

# 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 ArcSight1	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.

ArcSight Profile Compliance All polic	cies	
IP Address: 10.33.1.144 User: administrator Address: 0050569838a6	NetBIOS Hostname: 10-33-1-144 MA	c 🗟 🛈
Host Information		1
IP Address: MAC Address:	10.33.1.144 0050569838a6	
 DNS Name:	10-33-1-144.dom33.lab.forescout.c	om
NIC Vendor: ArcSight Messages:	VMWARE, INC. kill_process_	10/30/11 8:07:00 F
Open Ports:	135/ТСР	
	3380/TCP	
	[	◆ 11/1/11 9:32:51 AM

- 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 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 you 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 Integ	gration	Module License Request - Step 3 of 4	×
SIEM Inte	egrati	ion Module License Request	
		Capacity	
🖌 Com 🗸 Type	pany	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.	
Capao Requ	c <b>ity</b> est	Number of endpoints you want the module to support: 650 🛱	
		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.

	e Details										
Status	;										
Module Module	e Name: e Version:	SIEM Inte 1	egration Modu	le							
Module	e Description:	This mo ArcSight	dule includes , QRadar SIEN	the following SIEM 1 and CEF.	l integration p	lugins:					
Plugins	8:	CEF QRadar ArcSight	SIEM								
Licens	e Status:	Demo - 3	20 days left								
Licens Licens Licens	e Status: e Capacity: e Request Sta	Demo - : Total Ho itus: Saved to	20 days left <u>sts</u> file			350/unlimit	ed 7/11/13 3:1	4:14 PM			
Licens) Licens) Licens)	e Status: e Capacity: e Request Sta	Demo - : Total Ho itus: Saved to	20 days left sts file			<u>350/unlimit</u>	ed 7/11/133:1	4:14 PM			
Licens) Licens) Licens) Search	e Status: e Capacity: e Request Sta	Demo - : Total Ho tus: Saved to	20 days left sts file <b>Q</b> Total H	osts		<u>350/unlimit</u>	ed 7/11/13 3:1	4:14 PM			Hosts:3
Licens Licens Licens Search Online	e Status: e Capacity: e Request Sta 1 <b>Host v</b>	Demo - : Total Ho itus: Saved to Host IP	20 days left sts file Cotal H Segment	osts MAC Address	Comment	350/unlimit	ed 7/11/13 3:1: Switch IP and	4:14 PM Switch Port Ali	Switch Port Na	Network Funct	Hosts:3
Licens Licens Licens Search Online	e Status: e Capacity: e Request Sta n Host v 136.0.1.52	Demo - : Total Ho itus: Saved to Host IP 136.0.1.52	20 days left sts file Q Total H Segment	osts MAC Address 0000013601	Comment	350/unlimit	ed 7/11/13 3:1	4:14 PM Switch Port Ali	Switch Port Na	Network Funct	Hosts:3 Actions
Licensi Licensi Licensi Search Online	e Status: e Capacity: e Request Sta Host = 136.0.1.52 136.0.1.51	Demo - : Total Ho itus: Saved to Host IP 136.0.1.52 136.0.1.51	20 days left sts file Total H Segment	MAC Address 0000013601 0000013601	Comment	350/unlimit	ed 7/11/13 3:1-	4:14 PM Switch Port Ali	Switch Port Na	Network Funct CounterACT Linux	Hosts:3 Actions
Licens Licens Licens Search Online	e Status: e Capacity: e Request Sta Host 136.0.1.52 136.0.1.51 136.0.1.50	Demo - : Total Ho ttus: Saved to Host IP 136.0.1.52 136.0.1.51 136.0.1.50	20 days left sts file Segment	MAC Address           0000013601           0000013601           0000013601	Comment	350/unlimit	ed 7/11/13 3:1-	1:14 PM	Switch Port Na	Network Funct CounterACT Linux Gateway	Hosts:3 Actions

## More License Information

See the <u>CounterACT Console User Manual</u> 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 form 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.

Plugins extend Cou							
Default plugins app Additional plugins o Search	interACT's capabilitie ear here after the ini an be downloaded a	es by enabling in tial setup. <u>more</u> and installed fro	ntegration wi	th other tools, a cout website lo	llowing deeper in cated at: <u>www.for</u>	nspection, additional enforcement actions and more. escout.com/support.	
Plugin Name 👻	Status	Version	Build Nun	nbe Build Date	Module	Module Status	( Install
User Directory	Running 3	6.0.0	2613	Apr 4, 2013			
Syslog	Not running 3	3.0.2	60	Jul 25, 2012			( Uninstall
Switch	Not running 3	0 8.5.2	3271	Nov 11, 20			Rollback
Reports	Always Running 3	6 4.1.0	751	Aug 28, 20			In Start
NBT Scanner	Running 3	3.0.0	404	Aug 23, 20			-Di giani
Macintosh/Linux	Running 3	6.1.1	1015	Sep 3, 2012			Stop
iOS	Running 3	3.2.0	288	Mar 21, 20	Mobile Security I	Adule Demo - 9 days left	
HPS - Vulnerabilit.	Always Running 3	6 1.13030	62	Mar 13, 20			
HPS - Inspection	Running 3	🔕 10.0.0	4556	Mar 17, 20			Comigure
Hardware Watch	Not running 3	00 1.0	101	Nov 29, 20			Test
DNS Client	Running 3	2.11080	32	Aug 4, 2011			2 Holn
CounterACT 7.0	Always Running 3	<b>6</b> 1.3	303	Mar 27, 20			2. Eleih
							<u>å A</u> bout
	Search  Plugin Name  User Directory Systog Switch Reports NST Scanner Macintosht/Lnux IOS HPS - Vulnerabilit. HPS - Inspection DNS Client CounterACT 7.0	Search         Q           Plugin Name         Status           User Directory         Running 3           Systep         Not running 3           Switch         Not running 3           Bort Scanner         Running 3           Maxino Status         Running 3           Maxino Status         Running 3           HPS - Vulnerabilit         Aways Running 3           HPS - Vulnerabilit         Aways Running 3           HPS - Vulnerabilit         Aways Running 3           DNS Client         Running 3           CounterACT 7.0.         Aways Running 3	Q         Q           Plugin Name         Status         ½ Version           User Directory         Running 3         © 80.00           Systog         Not Running 3         © 80.02           Swetch         Net running 3         © 85.2           Reports         Always Furning 3         © 81.1           NMS Tosame         Running 3         © 81.1           OS         Running 3         © 81.1           OS         Running 3         © 11.3030           HP3 - Nutherabilit.         Always Running 3         © 11.00.0           Hardware Walch.         Running 3         © 10.0.0           Hardware Walch.         Not numing 3         © 10.0.0           DNS Client.         Running 3         © 11.3030           CounterACT 7.0         Always Running 3         © 1.3	Search         Q           Plugin Name         Status         Vir Version         Build Nam           User Directory         Running 3         © 6.0.0.2613         Status           Syslog         Not running 3         © 6.2.2         Status         Status         Status           Switch         Not running 3         © 6.2.2         Status         Status <td>Search         Q           Plugin Name         Status         % Version         Build Numbi- Build Date           User Directory         Running 3         © 6.0.0         2613         Apr4, 2013           Systog         Nort running 3         © 8.5.2         3271         Nort 1, 20.           Reports         Always Running 3         © 3.0.2         404         Aug 23, 20.           MacintoshLinuz.         Running 3         © 8.5.2         3271         Nort 1, 20.           MasintoshLinuz.         Running 3         © 8.1.1         1015         See 2.         100           MasintoshLinuz.         Running 3         © 8.1.1         1015         See 3.         100.0         455           HPS - Vulnerabilt.         Always Running 3         © 10.0.0         4555         Mar17, 20.         101         Nov 29, 20.           NPS - Svulnerabilt.         Always Running 3         © 1.0.0         4555         Mar17, 20.         101         Nov 29, 20.           DNS Client         Running 3         © 1.0.0         32.0         Aug 4, 2011         CounterACT 7.         Always Running 3         © 1.3         30.3         Mar 27, 20.</td> <td>Bearch         C           Plugin Name         Status         % Version         Build North/ Build Date         Module           User Directory         Running 3         © 60.00         2613         Apr 4, 2013         Secondary         Secondary</td> <td>Baarch         Vi         Version         Build Number Build Date         Module         Module Status           User Directory         Running 3         © 80.00         2813         Apr 4, 2013         Module         Module Status           Systep         Not running 3         © 80.20         2813         Apr 4, 2013         Module         Module Status           Swetch         Not running 3         © 80.22         627.11         Nov 11, 20.         Module Status           Reports         Anvers Furning 3         © 14.10         751         Aug 28, 20.         Module Status           Macintobultruix.         Running 3         © 13.00         40.44         Aug 32, 30.         Module Status           IOS         Running 3         © 1.10         105         Sae 3, 20.12         Module Status           HPS -Vulnerabilit.         Anvers Furning 3         © 1.10         10.52         Mar 17, 20.         Martine Status           HPS -Vulnerabilit.         Anvers Furning 3         © 1.10         Nov 32, 0.         Module Status         Martine Status           CeunterACT 7.0         Anvers Furning 3         © 1.13         30.3         Mar 27, 20.         Martine Status         Martine Status</td>	Search         Q           Plugin Name         Status         % Version         Build Numbi- Build Date           User Directory         Running 3         © 6.0.0         2613         Apr4, 2013           Systog         Nort running 3         © 8.5.2         3271         Nort 1, 20.           Reports         Always Running 3         © 3.0.2         404         Aug 23, 20.           MacintoshLinuz.         Running 3         © 8.5.2         3271         Nort 1, 20.           MasintoshLinuz.         Running 3         © 8.1.1         1015         See 2.         100           MasintoshLinuz.         Running 3         © 8.1.1         1015         See 3.         100.0         455           HPS - Vulnerabilt.         Always Running 3         © 10.0.0         4555         Mar17, 20.         101         Nov 29, 20.           NPS - Svulnerabilt.         Always Running 3         © 1.0.0         4555         Mar17, 20.         101         Nov 29, 20.           DNS Client         Running 3         © 1.0.0         32.0         Aug 4, 2011         CounterACT 7.         Always Running 3         © 1.3         30.3         Mar 27, 20.	Bearch         C           Plugin Name         Status         % Version         Build North/ Build Date         Module           User Directory         Running 3         © 60.00         2613         Apr 4, 2013         Secondary         Secondary	Baarch         Vi         Version         Build Number Build Date         Module         Module Status           User Directory         Running 3         © 80.00         2813         Apr 4, 2013         Module         Module Status           Systep         Not running 3         © 80.20         2813         Apr 4, 2013         Module         Module Status           Swetch         Not running 3         © 80.22         627.11         Nov 11, 20.         Module Status           Reports         Anvers Furning 3         © 14.10         751         Aug 28, 20.         Module Status           Macintobultruix.         Running 3         © 13.00         40.44         Aug 32, 30.         Module Status           IOS         Running 3         © 1.10         105         Sae 3, 20.12         Module Status           HPS -Vulnerabilit.         Anvers Furning 3         © 1.10         10.52         Mar 17, 20.         Martine Status           HPS -Vulnerabilit.         Anvers Furning 3         © 1.10         Nov 32, 0.         Module Status         Martine Status           CeunterACT 7.0         Anvers Furning 3         © 1.13         30.3         Mar 27, 20.         Martine Status         Martine Status

- 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.

Counter/	ACT Enterprise Manager Console
	This plugin is a component of the SIEM Integration Module. The demo license for the SIEM Integration Module will expire in 30 days. Would you like to continue with the installation?
	Yes No

- 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.

rcSight						
The ArcSight plugin	reports CounterACT host infi	ormation to the ArcSight server				
HP ArcSight As	set Connector configur	ration:				
Type filter text	٩					
Default	Name	Server DNS Name A	Port	Assigned Devices	Comment	🔶 Add
<b>1</b>	ArcSighttest	demo50sp1	8,443			
	fs ArcSight	demosp1	8,443	10.33.1.41,10.33.1.7,Enterprise Manager		🖌 Edit
	fgh ArcSight	demo50s	8,443			Remo
	dc31g	dc31ag	0			
4 items (1 selecter	d)					
4 items (1 selecte HP ArcSight Ev Type filter text	d) ent Connector configu	ration:	*****			
4 items (1 selecte HP ArcSight Ev Type filter text Default	d) ent Connector configu Q Name	P Address 🔺	Port	Assigned Droices	Comment	de saa
4 items (1 selecte HP ArcSight Ev Type filter text Default	d) ent Connector configu Q Name dc31	IP Address * 10.31.1.1	Port 514	Assigned Devices	Comment	<b>₽</b> <u>A</u> dd
4 items (1 selecte HP ArcSight Ev Type filter text Default	d) ent Connector configu Q Name dc31 DC33aqaq	P Address ↑ 10.31.1.1 89.195.215.138	Port 514 1,514	Assigned Devices 10.33.1.41 10.33.1.7,Enterprise Manager	Comment	♣ <u>A</u> dd ∠ Edit
4 items (1 selecte HP ArcSight Ev Type filter text Default	d) ent Connector configu Q Name dc31 DC33sqaq	ration: IP Address * 10.31.1.1 69.195.215.138	Port 514 1,514	Assigned Devices 10.33.1.41 10.33.1.7,Enterprise Manager	Comment DC33 -Syslog Server	<ul> <li>▲ Add</li> <li>✓ Edit</li> <li> <b>m</b> Remove      </li> </ul>
4 items (1 selecte HP ArcSight Ev Type filter text Default	d) ent Connector configu Q Name dc31 DC33aqaq	ration: IP Address • 10.311.1 69.195.215.138	Port 514 1,514	Assigned Devices 10.33.1.41 10.33.1.7,Enterprise Manager	Comment DC33-Syslog Server	<ul> <li>◆ Add</li> <li>✓ Edit</li> <li>iiii Remove</li> <li>Ø Options</li> </ul>
4 items (1 selecte HP ArcSight Ev Type filter text Default	d) ent Connector configu Q Name dc31 DC33eqaq	ration: IP Address * 10.31.1.1 09.195.215.139	Port 514 1,514	Assigned Devices 10.33.1.41 10.33.1.7,Enterprise Manager	Comment DC33-Syslog Server	<ul> <li>◆ <u>A</u>dd</li> <li>✓ Edit</li> <li>iiii Remove</li> <li>Ø Options</li> </ul>
4 items (1 selecte HP ArcSight Ev Type filter text Default 2 items (1 selecte	d) ent Connector configu Q Name dc31 DC33aqaq )	IP Address ▲ 1031.1.1 69.195.215.139	Port 514 1,514	Assigned Devices 10331.41 1033.1.7,Entreprise Manager	Comment DC33-Syslog Server	<ul> <li>▲ Add</li> <li>✓ Edit</li> <li>■ Remove</li> <li>Ø Options</li> </ul>
	HP ArcSight As: Type filter text Default	HP ArcSight Asset Connector configu Type fiber lead Q Default Name ArcSight hest fis ArcSight igh ArcSight ac31g	HP ArcSight Asset Connector configuration: Type fiber had Q Default Response A fiber had the constraint of the constrai	Arrsbight Asset Connector configuration         C           Type fair fair         C           Ordaut         C           S         Arrsbight Asset Connector configuration           S         Name         Server UNS Name ▲           S         Arrsbight Asset Connector configuration         6.443           S         Arrsbight         demostor         6.443           S         Arrsbight         demostor         6.443           dc31g         dc31g         dc31g         0	HP ArcSight Asset Connector configuration:       Type fait fait     Name     Server DNS Name ▲     Port     Assigned Devices       vil     Name     Genmd Ost 1     0,443     0.331.141,10.331.7,Enterprise Manager       igh ArcSight     demod0s     0,443     0.331.141,10.331.7,Enterprise Manager       dc31g     dc11g     0	HP ArcSight Asset Connector configuration: Type Bior Mud     Connector     Connector       Default     Name     Server DMS Name A     Port     Assigned Devices     Comment       vg0     ArcSight M     demostOpp1     8,443     0.333.141,10.33.17,Enterprise Manager     Comment       dc3tg     dc3tg     0     0     0     0

- **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.

	General		
General	Define basic server parame	ters.	
Assigned CounterACT devices			
	Name		
	Server DNS Name		
	Port	8443	
	User Name		
9	Password		
	Verify Password		
	Appliance Connector Prefix		
	Comment		
	Certificate	Use Certificate Browse	

**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.

	General	
General	Define basic server parameters.	
Assigned CounterACT devices		
	Name	
	Server DNS Name	
	Bott 0442	
	✓ Use one-time password for connectors registration	
	First credentials	
	User Name	
	Password	
8	Venny Password	
	Verny Password Second credentials	
	Verny Password Second credentials User Name	
	Verny Password Second credentials User Name Password	
	Venty Password	

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



	Assigned CounterACT devices
General Assigned CounterACT devices	Assign specific CounterACT devices to this server or designate this server as the default. The default server handles all CounterACT devices that are unassigned to a ArcSight server.
	<ul> <li>Default Server</li> <li>Assign CounterACT devices</li> <li>Enterprise Manager</li> <li>J6</li> </ul>

- 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 reregister 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.

Search	٩	ArcSight					
- GunterACT Devices	Î	The ArcSight	plugin reports CounterACT	host information to t			
→ ArcSight		HP ArcSight Asset Connector configuration:					
- SFireEye		Search	Search Q				
Cuest Registration		Default	Name	Port			
- Buser Directory		2	C Find	8,443			
HPS Inspection Engine     Wireless     General			<ul> <li>✦ Add</li> <li>∠ Edit</li> </ul>				
License Server     Discovery					Test		
D I NAC			Register Again				
- 🔁 Lists							

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.

👁 Action	×
Search  Search  Search  Search  Send CEF Compliance  Send CEF Message  Send CEF Non Compliance  Send Updates to HP ArcSight Asset Connector  Send Updates to UPArcSight Asset Connector  Send Updates to QRadar SIEM Server  Securption  Authenticate  Manage  Authenticate  Manage  Remediate  Remediate  Remediate  Restrict	This actions sends policy status and host information from CounterACT to ArcSight. Content Trigger Schedule Send host property results Send all Send specific Type filter text Name A Sold Select All Sold Status Clear All Sold Select Status

- **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.

Search Actions Audit Send CEF Compliance - Send CEF Message - Send CEF Non Compliance - Send Message to Syslog - Send Updates to HP ArcSight Asset Connector	This actions sends policy status and host information from CounterACT to ArcSight.
Send Opdates to Gikadar Siem Server	Image: Solid point and point

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.



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.



	🗲 Manag	er Receipt Time 🖨	1 End Time	Name	Device Vendo
	GMT+0	פבר 2:00 15:13:38 2012 19	2/19 15:13:16	Admission	ForeScout
	GMT+0	פבר 2:00 15:13:38 2012 19	2/19 15:13:16	Admission	ForeScout
	GMT+0	פבר 2:00 15:13:38 2012 19	2/19 15:13:16	Admission	ForeScout
	GMT+0	פבר 2:00 15:13:38 2012 19	2/19 15:13:16	Compliance Status	ForeScout
	GMT+0	פבר 2:00 15:13:38 2012 19	2/19 15:13:16	DHCP Server Address	ForeScout
	GMT+0	פבר 2:00 15:13:38 2012 19	2/19 15:13:16	Traffic seen	ForeScout
	GMT+0	פבר 2:00 15:13:38 2012 19	2/19 15:13:16	Corporate/Guest Status	ForeScout
	GMT+0	פבר 2:00 15:13:38 2012 19	2/19 15:13:16	DNS Name	ForeScout
Configure	þ	פבר 2:00 15:13:38 2012 19	2/19 15:13:16	IP Address	ForeScout
Coninguio	þ	פבר 2:00 15:13:38 2012 19	2/19 15:13:16	MAC Address	ForeScout
Delete Connector	þ	פבר 2:00 15:13:38 2012 19	2/19 15:13:16	Host is online	ForeScout
Set as Current Filter	)	פבר 2:00 15:13:38 2012 19	2/19 15:13:16	NIC Vendor	ForeScout
Social carrone ritto	þ	2:00 15:13:38 2012 פבר 19	2/19 15:13:16	Wireless Access Point Name	ForeScout
Add to Current Filter	b	פבר 2:00 15:13:38 2012 19	2/19 15:13:16	Wireless Host Authentication	ForeScout
Create Channel with Filter	5	2:00 15:13:38 2012 פבר 19	2/19 15:13:16	Wireless Connectivity Status	ForeScout
	2	3-00 15-13-20 2012 225 10	2/19 15:13:16	Wireless Controller IP	ForeScout
Send Command	•	Status 🕨	2/19 15:13:16	Wireless Host SSID	ForeScout
Export Connector Configuration A	5	Connector Process 🕨	2/19 15:13:16	Wireless Product	ForeScout
Towned Connection Configuration		Event Flow	2/19 15:13:16	Policies Status	ForeScout
Import Connector Configuration			2/19 15:13:16	Policies Status	ForeScout
Add to Package		Network •	2/19 15:13:16	Policies Status	ForeScout
		Upgrade 🕨 🕨	2/19 15:13:16	Policies Status	ForeScout
Grid View		Adjust 🕨	2/19 15:12:00	Open Ports	ForeScout
Graph View			2/19 15:12:00	Open Ports	ForeScout
		Tech Support	2/19 15:12:00	Open Ports	ForeScout
New Group		Mapping 🕨	2/19 15:12:00	Open Ports	ForeScout
Edit Group		Categorizer/manner	2/19 15:12:00	Open Ports	ForeScout
Delete Group	1	CaustanACT			ForeScout
			Add ArcSight Message eve	ent	ForeScout
Rename	D	2:00 15:12:22 2012 פבר 19	Remove ArcSight Message	event Hostname	ForeScout
Edit Access Control	þ	פבר 2:00 15:12:22 2012 19	Demous all AveCiable Manage		ForeScout
	þ	פבר 2:00 15:12:22 2012 19	Remove an Arcoignt Messa	age events	ForeScout
Show Invalid Reason	þ	פבר 2:00 15:12:22 2012 19	2/19 15:12:00	Admission	ForeScout
Validate Connector	þ	19 פבר 2:00 15:12:22	2/19 15:12:00	Classification Method	ForeScout
Lock Connector	þ	פבר 2:00 15:12:22 2012 19	2/19 15:12:00	Compliance Status	ForeScout
LOCK CONTINUED	þ	פבר 2:00 15:12:22 2012 15:19	2/19 15:12:00	DHCP Server Address	ForeScout
Unlock Connector	b	2:00 15:12:22 2012 פבר 19	2/19 15:12:00	HTTP User Agent	ForeScout
Set deprecated flag	D	2:00 15:12:22 2012 פבר 19	2/19 15:12:00	HTTP User Agent	ForeScout
	5	2:00 15:12:22 2012 פבר 19	2/19 15:12:00 HTTP User Agent		ForeScout
Remove deprecated hag					1

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

Command Parameters	Passilizati	×
Name	Value	
🗆 Misc		
IP Address		
Message		
		OK Cancel

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

	****	
ArcSight Profile Compliance All polic	cies	
IP Address: 10.33.1.144 User: administrator Address: 0050569838a6	NetBIOS Hostname: 10-33-1-144 MA	c 🗟 🗊
Host Information		<b>1</b>
IP Address: MAC Address:	10.33.1.144 0050569838a6	
DNS Name:	10-33-1-144.dom33.lab.forescout.	com
NIC Vendor: ArcSight Messages:	VMWARE, INC. kill_process_	10/30/11 8:07:00 F
Open Ports:	135/TCP	
	3380/TOP	<b>T</b>
4		<b>&gt;</b>
		◆ 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.



learch	Q,	ArcSight Messages: Indicates that a specific ArcSight message was sent to
Properties     Authentication     Zerassification     Zerassification (Advanced)     Computer Serial Number     Device Information	Î	CounterACT.  Meets the following criteria  Does not meet the following criteria  Any Value
<ul> <li>EDS Plugin Properties</li> <li>eEye Retina</li> <li>Fevents</li> <li>ARP Spoofing</li> </ul>		Match case
<ul> <li>Admission</li> <li>ArcSight Messages</li> <li>Malicious Event</li> </ul>		Received within the last V 1 Hours V
<ul> <li>Miscellaneous Events</li> <li>Sessions as Client</li> </ul>	-	Time Period No time and day defined

- **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 MERCHANTIBILITY 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: <u>documentation@forescout.com</u>

7/14/13