About this Release

Forescout version 8.1.1 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 8.1.1

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 1.1.1
  - Endpoint Module 1.1.1
  - Hybrid Cloud Module 2.0
  - Network Module 1.1.1

- Content Modules:
  - Device Profile Library 19.1.2
  - IoT Posture Assessment Library 19.0.4
  - 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. See Previous Releases to access Release Notes for previous version releases.
System Requirements

This section describes system requirements for users upgrading to Forescout version 8.1.1, 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 8.1.1 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 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
  - 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 8.1.1 can be installed on all hardware revisions of CounterACT physical Appliances and Enterprise Managers except for the following:

<table>
<thead>
<tr>
<th>Model</th>
<th>Revisions Not Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CTR</strong></td>
<td>CTR-11, CTR-12, CTR-13</td>
</tr>
</tbody>
</table>
| **CT100** | CT100-20, CT100F-20  
  CT100-21, CT100F-21  
  CT100-22, CT100F-22 |
| **CT1000** | CT1000-20, CT1000F-20  
  CT1000-21, CT1000F-21  
  CT1000-22, CT1000F-22, CT1000F2-20  
  CT1000-21, CT1000F-21, CT1000F2-21  
  CT1000-22, CT1000F-22, CT1000F2-22 |
CT-xxxx CounterACT devices based on hardware revision -10 or lower also do not support Forescout version 8.1.1.

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 Fixed Issues

This section describes fixed issues for this release. 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.
### Issue Description

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CA-15372</td>
<td>Upgrading the Forescout Console software was not supported for Linux and OS X operating systems.</td>
</tr>
<tr>
<td>CA-15143</td>
<td></td>
</tr>
<tr>
<td>CA-19577</td>
<td>The Delete Host action did not propagate properly to all Appliances.</td>
</tr>
<tr>
<td>CA-20362</td>
<td>Under certain circumstances, when there was no disk space available, an OOM database error occurred.</td>
</tr>
<tr>
<td>CA-22072</td>
<td>When a device is a member of the Passive Learning group, the DNS Name property returned a status of 'Irresolvable'. The accompanying troubleshooting message indicated that active inspection is blocked.</td>
</tr>
<tr>
<td>CA-22096</td>
<td>Switches sometimes appeared in the Switch tab of the Switch Plugin with a status of 'Loading...'.</td>
</tr>
<tr>
<td>CA-22260</td>
<td>Under certain rare circumstances, the Console Home view got stuck when scrolling quickly through devices before indexing was complete, and device information failed to load.</td>
</tr>
<tr>
<td>CA-22262</td>
<td>When there is an unstable connection between the Enterprise Manager and its Appliances, the upgrade status might appear as 'Upgrade failed' for a short period.</td>
</tr>
<tr>
<td>CA-22269</td>
<td>Some Forescout web portals failed to get configuration data during system startup, causing those portals to not load properly.</td>
</tr>
<tr>
<td>CA-22278</td>
<td>Under certain circumstances, users received an application error when trying to access Forescout web portals.</td>
</tr>
<tr>
<td>CA-22420</td>
<td>Non-compliant devices managed by SecureConnector continued to appear as compliant even after a compliance policy was started.</td>
</tr>
</tbody>
</table>

### Forescout Known Issues

This section describes known issues for this release. See Previous Releases for information about accessing Release Notes that include fixed issues from earlier releases.

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
</table>
| CA-22618 | Forescout can discover endpoints not assigned to any Appliance (outside the internal network range), but these endpoints cannot be properly resolved by policies.  
**Workaround:**  
It is recommended to explicitly limit the scope of your policies to endpoints within the internal network range. |
| CA-22666 | When upgrading Forescout to version 8.1.1 and the deployment includes a Recovery Enterprise Manager, the pre-upgrade verifier does not check the Recovery Enterprise Manager. |
Forescout 8.1.1
Release Notes

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
</table>
| CA-22870 | If the software upgrade of a Forescout device, whether Enterprise Manager or Appliance, fails due to a network connectivity issue, attempting to continue with that upgrade upon network connectivity being restored, results in the following error message:  
  ▪ Cannot Upgrade Appliance(s) that are already being upgraded  
  Appliances: <Forescout device name>  
  **Workaround:**  
  Instead, upon network connectivity being restored, do the following:  
  1. From the Linux bash of the Enterprise Manager, run the following fstool command:  
     `fstool message upgrade_status_reset`  
  2. Re-perform the software upgrade for the affected Forescout device. |
| CA-22884 | Running either the Linux bash command `reboot` or the Forescout command `fstool reboot` on the physical appliances CT-R and 5110 may result in the reboot processing being stuck/not completing, in which case manual power cycle of the appliance is necessary to reboot the appliance. |

---

**Upgrading to Version 8.1.1**

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 the following versions:
  - Forescout CounterACT version 7.0.0 with Service Pack 3.0.2.x installed
  - Forescout CounterACT version 8.0.1
  - Forescout version 8.1

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 8.1.1](#) 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:


• **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.

• 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 8.1.1

The following components are the optimal versions that are compatible when upgrading to Forescout version 8.1.1 from version 7.0.0. It is recommended to make sure that these versions are installed before performing the upgrade.

<table>
<thead>
<tr>
<th>Component Name</th>
<th>Optimal Versions Compatible for V8.1.1 Upgrade</th>
</tr>
</thead>
<tbody>
<tr>
<td>CounterACT 7.0.0 Service Pack</td>
<td>3.0.2.5010</td>
</tr>
<tr>
<td>802.1X Plugin</td>
<td>4.2.2</td>
</tr>
<tr>
<td>Advanced Tools Plugin</td>
<td>2.2.3</td>
</tr>
<tr>
<td>CEF Plugin</td>
<td>2.6.1</td>
</tr>
<tr>
<td>DHCP Classifier Plugin</td>
<td>2.0.6</td>
</tr>
<tr>
<td>DNS Client Plugin</td>
<td>3.0.0</td>
</tr>
<tr>
<td>DNS Enforce Plugin</td>
<td>1.1.6</td>
</tr>
<tr>
<td>External Classifier Plugin</td>
<td>2.2.2</td>
</tr>
<tr>
<td>Hardware Inventory Plugin</td>
<td>1.0.2</td>
</tr>
<tr>
<td>Hardware WatchDog Plugin</td>
<td>1.1.4</td>
</tr>
<tr>
<td>HPS Inspection Engine</td>
<td>10.7.2</td>
</tr>
<tr>
<td>Macintosh/Linux Property Scanner Plugin</td>
<td>7.0.2</td>
</tr>
<tr>
<td>Microsoft System Management Server (SMS) System Center Configuration Manager (SCCM) Plugin</td>
<td>2.2.5</td>
</tr>
<tr>
<td>NBT Scanner Plugin</td>
<td>3.0.4</td>
</tr>
<tr>
<td>OS X Plugin</td>
<td>2.0.2</td>
</tr>
<tr>
<td>Reports Plugin</td>
<td>4.2.0.1001</td>
</tr>
<tr>
<td>Switch Plugin</td>
<td>8.11.2</td>
</tr>
<tr>
<td>Component Name</td>
<td>Optimal Versions Compatible for V8.1.1 Upgrade</td>
</tr>
<tr>
<td>--------------------------------------------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>Syslog Plugin</td>
<td>3.2.0</td>
</tr>
<tr>
<td>Technical Support Plugin</td>
<td>1.1.2</td>
</tr>
<tr>
<td>User Directory Plugin</td>
<td>6.1.3</td>
</tr>
<tr>
<td>VMware vSphere Plugin</td>
<td>2.0.0</td>
</tr>
<tr>
<td>VPN Concentrator Plugin</td>
<td>4.0.8</td>
</tr>
<tr>
<td>Wireless Plugin</td>
<td>1.7.2</td>
</tr>
<tr>
<td>Cisco PIX/ASA Firewall Integration Plugin</td>
<td>2.0.2</td>
</tr>
<tr>
<td>Forescout Open Integration Module: Data Exchange Plugin</td>
<td>3.2.1</td>
</tr>
<tr>
<td>Forescout Extended Module for HPE ArcSight</td>
<td>2.7.1</td>
</tr>
<tr>
<td>MobileIron Plugin</td>
<td>1.7.1</td>
</tr>
<tr>
<td>Palo Alto Networks WildFire Plugin</td>
<td>2.0.0</td>
</tr>
<tr>
<td>Forescout Extended Module for Qualys VM</td>
<td>1.2.1</td>
</tr>
<tr>
<td>Forescout Extended Module for Splunk</td>
<td>2.7.0</td>
</tr>
<tr>
<td>Forescout Extended Module for Palo Alto Networks Next-Generation Firewall</td>
<td>1.1.1</td>
</tr>
<tr>
<td>Forescout Extended Module for Tenable Vulnerability Management</td>
<td>2.6.0</td>
</tr>
<tr>
<td>Forescout Extended Module for VMWare AirWatch MDM</td>
<td>1.7.2</td>
</tr>
<tr>
<td>Forescout Extended Module for Web API</td>
<td>1.2.2</td>
</tr>
<tr>
<td>Forescout Amazon Web Services (AWS) Plugin</td>
<td>1.1.1</td>
</tr>
<tr>
<td>IOC Scanner Plugin</td>
<td>2.1.0</td>
</tr>
<tr>
<td>FireEye NX Module</td>
<td>2.0.0</td>
</tr>
<tr>
<td>FireEye EX Plugin</td>
<td>1.1.0</td>
</tr>
<tr>
<td>FireEye HX Plugin</td>
<td>1.1.0</td>
</tr>
<tr>
<td>Forescout Extended Module for McAfee ePolicy Orchestrator</td>
<td>3.0.0</td>
</tr>
<tr>
<td>Forescout Extended Module for IBM QRadar</td>
<td>2.0.1</td>
</tr>
<tr>
<td>Forescout Extended Module for Rapid7 Nexpose</td>
<td>1.1.1</td>
</tr>
</tbody>
</table>
Components Not Supported for Version 8.1.1 (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
Not Supported for Version 8.1.1

Products that are not supported for Forescout 8.1.1 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 8.1.1, 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 8.1.1. These procedures are provided, due to Forescout version 8.1.1’s non-support of the Macintosh/Linux Property Scanner.

- Migrate Managed Linux and OS X Endpoints
- Disable SecureConnector Updates on Windows Endpoints

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 8.1.1.

Before upgrading to Forescout version 8.1.1, 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 8.1.1, 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.

1. 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 8.1.1 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:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Indicates the status of the High Availability Appliances connected to the Enterprise Manager.</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Indicates the status of the Enterprise Manager High Availability pair.</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Indicates that High Availability is down on the Appliance.</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Indicates that High Availability is down on the Enterprise Manager.</td>
</tr>
</tbody>
</table>
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.

   ![Upgrade Dialog]

   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:

![Icons](image)

<table>
<thead>
<tr>
<th>Icon</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Indicates the status of the High Availability Appliances connected to the Enterprise Manager.</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Indicates the status of the Enterprise Manager High Availability pair.</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Indicates that High Availability is down on the Appliance.</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Indicates that High Availability is down on the Enterprise Manager.</td>
</tr>
</tbody>
</table>

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 8.1.1 and Migrating to Flexx Licensing Mode

If you would like to upgrade your deployment to version 8.1.1 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 8.1.1.

> 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 8.1.1 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.


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-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

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:

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 Forescout Technologies, Inc. All rights reserved. Forescout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents can be found at https://www.forescout.com/company/legal/intellectual-property-patents-trademarks. Other brands, products, or service names may be trademarks or service marks of their respective owners.

2019-06-23 10:59