FORESCOUT

Forescout®

Endpoint Module: OS X Plugin

Configuration Guide

Version 2.2.3

Contact Information

Forescout Technologies, Inc.

190 West Tasman Drive

San Jose, CA 95134 USA

https://www.Forescout.com/support/

Toll-Free (US): 1.866.377.8771

Tel (Intl): 1.408.213.3191

Support: 1.708.237.6591

About the Documentation

- Refer to the Technical Documentation page on the Forescout website for additional documentation: https://www.Forescout.com/company/technical-documentation/
- Have feedback or questions? Write to us at documentation@forescout.com

Legal Notice

2020-02-12 14:18

Table of Contents

About This Plugin

The OS X Plugin is a component of the Forescout® 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

This section contains information common to plugins of the Endpoint Module.

Plugins of the Endpoint Module access endpoints to learn detailed information such as file metadata, operating system information, and more. In addition, the plugins run scripts on endpoints and perform other remediation actions.

- The HPS Inspection Engine interacts with Windows endpoints.
- The Linux Plugin interacts with Linux endpoints.
- The OSX Plugin interacts with OSX endpoints.

When you configure these plugins, you determine the methods you want to use to access and manage endpoints. When these access methods are successful, the endpoint is resolved as *Manageable* by the Forescout platform.

You can use 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* - The Forescout platform 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 of each plugin during plugin configuration.

The following properties indicate whether Remote Inspection is used to access and manage an endpoint:

- For Windows endpoints (supported by the HPS Inspection Engine):
  - Windows Manageable Domain
  - Windows Manageable Domain (Current)
  - Windows Manageable Local
- For Linux endpoints (supported by the Linux Plugin):
  - Linux Manageable (SSH Direct Access)
- For OSX endpoints (supported by the OSX Plugin):
  - Macintosh Manageable (SSH Direct Access)

SecureConnector™

SecureConnector is a small-footprint executable that runs on the endpoint. It reports endpoint information to the Forescout platform 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:

	Windows Endpoints	**Linux Endpoints**	**OS X Endpoints**
SecureConnector installer package provided by:	HPS Inspection Engine	Linux Plugin	OSX Plugin
Can install SecureConnector as a ***dissolvable utility***	✔	✔	✔
Can install SecureConnector as a ***permanent application***	✔	✘	✘
Can install SecureConnector as a ***permanent service / system daemon***	✔	✔	✔

The following properties indicate whether SecureConnector is used to access and manage an endpoint:

- For Windows endpoints (supported by the HPS Inspection Engine):
  - Windows Manageable SecureConnector
  - Windows Manageable SecureConnector (via any interface)
- For Linux endpoints (supported by the Linux Plugin):
  - Linux Manageable (SecureConnector)
- For OSX endpoints (supported by the OSX Plugin):
  - Macintosh Manageable (SecureConnector)

What to Do

Perform the following steps to work with this plugin:

1. Verify that you have met system requirements. See Requirements.
2. (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 roll out SecureConnector upgrades to OS X endpoints managed by SecureConnector.
3. Make OS X endpoints manageable. The standard Primary Classification policy provided with Forescout identifies Mac/OS X endpoints, and assigns 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.
   - 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.
4. Create Custom Policies that use the properties and actions provided by this plugin to manage endpoints.

Requirements

This section describes system requirements, including:

- Forescout Requirements
- Networking Requirements
- Supported Operating Systems

Forescout Requirements

The plugin requires the following:

- Forescout version 8.1.
- Endpoint Module version 1.1.0 including the following components:
  - Linux Plugin
  - HPS Inspection Engine

- If you are using Flexx licensing, ensure that you have a valid Forescout eyeControl (ForeScout CounterACT Control) license, to use enforcement actions provided by the component. Refer to the *Forescout Flexx Licensing How-to Guide* for more information about managing Flexx licenses.

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 the Forescout platform.

Supported Operating Systems

For detailed information about endpoint operating system versions validated for integration with this Forescout component, refer to the Forescout Compatibility Matrix.

Configure the Plugin

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

You can configure the plugin to:

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

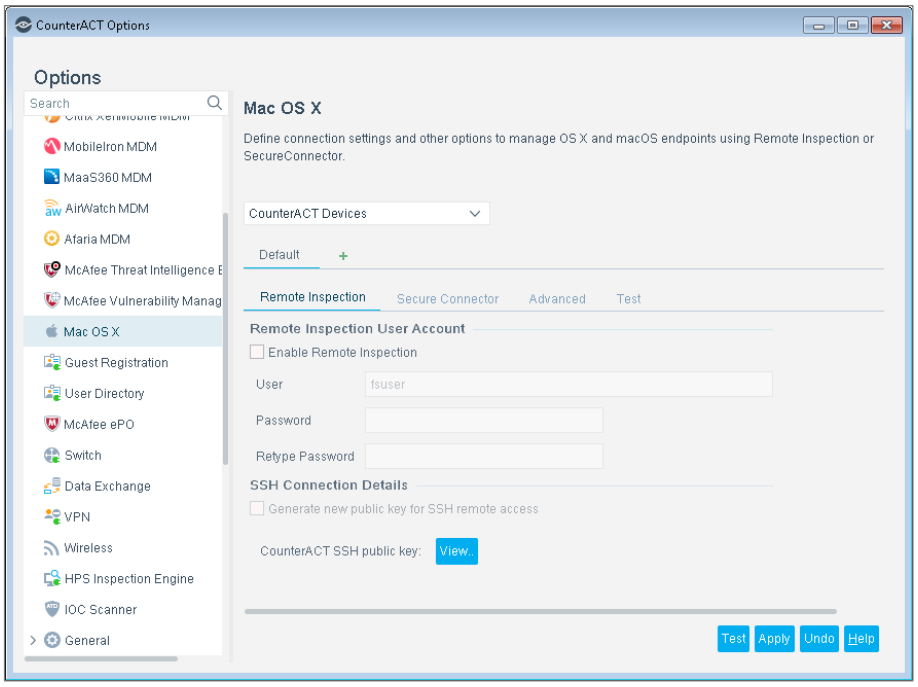
Configuration by Region or Appliance

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 Forescout 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**.

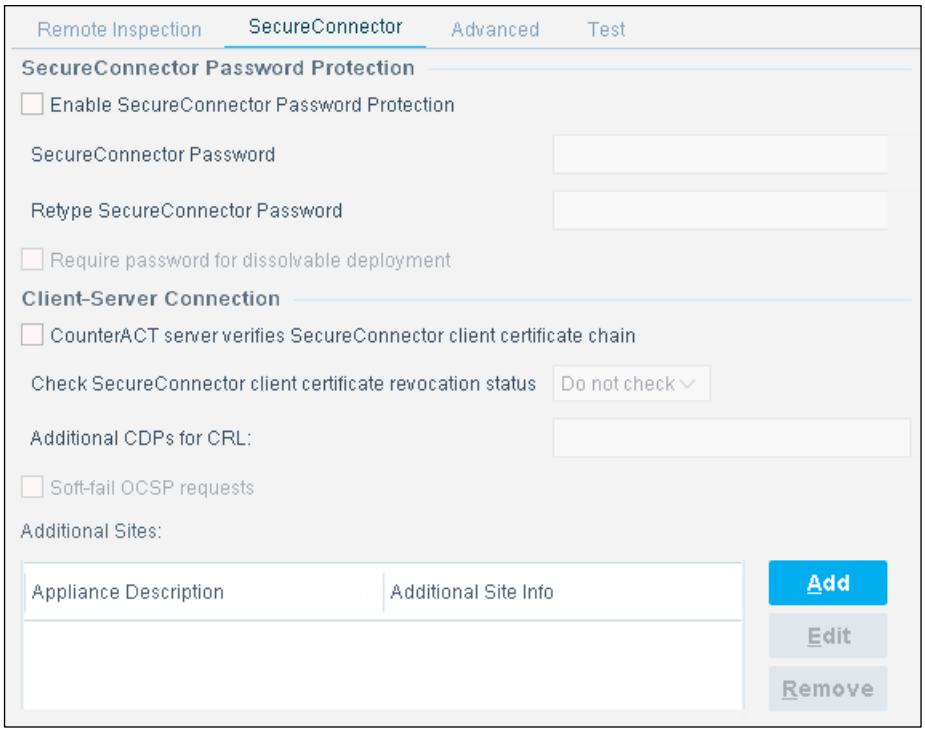
   The Remote Inspection tab of the OS X configuration pane is displayed.



3. The following options control how endpoints are accessed using Remote Inspection.

Enable Remote Inspection	Select this option to enable use of Remote Inspection methods to poll endpoints for information. Additional fields are relevant only if Remote Inspection is used. If you are not using Remote Inspection, disable this option to avoid unnecessary SSH network traffic. See Managing Endpoints Using Remote Inspection.
User	Specify the administrator user account 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. See Distribute the Public Key for details. 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 that is used for the SSH connection to endpoints. This key must be distributed to endpoints. See Distribute the Public Key for details.

4. Select the SecureConnector tab to define how SecureConnector is deployed on endpoints.

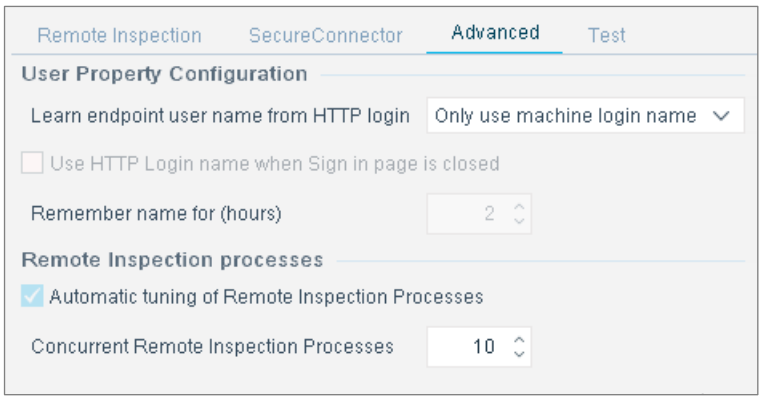


The following settings control SecureConnector password protection on endpoints.

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.
SecureConnector Password **Retype SecureConnector Password**	Enter the identical string in both fields to define the password that allows users to exit SecureConnector.
Require password for dissolvable deployment	When this option is selected and SecureConnector runs as a dissolvable application, it is password protected. A password is required to exit SecureConnector without logging out of the endpoint.
CounterACT server verifies SecureConnector client certificate chain	When this option is enabled, SecureConnector clients on endpoints present a certificate when they connect to Forescout devices. The Forescout platform validates the certificate chain. When you select this option, additional settings are required. 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).

Check SecureConnector client certificate revocation status	Select this option 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.
Additional Sites	Use this table to specify CounterACT devices that SecureConnector connects to when it cannot connect to the managing Appliance of the endpoint. SecureConnector first tries to connect to the Enterprise Manager that manages the Appliance, and then to the CounterACT devices listed here. To populate this table, see Defining Additional Sites.

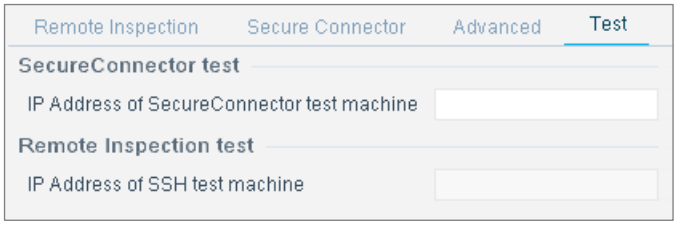
5. In the Advanced tab, the following settings are available:



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 Forescout Login session.
Use HTTP Login name when Sign in page is closed	If you choose options that resolve the **User** property based on a Forescout HTTP Login session on the endpoint, enable this option to retain that username even if the end user closes the Forescout Login Session window.
Remember name for (hours)	Specify the length of time (in hours) after initial login that the Forescout platform retains this username.
Automatic tuning of Remote Inspection Processes	You can tune the number of Remote Inspection and SecureConnector processes that run concurrently on each Appliance to resolve endpoint properties. You can use automatic tuning or customize tuning. **To enable automatic tuning:** Select **Automatic Tuning for HPS Inspection Engine Processe** to enable automatic tuning of HPS Inspection Engine processes. For each Appliance to which this setting applies, the maximum number of concurrent Remote Inspection and SecureConnector processes is determined dynamically as memory usage changes. **To customize tuning (for advanced use only):**

	1. Clear the **Automatic Tuning for HPS Inspection Engine Processes** checkbox. **2.** In the **Concurrent Remote Inspection Processes** field, set the maximum number of processes which communicate with endpoints managed by Remote Inspection that can be active at one time. *Configuring a higher maximum value allows more concurrent endpoint connections but consumes more Appliance resources. Tune these settings carefully. If Appliance performance is impacted, reduce these values.* *For more information, see* Tune HPS Inspection Engine Processes *in the* Forescout HPS Inspection Engine Configuration Guide*.*

6. In the Test tab, enter the 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 for Remote Inspection connections was installed.



7. Select **Apply** to save settings.

Verify That the Plugin Is Running

After configuring the plugin, verify that it is running.

To verify:

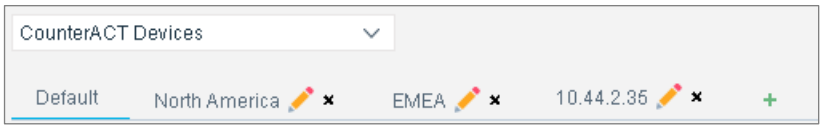
1. Select **Tools**>**Options** and then select **Modules**.
2. Navigate to the plugin and select **Start** if the plugin is not running.

Configuration for an Appliance or Group of Appliances

You can create and apply configurations for individual Appliances, or for a group of Appliances.

Configurations are organized using a row of tabs. ***Each tab duplicates all the configuration fields in the pane.***

Initially, only the Default tab is present. In the following example, an additional tab has been added, with the configuration for a specific Appliance.



Use the following controls to create and manage configurations:

- Select the Plus sign **+** to create a new configuration.
- When there are several configurations, it may be difficult to locate the configuration that applies to a specific device. Select the device from the *CounterACT Devices* drop-down. The configuration that applies to that device is highlighted for editing.

For more information about creating and applying configurations, see the *Forescout Administration Guide*.

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 Forescout Console, open the plugin configuration pane. See Configure the Plugin.
2. In the Remote Inspection tab, select **View** in the **CounterACT SSH Connection Details** area.
3. Copy the key to a clipboard or another application.

4. Write a script that 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 task bar. This icon indicates endpoint connectivity to the Forescout platform, compliance with compliance policies, and other information.
- Invisible deployment – no icon appears in the task bar.

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

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

Interactive Installation – the Start SecureConnector Action

The Start SecureConnector action installs SecureConnector on endpoints. 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 task bar

For details about working with this action, see *Working with Actions* in the *Forescout 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 this procedure.*

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 task bar:
      `-v 1` installs SecureConnector with a visible task bar icon.
      `-v 0` installs SecureConnector without a visible task 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

To roll out regular updates of SecureConnector for OS X provided by releases of this plugin, do one of the following:

- Create one or more policies based on the Upgrade SecureConnector for OS X Policy Template
- Create custom policies that apply the Upgrade OS X SecureConnector action.

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 *Forescout Administration Guide* or online Help.

Stopping SecureConnector from the Endpoint

By default, end users can stop SecureConnector on their devices as follows:

- By dragging the SecureConnector application to the OS X Trash Can on their device to uninstall.
- When the SecureConnector toolbar icon is visible, by selecting the icon and then selecting **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.

Defining Additional Sites

Additional Sites are CounterACT devices that SecureConnector connects to when it cannot connect to the managing Appliance of the endpoint. Use the Additional Sites table in the SecureConnector tab to define a list of alternative CounterACT Appliances. SecureConnector first tries to connect to the Enterprise Manager that manages its managing Appliance, and then steps through this list of CounterACT devices.

Endpoint Roaming

Use this table to support endpoint roaming in geographically disperse environments with several independent, regional Enterprise Managers. In each region, specify the Enterprise Managers of other regions as Alternative Appliances. When endpoints roam from their network location, they step through this list to find the Enterprise Manager of their new location. This ensures that roaming endpoints remain manageable. For more information, refer to the *SecureConnector Advanced Features How-to Guide*.

To define an alternative Appliance:

1. On the Appliance that you want to use as an alternative:
   a. Log in to the fs-cli interface.
   a. From the command line prompt, submit the following command:
   `fstool linux additional_sites`
   b. A string is generated. Copy the string.
2. In the Forescout Console:
   a. Open the Linux Plugin configuration that you want to modify and select the SecureConnector tab. Refer to Configure the Plugin.
   Alternative appliances are listed in a table.
   b. Select an existing entry in the table. The new alternative Appliance is added below the selected entry.
   c. Select **Add**. The Add dialog box appears. Specify the following information:

Appliance Description	A text description of this alternative Appliance.

Additional Site Info	The string that you generated on the alternative Appliance.

d. Select **OK**. The alternative Appliance appears in the table.

SecureConnector Details

Item	Detail
Size on disk	31.5 MB
Endpoint memory utilization	20 MB
Deployment type	Permanent service or dissolvable.
Visibility options	Visible (icon in task 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/.
SecureConnector Starts	Dissolvable: Runs once until user logout. No restart. Permanent service: System boot.

Certificate-Based Rapid Authentication of Endpoints

Typically Forescout 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 the Forescout platform 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 the Forescout platform. Endpoints are granted immediate network access based on a signed X.509 digital certificate. The Forescout platform 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 template:

- 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 Forescout policies before working with the templates. See the Templates and Policy Management chapters of the Forescout 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 *Primary Classification* policy template.

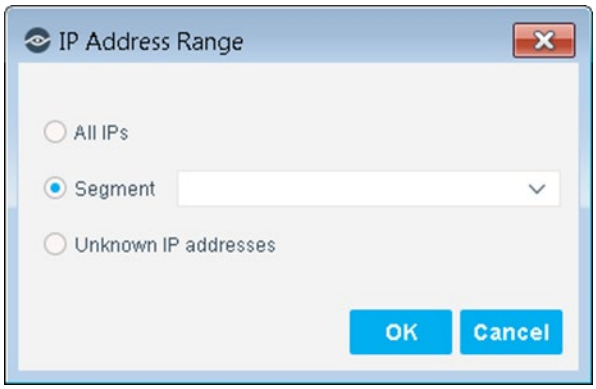
Create an Upgrade SecureConnector for OS X Policy Template

This section describes how to create a policy using the Upgrade SecureConnector for OS X 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 Forescout 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.
5. Define a unique name for the policy you are creating based on this template and enter a description.
   - 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 are taken.
   - Avoid having another policy with a similar name.

   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.
6. Select **Next.** The Scope pane opens, followed by the IP Address Range dialog box.
7. Use the IP Address Range dialog box to define which endpoints are inspected.



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** or **Cancel** to close this dialog box, and select **Segments** from the Scope pane.

- **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.

8. Select **OK**. The added range is listed 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 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 let you 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. 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, this 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 apply a policy action to endpoints that do or do not match property values defined in policy conditions.

Properties

Forescout *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

Forescout *actions* let you instruct the Forescout platform how to control detected devices. For example, assign a detected device to a quarantine VLAN or send an email to the device user or IT team. 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	Runs a command or file that detects specific endpoint attributes, statuses, or any other information defined in the script or command. Commands and files 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), the property is evaluated as *Irresolvable*. The Run Scripts 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) **OSX SecureConnector Connected/Disconnected**	Indicates whether the endpoint is connected to the Forescout platform via SecureConnector. OSX SecureConnector Connected/Disconnected is the related Track Changes property.
Macintosh Processes Running	Indicates the processes running on an endpoint.
Macintosh SecureConnector Version (OSX Plugin)	Indicates the version of the SecureConnector package 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, the Forescout platform 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 Forescout property for OS X endpoints.
OSX SecureConnector Connected/Disconnected	OSX SecureConnector Connected/Disconnected is the related Track Changes property.
User	This is a general Forescout 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 *Forescout Administration Guide* for details.

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

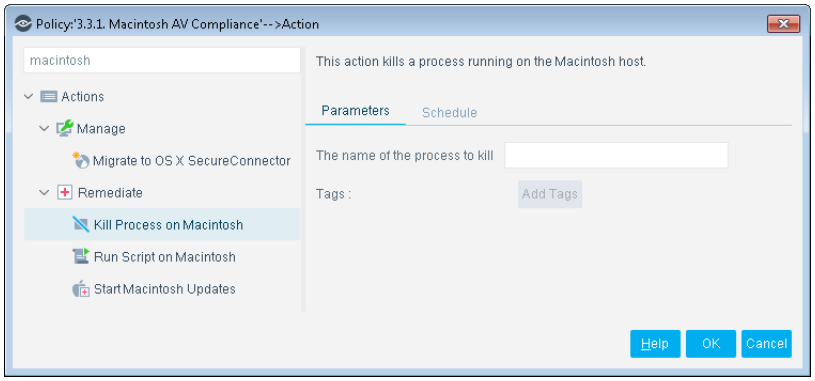
In addition, this plugin provides the following actions specific to OS X endpoints.

- Kill Process on Macintosh
- Run Scripts 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 username, you can add it as a variable using the **Add Tags** option. For example, if you enter the {user} tag, the username of the endpoint is automatically inserted into the process name. See the *Forescout Administration Guide* for details.

If you are using Flexx licensing, ensure that you have a valid *Forescout eyeControl* license to use this action. Refer to the *Forescout Flexx Licensing How-to Guide* for more information about managing licenses.

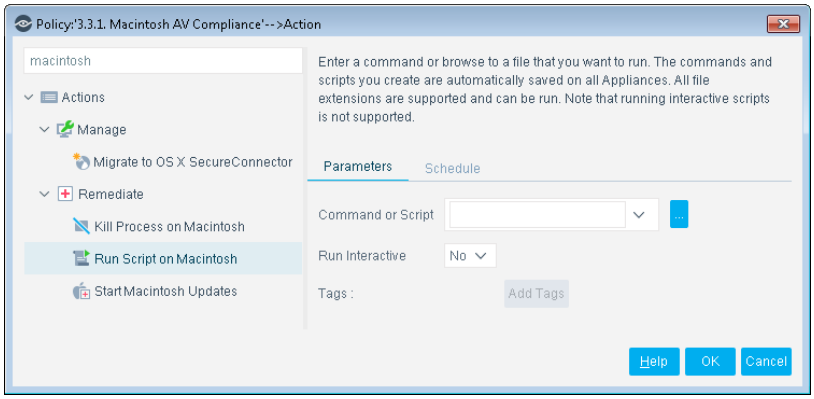


Run Scripts on Macintosh

If you are using Flexx licensing, ensure that you have a valid *Forescout eyeControl* license to use this action. Refer to the *Forescout Flexx Licensing How-to Guide* for more information about managing licenses.

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 set 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 *Forescout Administration Guide* for details.
   - Select **Continue** to select from the repository of user-defined scripts and commands. See the *Forescout Administration Guide* for details.
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) In the Schedule tab, specify when the action is applied, to delay application of the action, or to specify repeat application of the action.

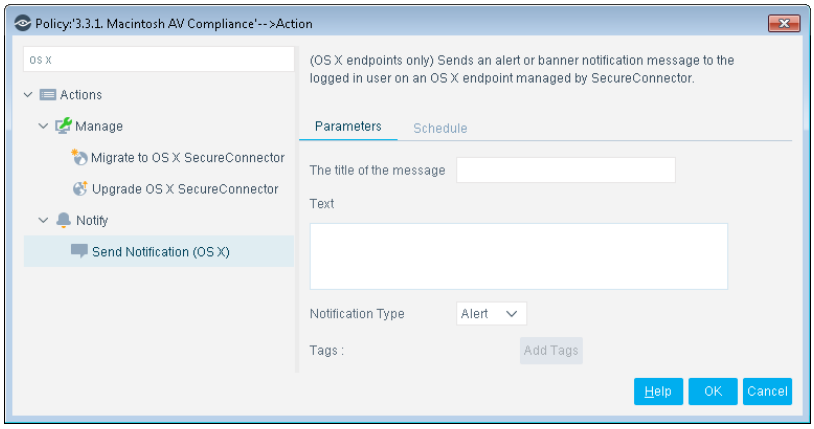
Send Notification (OS X)

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 *Forescout 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.

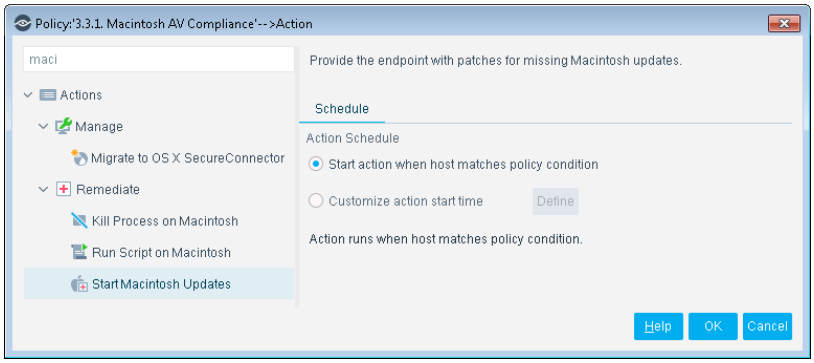


Start Macintosh Updates

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.

If you are using Flexx licensing, ensure that you have a valid *Forescout eyeControl* license to use this action. Refer to the *Forescout Flexx Licensing How-to Guide* for more information about managing licenses.

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



Upgrade OS X SecureConnector

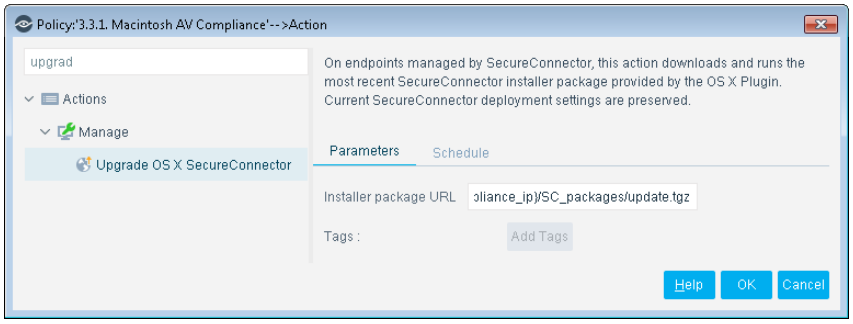
This action applies to endpoints already managed by the OS X Plugin.

> *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 task 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

If, after deploying SecureConnector, the Console shows that particular endpoints are not being managed by SecureConnector, use the following procedures 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 run the following command:

   `fstool osx_test -h <ip> -p <property> [-f <file>] [-c '<command>'] [-t]`

   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.

   `-t` retrieves troubleshooting information from the endpoint.

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. Run the following command:

   fstool osx_test -h <*IP*> -t <*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 Forescout Endpoint Module.

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

- HPS Agent Manager
- HPS Inspection Engine
- Hardware Inventory Plugin
- Linux Plugin

- Microsoft SMS/SCCM Plugin
- OS X Plugin

The Endpoint Module is a Forescout Base Module. Base Modules are delivered with each Forescout release. This module is automatically installed when you upgrade the Forescout version or perform a clean installation of the Forescout platform.

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

Additional Forescout Documentation

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

- Documentation Downloads
- Documentation Portal
- Forescout Help Tools

Documentation Downloads

Documentation downloads can be accessed from the Forescout Resources Page, and one of two Forescout portals, depending on which licensing mode your deployment is using.

- ***Per-Appliance Licensing Mode*** – Product Updates Portal
- ***Flexx Licensing Mode*** – Customer Portal

Software downloads are also available from these portals.

To identify your licensing mode:

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

Forescout Resources Page

The Forescout Resources page provides links to the full range of technical documentation.

To access the Forescout Resources page:

- Go to https://www.Forescout.com/company/resources/, select **Technical Documentation,** and search for documents.

Product Updates Portal

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

To access the Product Updates Portal:

- Go to https://updates.forescout.com/support/index.php?url=counteract and select the version you want to discover.

Customer Portal

The Downloads page on the Forescout Customer Portal provides links to purchased Forescout version releases, Base and Content Modules, and eyeExtend products, as well as related documentation. Software and related documentation only appear on the Downloads page if you have a license entitlement for the software.

To access documentation on the Forescout Customer Portal:

- Go to https://Forescout.force.com/support/ and select **Downloads**.

Documentation Portal

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

To access the Documentation Portal:

- Go to https://updates.forescout.com/support/files/counteract/docs_portal/

Forescout Help Tools

Access information directly from the Console.

Console Help Buttons

Use context-sensitive *Help* buttons to access information about tasks and topics quickly.

Forescout Administration Guide

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

Plugin Help Files

- After installing the plugin, select **Tools** > **Options** > **Modules**, select the plugin, and then select **Help**.

Online Documentation

- Select **Online Documentation** from the **Help** menu to access either the Forescout Resources Page (Flexx licensing) or the Documentation Portal (Per-Appliance licensing).