v8.5.3 Release Notes for Forcepoint Appliances

Use these Release Notes to learn about what is new and improved for Forcepoint™ V Series, X Series, and Virtual Appliances in version 8.5.3.

> **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 8.5.3*, page 7.

> **Important**
> **Dual Mode** appliances are not supported with version 8.3.0 and higher. See *Command-line interface (CLI)*, page 8.

Contents

For information about which product versions are supported on which appliance platforms, see *Forcepoint solutions on Forcepoint appliance platforms*, page 2, 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
- Upgrading to Forcepoint Email Security
- Upgrade Instructions: Forcepoint Web Security

New for v8.5.3 Forcepoint appliances

Forcepoint is pleased to release version 8.5.3 of the Forcepoint appliance infrastructure. For more information on new appliance features, see the Forcepoint Appliances Getting Started Guide.

Forcepoint solutions on Forcepoint appliance platforms

Product/Platform	V5000	V10000	V20000	X10G	VMware	Azure
Forcepoint Email Security	✔	✔	✔	✔	✔	✔
Forcepoint Web Security	✔	✔	✔	✔	✔	
Network Agent	✔	✔	✔			
Forcepoint URL Filtering	✔				✔	
Network Agent	✔					
Forcepoint DLP Analytics Engine					✔	

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.

V20000

Supported solutions

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

Supported models with v8.5.3

- V20000 G1

Network interfaces

All V20000 appliances come with 6 physical Ethernet interfaces

C — Supports Forcepoint appliance management communication

P1, **P2** — Support Content Gateway (web proxy) traffic (Email Security and Web Security)

E1, **E2** — Used for bonding with P1/P2

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.

Fiber NICs: Supports fiber NICs for C and N interfaces (requires 3 dual-port NICs to be installed).

V10000

Supported solutions

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

Supported models with v8.5.3

- V10000 G3 R2
- V10000 G4 R1
- V10000 G4 R2

Network interfaces

All V10000 appliances come with 6 physical Ethernet interfaces

C — Supports Forcepoint appliance management communication

P1, **P2**

- (G3 R2 and G4 R1) Support Content Gateway (web proxy) traffic (Web Security)
- (G4 R2) Support Email Security and MTA traffic

E1, **E2**

- (G3 R2 and G4 R1) Support Email Security and MTA traffic
- (G4 R2) Used for bonding with P1/P2

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

Supported solutions

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

Supported models with v8.5.3

- V5000 G4
- V5000 G3

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 v8.5.3

- 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 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 8.5.3 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 URL Filtering (certified)

Forcepoint Email Security VM specification

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

- 6 CPU cores
- 12 GB RAM
- 1 - 235 GB disk
- 1 - 100 GB disk
- 4 E1000 virtual network interfaces

> **Important**
> Starting in v8.5.0, the vCPU cores and RAM allocation can be increased. Disk size and network interface cannot be changed.

Network interfaces

All Forcepoint Email Security VMware virtual appliances come with four (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 8.5.3.

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**
> Starting in v8.5.0, the vCPU cores and RAM allocation can be increased. Disk size and network interface cannot be changed.

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 v8.5.3.

Direct upgrade to v8.5.3

V Series appliances can be upgraded to 8.5.3 from 8.2.x, 8.3.x, 8.4.x, and 8.5.x.

X Series appliances can be upgraded to 8.5.3 from 8.2.x, 8.3.x, 8.4.x, and 8.5.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 *Command-line interface (CLI)*, page 8.

DLP Analytics Engine (VA) now supports upgrades.

For upgrade instructions, see:

- V Series Upgrade Guide
- X Series Upgrade Guide
- Upgrading V-Series Dual Mode Appliances
- Upgrading to Forcepoint Email Security v8.5
- Upgrade Guide: Forcepoint Web Security

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 8.5.3

Version 8.5.3 is supported on these V Series appliances:

V20000	V10000	V5000
V20000 G1	V10000 G3 R2	V5000 G4
	V10000 G4	V5000 G3

Older V10000 G2 and V5000 G2 appliances, known as revision 1 (R1) or revision 2 (R2) appliances, are not supported with this version. See the V Series Appliances Certified Product Matrix for last supported versions. These models stopped shipping:

V10000 G2 R1:	Third quarter, 2011
V5000 G2 R1:	First quarter, 2012
V10000 G2 R2	Third quarter, 2017
V10000 G3 R1	Fourth quarter, 2018

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.

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. V5000 G2R2 is not supported on v8.5.3.

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.

Command-line interface (CLI)

Several commands have been added to the CLI for version 8.5.3, including commands to:

● Enhance the editing of ciphers.
● Allow more logs to be viewed.
● Allow file operations without a filestore.
● Temporarily disable the Network Agent container through the CLI.
● Configure log archive information for GDPR compliance.

Additionally, the format of the CLI Guide has changed from a tabled-based format to an entry-based format. 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. Portions of the API have been published for customer use.

With the release of Forcepoint appliance version 8.5.3, Security content has been added. For more information, see the Forcepoint Appliances section of the Forcepoint documentation page.

Security updates

This release addresses the following Common Vulnerabilities and Exposures.

Meltdown/Spectre Vulnerabilities

CVE-2017-5715 (Spectre Variant 2)
CVE-2017-5753 (Spectre Variant 2)
CVE-2017-5754 (Meltdown/Variant 3)
CVE-2018-3640 (Variant 3a)
CVE-2018-3639 (Variant 4)
CVE-2018-3615 (Foreshadow/SGX)
CVE-2018-3620 (Foreshadow-NG/OS)
CVE-2018-3646 (Foreshadow-NG/VMM)

> **Note**
> Separate BIOS updates are required.

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
- Upgrading to Forcepoint Email Security v8.5
- Upgrade Guide: Forcepoint Web Security
- V Series Upgrade Guide
- V Series Dual Mode Upgrade Guide
- V Series Quick Start Posters
- X Series Upgrade Guide

- [X Series Quick Start Posters](#)
- [X Series Switch Configuration Guide](#)
- [X Series Fiber Optics Kit](#)
- [10GbE NIC Installation Guide](#)

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.

New FIPS 140-2 Encryption in Appliances v8.5.3

Federal Information Processing Standard (FIPS) 140-2 Cryptography

Forcepoint V Series (V20K, V10K, and V5K) and X Series (X10G) and related Virtual Appliances use FIPS 140-2 validated cryptographic libraries for the protection of sensitive data.

These cryptographic modules are certified by NIST under the Cryptographic Module Validation Program (CMVP).

A list of Forcepoint's FIPS 140-2 certificates can be found on the NIST CMVP website (https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/ Validated-Modules).

Resolved and known issues for v8.5.3 V Series and X Series appliances

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.