



# ForeScout CounterACT®

## Version 8.0.1

### Release Notes

---

September 2018

## About this Release

ForeScout CounterACT® version 8.0.1 delivers important fixed issues and feature enhancements.

The following information is available:

- [System Requirements](#)
- [Feature Enhancements](#)
- [CounterACT Fixed Issues](#)
- [CounterACT Known Issues](#)
- [Upgrading to Version 8.0.1](#)
- [Rollback Information](#)

## Finding More Documentation

See [Additional CounterACT Documentation](#) for information about accessing guides referenced in this document.

## System Requirements

This section describes system requirements for installing CounterACT version 8.0.1:

- [Supported Virtual Systems](#)
- [CounterACT Console Operating System Requirements](#)
- [CounterACT Device Requirements](#)
- [Licensing and Sizing Requirements](#)

### Clean Installation

Installation instructions and requirements for a clean installation of this release are provided in the *CounterACT Installation Guide* version 8.0.



# ForeScout CounterACT®

## Version 8.0.1

### Release Notes

---

## Supported Virtual Systems

This section describes supported virtual systems.

The required specifications for virtual environments listed in the Licensing and Sizing Guide have increased for CounterACT version 8.0 compared to version 7.0.0. ***It is required to increase virtual machine resources according to these specifications before upgrading to CounterACT version 8.0.1.*** See [Licensing and Sizing Requirements](#) for more information.

### VMware Versions

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

- VMware ESXi v6.5
- VMware ESXi v6.0
- VMware ESXi v5.5
- VMware ESXi v5.1

The guest OS is defined as *Other Linux-2.6 64bit kernel*.

### Hyper-V Versions

The CounterACT 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

There is no support for Hyper-V Generation 2 virtual machines.

## CounterACT Console Operating System Requirements

This section describes CounterACT Console operating system requirements.

The following operating systems are supported:

- Windows 7, Windows 10
- Windows Server 2008 R2 / 2012 / 2012 R2 / 2016
- CentOS 7



# ForeScout CounterACT®

## Version 8.0.1

### Release Notes


## CounterACT Device Requirements

This section describes CounterACT Appliance and Enterprise Manager requirements.

### Physical CounterACT Devices

CounterACT version 8.0.1 can be installed on all hardware revisions of CounterACT physical Appliances and Enterprise Managers **except for the following**:

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

 *CT-xxxx CounterACT devices based on hardware revision -10 or lower also do not support CounterACT version 8.0.*

**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.

## Licensing and Sizing Requirements

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 *CounterACT Installation Guide*, *Switch Plugin Configuration Guide* and *Wireless Plugin Configuration Guide* are now in this new guide.

## Feature Enhancements

### New *fstool* rollback Command

The *fstool* command for performing a version rollback allows rollback of this release to CounterACT 8.0 on multiple Appliances. The following command switches are available:

`rollback -l` – to list the available rollback versions

`rollback -q <version>` – to perform a quiet rollback with no prompts

#### To rollback multiple Appliances:

1. In the Enterprise Manager CLI, run the command: `fstool rollback -l`
2. Select a version to roll back to
3. Run the command: `fstool oneach -c "fstool rollback -q <version>"`

[Track to CA-19561]

## CounterACT Fixed Issues

This section describes fixed issues for this release.

Issue	Description
CA-8010	The Packet Engine error log reported illegal characters used by the Packet Engine. The errors did not affect engine functionality.
CA-14470	When defined to display hosts with unknown IP address (MAC only), CounterACT displayed devices with MAC addresses that had IP addresses that were not included in the internal network range of IP addresses.
CA-14740	Using a Run Script on Windows action in a policy resulted in scripts being deleted from the script folder, and caused Security Policy templates that rely on those scripts to stop working properly.
CA-14982	The Asset Inventory pane in the Console kept reloading when a Filter search was applied.
CA-15041	The filter icon was not clearly visible under some screen resolution settings in the Console Home tab History > NAC Policy pane.
CA-15489	Using the keyboard commands <i>Shift + down arrow</i> to select hosts in the All Hosts pane in the Console failed when trying to select a long list of hosts.
CA-15759	MAC address reporting was case sensitive, and as a result, the VMware plugin and the Switch plugin reported the same host as two different entities.
CA-15839	The results of the <i>Windows Expected Script Result</i> property sometimes contained a nonsensical character instead of a line break.
CA-16031	Following HTTP Login redirection, the Guest Registration portal was not accessible, and Guest login failed
CA-16538	Hosts were displayed as being online for hours after they went offline.
CA-16924	Updating the IP address range of a network segment caused CounterACT to perform a Virtual Firewall action although the action was disabled in the policy sub-rule.
CA-16926	When adding a user profile with a defined IP range in the Console, the user could not add a MAC address to the list of ranges using the "+" (plus) key.
CA-16968	Exporting host properties to a table for many hosts failed due to reaching the allowed timeout interval.
CA-17042	When a policy condition contained a complex list (i.e open port ) and match all was enabled, the condition returned a result of false although the entire list matched the condition.



# ForeScout CounterACT®

## Version 8.0.1

### Release Notes

Issue	Description
<b>CA-17058</b>	CounterACT components now run the latest version of Tomcat. This addresses multiple Tomcat-related issues that are identified in, but not limited to, the following CVEs: CVE-2017-15706, CVE-2016-6325, CVE-2016-5425, CVE-2016-5388, CVE-2016-3092, CVE-2016-1240, CVE-2016-0763, CVE-2016-0714, CVE-2016-0706, CVE-2015-5351, CVE-2015-5346, CVE-2015-5345, CVE-2015-5174, CVE-2017-12617, CVE-2017-12616, CVE-2017-12615, CVE-2017-7675, CVE-2017-7674, CVE-2017-6056, CVE-2017-5664, CVE-2017-5651, CVE-2017-5650, CVE-2017-5648, CVE-2017-5647, CVE-2016-9775, CVE-2016-9774, CVE-2016-8747, CVE-2016-8745, CVE-2016-8735, CVE-2016-6817, CVE-2016-6816, CVE-2016-6797, CVE-2016-6796, CVE-2016-6794, CVE-2016-5018, CVE-2016-0762
<b>CA-17134</b>	The Advanced Compliance (SCAP and ARF) report page failed to load in the Reports portal.
<b>CA-17254</b>	CounterACT web portals did not allow a user to log in using a password with non-ASCII characters.
<b>CA-17350</b>	Endpoints added to a group are displayed in the Group Manager, but the hosts do not show that they are registered in the group.
<b>CA-17357</b>	Following a service restart, users could not log in to the Console.
<b>CA-17371</b>	Configuration scripts did not synchronize between the Enterprise Manager and Recovery Manager following a failover operation.
<b>CA-17699</b>	The CounterACT Console restarted due to resource cleanup problems.
<b>CA-17792</b>	When an endpoint was added to a group manually, based on the MAC address, the endpoint listing was not saved when the group listings were updated.
<b>CA-17829</b> <b>CA-18453</b>	This fix addresses vulnerabilities in the <i>openssl</i> that are identified in, but not limited to, the following CVEs: CVE-2017-3736, CVE-2017-3737, CVE-2017-3738 and CVE-2018-0739
<b>CA-17830</b>	The Apache software was updated to address security issues that are identified in, but not limited to, the following CVEs: CVE-2017-15710, CVE-2017-15715, CVE-2018-1283, CVE-2018-1301, CVE-2018-1302, CVE-2018-1303 and CVE-2018-1312
<b>CA-17884</b>	An automatic email notification was sent to the administrator when bandwidth exceeded the licensed limit. The automatic email notices have now been removed.
<b>CA-18106</b>	Upgrading from CounterACT 7.0.0 Service Pack 3.0.2 to CounterACT 8.0 failed.
<b>CA-18204</b>	Following rollback from CounterACT 7.0.0 with Service Pack 3.0.2 to CounterACT 7.0.0 with Service Pack 3.0.1 and upgrade to CounterACT 8.0, users could not access the CounterACT web portals.



# ForeScout CounterACT®

## Version 8.0.1

### Release Notes

Issue	Description
<b>CA-18353</b> <b>CA-18346</b>	This fix addresses vulnerabilities in the <i>openssh</i> that are identified in, but not limited to, the following CVE: CVE-2017-15906
<b>CA-18347</b>	The CentOS software was updated to address security issues that are identified in, but not limited to, the following CVE: CVE-2017-3145
<b>CA-18349</b>	This fix addresses DHCP-related issues specified in CESA-2018:0158.
<b>CA-18350</b>	This fix addresses multiple <i>systemd</i> -related issues that are identified in, but not limited to, the following CVEs: CVE-2018-1049.
<b>CA-18448</b>	CounterACT upgrade processes were updated, and now remove unused legacy Java packages. This addresses security issues that are identified in, but not limited to, the following CVEs: CVE-2018-2783, CVE-2018-2790, CVE-2018-2794, CVE-2018-2795, CVE-2018-2796, CVE-2018-2797, CVE-2018-2798, CVE-2018-2799, CVE-2018-2800, CVE-2018-2811, CVE-2018-2814, CVE-2018-2815, CVE-2018-2825, CVE-2018-2826.
<b>CA-18449</b>	This fix addresses multiple Kerberos package-related issues that are identified in, but not limited to, the following CVEs: CVE-2017-11368 and CVE-2017-7562.
<b>CA-18450</b>	The CentOS software was updated to address security issues that are identified in, but not limited to, the following CVEs: CVE-2014-9402, CVE-2015-5180, CVE-2017-12132, CVE-2017-15670, CVE-2017-15804 and CVE-2018-1000001
<b>CA-18451</b>	This fix addresses multiple <i>ntp</i> -related issues that are identified in, but not limited to, the following CVEs: CVE-2017-6462, CVE-2017-6463, CVE-2017-6464
<b>CA-18452</b>	This fix addresses vulnerabilities in the <i>openssh</i> that are identified in, but not limited to, the following CVE: CVE-2017-15906
<b>CA-18473</b>	Under certain circumstances, when CounterACT was deployed on KVM virtual systems, the CounterACT Packet Engine restarted every 2 hours, causing a range of traffic monitoring functionality to temporarily stop.
<b>CA-18580</b>	Applying a Delete Property action in a policy resulted in endpoints that were offline reported as being online.
<b>CA-18901</b>	License Request and License Install interactions did not support non-English character sets. Support was added for Turkish characters.



# ForeScout CounterACT®

## Version 8.0.1

### Release Notes

Issue	Description
CA-19598	User could not log in to the Enterprise Manager console after the CounterACT service stopped.

## CounterACT Known Issues

This section describes known issues for this release.

Issue	Description
CA-6935	The online Help library is not accessible if the CounterACT Console is not connected to an Enterprise Manager.
CA-6974	In a CounterACT deployment using Failover Clustering, actions that are performed by an Appliance different 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-13858	If your deployment is using Centralized Licensing Mode, the license file is not saved during system backup. If you still have the license file, and are restoring the backup file on the same machine that the backup was taken from, you can update the existing license file and re-upload the file after the restore. Otherwise, you will need to deactivate the license file, reinstall the CounterACT ISO file, and then activate a new license file. Refer to the <i>CounterACT Installation Guide</i> for more information on installing the CounterACT ISO file. If you need additional assistance, contact your ForeScout representative.
CA-15143 CA-15372	Upgrading the CounterACT Console software is not currently supported for Linux or OS X operating systems.
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	If your deployment is using Centralized Licensing Mode, 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-19577	The Delete Host action does not propagate properly to all Appliances.



📖 *For a list of known limitations on IPv6 support, refer to the Work with IPv6 Addressable Endpoints How-to Guide.*

## Upgrading to Version 8.0.1

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.

## Upgrading from CounterACT 7.0.0

This section provides important information for users upgrading from CounterACT version 7.0.0 to CounterACT version 8.0.1.

- It is recommended to upgrade from 7.0.0 directly to version 8.0.1. Refer to the CounterACT 8.0. Release Notes for information on new and enhanced features and fixes for CounterACT version 8.0. See [Additional CounterACT Documentation](#) for information about accessing this document
- Upgrade is supported starting from CounterACT version 7.0.0 with Service Pack 3.0.1 or above installed.
- Upgrade is not supported in systems that were previously upgraded from CounterACT version 6 to CounterACT 7.0.0. In such a system, perform a system backup and re-image the device before performing a clean installation of CounterACT 8.0.1.
- To upgrade, plugins installed in your system must be compatible with CounterACT 8.0.1. You should upgrade or roll back the plugin versions in your system to make sure they are aligned with the versions specified in the list of [Components Compatible for Upgrading to Version 8.0.1.](#)
- **Rollback is not supported from CounterACT 8.0 or 8.01 to CounterACT 7.0.0.**
- 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.
- You cannot add an Appliance running CounterACT version 7.0.0 or below to an Enterprise Manager running CounterACT version 8.0 or above.
- After upgrading, existing Failover Clustering configurations are deleted.

- The **Detected** tab is removed from the Groups Manager following upgrade to version 8.0.1.

## Pre-Upgrade Procedures for CounterACT 7.0.0 with 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 CounterACT version 8. These procedures are provided because CounterACT 8.0.1 does not support 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 CounterACT version 8.

**Before upgrading to CounterACT version 8.0.1**, 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 CounterACT version 8.0.1**, 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
```

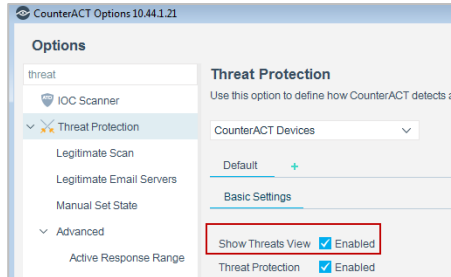
After upgrading your CounterACT deployment, automatic upgrade is disabled by default.

To display CounterACT endpoint detections for a specific group, in the Console **Home** tab, navigate to the **Filters** pane, open the **Groups** folder and select a *<group>*. The **All Hosts** pane displays the CounterACT-detected endpoints for the selected group.

- The Threat Protection view is disabled following upgrade to version 8.0.

#### To activate the Threat Protection view:

1. In the CounterACT Console, go to **Tools > Options > Threat Protection**.
2. Select **Show Threats View**.



## Upgrading from CounterACT 8.0

This section describes upgrade considerations for upgrading from CounterACT 8.0.0 to CounterACT 8.0.1.

### Extended Module Release Information

All Extended Modules are available with CounterACT 8.0.1 except for the following:

- Check Point Threat Prevention 1.1

## Components Compatible for Upgrading to Version 8.0.1

The following components are the versions that are compatible when upgrading to CounterACT version 8.0.1.

Component Name	Versions Compatible for Upgrade to V8.0.1
CounterACT 7.0.0 Service Pack	3.0.1 - 3.0.2.3
802.1X Plugin	4.2.0 - 4.2.2.1
Advanced Tools Plugin	2.2.3
AWS Plugin	1.1.1
CEF Plugin	2.6.1
Cisco PIX/ASA Firewall Integration Plugin	2.0.2
Data Exchange Plugin, ForeScout Open Integration Module: Data Exchange Plugin	3.2.1 - 3.2.1.1
DHCP Classifier Plugin	2.0.6 - 2.1.1
DNS Client Plugin	3.0.0 - 3.1.0



# ForeScout CounterACT®

## Version 8.0.1

### Release Notes

Component Name	Versions Compatible for Upgrade to V8.0.1
DNS Enforce Plugin	1.1.5 - 1.1.6
External Classifier Plugin	2.2.2
FireEye NX Module	2.0.0
FireEye EX Plugin	1.1.0
FireEye HX Plugin	1.1.0
ForeScout Extended Module for HPE ArcSight	2.7.1
ForeScout Extended Module for VMWare AirWatch MDM	1.7.2
Hardware Inventory Plugin	1.0.2 - 1.0.2.3
Hardware WatchDog Plugin	1.1.4
HPS Inspection Engine	10.7.1 – 10.8.0.1
IBM QRadar Plugin	2.0.1
IOC Scanner Plugin	2.1.0
Linux	1.1.0
Macintosh/Linux Property Scanner Plugin	7.0.1 - 7.0.2
Microsoft SMS/SCCM Plugin	2.2.5
NBT Scanner Plugin	3.0.4 - 3.0.4.1
OS X Plugin	2.0.0 - 2.0.2.1
Reports Plugin	4.2.0 – 4.2.1
Splunk Plugin	2.7.0
Switch Plugin	8.11.1 - 8.11.2
Syslog Plugin	3.2.0
Technical Support Plugin	1.1.2 - 1.2.0
Tenable VM Plugin	2.6.0 – 2.6.0.7
User Directory Plugin	6.1.2 - 6.1.3
VMware vSphere Plugin	2.0.0 - 2.1.0
VPN Concentrator Plugin	4.0.7 - 4.0.8.1
Wireless Plugin	1.7.0 - 1.7.2.1
MobileIron Plugin	1.7.1
Palo Alto Networks WildFire Plugin	2.0.0



# ForeScout CounterACT®

## Version 8.0.1

### Release Notes

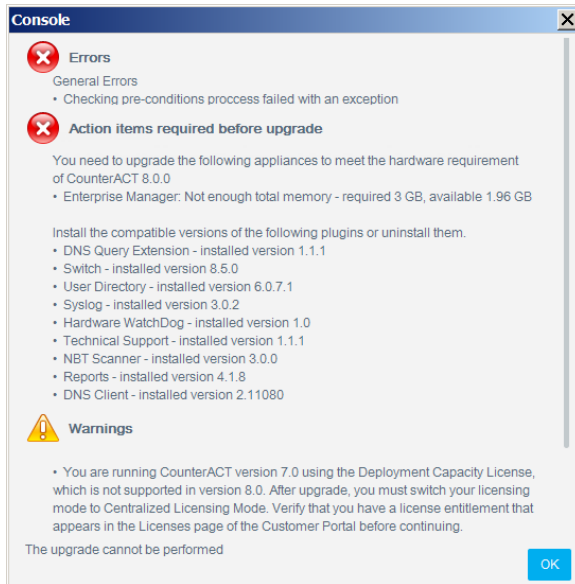
---

Component Name	Versions Compatible for Upgrade to V8.0.1
Qualys VM Plugin	1.2.1
Palo Alto Networks Next-Generation Firewall Extended Module	1.1.1
WebAPI Plugin	1.2.2
McAfee ePO Plugin, ForeScout Extended Module for McAfee ePO	3.0.0
Rapid7 Nexpose Plugin	1.1.1

## Components Not Supported for Version 8.0.1

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 extended module. The verification screen may ask you to upgrade or uninstall a plugin or extended module 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

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.

With this version, 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

## Performing the Upgrade


The Installer program automatically identifies an earlier CounterACT version on your system. Upgrade options allow you to either maintain the configuration parameters from the previous version or define new parameters.

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 *CounterACT Administration Guide*. See [Additional CounterACT 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, make sure the Secondary node is not accessible, and create the file `.ignorestandby` under `/etc/` on the node to be upgraded.

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

### To upgrade:





1. Before upgrading Appliances, you should upgrade your Enterprise Manager.
2. If you are upgrading and will continue to work in the Per-Appliance Licensing Mode, download the product upgrade file from the [Product Download page](#), and save it to a location on your computer.  
  
 *If you are upgrading and want to migrate to the Centralized Licensing Mode, see [Upgrading to Version 8.0.1 and Switching to Centralized Licensing Mode](#) for upgrade instructions.*
3. Select **Options** from the **Tools** menu.  
CounterACT devices or Appliances are shown with their current version.
4. Select an Enterprise Manager or 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. The file selection dialog box opens.
5. 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 CounterACT Upgrade screen opens.
6. Select the **I accept the Terms and Conditions** checkbox. It is recommended to read the Release Notes.
7. Select **Verify**. 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.



📄 *When upgrading an Appliance connected to an Enterprise Manager that was upgraded to the current CounterACT version, the pre-upgrade check is not performed, and the **Upgrade** button is immediately available in the CounterACT Upgrade screen.*

8. Select **Upgrade** when 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.
9. After the upgrade is complete, download the Console from the [Product Download page](#), 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 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.

10. 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.

## Upgrading to Version 8.0.1 and Switching to Centralized Licensing Mode

If you are running CounterACT version 7.0.0, you can upgrade your deployment to version 8.0.1 operating in Centralized Licensing Mode. All CounterACT releases prior to version 8.0 operate in Per-Appliance Licensing Mode. Refer to the *CounterACT Administration Guide* for more information about licensing.

**Contact ForeScout Support or your ForeScout representative for more information on how to switch licensing modes.**

- 📄 *In version 8.0, a **Migrate** button in the Console (Options > Licenses) facilitated the switch to Centralized Licensing Mode. This button was removed in version 8.0.1.*



# ForeScout CounterACT®

## Version 8.0.1

### Release Notes

---

Before switching modes, verify that you have:

- Valid credentials to access the [ForeScout Customer Portal](#). Contact your ForeScout representative for more information.
- A valid license entitlement for CounterACT version 8.0, operating in Centralized Licensing Mode.

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

## Rollback Information

Rollback is available for this release through a CLI command – see [New fstool rollback Command](#).

## Additional CounterACT Documentation

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

- [Documentation Downloads](#)
- [Documentation Portal](#)
- [CounterACT Help Tools](#)

### Documentation Downloads

Documentation downloads can be accessed from one of two ForeScout portals, depending on which licensing mode your deployment is using.

- **Per-Appliance Licensing Mode** - [Product Updates Portal](#)
- **Centralized Licensing Mode** - [Customer Portal](#)

 *Software downloads are also available from these portals.*

To learn which licensing mode your deployment is using, see [Identifying Your Licensing Mode in the Console](#).

### Product Updates Portal

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

#### To access the Product Updates Portal:

1. Go to <https://updates.forescout.com/support/index.php?url=counteract>.
2. Select the CounterACT version you want to discover.

### Customer Portal

The Downloads page on the ForeScout Customer Portal provides links to purchased CounterACT version releases, Base and Content Modules, and Extended Modules, 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. The Documentation page on the portal provides a variety of additional documentation.

#### To access documentation on the ForeScout Customer Portal:

3. Go to <https://forescout.force.com/support/>.
4. Select **Downloads** or **Documentation**.

## Documentation Portal

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

- 📄 *If your deployment is using Centralized Licensing Mode, you may not have credentials to access this portal.*

### To access the Documentation Portal:

5. Go to [https://updates.forescout.com/support/files/counteract/docs\\_portal/](https://updates.forescout.com/support/files/counteract/docs_portal/).
6. Use your customer support credentials to log in.
7. Select the CounterACT version you want to discover.

## CounterACT Help Tools

Access information directly from the CounterACT Console.

### **Console Help Buttons**

Use context sensitive *Help* buttons to quickly access information about the tasks and topics you are working with.

### **CounterACT Administration Guide**

Select **CounterACT Help** from the **Help** menu.

### **Plugin Help Files**

8. After the plugin is installed, select **Options** from the **Tools** menu and then select **Modules**.
9. Select the plugin and then select **Help**.

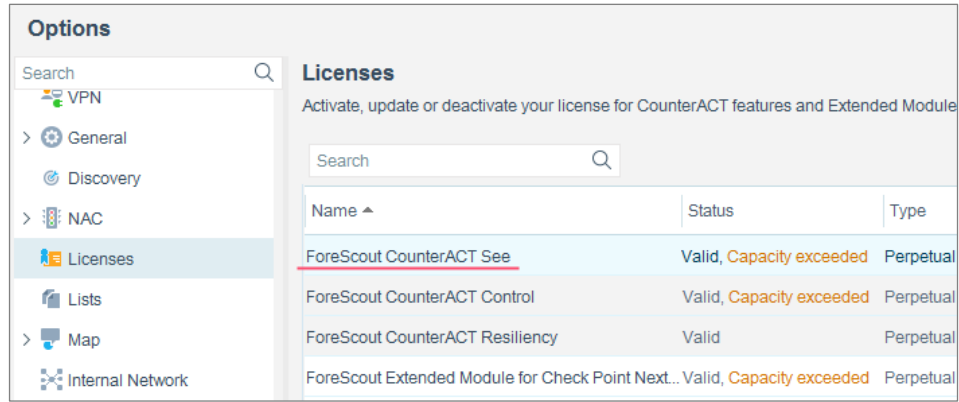
### **Documentation Portal**

Select **Documentation Portal** from the **Help** menu.

### *Identifying Your Licensing Mode in the Console*

If your Enterprise Manager has a *ForeScout CounterACT See* license listed in the Console, your deployment is operating in Centralized Licensing Mode. If not, your deployment is operating in Per-Appliance Licensing Mode.

Select **Options > Licenses** to see whether you have a *ForeScout CounterACT See* license listed in the table.



**Options**

Search

- VPN
- General
- Discovery
- NAC
- Licenses**
- Lists
- Map
- Internal Network

**Licenses**

Activate, update or deactivate your license for CounterACT features and Extended Module

Search

Name ▲	Status	Type
ForeScout CounterACT See	Valid, Capacity exceeded	Perpetual
ForeScout CounterACT Control	Valid, Capacity exceeded	Perpetual
ForeScout CounterACT Resiliency	Valid	Perpetual
ForeScout Extended Module for Check Point Next...	Valid, Capacity exceeded	Perpetual

Contact your ForeScout representative if you have any questions about identifying your licensing mode.



# ForeScout CounterACT<sup>®</sup>

## Version 8.0.1

### Release Notes

---

## Legal Notice

© 2018 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.

2018-09-27 13:34