About This Release

Forescout version 8.1.3 delivers important fixed issues.

In addition, issues have been fixed in Modules Packaged with This Release and are documented in the respective Release Notes document of the individual module.

The following information is available:

- System Requirements
- Forescout Fixed Issues
- Forescout Known Issues
- Upgrading to Version 8.1.

Modules Packaged with This Release

When you install or upgrade to this release, the following modules are included:

- Base Modules:
  - Authentication Module 1.1.2 – with *feature enhancements* and *fixed issues*
  - Core Extensions Module 1.1.3 – with *fixed issues*
  - Endpoint Module 1.1.3 – with *feature enhancements* and *fixed issues*
  - Hybrid Cloud Module 2.0.2 – with *feature enhancements* and *fixed issues*
  - Network Module 1.1.3 – with *feature enhancements* and *fixed issues*
- Content Modules:
  - Device Profile Library 19.1.9
  - IoT Posture Assessment Library 18.0.4
  - NIC Vendor Database 19.0.8
  - Security Policy Templates 19.0.9
  - Windows Applications 19.0.9
  - Windows Vulnerability DB 19.0.9

Refer to the respective Release Notes for more information about each module.

Finding More Documentation

See Additional Forescout Documentation for information about accessing guides referenced in this document. See Previous Releases to access Release Notes for previous version releases.

System Requirements

This section describes system requirements for users upgrading to Forescout version 8.1.3, including:

- Virtual System Supported Versions
- Forescout Console Hardware Requirement
- Physical and Virtual Appliance Requirements and Specifications
- Supported Hardware Revisions for Physical Appliances

Clean Installations

Installation instructions and requirements for clean installations are provided in the *Forescout Installation Guide* version 8.1.

Virtual System Supported Versions

This section describes supported versions for Forescout 8.1.3 virtual systems. For a complete list of supported hardware and software, see the Forescout Compatibility Matrix.

Supported VMware Versions

The Forescout virtual system is supported when running on the following VMware versions:

- VMware ESXi v6.7
- VMware ESXi v6.5
- VMware ESXi v6.0

Support for the following versions was removed in this release:

- VMware ESXi v5.5
- VMware ESXi v5.1

Supported Hyper-V Versions

The Forescout virtual system is supported when running on the following Hyper-V versions:

- Hyper-V Server 2016 v10x
- Hyper-V Server 2012 v6.x
- Hyper-V Server 2012 R2 v6.x

Supported KVM Versions

The Forescout virtual system is supported when running on the following KVM versions:

- Centos v7.x
  - Kernel 4.x/5.x
  - QEMU 1.x
- Ubuntu v18+
  - Kernel 4.x
  - QEMU 3.x

Forescout Console Hardware Requirements

You must supply a machine to host the Forescout Console application software. Minimum hardware requirements are:

- Non-dedicated machine, running:
  - Windows 7/8/8.1/10
  - Windows Server 2008/2008 R2/2012/2012 R2/2016
  - Linux RHEL/CentOS 7
  - macOS 10.12/10.13/10.14
- 2GB RAM
- 1GB disk space

Physical and Virtual Appliance Requirements and Specifications

Refer to the Forescout Licensing and Sizing Guide for requirements/specifications related to deployment sizing for physical and virtual CounterACT devices. Some of the requirements/specifications previously documented in the following documents are now in this new guide:

- *Forescout Installation Guide*
- *Network Module: Switch Plugin Configuration Guide*
- *Network Module: Wireless Plugin Configuration Guide*

Supported Hardware Revisions for Physical Appliances

This section describes CounterACT Appliance and Enterprise Manager requirements.

Physical CounterACT Devices

Forescout version 8.1.3 can be installed on all hardware revisions of CounterACT physical Appliances and Enterprise Managers ***except for the following***:

Model	Revisions Not Supported
CTR	CTR-11, CTR-12, CTR-13
CT100	CT100-20, CT100F-20 CT100-21, CT100F-21 CT100-22, CT100F-22
CT1000	CT1000-20, CT1000F-20, CT1000F2-20 CT1000-21, CT1000F-21, CT1000F2-21 CT1000-22, CT1000F-22, CT1000F2-22
CT-2000 **CEM-25** **CEM-50**	CT2000-20, CT2000F-20, CT2000F2-20 CT2000-21, CT2000F-21, CT2000F2-21 CT2000-22, CT2000F-22, CT2000F2-22
CT-4000 **CEM-100**	CT4000-20, CT4000F-20, CT4000F2-20, CT4000F10G-20 CT4000-21, CT4000F-21, CT4000F2-21, CT4000F10G-21 CT4000-22, CT4000F-22, CT4000F2-22, CT4000F10G-22
CT-10000 **CEM-150** **CEM-200**	CT10000-20, CT10000F-20, CT10000F2-20 CT10000-21, CT10000F-21, CT10000F2-21, CT10000F10G-21 CT10000-22, CT10000F-22, CT10000F2-22, CT10000F10G-22
CEM-05 **CEM-10**	CT1000MS-20, CT1000MS-21 CT1000MS-22

CT-xxxx CounterACT devices based on hardware revision -10 or lower also do not support Forescout version 8.1.3.

To determine the revision of a specific Enterprise Manager, do one of the following:

- Run the *fstool model* command on the Enterprise Manager.
- See the product label on the machine.

To determine the revision of a specific Appliance, do one of the following:

- Run the *fstool model* command on the Appliance.
- Run the *fstool tech-support oneachmodel* command on the Enterprise Manager. Running this command requires the ***Technical Support Plugin 1.1.2***.
- See the product label on the machine.

Contact your Forescout sales representative for alternative solutions if any of your Appliances are on this list of revisions not supported.

Forescout Fixed Issues

This section identifies the fixed issues for this release of the Forescout platform.

- Merged Hotfixes
- Fixed for This Version

See Previous Releases for information about accessing Release Notes that include fixed issues from earlier releases.

For a list of fixed issues in Modules Packaged with This Release, refer to the respective Release Notes document of each module.

Merged Hotfixes

The following, previously released hotfixes are merged into this version of the Forescout platform:

Hotfix	Description	Up to Version
8.0.1.2	Refer to Hotfix 8.0.1.2 Release Notes	8.0.1.2-102
8.1.2.1	Refer to Hotfix 8.1.2.1 Release Notes	8.1.2.1-102
Version 7.0, Service Pack Hotfix 3.0.2.5	Refer to Hotfix Version 7.0, Service Pack Hotfix 3.0.2.5	3.0.2.5044

Fixed for This Version

The following issues are newly fixed in this version of the Forescout platform:

Issue	Description
CA-19895	Fixed a known directory tranversal vulnerability in the Forescout platform. Zip file extraction now aborts when a directory traversal is detected.
CA-22238	The upgrade logs for the GuiManager were missing after an upgrade from 7.0 to 8.1.2.1.
CA-23807	Fixed a known vulnerability in using the Java RMI to log into the Forescout device.
CA-22849	Fixed a known vulnerability in the injection and execution of a persistent script in the comments field of the Enterprise Manager web application. Special characters such as `~!@#$%^&=*()+[]\;'/{}|:"? are no longer allowed in the comment field and are removed if entered.

Issue	Description
CA-23721	Users could not add, edit, or view deprecated actions, although the actions were still present in a policy. The editing of existing obsolete actions is now allowed, but without allowing the addition of obsolete actions as new actions.
CA-23744	Old Forescout logos appeared on various pages and in the GUI.
CA-23753	Updates were blocked if an installed version was not listed in the *fsp_comply.properties* or *plugin_comply.properties* files. For example, for the version list "1.0.0, 1.1.0, 2.0.0", if the installed version was 1.2.0, it would have been blocked.
CA-23804	HTTP requests included the current session token within the URL or in the resulting web page. The requested URLs stored in log files or saved as favorites in the browser could contain valid session tokens.
CA-23815	The Enterprise Manager allowed access by SSH to a restricted command shell.
CA-23872	After a reboot, the Enterprise Manager became stuck in an abort loop. Java services were unable to start.
CA-24037	Smart card authentication did not work after restoring from backup. The smart card configuration file was not backed up.
CA-24079	The Export and Import buttons of the legacy assets customization portal did not work.
CA-24143	DHCP properties with names ending in "(Obsolete)" no longer appear in the host profile under the "General" category. They now appear under the "More" category.
CA-24037	Smart card authentication did not work after restoring from backup. The smart card configuration file was not backed up.
CA-24079	The Export and Import buttons of the legacy assets customization portal did not work.
CA-24656	Scheduled asset inventory reports failed to generate and produced a Java exception when a property with parameters was updated.

Forescout Known Issues

This section describes known issues for this version of the Forescout platform. See Previous Releases for information about accessing Release Notes that include fixed issues from earlier releases.

Issue	Description
CA-23249	Navigating away from the Linux or Mac Options pages causes the "Changes not applied. Do you want to continue?" dialog to appear even though there were no changes.
CA-24103	Even though there are no changes, a warning about losing changes is displayed when canceling an Option>CEF>Edit for a server in the CounterAct GUI.

Issue	Description
CA-24180	Java core dumps on Enterprise Manager while adding cloud RM/Appliance to on-premise setup.
CA-24353	HPS Inspection Engine stuck in pending after an appliance failover Some properties are not synchronized by the failover mechanism, causing performance issues in the HPS Inspection Engine delaying the resolution of the Network Function property following a failover.
CA-24435	When reassigning segments from one appliance to another, the message "Loading completed from X our of X Appliances. Appliances omitted due to slow responsiveness" appears.
CA-24475	The number of managed hosts returned by the command **fstool sysinfo** does not match the number of managed hosts displayed in the console.
CA-24478	During an upgrade, the Enterprise Manager stalls on FSUpgradeStatusConfigParams$FSUpgradeStatusUpdater when an appliance is unresponsive.
CA-24489	The number of hosts in policy and the total number shown in the host view does not match.
CA-24495	A host stays matched to a policy even if the host is down and remains matched after a manual recheck.
CA-24585	Machine type capacity presented in the Forescout GUI does not match the capacity stated for each virtual machine in the Forescout Appliance Specs Guide.
CA-24602	The Forescout Specifications Guide does not align with the internally generated capacity calculations.

Upgrading to Version 8.1.3

This section:

- Explains how to upgrade a single Appliance or Enterprise Manager, or multiple Appliances and an Enterprise Manager
- Describes important upgrade considerations
- Provides End-of-Life and other information about components not supported.

Verify that you have met System Requirements before upgrading to this version.

Upgrade Considerations and Issues

Upgrade is supported from the following versions:

- Forescout CounterACT version 7.0.0 with Service Pack 3.0.2.5 installed
- Forescout CounterACT version 8.0.1
- Forescout version 8.1, 8.1.1, and 8.1.2.

To upgrade from version 8.0, first upgrade to version 8.0.1. It is recommended to make sure you have the Optimal Versions Compatible for Version 8.1.3 Upgrade from Version 8.0.1 installed before performing the upgrade.

- After performing a rollback, wait for a minimum of 30 minutes after High Availability Appliances have synchronized before beginning an upgrade.
- As of this version, the Forescout platform only reports (and resolves properties for) IPv6 addresses that are defined in segments that are part of the Internal Network.
- The Segment name field in the Internal Network page of the Initial Setup Wizard is now mandatory.
- If only empty segments are assigned to a failover cluster, you must remove them from all failover cluster folder assignments before you remove any of the segments. Refer to the *Forescout Administration Guide* for more information about defining Appliance folders and to the *Forescout Resiliency and Recovery Solutions User Guide* for more information about failover clusters.
- If you configured the list of IP addresses allowed to access Forescout web features separately for an individual Appliance or group of Appliances, these configuration changes will be lost after upgrade to version 8.1.

  Settings configured in the Default tab will not be lost after upgrade. Web access configuration settings are defined in the **Options > Access > Web** pane of the Console.

  Refer to the *Forescout Administration Guide* for more information about both defining web access and configuring features for an Appliance or group of Appliances.
- Before logging in to the Console using a Smart Card, you must first upgrade your Console to version 8.1.

  To upgrade your Console, do the following:

  a. Download the Console installer from the URL https://<your Enterprise Manager IP address>/install
  b. Run the installer (installs a new Console of the latest version)
  c. Log in to the Console using your Smart Card
- Upgraded versions of Forescout might include legacy Asset Classification policies that provide limited information about endpoints. To take advantage of more precise classification profiles, it is recommended to create and run Primary Classification policies.

  The Primary Classification policy provides more comprehensive classification in your environment than legacy Asset Classification policies. To use it as your primary classification policy, ensure that the Add to Group actions are enabled in the Primary Classification policy, and use the Policy Manager to stop your Asset Classification policies.
- An unsupported plugin version should be upgraded to a supported version (if available) or uninstalled before upgrading to version 8.1.3.

With the availability of the Forescout Flow Collector, the legacy NetFlow Plugin is deprecated. The Flow Collector provides more accurate and stable traffic flow detection and more scalable bandwidth capabilities than the NetFlow Plugin. For networks running the NetFlow Plugin with flow protocol higher than v5, it is recommended to configure and enable the Flow Collector, and then stop and uninstall the NetFlow Plugin. If your network uses NetFlow v5, do not replace the NetFlow Plugin with the Flow Collector until your network is upgraded to a newer flow protocol.

- Following upgrade to version 8.1.3, the configuration test of the Operational Technology Plugin always fails, due to communication timeout. In all other aspects, the plugin continues to properly function.

Optimal Versions Compatible for Version 8.1.3 Upgrade from Version 7.0.0

The following components are the optimal versions that are compatible when upgrading to Forescout version 8.1.3 from version 7.0.0. It is recommended to make sure that these **versions or above** are installed before performing the upgrade.

Component Name	Optimal Versions Compatible for V8.1.2 Upgrade from V7.0.0
802.1X	4.2.3
Advanced Compliance	1.1.1
Advanced Tools	2.2.3.1009
ARF Reports	1.0.2
AWS	1.1.1
CEF	2.6.1
Check Point Next Generation Firewall	1.0.2
Check Point Threat Prevention	1.0.0
Cisco PIX/ASA Firewall Integration	2.0.2
CounterACT 7.0.0 Service Pack	3.0.2.5010
CounterAct Infrastructure Update Pack	2.0.12
CrowdStrike	1.0.0
CyberArk	1.0.0
Device Classification Engine	1.0.0
Device Profile Library	2.0.9.1003
DEX Open Integration Module	3.2.2
DHCP Classifier	2.0.7
DNS Client	3.0.0
DNS Enforce	1.1.6

Component Name	Optimal Versions Compatible for V8.1.2 Upgrade from V7.0.0
External Classifier	2.2.2
FireEye EX	1.1.0
FireEye HX	1.1.0
FireEye NX	2.0.0
Hardware Inventory	1.0.3
Hardware WatchDog	1.1.4
HPE ArcSight	2.7.1
HPS Applications	2.1.18
HPS Inspection Engine	10.7.3
IBM BigFix	1.0.1
IBM MaaS360 MDM	1.7.1
IBM QRadar	2.0.1
IOC Scanner	2.1.0
Linux	1.1.1
Macintosh/Linux Property Scanner	7.0.2
McAfee ePolicy Orchestrator	3.0.1
Microsoft SMS/SCCM	2.2.5.3001
MobileIron	1.7.1
NBT Scanner	3.0.4.1005
NetFlow	1.1.2
Operating System Update Pack	1.2.6
OS X	2.0.3
Palo Alto Networks Next Generation Firewall	1.1.2
Palo Alto Networks WildFire	2.0.1
Qualys Vulnerability Management	1.2.1
Rapid7 Nexpose	1.1.2
Reports	4.2.1
Router Blocking	1.0
ServiceNow	1.1.0
Splunk	2.7.0
Switch	8.11.3
Symantec Endpoint Protection	1.0.1
Syslog	3.2.1
Technical Support	1.2.1

Component Name	Optimal Versions Compatible for V8.1.2 Upgrade from V7.0.0
Tenable Vulnerability Management	2.6.0.1012
User Directory	6.1.4
VMware AirWatch	1.7.2
VMware NSX	1.0.0
VMware vSphere	2.0.1
VPN Concentrator	4.0.9
Web API Open Integration Module	1.2.3
Wireless	1.7.3

Optimal Versions Compatible for Version 8.1.3 Upgrade from Version 8.0.1

The following components are the optimal versions that are compatible when upgrading to Forescout version 8.1.3 from version 8.0.1. It is recommended to make sure that these **versions or above** are installed before performing the upgrade.

Module Name	Component Name	Optimal Versions Compatible for V8.1.3 Upgrade from V8.0.1
	CounterACT Infrastructure Update Pack	3.0.2
Authentication (1.0.1)	RADIUS	4.3.1
	User Directory	6.3.1
Core Extensions (1.0.1)	Advanced Tools Plugin	2.2.4
	CEF	2.7.0
	Device Classification Engine	1.2.0
	DHCP Classifier	2.1.1
	DNS Client	3.1.0
	DNS Enforce	1.2.0
	DNS Query Extension	1.2.0
	External Classifier	2.2.3
	Flow Analyzer	1.4.0
	IOC Scanner	2.2.0
	IoT Posture Assessment Engine	1.0.0
	NBT Scanner	3.0.6
	NetFlow	1.2.0
	Reports	5.0.1

Module Name	Component Name	Optimal Versions Compatible for V8.1.3 Upgrade from V8.0.1
	Syslog	3.4.0
	Technical Support	1.2.1
	Web GUI	1.0.0
Endpoint (1.0.1)	Hardware Inventory	1.0.3
	HPS Inspection Engine	10.8.1
	Linux	1.2.1
	Microsoft SMS/SCCM	2.3.0
	OS X	2.1.1
Hybrid Cloud (1.2.0)	AWS	2.0.0
	VMware NSX	1.1.0
	VMware vSphere	2.2.0
Network (1.0.1)	Centralized Network Controller	1.0.0
	Switch	8.12.2
	VPN	4.1.1
	Wireless	1.8.2
Others	ARF Reports	1.0.3
	Cisco PIX/ASA Firewall Integration	2.1.0
	Router Blocking	1.1.0
Extended Modules	Advanced Compliance (SCAP)	1.2.0
	AirWatch MDM	1.8.0
	ArcSight	2.8.0
	Carbon Black	1.0.0
	Check Point Next Generation Firewall	1.1.0
	Check Point Threat Prevention	1.1.0
	Crowdstrike	1.1.0
	CyberArk	1.1.0
	Failover Clustering License	1.0.0
	FireEye EX	1.2.0
	FireEye HX	1.2.0
	FireEye NX	2.1.0
	IBM BigFix	1.1.0
	IBM MaaS360 MDM	1.8.0
	IBM QRadar	2.1.0
	McAfee ePolicy Orchestrator	3.1.0

Module Name	Component Name	Optimal Versions Compatible for V8.1.3 Upgrade from V8.0.1
	MobileIron	1.8.0
	Open Integration Module	1.1.0
	Palo Alto Networks Next Generation Firewall	1.2.0
	Palo Alto Networks WildFire	2.1.0
	Qualys Vulnerability Management	1.3.0
	Rapid7 Nexpose	1.2.0
	ServiceNow	1.3.0
	Splunk	2.8.0
	Symantec Endpoint Protection	1.1.1
	Tenable Vulnerability Management	2.7.1

Optimal Versions Compatible for Version 8.1.3 Upgrade from Version 8.1.0 or above

The following components are the optimal versions that are compatible when upgrading to Forescout version 8.1.3 from version 8.1.0. It is recommended to make sure that these **versions or above** are installed before performing the upgrade.

Module Name	Component Name	Optimal Versions Compatible for V8.1.3 Upgrade from V8.1.0 or above
	CounterACT Infrastructure Update Pack	3.0.2
Authentication (1.1.0)	RADIUS	4.4.0
	User Directory	6.4.0
Core Extensions (1.1.1)	Advanced Tools	2.3.0
	CEF	2.8.0
	Dashboard	1.1.0
	Device Classification Engine	1.3.0
	DHCP Classifier	2.2.0
	DNS Client	3.2.0
	DNS Enforce	1.3.0
	DNS Query Extension	1.3.0
	External Classifier	2.2.4
	Flow Analyzer	1.4.1
	Flow Collector	1.0.0

Module Name	Component Name	Optimal Versions Compatible for V8.1.3 Upgrade from V8.1.0 or above
	IOC Scanner	2.3.0
	IoT Posture Assessment Engine	1.1.2
	NBT Scanner	3.1.0
	Packet Engine	8.1.1
	Reports	5.1.0
	Syslog	3.5.0
	Technical Support	1.2.2
	Web Client	1.1.1
Endpoint (1.1.1)	Hardware Inventory	1.1.0
	HPS Agent Manager	1.0.1
	HPS Inspection Engine	11.0.1
	Linux	1.4.0
	Microsoft SMS/SCCM	2.4.0
	OS X	2.2.0
Hybrid Cloud (2.0.0)	AWS	2.1.0
	Azure	1.0.0
	VMware NSX	1.2.0
	VMware vSphere	2.4.0
Network (1.1.1)	Centralized Network Controller	1.1.0
	Rogue Device	1.0.0
	Switch	8.13.1
	VPN	4.2.0
	Wireless	1.9.0
Others	ARF Reports	1.0.3
	Cisco PIX/ASA Firewall Integration	2.2.0
	Router Blocking	1.2.0
Extended Modules	Advanced Compliance (SCAP)	1.2.0
	AirWatch MDM	1.9.0
	ArcSight	2.8.0
	Carbon Black	1.1.0
	Check Point Next Generation Firewall	1.2.0
	Check Point Threat Prevention	1.2.0
	Crowdstrike	1.2.0

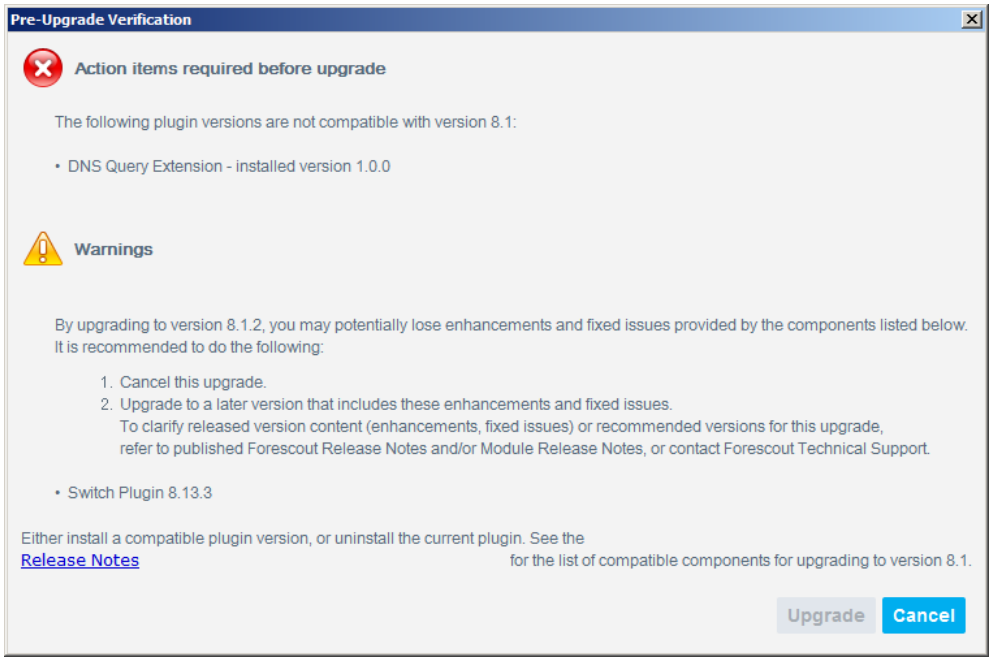
Module Name	Component Name	Optimal Versions Compatible for V8.1.3 Upgrade from V8.1.0 or above
	CyberArk	1.2.0
	FireEye EX	1.2.0
	FireEye HX	1.3.0
	FireEye NX	2.1.0
	Fortinet Next Generation Firewall	1.0.0
	IBM BigFix	1.2.0
	IBM MaaS360 MDM	1.9.0
	IBM QRadar	2.1.0
	McAfee ePolicy Orchestrator	3.2.0
	MobileIron	1.9.0
	Open Integration Module	1.2.0
	Palo Alto Networks Next Generation Firewall	1.3.0
	Palo Alto Networks WildFire	2.2.0
	Qualys Vulnerability Management	1.4.0
	Rapid7 Nexpose	1.3.0
	ServiceNow	2.0.0
	Splunk	2.9.0
	Symantec Endpoint Protection	1.2.0
	Tenable Vulnerability Management	2.8.0

Components Not Supported for Version 8.1.3

A pre-upgrade check is performed to verify that the environmental and software requirements have been met. When the verification finishes, the Pre-Upgrade Verification summary screen opens and verifies:

- Dependencies: The compatible version of each plugin or eyeExtend product (Extended Module). The verification screen may ask you to upgrade or uninstall a plugin or eyeExtend product before continuing the upgrade. With this Forescout version, pre-upgrade verification:
  - Notifies you when the Forescout version to which you are upgrading does not include plugin versions and hotfix versions that are currently installed
  - Provides an itemized list of the potentially impacted plugin and hotfix versions
- End-of Life and Non-Supported Modules/Plugins: You must uninstall them before continuing the upgrade

- Total Computer/Device Memory
- Appliance Model



End-of-Life

Products that have reached end-of-life (EOL) must be uninstalled from CounterACT ***before you upgrade the software***. The upgrade process does not continue when end-of-life products are detected.

As of version 8.0, the following components are ***end-of-life***:

- Aruba ClearPass
- Bromium Secure Platform
- Citrix XenMobile
- Damballa
- FireWall-1® ELA Client
- FireWall-1® SAM Client
- Invincea
- McAfee Threat Intelligence Exchange
- McAfee Vulnerability Manager
- NetScreen Firewall
- PCI
- Palo Alto Networks Firewall (base)
- SAP Afaria MDM

Not Supported for Version 8.1.3

Products that are not supported for Forescout 8.1.3 must be uninstalled before you upgrade the software. The upgrade process does not continue when non-supported products are detected.

With this version, the following plugin is not supported:

- Macintosh/Linux Property Scanner

Before upgrading your CounterACT deployment to version 8.1.3, consider performing the procedures provided in Pre-Upgrade Procedures for Non-Support of the Macintosh/Linux Property Scanner, if the Macintosh/Linux Property Scanner is managing Mac OS/OS X and Linux endpoints using Remote Inspection and SecureConnector in your existing CounterACT version 7.0.0 deployment.

Pre-Upgrade Procedures for Non-Support of the Macintosh/Linux Property Scanner

If the Macintosh/Linux Property Scanner is managing Mac OS/OS X and Linux endpoints using Remote Inspection and SecureConnector in your existing CounterACT version 7.0.0 deployment, perform the procedures provided in the following sections before upgrading to Forescout version 8.1.3. These procedures are provided, due to Forescout version 8.1.3's non-support of the Macintosh/Linux Property Scanner.

Migrate Managed Linux and OS X Endpoints

Previously, the Macintosh/Linux Property Scanner managed Mac OS/OS X and Linux endpoints using Remote Inspection and SecureConnector. The OS X Plugin and the Linux Plugin replace the Macintosh/Linux Property Scanner. The Macintosh/Linux Property Scanner is not supported for/incompatible with Forescout version 8.1.3.

Before upgrading to Forescout version 8.1.3, perform the following procedure to ensure that no Linux and no OS X endpoints are managed by the Macintosh/Linux Property Scanner:

To prepare managed Linux and OS X endpoints for upgrade:

1. Verify that the following plugin releases are installed and running in your environment:
   - Linux Plugin 1.1.0
   - OS X Plugin 2.0.3
   - Macintosh/Linux Property Scanner 7.0.0 or above
2. For endpoints managed using Remote Inspection:
   - Endpoints pass automatically from the Macintosh/Linux Property Scanner to the control of the OS X Plugin or the Linux Plugin.

- The new plugins inherit public and private keys for Remote Inspection used by the Macintosh/Linux Property Scanner.
- The new plugins do not inherit other Remote Inspection settings. Recreate these settings or customize Remote Inspection settings when you configure the Linux Plugin and the OS X Plugin.

3. For endpoints managed using SecureConnector:

   a. Create and run a policy based on the Migrate Linux SecureConnector policy template. This policy detects Linux endpoints managed by SecureConnector and migrates them to the control of the Linux Plugin.

   b. Create a policy or policy rule that:

      > Uses the **Macintosh SecureConnector Version** host property to detect existing OS X endpoints that run legacy versions of SecureConnector.

      > Applies the *Migrate to OS X SecureConnector* action to these endpoints. This action replaces the legacy version of SecureConnector on these endpoints with the latest version and the endpoints now communicate with the OS X Plugin.

Disable SecureConnector Updates on Windows Endpoints

This section describes how to configure existing CounterACT 7.0.x environments to disable automatic update/distribution of SecureConnector.

Before upgrading to Forescout version 8.1.3, perform the following procedure to prevent automatic distribution of SecureConnector after upgrade.

Perform the following configuration steps before upgrade:

1. Log in to the Enterprise Manager CLI.
2. Submit the following command:

```
fstool va set_property config.use_automatic_upgrade.value false

fstool oneach fstool va set_property
config.use_automatic_upgrade.value false
```

After upgrading your Forescout deployment, automatic upgrade is disabled by default.

Performing the Upgrade

You can upgrade your version of the software from the Console.

The Installer program automatically identifies an earlier Forescout version on your system. Upgrade options allow you to either maintain the configuration parameters from the previous version or define new parameters. If your deployment is operating in Per-Appliance Licensing Mode, and you want to simultaneously upgrade and switch to Flexx Licensing Mode, follow the procedure in Upgrading to Version 8.1.3 and Migrating to Flexx Licensing Mode.

- Upgrade the Enterprise Manager
- Upgrade One or More Appliances

- Manually Upload the Upgrade File to an Appliance
- Upgrade High Availability Devices

After you upgrade your Enterprise Manager to version 8.1, a new process will be available for upgrading Appliances, allowing you to upload the upgrade file prior to and independently of the upgrade itself. For larger deployments, this can significantly reduce the time it takes to perform the upgrade, allowing you to complete the process within a defined maintenance window.

The first time you upload a file to an Appliance/s, the file is uploaded to the Enterprise Manager before being copied to the Appliance. This initial upload may take some additional time. Once the file is uploaded to the Enterprise Manager, the upgrade file will be automatically stored for any future uploads/upgrades to other Appliances.

The upgrade installs the Forescout core platform as well the Base Modules, Content Modules and previously installed eyeExtend products (Extended Modules), unless the component is End-of-life.

Upgrade the Enterprise Manager

To upgrade Enterprise Manager software:

1. Download or obtain the upgrade file and save it to a location on your computer.
2. Select **Options** from the **Tools** menu and if necessary, select **CounterACT Devices**.

   The installed CounterACT devices and their current versions are displayed.
3. Select an Enterprise Manager and select **Upgrade**. Do not select an Enterprise Manager together with Appliances (they cannot be upgraded at the same time). The Upgrade Enterprise Manager dialog box opens.
4. Locate the upgrade file you saved on your computer and select **OK**. After a check of the digital signature of the upgrade file is performed, the CounterACT Upgrade screen opens.
5. Read the terms and conditions, and then select **I accept the Terms and Conditions**. It is recommended to read the Release Notes.

   When upgrading an Appliance connected to an Enterprise Manager already upgraded to the current Forescout version, the pre-upgrade check is not performed, and the Upgrade button is immediately available in the CounterACT Upgrade screen.
6. Select **Verify**. A pre-upgrade check is performed to verify that the environmental and software requirements are met. When the verification finishes, the Pre-Upgrade Verification summary screen opens.
7. Select **Upgrade** if you are sure you want to proceed with the upgrade. Once you confirm, the upgrade process proceeds to completion and cannot be interrupted or cancelled.

8. When the upgrade is completed successfully, select **Close**. If the upgrade is not successful, contact your Forescout representative and ***do not*** continue with more upgrades.
9. After the upgrade is complete, download the Console and install it.

   High Availability Devices – Upgrade for High Availability devices can take a long time (up to a number of hours). If the upgrade of the second node and the synchronization are not shown in the log, you can verify the status via icons on the Console status bar:

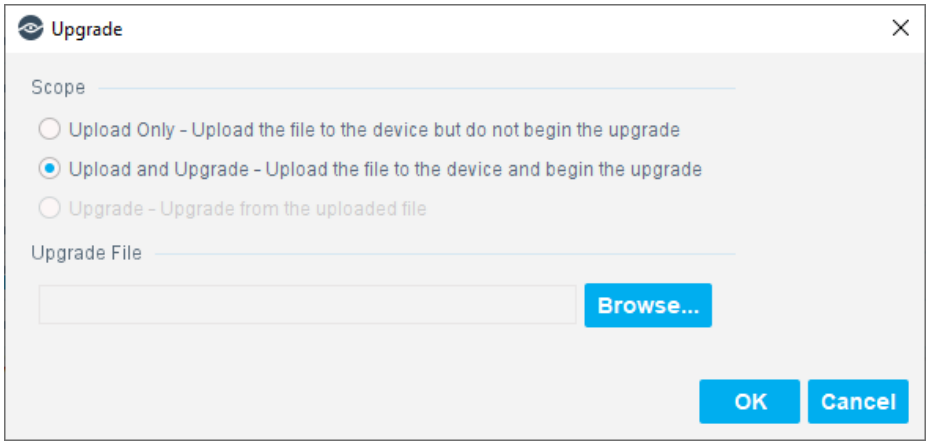
	Indicates the status of the High Availability Appliances connected to the Enterprise Manager.
	Indicates the status of the Enterprise Manager High Availability pair.
	Indicates that High Availability is down on the Appliance.
	Indicates that High Availability is down on the Enterprise Manager.

Upgrade One or More Appliances

To upgrade to a new version:

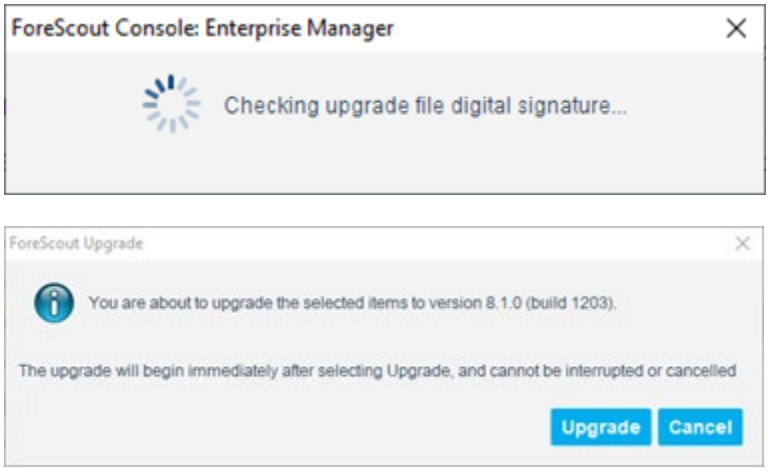
1. Before upgrading Appliances, you should upgrade the Enterprise Manager.
2. Download or obtain the upgrade file (FSP) for version 8.1.3 and save it to a location on your computer.
3. Select **Options** from the **Tools** menu.

   CounterACT devices or Appliances are shown with their current version.
4. Select an Appliance or group of Appliances and select **Upgrade**. Do not select Enterprise Managers together with Appliances, because you cannot upgrade both Appliances and Enterprise Managers at the same time.

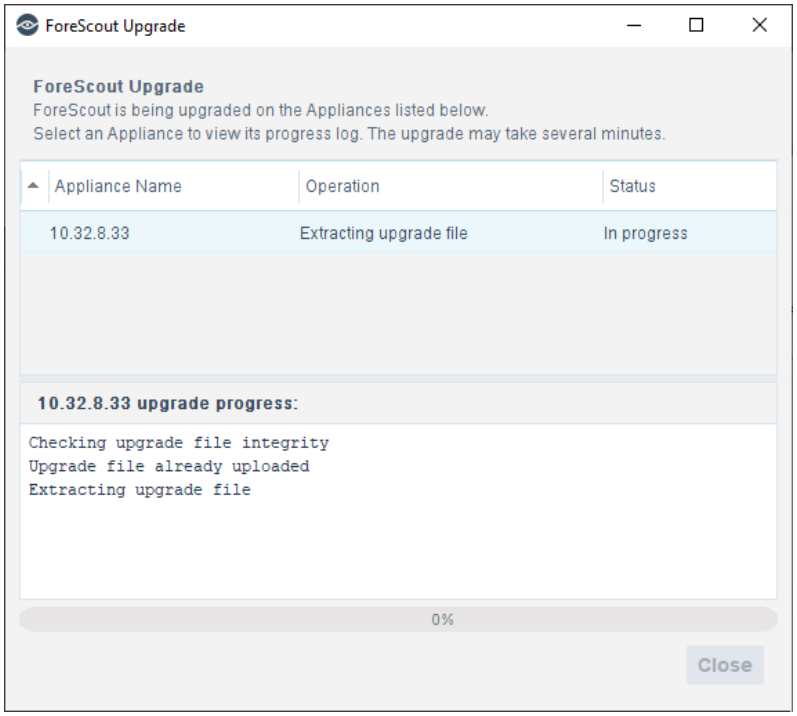


This dialog only appears after you upgrade your Enterprise Manager to version 8.1.

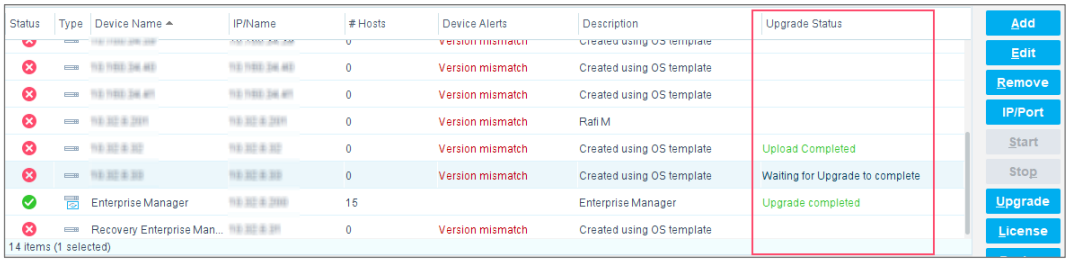
5. Select the scope of the upgrade:
   - Upload Only. Upload the file to the device but do not begin the upgrade.
   - Upload and Upgrade. Upload the file to the device and begin the upgrade.
   - Upgrade. Upgrade from the uploaded file. Only available after the file has already been uploaded to the Enterprise Manager.
6. Select **Browse...**, locate the upgrade file that you saved on your computer and select **OK**. After a check of the digital signature of the upgrade file is performed, the Forescout Upgrade screen opens.



7. Select **OK**. Once you confirm, the upgrade process proceeds to completion and cannot be interrupted or cancelled.



8. Review the Forescout Upgrade dialog box to see the status of the upgrade process. You can close the dialog box and continue to see the status in the Upgrade Status column of the CounterACT Devices pane. This column disappears when the upgrade has completed for all CounterACT devices in the deployment.



High Availability Devices – Upgrade for High Availability devices can take a long time (up to a number of hours). If the upgrade of the second node and the synchronization are not shown in the log, you can verify status via icons on the Console status bar:

	Indicates the status of the High Availability Appliances connected to the Enterprise Manager.
	Indicates the status of the Enterprise Manager High Availability pair.
	Indicates that High Availability is down on the Appliance.
	Indicates that High Availability is down on the Enterprise Manager.

9. When the upgrade is completed successfully, select **Close**. If the upgrade is not successful, contact your Forescout representative and **do not** continue with more upgrades.

Manually Upload the Upgrade File to an Appliance

In Forescout environments that experience connectivity issues (for example, the Appliance disconnects from the Enterprise Manager), you may prefer to manually upload the upgrade file to an Appliance/s.

To manually upload the file:

1. Before upgrading Appliances, you should upgrade the Enterprise Manager.
1. Download or obtain the upgrade file (FSP) and save it to a location on your computer.
2. Unzip the data.zip file from the FSP file.

   The unzip can be performed on any machine.

3. Rename the data.zip file to **fssetup.zip**.
4. Copy the extracted ZIP file to the following location on the Appliance machine:

/usr/src/**fssetup.zip**

The copied file will populate the Upgrade Status field in the Upgrade Status column of the CounterACT Devices pane after up to an hour from the time of copy, and only after the Enterprise Manager is upgraded with Forescout 8.1.

Upgrade High Availability Devices

For High Availability devices, back up the pair before you upgrade. The pair must be up when you upgrade. For High Availability upgrade information, refer to the section on upgrading High Availability systems in the *Forescout Administration Guide*. See Additional Forescout Documentation for information on how to access the guide.

To upgrade a single active High Availability node when the Secondary node has failed or has not been set up:

1. Make sure the Secondary node is not accessible
2. Create the file *.ignorestandby* under */etc/* on the node to be upgraded.

Upgrading to Version 8.1.3 and Migrating to Flexx Licensing Mode

If you would like to upgrade your deployment to version 8.1.3 operating in Flexx Licensing Mode, perform the following procedure. If your deployment is already operating in Flexx (Centralized) Licensing Mode, follow the procedure in Upgrading to Version 8.1.3.

All CounterACT releases prior to version 8.0 operate in Per-Appliance Licensing Mode. Refer to the Forescout Administration Guide *for more information about licensing. See Additional Forescout Documentation for information on how to access the guide.*

Before performing the migration, contact your Forescout representative to ensure you have a valid license entitlement for Forescout version 8.1, operating in Flexx Licensing Mode. Verify that you have credentials to access the Forescout Customer Portal and that the license entitlement has been added.

If you are using Forescout eyeExtend products (Extended Modules), be aware that Integration Modules, packaging together *groups of related licensed modules*, are not supported when operating in Flexx Licensing Mode. Only eyeExtend products, packaging *individual licensed modules* are supported. ***Before migration, uninstall any Integration Modules and reinstall them as eyeExtend products.*** Refer to the sections on Forescout eyeExtend products and Module Packaging in the *Forescout Administration Guide* for more information.

To upgrade and switch to Flexx licensing:

1. Back up Enterprise Manager system settings. Refer to the section on performing a one-time system backup in the *Forescout Administration Guide*. See Additional Forescout Documentation for information on how to access the guide.

2. Upgrade the Enterprise Manager to Forescout Version 8.1. See Upgrade the Enterprise Manager. Use the Forescout Upgrade file (FSP) for version 8.1.

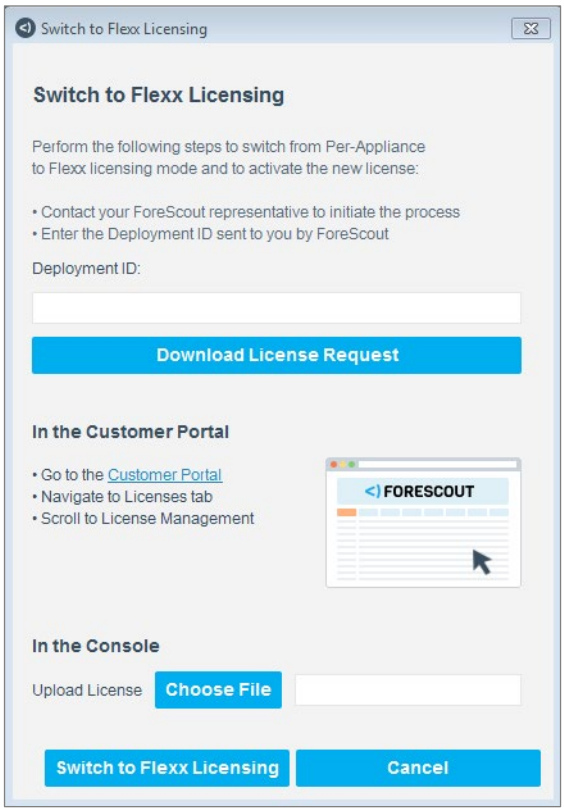
   After the upgrade, the Console is upgraded automatically, and all Appliances will become disconnected from the Enterprise Manager. The Appliances will continue to function normally and will reconnect to the Enterprise Manager after you upgrade the Appliances to Forescout Version 8.1.3 in step 12.

3. Upgrade the Recovery Enterprise Manager to Forescout Version 8.1. This procedure is only relevant if your deployment has a Recovery Enterprise Manager.

   After the upgrade, the Recovery Enterprise Manager will reconnect to the Enterprise Manager.

4. Log in to the Enterprise Manager via the Console.

5. Navigate to **Options > Licenses** and select **Switch to Flexx Licensing**.



6. In the Switch to Flexx Licensing dialog box, enter the Deployment ID, and then select **Download License Request**.

   The Deployment ID is listed in the Proof of Entitlement *email that you received from Forescout notifying you that your purchases are available in the Customer Portal.*

7. Select a file name and location to save the request file, and select **Save**.

8. In the Licenses tab of the Forescout Customer Portal, upload the license request file that you downloaded and then download the license file.
9. In the Console, select **Options > Licenses** and then **Switch to Flexx Licensing** to return to the Switch to Flexx Licensing dialog box.
10. In the **Upload License** field, select **Choose file** to find the new license file and then select **Switch to Flexx Licensing**.

    Continuing with the process will restart the Console, Enterprise Manager, and all connected Appliances in the deployment. The License Migration dialog box opens.

    If your deployment includes a Recovery Enterprise Manager or High Availability device, verify that it is connected to the Enterprise Manager before you activate the license file on your deployment.

11. Select **Yes**.

    A dialog box opens indicating that the license was activated successfully.
12. Upgrade each Appliance to Forescout Version 8.1.3. See Upgrade One or More Appliances. Use the Forescout Upgrade file (FSP) for version 8.1.3.

    After the upgrade, the Appliances will reconnect to the Enterprise Manager and then restart due to the change in licensing mode.
13. If the Failover Clustering Module is installed in your deployment, uninstall it from the Console (on the Enterprise Manager) in the Options > Modules page. In Flexx Licensing mode, Failover Clustering functionality is supported by the *Forescout eyeRecover (Forescout CounterACT Resiliency) License*. Refer to the section on the eyeRecover license in the *Forescout Administration Guide*. See Additional Forescout Documentation for information on how to access the guide.

Previous Releases

Installing this release also installs fixes and enhancements provided in the releases listed in this section. To view Release Notes of previous version releases, see:

https://www.forescout.com/company/resources/forescout-8-1-2-release-notes/

https://www.forescout.com/company/resources/forescout-8-1-1-release-notes/

https://www.forescout.com/company/resources/forescout-8-1-release-notes/

https://www.forescout.com/company/resources/counteract-version-8-0-1-release-notes/

https://www.forescout.com/company/resources/counteract-8-0-release-notes/

Additional Forescout Documentation

For information about other Forescout features and modules, refer to the following resources:

- Documentation Downloads
- Documentation Portal
- Forescout Help Tools

Documentation Downloads

Access documentation downloads from the Forescout Resources Page, or one of two Forescout portals, depending on which licensing mode your deployment is using.

- ***Per-Appliance Licensing Mode*** – Product Updates Portal
- ***Flexx Licensing Mode*** – Customer Portal

Software downloads are also available from these portals.

To identify your licensing mode:

- From the Console, select **Help > About Forescout**.

Forescout Resources Page

The Forescout Resources Page provides links to the full range of technical documentation.

To access the Forescout Resources Page:

- Go to https://www.Forescout.com/company/resources/, select **Technical Documentation,** and search for documents.

Product Updates Portal

The Product Updates Portal provides links to Forescout version releases, Base and Content Modules, and eyeExtend products, as well as related documentation. The portal also provides a variety of additional documentation.

To access the Product Updates Portal:

- Go to https://updates.forescout.com/support/index.php?url=counteract and select the version you want to discover.

Customer Portal

The Downloads page on the Forescout Customer Portal provides links to purchased Forescout version releases, Base and Content Modules, and eyeExtend products, as well as related documentation. Software and related documentation only appear on the Downloads page if you have a license entitlement for the software.

To access documentation on the Forescout Customer Portal:

- Go to https://Forescout.force.com/support/ and select **Downloads**.

Documentation Portal

The Forescout Documentation Portal is a searchable, web-based library containing information about Forescout tools, features, functionality, and integrations.

If your deployment is using Flexx Licensing Mode, you may not have received credentials to access this portal.

To access the Documentation Portal:

- Go to https://updates.forescout.com/support/files/counteract/docs_portal/ and use your customer support credentials to log in.

Forescout Help Tools

Access information directly from the Console.

Console Help Buttons

Use context-sensitive *Help* buttons to access information about tasks and topics quickly.

Forescout Administration Guide

- Select **Forescout Help** from the **Help** menu.

Plugin Help Files

- After installing the plugin, select **Tools** > **Options** > **Modules**, select the plugin, and then select **Help**.

Online Documentation

- Select **Online Documentation** from the **Help** menu to access either the Forescout Resources Page (Flexx licensing) or the Documentation Portal (Per-Appliance licensing).

Contact Information

Forescout Technologies, Inc.

190 West Tasman Drive

San Jose, CA 95134 USA

https://www.forescout.com/support/

Toll-Free (US): 1.866.377.8771

Tel (Intl): 1.408.213.3191

Support: 1.708.237.6591

About the Documentation

- Refer to the Resources page on the Forescout website for additional technical documentation: https://www.forescout.com/company/resources/
- Have feedback or questions? Write to us at documentation@forescout.com

Legal Notice

2019-11-06 15:30