ForeScout CounterACT® Linux Plugin

Configuration Guide

Version 1.1.0
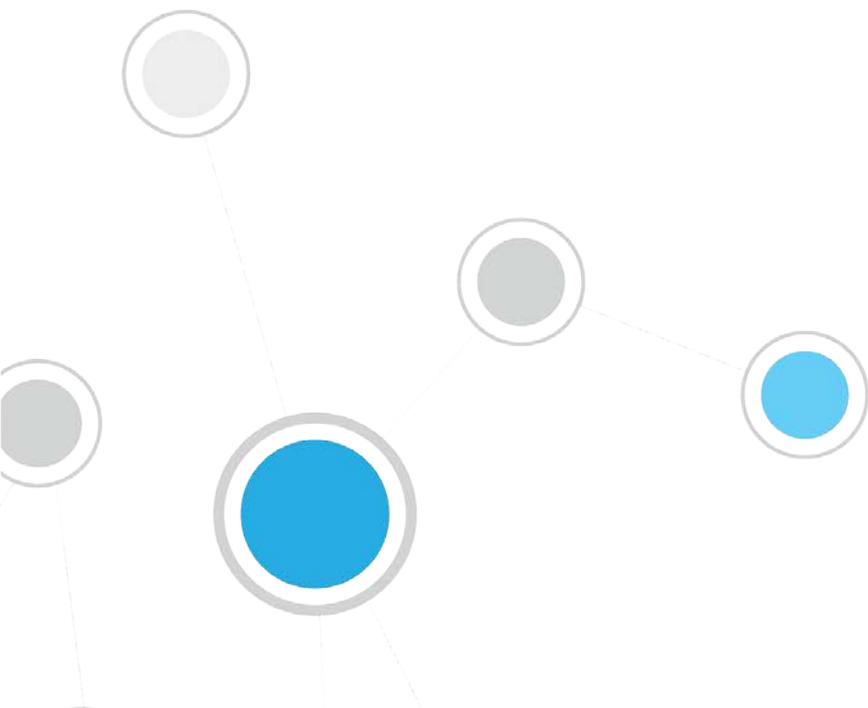
Table of Contents

About This Plugin

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.

Replacing Macintosh/Linux Property Scanner Plugin Functionality

With the release of this plugin, development of the Macintosh/Linux Property Scanner is discontinued, and its endpoint management functionality is replaced by the following plugins:

- Linux Plugin (this plugin) for managing endpoints running a Linux operating system
- OS X Plugin for managing endpoints running a Macintosh operating system

This plugin supersedes the Macintosh/Linux Property Scanner Plugin.

Accessing and Managing Endpoints

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

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

The plugin provides the following methods to access endpoints:

- Remote Inspection
- SecureConnector

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

Remote Inspection

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

Agentless

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

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

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

- Linux Manageable (SSH Direct Access)

- Macintosh Manageable (SSH Direct Access)

- Windows Manageable Domain

- Windows Manageable Domain (Current)

- Windows Manageable Local

SecureConnector

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

Agent-Based

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

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

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

- Linux Manageable (SecureConnector)

- Macintosh Manageable (SecureConnector)

- Windows Manageable SecureConnector

- Windows Manageable SecureConnector (via any interface)

What to Do

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

1. Verify that you have met system requirements. See Requirements.

2. Install the Plugin.

3. (Managed endpoints only) Redirect managed Linux endpoints to the Linux Plugin. Previously, the Macintosh/Linux Property Scanner Plugin supported interaction with Linux endpoints. When you install the Linux Plugin:

   - Linux endpoints managed using Remote Inspection pass automatically to the control of the Linux Plugin.

     The Linux Plugin uses the same public and private keys for Remote Inspection as the Macintosh/Linux Property Scanner did. During installation, the Linux Plugin copies these certificates and keys from the Macintosh/Linux Property Scanner.

After installation of the Linux Plugin, Remote Inspection settings of the Macintosh/Linux Property Scanner no longer affect Linux endpoints; you can recreate these settings or customize Remote Inspection settings for Linux endpoints when you Configure the Plugin.

– Linux endpoints managed using SecureConnector are still managed by the Macintosh/Linux Property Scanner Plugin, and still run the last version of SecureConnector that they received from the Macintosh/Linux Property Scanner Plugin. Create a policy using the Migrate Linux SecureConnector Policy Template that detects these endpoints and passes them to the control of the Linux Plugin. After this one-time migration, the Linux Plugin supports all Linux endpoints managed by SecureConnector.

4. Make Linux endpoints manageable. The standard *Asset Classification and Primary Classification* policies provided with CounterACT identify Linux endpoints, and assign 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 by CounterACT.

– To make an endpoint manageable by Remote Inspection, use your network's administrative tools to define a user account on the endpoint, and use the network's PKI to distribute the public key used for Remote Inspection connections to the endpoint. See Managing 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.

5. Create Custom Policies that use the properties and actions provided by this plugin to manage endpoints.

Requirements

This section describes system requirements, including:

▪ CounterACT Requirements

▪ Networking Requirements

▪ Endpoint Requirements

CounterACT Requirements

The plugin requires the following CounterACT releases and other components:

▪ CounterACT version 7.0.0

▪ Service Pack 2.3.3 or above
Install the latest Service Pack to take advantage of the most current updates.

▪ Macintosh/Linux Property Scanner 7.0.1 or above

▪ OS X Plugin 2.0.0 or above

▪ HPS Inspection Engine 10.7.0 or above

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 CounterACT.

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 or above
- Debian version 8 or above
- Fedora version 18 or above
- Red Hat Enterprise Linux version 6 or above
- Red Hat Enterprise Linux Desktop version 7 or above
- Red Hat version 7.2 or above
- OpenSUSE version 12 or above
- SUSE Enterprise version 11 or above
- Ubuntu version 12.04 or above

Install the Plugin

CounterACT is delivered with several bundled plugins, including this plugin.

New plugin functionality and supporting data may become available independently between major CounterACT version releases. This section describes how to install the plugin when a new plugin version becomes available between releases.

To install the plugin:

1. Navigate to the Customer Support, Base Plugins page and download the plugin `.fpi` file.

2. Save the file to the machine where the CounterACT Console is installed.

3. Log into the CounterACT Console and select **Options** from the **Tools** menu.

4. Select **Plugins**. The Plugins pane opens.

5. Select **Install**. The Open dialog box opens.

6. Browse to and select the saved plugin `.fpi` file.

7. Select **Install**.

8. An installation or upgrade information dialog box and a license agreement dialog box will open. Accept the license agreement to proceed.

9. Once the installation is complete, select **Close**. The plugin is listed in the Plugins pane.

# 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 CounterACT Console, select **Options** from the **Tools** menu.

2. Select **Plugins**. In the Plugins pane, select the Linux Plugin. Select **Configure**.
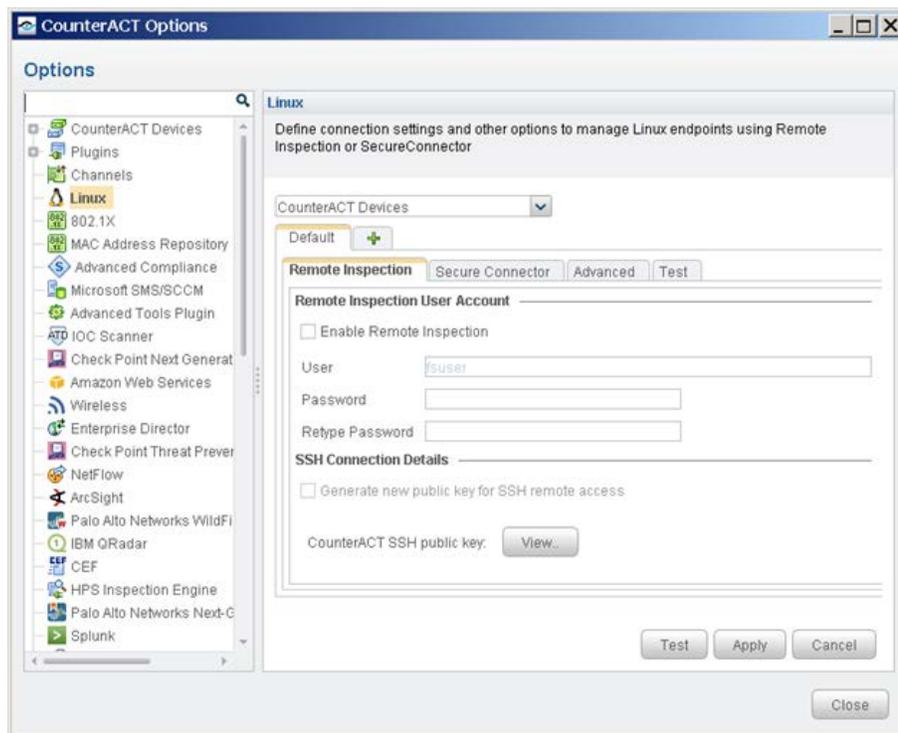
3. In the Remote Inspection tab, the following options control how CounterACT accesses endpoints by Remote Inspection.

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

Enable Remote Inspection	Select this option to enable use of Remote Inspection to poll endpoints for information. The other fields of this tab are only relevant if Remote Inspection is used in your environment.
	If you are not managing OS X endpoints using Remote Inspection, disable this option to avoid unnecessary SSH network traffic. See Managing Linux Endpoints Using Remote Inspection.
User	Specify an administrator user account that is used to establish an SSH connection with endpoints. This user account must be defined on each Linux endpoint.
Password	
Retype Password	
Generate new public key for remote SSH access	Select this option and select **Apply** to change the public key. The plugin changes the public key of the Enterprise manager, and synchronizes all Appliances with the new key.
	You must distribute the new key to endpoints using one of the methods described in Distribute the Public Key.
	Consult your PKI/network security team to determine how frequently this key should be regenerated.
CounterACT SSH public key	Select **View** to see the public key CounterACT uses for the SSH connection to endpoints. This key must be distributed to endpoints. See Distribute the Public Key for details.

4. Select the SecureConnector tab. These options control how SecureConnector works on endpoints.

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

Enable SecureConnector Password Protection	When this option is selected, endpoint users must enter the password you specify here to exit SecureConnector on their endpoints. See Stopping SecureConnector on the Endpoint.

Enter SecureConnector Password Retype SecureConnector Password	Enter the identical string into both fields to define the password that allows users to exit SecureConnector.
Require password for dissolvable deployment	When this option is selected, SecureConnector that runs as a dissolvable application is also password protected: to exit SecureConnector without logging out of the endpoint, a password is required.

5. Select the Advanced tab.

a. Configure the following options.

Learn endpoint user name from HTTP login	Indicates 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	Unless a new user login occurs, the User host property retains the username of the most recent HTTP login session, even after the session is closed.
Remember name for (hours)	Indicates how long the plugin retains the HTTP login name when the sign in page is closed. This time is calculated from the last successful login.

b. 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`

6. Select the Test tab.

7. Enter the IP addresses of endpoints that are 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 CounterACT was installed.

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

Configuration for an Appliance or Group of Appliances

You can create and apply plugin 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 plugin configurations, see the *Console User Manual*.

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

Perform this procedure to make newly detected Linux endpoints manageable by Remote Inspection.

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.

> 📄 *When you first install this plugin, it recognizes public keys already installed on existing endpoints that were managed by the Macintosh/Linux Property Scanner Plugin. There is no need to redistribute the public key to these endpoints.*

To create a script to distribute the public SSH key:

1. In the CounterACT Console, open the plugin configuration pane. See Configure the Plugin.

2. In the Remote Inspection tab, select the **View** button in the **CounterACT SSH Connection Details** area of the tab.

3. Copy the key to a clipboard or another application.

4. Write a script which does the following on each endpoint you want to manage via Remote Inspection:

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

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

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

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

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

   ```
   chmod 644 authorized_keys
   ```

Managing Endpoints Using SecureConnector

This section describes how to use SecureConnector to query and manage Linux endpoints. Refer to the CounterACT *Console User Manual* 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 menu bar.

- Invisible deployment – no icon appears in the menu 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

📄 *To migrate Linux endpoints managed by the Macintosh/Linux Plugin using legacy versions of SecureConnector, see Migrate Linux SecureConnector Policy Template.*

Interactive Installation – the Start SecureConnector Action

The *Start SecureConnector* action installs SecureConnector on endpoints detected by a CounterACT policy. Endpoints are redirected to the HTML page, where end users can download the appropriate installer package.

You can specify interaction and installation settings including:

- The text displayed to prompt end users to install the package
- Whether SecureConnector is deployed as a permanent service/system daemon, or as a dissolvable executable
- Whether the SecureConnector icon is visible in the menu 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 *Console User Manual* 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.

📄 *You can use third party endpoint management utilities to implement the procedure described here.*

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 *Console User Manual* or online Help.

Stopping SecureConnector on the Endpoint

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

- 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 also 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	20MB.
Installation type	System daemon or dissolvable. Defined in the **Start SecureConnector** action.
Visibility options (systray icon)	Visible and 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/.

Item	Detail
Dissolvable installation folder	The folder to which the installation package was 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.

Certificate Based Rapid Authentication of Endpoints

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

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

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

- Corporate endpoints and other trusted endpoints managed by SecureConnector immediately initiate certificate-based authentication as part of SecureConnector's TLS interaction with CounterACT. Endpoints are granted immediate network access based on a signed X.509 digital certificate. CounterACT continues the compliance checks defined in active policies, and may revoke or change endpoint access if these checks fail.

- A corporate policy may grant limited network access to endpoints without a valid rapid authentication certificate, or with an expired or revoked certificate, or endpoints not managed by SecureConnector, until normal, policy-driven compliance checks are run.

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

Run Policy Templates

This plugin provides the following policy template:

- Migrate Linux SecureConnector - this template generates a policy that detects Linux endpoints managed by SecureConnector, and migrates them to the control of the Linux Plugin. Create and run this policy after you install the Linux Plugin.

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

Migrate Linux SecureConnector Policy Template

This template generates a policy that detects Linux endpoints managed by SecureConnector, and migrates them to the control of the Linux Plugin. Create and run this policy after you install the Linux Plugin.

The main rule of this policy selects Linux endpoints that are managed using SecureConnector.

Sub-rules of the policy run scripts on Linux endpoints to upgrade SecureConnector on the endpoints. This upgrade uninstalls the legacy SecureConnector package that was installed by the Macintosh/Linux Property Scanner Plugin, and installs the SecureConnector for Linux release provided with the Linux Plugin.

After successful upgrade, Linux endpoints managed by SecureConnector interact with the Linux Plugin.

📄 *By default, policies created with this template install SecureConnector as a permanent service with a visible menu bar icon. See SecureConnector Deployment Options.*

Prerequisites

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

Run the Template

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

To run the template:

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

Name the Policy

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

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

Naming Tips

– Make sure names are accurate and clearly reflect what the policy does. For example, do not use a generic name such as My_Compliance_Policy.

– The name should indicate what the policy verifies and what actions are taken.

– The name should indicate whether policy criteria must be met or not met.

– Avoid having another policy with a similar name.

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

Define Which Hosts Will Be Inspected - Policy Scope

The Scope pane and IP Address Range dialog box let you define a range of endpoints to be inspected for this policy.
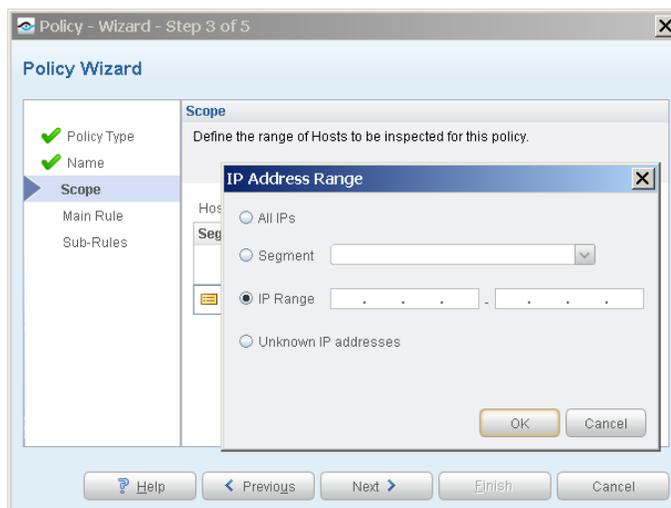
7. Use the IP Address Range dialog box to define which endpoints are inspected. The following options are available for defining a scope:

– **All IPs**: Include all addresses in the Internal Network. The Internal Network was defined when CounterACT was set up.

– **Segment**: Select a previously defined segment of the network. To specify multiple segments, select **OK** to close the IP Address Range dialog box, and select **Segments** from the Scope page.

– **IP Range**: Define a range of IP addresses. These addresses must be within the Internal Network.

– **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address. Not applicable for this policy template.

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

8. Select **OK**. The added range appears in the Scope pane.

9. Select **Next**.

10. Select **Finish**. The policy is created.

How Devices are Detected and Handled

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

Hosts that match the Main Rule pass to sub-rules of the policy for further evaluation. *Hosts that do not match the Main Rule are not passed to sub-rules of the policy*. Sub-rules allow you to automatically 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 selects Linux endpoints that are managed using SecureConnector. 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 run a script on Linux endpoints to upgrade SecureConnector on the endpoints, and check for successful result. The upgrade script first installs the new SecureConnector for Linux release provided with the Linux Plugin, and then uninstalls the legacy SecureConnector package installed by the Macintosh/Linux Property Scanner. After successful upgrade, Linux endpoints managed by SecureConnector interact with the Linux Plugin.

1. Install SecureConnector

   This rule detects endpoints on which the new SecureConnector for Linux release provided by the Linux Plugin is not installed or running. The script used to evaluate the endpoint installs this new SecureConnector release, if necessary.

2. Uninstall failed, install successful

   This rule detects endpoints on which the latest version of SecureConnector for Linux was successfully installed, but the legacy version of SecureConnector was not uninstalled.

3. Migration Successful

This rule detects endpoints running the latest version of SecureConnector for Linux.

4. Upgrade Failed

This rule detects endpoints on which the latest version of SecureConnector for Linux was not successfully installed, or the legacy version of SecureConnector was not uninstalled.

Create Custom Policies

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

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

CounterACT *actions* let you instruct CounterACT how to control detected devices. For example, assign a detected device to a quarantine VLAN or send the device user or IT team an email.

For more information about working with policies, select **Help** from the policy wizard.

To create a custom policy:

1. Log in to the CounterACT 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	Use this property to run a command or file that will detect certain 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 Script 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 CounterACT via SSH and is manageable via Remote Inspection.

Linux Manageable (SecureConnector)	Indicates whether the endpoint is connected to CounterACT 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 that is 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 CounterACT property for Linux endpoints.
User	This is a general CounterACT 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 that are supported by the Linux Plugin.

The plugin implements the following general actions on Linux endpoints managed by SecureConnector. Refer to the *Console User Manual* for details of these actions.

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

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

- Kill Process on Linux
- Run Script 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** button. For example, if you enter the {user} tag, the user name of the endpoint is automatically inserted into the process name. See the CounterACT *Console User Manual* for details.
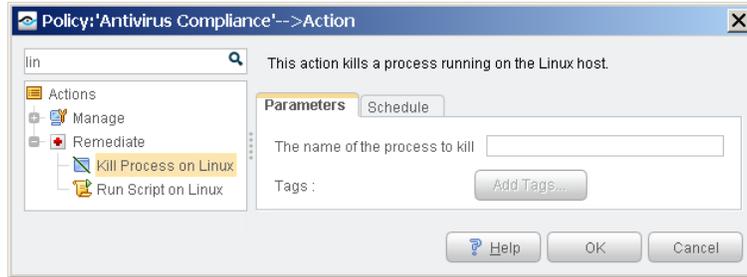
Run Script on Linux

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.
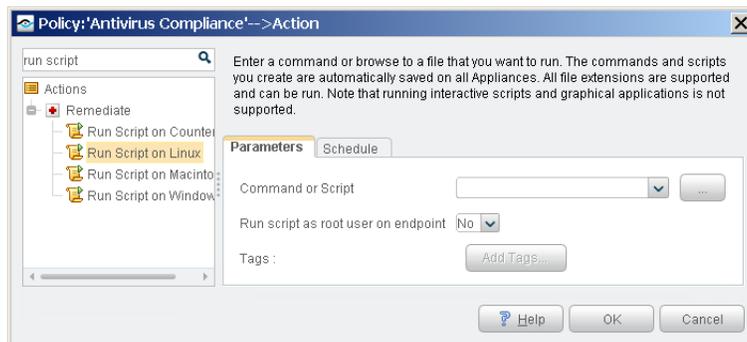
1. Specify a command or script to run on endpoints. Do one of the following:

   – 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 *Console User Manual*.

   – Select the Continue button to select from the repository of user-defined scripts and commands. See the *CounterACT Console User Manual* for more information about user-defined scripts.

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.*

Appendix 1: Troubleshooting Management of Linux endpoints by SecureConnector

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 you with 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.

```
[admin@shlomos-rh1 Desktop]$ ps auxww | egrep 'ForeScoutSecureConnector'
admin   31703  0.0  0.0 108040   884 pts/0   S+   10:08   0:00 egrep --color=auto ForeScoutSecureConnector
root    31796  0.0  0.0  10796   520 ?        S    Feb27   0:00 /usr/local/bin/daemon --respawn --name SecureConnector --pidfiles /var/run
--stdout daemon.info --stderr daemon.err -- /usr/lib/forescout/bin/ForeScoutSecureConnector
root    31806  0.0  0.6 226764 13880 ?        S    Feb27   0:06 /usr/lib/forescout/bin/ForeScoutSecureConnector.bin -daemon
root    31828  0.0  0.1 282388  2948 ?        S    Feb27   0:00 su -c /usr/lib/forescout/bin/ForeScoutSecureConnectorAgent -s /bin/sh admin
admin   31834  0.0  0.6 423936 14168 ?        Ssl  Feb27   0:00 /usr/lib/forescout/bin/ForeScoutSecureConnector.bin -agent
[admin@shlomos-rh1 Desktop]$
```

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

`service SecureConnector status`

```
[admin@shlomos-rh1 Desktop]$ service SecureConnector status
daemon:  SecureConnector is running (pid 31796)
[admin@shlomos-rh1 Desktop]$
```

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 Property Scanner Plugin. Commands are used depending on the actions that are to be performed on the endpoint. This may affect the minimum privilege requirements for CounterACT as configured at the Appliance.

The plugin can use the sudo utility when super user access is required to run scripts on Linux endpoints, 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

Additional CounterACT Documentation

For more detailed information about the CounterACT features described here or additional CounterACT features and plugins, refer to the following resources.

Documentation Portal

The ForeScout Documentation Portal is Web-based library containing information about CounterACT tools, features and functionality, and integrations.

To access the Documentation Portal:

1. Go to www.forescout.com/kb.

2. Use your customer support credentials to log in.

3. Select the CounterACT version you want to discover.

Customer Support Portal

The Customer Support Portal provides links to CounterACT version releases, hotfixes, plugins and modules as well as related documentation. The portal also provides a variety of How-to Guides, Installation guides and more.

To access the Customer Portal:

1. Go to https://updates.forescout.com/support/index.php?url=counteract.

2. Select the CounterACT version you want to discover.

CounterACT Console Help Tools

Access information directly from the CounterACT Console.

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

- *Console User Manual*
  Select **CounterACT Help** from the **Help** menu.

- *Installed Plugins Help*
  Select **Options** from the **Tools** menu and then select **Plugins**. Select a plugin and then select **Help**.

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

Legal Notice