ability to use Network Agent on the appliance. See *Re-enabling Network Agent if permanently disabled*. ● Temporarily disable the module. When Network Agent is temporarily disabled, a flag is set to indicate that Network Agent should be shut down on the appliance and not restarted the next time the appliance is restarted. **Note:** An important side effect of temporarily disabling Network Agent is that it must be re-enabled before you change the policy source, change the C interface IP address, or apply a patch. On average, it takes 10 minutes to re-enable Network Agent. When Network Agent is in the temporarily disabled state, both the Enable and Permanently Disable buttons display. For an introduction to the purpose of Network Agent, see *Configuring V-Series Network Agent Interface (N)*, page 23.
Stop Services Start Services (Network Agent)	Stop or start the Network Agent service on this appliance.
Restart (TRITON AP-EMAIL)	Stop and then restart all TRITON AP-EMAIL services on this appliance.
Stop Services Start Services (TRITON AP-EMAIL)	Stop or start all TRITON AP-EMAIL services on this appliance.

Re-enabling Network Agent if permanently disabled

If Network Agent is permanently disabled and you want to re-enable it, you must re-image the appliance. This wipes the current system and restores the original, unconfigured system image. See *Restoring to factory image* in the V-Series Getting Started Guide.

After re-imaging, you can apply patches and restore a full backup or module-level backups. If you restore a full backup, the backup must have been made when Network

Agent was enabled, otherwise the restore will fail because the configured systems are incompatible.

V-Series appliance CPU and memory status

Help | V-Series Appliance | v8.2.x

The **Status > CPU and Memory** page provides information about CPU and memory use by each software module running on this appliance, for the previous 60 seconds.

- **CPU Usage** displays:
  - An aggregate of all CPU usage during the previous 60 seconds, based on occupied resources and total available resources for the module
  - The percentage of each available CPU used by the module during the previous 60 seconds
- **Memory Usage** displays the:
  - Percentage of available memory used by the module during the previous 60 seconds
  - Actual memory used by the module during the previous 60 seconds, in megabytes
  - Total memory available to this module during the previous 60 seconds, in megabytes

V-Series appliance disk use by module

Help | V-Series Appliance | v8.2.x

The **Status > Disk Usage** page provides a summary of the previous 60 seconds of disk activity, as well as information about overall disk space availability, for each module on this appliance.

- **Disk Activity** shows average input/output operations per second (IOPS) and charts the previous 60 seconds of activity.
- **Usage Statistics** shows disk space used and available within the module.

The sections for the Appliance Controller, TRITON AP-WEB, and Network Agent modules show one summary of information for all components within the module. This is represented as **system** disk activity or usage.

The section for the Content Gateway module may also show information for cache and PreciseID disk activity and usage.

- The cache consists of a high-speed object database called the **object store**. The object store indexes objects according to URLs and associated headers, enabling Content Gateway to store, retrieve, and serve web pages, and also parts of web pages, providing optimum bandwidth savings. If the cache disk fails, Content Gateway goes into proxy-only mode (no caching).

- When Content Gateway integrates with TRITON AP-DATA, PreciseID Fingerprinting is used to detect sensitive information despite manipulation, reformatting, or other modification.

In addition to overall system information, the TRITON AP-EMAIL section also shows disk activity and usage information for the mail transfer agent (MTA) responsible for sending, receiving, and directing email messages.

V-Series appliance network bandwidth

Help | V-Series Appliance | v8.2.x

The **Status > Network Bandwidth** page provides information about throughput on the appliance network interfaces listed here:

- **Appliance Controller Interface** (C)
- **Content Gateway Interface** (P1) or (P1 and E1)
- **Content Gateway Interface** (P2) or (P2 and E2)
- **Network Agent Interface** (N)
- **TRITON AP-EMAIL** (E1) or (E1 and P1)
- **TRITON AP-EMAIL** (E2) or (E2 and P2)

Interfaces E1 and E2 are included on the V10000 models only. The disposition of P1, P2, E1 and E2 is dependent on the modules installed or the configuration applied. For information about configuring the interfaces, see *V-Series appliance network interface configuration*. The bandwidth display includes them only if they are enabled.

For each interface, the following information is displayed for the previous 60 seconds:

- Inbound/Outbound
  - current megabits per second, inbound and outbound, on the interface
  - maximum bandwidth capacity in megabits per second
- Bandwidth Statistics
  - total megabits of data received and sent
  - total number of packets received and sent
  - packets dropped, inbound and outbound
  - total errors, inbound and outbound
  - rate in megabits per second, inbound and outbound

V-Series appliance system watchdog

Help | V-Series Appliance | v8.2.x

V-Series appliances implement a system watchdog daemon to monitor critical system processes and conditions. Should one of the monitored processes or conditions fail or fault, the watchdog service performs a reset or restart.

Monitored processes and states include:

- Appliance kernel: Is the kernel active?
- Domain Agent: Is the Domain Agent running?

  This is an essential process that is responsible for communicating between the user interface and appliance back-end processes.
- Journal Commit I/O: Detect a “journal commit I/O” error.
- File table: Detect a file table overflow condition.

Watchdog actions are recorded in the system log file, which can be viewed on the **Administration** > **Logs** page.

2 V-Series Appliance Configuration

Help | V-Series Appliance | v8.2.x

Use the Configuration section of the Appliance manager to:

- Set the appliance time and date, host name, and description (see *V-Series appliance system configuration*).
- Define the network interfaces for the appliance (see *V-Series appliance network interface configuration*). Depending on your model, this may include C, P1, P2, N, E1, and E2.
- Optionally specify static routes for Content Gateway, TRITON AP-EMAIL, or for the appliance itself (see *V-Series appliance routing configuration*).
- Set up SNMP alerting (see *V-Series appliance alerting*).
- Identify which computer is hosting security configuration and policies for the network (see *Configuring V-Series appliance Web components*).

V-Series appliance system configuration

Help | V-Series Appliance | v8.2.x

Use the **Configuration > System** page to:

- Review basic appliance information, including the current appliance hostname, security mode (Web, Email, or Web and Email), version number, hardware platform, system date and time, and uptime.
- See which software modules are installed on the appliance and get their version numbers.

- Update the system **time and date**, either by manually entering a date and time, or by specifying which Network Time Protocol (NTP) servers to use to synchronize the appliance date and time.

  Important

  If any TRITON services are running:

  1. **Stop all TRITON services** before changing the time.
  2. Make your changes, making sure to keep the time consistent across **all servers**.
  3. Restart all TRITON services.

  If you do not stop the services first, client updates and policy changes entered after the time reset are not saved.

  - Use the **Time zone** list to select the time zone to be used on this system.

    GMT (Greenwich Mean Time), the default, is also known as UTC (Universal Time, Coordinated). Other time zones are calculated by adding or subtracting from GMT. GMT is sometimes chosen to provide a common time stamp for geographically distributed systems.

  - Use the **Time and date** radio buttons to indicate how you want to set the date. Time is set and displayed using 24-hour notation.

    - To synchronize with an NTP server (www.ntp.org.), select the **Automatically synchronize** option and enter the address of a primary NTP server. The secondary and tertiary fields are optional.

      Important

      If you synchronize the system clock with an NTP server, NTP protocol packets and their response packets must be allowed on any firewall or NAT device between the appliance and the NTP server. Ensure that you have outbound connectivity to the NTP servers. Add a firewall rule that allows outbound traffic to UDP port 123 for the NTP server.

      If interface C on this appliance is not connected to the Internet, then you must provide a way for interface C to reach an NTP server. One solution is to install an NTP server on the local network where interface C can reach it.

    - To set the time yourself, select the **Manually set** option and change the value in the Date and Time fields. Use the format indicated below the entry field.

  - Click **OK** to apply and save the changes.

- Set the appliance **hostname**, or system name (1 - 60 characters long).

  - The first character must be a letter.

- Other characters can be letters, numbers, dashes, or periods.
- The name cannot end with a period.

Important

If this is a TRITON AP-WEB appliance and Content Gateway will be configured to perform Integrated Windows Authentication (IWA), the hostname cannot exceed 11 characters, excluding the domain name.

In addition, the hostname should not be changed after the domain is joined. If it is changed, IWA will immediately stop working and will not work again until the domain is unjoined and then re-joined with the new hostname.

For more information, see the section titled “Integrated Windows Authentication” in the Content Gateway Manager Help.

- Create or edit a unique **appliance description** to help you identify and manage the system, particularly when there are multiple appliances deployed in a cluster.

  The description is displayed in the appliance list in the TRITON Manager when the appliance is added there.

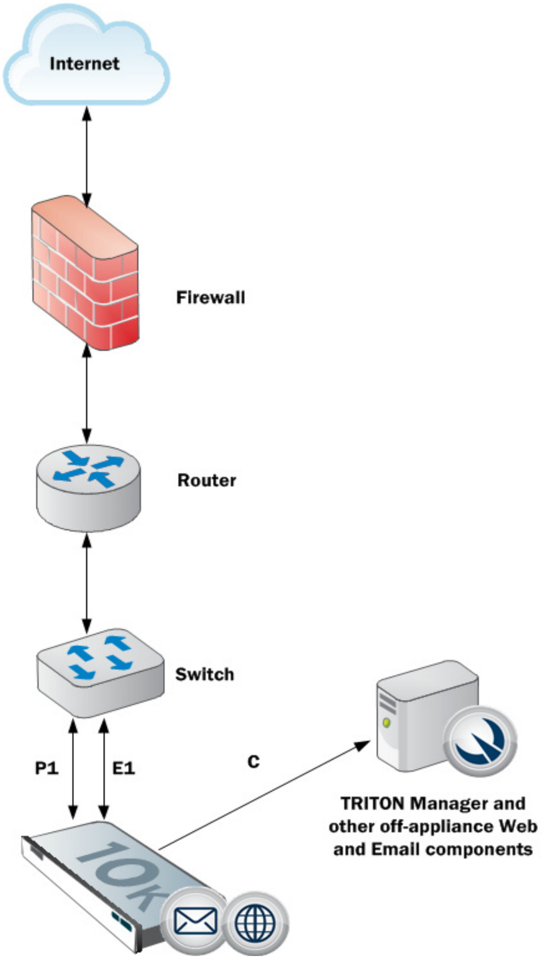
In each section that allows changes, **OK** saves and applies the new values. **Cancel** discards changes and restores entry field values to their current settings.

V-Series appliance network interface configuration

Help | V-Series Appliance | v8.2.x

Use the **Configuration > Network Interfaces** page to configure each network interface on the appliance.

- For more information about TRITON AP-WEB IPv6 support, see *V-Series support for IPv6*, page 19.
- For more information about TRITON AP-EMAIL support for virtual interfaces, see *V-Series appliance Email module virtual interfaces*, page 25.


Internet
Firewall
Router
Switch
P1
E1
C
TRITON Manager and other off-appliance Web and Email components
10k

For more information about configuring each appliance interface, see:

- *Configuring V-Series Appliance Controller interface (C)*
- *Configuring V-Series Content Gateway interfaces (P1 and P2)*
- *Configuring V-Series Network Agent Interface (N)*
- *Configuring V-Series TRITON AP-EMAIL interfaces (E1 and E2, or P1 and P2)*
- *V-Series appliance interface bonding*

Click **OK** to save and apply new values in each section.

V-Series support for IPv6

Help | V-Series Appliance | v8.2.x

Use the **Configuration > Network Interfaces > IPv6** pages to configure IPv6 support on V-Series appliances that host a web protection solution.

- TRITON AP-EMAIL does not include IPv6 support.
- IPv6 support is disabled by default.

Important

After you enable it, **disabling IPv6 support again requires a full restart of the appliance.**

When you enable, then disable IPv6 support, any existing IPv6 values remain in the configuration files, but they cannot be edited.

For all web protection solutions, IPv6 support includes:

- Dual IP stack configuration for interfaces C and N
- IPv6 traffic to the Internet or clients on interfaces C and N, including block pages sent on C or N
- IPv6 static routes
- SNMP traps and counters for IPv6 data
- Network diagnostic tools in the Command Line Utility and Command Line Interface

For TRITON AP-WEB, IPv6 support also includes:

- Dual IP stack implementation on interfaces P1 and P2
- Traffic to the Internet or clients on interfaces P1 and P2, and their bonded interface (E1/E2), if configured

Limits and restrictions:

- IPv6-only internal networks are not supported
- IPv4 must be used to communicate among V-Series appliances and with TRITON components

In any field that accepts an IPv6 address, the address can be entered in any format that conforms with the standard. For example:

- Leading zeros within a 16-bit value may be omitted.
- One group of consecutive zeros may be replaced with a double colon.

Configuring V-Series Appliance Controller interface (C)

Help | V-Series Appliance | v8.2.x

The Appliance Controller interface (C):

- Communicates with all TRITON management interfaces
- Communicates with the TRITON management server and TRITON AP-DATA (if used)
- Provides inter-appliance communication
- Optionally provides non-HTTP(S) protocol enforcement
- Handles Master Database downloads via the Internet (unless you optionally configure P1 for database downloads. For more information, see *Configuring Master Database downloads to use P1*, page 31.)

Initial C interface configuration occurs when an administrator runs the **firstboot** script to set up the appliance.

Important

Changing the C interface IP address significantly impacts the deployment and may require reinstallation of some components.

If your appliance is in production and you need to change the C interface IP address, see *Changing the C interface IP address*, page 27.

To enable the C interface IP address entry field, place the mouse pointer over the iHelp icon and click “Enable IP field” in the pop-up.

Guidelines for configuring network interface C

IP address (C interface)	Required This interface typically requires continual access to the Internet, though some sites use P1 for all communication with the Internet. If you change the IP address of the C interface, the update process may take about 10 minutes. After the IP address is changed, you are redirected to a logon page. Enter your user name and password. When you log on, the **Status** > **General** page will show that the services are starting up. Wait for all services to start.
Subnet mask (C)	Required
Default gateway (C)	Optional IP address of the router that allows traffic to be routed outside of the subnet

Primary DNS (C)	Required IP address of the domain name server
Secondary DNS (C)	Optional Serves as a backup in case the primary DNS is unavailable.
Tertiary DNS (C)	Optional Serves as a backup in case the primary and secondary DNSes are unavailable.

Configuring V-Series Content Gateway interfaces (P1 and P2)

Help | V-Series Appliance | v8.2.x

Content Gateway Interfaces (P1 and P2) handle traffic directed to and from the Content Gateway proxy module.

- Both the P1 and P2 proxy interfaces can be used to accept users' Internet requests (inbound traffic) and communicate with web servers (outbound traffic). In other words, both interfaces can be configured to handle traffic into and out of the proxy.
- Typically, P1 is used for both inbound and outbound traffic; P2 is not used.
- Optionally, configure P1 to accept users' Internet requests (inbound only) and P2 to communicate with web servers (outbound).

Important

If you use the P2 interface, the P1 interface is bound to eth0, and the P2 interface is bound to eth1. Keep this in mind when you configure Content Gateway.

For example, suppose you are using a transparent proxy deployment, and the P1 interface is connected to a WCCP router. In this case, you must configure Content Gateway to use eth0 for WCCP communications (in Content Gateway manager, see the General tab of the **Configure** > **Networking** > **WCCP** page).

Guidelines for configuring network interfaces P1 and P2

General guideline	The P1 and P2 interfaces can be in the same or different subnets. If they are in the same subnet, P2 is the default gateway (which is bound to eth1). Ensure that outbound packets can reach the Internet. When P1 and P2 are in different subnets, the gateway must be in the same subnet as the appliance interface used to send traffic to the Internet (typically P2). All traffic communicated between Content Gateway and origin servers should go through that interface (P2). For traffic communicated between Content Gateway and clients, please note: ● If the clients are in the same subnet as P1, then all traffic communicated between Content Gateway and clients should go through P1. ● If the clients are not in the same subnet as P1, then client-to-Content Gateway traffic goes through P1, while Content Gateway-to-client traffic goes through P2, regardless of whether an explicit or transparent deployment is used. Note, however, that you can set up static routes to send client traffic (on subnets not attached to P1) back through P1 (inbound traffic).
IP address (P1 or P2 interface)	Required
Subnet mask	Required
Default gateway	Required The gateway must be in the same subnet as the IP address of the interface (P1 or P2) used for communicating with the Internet (outbound traffic). If you use both P1 and P2, they must be located in the same subnet. The default gateway is automatically assigned to P2 (which is bound to eth1). Ensure that outbound packets can reach the Internet.
Primary DNS	Required IP address of the domain name server
Secondary DNS	Optional Serves as a backup in case the primary DNS is unavailable
Tertiary DNS	Optional Serves as a backup in case the primary and secondary DNSes are unavailable

Configuring V-Series Network Agent Interface (N)

Help | V-Series Appliance | v8.2.x

Network Agent is a software component used to provide security for protocols other than HTTP and HTTPS. It also provides bandwidth optimization data and enhanced logging detail.

Network Agent continually monitors overall network usage, including bytes transferred over the network. The agent sends usage summaries to other TRITON components at predefined intervals.

Network Agent is typically configured to see both inbound and outbound traffic in your network. The agent distinguishes between:

- Requests sent from internal machines to internal machines (hits to an intranet server, for example)
- Requests sent from internal machines to external machines such as Web servers (user Internet requests, for example)

You choose whether blocking information for non-HTTP protocols is routed through interface C or interface N.

Guidelines for configuring network interface N

Select an interface to use to send blocking information for non-HTTP(S) traffic	● Select **Interface C** only if you want to use interface C to send blocking information. ● Select **Interface N** if network interface N is connected to a bidirectional span port, and you want to use N to transport blocking information. Blocking NIC settings configured in the Web module of the TRITON Manager **do not** override the settings you enter in the Appliance manager.
IP address of interface N	Required Network Agent should be able to see the outbound and inbound traffic in your network. Network Agent ignores ports 80, 443, 8070, and 8080.
Subnet mask	Required if interface N is selected; otherwise the subnet mask has a fixed value of 255.255.255.255
Default gateway	Required if interface N is selected; otherwise, the field is disabled
Primary DNS	Required IP address of the domain name server
Secondary DNS	Optional Serves as a backup in case the primary DNS is unavailable
Tertiary DNS	Optional Serves as a backup in case the primary and secondary DNSes are unavailable

Network Agent can instead be installed on a different server in the network. See the V-Series appliance Getting Started Guide for requirements.

Configuring V-Series TRITON AP-EMAIL interfaces (E1 and E2, or P1 and P2)

Help | V-Series Appliance | v8.2.x

TRITON AP-EMAIL interfaces handle bidirectional email protection traffic.

Note

The names of the interfaces vary depending on the model of V-Series appliance.

- With V10000, E1 and E2 are used.
- With V5000, P1 and P2 are used.

- Both the E1 and E2 interfaces (V10000) or P1 and P2 interfaces (V5000) can be used to accept inbound traffic and send outbound traffic.
- In many deployments, E1 (or P1) is used for both inbound and outbound traffic; E2 (or P2) is not used.
- E1 (or P1) can be configured to accept inbound traffic and E2 (or P2) can be configured to send outbound traffic.

When you need to support a large volume of outbound traffic, you can configure virtual interfaces on E1 or E2 (P1 or P2). See *V-Series appliance Email module virtual interfaces*, page 25.

Important

On the V10000, if you use the E2 interface, the E1 interface is bound to eth0, and the E2 interface is bound to eth1.

On the V5000, if you use the P2 interface, the P1 interface is bound to eth0, and the P2 interface is bound to eth1.

Keep this in mind when you configure TRITON AP-EMAIL.

Guidelines for configuring network interfaces E1 and E2

Note

On a V5000, substitute P1 for E1 and P2 for E2.

If you use both E1 and E2, and you locate them in the same subnet, then the default gateway is automatically assigned to E2 (which is bound to eth1). Ensure that outbound packets can reach the Internet.

IP address (E1 or E2 interface)	Required
Subnet mask	Required
Default gateway	Required The gateway must be in the same subnet as the IP address of the interface (E1 or E2) used for communicating with the Internet (outbound traffic). If you use both E1 and E2, and you locate them in the same subnet, then the default gateway is automatically assigned to E2 (which is bound to eth1). Ensure that outbound packets can reach the Internet.
Primary DNS	Required IP address of the domain name server
Secondary DNS	Optional Serves as a backup in case the primary DNS is unavailable
Tertiary DNS	Optional Serves as a backup in case the primary and secondary DNSes are unavailable

V-Series appliance Email module virtual interfaces

Help | V-Series Appliance | v8.2.x

Note

On a V5000, substitute P1 for E1 and P2 for E2.

Multiple virtual IP addresses can be configured on E1 or E2.

- Virtual IP addresses are used for outbound traffic only.
- Virtual IP addresses are bound to the specified physical interface.
- Virtual IP addresses must be in the same subnet as the specified physical interface.
- A maximum of 10 virtual IP addresses can be specified for each physical interface (E1 and E2).

Multiple virtual interfaces can be helpful to support multiple domains and/or a large volume of outbound traffic.

To add virtual IP addresses to E1 or E2:

1. Go to **Configure** > **Network Interfaces** > **Virtual Interfaces** and click **Add**.
2. Select E1 or E2. If E2 has not been configured, it is not offered.
3. In the Virtual IP address field, enter one IPv4 address per line.

4. Click **Add Interfaces**.

To remove virtual IP addresses:

1. On the **Configure > Network Interfaces > Virtual Interfaces** page, select the check box to the left of the entries you want to remove and then click **Delete**.
2. Confirm your action.

V-Series appliance interface bonding

Help | V-Series Appliance | v8.2.x

V10000 appliances that run only one product can bond interfaces for failover or load balancing, as described below.

Interface bonding is not supported on V5000 appliances.

Important

Do **not** bond interfaces that have different speeds or duplex modes. Doing so can result in performance problems.

V10000 with TRITON AP-WEB only

Interfaces E1 and E2 can be cabled to your network and then bonded through software settings to a Content Gateway interface, with E1 optionally bonded to P1, and E2 optionally bonded to P2. No other pairing is possible.

Interface bonding provides these alternatives:

- Active/Standby mode: P1 (or P2) is active, and E1 (or E2) is in standby mode. Only if the primary interface fails would its bonded interface (E1 or E2) become active.
- Load balancing: If the switch or router that is directly connected to the V10000 supports load balancing (etherchannel, trunk group, or similar), then traffic to and from the primary interface can be balanced between the primary interface and its bonded interface (E1 or E2).

You can choose to bond or not bond each Content Gateway interface independently. You do not have to bond at all.

If you do bond an interface, choose one mode for that bonding (either active/standby or load balancing). You do not have to choose the same bonding mode for both interfaces.

Ensure that all interfaces are cabled properly before bonding.

V10000 with TRITON AP-EMAIL only

Interfaces P1 and P2 can be cabled to your network and then bonded through software settings to a TRITON AP-EMAIL interface, with P1 optionally bonded to E1, and P2 optionally bonded to E2. No other pairing is possible.

Interface bonding provides these alternatives:

- Active/Standby mode: E1 (or E2) is active, and P1 (or P2) is in standby mode. Only if the primary interface fails would its bonded interface (P1 or P2) become active.
- Load balancing: If the switch or router that is directly connected to the V10000 supports load balancing (etherchannel, trunk group, or similar), then traffic to and from the primary interface can be balanced between the primary interface and its bonded interface (P1 or P2).

You can choose to bond or not bond each TRITON AP-EMAIL interface independently. You do not have to bond at all.

If you do bond an interface, choose one mode for that bonding (either active/standby or load balancing). You do not have to choose the same bonding mode for both interfaces.

Ensure that all interfaces are cabled properly before bonding.

Changing the C interface IP address

Help | V-Series Appliance | v8.2.x

If possible, do not change the C interface IP address. The number of activities that must be performed and the service disruption can be significant.

Sometimes it is necessary to change the C interface IP address. What is affected depends on the configuration of your appliances and the details of your deployment.

In most cases, off-box components that depend on or directly service an appliance should be uninstalled prior to changing the C interface IP address and reinstalled after the IP address change is complete. These components include:

- TRITON Manager
- Filtering Service
- Network Agent
- Real Time Monitor
- DC Agent
- Logon Agent
- eDirectory Agent
- Radius Agent
- Remote Filtering Service
- Sync Service

- Linking Service

This document includes a summary of the considerations for 5 deployment scenarios when the C interface changes. See the technical paper V-Series: Changing the C Interface IP Address: Step-By-Step for more details.

Important

Back up your appliance and all affected off-box components before making any changes.

Find the scenario below that best matches your deployment for an overview of the update process.

- *Scenario 1: One TRITON AP-WEB-only appliance with two Windows servers (TRITON Manager and Log Server)*
- *Scenario 2: One or many TRITON AP-EMAIL appliances with two Windows servers (TRITON Manager and Log Server)*
- *Scenario 3: One TRITON AP-WEB and TRITON AP-EMAIL appliance with two Windows servers (TRITON Manager and Log Servers)*
- *Scenario 4: Multiple TRITON AP-WEB appliances in a cluster with two Windows servers (TRITON Manager and Log Server)*
- *Scenario 5: Multiple TRITON AP-WEB appliances in a cluster with off-box Policy Broker, TRITON Manager, and Log Server*

Scenario 1: One TRITON AP-WEB-only appliance with two Windows servers (TRITON Manager and Log Server)

1. If your deployment includes Web DLP, in the Content Gateway manager manually unregister Content Gateway with TRITON AP-DATA.
2. On the Windows server that hosts Log Server, stop the Log Server service.
3. On the TRITON management server machine, uninstall the TRITON Manager services and any other components from the list in the introduction to this topic that are on the machine. Make a list of uninstalled components.
4. On the appliance, change the C interface IP address.
5. Reinstall the TRITON management server components.
6. On the Log Server host, change the IP address of the Policy Server entry in the **websense.ini** file to the new C interface IP address and restart Log Server.
7. If your deployment includes Web DLP, restart the Content Gateway module to automatically re-register with the TRITON AP-DATA components.

Scenario 2: One or many TRITON AP-EMAIL appliances with two Windows servers (TRITON Manager and Log Server)

1. If your deployment includes Email DLP, unregister Email DLP.
2. On the appliance, change the C interface IP address.

3. In the Email module of the TRITON Manager, change the appliance IP address to the new value.
4. If your deployment includes Email DLP, re-register Email DLP.

Scenario 3: One TRITON AP-WEB and TRITON AP-EMAIL appliance with two Windows servers (TRITON Manager and Log Servers)

1. If your deployment includes Web DLP, in the Content Gateway manager manually unregister Content Gateway with TRITON AP-DATA.
2. If your deployment includes Email DLP, unregister Email DLP.
3. On the Windows server that hosts your Log Server instances, stop the Log Server and Email Log Server services.
4. On the TRITON management server, uninstall the TRITON Manager services and any other components from the list in the introduction to this topic that are on the machine. Make a list of uninstalled components.
5. On the appliance, change the C interface IP address.
6. Reinstall the TRITON management server components.
7. On the Log Server host, change the IP address of the Policy Server entry in websense.ini to the new C interface IP address and restart both Log Server instances.
8. In the Email module of the TRITON Manager, change the appliance IP address to the new value.
9. If your deployment includes Email DLP, re-register with TRITON AP-DATA components.
10. If your deployment includes Web DLP, restart Content Gateway to automatically re-register with the TRITON AP-DATA components.

Scenario 4: Multiple TRITON AP-WEB appliances in a cluster with two Windows servers (TRITON Manager and Log Server)

This provides a summary of the steps for each of the following:

- Changing the C interface of the full policy source appliance
- Changing the C interface of user directory and filtering appliances
- Changing the C interface of filtering only appliances

Changing the C interface of the full policy source appliance

1. If your deployment includes Web DLP, in the Content Gateway manager manually unregister Content Gateway with TRITON AP-DATA.
2. On the Windows server that hosts Log Server, stop the Log Server service.
3. On the TRITON management server machine, uninstall the TRITON Manager services and any other components from the list in the introduction to this topic that are on the machine. Make a list of uninstalled components.
4. Document the current policy source settings of all appliances in the cluster.

5. Change the policy source setting on all user directory and filtering and filtering only appliances to **Full policy source**.
6. On the original full policy source appliance, change the C interface IP address.
7. Re-apply the original policy source settings to each user directory and filtering and filtering only appliance, pointing the appliance to the new full policy source C interface IP address.
8. Reinstall the TRITON management server components.
9. On the Log Server host, change the IP address of the Policy Server entry in the **websense.ini** file to the new C interface IP address and restart Log Server.
10. If your deployment includes Web DLP, restart the Content Gateway module to automatically re-register with the TRITON AP-DATA components.

Changing the C interface of the user directory and filtering appliance

1. Uninstall off-box components (like DC Agent) that are registered to the user directory and filtering appliance whose C interface IP address will change.
2. Temporarily change the policy source mode of any filtering only appliances that depend on the user directory and filtering appliance whose C interface IP address will change to full policy source appliances.
3. Change the C interface IP address of the user directory and filtering appliance.
4. Re-apply the original policy source setting to the filtering only appliances, pointing them to the new user directory and filtering C interface IP address.
5. Reinstall off-box components that are registered to the user directory and filtering appliance.

Changing the C interface of the filtering only appliance:

1. Uninstall off-box components (like Network Agent) that are registered to the filtering only appliance whose C interface IP address will change.
2. Change the C interface IP address.
3. Reinstall off-box components that are registered to the filtering only appliance.

Scenario 5: Multiple TRITON AP-WEB appliances in a cluster with off-box Policy Broker, TRITON Manager, and Log Server

Note

No appliance is set to Full policy source.

1. If your deployment includes Web DLP, in the Content Gateway manager manually unregister Content Gateway with TRITON AP-DATA.
2. Uninstall off-box components that are registered to the appliances whose C interface IP address will change.
3. Document the policy source settings of all appliances in the cluster and then change the policy source setting of each to **Full policy source**.

4. Change the C interface IP address (or addresses, if more than one appliance must change).
5. Return the policy source settings of the appliances to their original mode. For appliances that connect to the appliance whose C interface changed, provide the new C interface IP address.
6. Reinstall off-box components that are registered to appliances in the cluster.
7. If your deployment includes Web DLP, restart the Content Gateway module to automatically re-register with the TRITON AP-DATA components.

Configuring Master Database downloads to use P1

Help | V-Series Appliance | v8.2.x

By default, Filtering Service uses the C interface for full Master Database downloads, real-time database updates, and real-time security updates.

In TRITON AP-WEB deployments, you may be able to instead route database downloads through the P1 interface. This involves configuring Filtering Service to perform the download via the Content Gateway proxy.

> **Important**
>
> Database download settings are shared by all Filtering Service instances that connect to the same Policy Server instance. For that reason, this procedure may not be appropriate in all deployments (for example, deployments where server-based and appliance-based instances of Filtering Service share the same Policy Server).
>
> Verify which Filtering Service instances will be affected before making this change.

Use the following steps to update your database download settings:

1. Log on to the Web module of the TRITON Manager and connect to the Policy Server instance for the Filtering Service instance that you want to update.
2. Navigate to the **Settings** > **General** > **Database Download** page.
3. Under Proxy Server or Firewall, mark the **Use proxy server or firewall** box.
4. Enter the P1 virtual interface (**169.254.254.1**).
5. Make sure that the default port (**8080**) is shown.
6. If Content Gateway is configure to use IWA or NTLM authentication, mark **Use authentication** and provide a valid user name and password.
7. Click **OK**, then **Save and Deploy** to cache and save your changes.
8. From the **Status** > **Dashboard** page (still in the Web module of the TRITON Manager), click **Database Download**.
9. Select the appropriate Filtering Service instance, then click **Update**.

   The Master Database is downloaded via the P1 interface.

V-Series appliance routing configuration

Help | V-Series Appliance | v8.2.x

Use the **Configuration > Routing** page to specify:

- Static routes from subnets and client computers through any active appliance interface, except N.

  If IPv6 is enabled, static IPv6 routes can also be added and imported.
- Module routes from appliance modules through appliance interface C to subnets.

  IPv6 module routes are **not** supported.

Static routes

- Static routes can be specified for any active interface on the appliance, except N, which is dedicated to Network Agent and cannot be routed.
- The same route cannot be added for 2 different interfaces on the same module. If attempted, the appliance displays an error.
- Static routes that are defined for an interface that is later made inactive remain in the routing table, and are displayed in gray to indicate that the routes are inactive.
- Static routes that become invalid because the IP address of the interface changes are disabled and displayed in red.
- Static routes can be added and deleted, but not modified. To modify a route, delete it and add a new route specifying the new values.
- When a static route is added, imported, or deleted, the services associated with the module that manage the specified interface must be restarted. For example, if static routes are added to interface P1, when the additions are complete, all Content Gateway services must be restarted.
- The static route table has a maximum limit of 5000 entries.

See *Working with V-Series appliance static routes*, page 33.

Component routes

Although the appliance C interface is typically reserved for management traffic, in some deployments it is necessary or desirable to route some web or email traffic through the C interface rather than P1/P2 or E1/E2.

The component route table has a maximum limit of 5000 entries.

See *Working with V-Series appliance component routes*, page 34.

Working with V-Series appliance static routes

Help | V-Series Appliance | v8.2.x

Adding static routes

Static routes can be added one at a time, or many at a time using an import file.

When a static route is added, data entered in each field is validated by the appliance, and an error message is displayed if there is an inconsistency in the route.

To add static routes, select the **IPv4** or **IPv6** tab of the **Configuration > Routing** page, then click **Add/Import** under **Static Routes**.

To manually add a single route:

1. Make sure the **Add individual route** radio button is selected.
2. Use the **Destination network** field to enter the subnet IP address for which traffic will be routed.
3. Enter the **Subnet mask** (IPv4) or **Subnet prefix length** (IPv6) for the network where the clients reside (for example, 255.255.0.0, or 64).
4. Enter the **Gateway** IP address that provides access from the proxy subnet to the client subnet. This address must be on the same subnet as the appliance.
5. Select the appliance **Interface** to be used for the static route. Only active interfaces appear in the drop-down list.
6. Click **Add Route**.

To add multiple routes using an import list file:

1. Prepare the import file. See *Import file specifications*, page 33, below.
2. Select the **Import route file** radio button.
3. Specify the full path and file name, or **Browse** to locate the file.
4. Click **Import Route** to import the routes specified in the file.

   The appliance reads the file, validates each route, and reports errors for lines that are invalid.

   Duplicate route entries are ignored; duplicate entries are not created.

   If the number of routes in the file, combined with the number of existing routes, exceeds the 5000 route table limit, the import fails. No routes are added and an error message displays.

Import file specifications

1. The file must be a plain text file. (Most routers export route tables to a plain text file.)
2. The file can contain comment lines. Comment lines begin with “#”.
3. A line that defines a route must include the following 4 fields in the order shown. Each field must be separated by a space.

   For IPv4:

```
destination netmask default-gateway interface
```

For IPv6:

```
destination prefix-length default-gateway interface
```

In these examples:

- *Destination* is a subnet address or host IP address.
- (IPv4) *Netmask* determines the proper value of *destination*.
- (IPv6) *Prefix-length* determines the proper value of *destination*.
- *Default-gateway* is the next hop.
- *Interface* is the appliance interface through which traffic is routed. The specified interface must be enabled. If it is disabled, the appliance reports an error and does not add the route.

Deleting static routes

1. In the Static Routes table, click the box to the left of each entry you want to delete.

   To delete all routes, click the box to the left of the label **Destination Network**.
2. Click **Delete**.

Exporting the route table

To export the route table to a text file, click **Export Table**. Click **Browse** to specify a location and name for the file.

All routes in the table, whether enabled or disabled, are exported.

Working with V-Series appliance component routes

Help | V-Series Appliance | v8.2.x

Adding a component route

1. In the **Component Route** section of the **Configuration** > **Routing** page, click **Add**.
2. Select a **Module** from the drop-down list.
   - Only modules installed on the appliance are listed.
   - The Network Agent module never appears in the list.
3. Use the **Destination Network** field to specify the subnet IP address for which traffic will be routed.
4. Enter the **Subnet mask** for the destination subnet.
5. Click **Add Route**.

Deleting a component route

1. In the Component Routes section, select the routes to be deleted.
   - To select 1 route, click the box to the left of the entry you want to delete.

- To select multiple entries, click the box to the left of each entry you want to delete.
- To delete all routes, click the box to the left of the label **Module**.

2. Click **Delete**.

V-Series appliance alerting

Help | V-Series Appliance | v8.2.x

V-Series appliances provide alerting options that include standard SNMP counters and system-level traps to help facilitate management and maintenance of your appliance.

Use the **Configuration > Alerting** page to enable and configure SNMP alerting.

There are 2 methods of SNMP alerting that you can enable on the **Setup** tab:

- Allow your SNMP manager to poll the appliance for standard SNMP counters. See *Enable SNMP polling (monitoring) on V-Series appliances*.
- Configure the appliance to send SNMP traps for selected events to your SNMP manager. See *Enable SNMP traps on V-Series appliances*.

  After enabling the SNMP trap server on the appliance, use the **Alerts** tab to configure which events cause a trap to be sent. See *Enable specific V-Series appliance alerts*, page 37.

Enable SNMP polling (monitoring) on V-Series appliances

Help | V-Series Appliance | v8.2.x

1. On the Setup tab of the **Configuration > Alerting** page in the Appliance manager, under Monitoring Server, click **On**.
2. Select the **SNMP version** (v1, v2c, or v3) used in your network.
   - With SNMP v1 and v2c, a suffix (-proxy, -web, -na, or -email) is appended to the community name to indicate the originating module for the counter.
   - With SNMP v3, you can specify the context name (PROXY, WEB, NA, or EMAIL) to poll counters for each module.
3. Do one of the following:
   - If you selected v1 or v2c, provide the **Community name** for the appliance, and then click **OK**.

     You have completed your SNMP monitoring configuration.
   - If you selected v3, select the **Security level** (None, Authentication only, or Authentication and Encryption) used in your network, and the **User name** to associate with SNMP communication.
4. If you selected a security level that includes authentication, also enter and confirm the **Password** for the selected user name, then select the **Authentication protocol** (MD5 or SHA).

5. If you selected authentication and encryption, select the **Encryption protocol** (DES or AES), and then enter and confirm the **Encryption key** used for encryption.
6. Click **OK** to implement your changes.

Enable SNMP traps on V-Series appliances

Help | V-Series Appliance | v8.2.x

1. On the Setup tab of the **Configuration** > **Alerting** page in the Appliance manager, under Trap Server, click the link to download the appliance **MIB file**.
   - The MIB file must be installed in your SNMP manager before it can interpret traps sent by the appliance.
   - The MIB file does not include severity recommendations. Severity recommendations can be found in the article Trap Severity Level Recommendations for V-Series Appliances.
2. When you are ready for the appliance to start sending SNMP traps, under Trap Server, click **On**, and then select the SNMP version (v1, v2c, or v3) used in your network.
3. Follow the steps below for the SNMP version that you selected.

For SNMP v1 or v2c:

1. Enter the **Community name** to associate with traps sent by the appliance.
2. Enter the IP address and port used by your SNMP manager.
3. To verify your configuration, click **Send Test Trap**. If the test trap succeeds, click **OK** to apply and save your changes. See *Enable specific V-Series appliance alerts*, page 37, to configure which events cause a trap to be sent.

   If there is a problem sending the test trap, verify the community name, IP address, and port, and make sure that the network allows communication between the appliance C interface and the SNMP manager.

For SNMP v3:

1. Enter the **Engine ID** and **IP address** of your SNMP manager, as well as the **Port** used for SNMP communication.
2. Select the **Security level** (None, Authentication only, or Authentication and Encryption) used in your network, and the **User name** to associate with SNMP communication.
3. If you selected a security level that includes authentication, enter the **Password** for the selected user name, and then select the **Authentication protocol** (MD5 or SHA).
4. If you selected authentication and encryption, select the **Encryption protocol** (DES or AES), and then enter the **Encryption key** used for encryption.

5. To verify your configuration, click **Send Test Trap**. If the test trap succeeds, click **OK** to implement your changes. See *Enable specific V-Series appliance alerts*, page 37, to configure which events cause a trap to be sent.

   If there is a problem sending the test trap, verify the engine ID and authentication settings and values, and verify that the network allows communication between the appliance and the SNMP manager.

Enable specific V-Series appliance alerts

Help | V-Series Appliance | v8.2.x

The appliance can send traps for each of its modules: Appliance Controller, Content Gateway, TRITON AP-WEB, Network Agent, and TRITON AP-EMAIL. The Alerts tab of the **Configuration > Alerting** page lists the alerts associated with only the modules that you have enabled.

When you have finished configuring alerts, click **OK** to implement the changes.

A table for each module lists:

- The hardware or software **Event** that triggers the alert (for example, a network interface link going down or coming up, or a TRITON service stopping).
- The **Threshold**, if applicable, that defines the alert condition (for example, CPU usage exceeding 90%, or free disk space reaching less than 10% of the total disk size).
- The **Type** of alert (system resource or operational event).
- Whether or not an SNMP trap is sent when the event occurs or the threshold is reached.

Mark the check box next to each event that you want to trigger an alert.

- To enable all alerts for a module, select the check box next to **SNMP** in the table header.
- To disable alerts for an event, clear the associated check box.

Time-based thresholds

Most of the events that have a configurable threshold also have a configurable time-based threshold, specified in minutes. When the time-based threshold is set and **both thresholds** are exceeded, an alert is sent. To enable time-based thresholds, select the **Enable time-based thresholds** check box at the top of the page. The time-based threshold is enabled on every event for which it is configurable.

Event-cleared alerts

In addition to generating event condition alerts, you can configure alerts to be sent when conditions return below the threshold. These are called **event-cleared alerts**. To enable event-cleared alerts, select the **Generate event-cleared alerts** check box at the top of the page.

The following events do not generate event-cleared alerts:

- Hostname change
- IP address change
- Scheduled backup failure
- SNMP authentication failure

Configuring V-Series appliance Web components

Help | V-Series Appliance | v8.2.x

Be sure that you have identified which machine will be the **policy source** for your deployment before making changes on the **Configuration > Web Components** page in the Appliance manager.

See *What is a policy source?*, page 38, and *What if an appliance is not the policy source?*, page 40, for detailed information to help you decide which set of components to enable on each of your V-Series appliances.

When you have planned the configuration of each of your appliances, use the **Configuration > Web Components** page to enable the correct set of components on the appliance.

1. Under **Policy Source**, select the configuration for this appliance:
   - **Full policy source** (default; includes Policy Broker, the Policy Database, and Policy Server, as well as the components listed in *What is a policy source?*).
   - **User directory and filtering** (includes Policy Server and User Service, as well as the components listed in *What if an appliance is not the policy source?*)
   - **Filtering only** (includes Filtering Service and Content Gateway; does not host Policy Server)
2. If this is a **user directory and filtering** appliance, provide the **policy source IP address** to allow components on the machine to connect to Policy Broker.
3. If this is a **filtering only** appliance, enter the IP address of a Policy Server instance. It does not have to be the policy source IP address.
4. Click **OK** to save and apply your changes.

What is a policy source?

Help | V-Series Appliance | v8.2.x

Every TRITON AP-WEB deployment must include a **policy source**. This is an appliance or other server that hosts TRITON Policy Broker, TRITON Policy Database, and TRITON Policy Server.

- When the policy source is a Windows server, TRITON management server components typically also reside on the machine.

- When the policy source is an appliance, the components listed below also reside on the machine.

All other V-Series appliances and other TRITON servers point to the policy source server or appliance and receive regular updates from it.

The Policy Database holds all security policies (including client definitions, filters, and filter components) for all appliances and all domains in the network. It also holds global configuration information that applies to the entire deployment.

Policy Broker controls access to the information in the Policy Database.

You deploy Policy Broker in standalone or replicated mode:

- In **standalone** mode, there is one Policy Broker for the entire deployment. All Policy Servers connect to the same Policy Broker. In this mode, Policy Broker can reside on a Windows or Linux server, or a V-Series appliance.
- In **replicated** mode, there is one **primary** Policy Broker, to which configuration and policy changes are saved, and one or more **replica** instances, each with its own read-only copy of the configuration and policy data. Each Policy Server can be configured to determine whether it attempts to connect to the primary Policy Broker or a replica instance at startup.

  In a replicated configuration, Policy Broker cannot reside on a V-Series appliance. Both the primary and replica instances must be hosted by a Windows or Linux server. See Managing Policy Broker Replication for more information.

When a TRITON AP-WEB only appliance is configured as a policy source, most Web components may run on that appliance, including:

- Policy Broker
- Policy Server
- User Service
- Control Service
- Directory Agent (requires Web Hybrid module; user directory and filtering appliances only)
- State Server (optional; disabled by default)
- Policy Database
- Filtering Service
- Usage Monitor
- Content Gateway
- Multiplexer (disabled by default; not available on filtering only appliances)
- Network Agent (optional)

Windows-only services, like Log Server, TRITON Manager, and optional services, like transparent identification agents, must run on other machines.

What if an appliance is not the policy source?

Help | V-Series Appliance | v8.2.x

A V-Series appliance that is not serving as the policy source can be designated as either a **user directory and filtering** or **filtering only** appliance.

- A **user directory and filtering** appliance is sometimes also called a “policy lite” machine. It runs:
  - Policy Server
  - User Service
  - Usage Monitor
  - Filtering Service
  - Control Service
  - Directory Agent (optional; see *Preparing V-Series appliances for a hybrid deployment*, page 41)
  - Content Gateway
  - Network Agent (optional)

  Having User Service on remote appliances makes it easier to obtain local network user names. Latency between User Service and Policy Server is eliminated, because both run on the same appliance.

  A user directory and filtering appliance is configured to point to the policy source for updates.

  - Whenever you make a policy change, that change is pushed from the policy source appliance to user directory and filtering appliances within 30 seconds.
  - User directory and filtering appliances can continue handling traffic for as long as 14 days if their connection with the policy source is interrupted. So even if a network connection is poor or is lost, traffic management continues as expected.
- A **filtering only** appliance does not run Policy Server. It runs only:
  - Filtering Service
  - Control Service
  - Content Gateway
  - Network Agent (optional)

  A filtering only appliance is configured to point to a Policy Server. This works best when the appliance is close to the Policy Server and on the same network.

  These appliances require a continual connection to the centralized policy server, not only to stay current, but also to continue handling traffic. If the connection to the policy server becomes unavailable for any reason, traffic handling on a Filtering only appliance can continue for up to 3 hours.

  If the Policy Server machine is on a remote network, with a WAN connection, it can be difficult to obtain user name/IP address maps for the local users.

Preparing V-Series appliances for a hybrid deployment

Help | V-Series Appliance | v8.2.x

When TRITON AP-WEB includes the Web Hybrid module, some users' traffic may be handled by the hybrid service in the cloud. In this situation, an interoperability component on the appliance called **Directory Agent** is required to enable user-, group-, and domain- (OU) based security.

Directory Agent must be able to communicate with:

- A supported LDAP-based directory service:
  - Windows Active Directory® (Mixed Mode)
  - Windows Active Directory (Native Mode®)
  - Oracle (Sun Java™) System Directory
  - Novell eDirectory
- Sync Service

After deployment, use the Web module of the TRITON Manager to configure User Service and Directory Agent.

- User Service configuration is performed on the **Settings > General > Directory Services** page.
- Directory Agent configuration is performed on the **Settings > Hybrid Configuration > Shared User Data** page.
  - You can have multiple Directory Agent instances.
  - Each Directory Agent must use a unique, non-overlapping root context.
  - Each Directory Agent instance must be associated with a different Policy Server.
  - All Directory Agent instances must connect to a single Sync Service. (A deployment can have only one Sync Service instance.)
  - Configure the Sync Service connection manually for Directory Agent instances running on user directory and filtering appliances. See the TRITON AP-WEB Administrator Help for details.

3 V-Series Appliance Administration

Help | V-Series Appliance | v8.2.x

Tips for administrators

Every V-Series administrator should have a Forcepoint account logon, accessed through the My Account portal. My Account is where administrators can download product updates, get patches and hotfixes, access customer forums, read product news, and access other technical support resources for TRITON software and appliances.

Using Appliance manager administration features

The Administration pages in the Appliance manager can be used to:

- Install software patches (see *V-Series appliance patch management*).
- Install software hotfixes (see *V-Series appliance hotfix management*).
- Prepare and restore backups of your appliance configuration, Web modules, and Email module (see *Using the V-Series appliance backup utility*).
- Access system logs for all active modules (see *V-Series appliance log files*).
- Customize block pages, enable remote access to the appliance command-line interface, and launch the command-line utility (see *V-Series appliance tools*).
- Change the Appliance manager or Content Gateway manager **admin** password (see *Account management*).

V-Series appliance patch management

Help | V-Series Appliance | v8.2.x

Related topics:

- *V-Series appliance patch update options*, page 45
- *V-Series appliance hotfix management*, page 48
- *V-Series appliance patches and hotfixes proxy settings*, page 50

Use the **Administration > Patches / Hotfixes > Patches** page in the Appliance manager to keep your V-Series appliance up to date. A patch typically upgrades the appliance controller and all software modules on the appliance while preserving your existing settings.

Appliances automatically check for new patches once a day. The time of the check is randomized, cannot be configured, and is different for every appliance. Click **Check for Patches** to initiate the check manually.

When a new patch is available, the patch version number, description, and status are displayed in the **Available patches** table, and an alert is displayed on the **Status > General** page.

- After a patch is downloaded it can be copied to another location on your network where it can be easily uploaded to multiple appliances.
- If the appliance management interface (C) does not directly connect to the Internet, you can configure a proxy server through which the appliance checks for patches. See *V-Series appliance patches and hotfixes proxy settings*, page 50.

For instructions on applying a patch, see *V-Series appliance patch update options*, page 45.

- A new appliance at your site should immediately be patched to the latest version.
- Keep all V-Series appliances on your network at the same version.
- Install software patches as soon as they become available.

Once a patch has been applied to the appliance, its details appear in the **Patch History** table. For each patch, the table displays:

- Version number
- Date and time of the patch installation
- Comments that confirm the success or failure of the patch installation
- A link to the patch log file, showing patch details

Patch process for appliances

Patch download and installation is initiated manually by the appliance administrator.

- Download and install each patch during a low-activity period on your network. See *V-Series appliance patch update options*, page 45, for details.
- If Network Agent has been temporarily disabled, re-enable it before starting the patch installation. See *Re-enabling Network Agent before installing a patch*, page 47.
- Install patches in consecutive sequence.
- On the **Patches** page, the “Appliance current version” number is the current appliance version (reflects the latest patch installed).
- Be sure that all TRITON modules running off the appliance, such as Log Server, are upgraded to the appropriate level each time you patch the appliance. See the patch release notes for details.

  The online V-Series Compatibility Matrix shows a table of the software module versions that are compatible with each appliance version.
- If multiple appliances are deployed in your network, they must all run the same version of software. Forcepoint LLC, does not support running different versions of the software on different appliances in the same network.

V-Series appliance patch update options

Help | V-Series Appliance | v8.2.x

Important

It is very important to read the release notes before applying a new patch.

In addition to a summary of changes contained in the patch, there is information about impacts to other modules and an estimate of the time it will take to apply the patch.

The following download and installation options are available for appliance patches:

Download	Start downloading an available patch. In the Status field, a progress bar displays the progress of the download. Another patch can be selected, and the download initiated, while the first download is underway. Such requests form a sequential download queue. When the patch download is complete: ● The **Download** button is replaced by **Install** and **Delete** buttons. (See below.) ● A **Save to network location** link is included after the patch description. Click the link to copy the patch file to another location on your network. This can be helpful if you have multiple appliances and do not want to download the patch separately for every appliance. Instead, on each appliance simply use the **Upload Patch Manually** function to upload the patch from the network location. It is recommended that patches be downloaded and applied in numeric sequence. In many cases, this is a requirement.
Pause	Temporarily pause the download process that is currently underway.
Cancel	Stop the download process that is currently underway.
Resume	When a patch download has been paused, you can click **Resume** to continue the download process.
Install	**IMPORTANT: Read the patch release notes** before installing the patch. **IMPORTANT:** If Network Agent is temporarily disabled and you **do not** want to permanently disable it (which requires re-imaging the appliance to regain its use), you must re-enable Network Agent before installing the patch. See *Re-enabling Network Agent before installing a patch*, page 47. **Install** is enabled only after a patch has been downloaded and verified. Click the button to apply the patch to the appliance. A series of pages prompt for confirmation and provide status. You are notified if a restart is required after installation. After the restart, the patch is removed from the patch queue and logged in the Patch History table. If an earlier, required patch has not been installed, a message in the **Status** column indicates which earlier patch is required and the Install button for the dependent patch is disabled. Install the earlier patch first. If a patch installation fails, any installed files from that patch are immediately uninstalled and a message displays indicating that the patch installation failed. You can try installing it again. If that fails, delete the patch, then download it again and re-attempt the installation.
Delete	Remove a patch file from the appliance.

Check for Patches	Manually check for new patches now.
Upload Patch Manually	Upload a patch from another location on your network. This can be a convenient and efficient method of distributing a patch among multiple appliances in a cluster or where multiple appliances have access to a local network. To upload patches you must use Internet Explorer 11 or higher, Firefox 4 or higher, or Chrome 11 or higher. For instructions on copying a patch file from an appliance to another location in the network, see the entry for **Download**, above.

Re-enabling Network Agent before installing a patch

Help | V-Series Appliance | v8.2.x

Follow these steps if Network Agent is temporarily disabled, you don't want to permanently disable it, and you want to install a patch.

1. If you have initiated an installation on the **Patches** page, and the **Network Agent Disable** dialog box has displayed, and you **do not** want to permanently disable Network Agent, select **Cancel** to close the dialog box and then go to the **Status** > **General** page. In the **Network Agent** area, click **Enable Module** and then **OK** to confirm the action. The appliance automatically restarts.
2. If you have **not** initiated an installation on the **Patches** page, go to the **Status** > **General** page and in the **Network Agent** area click **Enable Module** and then **OK** to confirm the action. The appliance automatically restarts.
3. After the appliance has restarted, log on, go to the **Administration** > **Patch / Hotfixes** > **Patches** page, and perform the patch installation.
4. When the patch installation is complete, if you want to again temporarily disable Network Agent, return to the **Status** > **General** page and disable Network Agent.

The reason that Network Agent must be re-enabled prior to patch installation (if it is not permanently disabled) is that if Network Agent is stopped and the patch includes updates to Network Agent, the updates are not made to the stopped module. Thus, if it is re-enabled some time in the future, it may be incompatible with other modules on the system.

V-Series appliance hotfix management

Help | V-Series Appliance | v8.2.x

Related topics:

- *Hotfix application process*, page 48
- *Hotfix history*, page 49

Use the **Administration > Patches / Hotfixes > Hotfixes** page to find, install, uninstall, and otherwise manage hotfixes for the appliance and its software modules.

- In the majority of cases, you are notified of hotfixes by either:
  - A Technical Alert email
  - A Forcepoint Technical Support agent (The agent provides the name of a specific hotfix to address the problem you reported.)
- As a best practice, install all security vulnerability hotfixes.
- A hotfix may address an issue on any module running on your appliance.
  - A hotfix should not be recommended to you for a module that you have not configured or are not running on your appliance.
  - The hotfix facility on the appliance will not install a hotfix that is not valid for the module versions on your appliance.
- A hotfix may have dependencies on one or more other hotfixes, in which case the hotfix facility will not allow the installation of the hotfix until after its dependents are installed.

Hotfix application process

To download and apply a hotfix to the V-Series appliance:

1. Under **Hotfix Installation**, enter the name of the hotfix and click **Find**.

   If the hotfix is not found, make sure the name is entered correctly:

   - Specify the exact name of the hotfix, including any leading or trailing zeros.
   - The format is: *Module-version-number* (for example: Email-8.1.1-001)

   If the name repeatedly returns not found, contact Forcepoint Technical Support.
2. When the hotfix is found, review the description in the Hotfix Details pop-up that is displayed.
   - If the description is what you expect, click **Download** to download the hotfix to the appliance.
   - Otherwise, click **Cancel**.
3. After the hotfix is downloaded, a description and status display in the **Downloaded hotfixes** table.

- Check the **Status** column of the table to confirm that the hotfix has no dependencies and is ready for installation.

  If the hotfix is dependent on another hotfix, you must download and install that hotfix first.
- If you plan to apply this hotfix to other V-Series appliances in your network, optionally click **Save to network location** to copy the hotfix file to a drive in your network. Once the file is saved, you can manually upload it to your other appliances.

4. Click **Install** to install the hotfix.

If you have already downloaded the hotfix file to a machine in your network, click **Upload Hotfix Manually** to copy the file to the appliance.

Hotfix history

Use the Hotfix History list to find the current appliance version, uninstall hotfixes, or review a record of installed or uninstalled hotfixes.

To start, select an option from the **View** drop-down list:

- **Installed hotfixes** populates the table with a list of hotfixes that have been installed, or that you attempted to install unsuccessfully.
- **Uninstalled hotfixes** populates the table with a list of hotfixes that have been uninstalled, or that you attempted to uninstall unsuccessfully.

Both lists show the Hotfix ID (the name of the hotfix file), the date the hotfix was installed or uninstalled, and the status of the hotfix installation or removal process.

The **Installed hotfixes** list also shows:

A radio button	Select the radio button to activate the **Uninstall** button. If the hotfix has dependencies that prevent it from being uninstalled, a message is displayed below the table.
Name	The name of the hotfix and a link to the Release Notes.
Module	The name of the affected appliance module.
Uninstall button	Use this button to initiate uninstallation of the selected hotfix.

The **Uninstalled hotfixes** list also shows a reason that you provide for uninstalling the hotfix. It is easy to lose track of why a hotfix was uninstalled. Recording a clear description here can save repeated errors and lost time in the future.

V-Series appliance patches and hotfixes proxy settings

Help | V-Series Appliance | v8.2.x

If the appliance management interface (C) does not directly connect to the Internet, you can configure a proxy server through which the appliance checks for patches and hotfixes. Use the **Administration > Patches and Hotfixes > Proxy Settings** page to configure a proxy server through which the appliance checks for patches and hotfixes.

1. Mark **Use proxy server** to prompt the patch and hotfix utilities to send their requests through a proxy server.
2. Enter the **Proxy IP address** and the connection **Port**.
3. If the proxy connection requires authentication, provide the **User name** and **Password** to use for authentication.
4. Click **Test Connection** to verify the proxy settings.
5. Click **OK** to save your new settings.

Using the V-Series appliance backup utility

Help | V-Series Appliance | v8.2.x

Related topics:

- *Scheduling V-Series appliance backups*, page 52
- *V-Series full appliance configuration backups*, page 53
- *V-Series component configuration backups*, page 54
- *Restoring a V-Series appliance backup file*, page 55

The **Administration > Backup Utility** page includes 2 tabs:

- Use the **Backup** tab to initiate configuration backups, schedule recurring backups, or manage existing backup files.
- Use the **Restore** tab to restore an appliance or module configuration from an existing backup file. See *Restoring a V-Series appliance backup file*, page 55.

Two types of backup are available on the V-Series appliance:

- A **full appliance configuration** backup saves all appliance settings, as well as configuration and policy information for all active modules (for example, TRITON AP-WEB and TRITON AP-EMAIL). The best practice is to run a full backup on every appliance in your network on a regular basis.

  Note that the full backup file may be smaller than the module backup files, because it is compressed.

- A **component configuration** backup saves all configuration information for the selected module. This includes any client and policy data stored on the selected appliance.

> **Note**
>
> Component configuration backup does not include a Content Gateway option.
>
> Content Gateway backups (snapshots) can be performed in Content Gateway manager. Snapshots must be performed manually; there is no scheduling facility.

Backup types and backup status information are shown in the Perform Backup list. To start or schedule a backup, first select the backup type, and then click either **Run Backup Now** or **Configure Backup Schedule** (for information about scheduling backups, see *Scheduling V-Series appliance backups*, page 52).

You must initially set up the backup function; it is not automatic. Once you schedule backups, however, those backups will continue to run at regular intervals without requiring further intervention. To stop a scheduled backup from recurring, click **Cancel Scheduled Backup**.

The Local Backup Files list shows all backup files stored on the current appliance. Select a backup type from the **View backups for** list to change the type of backup file shown.

Each entry in the list includes the date and time of the backup and the name of the backup file.

For full appliance configuration backup files, the following information is also included:

- The patch version of the appliance on which the backup was run. When you restore from a backup, the backup file must be the same version as the appliance you are restoring.
- The host name of the backup source.
- A comment on the protection mode and policy information in each backup file.

Comment	Protection Mode
TRITON AP-EMAIL	Indicates a full backup of a TRITON AP-EMAIL only appliance.

Comment	Protection Mode
Web Configuration (Full policy source) Web Configuration (User directory and filtering) Web Configuration (Filtering only)	Indicates a full backup of a TRITON AP-WEB only, or Web Filter & Security only appliance. The policy mode is indicated in parenthesis.
Web Configuration (Full policy source) and TRITON AP-EMAIL Web Configuration (User directory and filtering) and TRITON AP-EMAIL Web Configuration (Filtering only) and TRITON AP-EMAIL	Indicates a full backup of a TRITON AP-WEB and TRITON AP-EMAIL, or Web Filter & Security and TRITON AP-EMAIL appliance. The policy mode is indicated in parenthesis.

Up to 20 appliance backup files and 20 backup files for each module can be stored on the appliance. When the twenty-first backup file is created, the oldest file is automatically deleted.

To download a backup file to another machine, click the file name, then browse to the path where you want to save the file.

To delete local backup files manually, mark the check box next to the backup file name in the Local Backup Files list, and then click **Delete**.

Scheduling V-Series appliance backups

Help | V-Series Appliance | v8.2.x

Related topics:

- *Using the V-Series appliance backup utility*, page 50
- *V-Series full appliance configuration backups*, page 53
- *V-Series component configuration backups*, page 54
- *Restoring a V-Series appliance backup file*, page 55

Use the **Backup Utility > Configure Backup Schedule** page to specify how frequently and at what time of day the selected backup type is performed, and to select a location for storing backup files. Schedule each applicable backup type (full appliance, web, or TRITON AP-EMAIL separately.

To schedule backups:

1. Select a **Backup frequency**: daily, weekly, or monthly.
   - For weekly backups, select which day of the week the backup is run.
   - For monthly backups, select which day of the month the backup is run. You cannot schedule backups to run on the 29th, 30th, or 31st day of the month, because not all months have those days.
2. Specify a **Start time** for the backup process. Ideally, select a time when the appliance is unlikely to be under heavy load.

Enter the time in 24-hour format (where 00:00 indicates midnight, and 12:00 indicates noon).

3. Provide a **Storage location** for the backup files. Only one remote backup location can be configured for each backup type.
   - Select **Appliance** to have the file stored locally. A maximum of 20 backup files can be saved, and the backup file directory cannot be renamed, moved, or deleted.

     Backup files saved to the appliance can be viewed on the Backup Utility page, under Local Backup files.
   - Select **Remote machine** to store the backup file on another machine in the network, then indicate whether to use a **Samba file share** or **FTP server** and provide the following connection information:
     a. The **IP address/hostname** of the remote machine, and the connection **Port** to use.
     b. The **Default directory** in which backup files will be created. A different subdirectory will be created automatically for each backup file type.

Important

If you want to create backup files for multiple appliances on the same remote machine, be sure to use a separate directory for each appliance's backup files.

This avoids the possibility of conflicts that could lead to files being mistakenly overwritten or deleted.

     c. The **User name** and **Password** to use when connecting to the remote machine. If a network logon is used, also provide the **Domain** in which the account resides.
     d. Click **Test Connection** to make sure the appliance can communicate with the remote machine and write to the specified location.
     e. If you want remote backup files to be automatically deleted after a specified time period, mark the **Delete backup files that are older than** check box, and then select a time period from the list.

4. Click **OK** to save your changes and return to the Backup Utility page. The new backup schedule is displayed in the Perform Backup list.

V-Series full appliance configuration backups

Help | V-Series Appliance | v8.2.x

A full appliance configuration backup saves all appliance settings, as well as saving configuration and policy data for all active modules (TRITON AP-WEB, TRITON AP-EMAIL, or both) on the appliance. If you have multiple appliances, run backups on each one. The backup file includes data for only the appliance on which it is created.

Note

Components that do not reside on the appliance (like Log Server and TRITON Manager) should be backed up with the appropriate utilities, at approximately the same time that you back up your appliance. When you restore the system, this allows you to restore from a time-synchronized set of backups on all machines.

Full appliance configuration backup files for TRITON AP-WEB appliances include:

- All configuration files for the appliance on which the backup is run, including configuration files for the V-Series manager
- A snapshot, including all configuration data, of Content Gateway
- All configuration settings for TRITON AP-WEB including:
    - Global configuration information, stored in the Policy Database (if Policy Broker is running on the selected appliance)
    - Local configuration information, such as Filtering Service and Log Server settings, stored in the **config.xml** file (if Policy Server is running on the selected appliance)
    - Component initialization (.ini) and configuration (.cfg) files

Full appliance configuration backup files for TRITON AP-EMAIL appliances include:

- All configuration files for the appliance on which the backup is run, including configuration files for the V-Series manager
- Policy and configuration data for TRITON AP-EMAIL

For appliances running in Web and Email mode, both sets of information are included in full backup files.

V-Series component configuration backups

Help | V-Series Appliance | v8.2.x

Component configuration backups save all configuration information, including policy data, for the selected module.

- Web configuration backups performed on the *full policy source* appliance include all information stored in the Policy Database.
- TRITON AP-EMAIL configuration backups can be performed only if the Email module is enabled on the selected appliance.
- Component backup operations for Content Gateway are managed through Content Gateway manager. Click the Content Gateway manager link at the top of the Backup Utility page to open the console and initiate backups.

Restoring a V-Series appliance backup file

Help | V-Series Appliance | v8.2.x

Related topics:

- *Using the V-Series appliance backup utility*, page 50
- *Scheduling V-Series appliance backups*, page 52
- *V-Series full appliance configuration backups*, page 53
- *V-Series component configuration backups*, page 54

When you initiate the restore process, all current settings for the appliance or module are erased. Backup files stored on the appliance are not affected. When you are restoring the full appliance configuration, at the end of the restore process, the appliance restarts. The appliance is not restarted after you restore a module.

To restore an appliance or module to a saved configuration:

1. Stop all software components running off the appliance.

   For example, stop Log Server, Sync Service, Linking Service, transparent identification agents, all components associated with the TRITON Manager, and the integrated TRITON AP-DATA Server.

2. Open the V-Series manager on the appliance whose configuration you want to restore and go to the **Administration > Backup Utility** page.

3. Click the **Restore** tab, then select the configuration type that you want to restore from the **Select restore mode** list. Note that when you restore a full appliance configuration:

   - The current appliance version must match the version associated with the backup file. (The appliance version is displayed on the **Restore** tab.) Thus, a version 8.0 backup can be restored only on an appliance that is at version 8.0.
   - The current appliance policy source mode (Full policy source, User directory and filtering, or Filtering only) must match the policy source mode in effect when the backup file was created.
   - In most circumstances, the current appliance mode (Email, Web, Web and Email) must match that of the backup file. (For example, a backup from a TRITON AP-EMAIL-only appliance must be used to restore a TRITON AP-EMAIL-only appliance.)

     There is one exception. If you are running in Web and Email mode on a V10000 appliance, you can restore a Web full backup.
   - The hardware model of the current appliance must be the same as the model that was backed up. (For example, a backup from model V10000 G2R2 must be used to restore a model V10000 G2R2 appliance.)
   - The original appliance that was backed up cannot also be running elsewhere in the network. Restoring a full configuration re-creates the original appliance and makes use of unique ID numbers from that appliance.

4. Click **Run Restore Wizard**. The restore wizard opens.

5. Select a radio button to indicate where the backup file is stored, and then click **Next**.
    - **This remote machine:** <*host name or IP address*>: Retrieve the file from the default location on the specified machine. The default location is the path specified in the backup schedule for the selected backup type.
    - **This appliance**: Use a backup file that was saved locally.
    - **Another location (browse for file)**: Use a file saved on any accessible machine in the network.
6. Select or specify the file to use.
    - If you selected the default local or remote backup file location, you are given a list of available backup files to use. Select an entry in the list, and then click **Next**.
    - If you selected another location, browse to the path on the remote machine where the backup file is located, and then click **Next**.
7. Verify the details on the Confirm page, and then click **Restore Now**. The appliance is restored to the selected configuration.

    If you have initiated a full appliance configuration restore, the appliance is restarted during the restore process.
8. Before starting the off-box components, ensure that the system time of all TRITON component hosts is synchronized. On the appliance, either set the time manually, or, if an NTP server is configured, click OK to trigger an update with the NTP server.
9. Start the TRITON components located off the appliance.

    Note that if the restore process changed appliance IP addresses, you may need to reconfigure or reinstall off-box components to re-establish communication between on-box and off-box components.

V-Series appliance log files

Help | V-Series Appliance | v8.2.x

Forcepoint Technical Support may request log files to assist you with troubleshooting. This page provides access to these log files for viewing and download.

> ✓ **Note**
>
> Network Agent generates a log file only if protocol logging is enabled on the **Settings > Network Agent > Global** page in the Web module of the TRITON Manager.

Select the module for which you want to view logs:

- Appliance Controller
- Content Gateway

- TRITON AP-WEB
- Network Agent
- TRITON AP-EMAIL

If you are reviewing the Appliance Controller log, next select a **Date range**. Log files are available in weekly increments for up to 5 weeks.

For all log files, select from 2 **View options**:

- View the last 50, 100, or 500 lines of the log file in a pop-up window
- Download entire log file

Click **Submit** to begin the process of gathering the requested log file.

If you are downloading the entire log file, use the **File Download** dialog box to navigate to the save location.

V-Series appliance tools

Help | V-Series Appliance | v8.2.x

Use the **Administration > Toolbox** page to set up customized block pages, access basic Linux commands, and assist with troubleshooting.

- *Web block pages*
- *V-Series appliance command line*
- *Command line utility*
- *V-Series appliance technical support tools*

Web block pages

Help | V-Series Appliance | v8.2.x

With TRITON AP-WEB and Web Filter & Security, when a user request a URL in a a blocked category, the browser displays a block page, rather than displaying the requested site. The block page is a customizable HTML page with a brief explanation of why the requested URL has been blocked.

The V-Series appliance hosts a set of default Web block pages. For more information on how to customize these pages for your appliance, see the Block Pages article, available in the Forcepoint Technical Library.

V-Series appliance command line

Help | V-Series Appliance | v8.2.x

Use the **Appliance Command Line** section of the **Administration > Toolbox** page to:

- Turn on and off SSH remote access to the appliance **command line interface**. SSH access allows administrators to log on to the appliance command line shell from machines in the network that have a route to the appliance.
- Access a **command line utility** that is embedded within the Appliance manager. The command line utility provides convenient access to common troubleshooting commands.

SSH Remote Access

Use the **Remote Access** option to enable and disable SSH access to the appliance command line interface.

To connect to the appliance command line shell when SSH access is enabled:

1. Use a terminal emulator that supports SSH (like PuTTY) to connect to the IP address of the C interface.
2. Enter your Appliance manager **admin** logon credentials when prompted.
3. Run the **help** command to see the available commands.

The following commands are supported by the command line interface. The **debug-util** subcommands are also available in the command line utility. See *V-Series command line utility command options*, page 59, for more information.

admin email
debug-util controller
debug-util email
debug-util na
debug-util view
debug-util proxy
debug-util web
firstboot
help
history
ip address
ip dns
ip gateway
local-access
module disable
module enable
module restart
module start
module stop
password-logon disable
password-logon enable
patch delete
patch list
policy-source
quit
reload
remote-access disable
remote-access enable
reset password
show admin email
show cpu
show disk-io
show disk-space
show integration-mode
show interface c
show memory
show module
show module service
show password-logon
show patch
show patch history
show platform
show policy-source
show remote-access
show remote-access history
show security-mode

show smtp server
shutdown
ssh disable
show ssh
smtp server
ssh enable

Command line utility

Use the **Command Line Utility** to run troubleshooting, debugging, and utility commands.

1. Click **Launch Utility** to open the command utility. The utility opens in a separate window.
2. Select a module from the **Component** drop-down list. Available modules may include:
   - Appliance Controller
   - Content Gateway
   - TRITON AP-WEB or Web Filter & Security
   - Network Agent
   - TRITON AP-EMAIL
3. Select the command you want to run from the **Command** drop-down list, enter additional parameters (if any), then click **Run**. For details about the available commands, see *V-Series command line utility command options*, page 59.

   Results are displayed in the **Console output** section of the page. You can click **Download output file for last command** to export the results to a file on your local machine.
4. For commands that run continuously, click **Stop** to interrupt the command.
5. When you are finished using the command line utility, click **Exit**.

V-Series command line utility command options

The command line utility supports the following commands:

Command	Description	Parameters
arp	Displays the kernel ARP table for the selected module.	None
cache-user-names	(Web module only) Turn on or off, or query the status of caching of user names resolved from IP addresses by Content Gateway. Cached entries are valid for 10 minutes.	Enter **enable** to turn on user name caching. Enter **disable** to turn off user name caching. Enter **status** to display the status of user name caching.

Command	Description	Parameters
content-line -r	(Content Gateway module only) Use it to display the current value of a configuration variable in Content Gateway's records.config file.	Enter the name of the variable whose value you want to see. **Example**: `proxy.config.ldap.auth.enabled` This variable returns "0" (disabled) or "1" (enabled). For a complete list of valid configuration variables, click the **Content Gateway Help** link. (You may be prompted for logon credentials.)
content-line -s	(Content Gateway module only) Use it to set the value of a configuration variable in Content Gateway's records.config file. With this command, you can make changes to Content Gateway variables without restarting the proxy. To activate the changes, use the **content_line -x** command (described below).	Enter the name of the variable you want to modify and the value you want to supply the variable. **Example**: Enter the variable name **proxy.config.ftp.control_connection_timeout** and the value "120". This specifies how long Content Gateway waits, in seconds, for a response from the FTP server. For a complete list of valid configuration variables, click the **Content Gateway Help** link. (You may be prompted for logon credentials.)
content-line -x	(Content Gateway module only) Read and apply the values of all configuration variables in Content Gateway's records.config file. If you have changed any settings in the records.config file via the **content_line -s** command, you can activate your changes immediately (without restarting the proxy) with this command.	None
content-line -y	Clears all dynamic Certificates from the Content Gateway database	
debugging reset	Reset the debugging level to factory status.	None
debugging status	Show the debugging level status.	None
dig -t mx	(Email module only) Return information on the specified MX server.	Enter the domain name of the MX server you want to query.
dig -t txt	(Email module only) Return the SPF information from the specified server.	Enter the domain name of the server you want to query for SPF records.

Command	Description	Parameters
dig -x	(Email module only) Return the PTR information for the specified IP address.	Enter the IP address for the server you want to query for PTR information.
directory-agent-service	(Web module only; affects the Web Hybrid module) Disable or enable the Directory Agent service.	Enter **enable** to enable Directory Agent on the appliance. Enter **disable** to disable Directory Agent on the appliance.
email-subscription-reset	(Email module only; affects the Email Hybrid module) Clear all TRITON AP-EMAIL subscription information. After the command is run, the administrator must re-enter the subscription key. **Note:** If the network is unreachable, the command takes 30 minutes to time out.	None
email shell debug module	(Email module only) Debug the specified TRITON AP-EMAIL module. Click **Stop** to end the debug session.	Enter the name of the module you want to debug. Click the information icon for examples. Separate multiple entries with a comma. For example: `filter event all, config_daemon event all`

Command	Description	Parameters
ethtool	Display the current Ethernet card settings of the specified network interface (NIC) device. This includes: ● Advertised auto-negotiation ● Advertised pause frame use ● Advertised link modes ● Auto-negotiation setting ● Auto-negotiation support ● Current message level ● Duplex ● Link detection ● MDI-X ● Port ● Speed ● Supported link modes ● Supported ports ● PHYAD ● Transceiver ● Wake-on ● Wake-on status Use ethtool to verify local network connectivity. For example, if the ping command fails, use this to determine if you are using the right IP address.	None
ethtool -k	Display offload parameters, including checksum, for the selected network interface (NIC) device. This can be used to investigate a variety of problems. For example, if your NIC settings are right, but you are having duplex issues, you know you need to change your duplex settings.	None
ifconfig	Troubleshoot network interface issues. Identify IP issues and check subnets and network interfaces. Display status information about the specified network interface (NIC), including but not limited to: ● IP and broadcast address ● subnet mask ● number of packets received and transmitted ● number of bytes received and transmitted	Enter the NIC for which you want settings. Click the information icon for valid NIC values. Enter **all** to display all interface status. Example: eth0 or eth1

Command	Description	Parameters
maillog download	(Email module only) Download the specified maillog file.	Enter the file name for the mail log you want to download.
maillog show	(Email module only) Displays all available maillog file names, along with starting and ending timestamps and file size.	None
multiplexer	(Web module only) Enable and disable the Multiplexer service that supports SIEM integrations. Multiplexer service does not run on filtering only appliances.	Enter **enable** to enable the Multiplexer service. Enter **disable** to disable the Multiplexer service.
nc -uvz	The netcat (nc) utility attempts to read and write data across a network using user datagram protocol (UDP) to the specified server. Use it for component functional tests, to verify of connectivity, and to check data going across a UDP network. If you are having problems loading a web page, or are getting blocked, this command can help determine the problem. If you see a reset coming from the proxy, you can determine which module it is coming from. **-u** Run netcat in UDP mode **-v** Run netcat in verbose mode. **-z** Run netcat in zero I/O mode (used for scanning).	Enter the IP address of the server with which you want to communicate and the port number to use.
nc -vz	The netcat (nc) utility attempts to read and write data across a network using transmission control protocol (TCP) to the specified server. Use it for component functional tests and to verify of connectivity. **-v** Run netcat in verbose mode. **-z** Run netcat in zero I/O mode (used for scanning)	Enter the IP address of the server with which you want to communicate and the port number to use.

Command	Description	Parameters
netstat -neatup	Display a list of open sockets on the selected module, appended with the process column. **-n** Displays active TCP connections. Addresses and port numbers are expressed numerically, and no attempt is made to determine names. **-e** Displays ethernet statistics, such as the number of bytes and packets sent and received. **-a** Displays all active TCP connections and the TCP and UDP ports on which the computer is listening. **-t** Indicates which open ports are using TCP. **-u** Indicates which open ports are using UDP. **-p** Limits display of statistics or state of all sockets to those applicable to protocol.	None
netstat -ng	Display multicast group membership information about the selected module. **-n** Displays active TCP connections. Addresses and port numbers are expressed numerically, and no attempt is made to determine names. **-g** Shows the multicast group memberships for all interfaces.	None

Command	Description	Parameters
netstat - nItup	Display the following network statistics: ● the amount of traffic in your network ● all active TCP connections and the TCP and UDP ports on which the computer is listening Addresses and port numbers are expressed numerically, and no attempt is made to determine names. ● Ethernet statistics, such as the number of bytes and packets sent and received **-n** Displays active TCP connections and their ports. **-I** Shows the state of a particular interface, such as eth0 or eth1. **-t** Indicates which open ports are using TCP. **-u** Indicates which open ports are using UDP. **-p** Limits display of statistics or state of all sockets to those applicable to protocol.	None
netstat -s	Display summary statistics for each protocol in the selected module. By default, statistics are shown for IP, ICMP, TCP, UDP, and TCPEXT, including: ● the number of IP packets received, forwarded, and discarded ● the number of ICPM messages received, failed, sent ● the number of active and passive TCP connections and failed connection attempts ● the number of UDP packets received and sent ● TCPEXT statistics about SYN cookies, ACKs, packets received and queued, retransmits, and DSACKs	None

Command	Description	Parameters
nslookup	Query DNS servers to find DNS details, including IP addresses of a particular computer, MX records for a domain, and the DNS servers of a domain. Use this for DNS resolution problems.	Enter the hostname (for example myintranet.com) or IP address of the host for which you want DNS information, and the hostname or IP address of the DNS server for the appliance.
pem settings download	(Email module only) Download Personal Email Manager configuration settings, log files, and end-user personal Always Block/Permit files.	None
ping, ping6	Verify that a hostname or IP address exists and can accept requests from the selected module, and that DNS is resolving. Use this to test connectivity to another host— for example, the TRITON AP-DATA server or TRITON Manager machine—and determine response time. Use **ping** for IPv4 addresses, and **ping6** for IPv6 addresses. **Note:** **ping6** is not supported in either the TRITON AP-WEB or TRITON AP-EMAIL modules.	Enter the hostname (for example myintranet.com) or IP address of the host you want to test.
ping -I, ping6 -I	Verify that a network interface can communicate with a hostname or IP address and that DNS is resolving. **Note:** **ping6 -I** is not supported in the either the TRITON AP-WEB or TRITON AP-EMAIL modules.	Enter the name of the NIC you want to test (for example, eth0). Click the information icon for valid NIC values. Also enter the hostname or IP address of the host you want to test.
policy-broker-token	(Web module only) Use this command to retrieve the Policy Broker token for this appliance.	None
policy-engine	(Content Gateway module only) Start, stop, restart, or check the status of the policy engine.	Status: Enter ‘status’ to check the status of the policy engine Start: Enter ‘start’ to start the policy engine Stop: Enter ‘stop’ to stop the policy engine Restart: Enter ‘restart’ to restart the policy engine

Command	Description	Parameters
print-bypass	(Content Gateway module only) See which source and destination IPs the proxy is bypassing when Content Gateway is in transparent proxy caching mode. If a site is not loading correctly, identify if it is loading from your cache or being downloaded directly. All entries in the source and destination bypass tables for the proxy are printed to the output console. For more information on source and destination bypass, see the **Configuration Files > bypass.config** section of the Content Gateway Manager Help.	None
proxy-net-check	(Content Gateway module only) Display diagnostics for Content Gateway, such as: ● interface status ● connection to DNS name servers ● connection to Policy Server ● gateway packet loss ● ping statistics for various modules ● Internet connectivity ● filtering status This is useful for investigating latency issues, outages, policy enforcement problems, and so on.	None
route -A inet6 -n	Display the contents of the selected module's kernel IP routing table IPv6 entries in numeric format. This is useful in complex network environments—for example, those with proxy chaining—to see if the environment is set up properly.	Note: route -A inet6 -n is not supported in the TRITON AP-EMAIL module.
route -n	Display the contents of the selected module's kernel IP routing table in numeric format. This is useful in complex network environments—for example, those with proxy chaining—to see if the environment is set up properly.	None

Command	Description	Parameters
route add	(Content Gateway module only) This command supports all of the add route parameters available on the **Configuration > Routing** page of the Appliance manager. In addition, this command supports the ability to specify the maximum segment size (MSS).	Enter: ● the route type The host route is for routing to individual hosts. The net route is for an entire network or subnet. ● the target network address or host IP address for the route ● the netmask for the for the target network or host ● the IP address of the gateway (next hop router) ● the appliance interface to use for this route ● the maximum segment size to use for this route (expressed in octets)
state-server	(Web module only; full policy source or user directory and filtering appliance) In multiple Filtering Service deployments, State Server is required for proper application of time-based actions (Quota, Confirm, Password Override, and Account Override).	Enter **enable** to enable the State Server service. Enter **disable** to disable the State Server service.
sysctl-tcp-timestamps	(Content Gateway module only) View or change the setting for TCP time stamps. Edit this setting if you are experiencing performance problems with specific websites that do not properly support TCP time stamps. The operating system sets this kernel setting during installation. If the setting was changed and you are experiencing site latency with other sites—those that work best with TCP time stamps— return the setting to its default value and consider routing traffic to the problematic sites around the proxy. Be sure to choose a setting that works well for the sites that are most important to you. The setting affects the use of time stamps by the kernel for all TCP connections.	Enter **0** to disable the current time stamp setting, and restore it to its default. Enter **1** to re-enable a custom setting. Enter **view** to see the current setting.

Command	Description	Parameters
sysctl-tcp-window-scaling	(Content Gateway module only) View or change the setting for TCP window scaling. Edit this setting if you are experiencing performance problems with specific websites that do not properly support TCP windows scaling. The operating system sets this kernel setting during installation. If the setting was changed and you are experiencing site latency with other sites—those that work best with TCP windows scaling—return the setting to its default value and consider routing traffic to the problematic sites around the proxy. Be sure to choose a setting that works well for the sites that are most important to you. The setting affects the use of windows scaling by the kernel for all TCP connections.	Enter **0** to disable the current window scaling setting, and restore it to its default. Enter **1** to re-enable a custom setting. Enter **view** to view the current setting.

tcpdump	Get a raw packet dump to help diagnose web traffic issues—for example, if a site will not load or if you are having authentication problems.
	tcpdump intercepts and displays packets being transmitted or received by the specified network interface. Use the Expression field to select which packets are displayed.
	The output from **tcpdump** can help you determine whether all routing is occurring properly, to and from the interface. The output is verbose; it displays the data of each package in both hex and ASCII, and it includes a link-level header on each line.
	Note: If you do not stop the tcpdump command manually, 10,000 packets are captured, the maximum allowed.
		Enter the name of the NIC you are debugging (for example, eth0). Click the information icon for valid NIC values.
		Also enter a boolean expression that filters the packets to those of interest. Click the information icon for examples.
		Example 1: To capture all TCP traffic to and from the proxy on port 8080, enter this expression:
		`tcp port 8080`
		Example 2: To capture all TCP traffic to the site google.com, enter this expression:
		`tcp and dst host google.com`
		Example 3: To capture all TCP traffic from a specific end-user machine, enter this expression:
		`tcp and src host user.example.com`
		Note: You can enter a hostname if it is resolvable by a DNS server, but the output uses IP addresses.

Command	Description	Parameters
tcpdump -w	Dump traffic (raw packets) from the specified NIC to a file. To download the file, click **Download output file for last command** after running the command. This link is under the console output window. Forcepoint Technical Support may request this file on occasion.	Enter the name of the appliance NIC you are debugging. Click the information icon for valid NIC values. Also enter a boolean expression that filters the packets to those of interest. Click the information icon for examples. Enter **all** to capture all packets. **Note:** You can enter a hostname if it is resolvable by a DNS server, but the output uses IP addresses.
top -bn1	Display all operating system tasks that are currently running in the selected module to help diagnose CPU and memory issues. **-b** Run in batch mode. **-n** Update the display for a number of iterations, then exit. **-1** Do not display idle processes.	None
traceroute, traceroute6	Determine the route taken by packets across a network to a particular host. If some machines are not receiving policy enforcement, or if traffic is not getting to the appliance, this shows the devices (or hops) that are between the machines that may be blocking access to the host. Use **tcpdump** to get a packet capture from each device. If you are having latency issues, **traceroute** can also help identify the causes. Use **traceroute** for IPv4 addresses, and **traceroute6** for IPv6 addresses. **Note: traceroute** is of limited utility if an IP address is being spoofed. **Note: traceroute6** is not supported in the TRITON AP-WEB or the TRITON AP-EMAIL modules.	Enter the hostname or IP address of the host destination you are investigating

Command	Description	Parameters
user-group-ip-precedence	(Web module only) Change the precedence of identification attributes applied in policy enforcement. More details are available in the web protection Administrator Help.	Enter **enable** to modify the precedence order to: User > Group > Domain > Computer > Network Enter **disable** (default) to set the precedence order to: User > Computer > Network > Group > Domain Enter **status** to display the current setting. Filtering Service must stop and restart to change precedence settings.
wget	Initiate a non-interactive download of web files to diagnose connectivity issues. Use **wget**, for example, if you have configured the proxy, but cannot access the Web. **wget** simulates the proxy going out and retrieving the website. This command supports HTTP, HTTPS, and FTP protocols.	Enter the URL of the website from which you want to download files.
wget-proxy	Test connectivity between the specified URL and the proxy (file download not supported). Use **wget**, for example, if you have configured the proxy, but cannot access the Web. **wget** simulates the proxy going out and retrieving the website. This command supports HTTP, HTTPS, and FTP protocols.	Enter: ● the URL of the website to which you want to test connectivity ● the proxy IP address This is the IP address of the P1 interface on most appliance configurations. ● the port on which the proxy expects this traffic 8080 is configured for HTTP by default. 8070 is configured for HTTPS by default. ● the user name of the client, if required for authentication (otherwise, enter **none**) ● the password of the client, if required for authentication (otherwise, enter **none**)

V-Series appliance technical support tools

Help | V-Series Appliance | v8.2.x

When you collaborate with Forcepoint Technical Support or a Forcepoint partner to examine possible causes for network issues, these built-in tools can assist with troubleshooting:

Troubleshooting ports

TRITON AP-WEB provides the option to open troubleshooting ports temporarily, so that various troubleshooting tests can be run. (This facility is not available for TRITON AP-EMAIL.)

Use this tool only when directed to do so by Forcepoint Technical Support.

Mark **Enable troubleshooting ports**, then click **Save**.

Important

Clear the check box and click **Save** to disable the ports when Technical Support is done using them. Do not leave these ports open.

Appliance Configuration summary

The configuration summary tool gathers data from the appliance and generates an archive file that can be sent to Forcepoint Technical Support for analysis and debugging. The process takes 1 to 2 minutes.

When Forcepoint Technical Support requests this file:

1. Click **Generate File**.

   When the file is ready, a message appears at the top of the page: “Configuration summary has been successfully collected.”

2. Click the link in the message to download 7the archive file to your desktop.

   You can then open the file or save it to another location.

3. Your technician will provide an FTP site for secure file transfer to Forcepoint Technical Support.

Remote access

Enable remote access only at the request of Forcepoint Technical Support.

- When you click **On** and then click **Save**, a passcode is generated and displayed on screen.
- Provide the passcode to your Forcepoint Technical Support technician. This enables SSH, so that the technician can log on to your appliance.

- Each time you allow remote access to the appliance and a Forcepoint technician logs on, a record is added to the **Remote access logon history** at the bottom of the **Toolbox** page.
- When the technician is done, be sure to click **Off** and click **Save** to disable the access.

Account management

Help | V-Series Appliance | v8.2.x

Use the **Administration > Account Management** page to:

- Change the password for accessing the V-Series manager.
- Change the password for accessing Content Gateway manager when Content Gateway is run on the appliance.
- Specify the admin notification email address and SMTP server for Appliance manager password recovery email messages. For a description of the password recovery mechanism, see *V-Series manager password reset*.
- Change the help page language settings embedded in your appliance manager.
- Retrieve your password if you have lost or forgotten it.

Change password

In **Administration >Account Management > Change Password:**

1. Enter the current password.
2. Enter the new password.
3. Confirm the new password.
4. Select **OK** to save the new password.

Secure password guidelines

For V-Series appliances, the administrator password must meet the following requirements:

- Be between 8 and 15 characters in length
- Include 1 or more of the following:
  - Uppercase characters
  - Lowercase characters
  - Numbers
  - Special characters (for example, ! # % & ‘ ( ) * + , - . / < = > ? @ [ ] ^ _ { | } ~)

- Exclude all of the following:
  - The user name of any appliance service account (admin, root, websense-ts, audit)
  - Common appliance-related terms (e.g., appliance, filtering)
  - The name of TRITON services (e.g., TRITON, AP-WEB, AP-EMAIL, ContentGateway PolicyBroker, etc.)
  - The device’s hostname
- Do not repeat the previous 3 passwords for the account.

Change password for Content Gateway manager

In **Administration Account Management > Content Gateway Manager Password Reset:**

1. Select R**eset Password** to reset your proxy password.
2. The new password appears in the **Content Gateway Manager Password** group box. Write it down. Once you navigate away from the Account Management page, the password will no longer be displayed.
3. Log on to the Content Gateway manager with the new password.
4. Go to the **Configure > My Proxy > UI Setup > Login** page to change the password.

For additional guidance on how to create a strong, secure password, see *Secure password guidelines*.

Email notification and SMTP server for password recovery

In **Administration Account Management > Email Settings:**

1. In the **Notification email address** box, specify the email address to which password recovery email messages are sent.
2. In the **SMTP address** box, specify the SMTP server IP address
3. In the **Port** box, specify the port location.
4. If the SMTP connection requires authentication, select the checkbox labeled **SMTP server requires authentication**, and enter the Account and Password information in the corresponding boxes.
5. Select **Test Connection** to validate the SMTP settings.
6. Select **OK** to save the new values.

Language settings

In **Administration Account Management > Help Language Preference:**

- From the list of available languages in the drop-down list, select the language in which the Help system will display, then click **OK** to apply your selection.

V-Series manager password reset

If you forget or misplace your logon password, click **Forgot my password** on the Appliance manager logon page.

- If a notification email address and SMTP server have been configured, a temporary password is mailed to the email address. Log on using the temporary password within 1 hour and reset your password.
- If a notification email cannot be sent, an error message displays and you are advised to contact Forcepoint Technical Support. A security code is also provided. Make a note of it; it is required by Forcepoint Technical Support to generate a new password.

4 Copyrights and trademarks

Help | V-Series Appliance | v8.2.x

10900-A Stonelake Blvd, Quarry Oaks 1, Suite 350, Austin, TX 78759, USA

Published 2016
Printed in the United States of America

Every effort has been made to ensure the accuracy of this manual. However, Forcepoint LLC, makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. Forcepoint LLC shall not be liable for any error or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or the examples herein. The information in this documentation is subject to change without notice.

Trademarks

Forcepoint and ThreatSeeker are registered trademarks of Forcepoint LLC, in the United States and certain international markets. Forcepoint has numerous other unregistered trademarks in the United States and internationally. All other trademarks are the property of their respective owners.

Microsoft, Internet Explorer, and Active Directory are trademarks or registered trademarks of Microsoft Corporation.

The following is a registered trademark of Novell, Inc., in the United States and other countries: Novell Directory Services.

Adobe, Acrobat, and Acrobat Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Pentium is a registered trademark of Intel Corporation.

Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are the sole property of their respective manufacturers.

Other acknowledgments

Portions of this software may utilize the following copyrighted material, the use of which is hereby acknowledged.

CentOS

CentOS-6 EULA

CentOS-6 comes with no guarantees or warranties of any sorts, either written or implied.

The Distribution is released as GPL. Individual packages in the distribution come with their own licenses.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of

Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING

ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

Xen

Version 4.2.0

Copyright © 2005 XenSource, Inc. All use and distribution of this copyrighted material is governed by and subject to terms and conditions as licensed by XenSource, Inc. All other rights reserved. Unless otherwise specified, this software is licensed under the terms of the GNU General Public License, version 2. This software comprises a compilation work of XenSource, Inc., and is released under the terms of the GNU General Public License as a whole. Trademarks, service marks, and logos ("Trademarks") displayed are registered and unregistered Trademarks of XenSource, Inc. or of third parties.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING

ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

XML-RPC For C/C++ License

Version 1.16.24

Copyright (C) 2001 by First Peer, Inc. All rights reserved.

Copyright (C) 2001 by Eric Kidd. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

JRE

Version 1.8.0_45

Oracle Binary Code License Agreement for the Java SE Platform Products and JavaFX

1. DEFINITIONS. "Software" means the software identified above in binary form that you selected for download, install or use (in the version You selected for download, install or use) from Oracle or its authorized licensees, any other machine readable materials (including, but not limited to, libraries, source files, header files, and data files), any updates or error corrections provided by Oracle, and any user manuals, programming guides and other documentation provided to you by Oracle under this Agreement. "General Purpose Desktop Computers and Servers" means computers, including desktop and laptop computers, or servers, used for general computing functions under end user control (such as but not specifically limited to email, general purpose Internet browsing, and office suite productivity tools). The use of Software in systems and solutions that provide dedicated functionality (other than as mentioned above) or designed for use in embedded or function-specific software applications, for example but not limited to: Software embedded in or bundled with industrial control systems, wireless mobile telephones, wireless handheld devices, kiosks, TV/STB, Blu-ray Disc devices, telematics and network control switching equipment, printers and storage management systems, and other related systems are excluded from this definition and not licensed under this Agreement. "Programs" means (a) Java technology applets and applications intended to run on the Java Platform, Standard Edition platform on Java-enabled General Purpose Desktop Computers and Servers; and (b) JavaFX technology applications intended to run on the JavaFX Runtime on JavaFX-enabled General Purpose Desktop Computers and Servers. “Commercial Features” means those features identified in Table 1-1 (Commercial Features In Java SE Product Editions) of the Java SE documentation accessible at http://www.oracle.com/technetwork/java/javase/documentation/index.html. “README File” means the README file for the Software accessible at http://www.oracle.com/technetwork/java/javase/documentation/index.html.

2. LICENSE TO USE. Subject to the terms and conditions of this Agreement including, but not limited to, the Java Technology Restrictions of the Supplemental License Terms, Oracle grants you a non-exclusive, non-transferable, limited license without license fees to reproduce and use internally the Software complete and unmodified for the sole purpose of running Programs. THE LICENSE SET FORTH IN THIS SECTION 2 DOES NOT EXTEND TO THE COMMERCIAL FEATURES. YOUR RIGHTS AND OBLIGATIONS RELATED TO THE COMMERCIAL FEATURES ARE AS SET FORTH IN THE SUPPLEMENTAL TERMS ALONG WITH ADDITIONAL LICENSES FOR DEVELOPERS AND PUBLISHERS.

3. RESTRICTIONS. Software is copyrighted. Title to Software and all associated intellectual property rights is retained by Oracle and/or its licensors. Unless enforcement is prohibited by applicable law, you may not modify, decompile, or reverse engineer Software. You acknowledge that the Software is developed for general use in a variety of information management applications; it is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use the Software in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle disclaims any express or implied warranty of fitness for such uses. No right, title or interest in or to any trademark, service mark, logo or trade name of Oracle or its licensors is granted under this Agreement. Additional restrictions for developers and/or publishers licenses are set forth in the Supplemental License Terms.

4. DISCLAIMER OF WARRANTY. THE SOFTWARE IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. ORACLE FURTHER DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT.

5. LIMITATION OF LIABILITY. IN NO EVENT SHALL ORACLE BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, PUNITIVE OR CONSEQUENTIAL DAMAGES, OR DAMAGES FOR LOSS OF PROFITS, REVENUE, DATA OR DATA USE, INCURRED BY YOU OR ANY THIRD PARTY, WHETHER IN AN ACTION IN CONTRACT OR TORT, EVEN IF ORACLE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. ORACLE'S ENTIRE LIABILITY FOR DAMAGES HEREUNDER SHALL IN NO EVENT EXCEED ONE THOUSAND DOLLARS (U.S. $1,000).

6. TERMINATION. This Agreement is effective until terminated. You may terminate this Agreement at any time by destroying all copies of Software. This Agreement will terminate immediately without notice from Oracle if you fail to comply with any provision of this Agreement. Either party may terminate this Agreement immediately should any Software become, or in either party's opinion be likely to become, the subject of a claim of infringement of any intellectual property right. Upon termination, you must destroy all copies of Software.

7. EXPORT REGULATIONS. You agree that U.S. export control laws and other applicable export and import laws govern your use of the Software, including technical data; additional information can be found on Oracle's Global Trade Compliance web site (http://www.oracle.com/us/products/export). You agree that neither the Software nor any direct product thereof will be exported, directly, or indirectly, in violation of these laws, or will be used for any purpose prohibited by these laws including, without limitation, nuclear, chemical, or biological weapons proliferation.

8. TRADEMARKS AND LOGOS. You acknowledge and agree as between you and Oracle that Oracle owns the ORACLE and JAVA trademarks and all ORACLE- and JAVA-related trademarks, service marks, logos and other brand designations ("Oracle Marks"), and you agree to comply with the Third Party Usage Guidelines for Oracle Trademarks currently located at http://www.oracle.com/us/legal/third-party-trademarks/index.html . Any use you make of the Oracle Marks inures to Oracle's benefit.

9. U.S. GOVERNMENT LICENSE RIGHTS. If Software is being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), then the Government's rights in Software and accompanying documentation shall be only those set forth in this Agreement.

10. GOVERNING LAW. This agreement is governed by the substantive and procedural laws of California. You and Oracle agree to submit to the exclusive jurisdiction of, and venue in, the courts of San Francisco, or Santa Clara counties in California in any dispute arising out of or relating to this agreement.

11. SEVERABILITY. If any provision of this Agreement is held to be unenforceable, this Agreement will remain in effect with the provision omitted, unless omission

would frustrate the intent of the parties, in which case this Agreement will immediately terminate.

12. INTEGRATION. This Agreement is the entire agreement between you and Oracle relating to its subject matter. It supersedes all prior or contemporaneous oral or written communications, proposals, representations and warranties and prevails over any conflicting or additional terms of any quote, order, acknowledgment, or other communication between the parties relating to its subject matter during the term of this Agreement. No modification of this Agreement will be binding, unless in writing and signed by an authorized representative of each party.

SUPPLEMENTAL LICENSE TERMS

These Supplemental License Terms add to or modify the terms of the Binary Code License Agreement. Capitalized terms not defined in these Supplemental Terms shall have the same meanings ascribed to them in the Binary Code License Agreement. These Supplemental Terms shall supersede any inconsistent or conflicting terms in the Binary Code License Agreement, or in any license contained within the Software.

A. COMMERCIAL FEATURES. You may not use the Commercial Features for running Programs, Java applets or applications in your internal business operations or for any commercial or production purpose, or for any purpose other than as set forth in Sections B, C, D and E of these Supplemental Terms. If You want to use the Commercial Features for any purpose other than as permitted in this Agreement, You must obtain a separate license from Oracle.

B. SOFTWARE INTERNAL USE FOR DEVELOPMENT LICENSE GRANT. Subject to the terms and conditions of this Agreement and restrictions and exceptions set forth in the README File incorporated herein by reference, including, but not limited to the Java Technology Restrictions of these Supplemental Terms, Oracle grants you a non-exclusive, non-transferable, limited license without fees to reproduce internally and use internally the Software complete and unmodified for the purpose of designing, developing, and testing your Programs.

C. LICENSE TO DISTRIBUTE SOFTWARE. Subject to the terms and conditions of this Agreement and restrictions and exceptions set forth in the README File, including, but not limited to the Java Technology Restrictions and Limitations on Redistribution of these Supplemental Terms, Oracle grants you a non-exclusive, non-transferable, limited license without fees to reproduce and distribute the Software, provided that (i) you distribute the Software complete and unmodified and only bundled as part of, and for the sole purpose of running, your Programs, (ii) the Programs add significant and primary functionality to the Software, (iii) you do not distribute additional software intended to replace any component(s) of the Software, (iv) you do not remove or alter any proprietary legends or notices contained in the Software, (v) you only distribute the Software subject to a license agreement that: (a) is a complete, unmodified reproduction of this Agreement; or (b) protects Oracle's interests consistent with the terms contained in this Agreement and that includes the notice set forth in Section H, and (vi) you agree to defend and indemnify Oracle and its licensors from and against any damages, costs, liabilities, settlement amounts and/ or expenses (including attorneys' fees) incurred in connection with any claim, lawsuit or action by any third party that arises or results from the use or distribution of any and all Programs and/or Software. The license set forth in this Section C does not extend to the Software identified in Section G.

D. LICENSE TO DISTRIBUTE REDISTRIBUTABLES. Subject to the terms and conditions of this Agreement and restrictions and exceptions set forth in the README File, including but not limited to the Java Technology Restrictions and Limitations on Redistribution of these Supplemental Terms, Oracle grants you a non-exclusive, non-transferable, limited license without fees to reproduce and distribute those files specifically identified as redistributable in the README File ("Redistributables") provided that: (i) you distribute the Redistributables complete and unmodified, and only bundled as part of Programs, (ii) the Programs add significant and primary functionality to the Redistributables, (iii) you do not distribute additional software intended to supersede any component(s) of the Redistributables (unless otherwise specified in the applicable README File), (iv) you do not remove or alter any proprietary legends or notices contained in or on the Redistributables, (v) you only distribute the Redistributables pursuant to a license agreement that: (a) is a complete, unmodified reproduction of this Agreement; or (b) protects Oracle's interests consistent with the terms contained in the Agreement and includes the notice set forth in Section H, (vi) you agree to defend and indemnify Oracle and its licensors from and against any damages, costs, liabilities, settlement amounts and/or expenses (including attorneys' fees) incurred in connection with any claim, lawsuit or action by any third party that arises or results from the use or distribution of any and all Programs and/or Software. The license set forth in this Section D does not extend to the Software identified in Section G.

Tomcat

Version 7.0.54

Copyright © 2007 Apache Software Foundation (ASF)

Apache License
Version 2.0, January 2004
http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

a.You must give any other recipients of the Work or Derivative Works a copy of this License; and

b.You must cause any modified files to carry prominent notices stating that You changed the files; and

c.You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

d.If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

Anaconda

Version 13.21.239

Copyright, Continuum Analytics, Inc.

All rights reserved under the 3-clause BSD License:

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of Continuum Analytics, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL CONTINUUM ANALYTICS, INC. BE

LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.