About this Release

Forescout version 8.1 delivers new capabilities that significantly enhance operational technology support, classification, data center and cloud support, rogue device detection, IPv6 support, deployment, authentication, visibility, detection, control and security.

Some of these capabilities are supported by Modules Packaged with This Release and are documented in the respective Release Notes document of the individual module.

- Forescout Product Naming
- Flexx Licensing Enhancements
- Security Enhancements
- Dashboard Enhancements
- More Traffic Flow Protocols
- Upgrade Enhancements
- Monitoring of User Log In
- Control User Access to the Forescout Web Client

The following information is also 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
  - Core Extensions Module 1.1
  - Endpoint Module 1.1
  - Hybrid Cloud Module 2.0
  - Network Module 1.1
- Content Modules:
  - Device Profile Library 19.1.2
  - IoT Posture Assessment Library 18.0.4
  - NIC Vendor Database 19.0.2
  - Security Policy Templates 18.0.12
  - Windows Applications 19.0.1

– Windows Vulnerability DB 19.0.1

Refer to the respective Release Notes document for more information about these modules.

Finding More Documentation

See Additional Forescout Documentation for information about accessing guides referenced in this document.

System Requirements

This section describes system requirements for users upgrading to Forescout version 8.1, 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 virtual systems.

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 added in this release.*

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
- Hyper-V Server 2012
- Hyper-V Server 2012 R2

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

**Support added in this release.*

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 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.

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 Product Naming

As of this release, CounterACT is now referred to as the ***Forescout*** platform. For customers using Flexx licensing, the platform includes modular products. See Flexx Licensing Enhancements for more information.

Flexx Licensing Enhancements

This release significantly improves Flexx licensing with enhanced usability and modularity, as well as a new term licensing offering. Refer to the *Forescout Flexx Licensing How-to Guide* for more information about the features described in this section.

Flexx licensing was previously referred to as *Centralized licensing* in both the product and in documentation.

- New Product Naming
- Term Licenses
- Enhanced Product Modularity
- Improved Process for Switching to Flexx Licensing
- Self-Service Deployment Management and License Allocation
- Identifying Your Licensing Mode
- License Locking

New Product Naming

Forescout products are renamed as follows in this release. These names are reflected in the Forescout Console, Licenses page.

Original Product Name	New Product Name	Description
Forescout CounterACT See	Forescout eyeSight	Continuously discover, classify and assess devices upon connect without requiring agents or disrupting critical business operations.
Forescout CounterACT Control	Forescout eyeControl	Enforce and automate policy-based controls to proactively reduce your attack surface and rapidly respond to incidents.

Original Product Name	New Product Name	Description
Forescout CounterACT Resiliency	Forescout eyeRecover	Maintain continuity of Forescout services in single or multi-site deployments with failover clustering and high-availability pairing options.
Forescout Extended Module*	Forescout eyeExtend*	Share information and automate workflows through integrations with other IT and security products.

*The original product name will continue to appear on the Console Licenses page until the next license update is performed.

Term Licenses

Forescout now supports term licenses that authorize you to use licensed products for a defined period of time.

The Forescout Console displays both term and perpetual licenses that may be activated for a single product. A parent entry in the Licenses table (Options > Licenses) indicates the combined capacity of all such licenses. As long as one of the child entries is valid, regardless of its type, the licensed product is regarded as valid.

Name	Status	Type	Start Date	Expiration Date	Used Capacity	Free Capacity	Total Capacity
ForeScout eyeSight	Valid	Mixed			95	1105	1200
ForeScout eyeSight	Valid	Perpetual	11 Dec 2018	-			1000
ForeScout eyeSight	Valid	Perpetual	31 Dec 2018	-			100
ForeScout eyeSight	Valid	Beta	31 Dec 2018	15 Feb 2019			100

The Console also displays licenses that have a start date that is in the future. For example, even though you have a valid Forescout eyeSight license, you may have also activated the same product in anticipation of an approaching expiration date. In this case, the Console displays both the currently valid license and the newly added license.

Name	Status	Type	Start Date	Expiration Date
ForeScout eyeSight	Valid	Term		
ForeScout eyeSight	Valid	Term	05 Jan 2018	05 Jan 2019
ForeScout eyeSight	Invalid - Start date is in the future	Term	06 Jan 2019	06 Jan 2020

Enhanced Product Modularity

This release improves product modularity and granularity by allowing you to purchase the exact products that you need, with the specific license capacity that you want for each product:

- ***Purchase and install Forescout eyeSight and Forescout eyeControl product licenses separately***. Refer to the *Forescout Flexx Licensing How-to Guide* for a list of features supported by each license, including Forescout actions.
- ***Purchase and install eyeControl and eyeRecover products with license capacities equal to or less than the capacity of eyeSight***. eyeExtend license capacities varies my module, but cannot exceed the capacity of eyeSight.
- The base licensed product is eyeSight, which must be installed on each deployment. Purchase additional licensed products to expand capabilities and address specific business use cases.

Changes to eyeControl Supported Features

The following features, previously supported by eyeSight (Forescout CounterACT See) are now supported by eyeControl:

- Authentication and authorization of users and devices via the RADIUS Plugin
- Guest management functionality

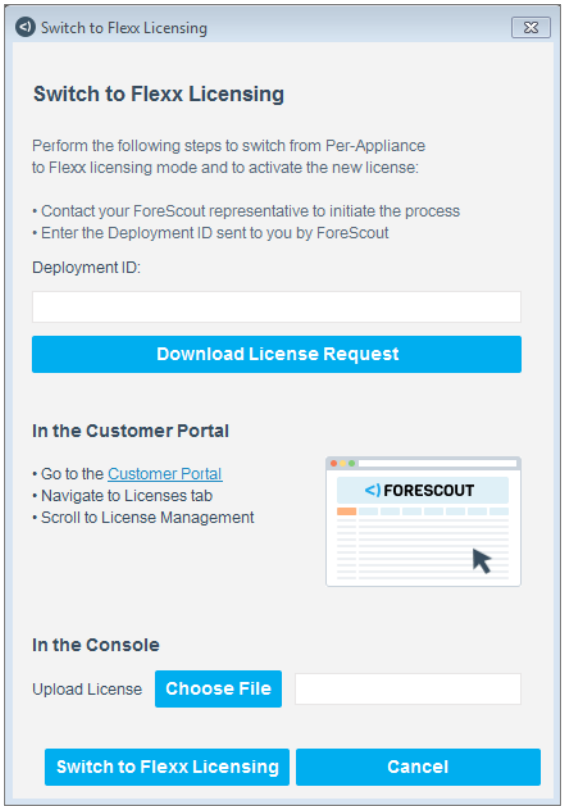
Known Limitation – Endpoint Count for eyeControl / eyeExtend

Certain complexly constructed policy conditions may result in an inaccurate count of endpoints against the product's license capacity.

Improved Process for Switching to Flexx Licensing

If you are running Forescout 8.1 in Per-Appliance licensing mode, you can switch to work with Flexx licensing in the Console only after completing the required migration process with your Forescout sales representative.

The flow in the Console has been improved to ensure that your new license is activated before you switch to Flexx licensing. Otherwise, you will remain in Per-Appliance mode.



Self-Service Deployment Management and License Allocation

You can now use the Forescout Customer Portal to actively manage your deployment/s and allocate purchased endpoint license capacity. If your organization has multiple deployments, each managed by a separate Enterprise Manager, add a new deployment in the Customer Portal for each additional deployment and allocate endpoint quantity across those deployments.

Allocate Endpoint Capacity Across Multiple Deployments

Some organizations have multiple deployments, each managed by a separate Enterprise Manager. To allocate purchased licensed products across deployments, add a new deployment in the Customer Portal for each deployment and follow the guidelines laid out in the use case examples described in the *Forescout Flexx Licensing How-to Guide*.

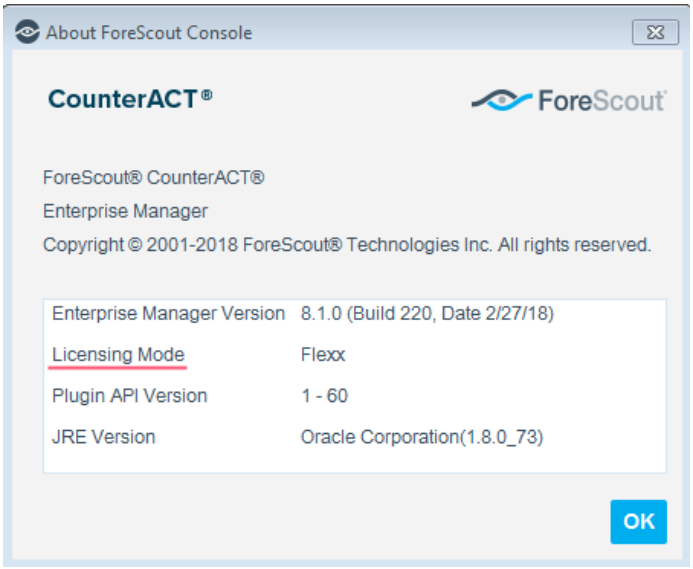
When product endpoint license capacity is already activated on a deployment, you cannot reduce the allocation quantity for that product until you first deactivate the license file and release the activated endpoints.

Identifying Your Licensing Mode

You can easily identify your licensing mode in the Console.

To identify your licensing mode:

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



License Locking

Once you activate the license using a specific Deployment ID, that ID is locked to the machine (either an Enterprise Manager or Standalone Appliance). If you try to activate a license on another machine using an already locked ID, activation will fail. You must first deactivate the license file on the original machine. For example, if you activated the license on a Standalone Appliance, and then later want to add that Appliance to a newly deployed Enterprise Manager (without an activated license), perform the following:

1. Deactivate the license file on the Standalone Appliance.
2. Add the Appliance to the Enterprise Manager.
3. Activate a new license file on the Enterprise Manager.

Security Enhancements

- New Forescout CLI (FS-CLI)
- Certification Compliance
- Enhanced Secure Communication
- Define Web Access for Specific Web Features

- Enhanced Authentication for Smart Card User Log In
- Prevent Concurrent Console and Web Portal User Sessions
- Repair Appliance Private Keys
- New Session ID Field in Audit Logs and Syslog Messages
- Display the User Login Summary

New Forescout CLI (FS-CLI)

FS-CLI is a proprietary Forescout command line interface that is designed to comply with security certification requirements.

The FS-CLI is installed by default in all Forescout version 8.1 systems. Depending on whether you performed a clean installation or upgraded to Forescout 8.1, FS-CLI may or may not be enabled when you log in to the CLI:

- ***Clean 8.1 installation***. FS-CLI is installed and enabled.
- ***Upgrade to 8.1***. FS-CLI is installed, but not enabled.

Refer to the *Forescout CLI Commands Reference Guide* for more information, and for a list of commands supported when FS-CLI is enabled.

To enable FS-CLI:

1. Log in to the CounterACT Appliance CLI (Bash shell).
2. Run: `fstool cli`

A special command is available that allows you to exit the FS-CLI and access the operating system's Bash shell.

To return to the Bash shell:

- Run: shell

Certification Compliance

Certification Compliance mode is a hardened configuration mode that enables advanced security features. If your organization needs to comply with strict security requirements, you can configure Forescout 8.1 to run in Certification Compliance mode during the initial Enterprise Manager/Appliance CLI configuration of a clean Forescout 8.1 installation.

Refer to the *Forescout Installation Guide* for information on how to configure Forescout 8.1 to run in Certification Compliance mode.

When Forescout 8.1 is running in Certification Compliance mode, the following features are affected:

- ***FS-CLI***. Users won't be able to access the Bash shell. FS-CLI, a proprietary Forescout command line interface, is the only CLI shell available.
- ***TLS***. The TLS version will be set to v1.2 with no option to change to lower versions.

- ***SNMP***. SNMPv3 will be set as the default. If you select a different version, a warning will appear.
- ***NTP***. Authenticated NTP will be set as the default. If you use unsecure, unauthenticated NTP, a warning will appear.
- ***Log and database partitions***. These partitions will be encrypted.
- ***FIPS Compliance*** will be enabled.
- Additional user actions will be written to the Audit Trails.

Enhanced Secure Communication

With this version, secure communication among the Enterprise Manager/the Appliances/the Console is enhanced with TLS v1.2 being the default communication protocol in use.

If a Forescout deployment requires modifying the default TLS version to use, do the following:

1. On the Enterprise Manager, log in to the command line interface (CLI)
2. To modify the setting for the Enterprise Manager, run the following fstool command:

   `fstool set property fs.supported.tls.protocols=`<*prioritized list of the TLS version(s) to use*>

3. To modify the setting for all Appliances, run the following fstool command:

   `fstool oneach –c fstool set property fs.supported.tls.protocols=`<*prioritized list of the TLS version(s) to use*>

Across all your Forescout devices (Enterprise Manager, all Appliances), you must uniformly modify the TLS version(s) to use.

Example:

Modify the setting for the Enterprise Manager so that TLSv1.1 is the default, protocol version to use and TLSv1.2 is the second protocol option to use. From the CLI of the Enterprise Manager, run the following fstool command:

`fstool set property fs.supported.tls.protocols=`TLSv1.1 TLSv1.2

Define Web Access for Specific Web Features

You can define a range or subnet of IP addresses allowed to access specific Forescout web features, such as Forescout web portals, the Forescout Compliance Center and the Forescout SecureConnector Distribution Tool. Previously, defined IP addresses were granted access to all web features. *If you do not assign any IP addresses to a web feature, no access will be allowed to that feature.*

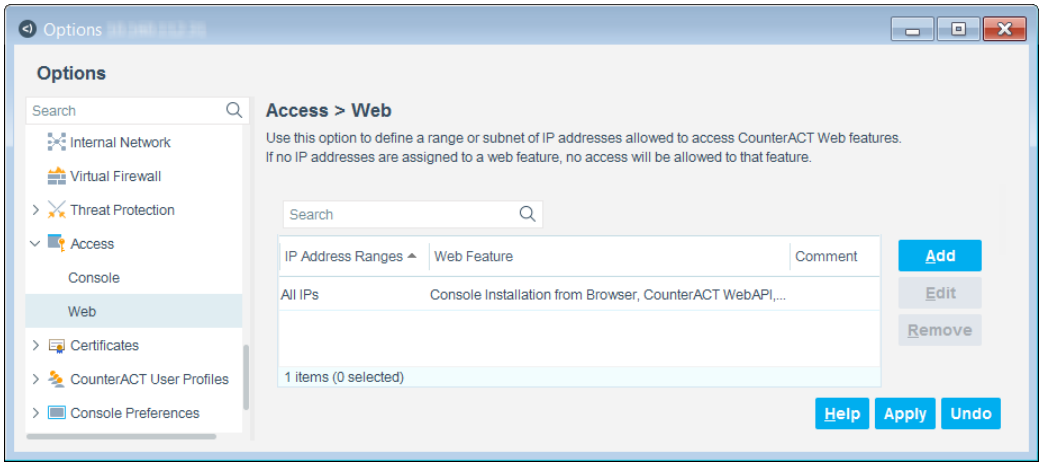
> *Grant web access only to IP addresses that are included in the Internal Network.*

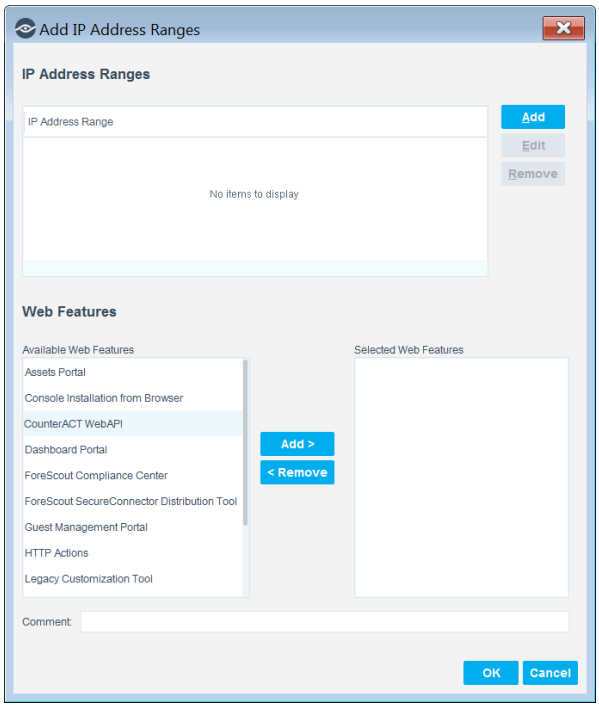
What Happens to My Configuration When I Upgrade to 8.1?

- If 'All IPs' was previously configured in Options > Access > Web, all IP addresses will be granted access to all web features after upgrade.
- If specific IP addresses were previously configured in Options > Access > Web, those IP addresses will be granted access to all web features after upgrade.

What Happens if I Perform a Clean Installation?

- All IP addresses will be granted access to all Forescout web features.
- If Forescout 8.1 is running in Certification Compliance mode, all IP addresses will be granted access to all Forescout web features except for the following features:
  - Guest Sponsors Portal
  - Assets Portal
  - Legacy Dashboard Portal
  - Reports Portal





Enhanced Authentication for Smart Card User Log In

The Forescout administrator can optionally require Forescout users, who are configured to log in using a Smart Card, to perform *two-factor authentication* when logging in to the Console and the Forescout Web Client.

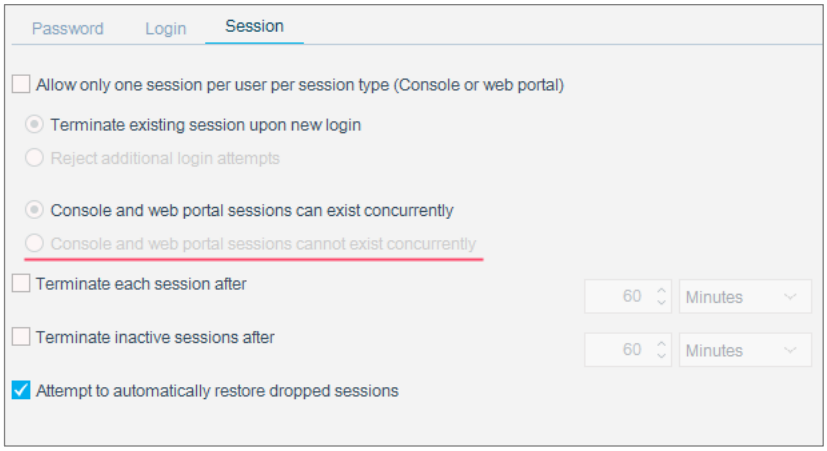
When configuring a Smart Card user in the Console's **Options** > **CounterACT User Profiles** > **Add User Profile** > **General** pane (Step 1), the administrator does the following to configure *two-factor authentication*:

1. Enable the **Requires two-factor authentication** option
2. Specify the verification method to be used in the two-factor authentication and complete the required fields for the specified method

Prevent Concurrent Console and Web Portal User Sessions

You can choose to prevent Forescout users from logging into both a Console and web portal session at the same time. By default, the system allows Console and web portal sessions to exist concurrently.

This option is configured in the Console, Tools > Options > CounterACT User Profiles > Password and Sessions > Session tab.



Repair Appliance Private Keys

All private keys of a Forescout deployment are encrypted with a password (a.k.a. site-key) that is shared by Enterprise Manager with all of the Appliances in the deployment. In the rare event, when attempting to join a standalone Forescout Appliance with an Enterprise Manager, that the join succeeds, but, for example, the Forescout web server fails to start. This situation is almost always due to private keys of system certificates remaining encrypted with the standalone Appliance's password, rather than being encrypted with the password of the Enterprise Manager. Use the following, newly available fstool command to repair private keys:

```
fstool certool fix_keys
```

To repair Appliance private keys, do the following:

1. On the Appliance, log into the command line interface (CLI).
2. Run the following sequence of commands:
   a. **`fstool certool fix_keys --list`**

      This command identifies all of the private keys on the Appliance that require repair.
   b. **`fstool certool fix_keys`**

      This command repairs the identified private keys
   c. **`fstool certool fix_keys --list`**

      After the repair, run this command again. The command issues the following statement: *All keys are intact* that identifies that there are no longer private keys requiring repair.

For example:

1. [root@ct8-app-0102 forescout]# **`fstool certool fix_keys --list`**

   cert:25744:1552486176.879096:Wed Mar 13 16:09:36 IST +0200 2019: main::_fix_keys:616: ***Key needs fixing***: */usr/local/forescout/etc/cert/endentity/store/1767bc59-cf28-4b80-be6c-eccdaf23d68f/private.key*; ***used by[net_portal]***

2. [root@ct8-app-0102 forescout]# **fstool certool fix_keys**

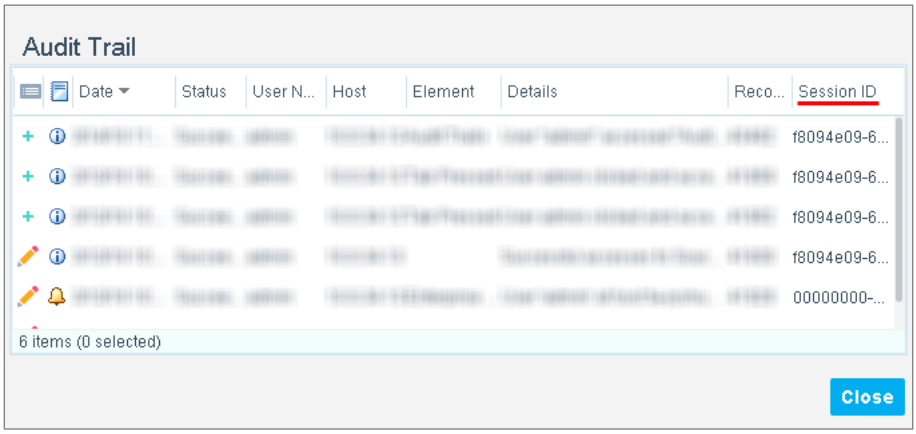
   cert:25896:1552486183.169912:Wed Mar 13 16:09:43 IST +0200 2019: main::_fix_keys:620: ***Fixing key*** */usr/local/forescout/etc/cert/endentity/store/1767bc59-cf28-4b80-be6c-eccdaf23d68f/private.key*
   writing RSA key
   writing RSA key
   cert:25896:1552486183.321347:Wed Mar 13 16:09:43 2019: main::_fix_keys:623: ***Key fixed successfully***: */usr/local/forescout/etc/cert/endentity/store/1767bc59-cf28-4b80-be6c-eccdaf23d68f/private.key*; ***used by[net_portal]***

3. [root@ct8-app-0102 forescout]# **fstool certool fix_keys --list**

   cert:26128:1552486186.754081:Wed Mar 13 16:09:46 IST +0200 2019: main::_fix_keys:608: ***All keys are intact***

New Session ID Field in Audit Logs and Syslog Messages

The new Session ID field lets you track events based on a Console user's session. A unique, positive integer value identifies the Forescout user session associated with the reported event. A null (zero) value indicates an event generated by internal audit processes. This field appears the Audit Log window, and is included in Syslog messages sent by Forescout.



Dashboard Enhancements

The Forescout Dashboard page is a web application that is provided by the Forescout Core Extensions Module: Dashboard Plugin. The Dashboard is an information center that provides an overview of your network and delivers dynamic at-a-glance information, including:

- Device compliance

- Device classification
- Device management status

Users access the Dashboard page from the Forescout Web Client. A primary Dashboard feature is the information widget; both Forescout *out-of-the-box* widgets and custom widgets that are created by users.

With this version, the following Dashboard enhancements are available:

- Edit Widgets
- Re-arrange the Widget Display

Edit Widgets

In the Dashboard, edit any widget. Select a custom widget and click **Edit** to open the Widget Builder. The Widget Builder wizard guides you through the editing process. Modify any of the following widget components:

- Widget display format - **DONUT**, **TREND** or **COUNTER**
- The policy that the widget must reference
- Based on the selected policy, modify the policy sub-rules that the widget must reference for information
- Widget title
- Widget sub-rule labels

Re-arrange the Widget Display

In the Dashboard widget area, drag and drop widgets to re-arrange their display in the page; click on a widget, drag it from its existing location to a different location in the Dashboard widget area and then click again to release (drop) it into its new location.

More Traffic Flow Protocols

More types of traffic flows can be analyzed and used to resolve endpoint properties.

The Flow Collector supports the following protocols, with or without Flexible NetFlow technology:

- NetFlow v9
- IPFIX
- sFlow

Upgrade Enhancements

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.

See Performing the Upgrade for more information.

Monitoring of User Log In

With this version, the following enhancements dealing with the monitoring of users' log in are available:

- Set the Period for Number of Logins Displayed
- Display the User Login Summary

Set the Period for Number of Logins Displayed

With this version, the Forescout administrator can configure the option **In the User Profiles table, show number of successful logins in the past** <*time period*>. The administrator specifies the time period by entering a number and selecting either *Days*, *Weeks* or *Months*. The option is available in the Console's **Options** > **CounterACT User Profiles** > **Password and Sessions** > **Login** tab.

Based on this option, the **Number of Logins** column in the **CounterACT User Profiles** table presents the number of successful Console and web portal logins that occurred within the configured time period, per user account name.

Display the User Login Summary

The Forescout administrator can enable/disable the display of a dialog summarizing the user's recent login activity. When the option is enabled, the dialog displays immediately after each, successful user log in. By default, this option is disabled.

In the Console **Options** > **CounterACT User Profiles** > **Password and Sessions** > **Login** tab, select the new option **After login, show the login summary dialog**.

Control User Access to the Forescout Web Client

The Forescout Web Client (FWC) provides the presentation framework for user access to Forescout web applications. Users access Forescout web applications either from the Console toolbar or via web browser > FWC login page. The currently available Forescout web application is the **Dashboard**. By default, all Forescout users can access the FWC and, as a result, the available Forescout web applications.

Several new fstool commands are now available that provide Forescout administrators with the capability to control user access to the FWC and, as a result, control user access to the Forescout web applications. Forescout administrators must run these fstool commands from the command line interface (CLI) of the Enterprise Manager.

Access control consists of the following activities:

- Block user access to the FWC
- List currently blocked users
- Allow user access to the FWC

Refer to the *Forescout Administration Guide, Chapter 17: The Dashboard* for details about using these fstool commands.

Forescout Fixed Issues

This section describes fixed issues for this release.

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

Issue	Description
CA-13858	For Flexx licensing customers: The license file was not saved during system backup.
CA-15372 **CA-15143**	Upgrading the Forescout Console software was not supported for Linux and OS X operating systems.
CA-19577	The Delete Host action did not propagate properly to all Appliances.

Forescout Known Issues

This section describes known issues for this release.

Issue	Description
CA-6935	The online Help library is not accessible if the Forescout Console is not connected to an Enterprise Manager.

Issue	Description
CA-6974	In a Forescout deployment using Failover Clustering, actions that are performed by an Appliance other than the one which manages the endpoint continue to be applied to excess endpoints for 30 minutes after failover. Failover excess endpoints are endpoints that, after a failover, exceed the capacity of the recipient Appliance and are not fully handled.
CA-13036	Under certain circumstances, hosts are listed twice with different keys under Groups Manager > Permanent tab. Workaround: manually delete the extra entry.
CA-16268	After a switchover from the Recovery Enterprise Manager back to the Enterprise Manager, the Reports Portal stops functioning when using some versions of Internet Explorer.
CA-16868	For Flexx licensing customers: After you successfully activate a license file containing one or more expired feature licenses, any attempt to update or deactivate the license file will fail when you upload the license request file to the Forescout Customer Portal. To update or deactivate license file in this case, contact your Forescout representative.
CA-19858	For Per-Appliance licensing customers: When an invalid eyeExtend product license (Extended Module license) becomes valid, previously configured actions supported by the license are not automatically performed. For example, an action that was scheduled to be performed every hour does not continue on schedule after the license becomes valid.
CA-21005	If there is an empty parent segment with one or more empty child segments, and you assign one of the child segments to an Appliance folder (as the only assigned segment) and then configure it as a failover cluster folder, you are allowed to delete that child segment from the Segment Manager. Additionally, the Appliance folder remains a failover cluster folder, even though the assigned segment is empty. Workaround: Verify that at least one IP address segment or range is directly assigned to the failover cluster folder. If none is assigned, either assign at least one IP address segment to it, or disable failover for the folder after assigning the segment to it.
CA-21590	The **Terminate inactive sessions after** option disconnects all Console and web sessions after the defined amount of time, but web users are automatically logged in again until **Terminate each session after** expires.

Issue	Description
CA-21906	If different DNS servers use different FDQNs to identify the same CounterACT device, an endpoint attempting to access a Forescout web portal might receive an "Error:Invalid request" message. Workaround: Log in to the CounterACT device CLI and run the following commands: ▪ **`fstool set_property fs.httpd.extra.hosts "<FQDN1> <FQDN2>"`** ▪ **`fstool www restart`** where the quotation marks contain a space-separated list of all the FQDNs by which the CounterACT device is known.
CA-22030	When uploading the Forescout version 8.1 upgrade file to multiple Appliances after an Enterprise Manager restart, and when multiple instances of the Console are connected simultaneously, the Forescout service may stall and the upgrade process may fail on some of the Appliances. This may occur when a Recovery Enterprise Manager is connected to the deployment.

Upgrading to Version 8.1

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 Forescout CounterACT version 7.0.0 with Service Pack 3.0.2.x installed and from Forescout CounterACT version 8.0.1. To upgrade from version 8.0, first upgrade to version 8.0.1. It is recommended to make sure you have the Optimal Component Versions Compatible for Upgrading from Version 7.0.0 to 8.1 installed before performing the upgrade.
- Upgrade ***is not supported for High Availability pairs,*** when such pairs are running Forescout CounterACT v7.0.0 installed with Service Pack 3.0.2.x and also installed with ***OSUP 1.2.5*** and ***CIUP 2.0.11***.

  However, an alternate method for accomplishing such an upgrade is available; the following article describes this alternate upgrade method:

  https://forescout.force.com/support/s/article/HA-upgrades-from-version-7-to-8-1-may-fail-with-Could-not-stop-services-on-stand-by-member
- ***Rollback is not supported by this version***. It is recommended that you back up your system before performing the upgrade. You can use the *Restore* tool if you need to revert to your previous system settings.

- 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.
- With the introduction of the Forescout Flow Collector, the legacy NetFlow Plugin has been 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.

Optimal Component Versions Compatible for Upgrading from Version 7.0.0 to 8.1

The following components are the optimal versions that are compatible when upgrading to Forescout version 8.1 from version 7.0.0. It is recommended to make sure that these versions are installed before performing the upgrade.

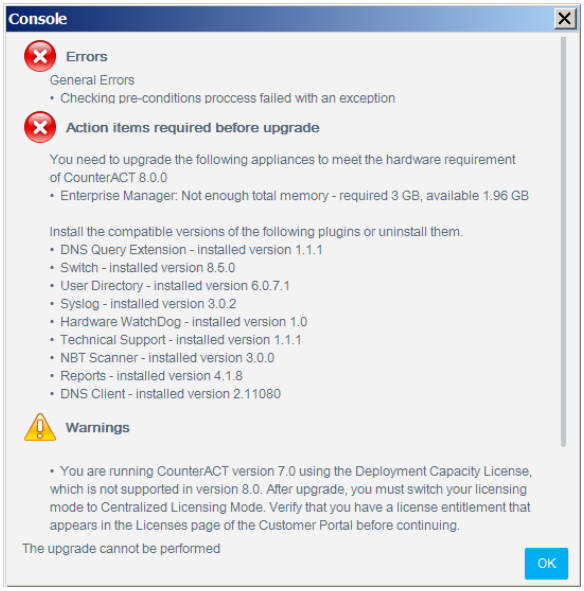
Component Name	Optimal Versions Compatible for V8.1 Upgrade
CounterACT 7.0.0 Service Pack	3.0.2.x
802.1X Plugin	4.2.2
Advanced Tools Plugin	2.2.3
CEF Plugin	2.6.1
DHCP Classifier Plugin	2.0.6
DNS Client Plugin	3.0.0
DNS Enforce Plugin	1.1.6
External Classifier Plugin	2.2.2
Hardware Inventory Plugin	1.0.2
Hardware WatchDog Plugin	1.1.4
HPS Inspection Engine	10.7.2
Macintosh/Linux Property Scanner Plugin	7.0.2
Microsoft System Management Server (SMS) System Center Configuration Manager (SCCM) Plugin	2.2.5
NBT Scanner Plugin	3.0.4
OS X Plugin	2.0.2
Reports Plugin	4.3.0
Switch Plugin	8.11.2
Syslog Plugin	3.2.0
Technical Support Plugin	1.1.2
User Directory Plugin	6.1.3
VMware vSphere Plugin	2.0.0
VPN Concentrator Plugin	4.0.8
Wireless Plugin	1.7.2
Cisco PIX/ASA Firewall Integration Plugin	2.0.2
Forescout Open Integration Module: Data Exchange Plugin	3.2.1
Forescout Extended Module for HPE ArcSight	2.7.1
MobileIron Plugin	1.7.1
Palo Alto Networks WildFire Plugin	2.0.0

Component Name	Optimal Versions Compatible for V8.1 Upgrade
Forescout Extended Module for Qualys VM	1.2.1
Forescout Extended Module for Splunk	2.7.0
Forescout Extended Module for Palo Alto Networks Next-Generation Firewall	1.1.1
Forescout Extended Module for Tenable Vulnerability Management	2.6.0
Forescout Extended Module for VMWare AirWatch MDM	1.7.2
Forescout Extended Module for Web API	1.2.2
Forescout Amazon Web Services (AWS) Plugin	1.1.1
IOC Scanner Plugin	2.1.0
FireEye NX Module	2.0.0
FireEye EX Plugin	1.1.0
FireEye HX Plugin	1.1.0
Forescout Extended Module for McAfee ePolicy Orchestrator	3.0.0
Forescout Extended Module for IBM QRadar	2.0.1
Forescout Extended Module for Rapid7 Nexpose	1.1.1

Components Not Supported for Version 8.1 (Upgrade from Version 7.0.0)

When upgrading from version 7.0.0, 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.
- 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

If you are upgrading from version 7.0.0, 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

Products that are not supported for Forescout 8.1 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, 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. These procedures are provided, due to Forescout version 8.1'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.

Before upgrading to Forescout version 8.1, 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 2.0.0
   - 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, 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 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.

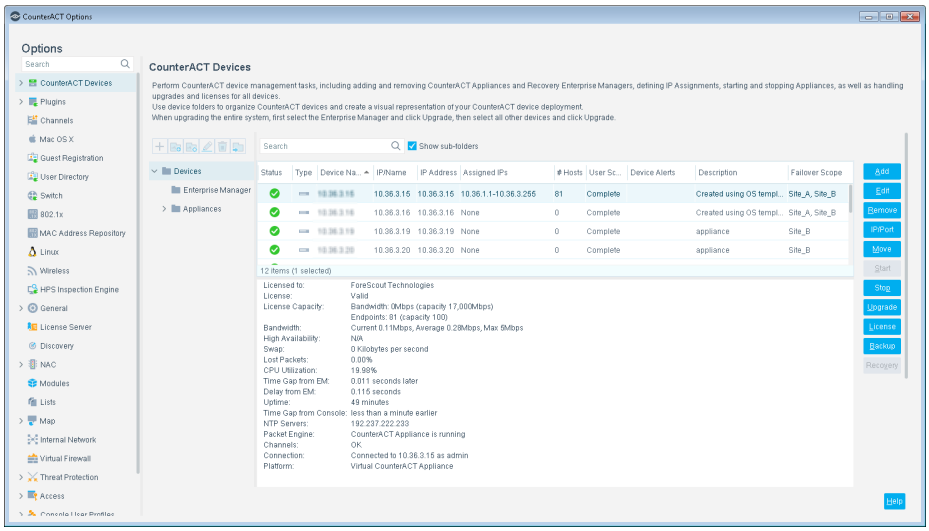
The upgrade installs the Forescout core platform as well the Base Modules, Content Modules and previously installed eyeExtend products (Extended Modules), unless the component is End-of-life.

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. 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.

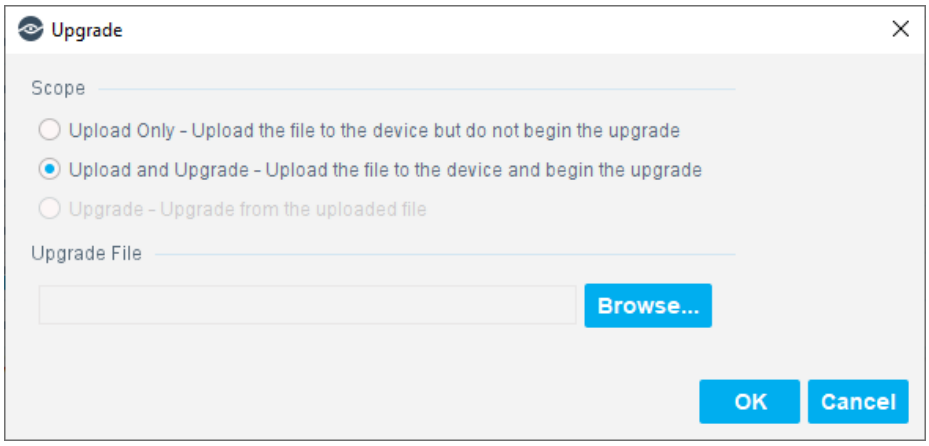
9. When the upgrade is completed successfully, select **Close**. If the upgrade is not successful, contact your Forescout representative and ***do not*** continue with more upgrades.

Upgrade One or More Appliances

To upgrade to a new version:

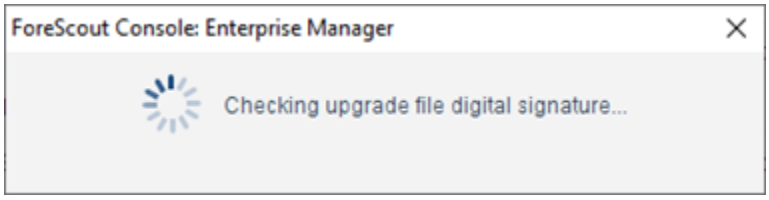
1. Before upgrading Appliances, you should upgrade the Enterprise Manager.
2. Download or obtain the upgrade file (FSP) for version 8.1 and save it to a location on your computer.
3. Select **Options** from the **Tools** menu.

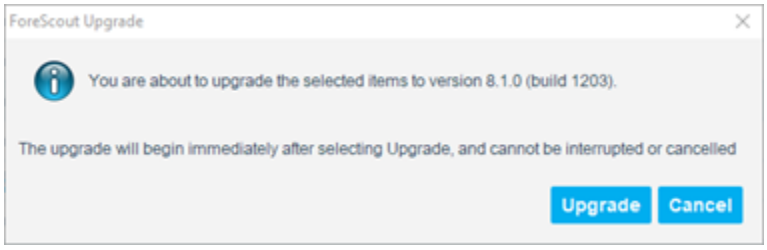
   CounterACT devices or Appliances are shown with their current version.
4. Select an Appliance or group of Appliances and select **Upgrade**. Do not select Enterprise Managers together with Appliances, because you cannot upgrade both Appliances and Enterprise Managers at the same time.



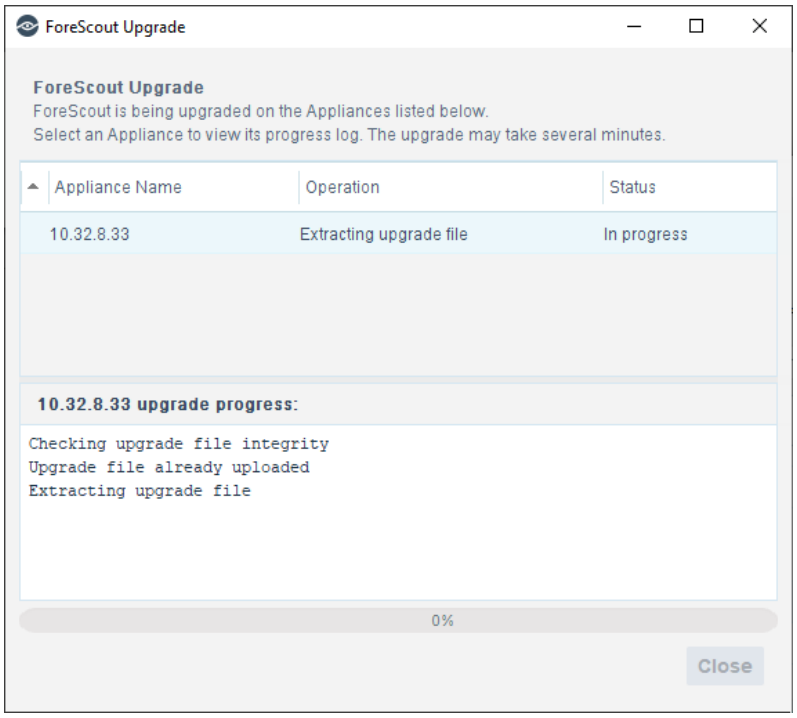
This dialog only appears after you upgrade your Enterprise Manager to version 8.1.

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.

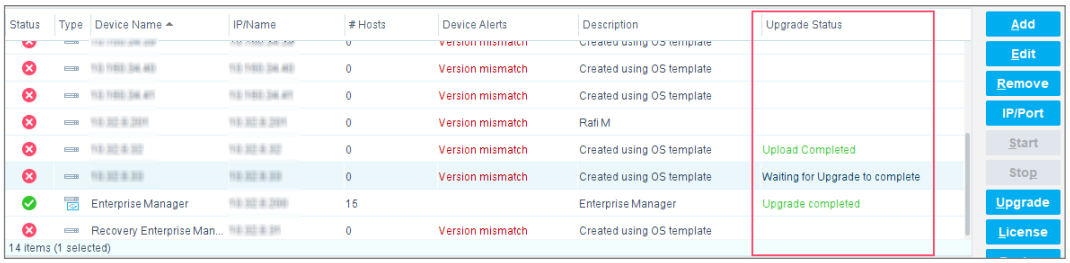




7. Select **OK**. Once you confirm, the upgrade process proceeds to completion and cannot be interrupted or cancelled.



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.
2. Download or obtain the upgrade file (FSP) and save it to a location on your computer.
3. Unzip the data.zip file from the FSP file.

   The unzip can be performed on any machine.

4. Rename the data.zip file to **fssetup.zip**.
5. 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 and Migrating to Flexx Licensing Mode

If you would like to upgrade your deployment to version 8.1 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.

- *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.

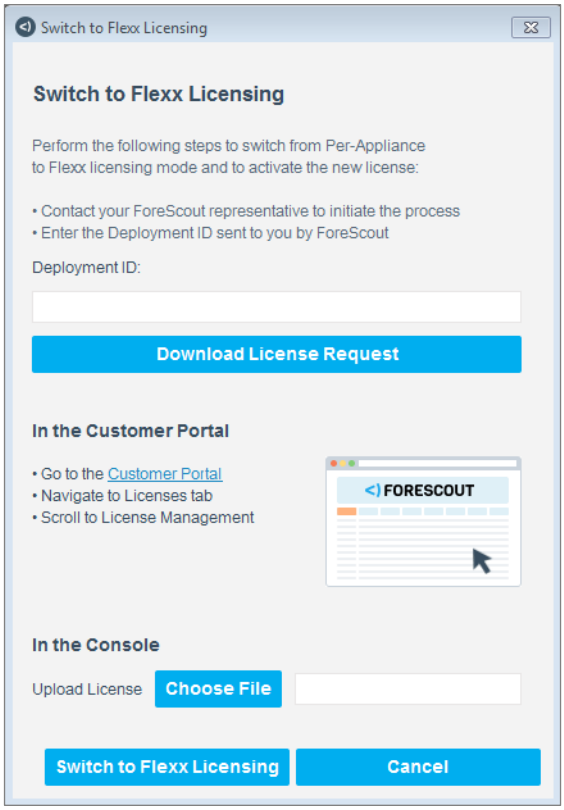
If you are using Forescout eyeExtend products (Extended Modules), be aware that Integration Modules, packaging together *groups of related licensed modules*, are not supported when operating in Flexx Licensing Mode. Only eyeExtend products, packaging *individual licensed modules* are supported. ***Before 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 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. See Upgrade One or More Appliances. Use the Forescout Upgrade file (FSP) for version 8.1.

    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.

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

Documentation downloads can be accessed 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 will 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 quickly access information about the tasks and topics you are working with.

Forescout Administration Guide

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

Plugin Help Files

- After the plugin is installed, 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

2019-05-15 15:29