

v8.4.0 Release Notes for Forcepoint Appliances

Release Notes | Forcepoint Appliances | v8.4.0

Use these Release Notes to learn about what is new and improved for Forcepoint™ V Series, X Series, and Virtual Appliances in version 8.4.0.



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 8.4](#), page 14.



Important

Dual Mode appliances are not supported with version 8.3.0 and higher. See [Dual Mode appliances](#), page 18.

Contents

- [New for v8.4.0 Forcepoint appliances](#), page 1
- [Resolved and known issues for v8.4.0 V Series and X Series appliances](#), page 28

For information about which product versions are supported on which appliance platforms, see [Forcepoint solutions on Forcepoint appliance platforms](#), page 5, and the Forcepoint [appliance compatibility matrix](#).

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

For information about upgrading Forcepoint appliances, see:

- [V Series Upgrade Guide](#)
- [X Series Upgrade Guide](#)
- [Upgrading V Series Dual Mode Appliances to Version 8.4](#)

New for v8.4.0 Forcepoint appliances

Forcepoint is pleased to release version 8.4.0 of the Forcepoint appliance infrastructure. For more information on new appliance features, see the [Forcepoint Appliances Getting Started Guide](#).

- *Product renaming*, page 3
- *Firstboot changes*, page 4
- *Forcepoint solutions on Forcepoint appliance platforms*, page 5
- *Direct upgrade to v8.4.0*, page 12
- *V Series appliance models supported with version 8.4*, page 14
- *Platform hardening*, page 15
- *System logging*, page 16
- *Audit logging*, page 17
- *No longer supported and notable restrictions*, page 18
- *Forcepoint Security Appliance Manager*, page 20
- *Support for custom appliance user account management*, page 21
- *Command-line interface (CLI)*, page 22
- *Forcepoint appliance API*, page 23
- *X10G HA Kit to simplify X10G Deployment*, page 24
- *10GbE fiber NIC on V10K G4*, page 25
- *Security updates*, page 27
- *Forcepoint Appliances documentation*, page 28
- *Resolved and known issues for v8.4.0 V Series and X Series appliances*, page 28,

Product renaming















Product names have changed in v8.4.0.

Former Name	New Name
TRITON AP-EMAIL (v8.x) TRITON Email Security Gateway / Anywhere (v7.8.4)	Forcepoint Email Security
TRITON AP-WEB (v8.x) TRITON Web Security Gateway / Anywhere (v7.8.4)	Forcepoint Web Security
Forcepoint Web Filter & Security (v8.x) Websense Web Security (v8.x)	Forcepoint URL Filtering
V-Series X-Series TRITON Appliances	V Series X Series Forcepoint Appliances

Firstboot changes

The Firstboot system has been redesigned to allow for plug-ins to be easily integrated. The new Firstboot system is divided into a UI section and an appliance initialization section. Each section can now be run independently, and code can more easily be maintained. For more information, see the [Forcepoint Appliance Getting Started](#) guide.

Forcepoint solutions on Forcepoint appliance platforms

Product \ Platform	V5000	V10000	X10G	VMware	Azure
Forcepoint Email Security					
Forcepoint Web Security Network Agent	 	 			
Forcepoint URL Filtering Network Agent	 				
Forcepoint DLP Protector Mobile Agent	 				
Forcepoint DLP with Email Gateway for Microsoft Office 365					

For detailed information about deploying any of the Forcepoint DLP solutions on Forcepoint appliances, see the Forcepoint DLP section of the [Forcepoint documentation](#) page.

For detailed information about deploying Forcepoint Web Security 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 specifications

Supported solutions

- Forcepoint Email Security (certified)
- Forcepoint Web Security (certified)

Supported models with v8.4

- V10000 G4

- V10000 G3

Network interfaces

All V10000 appliances come with 6 physical Ethernet interfaces

C — Supports Forcepoint appliance management communication

P1, P2 — Support Content Gateway (web proxy) traffic (Forcepoint Web Security only)

E1, E2 — Support MTA traffic (Forcepoint Email Security)

N — Supports Network Agent (Web protection solutions)

Interface bonding: With Forcepoint Web Security and Forcepoint Email Security, interfaces P1 and E1 can be bonded, and interfaces P2 and E2 can be bonded.

V5000 specifications

Supported solutions

- Forcepoint Email Security (certified)
- Forcepoint Web Security (certified)
- Forcepoint URL Filtering (certified)

Supported models with v8.4

- V5000 G4
- V5000 G3
- V5000 G2R2

Network interfaces

All V5000 appliances come with 4 physical Ethernet interfaces.

C — Supports Forcepoint appliance management communication

P1, P2 — Support Content Gateway (web proxy) traffic (Forcepoint Web Security) or MTA traffic (Forcepoint Email Security)

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

- Forcepoint Email Security (certified)

- Forcepoint Web Security (certified)

Supported models with v8.4

- X10G G2 blade server
- X10G G1 blade server

Network interfaces

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

All X10G security blades support 3 virtual Ethernet interfaces.

C — Supports Forcepoint appliance management communication

P1, P2 — Support Content Gateway (web proxy) traffic (Forcepoint Web Security) or MTA traffic (Forcepoint Email Security)

Forcepoint Virtual Appliance for Web and Email specifications

ESXi VMware

Version 8.4 Web and Email Virtual Appliances are certified for VMware ESXi 6.5 / 6.0 / 5.5. A stable release of ESXi, such as 6.5d (build 5310538) or later, is recommended to avoid unexpected issues.

Supported solutions

- Forcepoint Email Security (certified)
- Forcepoint Web Security (certified)

Forcepoint Email Security VM specification

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

- 6 CPU cores
- 12 GB RAM
- 1 - 225 GB disk
- 1 - 100 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 Forcepoint Email Security VMware virtual appliances come with 4 virtual Ethernet interfaces.

C - Supports Forcepoint appliance management communication

P1, P2 - Support MTA traffic

N - Reserved

Forcepoint Web Security VM specification



Note

The policy mode **Filtering only** is not supported on VMware virtual appliances with version 8.4.0.

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

- 6 CPU cores
- 12 GB RAM
- 1 - 128 GiB and 1 - 129 GiB 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 Forcepoint Web Security VMware virtual appliances come with 4 virtual Ethernet interfaces.

C - Supports Forcepoint 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 v8.4.0.

Upgrading from 8.0.0 or 8.0.1

Forcepoint appliances cannot be upgraded directly from v8.0.x to v8.4.0. To upgrade from v8.0.x to v8.4.0, use the [v8.3 upgrade guide](#) to upgrade from v8.0.x to v8.3.0, and then use the [V Series, X Series, and Virtual Appliance Upgrade Guide](#) to upgrade from v8.3.0 to v8.4.0.

When upgrading from v8.0.0 or v8.0.1 to v8.4.x, in order to retain SNMP configuration, you must install two hotfixes while the appliance is still running version 8.3. Hotfix files are available in the Appliance v8.3.0 section of the [Forcepoint Downloads page](#).

Before upgrading from v8.3.0 to v8.4.0:

1. Install Appliance Hotfix 01 (APP-8.3.0-001)
2. Restart the appliance
3. Install Appliance Hotfix 90 (APP-8.3.0-090)

Direct upgrade to v8.4.0

V Series appliances can be upgraded directly to 8.4.0 from any of these versions:

7.8.4, 8.1.x, 8.2.x and 8.3.x

X Series appliances can be upgraded directly to 8.4.0 from any of these versions:

8.1.x, 8.2.x, and 8.3.x

Forcepoint appliances cannot be upgraded directly from v8.0.x to v8.4.0. To upgrade from v8.0.x to v8.4.0, upgrade from v8.0.x to v8.3.0, and then use the [V Series, X Series, and Virtual Appliance Upgrade Guide](#) to upgrade from v8.3.0 to v8.4.0.



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 18](#).



Important

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](#)

Unified Appliance Installer for v8.4.0

Starting with v8.4.0, the appliance recovery and upgrade logic has been merged within a unified appliance installer file.

V Series, X Series, and related Virtual Appliance deployment for v8.3.0 and later require the same ISO file to perform a new install or to upgrade to a newer version.

Forcepoint Appliance upgrades to version 8.4.0 and later require different file types (ISO or RPM) depending on the Appliance version from which you are upgrading.

Upgrades from Appliance versions 8.2.x and previous require the RPM file type to upgrade to Appliance version 8.4.0 and later releases. This RPM file (“v8.4.0 Universal upgrade patch for V/X Series Appliances”) is available on the [Forcepoint Downloads page](#).

Upgrades from Appliance version 8.3.x require the ISO file type to upgrade to Appliance version 8.4.0 and later. This ISO file (“v8.4.0 Unified Appliance Installer”) is available on the [Forcepoint Downloads page](#).

V Series appliance models supported with version 8.4

Version 8.4.0 is supported on these V Series appliances:

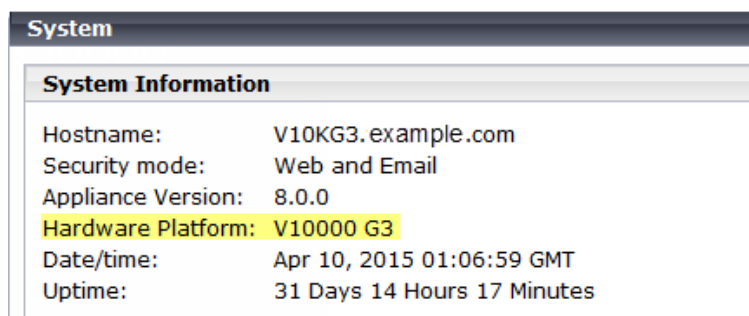
V10000	V5000
V10000 G4	V5000 G4
V10000 G3	V5000 G3
	V5000 G2 R2

Older V10000 G2 and V5000 G2 appliances, known as revision 1 (R1) or revision 2 (R2) appliances, are not supported with version 8.0.0 and higher. These appliance models are:

V10000 G2 R1:	Third quarter, 2011
V5000 G2 R1:	First quarter, 2012
V10000 G2R2:	Third quarter, 2017

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. V10000 G2R2 is not supported on v8.4.

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 Virtual Appliances.

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

System logging

Forcepoint 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 app --type audit --line 100
```

Typical entries look like:

```
2017-06-13 21:49:30,627 - INFO - appcli[165] - Account jdoe,
logged on from 10.64.161.8, entered view mode.
2017-06-13 21:49:59,042 - INFO - authentication - 13039 -
User jdoe attempting to log into API.
2017-06-13 21:49:59,094 - INFO - authentication - 13039 -
User jdoe authorization: True
2017-06-13 21:49:59,102 - INFO - common[976] - Account jdoe,
logged on from 10.64.161.8, entered config mode.
```

No longer supported and notable restrictions

- [Dual Mode appliances](#)
- [V Series Appliance Manager](#)
- [Changing the appliance management interface \(C\) IP address](#)

Dual Mode appliances

Version 8.4 does not support single appliances that host *both* Forcepoint Email Security, Forcepoint Web Security, or Forcepoint URL Filtering. These appliances, known as Dual Mode appliances, have always been limited to the V Series platform.

The new Forcepoint 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 v8.4, either the email or web module must be migrated to a new Forcepoint 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 8.4](#). Contact your Forcepoint account representative to learn about special promotions for Dual Mode deployments planning a v8.4 upgrade.

V Series Appliance Manager

In version 8.3 and later, the V Series Appliance Manager is replaced by the Forcepoint Security Appliance Manager (FSAM). The Forcepoint Security Appliance Manager was released in 2017. In addition, Forcepoint appliances can be fully and completely configured and monitored with the [Command-line interface \(CLI\)](#). And, of course, the CLI remains available now that the Forcepoint Security Appliance Manager is released.

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 Forcepoint Email Security 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 Forcepoint Web Security, changing the C IP address requires a full reinstall (re-image) of the appliance. See the knowledge base article [How to restore a Forcepoint appliance to a v8.4.x factory image](#).

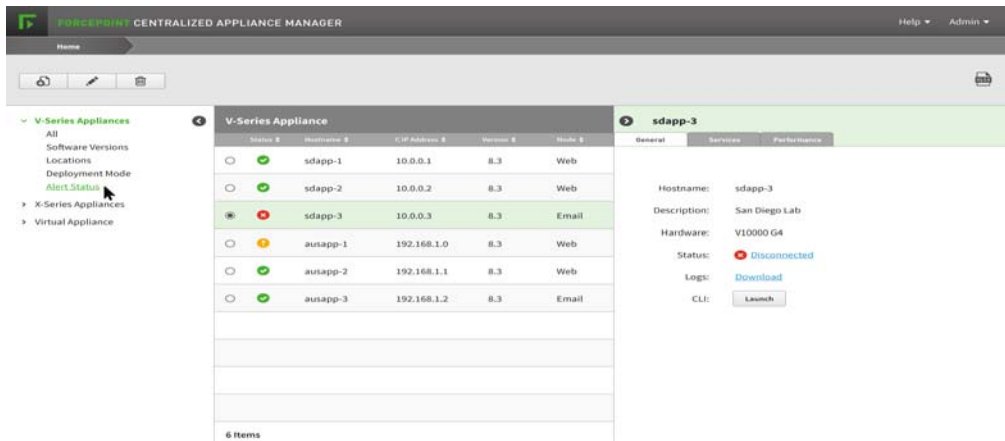


Warning

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

Forcepoint Security Appliance Manager

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



Support for custom appliance user account management

Custom appliance accounts can be created, allowing for more accurate user management and audit logging. Audit users can view configuration information; admin users can view and edit configuration information, and super admin users can also create, delete, and update user accounts. Multiple account instances can be created for specific roles.

Command-line interface (CLI)

New commands in v8.4

Several commands have been added to the CLI for version 8.4, most notably a set of commands specific to the Email module. For more details, see the [Forcepoint Appliances CLI Guide](#).

Forcepoint appliance API

In the new Forcepoint appliance architecture, all configuration, management, and troubleshooting functions are supported by a REST API that is used by all Forcepoint appliance platforms and Forcepoint solutions. The Forcepoint Appliance CLI uses the REST API, as does the Forcepoint Security Appliance Manager. In 2018, portions of the API will be published for customer use.

X10G HA Kit to simplify X10G Deployment

Starting with version 8.3.0, the Forcepoint X10G Appliance network design has been enhanced to enable switch High Availability (HA) either with VLAN or without VLAN configuration. This X10G appliance add-on is now provided to customers who require switch HA but hesitate to configure STP in their network. For installation instructions, see the [X10G Switch Stack Module Installation Guide](#).

10GbE fiber NIC on V10K G4

The 10GbE fiber NIC is supported on the V10K G4 appliance as a hardware add-on, allowing the V10K G4 to be deployed into the optical network. For installation instructions, see the [V10K 10GbE PCI NIC Installation Guide](#).

Decryption Port Mirror Expansion

In X Series appliances with the switch configuration port installed, the decryption mirror port expansion allows you to use the CLI or the API to enable the N interface as an SSL mirror port rather than a Network Agent port.

Security updates

This release addresses the following Common Vulnerabilities and Exposures.

Closed vulnerabilities

- [CVE-2014-3566](#) – POODLE Vulnerability in REST API
- Linux Kernel Vulnerabilities
 - CVE-2017-6346
 - [CVE-2017-2636](#)
 - [CVE-2016-8655](#)
 - [CVE-2016-6480](#)
 - [CVE-2016-6828](#)
 - CVE-2017-5551
 - [CVE-2016-7117](#)
 - [CVE-2016-9555](#)
 - CVE-2017-6074
 - CVE-2017-6001
 - CVE-2017-5986

Notable CVEs to which v8.4.0 appliances are not vulnerable

- Linux Kernel Vulnerabilities
 - CVE-2017-6345
 - CVE-2017-6347
 - CVE-2017-6348
 - CVE-2017-6353
 - CVE-2016-10150
 - CVE-2016-10153
 - CVE-2016-10154
 - CVE-2016-10208
 - CVE-2017-2583
 - CVE-2017-2596
 - CVE-2017-5546
 - CVE-2017-5547
 - CVE-2017-5548
 - CVE-2017-5576
 - CVE-2017-5577
 - CVE-2016-10044

Forcepoint Appliances documentation

All Forcepoint appliances share common operating and maintenance procedures.

The Forcepoint Appliances documentation set includes:

- This document — Forcepoint [Appliances Release Notes](#)
- Forcepoint [Appliances Getting Started: V Series, X Series, & Virtual Appliances](#)
- Forcepoint [Appliances CLI Guide](#)
- [V Series, X Series, and Virtual Appliances Upgrade Guide \(8.3 to 8.4\)](#)
- [V Series Upgrade Guide](#)
- [V Series Dual Mode Upgrade Guide](#)
- [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 Forcepoint documentation, including documents specific to Forcepoint Email Security, Forcepoint Web Security, Forcepoint URL Filtering, and Forcepoint Security Manager can be accessed at support.forcepoint.com/documentation.

Resolved and known issues for v8.4.0 V Series and X Series appliances

Release Notes | Forcepoint Appliances | v8.4.0

A [list of known issues](#) in this release is available to Forcepoint Email Security, Forcepoint Web Security, and Forcepoint URL Filtering customers.

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