ForeScout CounterACT®

Endpoint Module: OS X Plugin

Configuration Guide

Version 2.1

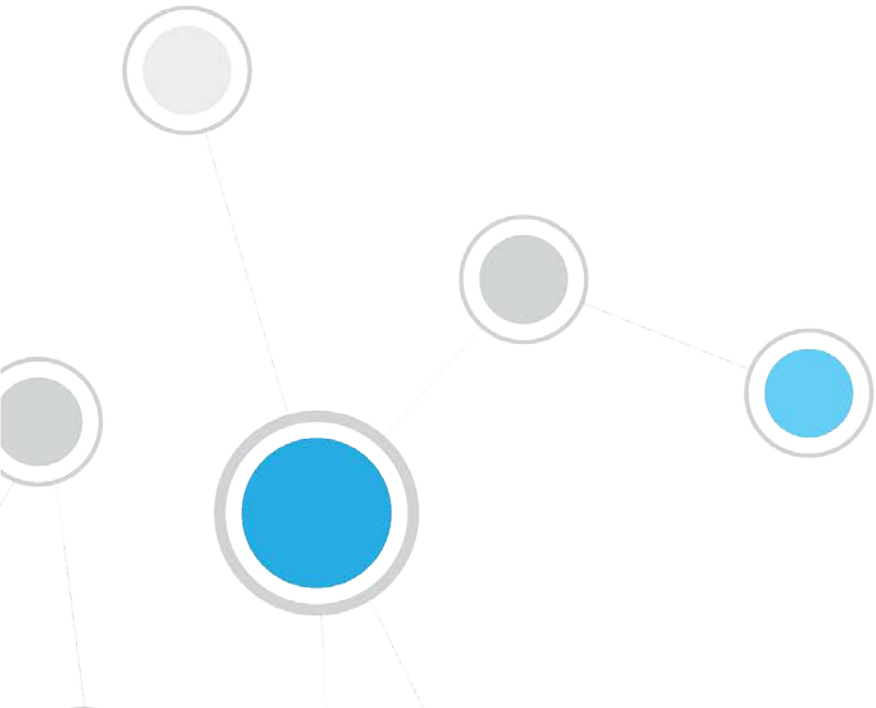


Table of Contents

About This Plugin

The OS X Plugin is a component of the ForeScout CounterACT® Endpoint Module. See Endpoint Module Information details about the module.

The OS X Plugin manages endpoints running Mac/OS X operating systems. It supports properties, actions and other management functionality for OS X endpoints. This plugin parallels the features of the HPS Inspection Engine which manages Windows endpoints, and the Linux Plugin which manages Linux endpoints.

Each OS X Plugin version provides the latest regularly updated version of SecureConnector that is native to OS X.

Accessing and Managing Endpoints

The plugin accesses endpoints to learn detailed information such as file metadata, operating system information, and more. In addition, the plugin is used to run scripts on endpoints and to perform other remediation actions.

When you configure the plugin, you determine the methods you want to use to access and manage endpoints. When CounterACT successfully implements these access methods on an endpoint, the endpoint is resolved as *Manageable* by CounterACT.

The plugin provides the following methods to access endpoints:

- Remote Inspection
- SecureConnector

Both methods can be deployed together in a single network environment.

Remote Inspection

Remote Inspection uses the SSH communications protocol to query the endpoint and to run scripts and implement remediation actions on the endpoint.

Agentless

Remote Inspection is *agentless* - CounterACT does not install any applications on the endpoint to query it. This makes Remote Inspection useful when administrators or end users do not want to install utilities or other executables on the endpoint.

Specify remote inspection settings in the Remote Inspection tab during plugin configuration.

The following properties indicate whether CounterACT accesses and manages an endpoint using Remote Inspection:

- Linux Manageable (SSH Direct Access)
- Macintosh Manageable (SSH Direct Access)
- Windows Manageable Domain
- Windows Manageable Domain (Current)
- Windows Manageable Local

SecureConnector

SecureConnector is a small-footprint executable that runs on the endpoint. It reports endpoint information to CounterACT, and implements actions on the endpoint. The *Start SecureConnector* action initiates SecureConnector installation on endpoints.

Agent-Based

The SecureConnector executable file must be installed and maintained on the endpoint. This may not be acceptable in certain network environments, or for some endpoints or users. SecureConnector can be installed in several ways:

SecureConnector on Endpoint	Windows Endpoints	Linux Endpoints	OS X Endpoints
As a dissolvable utility	✔	✔	✔
As a permanent application	✔	✘	✘
As a permanent service / system daemon	✔	✔	✔

The following properties indicate whether CounterACT accesses and manages an endpoint using SecureConnector:

- Linux Manageable (SecureConnector)
- Macintosh Manageable (SecureConnector)
- Windows Manageable SecureConnector
- Windows Manageable SecureConnector (via any interface)

What to Do

This section lists the steps you should take for the initial installation of this plugin.

1. Verify that you have met system requirements. See Requirements.
2. (Managed endpoints only) Redirect managed OS X endpoints to the OS X Plugin. Previously, the Macintosh/Linux Property Scanner supported OS X endpoints. When - the OS X Plugin is installed:
   - OS X endpoints managed using Remote Inspection pass automatically to the control of the OS X Plugin. The OS X Plugin uses the same public and private keys for Remote Inspection as the Macintosh/Linux Property Scanner did. Remote Inspection settings of the Macintosh/Linux Property Scanner no longer affect OS X endpoints; you can recreate these settings or customize Remote Inspection settings for OS X endpoints when you Configure the Plugin.
   - Existing OS X endpoints managed by SecureConnector must be redirected from the Macintosh/Linux Property Scanner to communicate with the OS X Plugin. See Migrate Endpoints Managed by SecureConnector to the OS X Plugin.
3. (SecureConnector only) Upgrade SecureConnector on OS X endpoints already managed by SecureConnector. New releases of the plugin often provide an updated version of SecureConnector native to OS X operating systems. This plugin does not automatically update SecureConnector on endpoints when - a

new release of the plugin is installed. Create one or more policies based on the Upgrade SecureConnector for OS X Policy Template that rollout SecureConnector upgrades to OS X endpoints managed by SecureConnector.

4. Make OS X endpoints manageable. The standard *Asset Classification and Primary Classification* policies provided with CounterACT identify Mac/OS X endpoints, and assign these endpoints to the *Macintosh* group. Create a policy that uses the **Macintosh Manageable** host properties to detect members of these groups that are not yet managed by CounterACT.
   - To make an endpoint manageable by Remote Inspection, use your network's administrative tools to define a user account on the endpoint, and use the network's PKI to distribute the public key used for Remote Inspection connections to the endpoint. See Managing Endpoints Using Remote Inspection.
   - Deploy SecureConnector on new, unmanaged OS X endpoints. You can use an interactive process to install SecureConnector, or install it silently using a background process. See Deploying SecureConnector.
5. Create Custom Policies that use the properties and actions provided by this plugin to manage endpoints.

Requirements

This section describes system requirements, including:

- CounterACT Requirements
- Networking Requirements
- Supported Operating Systems

CounterACT Requirements

The plugin requires the following CounterACT releases and other components:

- CounterACT version 8.0
- An active Maintenance Contract for CounterACT devices
- Endpoint Module version 1.0 including the following components:
  - Linux Plugin
  - HPS Inspection Engine

Networking Requirements

SecureConnector creates an encrypted tunnel from the endpoint to the Appliance through TCP port 10005. This port must be open on enterprise firewalls to support communication between SecureConnector and CounterACT.

Supported Operating Systems

This plugin supports OS X versions 10.8 through 10.12.

Configure the Plugin

The configuration options for this plugin duplicate similar configuration options of the HPS Inspection Engine, which are relevant to Windows endpoints. The settings you make here should match parallel settings of the HPS Inspection Engine if you would like uniform behavior across endpoints with different operating systems.

You can configure the plugin to:

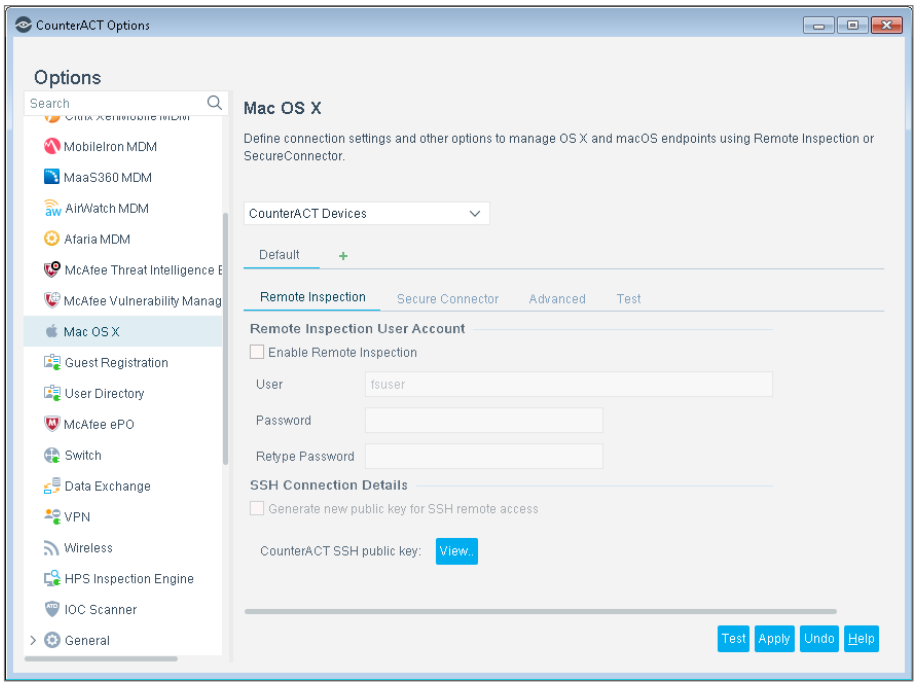
- Define general SecureConnector settings
- Specify resolution methods and default values for various global parameters

Configuration by Region or Appliance

By default, the settings you define are applied to all Appliances. If required, you can create separate configurations for each Appliance or for a group of Appliances in the same geographical region. See Configuration for an Appliance or Group of Appliances for details.

To configure the plugin:

1. In the CounterACT Console, select **Options** from the **Tools** menu.
2. Do one of the following:
   - In the Options tree, select **OS X**.
   - In the Options tree, select **Plugins**. In the Plugins table, select the **OS X** Plugin and select **Configure**.
3. The OS X configuration pane appears. The Remote Inspection tab is displayed.



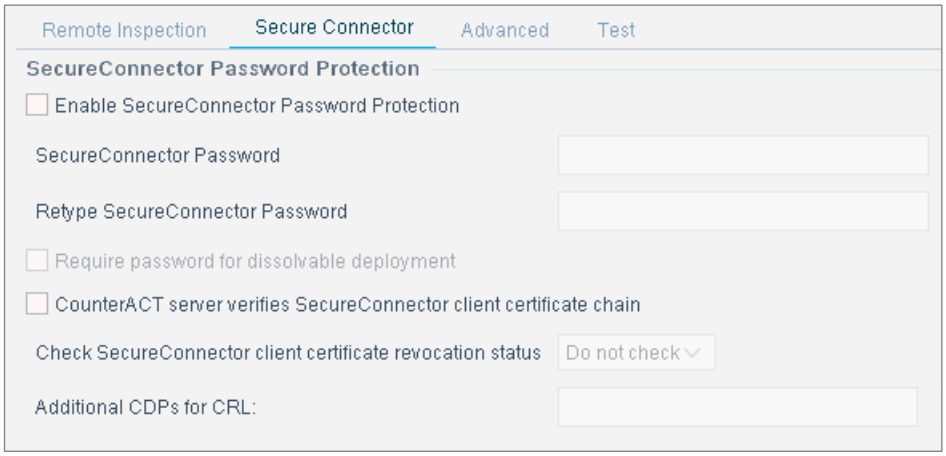
4. The following options control how CounterACT accesses endpoints by Remote Inspection.

If you used the Macintosh/Linux Property Scanner to manage OS X endpoints via Remote Inspection beforethis plugin is installed -, copy these settings from the Remote Inspection configuration tab of the Macintosh/Linux Property Scanner. The OS X Plugin will use the Remote Inspection user already defined on endpoints, and the existing public key. You do not need to redistribute the public key.

Enable Remote Inspection	Select this option to enable use of Remote Inspection methods to poll endpoints for information. The other fields of this tab are only relevant if Remote Inspection is used in your environment. If you are not managing OS X endpoints using Remote Inspection, disable this option to avoid unnecessary SSH network traffic. See Managing Endpoints Using Remote Inspection.
User	Specify an administrator user account that is used to establish an SSH connection with endpoints. This user account must be defined on each endpoint. A valid password must be provided to use actions or properties that require privileged access, such as the **Software Updates Missing** property or the *Run Interactive* option of the **Run Script** action.
Password	
Retype Password	

Generate new public key for remote SSH access	Select this option and select **Apply** to change the public key. The plugin changes the public key of the Enterprise Manager, and synchronizes all Appliances with the new key. You must distribute the new key to endpoints using one of the methods described in Distribute the Public Key. Consult your PKI/network security team to determine how frequently this key should be regenerated.
CounterACT SSH public key	Select **View** to see the public key CounterACT uses for the SSH connection to endpoints. This key must be distributed to endpoints. See Distribute the Public Key for details.

5. Select the SecureConnector tab. These options control how CounterACT deploys SecureConnector on endpoints.

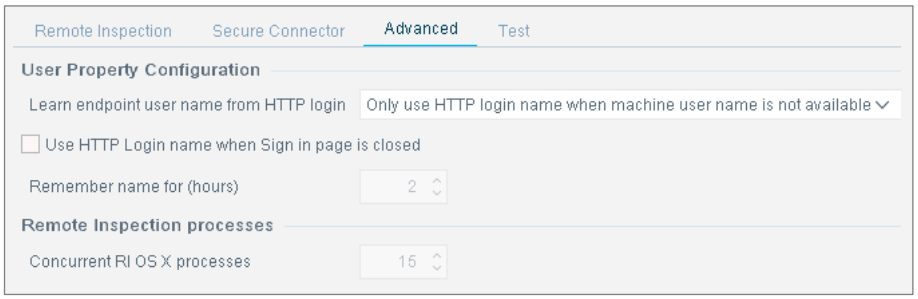


The SecureConnector Password Protection area contains settings that control password protection of SecureConnector on endpoints.

Enable SecureConnector Password Protection	When this option is selected, endpoint users must enter the password you specify here to exit SecureConnector on their endpoints. See Stopping SecureConnector from the Endpoint.
Enter SecureConnector Password **Confirm SecureConnector Password**	Enter the identical string into both fields to define the password that allows users to exit Secure connector.
Require password for dissolvable deployment	When this option is selected, SecureConnector that runs as a dissolvable application is also password protected: to exit SecureConnector without logging out of the endpoint, a password is required.
CounterACT server verifies SecureConnector client certificate chain	When this option is enabled, SecureConnector clients on endpoints present a certificate when they connect to CounterACT. CounterACT validates the certificate chain. When you select this option, additional required settings are active. To support certificate-based authentication of clients, endpoints managed by SecureConnector must have a signed client certificate and trust chain. Your PKI may define several certificates that can be used by

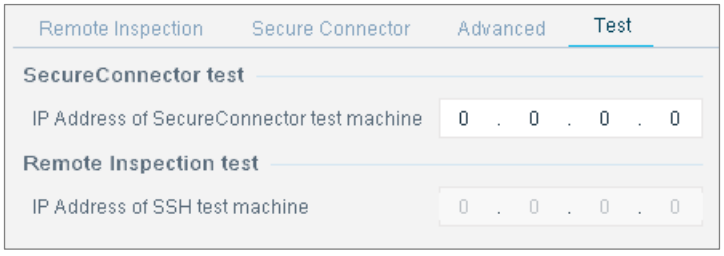
	SecureConnector, for example certificates defined by geographical location or endpoint roles and permissions. Use the Certificates pane of the Console to import the trust chain(s) into CounterACT.
Check SecureConnector client certificate revocation status	Check if the certificate is in the Certificate Revocation List (CRL) of the issuing Certificate Authority.
Additional CDPs for CRL	Enter a comma-separated list of CRL distribution points that should be queried.

6. In the Advanced tab, the following settings are available:



Learn endpoint user name from HTTP login	Specify how the **User** property is resolved. Typically the username currently logged in locally is used. When the **HTTP Login** action is applied to an endpoint, the User property can be based on the username from the CounterACT Login session.
Use HTTP Login name when Sign in page is closed	If you choose options that resolve the **User** property based on a CounterACT HTTP Login session on the endpoint, enable this option to retain that username even if the end user closes the CounterACT Login Session window. In the **Remember name for** field, specify the time period after initial login that CounterACT retains this username.
Remember name for (hours)	
Concurrent RI OS X processes	Set the maximum number of simultaneous Remote Inspection processes this plugin runs on each Appliance.

7. In the Test tab, enter IP addresses of endpoints that are used to test the plugin. To test Remote Inspection, verify the following on the endpoint:
   - The Remote Inspection user defined during plugin configuration exists.
   - The public key used by CounterACT was installed.



8. Select **Apply** to save settings.

Verify That the Plugin Is Running

After configuring the plugin, verify that it is running.

To verify:

1. Select **Tools**>**Options** and then select **Modules**.
2. Navigate to the plugin and select **Start** if the plugin is not running.

Managing Endpoints Using Remote Inspection

You can inspect endpoints using SSH remote access. SSH remote access requires distribution of the Appliance's public key to managed endpoints.

If you are not using Remote Inspection to manage OS X endpoints, disable Remote Inspection when you Configure the Plugin. This avoids the unnecessary network overhead of establishing unused SSH connections. When you disable Remote Inspection, you can use SecureConnector to manage devices. See Managing Endpoints Using SecureConnector for information about SecureConnector setup.

Define a Remote Inspection User on Endpoints

Define an admin-level user on each endpoint that you want to manage. This user should have the name you entered in the **User** field of the Remote Inspection tab during plugin configuration.

Distribute the Public Key

The public key allows SSH-based inspection of the endpoint without the endpoint user's password. This section describes how to create a custom script that distributes the key to endpoints. You may need an endpoint password to distribute the key.

To create a script to distribute the public SSH key:

1. In the CounterACT Console, open the plugin configuration pane. See Configure the Plugin.
2. In the Remote Inspection tab, select the **View** button in the **CounterACT SSH Connection Details** area of the tab.
3. Copy the key to a clipboard or another application.
4. Write a script which does the following on each endpoint you want to manage via Remote Inspection:

a. Create the folder **.ssh** under the user defined in the **Remote Inspection User** field of the plugin Configuration pane.

b. Change the **.ssh** folder permissions as follows:

chmod 755 .ssh (there is a space between **755** and the **.ssh** suffix).

c. Paste the public key into the file **.ssh/authorized_keys.** Save the file.

d. Change the file **.ssh/authorized_keys** permissions as follows:

chmod 644 authorized_keys

Managing Endpoints Using SecureConnector

This section describes how to use SecureConnector to query and manage OS X endpoints.

Deploying SecureConnector

SecureConnector can be installed on OS X endpoints in several ways:

- As a dissolvable utility
- As a permanent service

For both these installation types, you can specify SecureConnector visibility:

- Visible deployment - a SecureConnector icon appears in the menu bar. This icon indicates endpoint connectivity to CounterACT, compliance with CounterACT compliance policies, and other information.
- Invisible deployment – no icon appears in the menu bar.

Use one of these methods to install SecureConnector for the first time:

- Interactive Installation – the Start SecureConnector Action
- Background Installation of SecureConnector

To migrate OS X endpoints managed by the Macintosh/Linux Plugin using legacy versions of SecureConnector, see Migrate Endpoints Managed by SecureConnector to the OS X Plugin.

To update SecureConnector on OS X endpoints already managed by the OS X Plugin, use the Upgrade OS X SecureConnector action.

Interactive Installation – the Start SecureConnector Action

The *Start SecureConnector* action installs SecureConnector on endpoints detected by a CounterACT policy. Endpoints are redirected to the HTML page, where end users can download the appropriate installer package. You can specify interaction and installation settings including:

- The text displayed to prompt end users to install the package

- Whether SecureConnector is deployed as a permanent service or as a dissolvable executable
- Whether the SecureConnector icon is visible in the menu bar

For details about working with this action, see *Working with Actions* in the *CounterACT Administration Guide* or online Help.

Background Installation of SecureConnector

This procedure installs SecureConnector on endpoints with no user interaction. Use this procedure for fresh (scratch) installation on endpoints that run OS X 10.8 or above.

You can use third party endpoint management utilities such as Jamf Pro/Casper Suite to implement the procedure described here.

To install SecureConnector in the background:

1. Copy the installer **update.tgz** from Enterprise Manager. See Appendix 2: SecureConnector Installer Packages.
2. Distribute this file to target endpoints.
3. Use the command line interface or a script to perform the following:
   a. Unpack the archive.
   b. Run the ./Update.sh script in the archive, using the following syntax:

      To install SecureConnector as a dissolvable executable:

      ./Update.sh -t dissolvable -v {0|1}

      To install SecureConnector as a permanent service:

      sudo ./Update.sh -t daemon -v {0|1}

      Where **-v** determines if the SecureConnector icon is visible in the menu bar:

      -v 1 installs SecureConnector with a visible menu bar icon.

      -v 0 installs SecureConnector without a visible menu bar icon.

      Invoke sudo mode only to install SecureConnector as a permanent service. Do not invoke sudo mode to install SecureConnector as a dissolvable executable.

Upgrading SecureConnector on Endpoints Managed by SecureConnector

Do one of the following:

- If you previously used the Mac/Linux Property Scanner to manage OS X endpoints using SecureConnector, you must transfer these endpoints to the control of the OS X Plugin. Typically this is a one-time procedure when you install the OS X Plugin. Refer to Migrate Endpoints Managed by SecureConnector to the OS X Plugin.

- To roll out regular updates of SecureConnector for OS X provided by releases of this plugin, create one or more policies based on the Upgrade SecureConnector for OS X Policy Template.

Migrate Endpoints Managed by SecureConnector to the OS X Plugin

The OS X Plugin supports SecureConnector for endpoints running the OS X operating system.

Previously, the Macintosh/Linux Property Scanner supported SecureConnector interaction with OS X endpoints. To maintain management continuity, release 7.0.0 and above of the Macintosh/Linux Property Scanner support existing OS X endpoints using legacy versions of SecureConnector on these endpoints.

When the OS X Plugin is installed, it is strongly recommended to transfer existing OS X endpoints to the management control of the OS X Plugin, so they will receive updated versions of SecureConnector. After this one-time migration:

- The Macintosh/Linux Property Scanner no longer handles SecureConnector interaction for these endpoints.
- The OS X Plugin supports all SecureConnector interactions for the endpoint, including distribution of updated SecureConnector releases.

This section describes the upgrade and migration sequence for OS X endpoints managed by SecureConnector through the Macintosh/Linux Property Scanner.

To migrate SecureConnector managed OS X endpoints from the Macintosh/Linux Property Scanner to the OS X Plugin:

1. Verify that you have installed release 7.0.0 or above of the Macintosh/Linux Property Scanner. This release provides the action required to migrate endpoints.
2. Install this release of the OS X Plugin.
3. Create a policy or policy rule that does the following:
   - 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.

   The OS X Plugin replaces the legacy version of SecureConnector on these endpoints with the latest version, and the endpoints now communicate with the OS X Plugin.

For more information on the **Migrate to OS X SecureConnector** action, refer to the *Configuration Guide* for version 7.0.0 of the Macintosh/Linux Property Scanner. See Additional CounterACT Documentation.

Stop SecureConnector

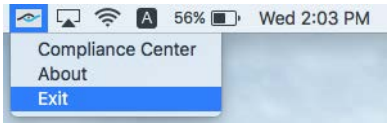
The **Stop SecureConnector** action stops the SecureConnector executable and removes all files related to SecureConnector from the endpoint. For details about

working with this action, see *Working with Actions* in the *CounterACT Administration Guide* or online Help.

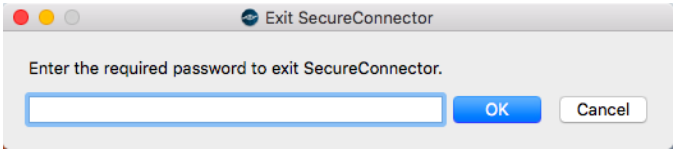
Stopping SecureConnector from the Endpoint

By default, end users can stop SecureConnector on their devices by doing one of the following:

- Drag the SecureConnector application to the OS X Trash Can on their device to uninstall.
- When the SecureConnector toolbar icon is visible, select the icon, then select **Exit**. SecureConnector stops, but is not uninstalled.



When you Configure the Plugin you can enable password protection for SecureConnector on endpoints. When password protection is enabled, users who try to **Exit** SecureConnector are prompted for a password.



SecureConnector Details

Item	Detail
Size on disk	25 MB
Endpoint memory utilization	20 MB
Deployment type	Permanent service or dissolvable.
Visibility options	Visible (icon in menu bar) or non-visible
Deployment options	Interactive: HTTP redirection to download portal. Defined in the **Start SecureConnector** action. Background: download and installation of setup file using shell script or third party software distribution tool. See Background Installation of SecureConnector
Endpoint privilege level	Dissolvable: no privileges required. Installs and runs under currently active user session. Permanent service: admin privileges required. Installed under root.
Installation folder	Dissolvable: $TMPDIR Permanent service: /Applications
Script folder	Folders are created for downloaded scripts under /var/folders/ .

Item	Detail
SecureConnector Starts	Dissolvable: Runs once until user logout. No restart. Permanent service: System boot.

Certificate Based Rapid Authentication of Endpoints

Typically CounterACT endpoint detection capabilities are combined with endpoint authentication and compliance policies to enforce network access control: Upon connection, network access of endpoints is restricted (typically to the DHCP and DNS servers and to CounterACT for detection and remediation interactions) until the user/endpoint is authenticated and compliance is proven. Only then is the necessary network access granted. However, authenticating endpoints and verifying compliance can cause a delay during which even legitimate endpoints have only restricted access. If complex compliance policies are in place, this delay in network access may be noticeable, resulting in an unsatisfactory user experience for corporate users.

Certificate based rapid authentication provides a strong, secure and extremely fast endpoint authentication mechanism. It uses your corporate PKI (Public Key Infrastructure) to provide immediate, authenticated network access for corporate users and other known endpoints.

The following describes a typical scenario when endpoints connect to the network:

- Corporate endpoints and other trusted endpoints managed by SecureConnector immediately initiate certificate-based authentication as part of SecureConnector's TLS interaction with CounterACT. Endpoints are granted immediate network access based on a signed X.509 digital certificate. CounterACT continues the compliance checks defined in active policies, and may revoke or change endpoint access if these checks fail.
- A corporate policy may grant limited network access to endpoints without a valid rapid authentication certificate, or with an expired or revoked certificate, or endpoints not managed by SecureConnector, until normal, policy-driven compliance checks are run.

For more information about implementing certificate-based rapid authentication in your environment, see the *SecureConnector Advanced Features How-to Guide*.

Run Policy Templates

This plugin provides the following policy templates:

- Upgrade SecureConnector for OS X - this template creates a policy that upgrades SecureConnector on OS X endpoints managed by SecureConnector. Use this policy to roll out the newest version of SecureConnector for OS X each time you upgrade the OS X Plugin.

You should have a basic understanding of CounterACT policies before working with the templates. See the CounterACT Templates and Policy Management chapters of the CounterACT Administration Guide.

Upgrade SecureConnector for OS X Policy Template

This template generates a policy to identify endpoints that are not running the most recent release of SecureConnector for OS X, and to upgrade SecureConnector on those endpoints. Use this policy to roll out the newest version of SecureConnector for OS X each time you upgrade the OS X Plugin.

The main rule of this policy selects OS X endpoints.

Sub-rules of the policy examine the version of SecureConnector running on each endpoint. If an endpoint is running an older version of SecureConnector, the policy installs the most recent version of SecureConnector.

Prerequisites

Policies you create with this template detect OS X endpoints. Before you run a policy based on this template, verify that you have run policies based on the *Asset Classification* or *Primary Classification* policy templates.

Run the Template

This section describes how to create a policy from the policy template. For details about how the policy works, see How Devices are Detected and Handled.

To run the template:

1. Log in to the CounterACT Console and select the **Policy** tab.
2. Select **Add** from the Policy Manager. The Policy Wizard opens.
3. Expand the Mac OS X folder and select **Upgrade SecureConnector for OS X**.
4. Select **Next.** The **Name** page opens.

Name the Policy

The Name pane lets you define a unique policy name and useful policy description. Policy names appear in the Policy Manager, the Views pane, Reports and in other features. Precise names make working with policies and reports more efficient.

5. Define a unique name for the policy you are creating based on this template, and enter a description.

   Naming Tips

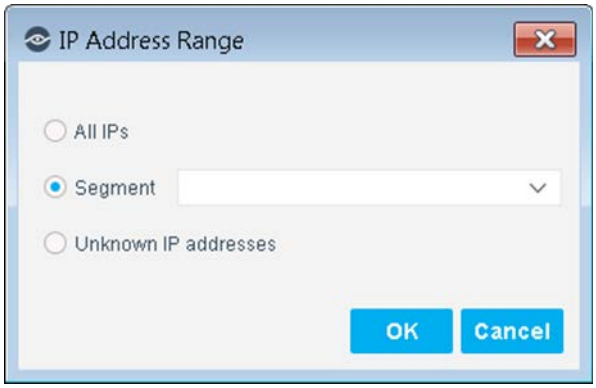
   – Make sure names are accurate and clearly reflect what the policy does. For example, do not use a generic name such as My_Compliance_Policy.
   – Use a descriptive name that indicates what your policy is verifying and which actions will be taken.

– Avoid having another policy with a similar name.

6. Select **Next.** The Scope pane and IP Address Range dialog box opens.

Define which Hosts will be Inspected - Policy Scope

7. Use the IP Address Range dialog box to define which endpoints are inspected.



Define Policy Scope

The following options are available:

– **All IPs**: Include all IP addresses in the Internal Network.
– **Segment**: Select a previously defined segment of the network. To specify multiple segments, select **OK** to close this dialog box, and select **Segments** from the Scope page.
– **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.

Filter the range by including only certain CounterACT groups and/or by excluding certain endpoints or users or groups when using this policy.

8. Select **OK**. The added range appears in the Scope pane.
9. Select **Next**.
10. Select **Finish**. The policy is created.

How Devices are Detected and Handled

This section describes the main rule and sub-rules of the policy created by the Upgrade SecureConnector for OS X template. Policy rules instruct CounterACT how to detect and handle hosts defined in the policy scope.

Hosts that match the Main Rule are passed to sub-rules of the policy for further evaluation. *Hosts that do not match the Main Rule are not passed to sub-rules of the policy*. Sub-rules allow you to follow up after initial detection and handling with separate detection and remediation actions, in one automated sequence.

For each endpoint that matches the Main Rule, the condition of each sub-rule is evaluated in order until a condition is matched. When a match is found, the

corresponding action is applied to the host. If an endpoint does not match the condition of a sub-rule, evaluation moves to the next rule.

Main Rule

The main rule of this policy uses the **Network Function** property to detect OS X endpoints. It also specifies recheck behavior for the policy. By default, the policy is evaluated every eight hours, and is applied to newly discovered endpoints.

Sub-Rules

Sub-rules of the policy examine the version of SecureConnector for OS X running on each endpoint, and upgrade SecureConnector if necessary.

1. Unmanaged Endpoints

   This rule detects OS X endpoints that are not managed by CounterACT. No actions are applied to these endpoints.

2. SSH Managed Endpoints

   This rule detects endpoints on that are managed using Remote Inspection. No actions are applied to these endpoints.

3. SC managed endpoints running the LATEST version of SC

   This rule detects endpoints that are already running the latest version of SecureConnector for OS X. No actions are applied to these endpoints.

4. SC managed endpoints an earlier version of SC

   This rule detects endpoints that are not running the latest version of SecureConnector for OS X.

   The **Upgrade OS X SecureConnector** action is used to install the latest version of SecureConnector for OS X to these endpoints. By default, the action is disabled. After verifying that the policy correctly detects upgrade candidates in your environment, enable this action.

Create Custom Policies

Use the properties and actions provided by this plugin to detect and handle endpoints. You can use the policy to instruct CounterACT to apply a policy action to endpoints that do or do not match property values defined in policy conditions.

For example, when this plugin is installed you must redirect existing OS X endpoints managed by SecureConnector to this plugin. This custom policy is described in Migrate Endpoints Managed by SecureConnector to the OS X Plugin.

Properties

CounterACT properties let you create policy conditions that detect hosts with specific attributes. For example, create a policy that detect hosts running a certain Operating System or having a certain application installed.

Actions

CounterACT actions let you instruct CounterACT how to control detected devices. For example, assign a detected device to a quarantine VLAN or send the device user or IT team an email. For more information about working with policies, select **Help** from the policy wizard.

To create a custom policy:

1. On the Console toolbar, select the **Policy** tab. The Policy Manager opens.
2. Select **Add** to create a policy.

Detecting OS X Devices – Policy Properties

The OS X Plugin supports the following properties for OS X endpoints.

Macintosh Applications Installed	Indicates the applications present on an endpoint. ▪ For endpoints running OS X 10.8, the **Certificate** field is not reported.
Macintosh Expected Script Result	Use this property to run a command or file that will detect certain endpoint attributes, statuses or any other information defined in the script or command. Commands and file can also be used to carry out actions on endpoints. Scripts must be in a Unix-based format. Convert scripts written on DOS-based platforms. When script evaluation times out (for example, if an endless loop results from running the script) CounterACT evaluates the property as *Irresolvable*. The Run Script on Macintosh action is also available.
Macintosh File Date	Indicates the last modification date and time of a defined file on an endpoint.
Macintosh File Exists	Indicates the existence of a specified file on an endpoint.
Macintosh File Size	Indicates the size (in bytes) of a specified file on an endpoint.
Macintosh Hostname	Indicates the OS X host name.
Macintosh Manageable (SecureConnector)	Indicates whether the endpoint is connected to CounterACT via SecureConnector.
Macintosh Processes Running	Indicates the processes running on an endpoint.
Macintosh SecureConnector Version	Indicates the version of the SecureConnector package that is running on the endpoint.
Macintosh Software Updates Missing	Indicates OS X security and other updates that are missing on the detected endpoint. To resolve this property on endpoints running macOS 10.8, CounterACT must use an admin account to access the endpoint.
Macintosh User	Indicates all the users logged in to the endpoint. The list of usernames is comma separated.
Macintosh Version	Indicates the version of OS X running on the endpoint.

OS CPE Format	Indicates the operating system running on the endpoint, in Common Platform Enumeration format. The plugin resolves this general CounterACT property for OS X endpoints.
User	This is a general CounterACT property. For OS X endpoints, the plugin populates this property with the username of the user currently logged in to the endpoint console. You can query the User Directory based on this value.

Managing OS X Devices – Policy Actions

This section describes the actions that are supported by the OS X Plugin.

The plugin implements the following general actions on OS X endpoints managed by SecureConnector. See the *CounterACT Administration Guide* for details of these actions.

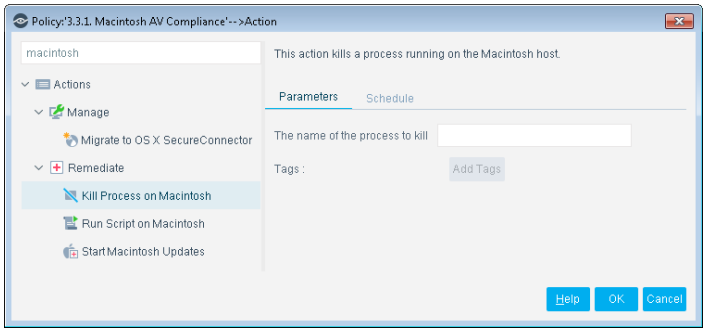
- HTTP Login
- HTTP Localhost Login
- HTTP Notification
- HTTP Redirection to URL
- HTTP Sign Out
- Start SecureConnector
- Stop SecureConnector

In addition, this plugin provides the following actions specific to OS X endpoints.

- Kill Process on Macintosh
- Run Script on Macintosh
- Send Notification (OS X)
- Start Macintosh Updates
- Upgrade OS X SecureConnector

Kill Process on Macintosh

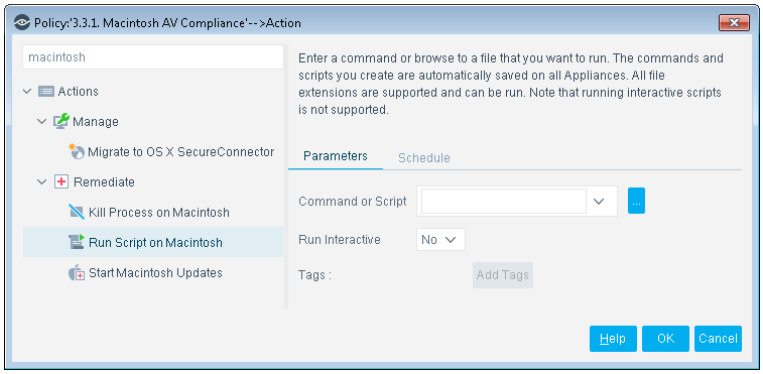
This action halts specific OS X processes. If the process name includes endpoint-specific or user-specific data such as the user name, you can add it as a variable using the **Add Tags** button. For example, if you enter the {user} tag, the user name of the endpoint is automatically inserted into the process name. See the CounterACT Administration *Guide* for details.



Run Script on Macintosh

You can leverage scripts to:

- Automatically deploy vulnerability patches and antivirus updates.
- Automatically delete files.
- Create customized scripts to perform any action that you want.



To use this action:

1. Specify a command or script to run on endpoints. Do one of the following:
   - Enter a command in the **Command or Script** field. To run a file that already exists on the endpoint, enter its absolute path. You can use property tags to include endpoint-specific or user-specific values in this field. See the *CounterACT Administration Guide* for details.
   - Select the Continue button to select from the repository of user-defined scripts and commands. See the *CounterACT Administration Guide* for more information about user-defined scripts.
2. (Optional) To run interactive scripts on OS X endpoints, select the **Run Interactive** option.

   For endpoints managed by SecureConnector, scripts and commands always run in the user *context when this option is selected, even when SecureConnector runs on the endpoint as a permanent service/daemon.*

3. (Optional) Use the Schedule tab to specify when the action is applied, to delay application of the action, or to specify repeat application of the action.

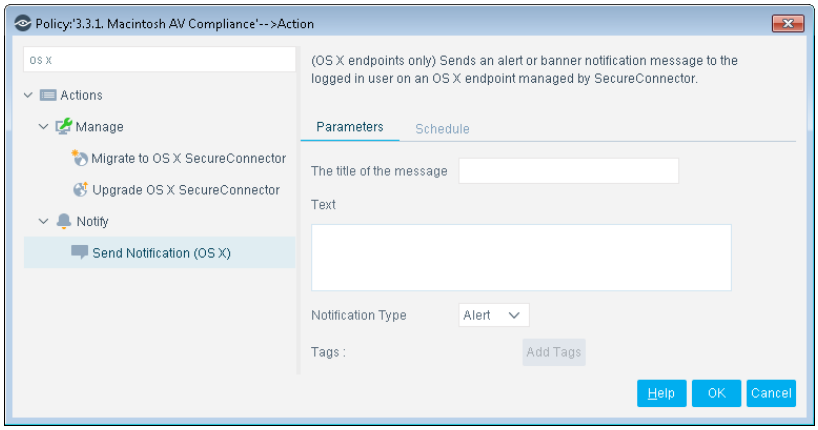
Send Notification (OS X)

This action sends an alert or banner notification message to an OS X endpoint managed by SecureConnector. The notification is handled by the Notification Center of the user currently logged in to the endpoint. This action parallels the **Send Balloon Notification** action for Windows endpoints.

You can use property tags to include endpoint-specific host property values in the notification. See the *CounterACT Administration Guide* for details.

Banner notifications appear briefly on screen. Alerts persist on screen until the user interacts with them.

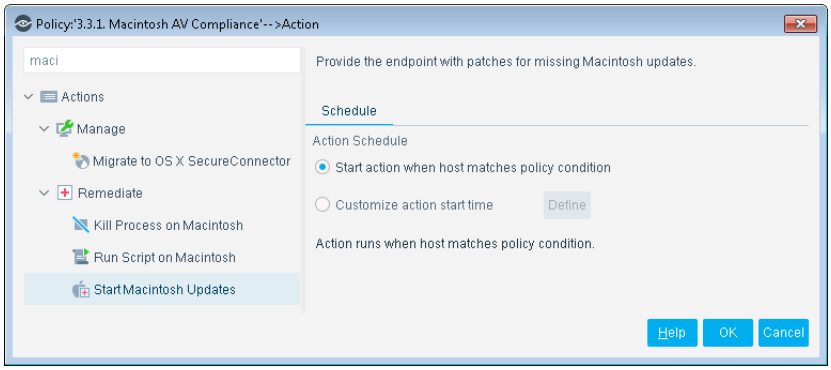
- This action is not supported by endpoints that run OS X 10.8



Start Macintosh Updates

This action triggers automatic operating system updates on the endpoint. Use the action in policies that have incorporated the *Macintosh Software Updates Missing* property, which indicates the software updates that are missing on the endpoint.

To perform this action on endpoints running macOS 10.8, CounterACT must use an admin account to access the endpoint.



Upgrade OS X SecureConnector

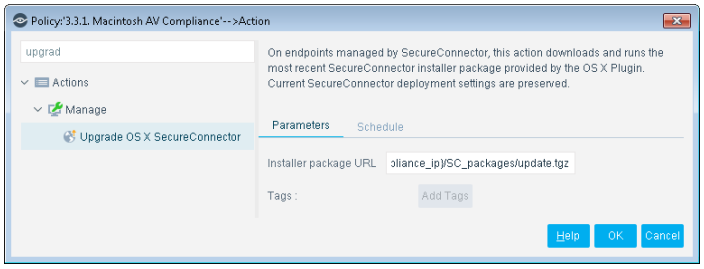
This action applies to endpoints already managed by the OS X Plugin.

- To update SecureConnector on OS X endpoints still managed by the Macintosh/Linux Property Scanner, see Migrate Endpoints Managed by SecureConnector to the OS X Plugin.
- For first time (scratch) installation of SecureConnector, use the Start SecureConnector action or Background Installation of SecureConnector.

This action updates the SecureConnector package running on an OS X endpoint. Deployment type (permanent/dissolvable) and menu bar visibility options are preserved during upgrade.

The OS X Plugin does not automatically update SecureConnector on endpoints when a new release of the plugin is installed. Use this action to update SecureConnector on OS X endpoints.

In the **Installer package URL** field, specify a valid network path to the **`update.tgz`** archive that is used to update endpoints. By default, this field points to the file that the OS X Plugin places on each CounterACT Appliance. If you copy this archive to a content distribution network or server, specify the full network path to this new location. See Appendix 2: SecureConnector Installer Packages.



Appendix 1: Troubleshooting Management of OS X endpoints by SecureConnector

If after deploying SecureConnector, the Console shows that particular endpoints are not being managed by SecureConnector, use the procedures described in this section to verify that SecureConnector is running on the affected endpoints.

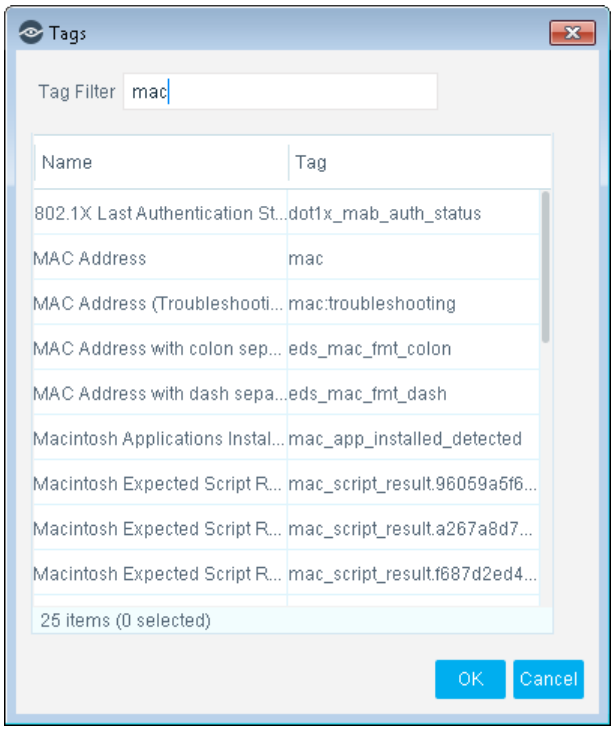
1. Confirm that the following processes are running:
   - When SecureConnector is installed as a service:
     ForeScout SecureConnector –daemon
     ForeScout SecureConnector –agent: one process for each logged-in user
   - When SecureConnector is running as a dissolvable application:
     ForeScout SecureConnector –local
2. Verify that SecureConnector is connecting to the IP address of the CounterACT Appliance that manages the endpoint.
3. To test SecureConnector connectivity to managed endpoints, log in as root to the Appliance that manages the endpoint, and use the following command:

   `fstool osx_test -a <`*ip*`> -p <`*property*`> [-f <`*file*`>] [-c '<`*command*`>']`

   where

   <*ip*> is the IP address of an OS X endpoint managed by SecureConnector.

   <*property*> is the internal property tag of a property reported by this plugin. See Detecting OS X Devices – Policy Properties.



The test returns the current value of the property on the endpoint.

<*file*> is the pathname of a file on the endpoint. The test indicates whether the file exists at the specified location on the endpoint. This parameter is relevant when resolving properties that require a file path.

<*command*> is a command expression that the test runs on the endpoint. The expression enclosed in quotes should include all parameters and flags, as in typical CLI usage. The test returns the output of the command. This parameter is relevant to the **OS X Expected Script Result** property.

SecureConnector Client Log Files

SecureConnector maintains a log file on managed endpoints. When SecureConnector is installed as a service, log files are located at:

/Applications/ForeScout SecureConnector/Contents/log/

When SecureConnector is deployed as a dissolvable executable, log files are located at:

$TMPDIR/Applications/ForeScout SecureConnector/Contents/log/

A series of up to 10 files is maintained:

fs_sc.log, fs_sc.log.1, …fs_sc.log.10

Each file contains up to 10MB of data. Files are rolled over on a FIFO basis.

To retrieve the most recent 500KB of data from these log files:

1. Log in as root to the Appliance that manages the endpoint.
2. Submit the following command:

   fstool osx_test -a <*IP***> -l <***pathname***>**

   Where

   <*IP*> is the IP address of the endpoint to query.

   <*pathname*> is the full pathname under root at which retrieved data is saved.

Appendix 2: SecureConnector Installer Packages

SecureConnector is agent-based – a small-footprint executable is installed on endpoints to make them manageable. When the plugin is installed, a set of SecureConnector installer packages is generated and placed on each CounterACT Appliance in your environment. The following file contains a script based installer for SecureConnector:

https://<*Appliance_IP***>/SC_packages/update.tgz**

where <*Appliance_IP*> is the IP address of Enterprise Manager or the Appliance that manages the endpoint.

When you launch this script on an endpoint, run-time flags set deployment options such as permanent/dissolvable installation, and SecureConnector toolbar icon visibility. See Background Installation of SecureConnector for details.

This installer also supports the Upgrade OS X SecureConnector action. When you use the action, you must specify a valid network path to an instance of the archive.

Endpoint Module Information

The OS X plugin is installed with the CounterACT Endpoint Module.

The Endpoint Module provides connectivity, visibility and control to network endpoints through the following CounterACT components:

- HPS Inspection Engine
- Linux Plugin
- OS X Plugin
- Microsoft SMS/SCCM
- Hardware Inventory Plugin

The Endpoint Module is a ForeScout Base Module. Base Modules are delivered with each CounterACT release.

Components listed above are released and rolled back with the Endpoint Module.

Refer to the *CounterACT Endpoint Module Guide* for basic information on other plugins included in this module, module requirements as well as upgrade and rollback instructions. See *Additional CounterACT Documentation* for information about how to access the module 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**.

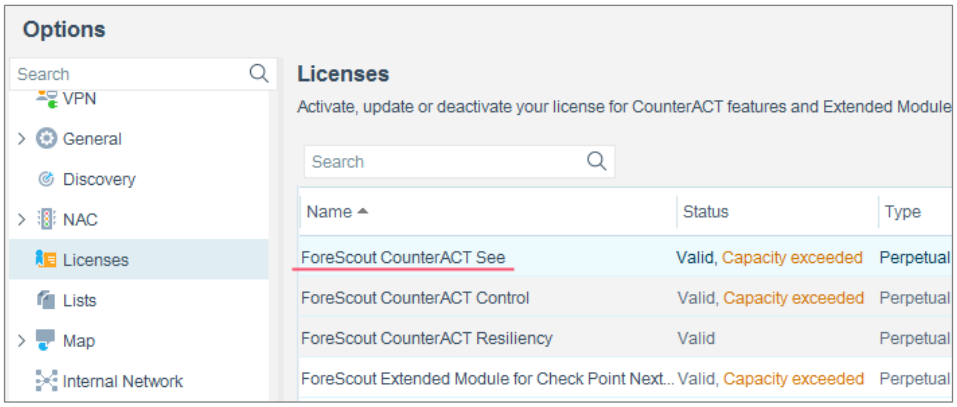
Documentation Portal

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

2018-04-10 09:21