

## About the 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.

Refer to the relevant configuration guides for detailed information about how to work with and configure components included with this module. See [Additional ForeScout Documentation](#) for information about how to access these guides, and other documentation.

## ForeScout Requirements

This module requires ForeScout version 8.1.

Components described in this document may have additional requirements and dependencies.

## About This Release

This section describes updates and important information related to components delivered in this version of the Endpoint Module.

- [Hardware Inventory Plugin](#)
- [HPS Agent Manager](#)
- [HPS Inspection Engine](#)
- [Linux Plugin](#)
- [Microsoft SMS/SCCM Plugin 2.4](#)
- [OS X Plugin](#)

This release also includes enhancements and fixes provided in previous releases.

## Module-Level Enhancements

### New HPS Agent Manager Plugin

From this release, the Endpoint Module includes a new component. The HPS Agent Manager performs various background functions to support the endpoint discovery and management activities of the Endpoint Module.

Currently, no configuration is required for this component.

### Hardware Inventory Plugin 1.1

There are no feature enhancements or fixed issues for this release.

### Requirements

- The HPS Inspection Engine must be running.

### HPS Agent Manager 1.0

This is a new component in the Endpoint Module, introduced with this release. No configuration is required for this component.

### HPS Inspection Engine 11.0

This section describes important information about the HPS Inspection Engine version 11.0.

### Requirements

- Core Extensions Module version 1.1.0 including the DNS Client Plugin
- The following Content Modules:
  - Windows Applications version 19.0.1
  - NIC Vendor DB version 19.0.2
  - Windows Vulnerability DB version 19.0.1
- (Flexx licensing) A valid Forescout eyeControl (ForeScout CounterACT Control) license, to use enforcement actions provided by the plugin/component. If you do not have this license, these actions will be disabled in the Console. Refer to the *Forescout Flexx Licensing How-to Guide* for more information about managing Flexx licenses and how to request/purchase this license.

## Feature Enhancements

This section describes feature enhancements for this release.

### More Efficient Remote Inspection Connection

This release optimizes attempts to connect to Windows endpoints for Remote Inspection. Typically, several sets of domain credentials are defined in Forescout to support Remote Inspection. Before this release, Forescout stepped through this list until connection succeeded. This caused unnecessary traffic, and sometimes multiple failed logins triggered lockout from endpoints.

From this release, the following logic is used to select credentials for Remote Inspection:

- At first connection, Forescout identifies an endpoint's domain, and starts with credentials in that domain.
- Subsequent connections start with the credentials used in the last successful connection to the endpoint.

### Enhanced Detection- New Host Properties for Windows Users and Processes

Use the following new properties to detect Windows endpoints based on active users and running processes on the endpoint.

<b>Windows Processes Running and User</b>	Indicates a currently active process on a Windows endpoint, and the username/domain of the user that owns the process.
<b>Windows Active Users</b>	Indicates the username/domain of one or more users currently logged in to a Windows endpoint

## Fixed Issues

This section describes fixed issues for this release.

Issue	Description
<b>HPS-4731</b>	In rare cases, after upgrade to CounterACT version 8.0, the Forescout SecureConnector Distribution Tool web page could not generate SecureConnector installer packages for Windows endpoints.
<b>HPS-4857</b>	On Windows Endpoints managed by SecureConnector, scheduled tasks related to scripts run on the endpoint were not handled correctly.

For information about the following fixed issues from the recently released HPS Inspection Engine hotfixes that are incorporated into this plugin version, refer to the following:

- Hotfix 10.8.2.1:

HPS-1729	HPS-4857	HPS-4877	HPS-4917
HPS-4731	HPS-4861	HPS-4906	HPS-4943
HPS-4779	HPS-4867	HPS-4907	

<https://forescout.force.com/support/s/article/Wireless-Plugin-HF-builds-1-8-2-1xxx>

## Known Issues

This section describes known issues for this release.

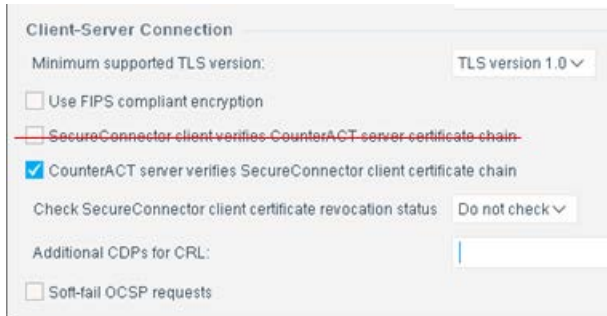
Issue	Description
<b>HPS-1927 62969</b>	The <i>Disable External Device</i> action does not work with Seagate portable external drives.
<b>64724</b>	When the <i>Start SecureConnector</i> action is applied to an endpoint running Windows XP, SecureConnector cannot be installed as a <i>Dissolvable</i> or <i>Application</i> deployment using remote installation.
<b>HPS-2806 73636</b>	This release supports Kerberos authentication for Remote Inspection of endpoints.  When the Forescout platform has previously logged in successfully to an endpoint using Kerberos, and the endpoint is removed from the Domain and then rejoins, the Forescout platform cannot reconnect to the endpoint until the domain controller renews the Ticket-Granting Ticket (TGT) used for Kerberos authentication; typically the TGT is renewed every 10 hours. During this period, resolution of properties and other Remote Inspection tasks are not performed for the endpoint.
<b>HPS-2112 75461</b>	Following removal of SecureConnector, disabled external devices remain disabled.

## Upgrade Considerations

This section describes upgrade considerations for this release.

### Changes to SecureConnector Certificate Options

Previously, configuration options let you require both the SecureConnector client and the Forescout server to present certificates. In this release, one of these options has been removed from the SecureConnector tab of plugin configuration. The **SecureConnector client verifies CounterACT server certificate chain** option is no longer available.



When you upgrade to this release, the existing setting of your environment is preserved. If this option was enabled in your environment before upgrade, Forescout continues to present a certificate to the SecureConnector client during the connection handshake.

### Backward Compatibility

HPS Inspection Engine and SecureConnector share the same version number and are bundled in the release.

This release of the HPS Inspection Engine 11.0 is backward compatible with SecureConnector Versions 10.8.0 (Forescout version 8.0) and 10.8.01 (Forescout version 8.0.1).

- 📖 *Certain features or settings described in this section might differ or not be supported if Forescout 8.1 runs in Certification Compliance mode. Refer to the Forescout Installation Guide for more information about this mode.*

## Linux Plugin 1.4

This section describes important information about Linux Plugin version 1.4.

### Requirements

This section lists requirements for this component.

#### Forescout Requirements

- Endpoint Module version 1.1.0 with the following components:
  - OS X Plugin
  - HPS Inspection Engine
- (Flexx licensing) A valid Forescout eyeControl (ForeScout CounterACT Control) license, to use enforcement actions provided by the plugin/component. If you do not have this license, these actions will be disabled in the Console. Refer to the *Forescout Flexx Licensing How-to Guide* for more information about managing Flexx licenses and how to request/purchase this license.

### Networking Requirements

SecureConnector creates an encrypted tunnel from the endpoint to the Appliance through TCP port 10006. This port must be open on enterprise firewalls to support communication between SecureConnector and the Appliance.

### Endpoint Requirements

When Remote Inspection is used to manage endpoints, Python 2.7 or above is required on endpoints.

Endpoints must run one of the following Linux operating systems:

- CentOS version 6
- Debian version 8
- Fedora version 18
- Kali version 4.6.0 (32 bit)
- Mint version 4.4.4 (64 bit)
- Red Hat Enterprise Linux version 6
- Red Hat Enterprise Linux Desktop version 7
- Red Hat version 7.2
- OpenSUSE version 12
- SUSE Enterprise version 11
- Ubuntu version 12.04

### Feature Enhancements

This section describes feature enhancements for this release.

#### Support for OCSP Certificate Checks

Previous releases let you use CRLs to validate the certificates used in SecureConnector connections. In this release, you can query an OCSP server for the certificate's revocation status, as in the HPS Inspection Engine.

The following configuration options were added to the SecureConnector tab of the plugin configuration screen.

<b>Check SecureConnector client certificate revocation status</b>	<p>Check that the client certificate has not been revoked. From the drop-down menu, select how the client certificate revocation status is determined:</p> <ul style="list-style-type: none"> <li>▪ Using CRL: Check if the certificate is in the Certificate Revocation List (CRL) of the issuing Certificate Authority.</li> <li>▪ Using OCSP: Send an Online Certificate Status Protocol (OCSP) request for the certificate revocation status.</li> </ul>
<b>Soft-fail OCSP requests</b>	<p>When no response is received from the OCSP Responder, the certificate is considered valid. By default, hard-fail is applied.</p>

## Fixed Issues

For information about the following fixed issues from the recently released Linux Plugin hotfixes that are incorporated into this plugin version, refer to the following:

- Hotfix 1.1.0.1:

LNX-404	LNX-470
LNX-451	LNX476
LNX-461	

<https://forescout.force.com/support/s/article/Linux-Plugin-HF-builds-1-1-0-1xxx>

- Hotfix 1.1.0.2:

- LNX-510

<https://forescout.force.com/support/s/article/Linux-Plugin-HF-builds-1-1-0-2xxx>

- Hotfix 1.1.1.1:

- LNX-603

<https://forescout.force.com/support/s/article/Linux-Plugin-HF-builds-1-1-1-1xxx>

- Hotfix 1.2.1.1:

- LNX-618

<https://forescout.force.com/support/s/article/Linux-Plugin-HF-builds-1-2-1-1xxx>

## Known Issues

This section describes known issues for this release.

Issue	Description
<b>LNX-517</b>	The SecureConnector icon does not display in Ubuntu operating systems when Dissolvable or visible daemon deployment is selected. Upon reboot, the icon is visible with visible daemon deployments.

## Microsoft SMS/SCCM Plugin 2.4

There are no fixed issues for this release.

## Requirements

- (Flexx licensing) A valid Forescout eyeControl (ForeScout CounterACT Control) license, to use enforcement actions provided by the plugin/component. If you do not have this license, these actions will be disabled in the Console. Refer to the *Forescout Flexx Licensing How-to Guide* for more information about managing Flexx licenses and how to request/purchase this license.

## Feature Enhancements

This release:

- Supports the ability to enable and disable server certificate validation.
- Supports Certification Compliance mode. For information about this mode, refer to the *ForeScout Installation Guide*.

## OS X Plugin 2.2

This section describes important information about the OS X Plugin version 2.2.

### Requirements

This section lists requirements for this component.

#### ForeScout Requirements

- Endpoint Module version 1.1.0 including the following components:
  - Linux Plugin
  - HPS Inspection Engine
- (Flexx licensing) A valid ForeScout eyeControl (ForeScout CounterACT Control) license, to use enforcement actions provided by the plugin/component. If you do not have this license, these actions will be disabled in the Console. Refer to the *ForeScout Flexx Licensing How-to Guide* for more information about managing Flexx licenses and how to request/purchase this license.

#### 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.

#### Endpoint Requirements

This plugin supports OS X operating software versions 10.8 through 10.13.

## Feature Enhancements

This section describes feature enhancements for this release.

#### Support for OCSP Certificate Checks

Previous releases let you use CRLs to validate the certificates used in SecureConnector connections. In this release, you can query an OCSP server for the certificate's revocation status, as in the HPS Inspection Engine.

The following configuration options were added to the SecureConnector tab of the plugin configuration screen.



<b>Check SecureConnector client certificate revocation status</b>	Check that the client certificate has not been revoked. From the drop-down menu, select how the client certificate revocation status is determined: <ul style="list-style-type: none"> <li>▪ Using CRL: Check if the certificate is in the Certificate Revocation List (CRL) of the issuing Certificate Authority.</li> <li>▪ Using OCSP: Send an Online Certificate Status Protocol (OCSP) request for the certificate revocation status.</li> </ul>
<b>Soft-fail OCSP requests</b>	When no response is received from the OCSP Responder, the certificate is considered valid. By default, hard-fail is applied.

### New Host Property - Track Changes in OSX SecureConnector Connection

The new **OSX SecureConnector Connected/Disconnected** property lets you detect OSX endpoints managed by SecureConnector when SecureConnector establishes a session with CounterACT, or when the session terminates.

### Fixed Issues

For information about the following fixed issues from the recently released OS X Plugin hotfixes that are incorporated into this plugin version, refer to the following:

- Hotfix 2.0.0.1:

OSX-687	OSX-767
OSX-693	OSX-784
OSX-708	OSX-800

<https://forescout.force.com/support/s/article/OSX-Plugin-HF-builds-2-0-0-1xxx>

- Hotfix 2.0.2.1:

- OSX-795
- OSX-819

<https://forescout.force.com/support/s/article/OSX-Plugin-HF-builds-2-0-2-1xxx>

- Hotfix 2.1.0.1:

- OSX-853

<https://forescout.force.com/support/s/article/OSX-plugin-HF-builds-2-1-0-1xxx>

### Known Issues

This section describes known issues for this release.

Issue	Description
<b>OSX-281 72965</b>	When uploading scripts to CounterACT for the <b>Macintosh Expected Script Result</b> property or <i>Run Script on Macintosh</i> action, the file must be formatted with UNIX line endings, otherwise the script execution on the endpoint may fail.

## Backward Compatibility

OS X 2.2 is backward compatible with SecureConnector Version 16.0. However, to take advantage of new functionalities introduced in OS X 2.2/SecureConnector Version 17.0, you must upgrade both components.

## Upgrading the Module


New module releases may become available between ForeScout releases. This section describes how to install the module when a new release becomes available.


### To install the module:

1. Navigate to one of the following ForeScout download portals, depending on the licensing mode your deployment is using:
  - [Product Updates Portal](#) - **Per-Appliance Licensing Mode**
  - [Customer Portal, Downloads Page](#) - **Flexx Licensing Mode**


To identify your licensing mode, select **Help > About ForeScout** from the Console.

2. Download the module **.fpi** file.
3. Save the file to the machine where the Console is installed.
4. Log into the Console and select **Options** from the **Tools** menu.
5. Select **Modules**. The Modules pane opens.
6. Select **Install**. The Open dialog box opens.
7. Browse to and select the saved module **.fpi** file.
8. Select **Install**. The Installation screen opens.
9. Select **I agree to the License Agreement** to confirm that you have read and agree to the terms of the License Agreement, and select **Install**. The installation will not proceed if you do not agree to the license agreement.

 *The installation will begin immediately after selecting Install, and cannot be interrupted or canceled.*

 *In modules that contain more than one component, the installation proceeds automatically one component at a time.*

10. When the installation completes, select **Close** to close the window. The installed module is displayed in the Modules pane.

 *Some components are not automatically started following installation.*

## Module and Component Rollback

The following rollback/upgrade activities are not supported:

- Rolling back this module (or one of its components) to a version released prior to Forescout 8.1.
- If you are running a version of Forescout lower than 8.1 with the corresponding version of this module installed, you cannot upgrade to this module version (or one of its components).

If you upgrade to a newer module or component version that becomes available after this release, you may be able to roll it back. When rollback is supported, the Rollback button is enabled in the Console.

Modules/components on Appliances connected to the Enterprise Manager are rolled back to the selected version. Modules/components on Appliances that are not connected to the Enterprise Manager during the rollback are rolled back when the Enterprise Manager next reconnects to the Appliances.

### To roll back the module or component:

1. Select **Options** from the Console **Tools** menu.
2. Navigate to the **Modules** folder.
3. In the Modules pane, select the module or component to be rolled back.
4. Select **Rollback**. A dialog box opens listing the versions to which you can roll back.
5. Select a version and select **OK**. A dialog box opens showing you the rollback progress.

## Additional Forescout Documentation

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

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

### Documentation Downloads

Documentation downloads can be accessed from the [Forescout Resources Page](#), or one of two Forescout portals, depending on which licensing mode your deployment is using.

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

 *Software downloads are also available from these portals.*

**To identify your licensing mode:**

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

**Forescout Resources Page**

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

**To access the Forescout Resources Page:**

- 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 will only appear on the Downloads page if you have a license entitlement for the software.

**To access documentation on the Forescout Customer Portal:**

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

**Documentation Portal**

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

 *If your deployment is using Flexx Licensing Mode, you may not have received credentials to access this portal.*

**To access the Documentation Portal:**

- Go to [https://updates.forescout.com/support/files/counteract/docs\\_portal/](https://updates.forescout.com/support/files/counteract/docs_portal/) and use your customer support credentials to log in.

**Forescout Help Tools**

Access information directly from the Console.

**Console Help Buttons**

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

***ForeScout Administration Guide***

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

***Plugin Help Files***

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

***Online Documentation***

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

## Contact Information

ForeScout Technologies, Inc.

190 West Tasman Drive

San Jose, CA 95134 USA

<https://www.forescout.com/support/>

Toll-Free (US): 1.866.377.8771

Tel (Intl): 1.408.213.3191

Support: 1.708.237.6591

## About the Documentation

- Refer to the Resources page on the ForeScout website for additional technical documentation: <https://www.forescout.com/company/resources/>
- Have feedback or questions? Write to us at [documentation@forescout.com](mailto:documentation@forescout.com)

## Legal Notice

© 2019 ForeScout Technologies, Inc. All rights reserved. ForeScout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents can be found at <https://www.forescout.com/company/legal/intellectual-property-patents-trademarks>. Other brands, products, or service names may be trademarks or service marks of their respective owners.

2019-06-13 15:14