ForeScout CounterACT®
Version 8.0
Release Notes

May 2018

About this Release

ForeScout CounterACT® version 8.0 delivers new capabilities that significantly enhance deployment, authentication, visibility, detection, classification, control and security.

The following information is also available:

Finding More Documentation

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

System Requirement Updates

This section describes system requirement updates for users upgrading to CounterACT version 8.0, including:

Clean Installations

Installation instructions and requirements for clean installations are provided in the *CounterACT Installation Guide* version 8.0.

Virtual System Updates

This section describes CounterACT version 8.0 virtual system updates.

VMware Versions

Added support for:

- VMware ESXi v6.5

Removed Support:

- VMware ESX and ESXi v4.1 updates 1 through 3
- VMware ESX and ESXi v4.0 updates 1 through 4
- VMware ESX and ESXi v3.5 update 5

Hyper-V Versions

Added support for:

- Hyper-V Server 2016

CounterACT Console Operating System Requirement Updates

This section describes the following Console Hardware Requirement Updates.

- Support for Windows XP/Vista has been removed

- Support has been added for:
  - Windows Server 2008 R2 / 2012 / 2012 R2 / 2016
  - CentOS 7

CounterACT Device Requirements

This section describes CounterACT Appliance and Enterprise Manager requirements.

For information on newly supported physical ForeScout Appliances and virtual ForeScout Appliance configurations, see New ForeScout 5100-Series Physical Appliances and Virtual Configurations.

Physical CounterACT Devices

CounterACT version 8.0 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 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.

Core Platform Enhancements

New ForeScout 5100-Series Physical Appliances and Virtual Configurations

A new ForeScout 5100-series of physical Appliances and virtual ForeScout Appliance configurations support the increased flexibility and scalability provided by the Centralized Licensing paradigm.

This series offers increased performance capacity, allowing handling of up to 20,000 endpoints by a single device and up to two million endpoints across a deployment managed by a single Enterprise Manager (running on a 5160 device).

In addition, the new 51xx physical devices use only one rack unit (1U), minimizing vertical rack size.

New 51xx Physical ForeScout Appliances

- 5110
- 5120
- 5140
- 5160

New Virtual ForeScout Appliances

- X-Small
- Small
- Medium
- Large

Refer to the ForeScout Licensing and Sizing Guide for requirements/specifications related to deployment sizing for physical and virtual Appliances. 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.

Centralized Licensing

This version introduces a new, centralized licensing paradigm that provides a simple and flexible way to purchase, deploy and manage ForeScout software and hardware across heterogeneous environments.

Key benefits of the centralized licensing paradigm include:

- ***Flexible Software Consumption Model***
  - Decouple software licenses from hardware Appliances.
  - Maintain a shared license pool across a deployment, centrally managed by an Enterprise Manager.
  - Purchase hardware as needed, without finalizing all aspects of your deployment architecture before purchasing software licenses.
- ***Ability to Evolve Deployment with Changing Needs***
  - Move, add and make changes to Appliances within a deployment without making license changes.

  - Adopt use cases that require different Appliance configurations with greater ease.

- ***Streamlining of License Management***
  - Easily manage your entitlements, licenses and downloads from a unified portal.
  - Get aggregated view of license consumption to facilitate license auditing, compliance.

New ForeScout 5100-Series Physical Appliances and Virtual Configurations support the flexibility and scalability provided by this paradigm.

Licensing Modes in CounterACT

This version of CounterACT supports both the *Centralized Licensing Mode* and the *Per-Appliance Licensing Mode*.

Each CounterACT deployment operates in one of the two modes. You may have multiple deployments that use different licensing modes. License requirements differ according to the licensing mode activated on your deployment.

The following table describes each mode and lists the components/features that need to be licensed.

Licensing Mode	Description	What needs to be licensed?
Centralized Licensing Mode	▪ Licenses are activated centrally on the Enterprise Manager or Standalone Appliance. ▪ License endpoint capacity is calculated per-*deployment*; you can distribute this capacity across Appliances as you see fit. ▪ Extended Modules are acquired separately and with an associated endpoint count. *Prior to the release of CounterACT 7.0.0 Service Pack 2.3.0, groups of related licensed modules were packaged into Integration Modules. These are not supported in Centralized Licensing Mode.*	▪ Each licensed feature and Extended Module per deployment. Licensed features enable specific capabilities in CounterACT (See and Control, Resiliency, Extended Modules). See Licensed Features.
Per-Appliance Licensing Mode	▪ Licenses are activated separately on the Enterprise Manager and on each Appliance in the deployment. ▪ License endpoint capacity is calculated per-*Appliance*; each Appliance license includes a specific number of endpoints that the Appliance can handle. ▪ Extended Modules are acquired separately and with an associated endpoint count.	▪ Each Appliance and Enterprise Manager in your deployment. ▪ Each Extended Module. Refer to the section on the Per-Appliance Licensing Mode in the *ForeScout CounterACT Administration Guide* for more information.

Default Licensing Modes

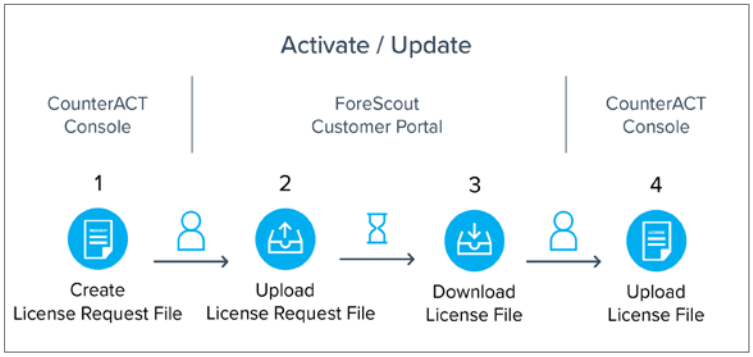
The following table describes the default licensing modes in use, based on the version of CounterACT that you are using.

CounterACT Version	Licensing Mode	Notes
All releases prior to version 8.0	Per-Appliance Licensing Mode	If you upgrade to CounterACT version 8.0, you can choose to migrate to the Centralized Licensing Mode. Refer to Upgrading to Version 8.0 and Migrating to Centralized Licensing Mode or the upgrade/migration procedure documented in the *CounterACT Installation Guide*.
CounterACT version 8.0 (*Upgrade from previous version*)	Per-Appliance Licensing Mode	All license information is retained after upgrade. You can migrate to the Centralized Licensing Mode. Refer to the chapter on License Management in the *ForeScout CounterACT Administration Guide* for more information.
CounterACT version 8.0 (*New installation*)	Licensing mode is determined during purchase.	You are asked to identify the predetermined licensing mode during initial installation and configuration of your CounterACT device. Refer to the *CounterACT Installation Guide* for information about CounterACT device installation and configuration.

About Centralized Licensing

If you are operating in Centralized Licensing Mode, you must activate a new license file containing valid licenses for each feature you want to work with in your CounterACT deployment. Licensed features include *See*/*Control*- and *Resiliency*-related features, as well as Extended Modules. Contact your ForeScout representative to request licenses.

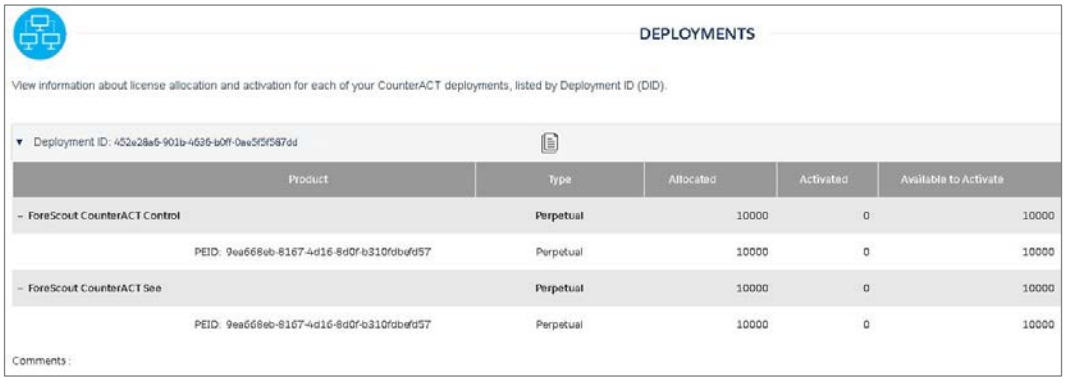
License management is performed in stages using two different tools (Console/ ForeScout Customer Portal):



1. *CounterACT administrator* creates and saves a license request file in the Console using the Deployment ID listed in the *Proof of Entitlement* email sent from ForeScout notifying that purchases are available in the Customer Portal.
2. *Entitlement administrator* uploads the license request file in the Customer Portal.
3. *Entitlement administrator* downloads the license file in the Customer Portal.
4. *CounterACT administrator* uploads the license file in the Console to activate or update licenses.

Managing License Entitlements in the ForeScout Customer Portal

Each customer is assigned at least one *Entitlement administrator* who has permissions to download license files, software and documentation in the Customer Portal for all customer deployments. The *Entitlement administrator* is notified by email when a purchase entitlement is created. Once created, the administrator can view the entitlement in the Customer Portal.



Licensed Features

Licensed features enable specific CounterACT features and capabilities. Each licensed feature supports a defined number of endpoints that the license can handle. The

basic feature license is the ForeScout CounterACT See and Control License which must be installed on each deployment. In addition to this license, you can purchase a ForeScout CounterACT Resiliency License and ForeScout Extended Module Licenses to extend CounterACT functionality to other areas.

Each licensed feature has an associated capacity, indicating the number of endpoints the license can handle.

Refer to the *ForeScout CounterACT Administration Guide* for more information about CounterACT features supported by these licenses.

- ***ForeScout CounterACT See and Control License***
  - This license provides the following:

    > In-depth visibility using a combination of active and passive monitoring techniques to discover endpoints when they enter the network.

    > Allow, deny or limit network access based on device posture and security policies.
- ***ForeScout CounterACT Resiliency License***
  - This license provides access to ForeScout resiliency solutions that support the availability of CounterACT services to minimize down-time in cases of system failure. The capacity of the license should include the total number of unique endpoints that are handled by either Failover Clusters or High Availability pairs. An endpoint handled by both of the above-mentioned resiliency solutions is counted as a single endpoint for licensing purposes.

    Refer to the *CounterACT Resiliency Solutions Guide* for more information about the features provided by the *Resiliency* license.
- ***ForeScout Extended Module Licenses***
  - Extended Module licenses provide access to Extended Modules. The capacity of each Extended Module license varies by module, but cannot exceed the capacity of the *ForeScout CounterACT See and Control* licenses. See Extended Module Release Information for details about the availability of Extended Modules for version 8.0.

10Gbps Traffic Inspection

This release introduces an infrastructure change to enable up to 10Gbps traffic inspection on ForeScout 5160 Appliances. 10Gbps support includes the following features:

- Higher performance for passive discovery and classification.
- More reliable network traffic-based controls (Virtual Firewall, HTTP actions, etc.).

High Availability Improvements

This release improves the existing High Availability Pairing solution with enhanced usability and stability. For example,

- The High Availability setup reconfiguration process now takes up to minute. Previously the process took approximately between 30 to 60 minutes.
- The High Availability configuration display for other HA node is improved. Now you can see what High Availability configuration you retrieved from Active Node, and what will be applied.
- Users are warned if a configuration cannot be retrieved. Failures messages are also now displayed explained.
- A bond interface was added to simplify dual sync handling and processing.
- The High Availability setup now validates High Availability configuration before applying so users can reconfigure if required. Previously the installation did not alert in a timely manner.

Refer to the *CounterACT Resiliency Solutions Guide* for more information about High Availability.

Installation and Upgrade Improvements

Release and Packaging Transformation

CounterACT version 8.0 transforms the way ForeScout delivers core and base software packages.

These changes reduce the highly fragmented software delivery and thus simplify software adoption. Users also retain the ability to install modules without the need to fully upgrade CounterACT, which helps in reduce the upgrade risk in complex deployments.

- Software Updates

CounterACT Software Releases Package

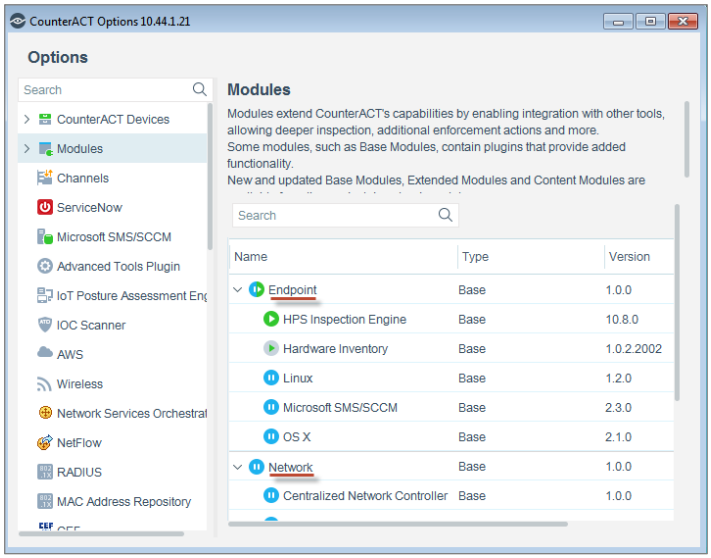
CounterACT core content is delivered with the:

- ISO image
- Virtual images (for example, OVF)
- Upgrade file (.fsp)
- Console installation files
- Service Packs, CounterACT Operating System Update Pack and CounterACT Infrastructure Update Pack and the Hardware Watchdog Plugin have been discontinued as standalone components, and are now an integral part of the CounterACT software.

Plugin Consolidation into Modules

Base Modules enhance CounterACT visibility, network connectivity, detection and control capabilities. Each module consolidates several base plugins into a logical package.

Content is delivered through Content Modules.



Base Modules

Base modules are delivered with major CounterACT releases, and also have their own release life cycle.

Base Modules	Plugins/Components
Authentication	▪ RADIUS ▪ User Directory
Core Extensions	▪ Advanced Tools ▪ CEF ▪ Device Classification Engine ▪ DHCP Classifier ▪ DNS Client ▪ DNS Enforce ▪ DNS Query Extension ▪ External Classifier ▪ Flow Analyzer ▪ IOC Scanner ▪ IoT Posture Assessment Engine ▪ NBT Scanner ▪ Reports ▪ Syslog ▪ Technical Support ▪ NetFlow ▪ Web GUI (Dashboard)
Endpoint	▪ HPS Inspection Engine ▪ Hardware Inventory ▪ Linux ▪ Microsoft SMS/SCCM ▪ OS X
Hybrid Cloud	▪ AWS ▪ VMware NSX ▪ VMware vSphere
Network	▪ Centralized Network Controller ▪ Switch ▪ VPN Concentrator ▪ Wireless

Refer to the related base module Release Notes for information on updates to these components for version 8.0.

Content Modules

Content Modules deliver data that is used by other Modules for classification, inspection and control. For example the Windows Applications Module delivers host properties and actions used by the HPS Inspection Engine to support in-depth discovery and management of software and applications on Windows endpoints.

Content Modules include:

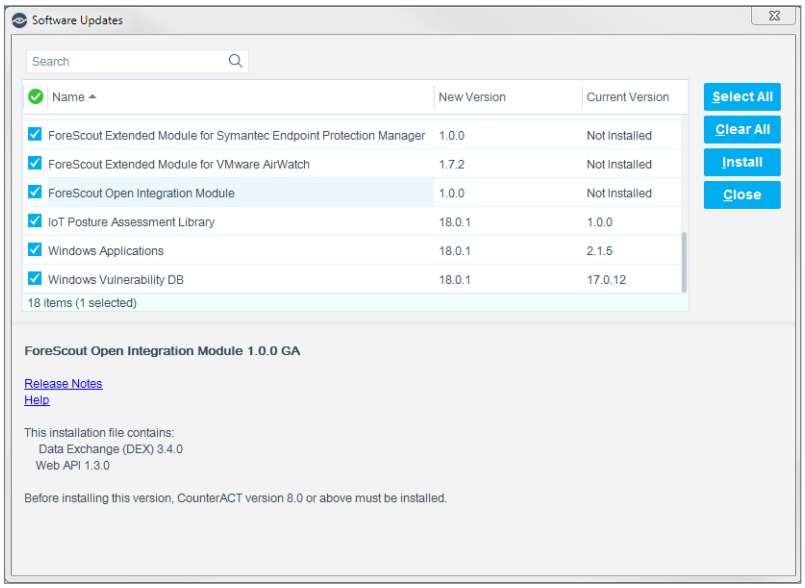
- Device Profile Library
- IoT Posture Assessment Library
- NIC Vendor DB
- Security Policy Templates
- Windows Applications
- Windows Vulnerability DB

Refer to the related content module Release Notes for information on updates to these components for version 8.0.

Software Updates

The Check for Updates feature has been enhanced and now includes:

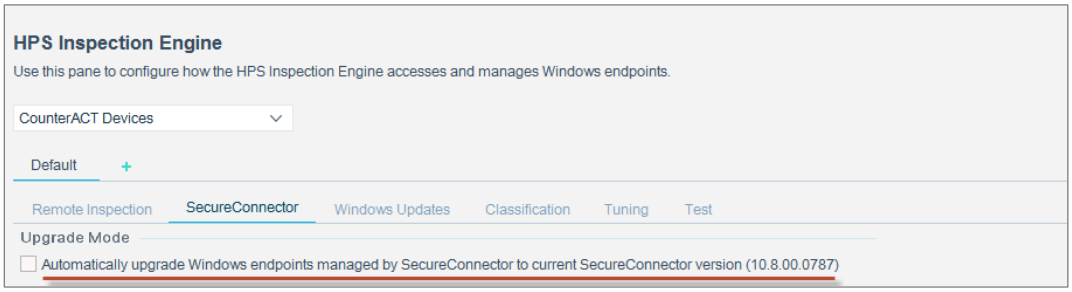
- Notification of available CounterACT core software upgrades (installation is via the Upgrade utility in the CounterACT Devices pane)
- Multiple version / pin-point version selection (available for deployments operating in Central Licensing Mode)
- Displays details about the released software package:
  - Release status
  - List of components included in the package
  - Dependencies



Automatic SecureConnector™ Gradual Upgrade

Previously, when you upgraded the HPS Inspection Engine, CounterACT automatically downloaded the new version of SecureConnector to Windows endpoints that are running SecureConnector. In networks with large numbers of endpoints managed by SecureConnector, this behavior can cause a spike in network resource usage.

In this release, SecureConnector is not automatically distributed to Windows endpoints when you upgrade the Endpoint Module. This enhancement provides uniform behavior for SecureConnector rollout on Windows, Linux and OS X endpoints.



Refer to the *CounterACT Endpoint Module Release Notes* for more information.

New Options for Initial CounterACT Installation

For CounterACT devices of type CT-xxxx, two CounterACT versions are available to the user at the beginning of the installation process:

- You can install CounterACT 7.0.0 without having to download or obtain the installation file.
- You can configure CounterACT 8.0.0 without any additional installation time required.

When you initialize a new CT-xxxx CounterACT device, you will see either CounterACT 7.0.0 or CounterACT 8.0.0 listed as the version at the top of the configuration or installation menu.

```
CounterACT 8.0.0-<build> options:


1) Configure CounterACT
2) Restore saved CounterACT configuration
3) Identify and renumber network interfaces
4) Configure keyboard layout
5) Turn machine off
6) Reboot the machine
```

```
Choice (1-6) :1
```

- If you see CounterACT 7.0.0, you can either upgrade to or perform a fresh installation of version 8.0.0. After upgrade or installation to version 8.0.0, you will see the menu listed above.
- If you see CounterACT 8.0.0, the menu offers an option to install CounterACT 7.0.0 or CounterACT 8.0.0, as shown below. If you select CounterACT 7.0.0, you will not be able to reinstall CounterACT 8.0.0 through the Configuration menu. See the *CounterACT Installation Guide version 7.0.0* for details on configuring CounterACT 7.0.0.

```
CounterACT 8.0.0-<build> options:


1) Install CounterACT 7.0.0-<build>
2) Configure CounterACT 8.0.0-<build>
3) Restore saved CounterACT configuration
4) Identify and renumber network interfaces
5) Configure keyboard layout
6) Turn machine off
7) Reboot the machine

Choice (1-7) :
```

CounterACT Deployment on KVM

This release supports the deployment of CounterACT on KVM virtual machines. It is recommended to work with the Linux RHEL/Centos 7 operating system. See CounterACT Known Issues for a known issue related to KVM virtual machines.

Refer to *CounterACT Virtual Systems* in the *CounterACT Installation Guide* for more information

Enhanced Mapping of CounterACT Appliances to the Network Environment

This release enhances the tools you use to map your network to CounterACT Appliances. Now it is easier to:

- Use Auto IP-Allocation to efficiently let groups of CounterACT Appliances support segments of the network.
- Support CounterACT in large, dispersed networks
- Work with the large address space in IPv6 addressable environments

The new IP Assignment and Failover pane replaces the IP Assignment pane. It provides enhanced tools that let you:

- Organize Appliances using a hierarchical tree of folders.
- Assign Internal Network segments to individual Appliances.
- Easily configure *Auto IP-Allocation* by assigning Internal Network segments to a folder containing Appliances.
- Configure a folder as a failover cluster. Refer to the *ForeScout CounterACT Resiliency Solutions Guide* for details about Failover Clustering.
- Identify gaps and changes in network coverage. If CounterACT detects an endpoint that is within the Internal Network, but not assigned to an Appliance, it generates an Event Log entry that can be used to alert administrators.

When you upgrade to this release, note that:

- Some tools in this screen originally appeared in the CounterACT Devices pane. Appliance management and IP assignment functions are now clearly separated between the two panes.
- When you upgrade to this release, the existing tree of Appliance Folders is preserved. However, failover cluster configuration is not preserved.
- To consistently work with large networks and/or dual-stack environments, only Internal Network segments (and not ad-hoc ranges) are used to assign IP addresses to Appliances and folders in the tree. When you upgrade to this release, existing IP assignments that use ranges are preserved.

Refer to *Working with Appliance Folders* in the *CounterACT Administration Guide* for details of updated functionality for more information.

Note on Conflicting Configuration Settings

When you configure CounterACT modules and other components, you can define groups of Appliances that have the same configuration settings, as described in Configuring Features for an Appliance or Group of Appliances in the *CounterACT Administration Guide.*

In some cases, these configuration settings may conflict with your definitions in the Appliance Folders tree. For example, endpoint connection settings of the Endpoint Module may conflict with endpoint connection settings of the Appliance Folders tree. A popup message notifies you of any conflicts when you save your Appliance Folders configuration. Review the two configurations applied to the Appliance to identify and resolve the conflict.

Efficient Endpoint Support with Auto IP-Allocation

In previous releases, you used Appliance folders to group CounterACT Appliances in a tree that reflected your network structure. However, each Appliance was statically assigned to a specific subnet or segment of your network, and only handled endpoints in that subnet.

In this release, each Appliance folder can function as an *Auto IP-Allocation* cluster - a group of Appliances that handle the Internal Network segments assigned to the folder, as follows:

1. Define a folder, and move Appliances into the folder.
2. Assign Internal Network segments *to the folder* (not to an Appliance).
3. Interactions with endpoints in these segments are dynamically distributed among the Appliances of the folder, in proportion to each Appliance's licensed capacity.

   If you add or remove IP addresses or Appliances to/from the folder, allocation is dynamically optimized among the Appliances.

Auto IP-Allocation significantly increases the efficiency and resiliency of your CounterACT deployment.

To dedicate a CounterACT Appliance to a specific network segment, you can configure a *static assignment* between an Appliance and an Internal Network segment, as in previous releases. This Appliance does not participate in Auto IP-Allocation within its folder. For each folder, the IP Assignment and Failover pane indicates which IP addresses are supported by Auto IP-Allocation and which are statically assigned to Appliances.

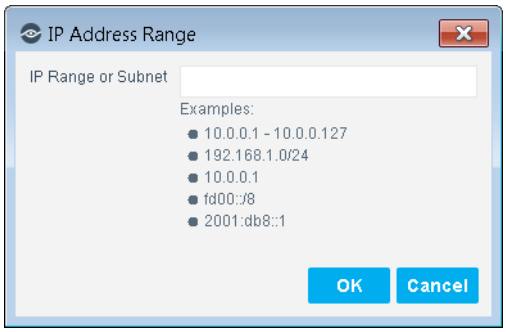
Enhanced Specification of IP Subnets and Internal Network Segments

Until now, CounterACT used the words *range* and *segment* loosely to describe both segments of the user's network environment, and the Internal Network segments you define in CounterACT for management purposes using Segment Manager. This sometimes led to confusion when working with the IP Allocation, Segment Manager and related features.

In addition, new conventions have emerged to specify segments of the large address space in IPv6 environments.

The following changes are introduced to avoid confusion in large networks and/or dual-stack environments:

- Field labels and descriptions have been generalized to include both IPv4 and IPv6 addresses. The term *IP addresses* is used when any IPv4/IPv6 address or subnet can be specified.
- The term *Internal Network segment* replaces the term *segment* and refers to segments defined in CounterACT using Segment Manager.
- For clarity, the term *subnet* is used in addition to the term *range*, and instead of the term *segment* in some fields that accept both IP ranges and subnets.
- CIDR notation can be used in fields to specify IPv4 and IPv6 subnets.



As of this release, language changes have not been implemented in all Console windows, or in all CounterACT documentation. Ongoing updates will be made in upcoming releases.

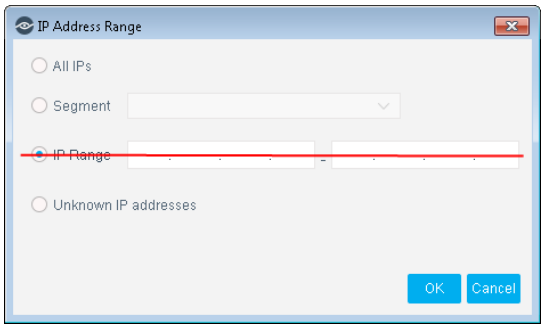
In some interactions, you can no longer directly specify IP address ranges. Define and use Internal Network segments to specify groups of IP addresses. For example:

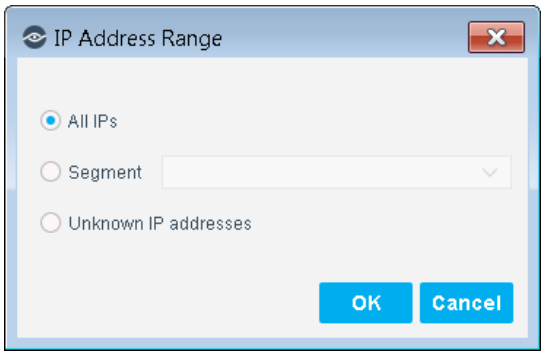
- In the Internal Network pane, you can only add or remove Internal Network segments that you defined in Segment Manager.

  Existing IP address ranges in the Internal Network are preserved during upgrade.

  You can directly specify IP ranges when you first define the Internal Network with the Initial Setup wizard.

- In policy wizards and some other areas, the IP Range option has been removed. Select an existing Internal Network segment or define a new Internal Network segment in Segment Manager.





Discovery Enhancements

The following discovery enhancements were made:

- Discovery of Endpoints Connected to the Cisco Meraki Cloud
- Enhanced IPv6 Support

Discovery of Endpoints Connected to the Cisco Meraki Cloud Networking Solution

The Centralized Network Controller Plugin lets you monitor Cisco Meraki, cloud-managed networks. The integration enables real time discovery of endpoints connected to Meraki Switches (MS) and Wireless Access Points (MR).

Once discovered, endpoints go through CounterACT classification and assessment processes.

Refer to the *Network Module Release Notes* for more information.

Enhanced IPv6 Support

CounterACT 8.0 introduces enhanced support for dual-stack network environments. It removes limitations in IPv6 support that were present in earlier releases.

Currently, the core CounterACT product and the following components fully support IPv6 addressable endpoints:

- The following Endpoint Module components:
  - HPS Inspection Engine
    *SecureConnector for HPS Inspection Engine is **not** supported.*
  - Linux Plugin
  - OS X Plugin
- The following Network Module components:
  - Switch Plugin
  - Wireless Plugin

  For vendor-specific details of IPv6 support see the *Network Module Release Notes* and related Plugin Configuration Guides.
- Authentication Module - all components
- The following Core Extensions Module components:
  - DNS Client Plugin
  - Reports Plugin
  - Device Classification Engine
  - External Classifier
  - Syslog Plugin
- Related databases and profile libraries, including:
  - Device Profile Library
  - NIC Vendor DB
  - Security Policy Templates
  - Windows Applications
  - Windows Vulnerability DB

Subsequent CounterACT 8.x releases may include IPv6 support for additional CounterACT components. Currently, IPv6 support has not been implemented or verified for such components. Typically the properties, actions, and policy templates provided by these components currently ignore or do not detect IPv6-only endpoints.

Refer to the *Work with IPv6 Addressable Endpoints How-to Guide* for more information. This guide also contains a list of known limitations on IPv6 support.

Working with Groups Manager

Use the Groups Manager to edit group structure and to view and edit static content.

- Use the Groups Manager to *permanently* assign IP or MAC addresses to groups.
- Use the *Add to Group* action in a policy to *conditionally* place endpoints in groups.

When you use Groups Manager, you can use the IPv4 address, the IPv6 address, or the MAC address as the key value for a group. Endpoints are added to the group based on their IPv4 or IPv6 addresses. However, when you use the *Add to Group* action to add an endpoint to a group, only the IPv4 and the MAC addresses of the endpoint can be used as a key value.

Network Connectivity, Visibility and Control Enhancements

Version 8.0 enhances network connectivity, visibility and control with the following:

- Wireless Plugin Support for Ruckus ZoneDirector
- Wireless Policy Template for Classifying KRACK Vulnerability
- Added Detection of Vendors' Lightweight Wireless Access Points
- Switch Policy Template Detects and Ignores Switch Virtual Interfaces

Wireless Plugin Support for Ruckus ZoneDirector

Plugin management of Ruckus **ZoneDirector** WLAN Controller has been added. This and allows discovery wireless clients (endpoints) connected through Ruckus WLAN network infrastructure and the ability to restrict their network access as needed.

Wireless Policy Template for Classifying KRACK Vulnerability

The new *VR WPA2 KRACK* policy template provided Security Policy Template version 18.0.2 or above:

- Classifies the following according to their KRACK vulnerability:
  - Aruba and Cisco WLAN devices
  - Aruba and Cisco Lightweight APs
  - Wireless clients (endpoints) connected to any of the above and running one of the following operating systems:
    - ✓ Windows (both HPS-managed and unmanaged endpoints)
    - ✓ Android

- ✓ Linux
- ✓ iOS
- ✓ Macintosh

- Evaluates the new **WLAN Device Software** property, which identifies the software release that is running on the lightweight AP to which the wireless client is connected.

Added Detection of Vendors' Lightweight Wireless Access Points

For the following WLAN device vendors, added Wireless Plugin detection and reporting of information about the lightweight access points (AP) being managed by a plugin-managed WLAN controller:

- Aruba
- Ruckus

Switch Policy Template Detects and Ignores Switch Virtual Interfaces

The new *Ignore Switch Virtual Interfaces* policy template creates a policy that identifies Switch Virtual Interfaces (SVIs) and adds matched SVIs to CounterACT's **Ignored IPs** group. SVIs that are not assigned to the **Ignored IPs** group are included in the CounterACT endpoint licensing capacity count.

Refer to the *Network Module Release Notes* for more information about features described in this section.

Out-of-the-Box Device Classification Enhancements

This release builds on the classification paradigm introduced in CounterACT version 7.0 Service Pack 3.0.0, and now provides:

- The ability to preview the impact to classification in your environment before you apply newly available classification profile updates.
- Additional updates and improvements to the classification profile library, increasing accuracy, precision and breadth.

Refer to the *Device Profile Library Release Notes* for more information.

New Assessment of IoT Devices for Weak Credentials

This release provides increased device security by providing a CounterACT policy template for detecting connected IoT devices that use weak credentials, such as commonly used or manufacturer default credentials.

Refer to the *Core Extensions Module Release Notes* for more information.

New Customizable Dashboard

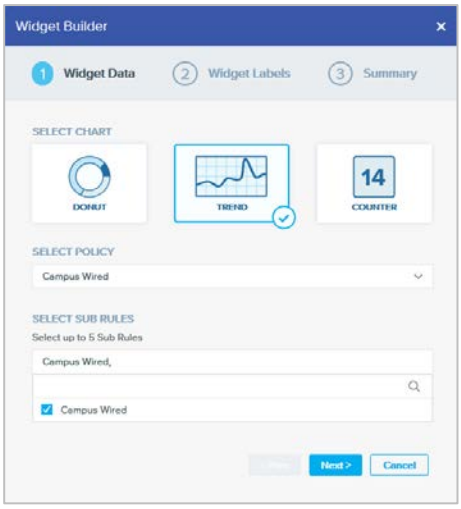
This release introduces a new web-based dashboard. The dashboard is designed for corporate executives who want a quick overview of important network activities, and for security administrators that would like to easily monitor their security state. This information is collected from CounterACT policies and is periodically updated as endpoints are monitored and controlled by CounterACT.

Use the dashboard to gain dynamic at-a-glance visibility into endpoints on the network including:

- Device compliance
- Device classification
- Device management status

The new dashboard design offers:

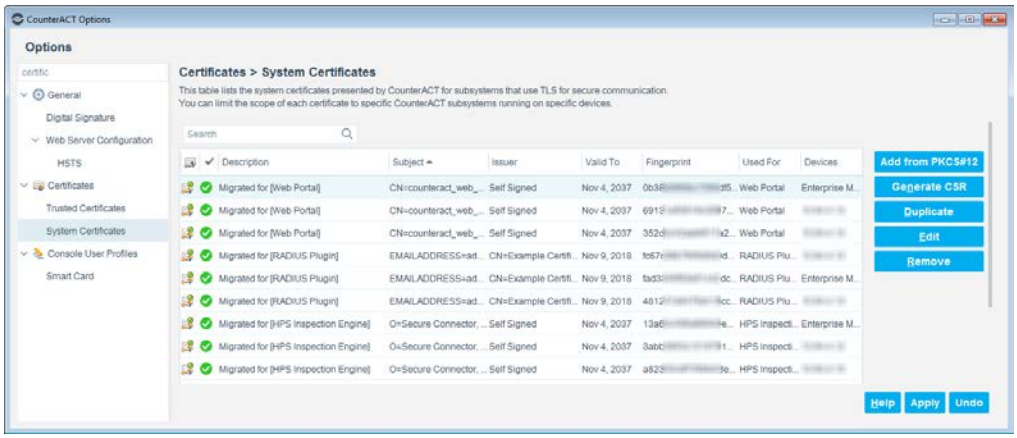
- Modern look-and-feel and user experience.
- Drill down from high-level findings to see information about specific endpoints.
- Customize the dashboard to show policy information using the Widget Builder.



Refer to the chapter on the Dashboard in the *CounterACT Administration Guide* for more information

New Certificate Management User Interface

A new certificates interface allows you to import, export, and manage Trusted Certificates and System Certificates.



The Console Certificates pane (**Options** > **Certificates**) provides the following capabilities:

- Generate, download, or display a Certificate Signing Request (CSR)
- Import a signed certificate into CounterACT
- Import root CA and chain certificates to verify presented certificates
- Import certificates and full issuer chains as PKCS#7
- Export certificates as PKCS#12
- Add multi-scope assignments to certificates for CounterACT subsystems and Appliances.

The following CounterACT components require use of the Console's certificate interface for managing system certificate(s), trusted certificate(s) or both:

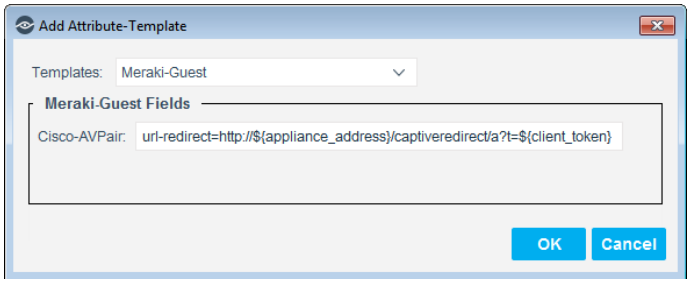
- ForeScout CounterACT® Authentication Module: RADIUS Plugin 4.3
- ForeScout CounterACT® Authentication Module: User Directory Plugin 6.3
- ForeScout CounterACT® Core Extensions Module: Syslog Plugin 3.4
- ForeScout CounterACT® Endpoint Module: HPS Inspection Engine 10.8
- ForeScout CounterACT® Endpoint Module: Linux Plugin 1.2
- ForeScout CounterACT® Endpoint Module: OS X Plugin 2.1
- ForeScout® Extended Module for McAfee® ePolicy Orchestrator® 3.1
- ForeScout® Extended Module for Tenable™ Vulnerability Management 2.7
- Access of Web Portals – for CounterACT user access of any CounterACT Web-based portal, for example, the **Dashboard**, the **Assets Portal**, the **Reports Portal**, the **User Portal Builder**

Refer to the section on *Configuring the Certificate Interface* in the *CounterACT Administration Guide* for more information.

Guest Management Enhancements

This release introduces enhancements to guest management.

- A new easy-to-use User Portal Builder that allows you to customize the look and feel of CounterACT user portal interfaces for various device types, such as mobile devices.
- Out-of-the-box Guest Management templates for Cisco and Meraki Centralized Web Authentication.



- Additional improvements to the guest user experience.

Refer to the *Authentication Module Release Notes* for more information.

RADIUS Plugin Enhancements

The 802.1x Plugin has been renamed RADIUS Plugin.

The following RADIUS Plugin enhancements are available.

- Streamlined Configuration-Deployment Process
- RADIUS Plugin Support for IPv6
- Support Network Device Administration Use Case
- Authentication Enhancements
- Endpoint RADIUS Information Display

Refer to the *Authentication Module Release Notes* for more information on the items described in this section.

Streamlined Configuration-Deployment Process

The release streamlines the CounterACT user's configuration-deployment process:

- Join of CounterACT Devices to Active Directory Domains
- Robust Test Functionality
- Pre-Admission Authorization - Rules and Treatments

RADIUS Plugin Support for IPv6

The RADIUS Plugin now provides IPv6 support for purposes of performing endpoint authentication, authorization and guest centralized web authentication (CWA).

Support Network Device Administration Use Case

The plugin now supports secure management of network devices based on generic RADIUS authentication and authorization.

Authentication Enhancements

The plugin provides the following authentication enhancements

- Support the use of the ***Protected EAP-TLS*** authentication protocol.
- With both Protected EAP-MSCHAPv2 and Protected EAP-TLS authentication processes, the plugin extracts both the outer user name and the inner user name of the supplicant. As a result, new attributes and properties are available for use

Endpoint RADIUS Information Display

Endpoint-related RADIUS information is now available for display in the Console Home > **All Hosts** pane.

Security Enhancements

This section describes important security enhancements.

CounterACT OS Hardened to Meet Certification/STIG requirements

CounterACT OS has been hardened to meet certification/STIG requirements.

https://nvd.nist.gov/ncp/checklist/816

Events Auditing Updated

Events auditing has been revamped to meet Common Criteria cPP_ND requirements. Additional auditing for user-related actions, connection establishment and termination, and certificate verification are now supported.

Improved Secure Communications with TLS 1.2 and 1.1

CounterACT Secure Communications have been improved, and now use TLS 1.2 by default, and also support TLS 1.1.

Under some scenarios, SecureConnector may use TLS 1.0 for communication.

Service Banners

Administrators can choose to display a notification message (banner) to users before they login to the Console. Users must confirm the message to continue. This message can serve to describe restrictions of use, legal restrictions or other relevant information. Refer to the *CounterACT Administration Guide* for more details.

Enhanced Password Policy

CounterACT password requirements for Console users have been enhanced to provide better security for CounterACT users.

The following password requirements can now be configured:

- Minimum number of characters that the password must differ from the previous password.

- If password can contain commonly used weak passwords. (Selecting this option also enforces additional requirements.
- Amount of time allowed between password changes.

  This only applies when the password was last changed by the same user. If, for example, an admin user last changed the password of a non-admin user, the non-admin user is not restricted by the time defined in this setting.
- If users must change their password at next login after it was changed by admin user.

Refer to the *CounterACT Administration Guide* for more information.

Trusted Connections Between CounterACT Devices

Connections between CounterACT devices now use fingerprints for verification purposes. When a connection is established, the fingerprints of the two CounterACT devices are compared. If they match, the connection is accepted. This ensures that only trusted CounterACT devices are connecting with each other. Refer to the *CounterACT Administration Guide* for more details.

Authenticate Backup Destination Server

You can now validate the server used during the transfer of CounterACT system and component backup files (SFTP and SCP only). Refer to the *CounterACT Administration Guide* for more details.

CounterACT Fixed Issues

This section describes fixed issues for this release.

Issue	Description
CA-12518	Under some scenarios, CounterACT cannot handle properties that include settings for dates that are in the future.
CA-12524	The **`fstool va uninstall`** command did not include a warning message before execution.
CA-13114	Multiple selection of Host Properties was enabled when the parent check box was NOT selected.
CA-13304	Web portal login with Smart Card was not working in FIPS mode.

Issue	Description
CA-13536	The boot partition mounting options in CounterACT devices were updated to handle a potential low level vulnerability.
CA-13538	The **User Home Directory** mode for the *fshttp* user was updated to resolve a security vulnerability.
CA-13541	When the failover license limit was exceeded and a new license was generated with higher limit, failover hosts were still reported as exceeding the limit.
CA-13881	The **`fstool maild`** command, used to start, stop or restart the mail daemon running on CounterACT, did not include an option to check the status of the service. The command now includes a "status" option which indicates if the daemon is running or stopped, and, if running, indicates the process ID.
CA-13910 **CA-14541**	The Packet Engine did not parse the NetBIOS domain name properly.
CA-13947	License verification failed if the Appliance machine time setting was changed to a future date and then reverted to present date
CA-13964	Lines of text that are beyond the fixed size of the text box in the **Condition** pane **Open Ports** property **Add** or **Edit** screen could not be viewed.
CA-13985	The disk cleaning process did not clean up large log files properly, and as a result, CounterACT occasionally restarted.
CA-14062	When adding an exception rule in the virtual firewall policy action to allow traffic to restricted/matched host IP addresses, the packet engine did not block traffic from the restricted host IP addresses to the target port defined in the exception rule.
CA-14106	Radius and TACACS servers were mistakenly included in the list of *Group - External User Directory* servers when adding a Console User Profile.
CA-14259	The text in the *Send Message to Syslog* action was arriving truncated at the Syslog server.
CA-14292	Duplicating a newly discovered switch entry failed if the switch entry had not yet been approved.
CA-14451	The composite properties report was truncated in host logs in CSV format.
CA-14453 **CA-14454**	The Apache web server software was updated to address security issues described in CVE-2017-5664.
CA-14614	The Console occasionally restarted due to an out-of-memory error that occurred when a new policy containing NIC Vendor conditions was sent to the Enterprise Manager.

Issue	Description
CA-14687	CounterACT appliances were disconnected sporadically from the Enterprise Manager.
CA-15048	When multiple Appliances try to connect the Recovery Enterprise Manager at the same time after failover from the Enterprise Manager, some Appliances failed to connect to the Recovery Enterprise Manager.
CA-15049	Under some scenarios, files in the Recovery Enterprise Manager were not automatically deleted when synchronizing with the Enterprise Manager.
CA-15192	The Audit Trails log recorded an Active Directory group user as Administrator instead of using the actual user name.
CA-15314	The web server failed to restart due to a DNS resolution error.
CA-15422	CounterACT users with Update Policy Control permissions in the Console were unable to perform manual actions on hosts
CA-16071 **CA-14875** **CA-16896**	In some cases, using the CLI command **`fstool hostinfo_all`** on an Appliance caused the Appliance to restart.
CA-16360	CounterACT upgrade was not supported on a High Availability system with only one node
CA-16474	The Event Viewer now provides status information about allocated and unallocated IPs in Internal Network.
CA-16558	The default for the **Show Threats View** option in **CounterACT Console Options > Threat Protection** was changed to not selected (disabled).

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.

Issue	Description
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 *CounterACT Installation Guide* 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-18473	Under certain circumstances, when CounterACT is deployed on KVM virtual systems, the CounterACT Packet Engine restarts every 2 hours, causing a range of traffic monitoring functionality to temporarily stop. Appliances which do not utilize SPAN/mirrored traffic are not affected.

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

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.

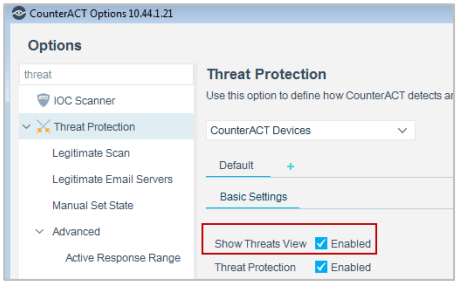
Important Upgrade Information

- ***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.
- Upgrade is supported starting from CounterACT version 7.0.0 with Service Pack 2.3.3 or above installed. In addition, **CounterACT version 7.0.0 with Service Pack 3.0.2 or above and plugins released with Service Pack 3.0.2 or above are not supported for upgrade to version 8.0**. To upgrade anyway, you must first roll back the Service Pack and the individual plugin versions to the compatible versions listed in Components Supported in Upgrading to Version 8.0.
- 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.

  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 then 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**.



Components Supported in Upgrading to Version 8.0

The following components are compatible when upgrading to CounterACT version 8.0.

Component Name	Versions Compatible for V8.0 Upgrade	Comments
CounterACT 7.0.0 Service Pack	2.3.3 2.3.4 3.0.0 3.0.1	**All Hotfix versions released within one of the GA versions shown on the left are supported for V8 upgrade.** For example, Service Pack 3.0.1.1001 is compatible when upgrading to CounterACT version 8.0
802.1X Plugin	4.1.0 4.2.0	
Advanced Tools Plugin	2.2.2 2.2.3	
CEF Plugin	2.6.1	
DHCP Classifier Plugin	2.0.5 2.0.6 2.1.0	
DNS Client Plugin	2.11080 3.0.0	
DNS Enforce Plugin	1.1.5	
External Classifier Plugin	2.2.2	
Hardware Inventory Plugin	1.0.2	
Hardware WatchDog Plugin	1.1.4	
HPS Inspection Engine	10.4.1 10.6.0 10.6.1 10.6.2 10.7.0 10.7.1	
Macintosh/Linux Property Scanner Plugin	6.1.x 7.0.0 7.0.1	
Microsoft SMS/SCCM Plugin	2.2.5	

Component Name	Versions Compatible for V8.0 Upgrade	Comments
NBT Scanner Plugin	3.0.2 3.0.4	
OS X Plugin	1.2.0 2.0.0	
Reports Plugin	4.1.5 4.2.0	
Switch Plugin	8.9.5 8.11.0 8.11.1	
Syslog Plugin	3.1.4 3.2.0	
Technical Support Plugin	1.1.1 1.1.2	
User Directory Plugin	6.1.0 6.1.2	
VMware vSphere Plugin	2.0.0	
VPN Concentrator Plugin	4.0.6 4.0.7	
Wireless Plugin	1.5.1 1.7.0	
Cisco PIX/ASA Firewall Integration Plugin	2.0.2	
Data Exchange Plugin, ForeScout Open Integration Module: Data Exchange Plugin	3.1.0 3.2.0 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	
Qualys VM Plugin	1.2.1	
Splunk Plugin	2.5.0 2.7.0	

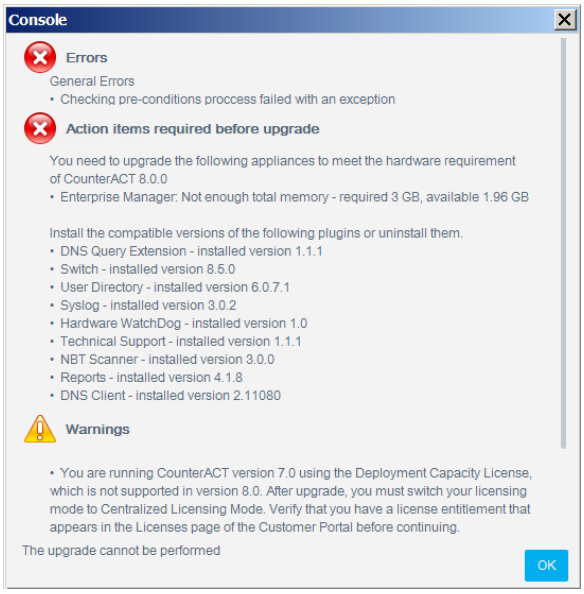
Component Name	Versions Compatible for V8.0 Upgrade	Comments
Palo Alto Networks Next-Generation Firewall Extended Module	1.0.0 1.1.0 1.1.1	
Tenable VM Plugin	2.5.0 2.6.0	
ForeScout Extended Module for VMWare AirWatch MDM	1.7.2	
WebAPI Plugin	1.2.0 1.2.1 1.2.2	
AWS Plugin	1.1.0 1.1.1	
IOC Scanner Plugin	2.0.0 2.0.1 2.1.0	
FireEye NX Module	2.0.0	
FireEye EX Plugin	1.1.0	
FireEye HX Plugin	1.1.0	
McAfee ePO Plugin, ForeScout Extended Module for McAFee ePO	2.7.0 3.0.0	
IBM QRadar Plugin	2.0.0 2.0.1	
Rapid7 Nexpose Plugin	1.1.0 1.1.1	

Components Not Supported for Version 8.0

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 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

Not Supported for Version 8.0

Products that are not supported for CounterACT 8.0 must be uninstalled from CounterACT 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, 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.

Extended Module Release Information

All Extended Modules are available with version 8.0 with the exception of the following, which will be supported after ***June 30th*** 2018.

- Advanced Compliance (SCAP) 1.2
- Check Point Threat Prevention 1.1

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 CounterACT version 8. These procedures are provided, due to CounterACT version 8'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 CounterACT version 8.

Before upgrading to CounterACT version 8.0, 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, 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.

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 the 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 and Migrating 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 and Migrating to Centralized Licensing Mode

If you are running CounterACT version 7.0.0 and would like to upgrade your deployment to version 8.0 operating in Centralized Licensing Mode, perform the following upgrade/migration procedure.

> *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. See Additional CounterACT 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 CounterACT version 8.0, operating in Centralized 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 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.

To upgrade and migrate to Centralized Licensing Mode:

1. Back up Enterprise Manager system settings. Refer to the section on performing a one-time system backup in the *CounterACT Administration Guide*.
2. Upgrade the Enterprise Manager to CounterACT Version 8.0. See Upgrading to Version 8. Use the CounterACT Upgrade file (FSP) for version 8.0.

   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 CounterACT Version 8.0 in step 6.
3. Upgrade the Recovery Enterprise Manager to CounterACT Version 8.0. This procedure is only relevant if your deployment has a Recovery Enterprise Manager. See Upgrading to Version 8.

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

4. Configure the Enterprise Manager to operate in Centralized Licensing mode:
   a. Log in to the Enterprise Manager via the Console.
   b. Navigate to **Options > Licenses** and select **Migrate**. Continuing with the migration will restart the CounterACT Console and the Enterprise Manager and all CounterACT devices in the deployment that are connected to the Enterprise Manager. The License Migration dialog box opens.
   c. Select **Migrate**.

   After the Enterprise Manager is up and running, the licenses are invalid and CounterACT features will not function properly.
5. Activate a new license file. Refer to the section on activating a new license file (Centralized Licensing Mode) in the *CounterACT Administration Guide*.

   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.
6. Upgrade each Appliance to CounterACT Version 8.0. See Upgrading to Version 8. Use the CounterACT Upgrade file (FSP) for version 8.0.

   After the upgrade, the Appliances will reconnect to the Enterprise Manager and then restart due to the change in licensing mode.
7. 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 Centralized Licensing mode, Failover Clustering functionality is supported by the *Resiliency License*. Refer to the section on the Resiliency License in the *CounterACT Administration Guide*.

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:

1. Go to https://forescout.force.com/support/.
2. 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:

1. Go to www.forescout.com/docportal.
2. Use your customer support credentials to log in.
3. 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

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

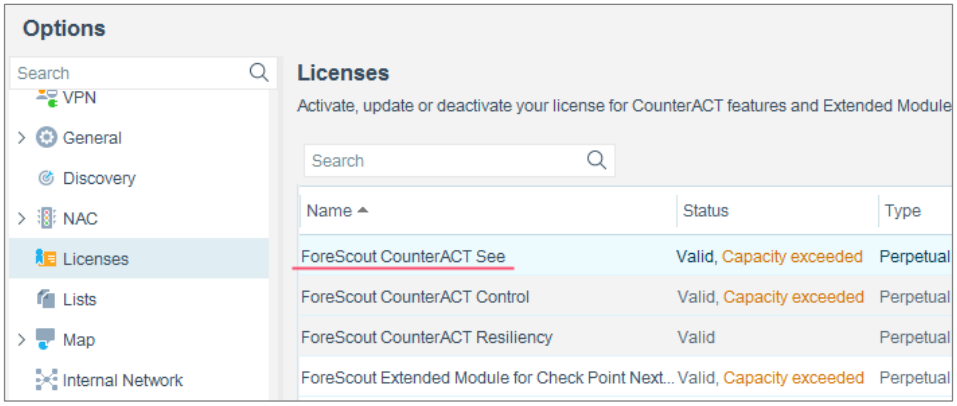
Documentation Portal

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.



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

Legal Notice

2018-05-08 17:12