FORESCOUT

Forescout

Endpoint Module: Linux® Plugin

Configuration Guide

Version 1.5

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

2020-02-13 15:06

Table of Contents

About the Linux Plugin

The Linux Plugin is a component of the Forescout® Endpoint Module. See Endpoint Module Information for details about the module.

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

Each Linux Plugin version provides the latest regularly updated version of SecureConnector™ that is native to Linux.

Accessing and Managing Endpoints

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

Endpoint Module plugins access endpoints to learn detailed information about the endpoint, such as file metadata and operating system information. 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 OS X Plugin interacts with OS X endpoints.

When you configure these plugins, you determine the methods used to access and manage endpoints. When these access methods are successful, the endpoint is resolved as *Manageable*.

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 back to Forescout eyeSight, and implements Forescout 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. Install the Endpoint Module.
3. Make Linux endpoints manageable. The standard Primary Classification policy provided with Forescout identifies Linux endpoints, and assigns these endpoints to the Linux/Unix group. Create a policy that uses the **Linux 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 Linux Endpoints Using Remote Inspection.
   - Deploy SecureConnector on new, unmanaged Linux 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
- Endpoint Requirements

Forescout Requirements

The plugin requires the following:

- Forescout version 8.2.
- Endpoint Module version 1.2 with the following components:
  - OS X 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 10006. This port must be open on enterprise firewalls to support communication between SecureConnector and the Appliance.

Endpoint Requirements

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

Using Remote Inspection to manage endpoints requires Python 2.7 or above. Endpoints must run one of the following Linux operating systems:

- CentOS
- Debian
- Fedora
- Kali
- Mint
- Red Hat Enterprise Linux Workstation/Server
- OpenSUSE
- SUSE Enterprise
- Ubuntu

Supported Operating Systems and Other Vendors

For information about the vendor models (hardware/software) and versions (product/OS) that are validated for integration with this Forescout component, refer to the Forescout Compatibility Matrix.

Configure the Plugin

Configure the plugin to:

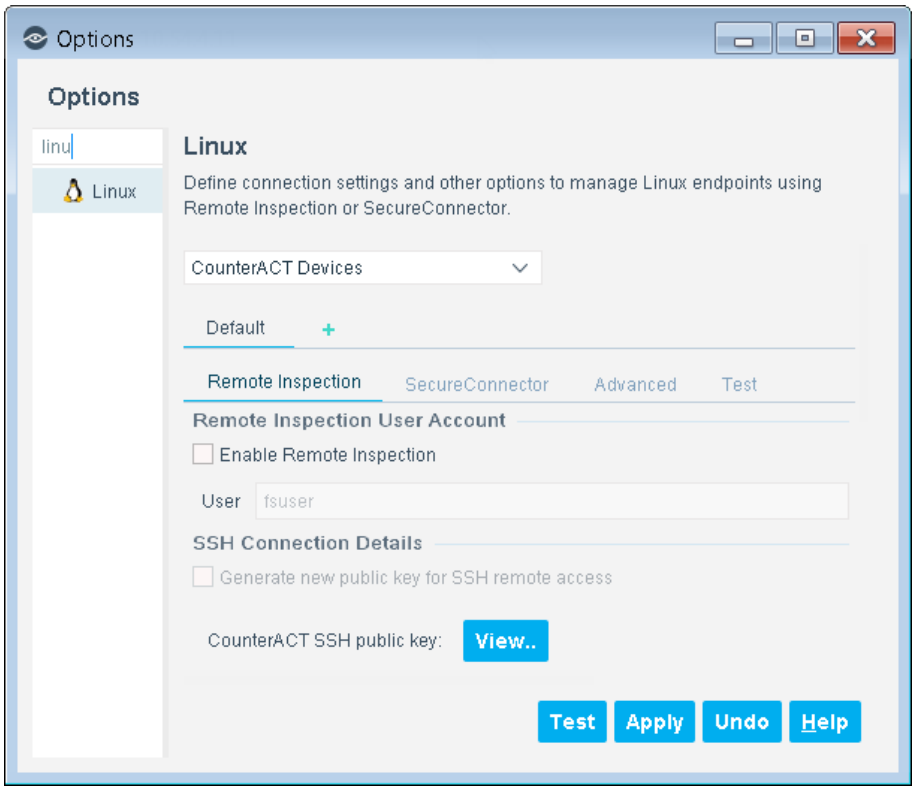
- Define global settings for Remote Inspection and SecureConnector.
- Specify test parameters and test connectivity.

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. Select **Plugins**. In the Plugins pane, select the Linux Plugin, and then select **Configure**.

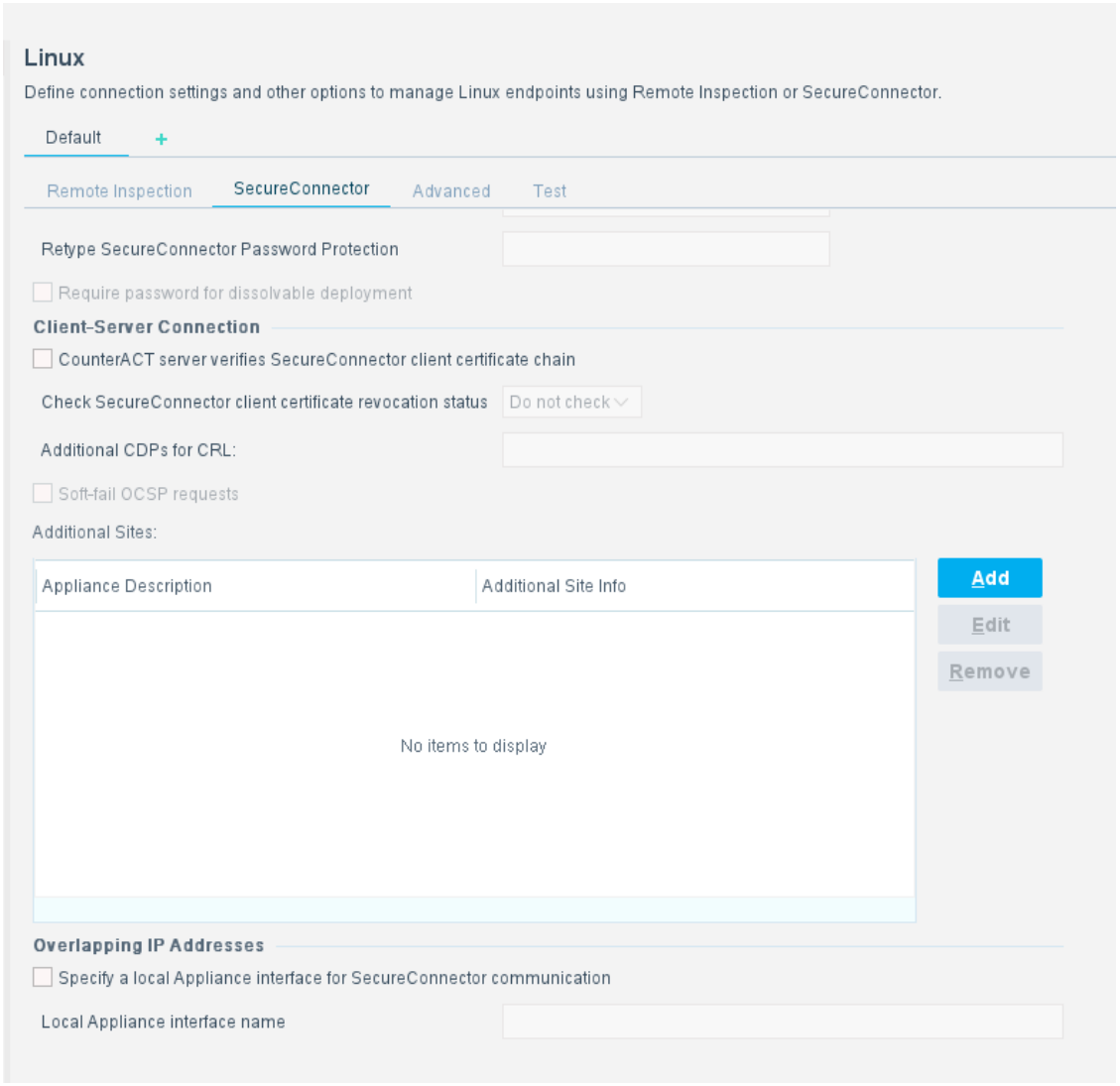


3. In the Remote Inspection tab, define how endpoints are accessed using Remote Inspection.

Enable Remote Inspection	Select this option to enable use of Remote Inspection to poll endpoints for information. Additional fields are relevant only 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 Linux 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 Linux endpoint.

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 works on endpoints.

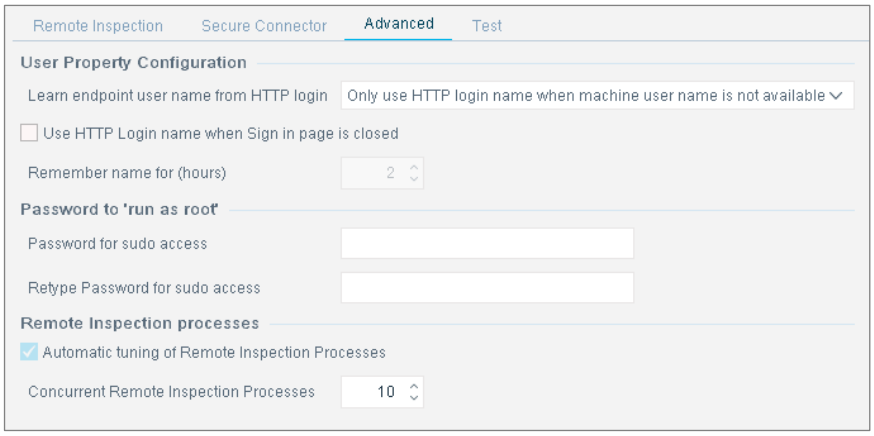


The following settings configure SecureConnector password protection on endpoints:

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 on 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 device 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	Check that the client certificate has not been revoked. From the drop-down menu, select how the client certificate revocation status is determined: ▪ Using CRL: Check if the certificate is in the Certificate Revocation List (CRL) of the issuing Certificate Authority. ▪ Using OCSP: Send an Online Certificate Status Protocol (OCSP) request for the certificate revocation status.
Additional CDPs for CRL	Enter a comma-separated list of CRL distribution points that should be queried.
Soft-fail OCSP requests	When no response is received from the OCSP Responder, the certificate is considered valid. By default, hard-fail is applied.
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.

Specify a local Appliance interface for SecureConnector communication	Each Appliance's installer uses a named local interface for SecureConnector communication. See the *Working with Overlapping IP Addresses How-to Guide* before enabling this option.
Local Appliance interface name	Enter the text label of a local interface on the Appliance. SecureConnector contacts the Appliance through this interface.

5. Select the Advanced tab.



6. In the User Property section, configure the following options:

Learn endpoint user name from HTTP login	Select the method used for learning endpoint user names. This information is used to evaluate the User host property.
Use HTTP Login name when the Sign In page is closed	When this option is selected, the User host property retains the username of the most recent HTTP login session, even after the session is closed – unless a new user login occurs.
Remember name for (hours)	Specify the length of time (in hours) that the plugin retains the HTTP login name when the sign in page is closed. This time is calculated from the last successful login.

7. In the Password to 'run as root' section, configure the following option:

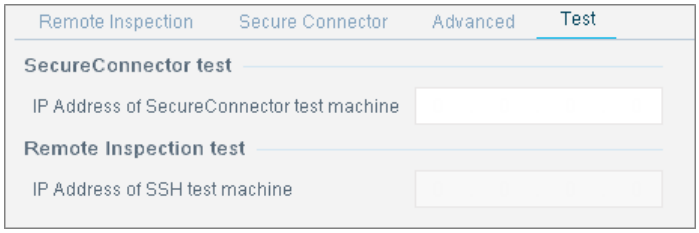
Password for sudo access	The plugin uses the sudo mode when the *Run script as root user on endpoint* option is enabled for the **Run Script on Linux** action or the **Linux Expected Script Result** host property. On endpoints where sudo mode is not password protected, this field is ignored. To use this feature, configure Linux endpoints in your environment to require a fixed sudo password for the user specified in the Remote Inspection configuration tab. For example, you can specify the root password in this field, and add the following line to the /etc/sudoers file: **`Defaults rootpw`**

	On endpoints running variants of Centos Linux, disable the following line in the sudoers file: **`Defaults requiretty`**

8. In the Remote Inspection processes section, configure the following option:

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 of Remote Inspection 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 of Remote Inspection 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.*

9. Select the **Test** tab.



10. Enter an IP address (either IPv4 or IPv6) that defines Linux endpoints used to test the plugin's ability to connect to endpoints. Verify that the following steps were completed on the test endpoint for Remote Inspection:

- The Remote Inspection user defined during plugin configuration exists.
- The public key used by Forescout was installed.

11. Select **Apply** to save settings.

Ensure That the Component Is Running

After installing the component (and configuring it, if necessary), ensure that it is running.

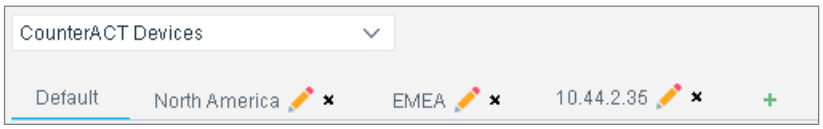
To verify:

1. Select **Tools** > **Options** > **Modules**.
2. Navigate to the component and hover over the name to view a tooltip indicating if it is running on Forescout devices in your deployment. In addition, next to the component name, you will see one of the following icons:
   - - The component is stopped on all Forescout devices.
   - - The component is stopped on some Forescout devices.
   - - The component is running on all Forescout devices.
3. If the component is not running, select **Start**, and then select the relevant Forescout devices.
4. Select **OK**.

Configuration for an Appliance or Group of Appliances

You can create 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.
- To locate the configuration that applies to a device, select the device in 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 Linux 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 Linux 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 Linux 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 Linux endpoints. Refer to the *Forescout Administration Guide* and the *HPS Inspection Engine Configuration Guide* for more information about SecureConnector.

SecureConnector Deployment Options

SecureConnector can be implemented on the endpoint as a dissolvable executable, a permanent application, or a service.

- A dissolvable executable runs once on installation, and does not run again after the user logs out or the machine is rebooted.
- When installed as a permanent application, SecureConnector will run every time the user logs in, and in some cases as soon as the machine boots.

  Deployment as a permanent application is only available for Windows endpoints.

- When installed as a permanent service, SecureConnector will run when the machine boots.

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

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

- Visible deployment - a SecureConnector icon appears in the task bar.
- Invisible deployment – no icon appears in the task bar. SecureConnector is invisible on the desktop.

  Some operating system distributions may not support the SecureConnector icon.

Deploying SecureConnector

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

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

For appliances that are configured with overlapping IP addresses, SecureConnector installers are not uniform across the network. In each overlapping site, SecureConnector must be downloaded from an Appliance in the site. SecureConnector can only communicate with this Appliance. For more information, see the Working with Overlapping IP Addresses How-to Guide.

Interactive Installation – the Start SecureConnector Action

The Start SecureConnector action installs SecureConnector on endpoints detected by a Forescout 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/system daemon, or as a dissolvable executable
- Whether the SecureConnector icon is visible in the task bar

When the **Start SecureConnector** action is applied to Linux endpoints, configure the following action options as follows:

Install Method	Only the **HTTP installation at the endpoint** installation method is supported.
Deployment Type	Only the **Install Dissolvable** and **Install Permanent as Service** options are supported for Linux endpoints.

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

Background Installation of SecureConnector

This procedure installs SecureConnector on endpoints with no user interaction. Use this procedure for fresh (scratch) installation on endpoints.

You can use third-party endpoint management utilities to perform this procedure.

To install SecureConnector in the background:

1. Copy the installer file corresponding to the type of SecureConnector deployment you want to distribute from Enterprise Manager. See SecureConnector Deployment Options.

2. Distribute this file to target endpoints.
3. Use the command line interface or a script to perform the following on the endpoint:
   a. Unpack the archive.
   b. Install SecureConnector.

      Use the **`install.sh`** command to install SecureConnector as a system daemon.

      Use the **`run.sh`** command to run SecureConnector as a dissolvable executable.

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

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*.

Stopping SecureConnector on the Endpoint

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

- End users can select the SecureConnector toolbar icon, and then select **Exit**.
  - When SecureConnector is installed as a service/daemon, this stops SecureConnector for the current session. The daemon runs at the next session.
  - When SecureConnector runs as a dissolvable executable, this stops and removes SecureConnector.
- End users can use the following command to uninstall SecureConnector from their device:

  `bash /usr/lib/forescout/Uninstall.sh`

When you configure the plugin, you can enable password protection for SecureConnector on endpoints. When password protection is enabled, users who try to stop or uninstall SecureConnector are prompted for a password.

SecureConnector Details

Item	Detail
Size on disk	20 MB.
Installation type	System daemon or dissolvable. Defined in the **Start SecureConnector** action.

Item	Detail
Visibility options (systray icon)	Visible 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.
SecureConnector privilege level:	Daemon installation: root privilege. Dissolvable installation: user privilege.
Daemon/service installation folder	The default installation directory is /usr/lib/forescout/.
Dissolvable installation folder	The folder where the installation package is deposited, and from which the Run.sh script runs.
Daemon/serviced script folder	/tmp/
Dissolvable script folder	/tmp/
Starts on boot	Daemon/service mode: Yes. Dissolvable mode: No. Installation mode is set in the Start SecureConnector action.

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.
   b. From the command line prompt, submit the following command:
      `fstool linux additional_sites`
   c. 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.

Using Certificates to Authenticate the SecureConnector Connection

When an endpoint managed by SecureConnector accesses the network, the SecureConnector client on the endpoint connects to the CounterACT Appliance that manages the endpoint. This client-server connection is secured using X.509-compliant public key certificates, as follows:

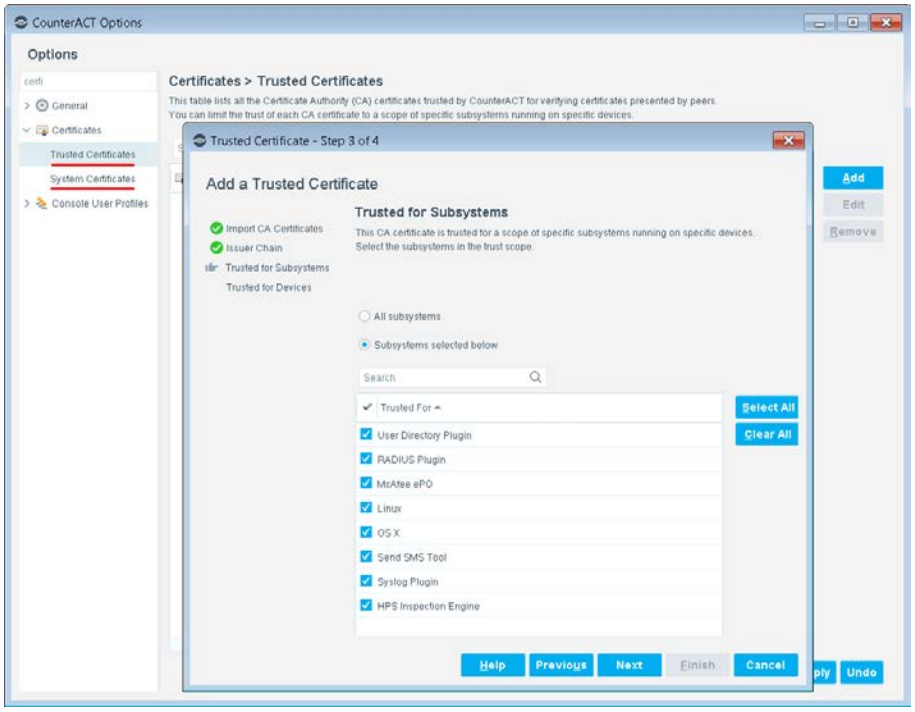
- The CounterACT Appliance presents a server-side certificate that is used by the SecureConnector client to authenticate the connection. *To work with SecureConnector, trust chain(s) and certificate(s) for this authentication* ***must*** *be imported at the Forescout Console.*

  When multi-domain certificates are used, SecureConnector authenticates the server-side certificate using the Subject Alternate Name (SAN) extension field in addition to the Subject Common Name field.

- When Forescout runs in Certification Compliance mode, optional configuration settings let you require a client-side certificate. When this option is enabled, SecureConnector on endpoints must present a certificate to the CounterACT Appliance. Refer to the *Forescout Installation Guide* for more information about Certification Compliance mode.

Use the Trusted Certificates and System Certificates panes of the Console to install required trust chains and certificates in Forescout. Specify the relevant plugins of the

Endpoint Module when you configure the Scope/Subsystem fields. For details, refer to the *Forescout Administration Guide*.



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*. See Additional Forescout Documentation for information about how to access this guide.

Create Custom Policies

Use the properties and actions provided by this plugin to detect and handle endpoints. Define policy conditions based on property values, and specify actions that are applied to endpoints that match the conditions.

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.

Forescout *actions* let you manage and 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. Log in to the Forescout Console.
2. On the Console toolbar, select the **Policy** tab. The Policy Manager opens.
3. Select **Add** to create a policy.

Detecting Linux Devices – Policy Properties

The Linux Plugin supports the following properties for Linux endpoints.

Linux Expected Script Result	Runs a command or file that detects specific endpoint attributes, statuses, or any other information, or to carry out actions on endpoints. All file extensions are supported and can be run. The Run Scripts on Linux action is also available. The plugin can use the sudo utility when super-user access is required to run scripts on endpoints. See Configure the Plugin.
Linux File Date	Indicates the last modification date and time of a defined file on an endpoint.
Linux File Exists	Indicates whether a specified file exists on an endpoint.
Linux File Size	Indicates the size (in bytes) of a specified file on an endpoint.
Linux Hostname	Indicates the Linux host name.
Linux Manageable (SSH Direct Access)	Indicates whether the endpoint is connected to the Forescout platform via SSH and is manageable via Remote Inspection.

Linux Manageable (SecureConnector)	Indicates whether the endpoint is connected to the Forescout platform via SecureConnector.
Linux Processes Running	Indicates the full pathnames of processes running on an endpoint.
Linux SecureConnector Version	Indicates the version of the SecureConnector package running on the endpoint.
Linux User	Indicates all the users logged in to the endpoint. The list of usernames is comma-separated.
Linux Version	Indicates the specific version of Linux 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 Linux endpoints.
User	This is a general Forescout property. For Linux 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 Linux Devices – Policy Actions

This section describes the actions supported by the Linux Plugin.

The plugin implements the following general actions on Linux endpoints managed by SecureConnector. Refer to the *Forescout Administration Guide* for details.

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

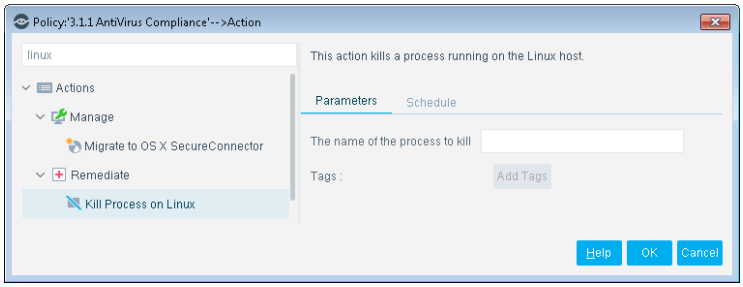
In addition, this plugin provides the following actions specific to Linux endpoints.If you are using Flexx licensing, ensure that you have a valid Forescout eyeControl license to use these actions. Refer to the *Forescout Flexx Licensing How-to Guide* for more information about managing licenses.

- Kill Process on Linux
- Run Scripts on Linux

Kill Process on Linux

This action halts specific Linux 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** option. For example, if you enter the {user} tag, the user name

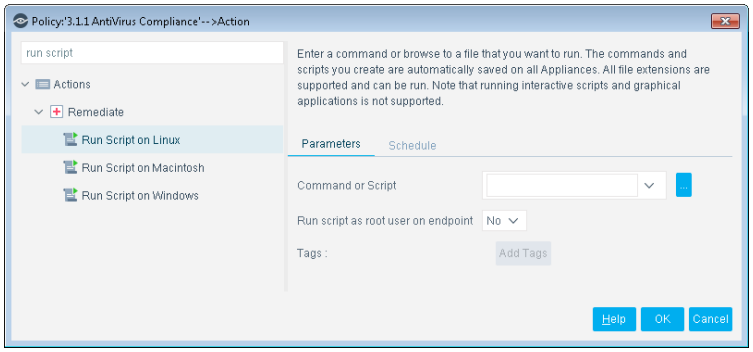
of the endpoint is automatically inserted into the process name. See the *Forescout Administration Guide* for details.



Run Scripts on Linux

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 on the endpoint, enter its absolute path. You can use property tags to include endpoint-specific or user-specific values. 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) If the script requires root/super user access, set the **Run script as root user on endpoint** option to *Yes*.

   The plugin uses the sudo utility when super user access is required to run scripts on Linux endpoints. See Configure the Plugin.

   This action completes successfully when the script launches on the endpoint, whether or not the script returns a value or successfully runs to conclusion.

Endpoint Module Information

The Linux 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 Technical Documentation 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 Support Portal

Software downloads are also available from these portals.

To identify your licensing mode:

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

Forescout Technical Documentation Page

The Forescout Technical Documentation Page provides access to a searchable, web-based Documentation Portal as well as PDF links to the full range of technical documentation.

To access the Technical Documentation Page:

- Go to https://www.Forescout.com/company/technical-documentation/

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 Support Portal

The Downloads page on the Forescout Customer Support 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 Customer Support 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 quickly access information about the tasks and topics you are working with.

Forescout Administration Guide

- Select **Administration Guide** from the **Help** menu.

Plugin Help Files

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

Documentation Portal

- Select **Documentation Portal** from the **Help** menu to access the Documentation Portal.

Appendix 1: Troubleshooting Management of Linux Endpoints

If, after deploying SecureConnector, the Console shows that particular endpoints are not being managed by SecureConnector, verify that SecureConnector is running on the affected endpoints.

For Daemon Installation

Run the following command on the endpoint:

ps auxww | egrep 'ForeScoutSecureConnector'

The resulting output provides the following information (for daemon installation):

- Confirms that SecureConnector daemon process is running by listing the **ForeScoutSecureConnector.bin -daemon** process. See line 5 in the example below.
- Confirms that SecureConnector daemon process is running by listing the **ForeScoutSecureConnector.bin -agent** process. See line 7 in the example below.
- Confirms that the daemon is active by listing the following process:

  /usr/local/bin/daemon --respawn --name SecureConnector --pidfiles /var/run --stdout daemon.info --stderr daemon.err -- /usr/lib/forescout/bin/ForeScoutSecureConnector

  See line 3 in the example below.

In addition, you can verify that the daemon is running by running the following command:

service SecureConnector status

SecureConnector log files are located on the endpoint at:

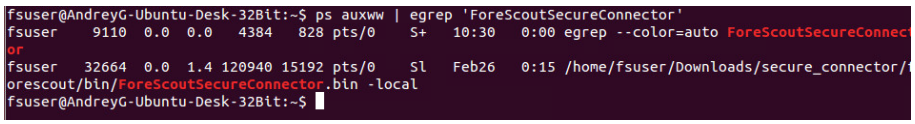
/usr/lib/forescout/bin/log/fs_sc.log

For Dissolvable Installation

Run the following command on the endpoint:

ps auxww | egrep 'ForeScoutSecureConnector'

This command should produce a listing similar to the following:



SecureConnector log files are located on the endpoint at:

<*SC_running_path***>/forescout/bin/log/fs_sc.log**

Appendix 2: Linux Commands Used by the Plugin

This section lists Linux commands used by the Linux Plugin. The commands used depend on the actions to be performed on the endpoint. This may affect the minimum privilege requirements for Forescout as configured at the Appliance.

The plugin can use the sudo utility when super-user access is required to run scripts on Linux endpoints, such as when the **Run script as root user on endpoint** option is enabled for the **Run Script on Linux** action or the **Linux Expected Script Result** host property.

The following Linux commands are used to resolve properties and for actions by all inspection methods:

- **`cat /etc/issue;uname –rs`**: Operating system
- **`hostname`**
- **`killall`**: Process termination
- **`ps -eo command c`**: Processes
- **`stat –t`**: File-relevant properties
- **`who`**: Logged in users

SecureConnector uses the following set of Linux commands:

awk	grep	ls	nohup
cd	kill	mv	ps axwwo pid, ppid, command
chmod	ln	netstat –nlp	rm, rm -rf