



CounterACT ArcSight Plugin Configuration Guide

Version 2.5.0 and Above





Table of Contents

- About the CounterACT ArcSight Plugin 3**
 - HP ArcSight Asset Connector Server Integration 3
 - Message Send/Receive Flow 4
 - Appliance/Enterprise Manager Architecture 4
 - What You Need Do 5
 - Plugin Module Licensing 5
 - Module Capacity 5
 - More License Information 6
- Requirements 7**
- Installation 7**
 - CounterACT ArcSight Plugin 7
 - ArcSight SmartConnector Plugin 7
 - Install the Plugin 7
 - Define Target Asset Connector Servers 9
- Send Host and Policy Data from CounterACT to ArcSight..... 12**
- Use ArcSight Action Connector Commands in CounterACT Conditions..... 14**

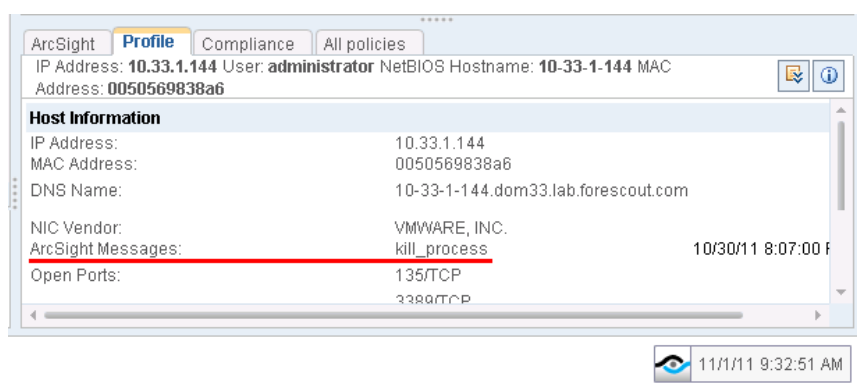
About the CounterACT ArcSight Plugin

CounterACT integrates with HP ArcSight Asset Connector servers to provide complete visibility of network endpoints, including unmanaged endpoints. In addition, ArcSight users can leverage CounterACT tools to quickly take action on network hosts; reduce network risks and control network endpoints.

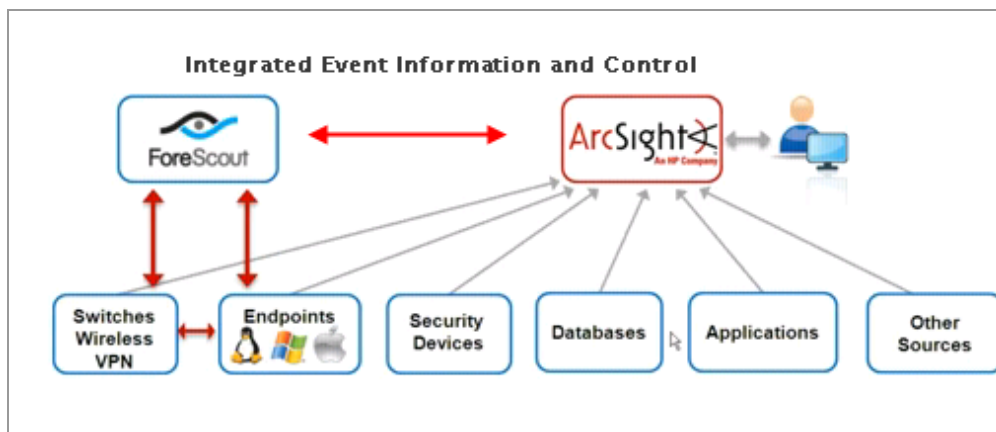
HP ArcSight Asset Connector Server Integration

HP ArcSight Asset Connector server integration lets you:

- Display ArcSight event discoveries at the CounterACT Console.



- Send important policy status and host information from CounterACT to the ArcSight Console, for example:
 - An extensive range of host properties discovered by CounterACT
 - Policy status information
- Correlate information from an extensive range of ArcSight sources to help you assess risks and quickly trigger actions at CounterACT, for example:
 - *In an ArcSight environment working with Retina servers that discovered vulnerabilities*
ArcSight can correlate information detected by Retina and CounterACT and then instruct CounterACT to follow up with remediation.
 - *In an ArcSight environment working with Tipping Point IPS systems that discovered host attacks*
ArcSight can correlate information detected by Tipping Point and CounterACT and then instruct CounterACT to follow up with remediation or blocking.
 - *In an environment where CounterACT reports network guests to ArcSight and a 3rd party reports a vulnerability on the guest*
Correlate the information at ArcSight and instruct CounterACT to take action on the vulnerable guest host.



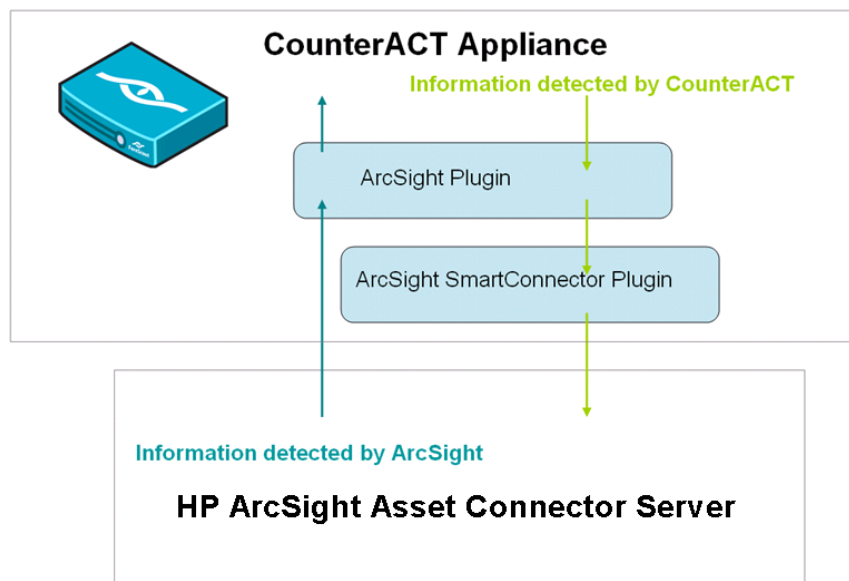
Message Send/Receive Flow

Messages from CounterACT to the ArcSight Asset Connector server take the following path:

CounterACT Appliance ArcSight Plugin > ArcSight SmartConnector Plugin > ArcSight Asset Connector server

ArcSight Asset Connector server sends integrated command messages to CounterACT through the following path:

ArcSight Asset Connector server > ArcSight-Plugin > CounterACT Appliance > Plugin
(required only to start plugin)



Appliance/Enterprise Manager Architecture

ArcSight can be integrated with CounterACT devices in several configurations.

In the simplest case, you define a single ArcSight server target. By default, all CounterACT appliances communicate with that server.

If you define more than one ArcSight server, you can assign individual CounterACT appliances to each ArcSight server. Each CounterACT device communicates with a single ArcSight server. One ArcSight server is designated the default server, and handles CounterACT devices that have not been assigned to another ArcSight server.

The **Appliance Connector Prefix** is a required field that identifies all Appliances connected to an ArcSight server. This field should be unique for each ArcSight server that communicates with CounterACT devices.

See *Send Host and Policy Data from CounterACT to ArcSight* for configuration instructions.

What You Need Do

Perform the following in order to carry out the integration:

- Download and install the *ArcSight Plugin* and the *ArcSight SmartConnector Plugin* from the ForeScout website: www.forescout.com/support. See *Installation* for details.
- Verify that requirements are met. See *Requirements* for details.
- Set up the servers to work with CounterACT. See *Define Target Asset Connector Servers*.

Plugin Module Licensing

This plugin is a component of the SIEM Integration Module, and requires a module license. This module license will include endpoints managed by the ArcSight plugin, but may also include endpoints managed by the following other SIEM Integration Module plugins:

- QRadar Plugin
- CEF Plugin

When installing the plugin you will be provided with a 30-day demo module license. When this period expires, you will be required to purchase a permanent module license. *In order to continue working with module features, you must purchase the license.* If you would like to continue exploring the module before purchasing a permanent license, you can request a demo extension. The permanent license and demo extension license request are made from the CounterACT Console.


You will receive email notification and alerts at the Console before the demo period expires.

If you install this plugin and later install other plugins included in this module, the demo expiration period is calculated from the first plugin installation.

Module Capacity

When requesting a permanent license or demo extension, you will be asked to provide the endpoint *capacity* requirements, i.e. the number of endpoints that will be covered by the module license. Permanent licenses for this module are based on the number of endpoints your CounterACT system was licensed to handle. You can request a module license above

this capacity to support additional endpoints as your deployment grows. However, the request should not be less than the current capacity of your CounterACT deployment. You should enter this number in the Capacity tab of the Module License Request wizard.



SIEM Integration Module License Request

Company ✓
Type ✓
Capacity
Request

Capacity
This module license is based on the capacity of your current CounterACT deployment. Request a license above this capacity to support additional endpoints as your deployment grows.

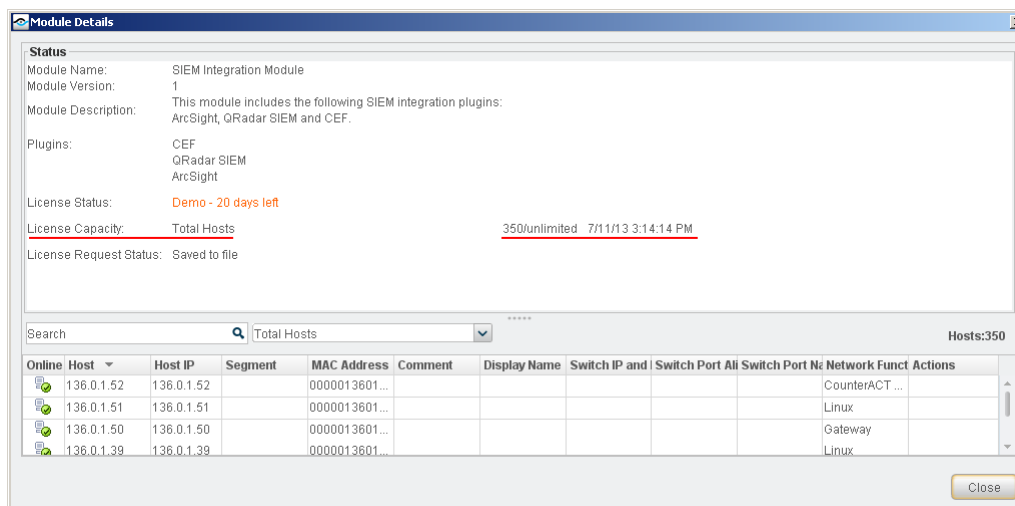
Number of endpoints you want the module to support: 650

Help Previous Next Finish Cancel

You can gain a better understanding of the license capacity you need by reviewing the total endpoints covered by all CounterACT Appliances. The capacity value you should enter should reflect this value.

To review module license capacity:

1. Select **Tools>Options>Modules**
2. Select the SIEM Integration Module. The current capacity is displayed in the Status section, **License capacity** field.



Module Details

Status
Module Name: SIEM Integration Module
Module Version: 1
Module Description: This module includes the following SIEM integration plugins:
ArcSight, QRadar SIEM and CEF.
Plugins: CEF, QRadar SIEM, ArcSight
License Status: Demo - 20 days left
License Capacity: Total Hosts 350/unlimited 7/11/13 3:14:14 PM
License Request Status: Saved to file

Search Total Hosts Hosts:350

Online	Host	Host IP	Segment	MAC Address	Comment	Display Name	Switch IP and	Switch Port Ali	Switch Port No	Network Funct	Actions
	136.0.1.52	136.0.1.52		0000013601...						CounterACT ...	
	136.0.1.51	136.0.1.51		0000013601...						Linux	
	136.0.1.50	136.0.1.50		0000013601...						Gateway	
	136.0.1.39	136.0.1.39		0000013601...						Linux	

Close

More License Information

See the [CounterACT Console User Manual](#) for information on requesting a permanent license or a demo license extension. You can also contact your ForeScout representative for more information or contact ForeScout support at support@forescout.com.

Requirements

- CounterACT version 7.0.0, with Hotfix1.2.
- Verify that ArcSight servers can receive messages from CounterACT Appliances and Enterprise Managers.

Installation

ArcSight support in CounterACT is packaged as a kit of two plugins:

- The *CounterACT ArcSight Plugin* installs CounterACT-specific features for ArcSight support.
- The *ArcSight SmartConnector Plugin* installs a standard data integration package provided by ArcSight.

CounterACT ArcSight Plugin

Install this plugin to implement ArcSight integration features in CounterACT. With this plugin, CounterACT does the following:

- Establish an authenticated connection between CounterACT and the ArcSight server.
- Receive Integrated Commands from the Asset Connector server.
- Provide ArcSight related properties and actions.

New CounterACT features and fixes are released in this plugin.

ArcSight SmartConnector Plugin

This plugin installs the *ArcSight SmartConnector* application on the Appliance. This application is provided by ArcSight to enable communication and data integration with the Asset Connector server. The ArcSight SmartConnector Plugin remains running after installation and cannot be stopped. This plugin requires 100 MB of disk space. This plugin is only updated when ArcSight updates the SmartConnector application, and does not require any configuration.

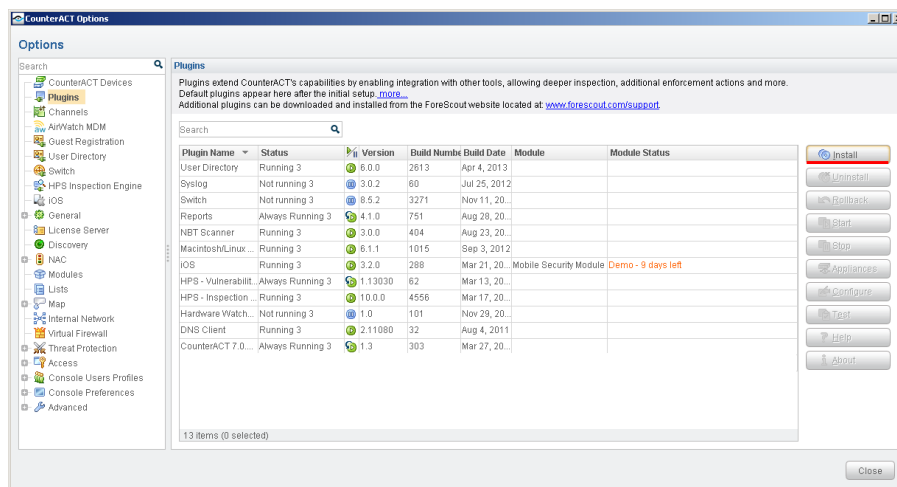
Install the Plugin

This section describes how to install the plugin.

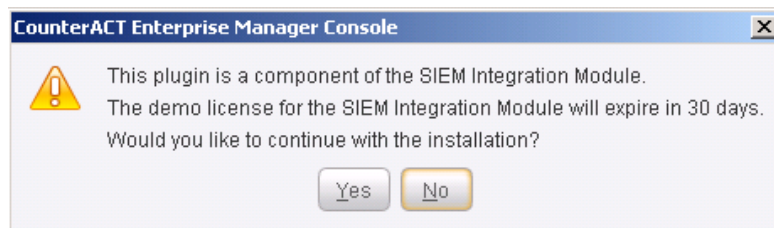
To install the plugin:

1. Download the plugin from the CounterACT [Customer Support portal](#).
2. Save the plugin installation file to the machine where the CounterACT Console is installed.
3. Log in to CounterACT and select **Options** from the **Tools** menu.

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



6. The Open dialog box opens. Navigate to the location where you saved the plugin installation file and select **Install**.
7. A message appears indicating that the plugin is installed with a demo module license.



-  *If you install this plugin on a CounterACT version earlier than 7.0.0, licensing prompts do not appear.*

8. Select **Yes**, and then select **Install**.
9. Once the installation is complete, select **Close**.
10. The plugin is listed in the Plugins folder. The Module Status column indicates the time remaining for the demo license. See [Plugin Module Licensing](#) and the *Console User Guide* for information on requesting a permanent license or a demo license extension.

Define Target Asset Connector Servers

To support interaction with ArcSight, you map CounterACT Appliances or the Enterprise Manager to an ArcSight server.

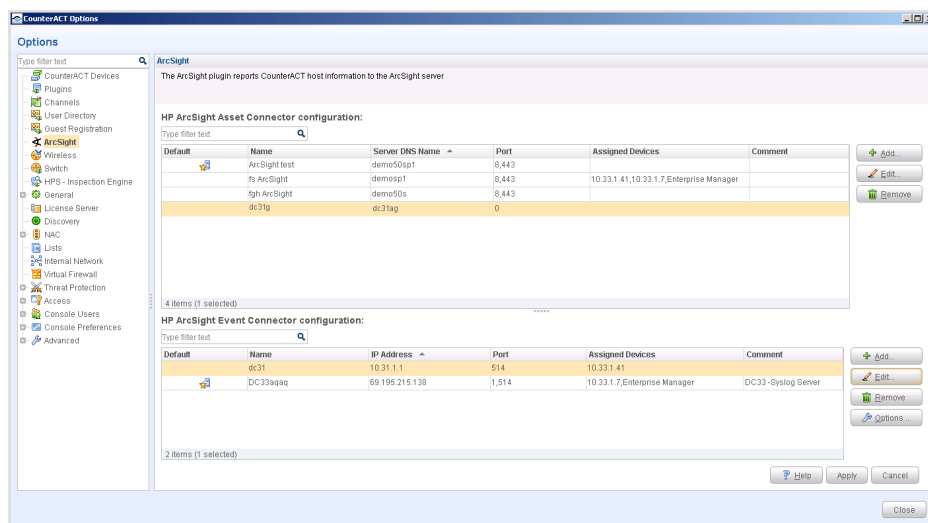
In the simplest case, you define a single ArcSight server target. By default, all CounterACT appliances communicate with that server.

If you define more than one ArcSight server, you can assign individual CounterACT appliances to each ArcSight server. Each CounterACT device communicates with a single ArcSight server. One ArcSight server is designated the default server, and handles CounterACT devices that have not been assigned to another ArcSight server.

The **Appliance Connector Prefix** is a required field that identifies all Appliances connected to an ArcSight server. This field should be unique for each ArcSight server that communicates with CounterACT devices.

To define ArcSight server targets for CounterACT:

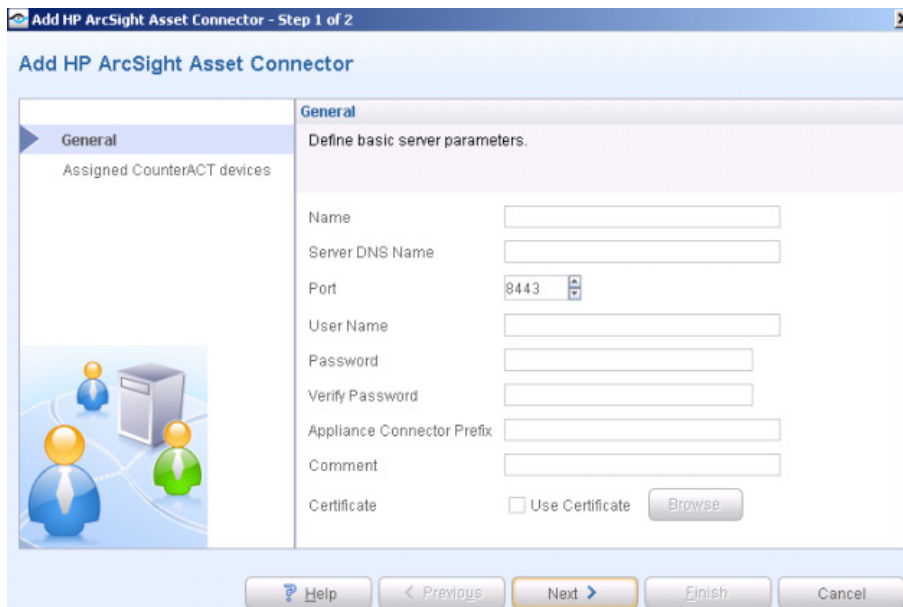
1. Select Options from the Tools menu at the Console.
2. Navigate to the ArcSight folder. The ArcSight Pane opens.



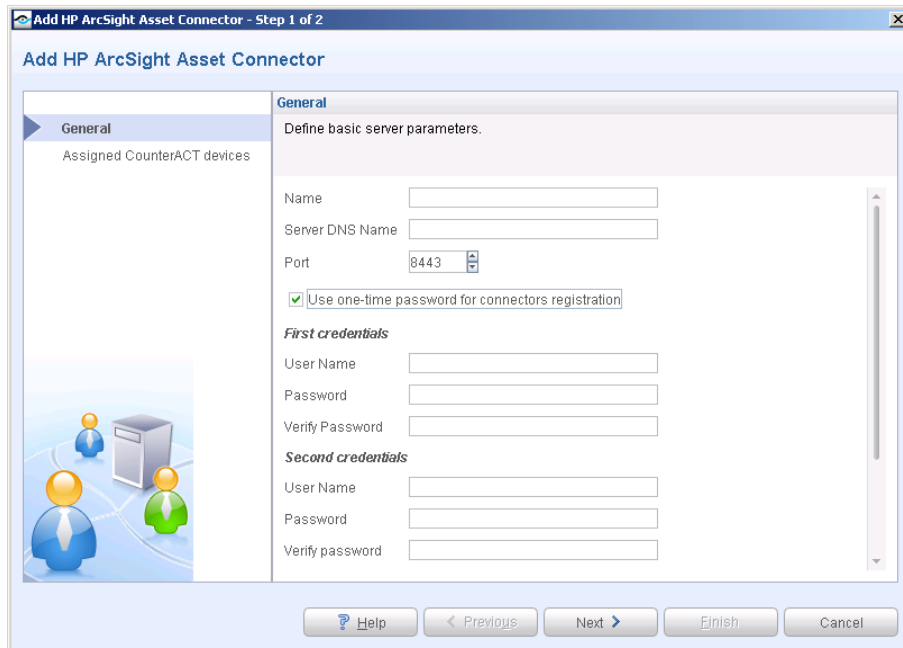
3. Select **Add** from the ArcSight Asset Connector server section. The Add HP ArcSight Asset Connector wizard opens.
4. In the General tab, define the following parameters:
 - In the **Name** field, enter the server name.
 - In the **Server DNS Name** field, enter the ArcSight server DNS name to which CounterACT will connect. Spelling is case sensitive. Do not use an IP address number.
 - Enter the port used by the ArcSight server. The default is 8443.
 - In the **Password** field, enter a password.
 - In the **Appliance Connector Prefix** field, enter the connector prefix for the Appliance that will connect to this server. The name should be identical for

this and any other Appliance connected to this server, but unique to Appliances connected to other ArcSight servers.

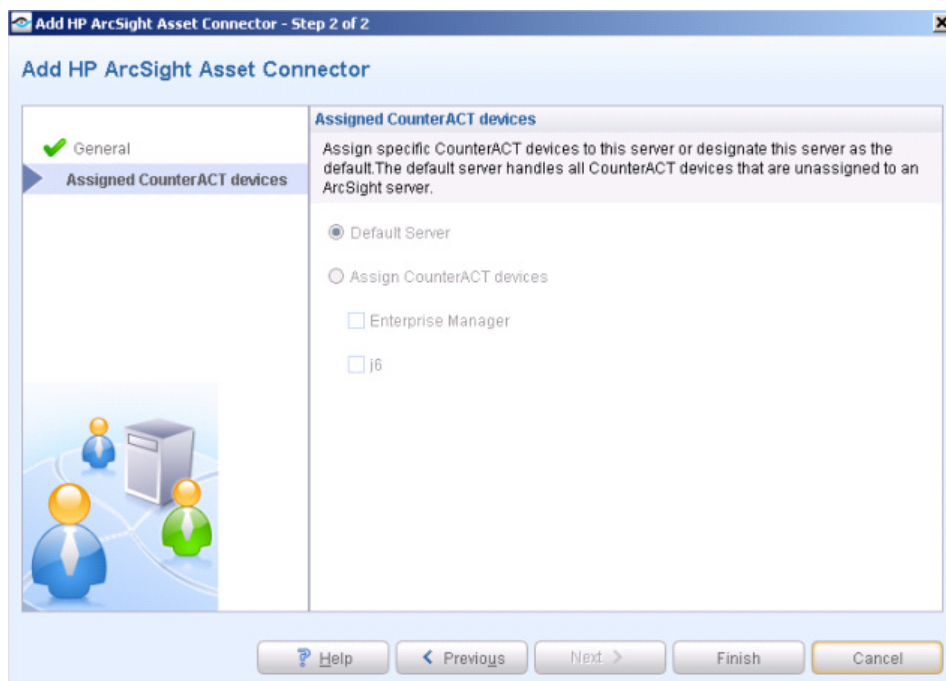
- In the **Comment** field, enter comments about the server.



5. (Optional) To work with one-time passwords, select the **Use one-time password for connector registration** option. Specify the passwords needed to connect to the ArcSight server. Specify two passwords for the Event Connector, and two passwords for the Asset Connector.



6. Select **Next**. The **Assigned CounterACT devices** pane opens.



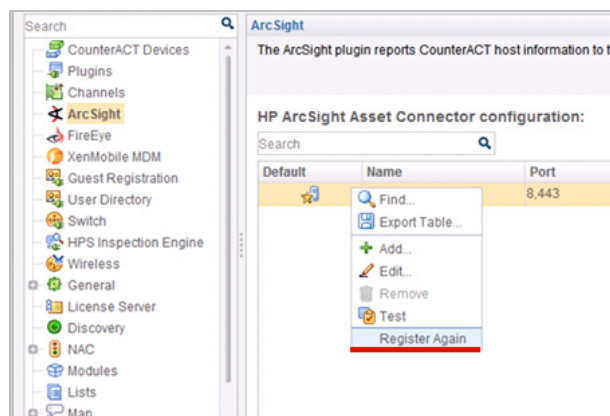
7. In the Assigned CounterACT devices pane, choose one of the following options:
 - Select **Default Server** to make this server the target for all CounterACT devices not assigned to another ArcSight server. Until you define more than one server, this is the only option available.
 - Select **Assign CounterACT devices** to specify CounterACT devices that communicate with this server.

Select **Finish**. The server appears in the ArcSight pane.

8. (Optional) Repeat Steps


Connector Maintenance

When you define configuration settings for an ArcSight server, the plugin accesses the server and registers your CounterACT device as an ArcSight connector. In some cases, the CounterACT device may not successfully register as a connector, or you may need to re-register it, for example after certain actions are taken on the ArcSight server. The **Register Again** option lets you re-register your CounterACT device with the server.



Before using this option, verify the status of the CounterACT connector in the Access Console view of the ArcSight Server management interface. You must re-register the CounterACT device if:

- The status at the ArcSight Access Console is *Down*. In this case, remove the connector at the ArcSight server before you select **Register Again** in the CounterACT Console.
- You do not see it displayed at the ArcSight Access Console.

 Using the **Register Again** option on a connection that is working properly can disconnect the CounterACT connector.

Send Host and Policy Data from CounterACT to ArcSight

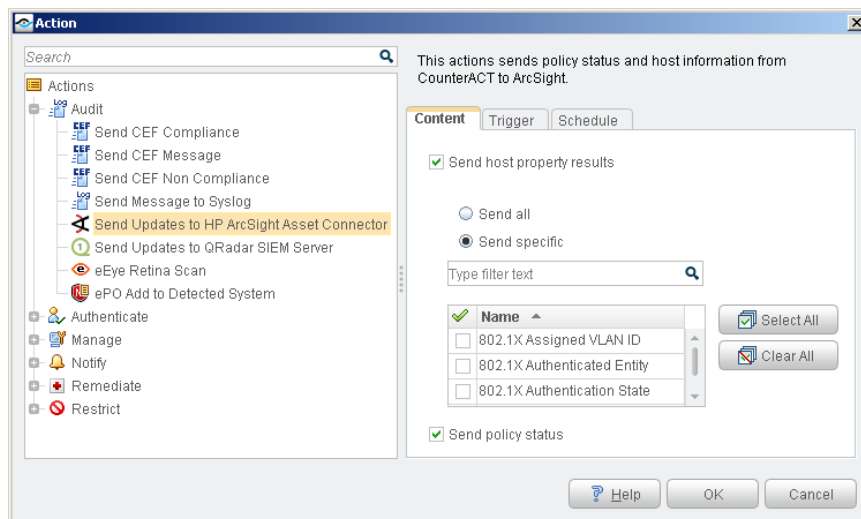
You can send policy status and host information from CounterACT to the ArcSight Console, on a permanent or temporary basis; or according to a specific schedule. Once sent, ArcSight can correlate this information with other data stored from other sources in order to perform comprehensive host evaluation. The following options are available:

- Send host property results, for example switch related information, device information, authentication information, and more.
- Send policy status information, including the match/unmatched status.

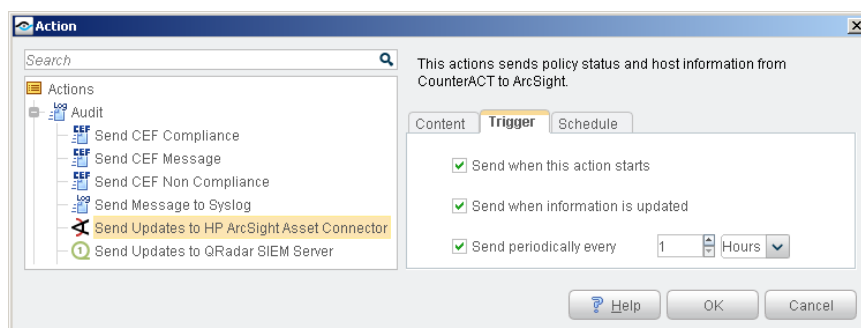
To create actions:

1. Create or edit a policy and navigate to the policy actions.

2. Navigate to the **Audit** folder and select **Send Updates to HP ArcSight Asset Connector**. The Contents tab opens.



3. Select the **Send host property results** check box to instruct CounterACT to send property results to the ArcSight server.
 - Select **Send all** to send results of all property results discovered
 - Select **Send specific** to send the results of specific properties, and select the properties of interest to you.
 - Select **Send policy status** to send the CounterACT policy status (match/unmatch/pending/irresolvable)
4. Select the Trigger tab. Use the options to indicate when to initiate updates to the ArcSight server. Later you can use the options in the Schedule tab to further customize your event delivery strategy.



Select the following options:

- Select **Send when the action starts** to send information once when the conditions of the policy are met.
- Select **Send when information is updated** to send information when there is a change in the host properties you specified in the Content tab.
- Select **Send periodically every** to send information at fixed intervals.

5. Select the **Schedule** tab. You can use these standard action scheduling options to further customize message delivery. For example, you can choose the **Customize action start time** option to delay message delivery, or to limit the duration of repeated or regularly scheduled messages.


Use ArcSight Action Connector Commands in CounterACT Conditions

You can instruct CounterACT to carry out specific actions when an Action Connector Command message is received from ArcSight. For example, configure a CounterACT policy to assign hosts to a specific VLAN when the message *Vulnerability detected by Vendor A* is sent by ArcSight

In order to achieve this, the following must occur.

- Define relevant Action Connector Commands in ArcSight.
- Define a CounterACT policy that detects hosts which received the Action Connector Command.
- Review detections at the ArcSight Console and send an Action Connector Command message to CounterACT.
- The CounterACT policy detects hosts for which the Action Connector message was received.
- CounterACT implements the actions defined in the policy.

Action Connector also supports start/stop functionality. When you stop a message to CounterACT, the related CounterACT action is also stopped.

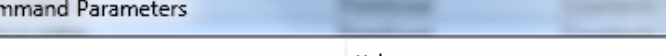
 *In order to work with these features, you must start the CounterACT plugin but are not required to configure it.*

To send an Action Connector Command to CounterACT:

1. Right-click the detections of importance to you.
2. Select **Send Command>CounterACT** and then select a command message.

	Manager Receipt Time	End Time	Name	Device Vendor
	GMT+02:00 15:13:38 2012 19 فبر	2/19 15:13:16	Admission	ForeScout
	GMT+02:00 15:13:38 2012 19 فبر	2/19 15:13:16	Admission	ForeScout
	GMT+02:00 15:13:38 2012 19 فبر	2/19 15:13:16	Admission	ForeScout
	GMT+02:00 15:13:38 2012 19 فبر	2/19 15:13:16	Compliance Status	ForeScout
	GMT+02:00 15:13:38 2012 19 فبر	2/19 15:13:16	DHCP Server Address	ForeScout
	GMT+02:00 15:13:38 2012 19 فبر	2/19 15:13:16	Traffic seen	ForeScout
	GMT+02:00 15:13:38 2012 19 فبر	2/19 15:13:16	Corporate/Guest Status	ForeScout
	GMT+02:00 15:13:38 2012 19 فبر	2/19 15:13:16	DNS Name	ForeScout
Configure	32:00 15:13:38 2012 19 فبر	2/19 15:13:16	IP Address	ForeScout
Delete Connector	32:00 15:13:38 2012 19 فبر	2/19 15:13:16	MAC Address	ForeScout
Set as Current Filter	32:00 15:13:38 2012 19 فبر	2/19 15:13:16	Host is online	ForeScout
Add to Current Filter	32:00 15:13:38 2012 19 فبر	2/19 15:13:16	NIC Vendor	ForeScout
Create Channel with Filter	32:00 15:13:38 2012 19 فبر	2/19 15:13:16	Wireless Access Point Name	ForeScout
	32:00 15:13:38 2012 19 فبر	2/19 15:13:16	Wireless Host Authentication	ForeScout
	32:00 15:13:38 2012 19 فبر	2/19 15:13:16	Wireless Connectivity Status	ForeScout
Send Command	32:00 15:13:38 2012 19 فبر	2/19 15:13:16	Wireless Controller IP	ForeScout
Export Connector Configuration As...	32:00 15:13:38 2012 19 فبر	2/19 15:13:16	Wireless Host SSID	ForeScout
Import Connector Configuration...	32:00 15:13:38 2012 19 فبر	2/19 15:13:16	Wireless Product	ForeScout
Add to Package	32:00 15:13:38 2012 19 فبر	2/19 15:13:16	Policies Status	ForeScout
Grid View	32:00 15:13:38 2012 19 فبر	2/19 15:13:16	Policies Status	ForeScout
Graph View	32:00 15:13:38 2012 19 فبر	2/19 15:13:16	Policies Status	ForeScout
New Group	32:00 15:13:38 2012 19 فبر	2/19 15:13:16	Policies Status	ForeScout
Edit Group	32:00 15:13:38 2012 19 فبر	2/19 15:13:16	Policies Status	ForeScout
Delete Group	32:00 15:13:38 2012 19 فبر	2/19 15:13:16	Policies Status	ForeScout
Rename	32:00 15:12:22 2012 19 فبر	2/19 15:12:00	Open Ports	ForeScout
Edit Access Control	32:00 15:12:22 2012 19 فبر	2/19 15:12:00	Open Ports	ForeScout
Show Invalid Reason	32:00 15:12:22 2012 19 فبر	2/19 15:12:00	Open Ports	ForeScout
Validate Connector	32:00 15:12:22 2012 19 فبر	2/19 15:12:00	Open Ports	ForeScout
Lock Connector	32:00 15:12:22 2012 19 فبر	2/19 15:12:00	Open Ports	ForeScout
Unlock Connector	32:00 15:12:22 2012 19 فبر	2/19 15:12:00	Open Ports	ForeScout
Set deprecated flag	32:00 15:12:22 2012 19 فبر	2/19 15:12:00	Open Ports	ForeScout
Remove deprecated flag	32:00 15:12:22 2012 19 فبر	2/19 15:12:00	Open Ports	ForeScout

3. Add any variables values or other data strings, and send the message.



Name	Value
Misc	
IP Address	
Message	

The ArcSight command message is sent to CounterACT. This event appears with other hosts information, for example in the Profile tab.

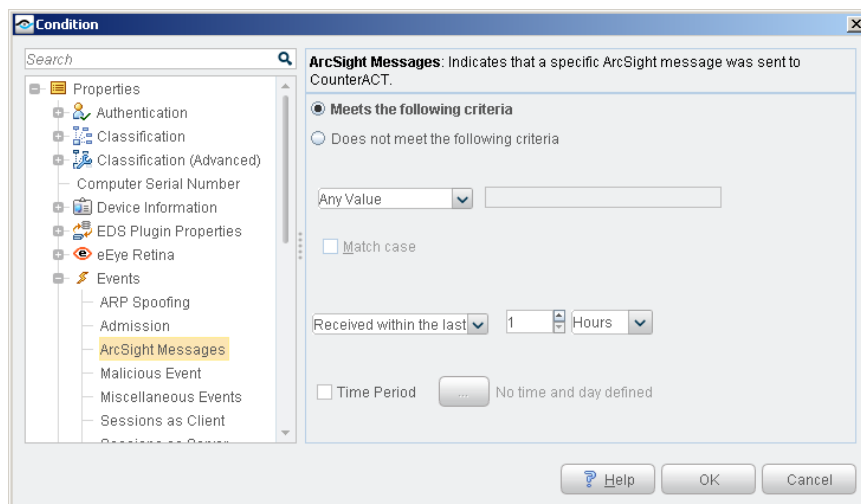
The screenshot shows the ArcSight console interface. At the top, there are tabs for 'ArcSight', 'Profile', 'Compliance', and 'All policies'. Below the tabs, a status bar displays: 'IP Address: 10.33.1.144 User: administrator NetBIOS Hostname: 10-33-1-144 MAC Address: 0050569838a6'. To the right of this bar are two icons: a document with a checkmark and a question mark. The main content area is titled 'Host Information' and contains a table with the following data:

IP Address:	10.33.1.144
MAC Address:	0050569838a6
DNS Name:	10-33-1-144.dom33.lab.forescout.com
NIC Vendor:	VMWARE, INC.
ArcSight Messages:	kill_process
Open Ports:	135/TCP
	3389/TCP

On the right side of the 'Host Information' section, there is a timestamp: '10/30/11 8:07:00 PM'. At the bottom of the console, there is a system tray with the ArcSight logo and the date/time '11/1/11 9:32:51 AM'.

To use an ArcSight message event in a CounterACT policy:

1. Create or edit a policy, and edit policy conditions.
2. In the Properties tree, navigate to **Events>ArcSight Messages**.



3. Define a property based on the Action Connector Command message text sent by ArcSight. Options include:
 - Select **Does not meet the following criteria** to match all Integrated Message strings *except* the specified text.
 - Use the **Received** dropdown and the **Time Period** options to define a time window for the command message. For example, you can specify that only messages received during working hours between Monday and Friday match the condition.
4. Create an action for the policy. The action is implemented when the condition is met.

Legal Notice

Copyright © ForeScout Technologies, 2000-2013. All rights reserved.

The copyright and proprietary rights in the guide belong to ForeScout Technologies. It is strictly forbidden to copy, duplicate, sell, lend or otherwise use this guide in any way, shape or form without the prior consent of ForeScout Technologies.

This product is based on software developed by ForeScout Technologies. The products described in this document are protected by U.S. patent # 6,363,489 issued March 2002 and may be protected by other U.S. Patents and foreign patents.

Redistribution and use in source and binary forms are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials and other materials related to such distribution and use, acknowledge that the software was developed by ForeScout Technologies.

THIS SOFTWARE IS PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

All other trademarks used in this document are the property of their respective owners.

Send comments and questions regarding documentation to: documentation@forescout.com

7/14/13