

v8.3.0 Release Notes for TRITON Appliances

Release Notes | TRITON Appliances | 17-May-2017

Use these Release Notes to learn about what's new and improved for TRITON® V-Series™, X-Series™, and Forcepoint™ APX Virtual Appliance in version 8.3.0.



Important

Some older V10000 and V5000 appliances are not supported with versions of 8.0 and higher. See [V-Series appliance models supported with version 8.3](#), page 10.



Important

Dual Mode appliances are not supported with version 8.3.0 and higher. See [Dual Mode appliances](#), page 13.

Contents

- [New for v8.3.0 TRITON appliances](#), page 2
- [Resolved and known issues for v8.3.0 V-Series and X-Series appliances](#), page 24

For information about which product versions are supported on which appliance platforms, see [TRITON solutions on TRITON appliance platforms](#), page 4, and the Forcepoint [appliance compatibility matrix](#).

For information about getting started with TRITON appliances, see [TRITON Appliances Getting Started](#).

For information about upgrading TRITON appliances, see:

- [V-Series Upgrade Guide](#)
- [V-Series Appliances: 5-Step Upgrade Guide to v8.3](#)
- [X-Series Upgrade Guide](#)
- [Upgrading V-Series Dual Mode Appliances to Version 8.3](#)

Also see these companion Release Notes for information about the TRITON protection solutions that run on TRITON appliances:

- [v8.3.0 Release Notes for TRITON Web Protection Solutions](#)
- [v8.3.0 Release Notes for TRITON AP-EMAIL](#)
- [v8.3.0 Release Notes for TRITON AP-DATA](#)
- [v8.3.0 TRITON Manager Release Notes](#)

New for v8.3.0 TRITON appliances

Release Notes | TRITON Appliances | 17-May-2017

Forcepoint is pleased to release version 8.3.0 of the Forcepoint appliance infrastructure. Changes in this update improve every aspect of TRITON appliance form and function, and establish the foundation for future advances.

Because of the scope of the changes, these release notes are lengthy.

- *Forcepoint TRITON appliance architecture*, page 3
- *TRITON solutions on TRITON appliance platforms*, page 4
- *Direct upgrade to v8.3.0*, page 9
- *V-Series appliance models supported with version 8.3*, page 10
- *Platform hardening*, page 11
- *System logging*, page 12
- *Audit logging*, page 12
- *No longer supported and notable restrictions*, page 12
- *Forcepoint Security Appliance Manager*, page 16
- *Command-line interface (CLI)*, page 16
- *TRITON appliance API*, page 20
- *Changes for V-Series*, page 21
- *Changes for X-Series*, page 22
- *Web protection features*, page 22
- *Security updates*, page 23
- *TRITON Appliances documentation*, page 24

Forcepoint TRITON appliance architecture

The Forcepoint TRITON appliance infrastructure has a new architecture. The new architecture:

- Is a single common architecture used by all TRITON appliance platforms: V-Series, X-Series, Forcepoint APX Virtual Appliance.
- Is a single common code base that delivers a more efficient and stable environment.
- Is a more secure environment. The common architecture and code base, in addition to platform hardening, reduce attack surfaces.
- Allows a single ISO/OVA/VHD to be used to install TRITON software on all TRITON appliance platforms.
- Quickly and easily supports new hardware and virtual appliance platforms.
- Quickly and easily supports TRITON product integration using a standardized data specification and calls to the [TRITON appliance API](#).
- Maintains a clean separation between TRITON products and appliance code. There is no mixing of TRITON product code with TRITON appliance code.
- Uses LXC (Linux Containers) to host TRITON product modules, such as the core web protection module, web proxy module, core email module, and others.

LXC replaces the former XEN and guests architecture.

Benefits of LXC include:

- More efficient and flexible allocation, protection, control, and monitoring of system resources.
- Improved performance.
- An environment that more quickly and easily supports new Forcepoint technologies and appliance platforms.
- Includes a command-line interface (CLI), that supports all appliance configuration, maintenance, monitoring, and troubleshooting functions. See [Command-line interface \(CLI\)](#).
- Includes an appliance management REST API that supports all appliance functions. See [TRITON appliance API](#).
- Uses CentOS 7.2 as the base operating system and with the TRITON AP-EMAIL container. Uses CentOS 6.8 in web protection solution containers.
















Modules

The TRITON appliance controller software (installed in the base operating system) and the functional units of TRITON software installed in the LXC containers, are each a **module** of the appliance. TRITON appliance modules have the following names:

app	TRITON appliance controller
email (old name: esg)	TRITON AP-EMAIL

web (old name: wse)	TRITON web protection
proxy (old name: wcg)	Content Gateway web proxy – TRITON AP-WEB only
network-agent (old name: na)	TRITON web protection (V-Series only)

TRITON solutions on TRITON appliance platforms

Product \ Platform	V5000	V10000	X10G	VMware	Azure
TRITON AP-EMAIL					
TRITON AP-WEB					
Network Agent					
Web Filter & Security					
Network Agent					
TRITON AP-DATA					
Protector					
Mobile Agent					
TRITON AP-DATA with Email Gateway for Microsoft Office 365					

For detailed information about deploying any of the TRITON AP-DATA solutions on TRITON appliances, see the **TRITON AP-DATA** section of the [Forcepoint documentation](#) page.

For detailed information about deploying TRITON AP-WEB Cloud with an i-Series appliance, see the **Forcepoint i-Series Appliance** section of the [Forcepoint Documentation](#) page.

V-Series specifications

1 rack-unit form factor

See the [V-Series Appliance datasheet](#) (PDF on the Forcepoint website) for specifications of the currently shipping model.

V10000

Supported solutions

- TRITON AP-EMAIL (certified)
- TRITON AP-WEB (certified)

Supported models with v8.3

- V10000 G4
- V10000 G3
- V10000 G2R2

Network interfaces

All V10000 appliances come with 6 physical Ethernet interfaces

C — Supports TRITON appliance management communication

P1, P2 — Support Content Gateway (web proxy) traffic (TRITON AP-WEB only)

E1, E2 — Support MTA traffic (TRITON AP-EMAIL)

N — Supports Network Agent (Web protection solutions)

Interface bonding: With TRITON AP-WEB and TRITON AP-EMAIL, interfaces P1 and E1 can be bonded, and interfaces P2 and E2 can be bonded.

V5000 specification

Supported solutions

- TRITON AP-EMAIL (certified)
- TRITON AP-WEB (certified)
- Forcepoint Web Filter & Security (certified)

Supported models with v8.3

- V5000 G4
- V5000 G3
- V5000 G2R2

Network interfaces

All V5000 appliances come with 4 physical Ethernet interfaces.

C — Supports TRITON appliance management communication

P1, P2 — Support Content Gateway (web proxy) traffic (TRITON AP-WEB) or MTA traffic (TRITON AP-EMAIL)

N — Supports Network Agent (Web protection solutions)

X-Series specifications

10 rack-unit form factor; chassis hosts up to 16 X10G blade servers

See the [X-Series Appliance datasheet](#) (PDF on the Forcepoint website) for specifications of the currently shipping model.

Supported solutions

- TRITON AP-EMAIL (certified)
- TRITON AP-WEB (certified)

Supported models with v8.3

- X10G G2 blade server
- X10G G1 blade server

Network interfaces

All X-Series appliances come with 2 PowerConnect M6220 switches. Each supports 2 10Gb SFP+ ports.

All X10G security blades support 3 virtual Ethernet interfaces.

C — Supports TRITON appliance management communication

P1, P2 — Support Content Gateway (web proxy) traffic (TRITON AP-WEB) or MTA traffic (TRITON AP-EMAIL)

Forcepoint APX Virtual Appliance specifications

ESXi VMware

New for v8.3.0, Forcepoint APX Virtual Appliance certified with ESXi v6.0, and supported on v5.5 and other versions of 6.x.

Supported solutions

- TRITON AP-EMAIL (certified)
- TRITON AP-WEB (certified)
- Forcepoint Web Filter & Security (supported)

TRITON AP-EMAIL VM specification

The install OVA creates a virtual machine with the following specifications:

- 4 CPU cores
- 12 GB RAM
- 1 - 100 GB disk
- 1 - 245 GB disk
- 4 E1000 virtual network interfaces



Important

These resources must be maintained as specified. When the Forcepoint security software starts, if the resources do not match the specification the application containers will not start. In the CLI, a persistent message displays indicating that the resources have been modified.

Network interfaces:

All TRITON AP-EMAIL VMware virtual appliances come with 4 virtual Ethernet interfaces.

C — Supports TRITON appliance management communication

P1, P2 — Support MTA traffic

N — Reserved

TRITON AP-WEB and Forcepoint Web Filter & Security VM specification



Note

The policy mode **Filtering only** is not supported on VMware virtual appliances with version 8.3.0.

The install OVA creates a virtual machine with the following specifications:

- 6 CPU cores
- 12 GB RAM
- 2 - 100 GB disk

- 4 E1000 virtual network interfaces (1 reserved port)

**Important**

These resources must be maintained as specified above. When the Forcepoint security software starts, if the resources do not match the specification the application containers will not start. In the CLI, a persistent message displays indicating that the resources have been modified.

Network interfaces

All TRITON AP-WEB and Forcepoint Web Filter & Security VMware virtual appliances come with 4 virtual Ethernet interfaces.

C — Supports TRITON appliance management communication

P1, P2 — Support Content Gateway web proxy traffic

N — Reserved; Network Agent and Content Gateway decryption port mirror are not supported on VMware virtual appliances in v8.3.0.

Azure virtual appliance specifications

TRITON AP-DATA Email Gateway for Microsoft Office 365

TRITON AP-DATA Email Gateway for Microsoft Office 365 is a virtual appliance for the Azure cloud infrastructure that allows you to protect data being sent through Exchange Online email. For detailed information, see .

Direct upgrade to v8.3.0

V-Series appliances can be upgraded directly to 8.3.0 from any of these versions:

7.8.4, 8.0.x, 8.1.x, 8.2.x.

X-Series appliances can be upgraded directly to 8.3.0 from any of these versions:

8.0.x, 8.1.x, 8.2.x.



Important

Dual Mode appliances are not supported with version 8.3.0 and higher. Either TRITON AP-EMAIL or the web protection solution must be migrated to a new appliance. For more information, see [Dual Mode appliances](#), page 13.

Forcepoint V5000 G2R2 Appliance customers may encounter a memory shortage after upgrading to version 8.2 or later. This issue is the result of newer versions of software requiring additional memory, and was only captured under a very heavy load. A DIMM Kit (2 x 8GB) is certified to expand the physical memory of the V5000 G2R2 Appliance. It is now generally available and recommended for V5000 G2R2 deployment moving to versions 8.2 and later. Please contact your sales representatives for purchase information. For more details, see the related [Knowledge Base article](#) and the [DIMM Kit installation instructions](#).

For upgrade instructions, see:

- [V-Series Upgrade Guide](#)

- [X-Series Upgrade Guide](#)
- [Upgrading V-Series Dual Mode Appliances to Version 8.3](#)

V-Series appliance models supported with version 8.3

Version 8.3.0 is supported on these V-Series appliances:

V10000	V5000
V10000 G4	V5000 G4
V10000 G3	V5000 G3
V10000 G2 R2	V5000 G2 R2

Older V10000 G2 and V5000 G2 appliances, known as revision 1 (or R1) appliances, are not supported with version 8.0.0 and higher. These models stopped shipping:

V10000 G2 R1:	Third quarter, 2011
V5000 G2 R1:	First quarter, 2012

If you plan to upgrade from any version of 7.x to any version of 8.x, you should verify the full hardware platform model of the appliances you plan to upgrade.

In some cases your hardware platform information is available on the **Configuration > System** page in the Appliance manager. Refer to the **System Information** box at the top of the page.

System	
System Information	
Hostname:	V10KG3.example.com
Security mode:	Web and Email
Appliance Version:	8.0.0
Hardware Platform:	V10000 G3
Date/time:	Apr 10, 2015 01:06:59 GMT
Uptime:	31 Days 14 Hours 17 Minutes

This will tell you if you have a G3 or G4 appliance. However, for V10000 G2 and V5000 G2 machines, the summary does not indicate whether the appliance is an R1 or R2 model.

If you have a G2 appliance, use the following steps to determine if it's R1 or R2 hardware.

1. Record your appliance service tag numbers (STN). You can find the STN printed on the pull out tag on the front of the appliance, behind the bezel (if installed). The STN is a 7 character code (for example: 9DZTBQ1).

2. Contact Forcepoint Technical Support and request assistance in identifying the full model version of your appliances.

Platform hardening

These measures harden all V-Series, X-Series, and Forcepoint APX Virtual Appliances.

- CentOS 7.2 operating system — Base operating system and TRITON AP-EMAIL container
- CentOS 6.8 operating system — Web protection containers (Web, Proxy, Network Agent)
- SELinux enabled (not enforcing)
- Apache Tomcat removed

System logging

TRITON appliances use Python and **syslog** for system logging. Logs are located in `/var/log/appliances/`

Logs are available for:

- The base operating system (app module): system and audit
- Each container has a “module” log (email, web, proxy, network-agent)

To view system logs in the CLI, use the ‘show log’ commands.

Audit logging

All CLI access and command activity is recorded in an audit log.

To view the log, use the ‘show log’ commands. For example, to display the last 100 lines of the audit log use:

```
show log lastline --module app --type audit --line 100
```

Typical entries look like:

```
2016-12-13 21:49:30,627 - INFO - appcli[165] - Account
admin, logged on from 10.64.161.8, entered view mode.
2016-12-13 21:49:59,042 - INFO - authentication - 13039 -
User <admin> attempting to log into API.
2016-12-13 21:49:59,094 - INFO - authentication - 13039 -
User <admin> authorization: True
2016-12-13 21:49:59,102 - INFO - common[976] - Account
admin, logged on from 10.64.161.8, entered config mode.
```

No longer supported and notable restrictions

- *Dual Mode appliances*
- *V-Series Appliance Manager*
- *Accessing V-Series appliances*
- *Changing the appliance management interface (C) IP address*
- *Rerun of firstboot*
- *Content Gateway Manager 2-factor authentication*

Dual Mode appliances

Version 8.3 does not support single appliances that host *both* TRITON AP-EMAIL and TRITON AP-WEB or Web Filter & Security. These appliances, known as Dual Mode appliances, have always been limited to the V-Series platform.

The new TRITON appliance architecture streamlines and optimizes the allocation and supervision of platform resources and processes to provide the best performance for the hosted Forcepoint solution. Stability, scaling, and operating efficiencies all improve in the single mode environment.

Before upgrading a Dual Mode appliance to v8.3, either the email or web module must be migrated to a new TRITON appliance. To ease the migration effort, special tools have been developed, and a special procedure is recommended. For details, see [Upgrading V-Series Dual Mode Appliances to Version 8.3](#). Contact your Forcepoint account representative to learn about special promotions for Dual Mode deployments planning a v8.3 upgrade.

V-Series Appliance Manager

In version 8.3, the V-Series Appliance Manager is replaced by the *Forcepoint Security Appliance Manager*. The Forcepoint Security Appliance Manager will be released in 2017. These release notes will be updated when the Forcepoint Security Appliance Manager becomes available. Until then, TRITON appliances can be fully and completely configured and monitored with the *Command-line interface (CLI)*. And, of course, the CLI remains available after the Forcepoint Security Appliance Manager is released.

A special document is available that maps V-Series Appliance Manager functions to CLI equivalents. See the [V-Series: Visual Primer for CLI v8.3](#) (PDF).

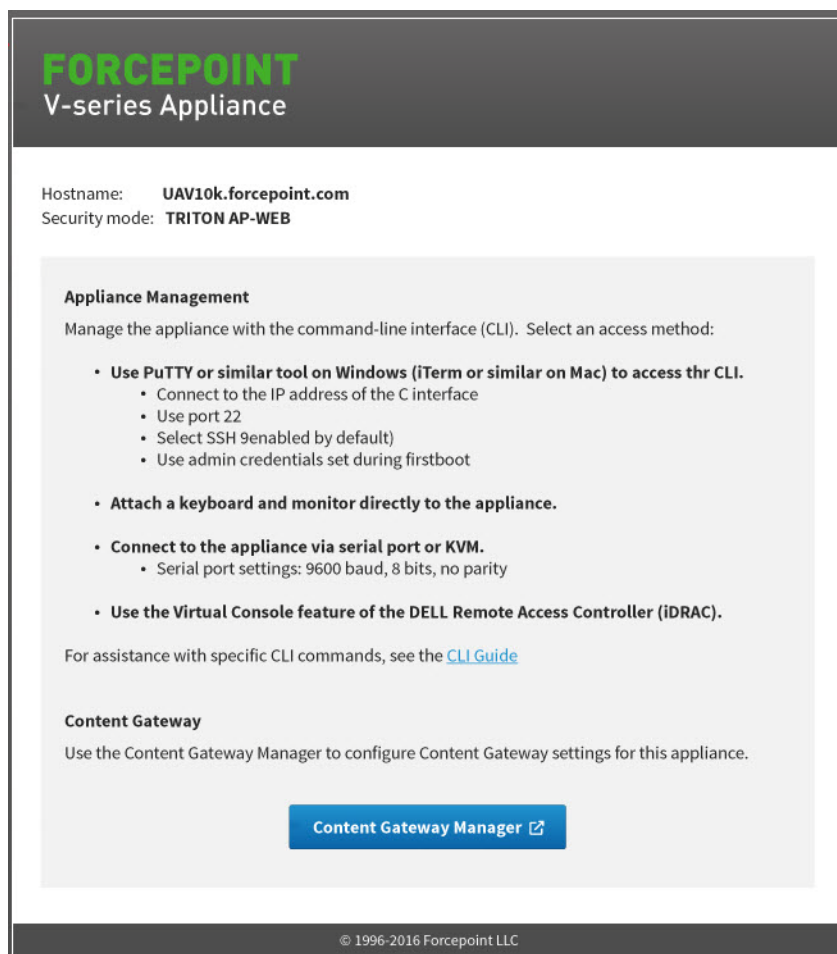
Accessing V-Series appliances

In v8.2 and earlier, V-Series appliances provided a logon portal to the Appliance Manager and Content Gateway Manager (TRITON AP-WEB). The portal could be accessed directly in a browser or, if the appliance was registered in TRITON Manager, via a single sign-on link.

In v8.3, as in past releases, TRITON appliances can be registered in the TRITON Manager, and the single sign-on feature can be enabled. (For details, see **Accessing Appliances** in [TRITON Manager Help](#).) However, until the Forcepoint Security Appliance Manager is available, the logon portal (accessed via the single sign-on link, directly on port 9447 of the C interface IP address, and via bookmarks), opens a temporary page that:

- Identifies the target appliance
- Describes access alternatives to connect to the command-line interface
- Includes a link to Content Gateway Manager when the appliance hosts TRITON AP-WEB

The page is similar to:



Accessing the Content Gateway manager

Content Gateway Manager hosted on any appliance or standalone server can be accessed in a browser by going to:

`https://<C interface IP address>:8081`

Changing the appliance management interface (C) IP address

If at all possible, do not change the appliance management interface (C) IP address of your appliance. What is affected and what must be done depends on the configuration of your appliance.

If your appliance hosts TRITON AP-EMAIL and you must change the C interface IP address, follow the procedure in the [Changing the C Interface IP Address](#) technical article.

If your appliance hosts TRITON AP-WEB, changing the C IP address requires a full reinstall (re-image) of the appliance. See the knowledge base article [How to restore a V-Series or X-Series appliance to a v8.3.x factory image](#).



Warning

The **set interface ipv4** command allows you to change the configuration of any available network interface, including the C interface IP address.

Rerun of firstboot

In version 8.3, it is no longer possible to rerun firstboot after it has successfully completed. However, every setting *except* the security mode, can be updated in the CLI.

To change the security mode (TRITON AP-EMAIL, TRITON AP-WEB, Web Filter & Security), the appliance must be re-imaged.

Content Gateway Manager 2-factor authentication

Content Gateway Manager 2-factor authentication is supported, however, when Content Gateway is on an appliance, you must contact Technical Support for assistance with disabling direct logon.

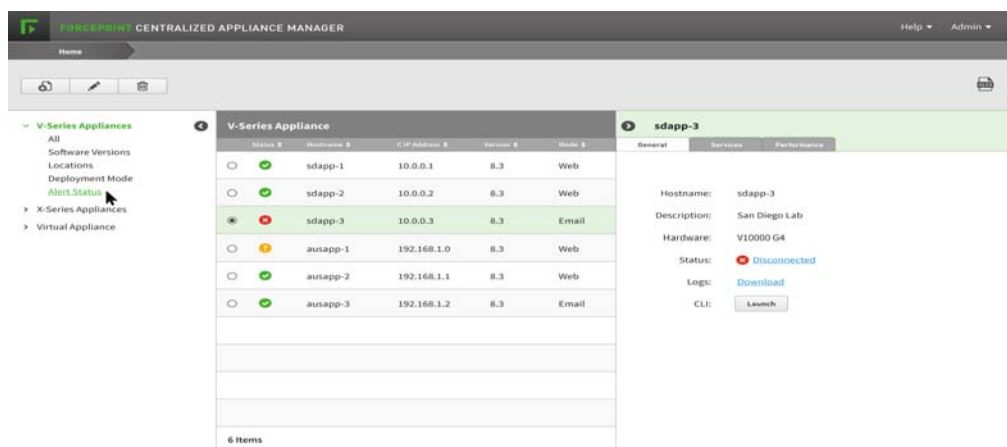
Forcepoint Security Appliance Manager

Coming in 2017 is a completely new, web-based GUI interface—the **Forcepoint Security Appliance Manager**. The Forcepoint Security Appliance Manager is a single, centralized management console for all models of TRITON appliances in your deployment. It will be located on the TRITON Management Server and integrate with TRITON Manager.



Important

Forcepoint Security Appliance Manager will be available in 2017.



Command-line interface (CLI)

In version 8.3, all appliances can be configured and maintained through a command-line interface (CLI). The CLI is familiar to X-Series users, for whom it has been the sole appliance management and configuration interface since v7.8.2. While V-Series users have for many releases had a CLI containing a subset of management and configuration commands, the v8.3 CLI is significantly expanded. It also uses a different structure and syntax. (V-Series administrators who prefer a GUI can look forward to the introduction of the [Forcepoint Security Appliance Manager](#) in 2017.)

Below is a small introduction to the CLI. For complete details, see the [TRITON Appliances CLI Guide](#). See also, the [V-Series: Visual Primer for CLI v8.3](#), and the [CLI Command Comparison Table 8.2 to 8.3](#).

In this section:

- [Accessing the CLI](#), page 17
- [CLI modes](#), page 18
- [Command-line structure](#), page 18

- [Functional areas](#), page 19
- [Embedded CLI help](#), page 19
- [New commands in v8.3](#), page 20

Accessing the CLI

Depending on appliance model, there are several ways to connect to the appliance console and, hence, the CLI. Once connected, the console presents a logon prompt. Log on with the **admin** credentials.

All platforms: SSH

All appliance platforms can connect to the appliance console with SSH. You can enable SSH access via the CLI through one of the other access methods for your platform. Use the following command in **config** mode to enable SSH.

```
set access ssh --status on
```

To connect with SSH, on a Windows system use **PuTTY**, or similar. On a Mac system use **Terminal**.

Connect to the appliance management interface (C) IP address on port 22.

V-Series and X-Series

iDRAC

All X-Series appliances and most V-Series appliances supported with v8.3.0, have an integrated DELL Remote Access Controller (iDRAC).

Log on to the iDRAC and go to **Overview > Server**. In the upper right **Virtual Console Preview** area, click **Launch**.

VGA and USB

Connect a monitor and keyboard directly to the appliance.

Serial port

Configure a serial connection to a monitor and keyboard. The connection should be set to:

- 9600 baud rate
- 8 data bits
- no parity

VMware virtual appliance

vSphere Client

Use the Console feature of the vSphere Client. In vSphere Client, select the virtual machine, open the Console, and click into the window to give it focus.

CLI modes

The CLI has 3 modes.

Mode Name	Description
view	The default mode. Used for displaying status and settings.
config	The mode required for changing settings and enabling/disabling options.
diagnose	The mode used to perform troubleshooting. It includes system and network diagnostic commands.

Command-line structure

The CLI syntax follows this format:

Command + Option + Parameter

Typically, verbs such as **show**, **set**, and **save** are used to view status or statistics, to change the configuration, and to initiate actions.

For example:

```
# set system clock --date <yyyy/mm/dd>
```

In this example:

- **set system** is the command.
- **clock** is the option.
- **--date** is the parameter, which takes a value in the format yyyy/mm/dd.

Other conventions include:

- Angled bracket, which indicate the value or set of options available for a parameter:
`--mask <ip_address>`
`--module <email|web|proxy>`
- Square brackets, which indicate that the parameter is optional:
`[--description <description>]`
- Pipes or vertical bars, which separate parameter options:
`<email|web|proxy>`

Functional areas

The CLI commands may be grouped into these functional areas:

- Configuration
 - Time and date
 - Hostname and description
 - Filestore definition and file save commands
 - Network interface configuration
 - Static routes
 - Appliance status
 - SNMP monitoring and traps
 - Module-specific commands
- Maintenance and support
 - Starting and stopping services
 - Module status and services details
 - Setting the web protection policy mode
 - Upgrades and hotfixes
 - Backup and restore
 - Log files
- Diagnostics

Embedded CLI help

Assistance is built into the CLI. There are 4 ways to get assistance.

1. Use the **help** command to access help information at any level.

```
# help
# help show
# help show log
```
2. Use the question mark character (?) to display help information for the current command path without pressing **Enter** and without losing the current input.

```
# ?
# show ?
# show system ?
```
3. Use the **Tab** key to auto-complete command elements, or to display a list of available keywords or phrases to complete a command.
4. Use the up arrow key to display the previous command.

New commands in v8.3

Several commands have been added to the CLI for version 8.3. For a comprehensive list of all CLI command changes between v8.2 and v8.3, see the CLI Command Comparison Guide 8.2 to 8.3.

sync system ntp	show component_route
show interface unused	set component_route
delete interface ipv4	delete component_route
delete interface dns	show appliance status
delete interface vlan	show network-agent
show interface bond	set mode full
set interface bond	set mode user
set interface unbond	set mode filter
show interface assignment	show hotfix history
set interface assignment	cancel download hotfix
delete interface assignment	show download
show diagnostic_ports	cancel download
set diagnostic_ports	pause download
show vswitch status	resume download
show decrypt_port_mirror	
set decrypt_port_mirror	

TRITON appliance API

In the new TRITON Appliance architecture, all configuration, management, and troubleshooting functions are supported by a REST API that is used by all TRITON appliance platforms and Forcepoint solutions. The TRITON Appliance CLI uses the REST API, as does the Forcepoint Security Appliance Manager. In 2017, portions of the API will be published for customer use.

Changes for V-Series

Appliance Manager replaced with CLI and Forcepoint Security Appliance Manager

See [V-Series Appliance Manager](#).

Define a filestore

In version 8.2 and earlier, the V-Series Appliance Manager was used to move files to and from an appliance.

In v8.3, CLI commands are used to move files to and from an appliance, as well as when saving a file. Only system backup files can be saved locally, on the appliance. Therefore, a remote **filestore** location must be defined to facilitate working with files in the off-appliance location. You can define one or many filestores. The supported file transfer protocols include **ftp**, **tftp**, and **samba**.

A filestore is defined with the CLI command:

```
set filestore --alias <name> --type <ftp|samba|tftp>
--host <ip_address> [--port <port>]--path <share_directory>
[--user <user_name>]
```

The filestore definition includes:

- A unique name, known as the **filestore alias**.
- The IP address of the filestore host and the port on which to connect.
- The protocol to use to move files between the filestore and the appliance.
- The directory path (ftp, tftp) or share (samba) on the host.
- If needed, the name of a user (account) with permissions on the filestore.

Example:

```
set filestore --alias fstore --type samba
--host 10.123.48.70 --path appliance1_files --user jdoe
```

Displaying network interface status

In the v8.2 and earlier V-Series Appliance Manager, on the **Status > General** page some network interface status could be displayed by hovering the mouse pointer over an interface label, such as C or P1. To see similar information in the CLI, use the “show bandwidth” command. In **diagnose** mode, use the “ethtool --interface” command.

[\[APA-2132\]](#)

Changes for X-Series

Appliance management network interface (C)

X-Series appliances add a C network interface dedicated to TRITON management communication. In versions 8.2 and prior, TRITON management traffic was handled on interface P1. Adding the C interface separates management traffic onto a dedicated channel, and makes X-Series platforms consistent with other TRITON appliance platforms.

Adding the C interface impacts X10G appliance upgrades to v8.3. Prior to applying the v8.3 upgrade patch, administrators must apply Hotfix830 and then configure the C interface in the CLI. The configuration data is stored until the upgrade is applied at which time the interface is added. For complete upgrade instructions, see the [X-Series Upgrade Guide](#).

Web protection features

The following new web protection features are supported on TRITON appliances. See the [v8.3.0 Release Notes for TRITON Web Protection Solutions](#) for details.

Web Management API

Administrators can create scripts to import threat intelligence from third-party sources into TRITON AP-WEB. If you have linked your TRITON AP-EMAIL channel with TRITON AP-WEB, then both can benefit directly from this functionality.

See the section titled **Management API (Appliance or Linux deployments)** in the [v8.3.0 Release Notes for TRITON Web Protection Solutions](#).

Content Gateway decryption port mirroring

Supported with TRITON AP-WEB on V10000 appliances.

When Content Gateway is enabled to decrypt HTTPS traffic for content analysis, the decrypted content can also be sent to a physical network interface to allow a trusted service to inspect the data for its own purposes. Note that the trusted device cannot modify the decrypted traffic and inject it back into the data stream.

The feature can be enabled and configured using CLI commands. ([APA-950](#))

For more details, see the section titled **SSL Decryption port mirroring (Content Gateway)** in the [v8.3.0 Release Notes for TRITON Web Protection Solutions](#).

Custom block pages

In version 8.3, customization of block pages hosted on appliances is facilitated with appliance API calls that download and upload your customized block page files. For comprehensive details, see the [Creating Custom Block Pages](#) technical paper.

Policy Broker replication

All TRITON appliances in TRITON AP-WEB deployments that configure [Policy Broker replication](#) automatically fail-over to a backup Policy Broker instance in the event that the primary Policy Broker becomes unavailable. No special configuration is needed.

Security updates

This release addresses the following Common Vulnerabilities and Exposures.

Closed vulnerabilities

- OpenSSL Security Vulnerabilities
[CVE-2016-2177](#)
[CVE-2016-2178](#)
[CVE-2016-2179](#)
[CVE-2016-2180](#)
[CVE-2016-2181](#)
[CVE-2016-2182](#)
[CVE-2016-2183](#)
[CVE-2016-6302](#)
[CVE-2016-6303](#)
[CVE-2016-6306](#)
- [CVE-2016-5195](#) – Dirty COW Security Vulnerability
- [CVE-2016-6304](#) – OSCP Status Request Extension Security
- [Shared challenge ACK vulnerability](#)

Notable CVEs to which v8.3.0 appliances are not vulnerable

- [HTTProxy CGI HTTP_PROXY Variable Multiple Vulnerabilities](#)
- Open SSL Vulnerabilities
[CVE-2016-2105](#)
[CVE-2016-2106](#)
[CVE-2016-2107](#)
[CVE-2016-2108](#)
[CVE-2016-2109](#)
[CVE-2016-2176](#)

- [CVE-2016-1950](#) – Buffer Overflow in Mozilla Network Security Services Vulnerability
- [CVE-2016-2118](#) and [CVE-2016-0128](#) – Badlock Vulnerability

TRITON Appliances documentation

All TRITON appliances share common operating and maintenance procedures.

The TRITON Appliances documentation set includes:

- This document — [TRITON Appliances Release Notes](#)
- [TRITON Appliances Getting Started: V-Series, X-Series, & Virtual Appliances](#)
- [TRITON Appliances CLI Guide: V-Series, X-Series, & Virtual Appliances](#)
- [TRITON Appliances CLI Command Comparison Table 8.2 to 8.3](#)
- [V-Series Appliances: Visual Primer for the v8.3 Appliance CLI](#)
- [V-Series Appliances: 5-Step Upgrade Guide to v8.3](#)
- [V-Series Upgrade Guide](#)
- [V-Series: Upgrading DUAL MODE Appliances to Version 8.3](#)
- [V-Series Quick Start Posters](#)
- [X-Series Upgrade Guide](#)
- [X-Series Quick Start Poster](#)
- [X-Series Switch Configuration Guide](#)
- [X-Series Fiber Optics Kit](#)

All TRITON documentation, including documents specific to TRITON AP-EMAIL, TRITON AP-WEB, Web Filter & Security, and TRITON Manager can be accessed at support.forcepoint.com/documentation.

Resolved and known issues for v8.3.0 V-Series and X-Series appliances

60227 | Release Notes | TRITON Appliances | 17-May-2017

A [list of known issues](#) in this release is available to TRITON AP-EMAIL, TRITON AP-WEB, and Web Filter & Security customers.

If you are not currently logged in to Forcepoint My Account, the above link takes you to a login prompt.