



ForeScout

eyeExtend for ArcSight

Configuration Guide

Version 2.9.1



Contact Information

Forescout Technologies, Inc.

190 West Tasman Drive

San Jose, CA 95134 USA

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

Toll-Free (US): 1.866.377.8771

Tel (Intl): 1.408.213.3191

Support: 1.708.237.6591

About the Documentation

- Refer to the Technical Documentation page on the Forescout website for additional documentation: <https://www.Forescout.com/company/technical-documentation/>
- Have feedback or questions? Write to us at documentation@forescout.com

Legal Notice

© 2020 Forescout Technologies, Inc. All rights reserved. Forescout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents can be found at <https://www.Forescout.com/company/legal/intellectual-property-patents-trademarks>. Other brands, products, or service names may be trademarks or service marks of their respective owners.

2020-06-30 10:52

Table of Contents

About the ArcSight Integration	5
About Certification Compliance Mode	5
Use Cases	6
Send Endpoint Status, Compliance, or Property Changes from the Forescout Platform to ArcSight	6
SmartConnector Health and Compliance for Windows	6
Dynamically Update ArcSight Assets	6
Trigger a Forescout Platform Policy and/or Action from ArcSight Correlation Rule	7
ArcSight Network Integration Flow.....	7
SNMP Management Information Base (MIB) and Trap Notifications	9
About Support for Dual Stack Environments.....	9
What to Do	10
Requirements.....	10
Forescout Requirements.....	10
3rd Party Vendor Requirements.....	10
Forescout eyeExtend (Extended Module) Licensing Requirements	10
Per-Appliance Licensing Mode	11
Flexx Licensing Mode	12
More License Information	13
How to Install	13
Configure the Module	14
Register CounterACT Devices with ArcSight.....	14
Test the Module	19
Verify SmartConnectors are Running.....	19
Troubleshoot Registration at the ArcSight Server	20
Define Performance Thresholds	22
Run ArcSight Policy Templates.....	23
ArcSight Action on Disposition Template	24
ArcSight Send SIEM Updates Template.....	28
ArcSight SmartConnector Compliance Template.....	32
Create Custom ArcSight Policies.....	36
Detect ArcSight Devices – Policy Properties.....	36
Manage ArcSight Devices – Policy Actions	37
Send Host and Policy Data from the Forescout Platform to ArcSight	37
Use ArcSight.....	40
ArcSight Action Connector Commands and the Forescout Platform	40
Send an ArcSight Action Connector Command to the Forescout Platform	40
Add a New Host Property to the Forescout Platform.....	43

Health Monitoring.....45

 SNMP MIB for Fore Scout eyeExtend for ArcSight45

 ArcSight MIB Table Attributes46

 SNMP Trap Notifications49

Additional Fore Scout Documentation..... 54

 Documentation Downloads54

 Documentation Portal55

 Fore Scout Help Tools.....55

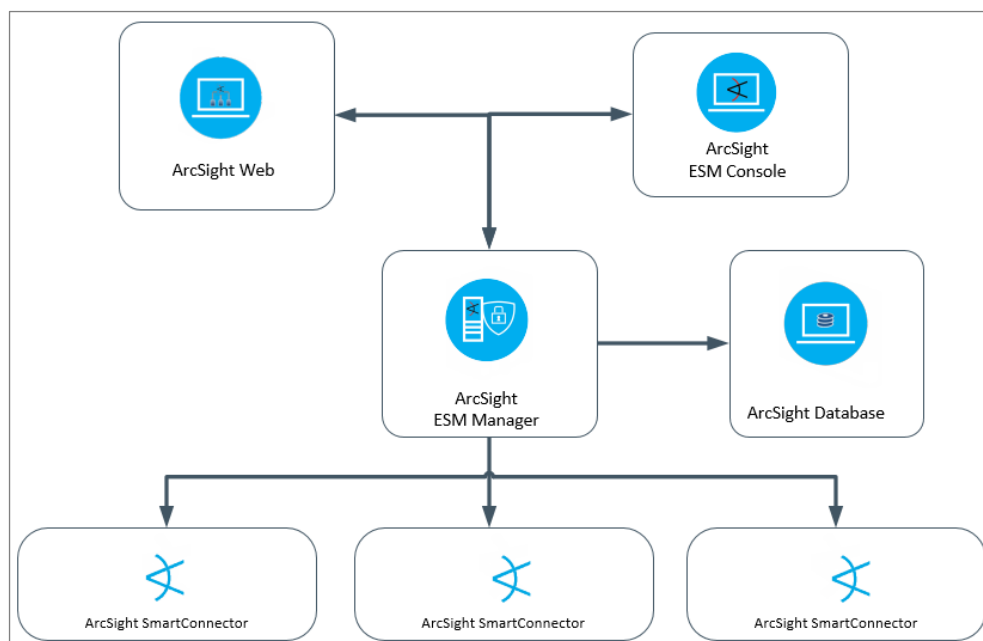
About the ArcSight Integration

The Forescout platform integrates with *ArcSight Enterprise Security Manager (ESM)* ("ArcSight") to provide complete visibility of network endpoints, including unmanaged endpoints. In addition, ArcSight users can leverage Forescout platform tools to quickly take action on network hosts; reduce network risks and control network endpoints.

ArcSight ESM is a product designed for security information and event management (SIEM). ArcSight ESM collects security log data from an enterprise's security technologies, operating systems, applications and other log sources, and analyzes that data for signs of compromise, attacks or other malicious activity.

The following components of ArcSight may be referred to in this document. Refer to the *ArcSight User Guide* for further definitions of:

- ArcSight Enterprise Security Manager (ESM)
- ArcSight Database
- ArcSight SmartConnectors
- ArcSight Web (user interface)
- ArcSight Console (user interface)



About Certification Compliance Mode

Forescout eyeExtend for CrowdStrike supports Certification Compliance mode. For information about this mode, refer to the *Forescout Installation Guide*. See [Additional Forescout Documentation](#) for information on how to access this guide.

Use Cases

This section describes important use cases supported by this module.

- [Send Endpoint Status, Compliance, or Property Changes from the Forescout Platform to ArcSight](#)
- [SmartConnector Health and Compliance for Windows](#)
- [Dynamically Update ArcSight Assets](#)
- [Trigger a Forescout Platform Policy and/or Action from ArcSight Correlation Rule](#)

Send Endpoint Status, Compliance, or Property Changes from the Forescout Platform to ArcSight

You can send important policy status and host information from the Forescout platform to ArcSight. This is done by using the Actions feature in the Forescout platform.

By sending updates from the Forescout platform to ArcSight, you can send either all host properties discovered or just specific properties.

Details of any changes in the host properties are sent to ArcSight. For example, the host IP property and its anti-virus properties are sent to ArcSight. If either of these properties is updated, that information will be sent. This is vital to identifying specific endpoint events.

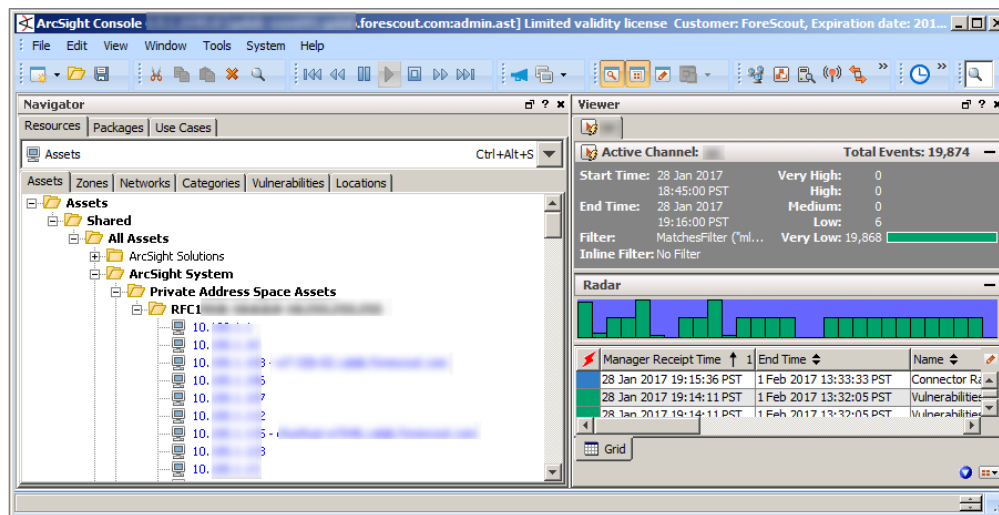
For more information, see [ArcSight Send SIEM Updates Template](#).

SmartConnector Health and Compliance for Windows

An ArcSight security administrator can ensure that the ArcSight SmartConnector agents are installed and functioning properly on Windows endpoints within the corporate network. A SmartConnector agent is a Windows Log Collection Agent, a stand-alone Windows application that is installed on a Windows host to allow ArcSight to collect event logs. For more information, see [Verify SmartConnectors are Running](#) or refer to the *ArcSight User Guide*.

Dynamically Update ArcSight Assets

The Assets tab in the ArcSight Console is not a traditional NAC + SIEM use case of receiving and correlating events. An asset record is built for each IP address and can be referenced in Forescout platform rules, actions, etc. This is a powerful and unique integration with ArcSight where you can effectively replicate the host profile record in the Forescout platform from Forescout eyeExtend for ArcSight via the Assets tab of the Navigator in the ArcSight Console.



For more information, see [ArcSight Action Connector Commands and the ForeScout Platform](#).

Trigger a ForeScout Platform Policy and/or Action from ArcSight Correlation Rule

An organization uses a network firewall to detect targeted Denial of Service (DOS) attacks on their web applications. The same organization also has ArcSight SIEM to collect and aggregate logs from the ForeScout platform, firewall, and web applications. When ArcSight detects a targeted DOS attack via firewall log correlation, a correlated event is generated.

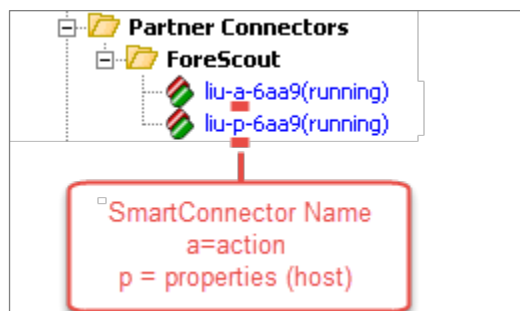
To prevent further disruption of service to the application(s) on the network, the security administrator could leverage a ForeScout platform policy to have the source of the attack automatically blocked by the firewall. There are two methods to do this: manually and automatically.

For more information, see [ArcSight Action Connector Commands and the ForeScout Platform](#) and [Send an ArcSight Action Connector Command to the ForeScout Platform](#).

ArcSight Network Integration Flow

In the ArcSight Console, the Partner Connectors folder called *ForeScout* registers two CounterACT® devices: *p SmartConnector* and a *SmartConnector*

To tell the difference between these two SmartConnectors, look at the name of the SmartConnector.



- **p = properties** - <your prefix>-**p**-XXXX - From the Forescout platform, host properties, asset data and automated compliance messages are sent through the *Properties (p) SmartConnector* and then to the ArcSight Console.
- **a = action** - <your prefix>-**a**-XXXX - From the ArcSight Console, customized actions are sent through the *Action (a) SmartConnector* and then to the Forescout platform. You can right-click on the *Action SmartConnector* and select an action to be done on a detected device. For more information, see [Managing ArcSight Devices – Policy Actions](#). Alternately, you can use the *Action SmartConnector*.

From the Forescout Platform to ArcSight

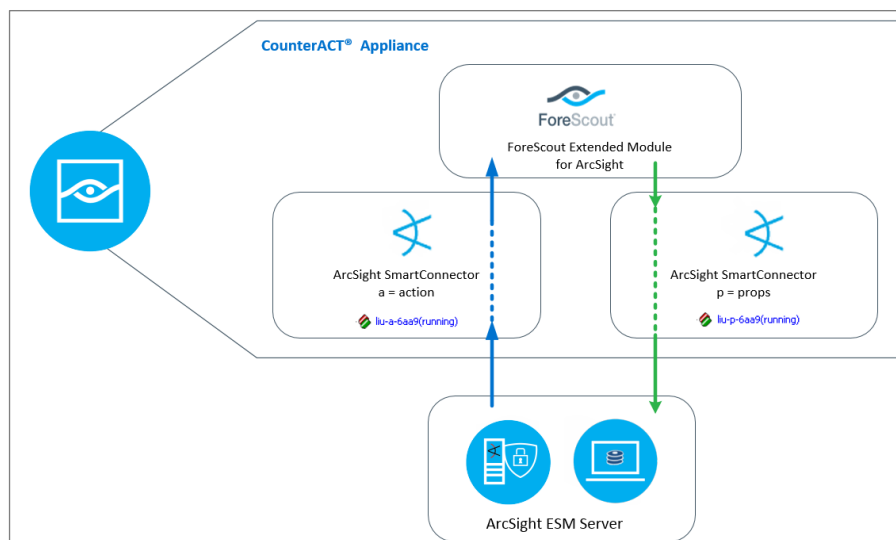
Data flow from the Forescout platform to the ArcSight server are transmitted in this order:

1. Forescout eyeExtend for ArcSight
2. ArcSight SmartConnector, sending host properties (p)
3. ArcSight server

From ArcSight to the Forescout Platform

The ArcSight server sends data flow to the Forescout platform in this order:

1. ArcSight server
2. ArcSight SmartConnector, sending action commands (a)
3. Forescout eyeExtend for ArcSight



SNMP Management Information Base (MIB) and Trap Notifications

Forescout eyeExtend for ArcSight provides a Management Information Base (MIB) that enables remote monitoring of module health – operational status and changes in configuration, performance and status. The MIB makes the following SNMP information available:

- [ArcSight MIB Table Attributes](#) – attributes that provide operational status information about the interaction between the module and its ArcSight server peer. It is assumed that external management systems query the Enterprise Manager for module status information.
- [SNMP Trap Notifications](#) – trap notifications, resulting from the occurrence of status, configuration and performance changes, are issued by the module. Each trap notification provides details about the specific change event that occurred. Trap notifications, issued by CounterACT Appliances and their modules, are forwarded to the Enterprise Manager and can be listened for/monitored by external management systems.

About Support for Dual Stack Environments

The Forescout platform detects endpoints and interacts with network devices based on both IPv4 and IPv6 addresses. However, **IPv6 addresses are not yet supported by this eyeExtend module.** The functionality described in this document is based only on IPv4 addresses. IPv6-only endpoints are typically ignored or not detected by the properties, actions, and policies provided by this eyeExtend module.

What to Do

Perform the following in order to carry out the integration:

- Verify that you have met the [Requirements](#).
- [Install the ArcSight Module](#).
- Set up the ArcSight servers to work with the Forescout platform. See [Register CounterACT Devices with ArcSight](#) and [Define Performance Thresholds](#).

Requirements

This section describes:

- [Forescout Requirements](#)
- [3rd Party Vendor Requirements](#)
- [Forescout eyeExtend \(Extended Module\) Licensing Requirements](#)

Forescout Requirements

This module requires the following Forescout releases and other components:

- Forescout version 8.2.
- A module license for Forescout eyeExtend for ArcSight. See [Forescout eyeExtend \(Extended Module\) Licensing Requirements](#).

3rd Party Vendor Requirements

The following 3rd-Party vendor packages are required to install this release:

- ArcSight 6.9.1.c
- For information about the vendor models (hardware/software) and versions (product/OS) that are validated for integration with this Forescout component, refer to the [Forescout Compatibility Matrix](#).

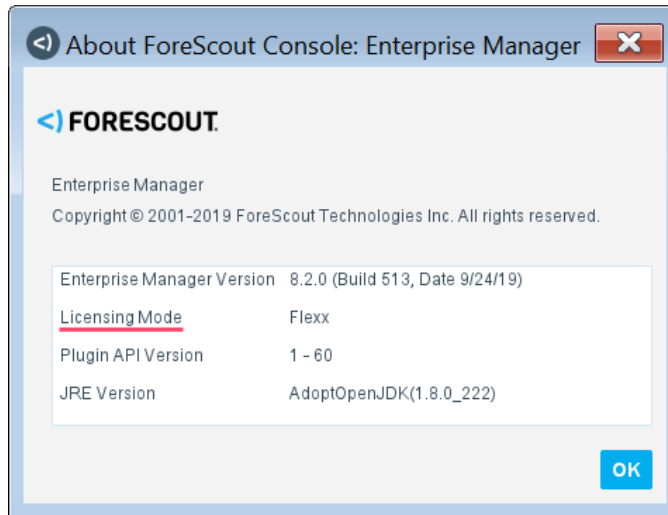
Forescout eyeExtend (Extended Module) Licensing Requirements

This Forescout eyeExtend module requires a valid license. Licensing requirements differ based on which licensing mode your deployment is operating in:

- [Per-Appliance Licensing Mode](#)
- [Flexx Licensing Mode](#)

To identify your licensing mode:

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




Per-Appliance Licensing Mode

When installing the module, you are provided with a 90-day demo license.

If you would like to continue exploring the module before purchasing a permanent license, you can request a demo license extension. Consult with your Forescout representative before requesting the extension. You will receive email notification and alerts at the Console before the demo period expires.

To continue working with the module after the demo period expires, you must purchase a permanent module license.

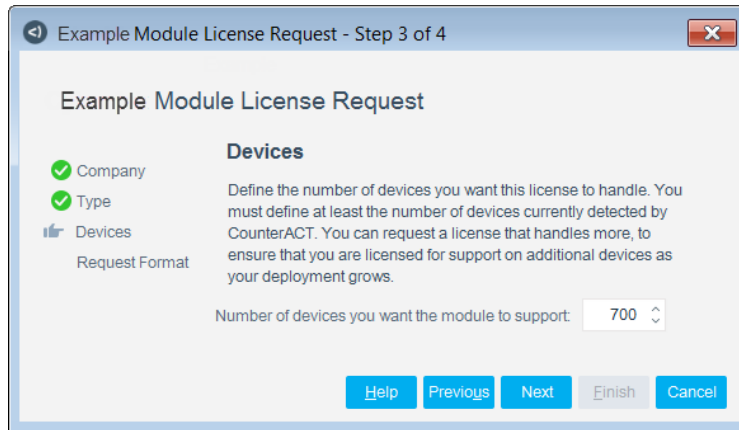
Demo license extension requests and permanent license requests are made from the Console.

 *This module may have been previously packaged as a component of an Integration Module which contained additional modules. If you already installed this module as a component of an Integration Module, you can continue to use it as such. Refer to the section about module packaging in the Forescout Administration Guide for more information.*

Requesting a License

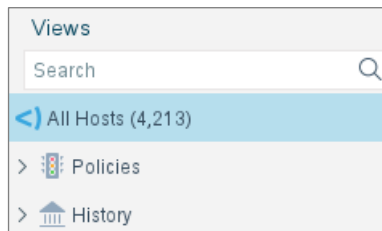
When requesting a demo license extension or permanent license, you are asked to provide the device *capacity* requirements. This is the number of devices that you want this license to handle. You must define at least the number of devices currently detected by the Forescout platform. You can request a license that handles more to ensure that you are licensed for support on additional devices as your deployment grows.

Enter this number in the **Devices** pane of the Module License Request wizard, in the Console Modules pane.



To view the number of currently detected devices:

1. Select the **Home** tab.
2. In the Views pane, select the **All Hosts** folder. The number in parentheses displayed next to the **All Hosts** folder is the number of devices currently detected.



Flexx Licensing Mode

When you set up your Forescout deployment, you must activate a license file containing valid licenses for each feature you want to work with in your deployment, including eyeExtend modules. After the initial license file has been activated, you can update the file to add additional eyeExtend licenses or change endpoint capacity for existing eyeExtend modules. For more information on obtaining eyeExtend licenses, contact your Forescout sales representative.

 *No demo license is automatically installed during system installation.*

License entitlements are managed in the [Forescout Customer Portal](#). After an entitlement has been allocated to a deployment, you can activate or update the relevant licenses for the deployment in the Console.

Each eyeExtend license has an associated capacity, indicating the number of endpoints the license can handle. The capacity of each eyeExtend license varies by module but does not exceed the capacity of the Forescout eyeSight license.

- Integration Modules, which package together groups of related licensed modules, are not supported when operating in Flexx Licensing Mode. Only eyeExtend modules, packaging individual licensed modules are supported. The eyeExtend Connect Module is an eyeExtend module even though it packages more than one module.

More License Information

For more information on eyeExtend (Extended Module) licenses:

- **Per-Appliance Licensing.** Refer to the *Forescout Administration Guide*.
- **Flexx Licensing.** Refer to the *Flexx Licensing How-to Guide*.

You can also contact your Forescout sales representative for more information.

How to Install

To install the module:

1. Navigate to one of the following Forescout download portals, depending on the licensing mode your deployment is using:

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

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

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

- The installation begins immediately after selecting Install and cannot be interrupted or canceled.

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

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

- Some components are not automatically started following installation.

Configure the Module

This section describes how to configure Forescout eyeExtend for ArcSight, including how to:

- [Register CounterACT Devices with ArcSight](#)
- [Test the Module](#)
- [Verify SmartConnectors are Running](#)
- [Define Performance Thresholds](#)

Register CounterACT Devices with ArcSight

To enable communication with ArcSight, you should register CounterACT Appliances or the Enterprise Manager to an ArcSight server.

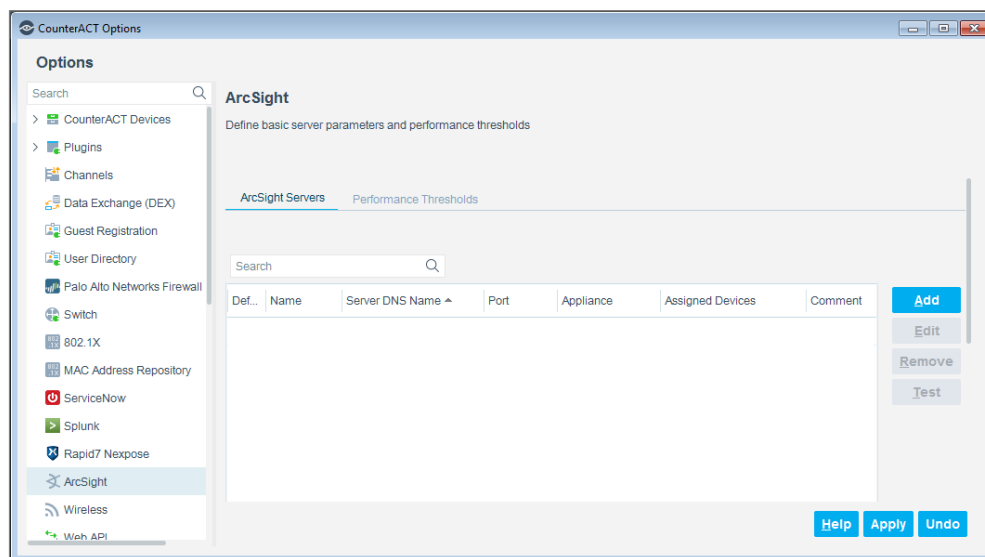
In the simplest case, you register a single ArcSight server. By default, all CounterACT devices communicate with that server.

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

The **Agent Name** is a required configuration field that identifies all Appliances connected to an ArcSight server. This field should be unique for each ArcSight server that communicates with CounterACT Appliances.


To start Forescout eyeExtend for ArcSight:

1. In the Options pane, select **Modules**.
2. In the Modules pane, select **ArcSight** and then select **Start**. Forescout eyeExtend for ArcSight and its SmartConnectors will be started.
3. Select **Configure**.



4. Continue to the next section.

To register CounterACT devices with an ArcSight server:

 Before proceeding, be sure that you have the electronic copy of the server certificate on hand. This requirement only applies if the ArcSight server is running with a non-default demo CA certificate such as a self-signed or CA certificate. If you are not intending to import an ArcSight certificate during the setup, do not select the **Verify Server Certificate** option.

1. In the ArcSight Servers tab, select **Add**.

Add ArcSight Server - Step 1 of 2

Add ArcSight Server

General
Assigned CounterACT devices

Define basic server parameters.

Name

Server DNS Name

Port

☐ Use one-time password for connectors registration

User Name

Password

Verify Password

Appliance

Connector Name

Comment

Certificate ☒ Verify server certificate

2. Enter the *server details*:

- In the **Name** field, enter the server name.
- In the **Server DNS Name** field, enter a fully qualified domain name (FQDN) as the ArcSight server name. Do not use an IP Address.
- Enter the port used by the ArcSight server. The default is 8443.
- In the **User Name** field, enter the name of the user logged in to the ArcSight server.
- In the **Password** field, enter a password of the user logging into the ArcSight server.
- In the **Verify Password** field, re-enter the password to verify it.
- (Optional) If you want to work with one-time passwords, select the **Use one-time password for connector registration** option. The purpose of this field is in support of the registration process. In case the first credentials do not work, the server is to use the second credentials for logging in.

☒ Use one-time password for connectors registration

First credentials

User Name

Password

Verify Password

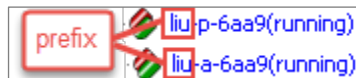
Second credentials

User Name

Password

Verify password

- In the **Appliance** field, select the CounterACT device that will communicate directly with the ArcSight server.
- In the **Connector Name** field, enter the connector prefix for the Appliance that will be registered 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.



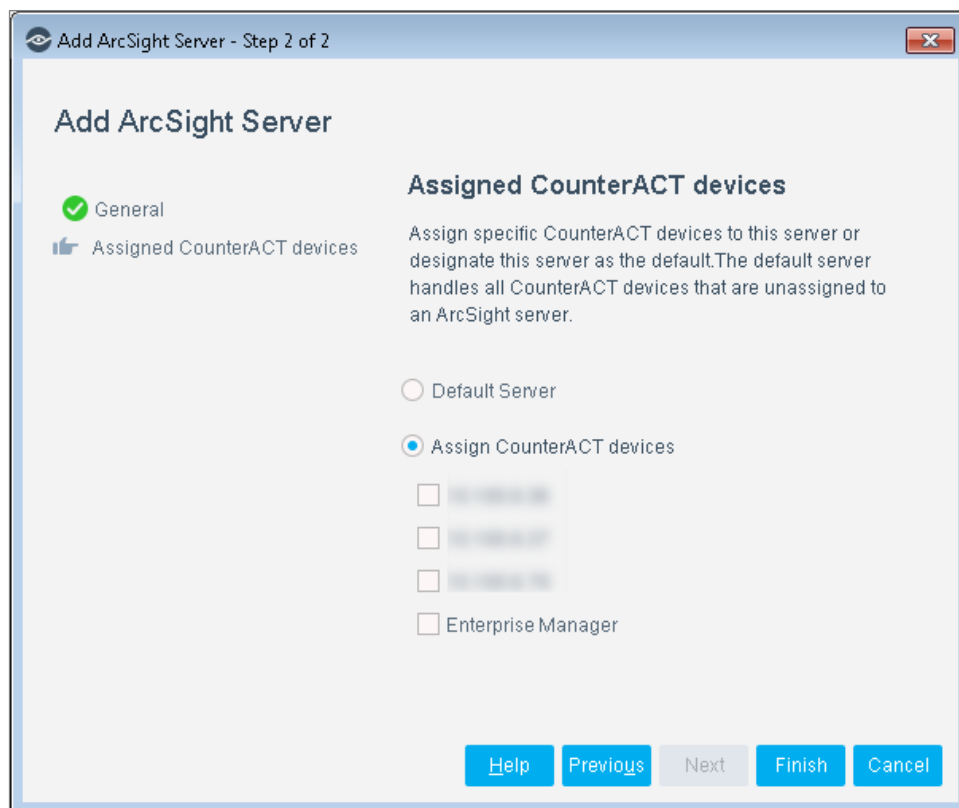
- (Optional) In the **Comment** field, enter comments about the server.
- In the **Certificate** field, if ArcSight is using its default certificate, you can register the SmartConnectors using the username and password of the user logging into the ArcSight server. However, for your protection, it is recommended that you import a new certificate. If you are not intending to import an ArcSight certificate during setup, do not select the **Verify Server Certificate** option.

If ArcSight is using either a self-signed or CA certificate, then the user is required to get the certificate (PEM format) from the ArcSight server and then upload to the Forescout platform using the Browse option.

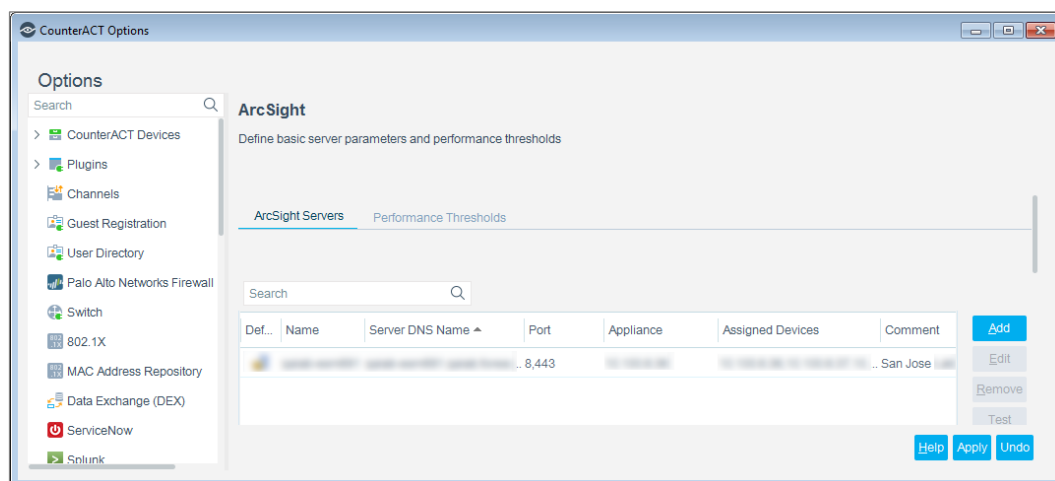
The **Verify server certificate** option is for validating that the uploaded certificate is in the correct format.

To get the **Certificate**, refer to the ArcSight documentation.

3. Select **Next**.



4. In the Assigned CounterACT devices pane, choose one of the following options:
 - Select **Default Server** to make this server the target for all CounterACT Appliances 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 Appliances that communicate with this server.
5. Select **Finish**. The server is listed in the ArcSight pane.



6. (Optional) Repeat steps [3](#) through [7](#) to add another ArcSight server. No more than one CounterACT Appliance can be registered to an ArcSight server.
7. Select **Apply**.
8. In the Options pane, select **Modules**.
9. In the Modules pane, select **ArcSight** and select **Start**.
10. Select each CounterACT device selected in step [6](#) to communicate with an ArcSight server, and select **OK**. Forescout eyeExtend for ArcSight starts on the selected devices.

Test the Module

You can run an optional test to check the network and SSL connection to an ArcSight server, and to display the ArcSight server certificate.

The displayed certificate can be copied, saved and selected as the certificate to use for future ArcSight server certificate verification.

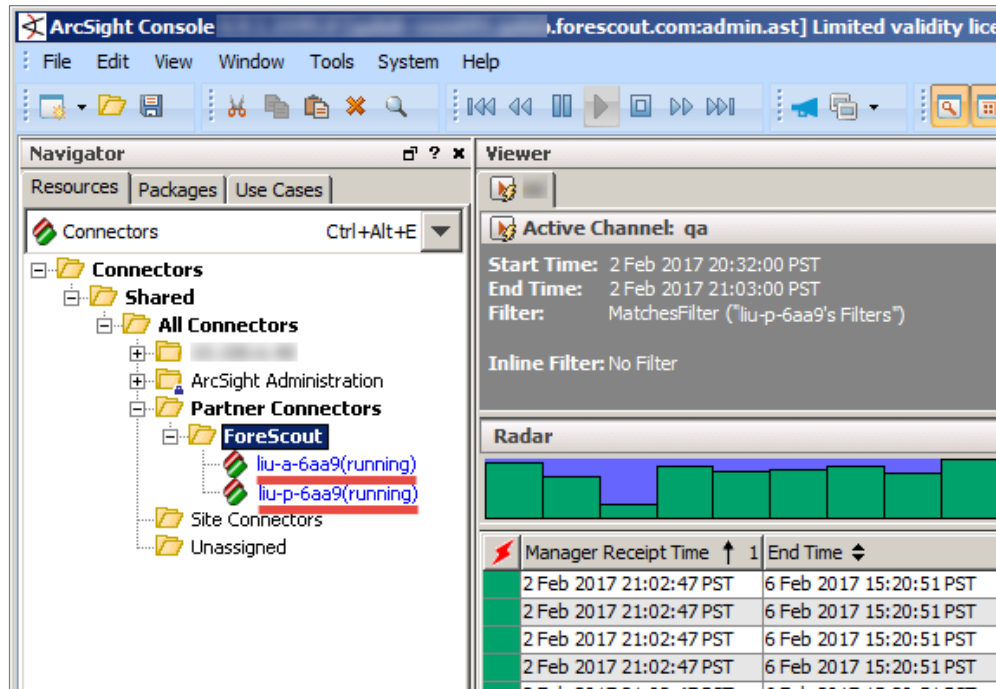
 *The test does not verify user credentials.*

To test the module configurations:

1. In the Options pane, select **Modules** and then select **ArcSight**.
2. Select an item in the ArcSight Servers tab and then select **Test**. Using configured settings, the Forescout platform attempts to connect with the ArcSight server and to retrieve endpoint property values for the specified device.
3. The test results are displayed.
4. If the test passed, select **Close**. If the test failed, see [Troubleshoot Registration at the ArcSight Server](#).

Verify SmartConnectors are Running

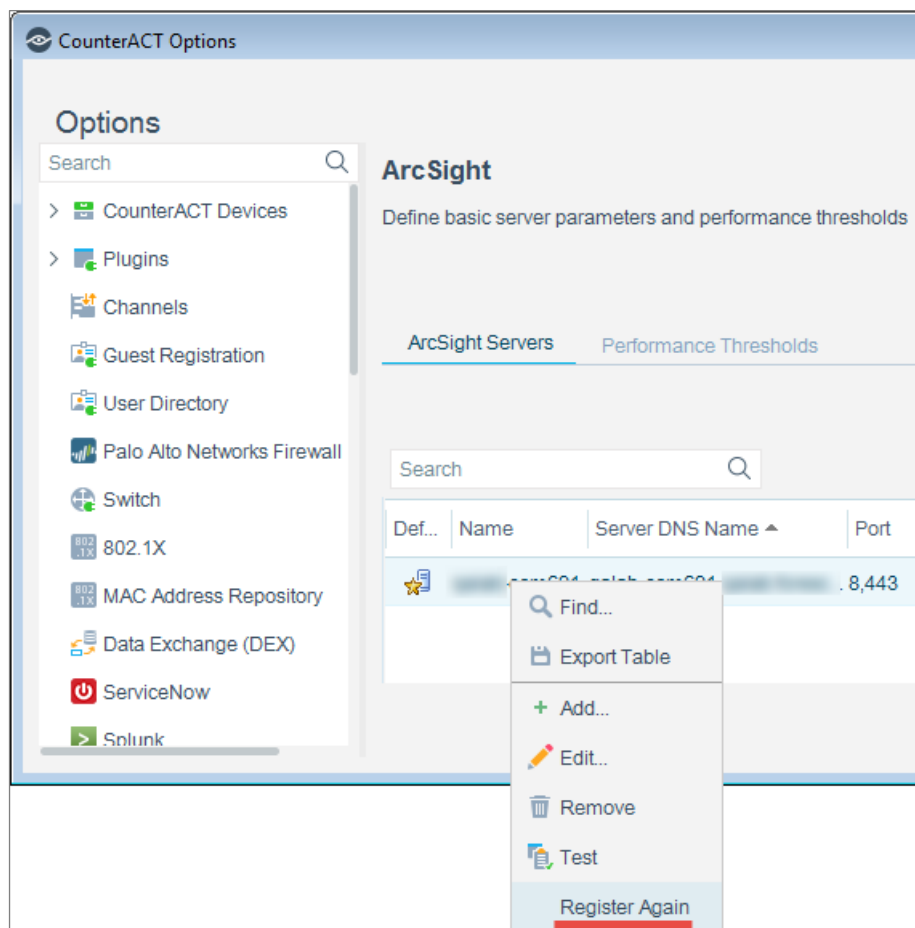
1. Log in to the ArcSight Console.
2. In the Resources tab of the Navigator, browse to **Connectors**, expand **Shared**, expand **All Connectors** and expand **Partner Connectors**.
3. Expand **Forescout**. There should be two SmartConnectors listed in blue font:
 - <your prefix>-a-XXXX(running), where *a* = Action.
 - <your prefix>-p-XXXX(running), where *p* = Properties



4. If the two SmartConnectors are not there, see [Troubleshoot Registration at the ArcSight Server](#).

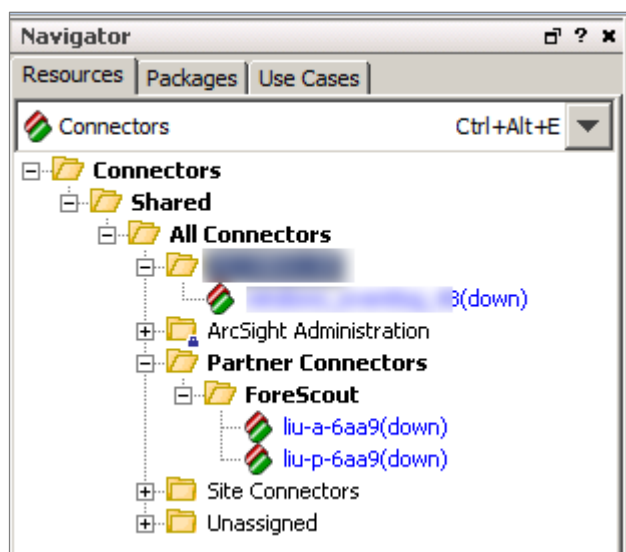
Troubleshoot Registration at the ArcSight Server

When you define configuration settings for an ArcSight server, the module accesses the server and registers your CounterACT Appliance as an ArcSight connector. In some cases, the CounterACT Appliance 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 Appliance with the server.



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

- The status at the ArcSight Access Console is *down*.



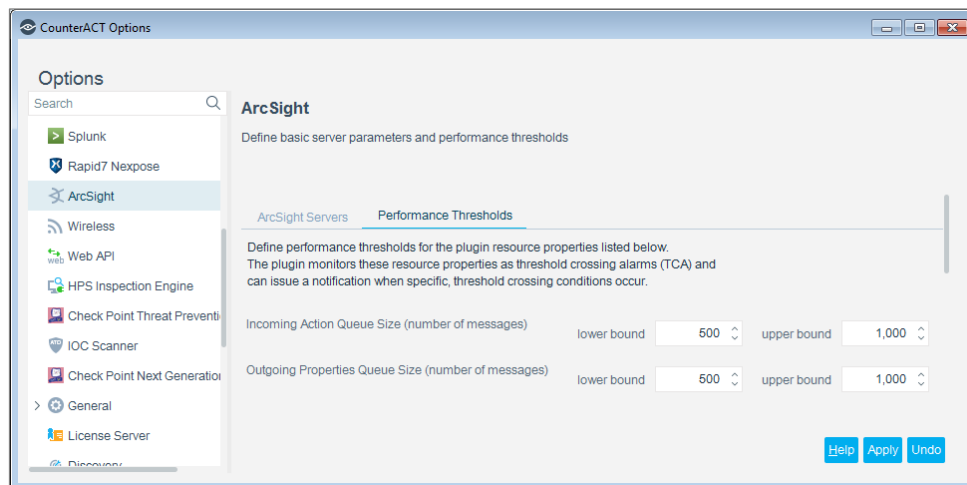
In this case, remove the connector at the ArcSight server in the Forescout Console before you select **Register Again**.

- You do not see it displayed in the ArcSight Console.
- 📄 Using the **Register Again** option on a connection that is working properly can disconnect the connector.

Define Performance Thresholds

Forescout eyeExtend for ArcSight reports, via its *Outgoing Properties* queue, endpoint property information to an ArcSight server. The module receives from an ArcSight server, via its *Incoming Action* queue, policy actions to execute. Define performance thresholds for the following module resource properties:

- Incoming Action Queue Size (number of messages)
- Outgoing Properties Queue Size (number of messages)



For each resource property, both an upper threshold value (upper bound) and a lower threshold value (lower bound) are defined. The module monitors these resource properties as threshold crossing alarms (TCA) and can issue a notification, for example, an SNMP trap notification. The following threshold crossing conditions are monitored:

- When the property's current value exceeds its upper bound value (now in HIGH/EXCEEDED capacity state) after being in the NORMAL capacity state (that is, previously below the lower bound value). Notification trap severity varbind is set to *Warning*.
- When the property's current value moves below its lower bound value (now in NORMAL capacity state) after being in the HIGH/EXCEEDED capacity state (that is, previously exceeded the upper bound value). Notification trap severity varbind is set to *Cleared*.

To define the performance thresholds of resource properties:

- In the Console, select **Tools** and then select **Options**. The Options pane opens.
- Under **Modules**, select the **ArcSight** folder.
- Select the Performance Thresholds tab.

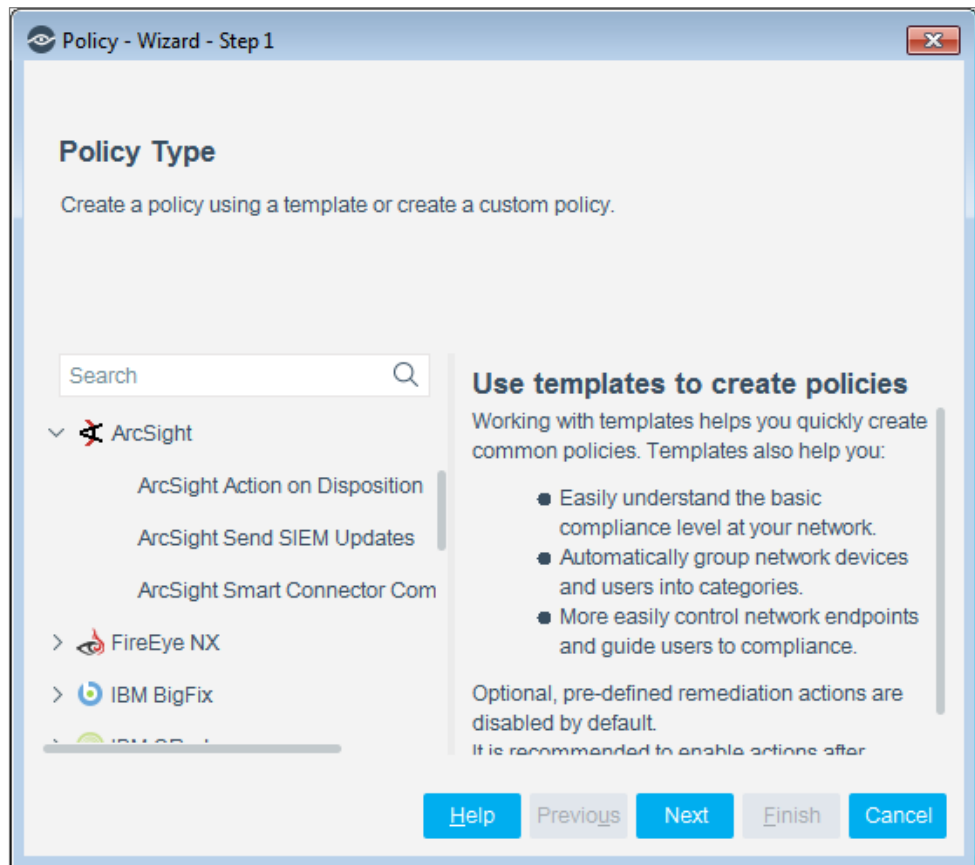
Run ArcSight Policy Templates

Forescout platform templates help you quickly create important, widely used policies that easily control endpoints and can guide users to compliance.

Some predefined actions are enabled by default - no fine tuning is necessary. For actions that are disabled by default, only enable them after some testing and fine tuning.

The following templates are available for detecting and managing endpoints:

- [ArcSight Action on Disposition Template](#)
- [ArcSight Send SIEM Updates Template](#)
- [ArcSight SmartConnector Compliance Template](#)



For more information about creating policies, refer to the Forescout Templates and the Policy Management chapters in the *Forescout Administration Guide*.

For more information on how these templates work in ArcSight, see [Using ArcSight](#)


ArcSight Action on Disposition Template

The Forescout platform can send policy and host information to ArcSight based on set policy conditions, or on a regular schedule.

Forescout platform policies use a wide range of host conditions to trigger various management and remediation actions. When the conditions of the policy are met, the actions are implemented. With Forescout eyeExtend for ArcSight, Forescout platform policies can include notification messages to ArcSight servers as an action.

To implement ArcSight reporting, define a Forescout platform policy that includes the ArcSight update action. When the conditions of this policy are met, ArcSight notification is implemented in one of several modes:

- **One-time report:** current policy/host information is sent once when the conditions of the policy are met.
- **Update reporting:** a message is sent whenever the host information or policy status changes.
- **Periodic reporting:** a message is sent at regularly defined intervals.

 *The policy conditions must be met at least once to initiate update reporting or periodic reporting. Similarly, the Forescout platform stops change reporting and periodic reporting when the conditions of the policy are no longer met.*

You can further modify notification behavior using standard action scheduling options.

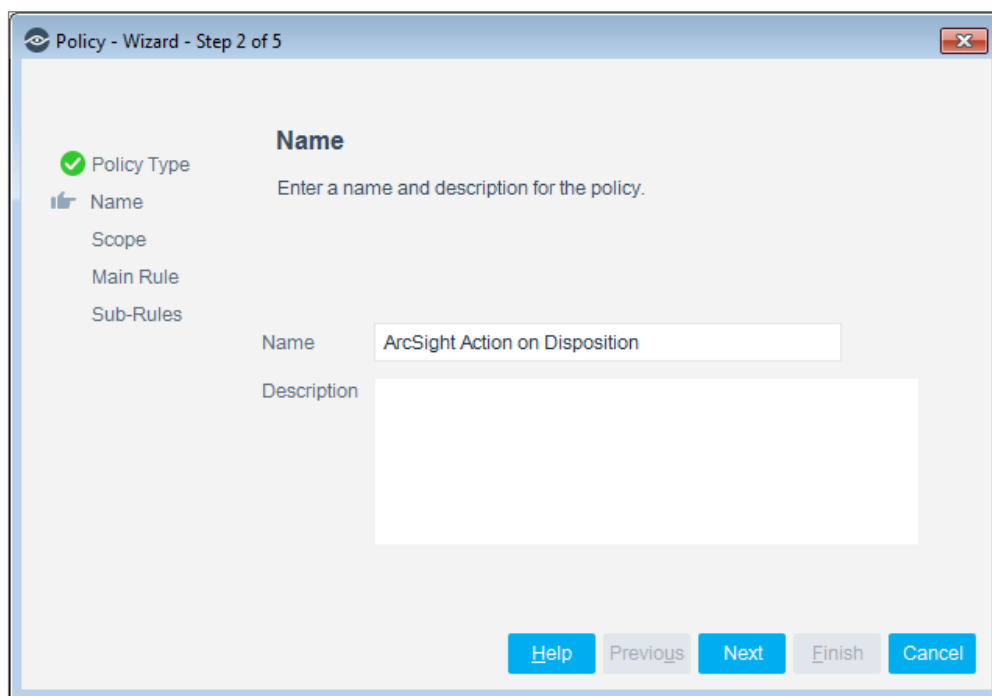
To use the ArcSight Action on Disposition policy template:

Use this template to apply actions to an endpoint for which the Forescout platform received a disposition event message from ArcSight. Sub-rules of the policy apply specific actions depending upon the disposition of the most recent ArcSight event received for the endpoint. The sub-rules will indicate that an ArcSight operator or administrator has requested the following actions be taken on an endpoint identified by the disposition.

1. Log in to the Console and select **Policy**.
2. Select **Add** from the Policy Manager. The Policy Wizard opens.
3. Expand the **ArcSight** folder and select **ArcSight Action on Disposition**. The ArcSight Action on Disposition pane opens.
4. Select **Next**.

Name the Policy

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

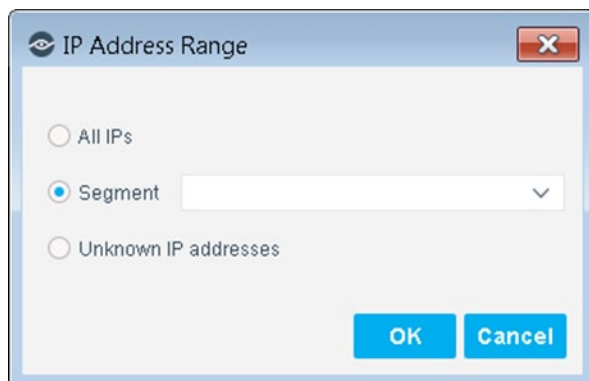


5. Define a unique name for the policy you are creating based on this template, and enter a description.
 - Make sure names are accurate and clearly reflect what the policy does. For example, do not use a generic name such as `My_Compliance_Policy`.
 - Use a descriptive name that indicates what your policy is verifying and which actions will be taken.
 - Ensure that the name indicates whether the policy criteria must be met or not met.
 - Avoid having another policy with a similar name.
6. Select **Next**. Both the Scope pane and the IP Address Range dialog box open.

Define Which Endpoints 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:

- **All IPs:** Include all IP addresses in the Internal Network.
- **Segment:** Select a previously defined segment of the network. To specify multiple segments, select **OK** or **Cancel** to close this dialog box, and select **Segments** from the Scope pane.
- **Unknown IP addresses:** Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.

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

9. Select **Next**. The Main Rule pane opens.

How Endpoints Are Detected and Handled

This section describes the main rule and sub-rules of the policy created by this template. Policy rules instruct the Forescout platform how to detect and handle endpoints defined in the policy scope.

Endpoints that match the Main Rule are included in the policy inspection. Endpoints that do not match this rule are not inspected for this policy. Sub-rules automatically follow up with endpoints after initial detection and handling, streamlining separate detection and actions into one automated sequence.

Sub-rules are performed in order until a match is found. When a match is found, the corresponding action is applied to the endpoint. If the endpoint does not match the requirements of the sub-rule, it is inspected by the next rule.

Main Rule

The main rule of this policy does not filter hosts, but it specifies recheck behavior for the policy. By default, the policy is evaluated every eight hours, and is applied to newly discovered endpoints.

The main rule of this policy states to apply actions to an endpoint for which the Forescout platform received a disposition event message from ArcSight.

Policy - Wizard - Step 4 of 5

✓ Policy Type
✓ Name
✓ Scope
Main Rule
Sub-Rules

Main Rule

Use this screen to review policy sub-rule definitions.
Hosts are inspected by each sub-rule in the order shown. When a match is found, the action defined is applied. If no match is found, the host is inspected against the next sub-rule.

Condition

A host matches this rule if it meets the following condition:

All criteria are True

Criteria
ArcSight Messages - Any Value Within the last 1 hour

Add Edit Remove

Actions

Actions are applied to hosts matching the above condition.

Ena...	Action	Details
No items to display		

Add Edit Remove

Help Previous Next Finish Cancel

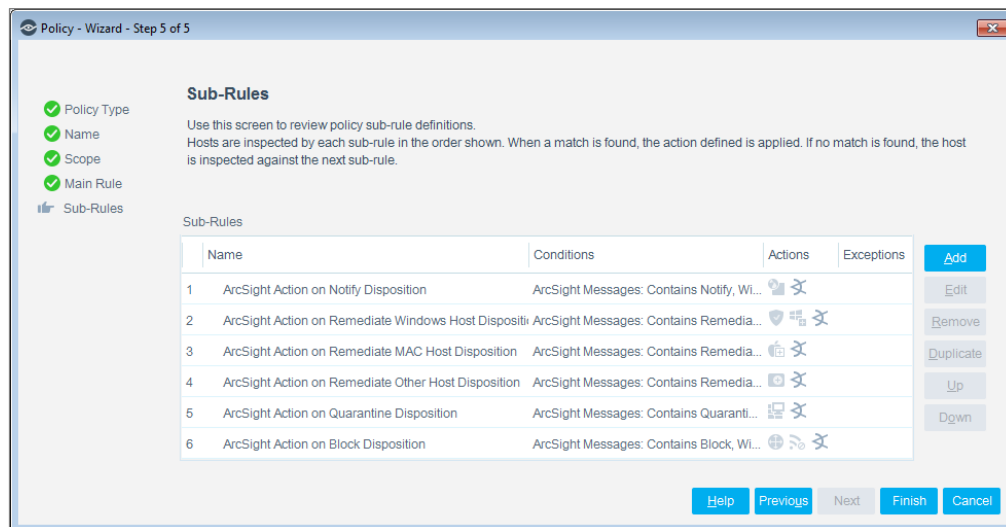
10.Select **Next**. The Sub-Rules pane opens.

Sub-Rules

Hosts that match the Main Rule are included in the policy inspection. Hosts that do not match this rule are not inspected for this policy.

Sub-rules allow you to automatically follow up with hosts after initial detection and handling. Creating sub-rules lets you streamline separate detection and actions into one automated sequence. Sub-rules are performed in order until a match is found.

The sub-rules of this policy apply specific actions depending upon the disposition of the most recent ArcSight event received for the endpoint. The sub-rules will indicate that an ArcSight operator or administrator has requested the following actions be taken on an endpoint identified by the disposition.



11. Select **Finish**.

12. In the Console, select **Apply** to save the policy.

ArcSight Send SIEM Updates Template

Use this template to periodically send host information to ArcSight Console. By default, this policy sends all property and policy information, for all endpoints, using syslog as a communication method configured for ArcSight interaction.

To use the ArcSight Send SIEM Updates policy template:

1. Log in to the Console and select **Policy**.
2. Select **Add** from the Policy Manager. The Policy Wizard opens.
3. Expand the **ArcSight** folder and select **ArcSight Send SIEM Updates**. The ArcSight Send SIEM Updates pane opens.
4. Select **Next**.

Name the Policy

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

Policy - Wizard - Step 2 of 5

Name
Enter a name and description for the policy.

Policy Type
Name
Scope
Main Rule
Sub-Rules

Name: ArcSight Send SIEM Updates
Description:

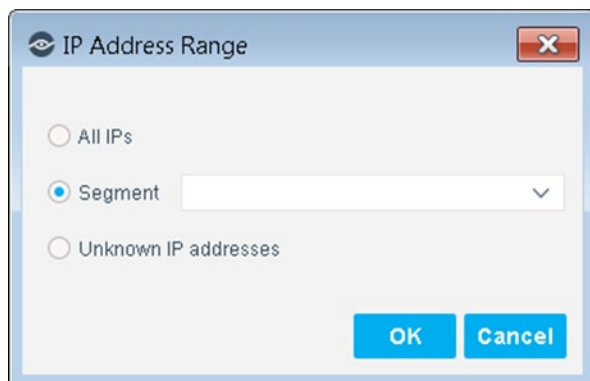
Help Previous Next Finish Cancel

5. Define a unique name for the policy you are creating based on this template, and enter a description.
 - 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`.
 - Use a descriptive name that indicates what your policy is verifying and which actions will be taken.
 - Ensure that the name indicates whether the policy criteria must be met or not met.
 - Avoid having another policy with a similar name.
6. Select **Next**. Both the Scope pane and the IP Address Range dialog box open.

Define Which Endpoints 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:

- **All IPs:** Include all IP addresses in the Internal Network.
- **Segment:** Select a previously defined segment of the network. To specify multiple segments, select **OK** or **Cancel** to close this dialog box, and select **Segments** from the Scope pane.
- **Unknown IP addresses:** Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.

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

9. Select **Next**. The Main Rules pane opens.

How Endpoints Are Detected and Handled

This section describes the main rule and sub-rules of the policy created by this template. Policy rules instruct the Forescout platform how to detect and handle endpoints defined in the policy scope.

Endpoints that match the Main Rule are included in the policy inspection. Endpoints that do not match this rule are not inspected for this policy. Sub-rules automatically follow up with endpoints after initial detection and handling, streamlining separate detection and actions into one automated sequence.

Sub-rules are performed in order until a match is found. When a match is found, the corresponding action is applied to the endpoint. If the endpoint does not match the requirements of the sub-rule, it is inspected by the next rule.

Main Rule

The main rule of this policy does not filter hosts, but it specifies recheck behavior for the policy. By default, the policy is evaluated every eight hours, and is applied to newly discovered endpoints.

The main rule of this policy is an action - periodically send host information to ArcSight. By default, this policy sends all property and policy information, for all endpoints, using all syslog as a communication method configured for ArcSight interaction.

Policy - Wizard - Step 4 of 5

- ✓ Policy Type
- ✓ Name
- ✓ Scope
- Main Rule
- Sub-Rules

Main Rule

Use this screen to review policy sub-rule definitions.
Hosts are inspected by each sub-rule in the order shown. When a match is found, the action defined is applied. If no match is found, the host is inspected against the next sub-rule.

Condition

A host matches this rule if it meets the following condition:

All criteria are True

Criteria

No items to display

Actions

Actions are applied to hosts matching the above condition.

Enable	Action	Details
<input checked="" type="checkbox"/>	Send Updates to HPE ArcSight Asset ...	Send Updates to...

Buttons: Add, Edit, Remove

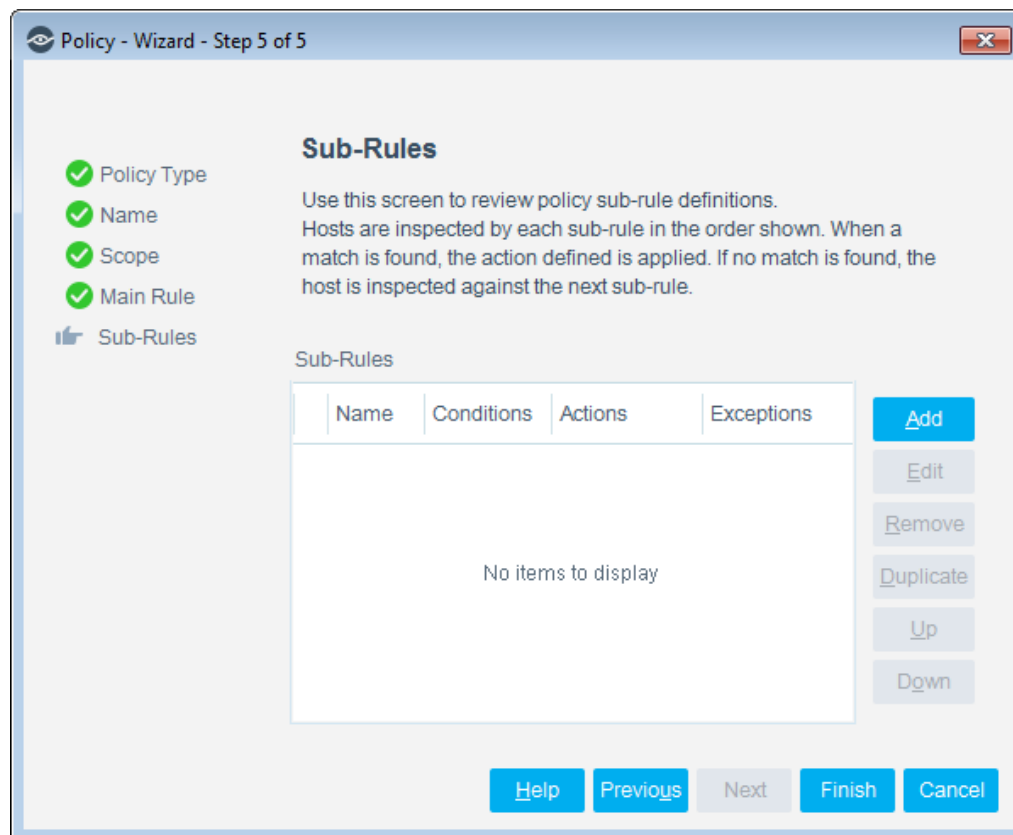
Buttons: Help, Previous, Next, Finish, Cancel

10.Select **Next**. The Sub-Rules pane opens.

Sub-Rules

Hosts that match the Main Rule are included in the policy inspection. Hosts that do not match this rule are not inspected for this policy.

Sub-rules allow you to automatically follow up with hosts after initial detection and handling. Creating sub-rules lets you streamline separate detection and actions into one automated sequence. Sub-rules are performed in order until a match is found.



11. Select **Finish**.

12. In the Console, select **Apply** to save the policy.

ArcSight SmartConnector Compliance Template

Use this template to create a Forescout platform policy that:

- Detects endpoints on which the ArcSight SmartConnector is installed and running.
- Detects endpoints on which the ArcSight SmartConnector is installed but not running.
- Detects endpoints on which the ArcSight SmartConnector is not installed.
- Detects endpoints on which the ArcSight SmartConnector status is irresolvable.

In addition, optional actions can be used to:

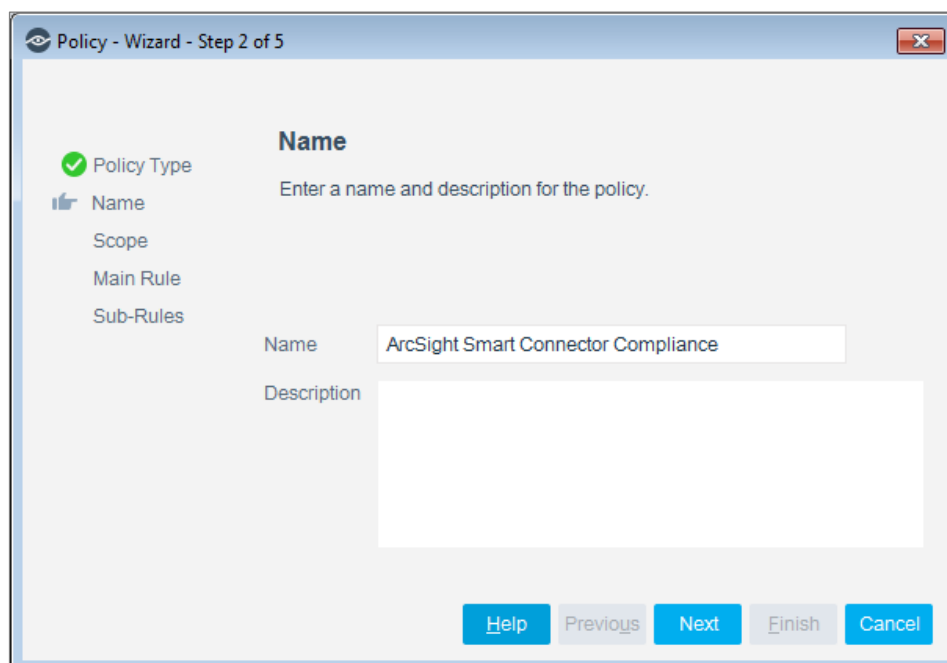
- Directs users to a URL from which to install the agent if it is not installed. It is recommended that the URL be available from outside the network.
- Run a script to start the ArcSight SmartConnector if it is installed but not running.

To use the ArcSight SmartConnector Compliance policy template:

1. Log in to the Console and select **Policy**.
2. Select **Add** from the Policy Manager. The Policy Wizard opens.
3. Expand the **ArcSight** folder and select **ArcSight SmartConnector Compliance**. The ArcSight SmartConnector Compliance pane opens.
4. Select **Next**.

Name the Policy

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

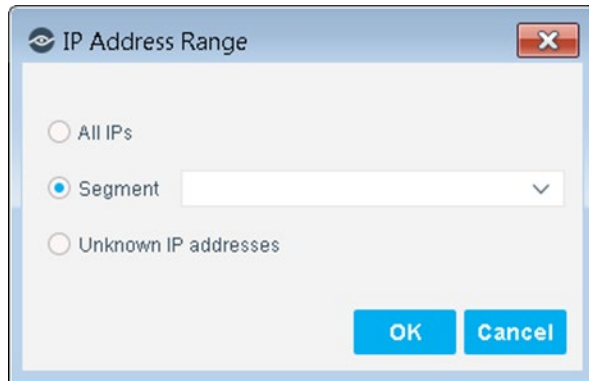


5. Define a unique name for the policy you are creating based on this template, and enter a description.
 - Make sure names are accurate and clearly reflect what the policy does. For example, do not use a generic name such as `My_Compliance_Policy`.
 - Use a descriptive name that indicates what your policy is verifying and which actions will be taken.
 - Ensure that the name indicates whether the policy criteria must be met or not met.
 - Avoid having another policy with a similar name.
6. Select **Next**. Both the Scope pane and the IP Address Range dialog box open.

Define Which Endpoints 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:

- **All IPs:** Include all IP addresses in the Internal Network.
- **Segment:** Select a previously defined segment of the network. To specify multiple segments, select **OK** or **Cancel** to close this dialog box, and select **Segments** from the Scope pane.
- **Unknown IP addresses:** Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.

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

9. Select **Next**. The Main Rules pane opens.

How Endpoints Are Detected and Handled

This section describes the main rule and sub-rules of the policy created by this template. Policy rules instruct the Forescout platform how to detect and handle endpoints defined in the policy scope.

Endpoints that match the Main Rule are included in the policy inspection. Endpoints that do not match this rule are not inspected for this policy. Sub-rules automatically follow up with endpoints after initial detection and handling, streamlining separate detection and actions into one automated sequence.

Sub-rules are performed in order until a match is found. When a match is found, the corresponding action is applied to the endpoint. If the endpoint does not match the requirements of the sub-rule, it is inspected by the next rule.

Main Rule

The main rule of this policy detects all Windows devices detected by the Forescout platform to identify them as in scope for the ArcSight SmartConnector Compliance policy. By default, the policy is evaluated every eight hours, and is applied to newly discovered endpoints.

Policy - Wizard - Step 4 of 5

☒ Policy Type
☒ Name
☒ Scope
☒ Main Rule
☐ Sub-Rules

Main Rule

Use this screen to review policy sub-rule definitions. Hosts are inspected by each sub-rule in the order shown. When a match is found, the action defined is applied. If no match is found, the host is inspected against the next sub-rule.

Condition

A host matches this rule if it meets the following condition:

All criteria are True

Criteria
Member of Group - Windows

Add Edit Remove

Actions

Actions are applied to hosts matching the above condition.

Ena...	Action	Details
No items to display		

Add Edit Remove

Help Previous Next Finish Cancel

10. Select **Next**. The Sub-Rules pane opens.

Sub-Rules

Hosts that match the Main Rule are included in the policy inspection. Hosts that do not match this rule are not inspected for this policy.

Sub-rules allow you to automatically follow up with hosts after initial detection and handling. Creating sub-rules lets you streamline separate detection and actions into one automated sequence. Sub-rules are performed in order until a match is found.

Policy - Wizard - Step 5 of 5

☒ Policy Type
☒ Name
☒ Scope
☒ Main Rule
☒ Sub-Rules

Sub-Rules

Use this screen to review policy sub-rule definitions. Hosts are inspected by each sub-rule in the order shown. When a match is found, the action defined is applied. If no match is found, the host is inspected against the next sub-rule.

Sub-Rules

	Name	Conditions	Actions	Exceptions
1	ArcSight Smart Conn Windows Services Running: Starts With arc			
2	ArcSight Smart Conn Windows Services Installed: Starts With arc			
3	ArcSight Smart Conn NOT Windows Services Installed: Matches winc - Match ca...			
4	ArcSight Smart Conn No Conditions			

Add Edit Remove Duplicate Up

Help Previous Next Finish Cancel

11. Select **Finish**.

12. In the Console, select **Apply** to save the policy.

Create Custom ArcSight Policies

You may need to create a custom policy to deal with issues not covered in the ArcSight policy templates.

Custom policy tools provide you with an extensive range of options for detecting and handling endpoints. Specifically, you can use the policy to instruct the Forescout platform to apply a policy action to endpoints that do or do not match property values defined in policy conditions.

Properties

Policy properties let you instruct the Forescout platform to detect hosts with specific attributes. For example, create a policy that instructs the Forescout platform to detect hosts running a certain Operating System or having a certain application installed. See [Detecting ArcSight Devices – Policy Properties](#) for more information.

Actions

Policy actions let you instruct the Forescout platform how to control detected devices. For example, assign a detected device to an isolated VLAN or send the device user or IT team an email.

You may need to create a custom policy to deal with issues not covered in the Action on Disposition, Send SIEM Updates or SmartConnector Compliance policy templates.

In addition to the bundled Forescout platform properties and actions available for detecting and handling endpoints, you can work with ArcSight-related properties and actions to create the custom policies. These items are available when you install the module.

See [Managing ArcSight Devices – Policy Actions](#) for more information.

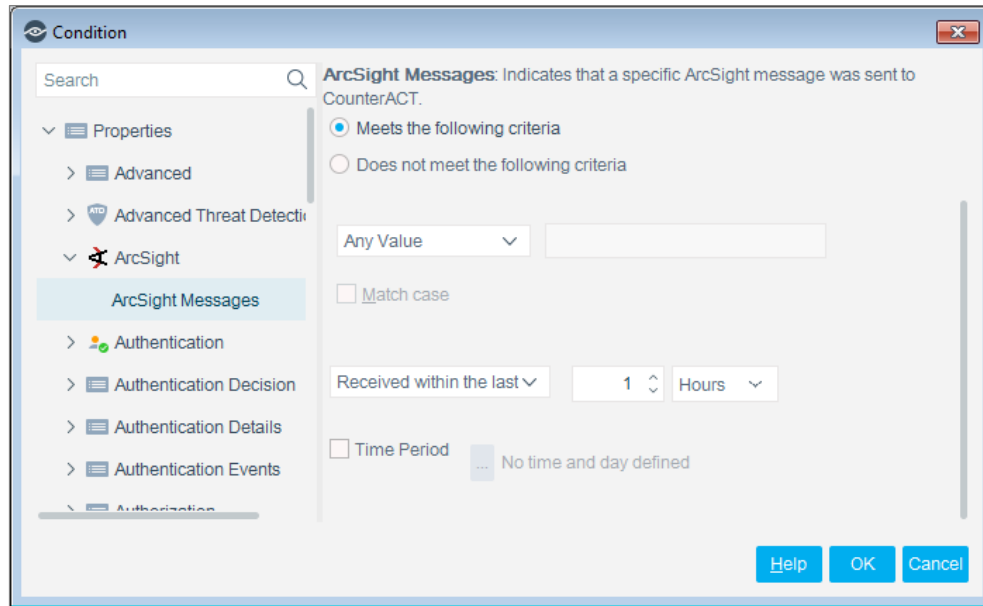
For more information about working with policies, select **Help** from the policy wizard.

Detect ArcSight Devices – Policy Properties

The following properties contain data reported by Forescout eyeExtend for ArcSight. The ArcSight Messages property is available when you install the module.

To set an ArcSight message event in a Forescout platform policy:

- 1.** Create or edit a policy, and then edit policy conditions.
- 2.** In the Properties tree, select **ArcSight** and then select **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. Select **OK**. The Main Rule pane of the policy opens.
5. (Optional) Create an action for the policy. The action is implemented when the condition is met.
6. When finished creating/editing the policy, select **Finish**.

Manage ArcSight Devices – Policy Actions

This section covers ArcSight policy actions and how to configure them.

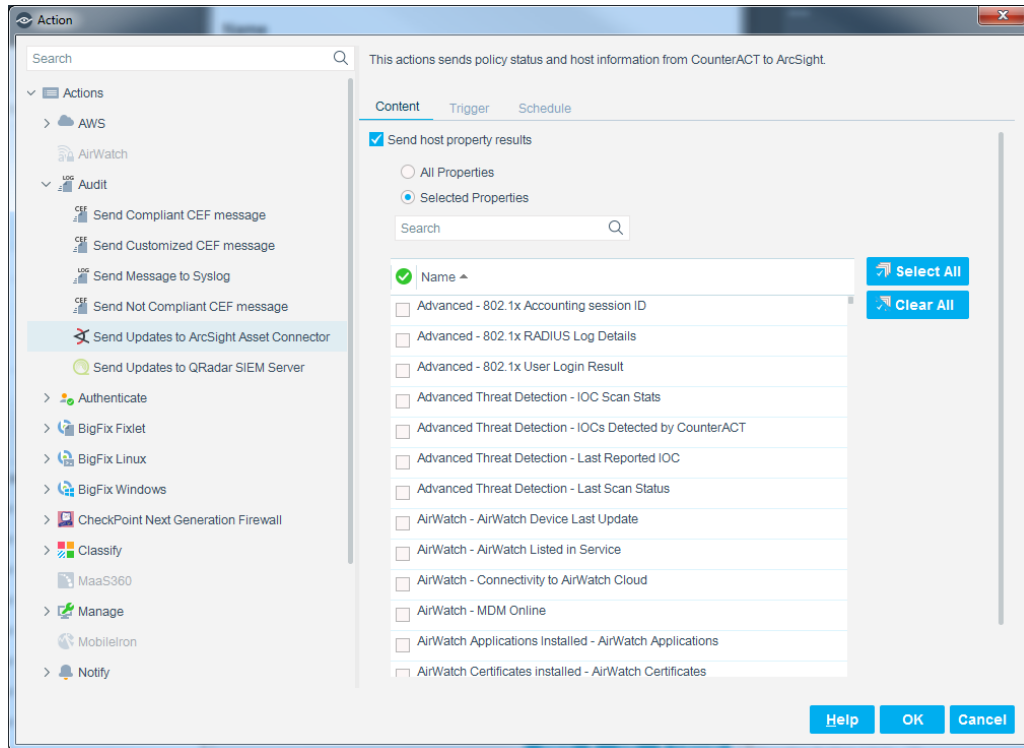
Send Host and Policy Data from the Forescout Platform to ArcSight

You can send policy status and host information from the Forescout platform 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:

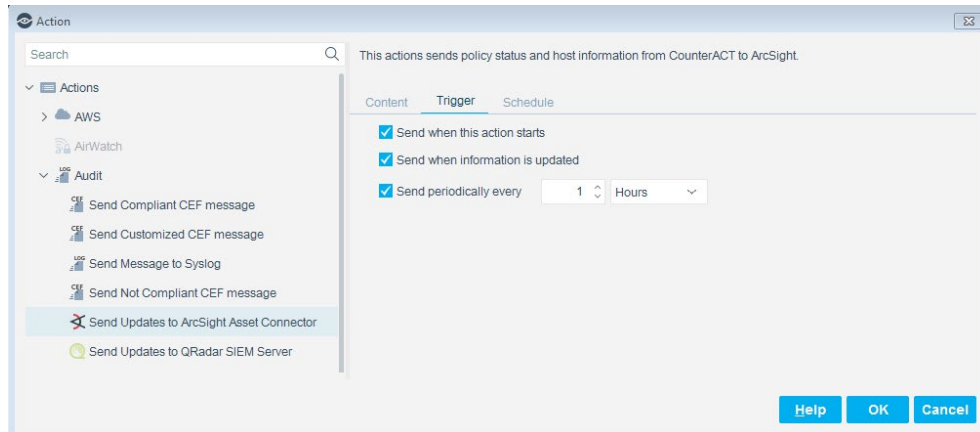
- Send host property results, for example switch related information, device information, authentication information, and more.
- Send policy status information, including the match/unmatched status.

To create actions:

1. Create or edit a policy and then go to the policy actions.
2. Go to the **Audit** folder and select **Send Updates to ArcSight Asset Connector**.

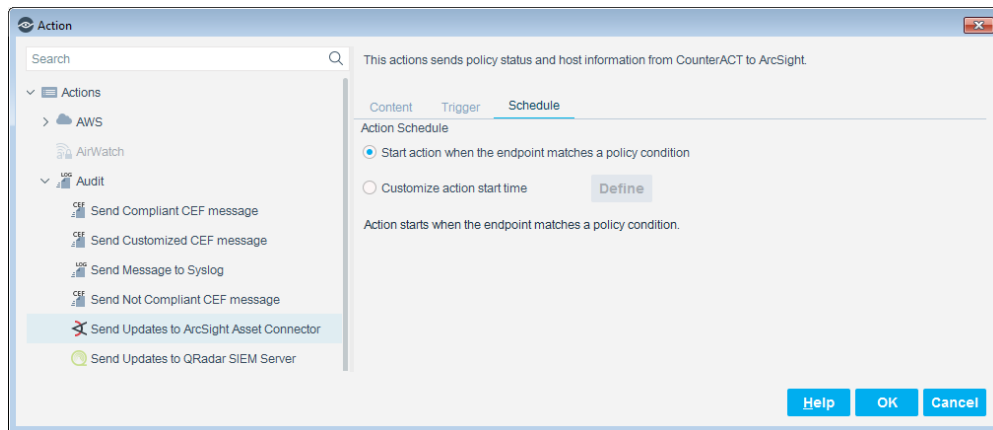


3. Select the **Send host property results** option to instruct the Forescout platform to send property results to the ArcSight server.
 - Select **All Properties** to send results of all property results discovered.
 - Select **Selected Properties** to send the results of specific properties, and then select the properties of interest to you.
 - Select **Send policy status** to send the Forescout platform 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 this 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.



6. When finished, select **OK** and continue creating/editing the policy.

Use ArcSight

This section addresses how to use some of the ArcSight functions.


ArcSight Action Connector Commands and the Forescout Platform

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

To instruct the Forescout platform to carry out specific actions when an Action Connector Command message is received:

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

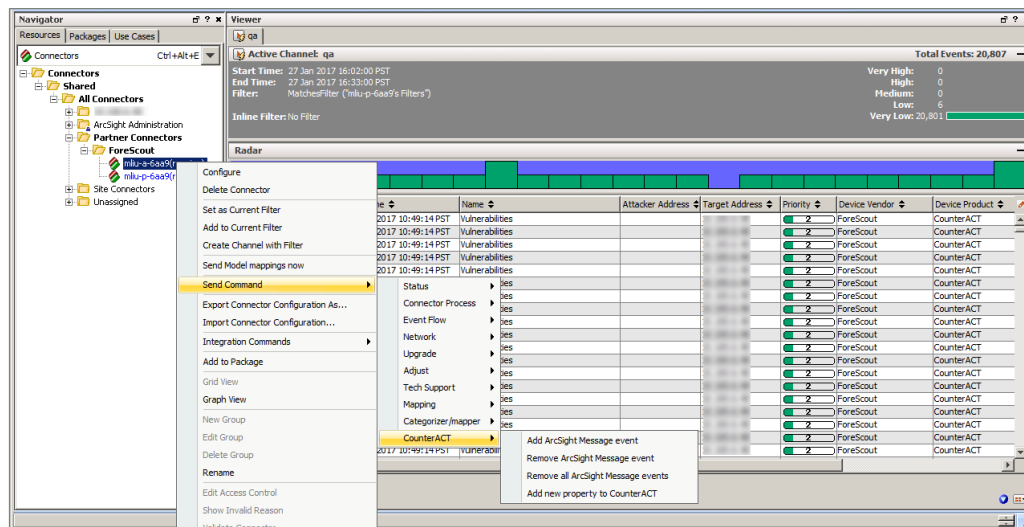
Action Connector also supports start/stop functionality. When you stop a message to the Forescout platform, the related Forescout platform action is also stopped.

 *To work with these features, you must start the Forescout platform module but you are not required to configure it.*

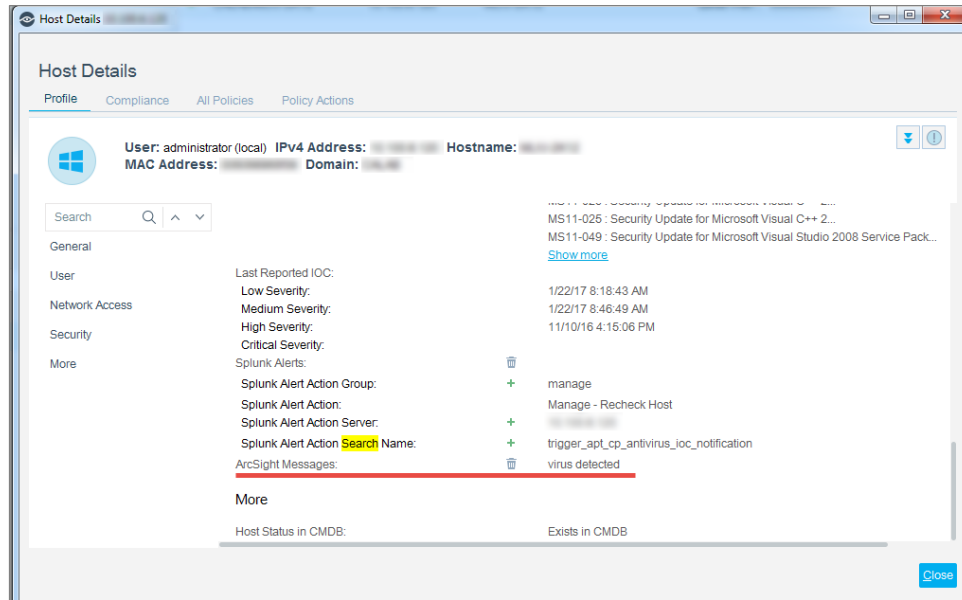
Send an ArcSight Action Connector Command to the Forescout Platform

To send an ArcSight Action Connector Command to the Forescout platform:

1. Log into the ArcSight Console.
2. In the Navigator, select **Connectors**, select **Shared**, select **All Connectors**, select **Partner Connectors**, and then select **Forescout**.
3. Right-click the detections of importance to you and select **Send Command**, select **CounterACT** and then select a command message.



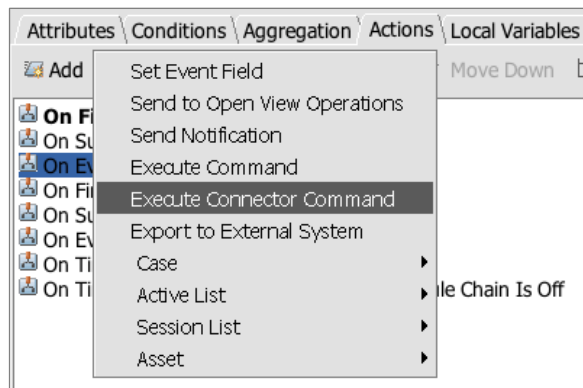
- Select **Add ArcSight Message event** to issue an add command message to one or more selected IP addresses. This option inserts an ArcSight message to the target *ArcSight Messages* host property with the pre-defined IP address.
 - Select **Remove ArcSight Message event** to issue a remove command message. This removes a particular ArcSight message on the ArcSight message host property from one or more target host(s) with the pre-defined IP address.
 - Select **Remove all ArcSight Message events** to issue a remove all message. This removes all ArcSight messages on host properties from one or more target host(s) with the pre-defined IP address.
 - Select **Add new property to CounterACT** to allow the ArcSight administrator to add or update Forescout platform host properties from one or more target hosts with the pre-defined IP addresses. For more information, see [Add a New Host Property to the Forescout Platform](#).
4. The Command Parameters dialog box opens to display the IP Address and Message fields.
 5. Select the Message event and enter any variable values or other data strings. You can enter a message that has a policy associated with it, for example, Block.
- If this command is going to multiple hosts, be sure to enter a space between each IP address.*
6. Select **OK**; the ArcSight command message is sent to the Forescout platform. This event is displayed with other information, for example, host information listed in the Host Details Profile tab.



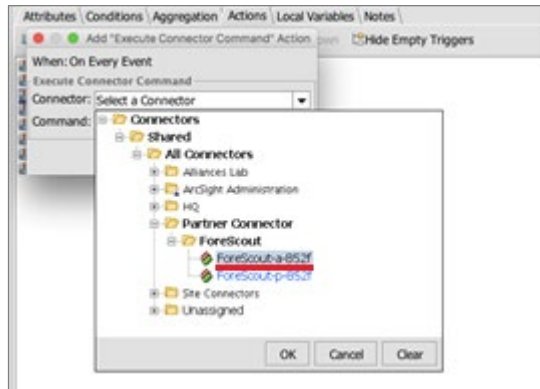
To automatically update endpoint properties through the correlation rule:

Refer to the *ArcSight User Guide* for creating correlation rules and action triggers.

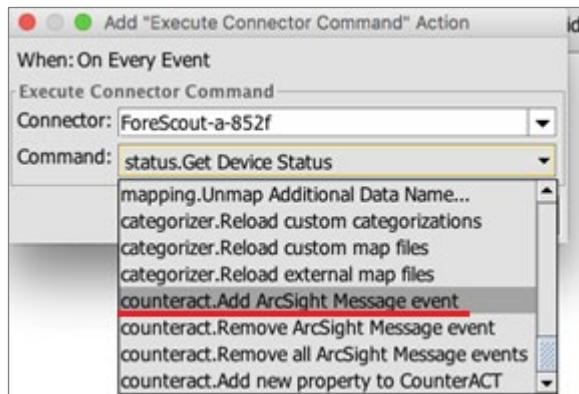
1. In ArcSight, create a new correlation rule and fill in the required fields.
2. In the Inspect/Edit pane, select the Rule Editor tab and then select the Actions tab.
3. In the **Rule Type** field, select the appropriate action rule. The Attributes tab opens.




4. Select a condition, right-click and then select **Execute Connector Command**.
5. The Add Execute Connector Command Action dialog box opens.



6. In the **Connector** field, navigate to and select your Forescout Action (a) SmartConnector and then select **OK**.



7. In the Command field, select **counteract.Add ArcSight Message event**.
8. Enter information into the **IP Address** and **Message** fields.

 Refer to the *ArcSight User Guide* for setting Action and meta-filled variables such as `$deviceHostName`, `$srcIP`, `$agentName`, etc.

9. Select **OK**.

For advanced use cases, there is an option to update or change Forescout platform endpoint properties through the ArcSight Console. For more information, see [Add a New Host Property to the Forescout Platform](#).

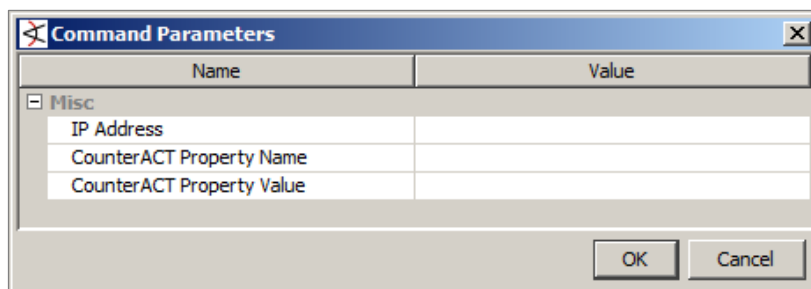
Add a New Host Property to the Forescout Platform

This command enables the user to modify a Forescout platform host property. It acts as the Forescout platform learner module.

To add a new host property to the Forescout platform:

1. Log into the ArcSight Console.
2. In the Navigator, select **Connectors**, select **Shared**, select **All Connectors**, select **Partner Connectors**, and then select **Forescout**.

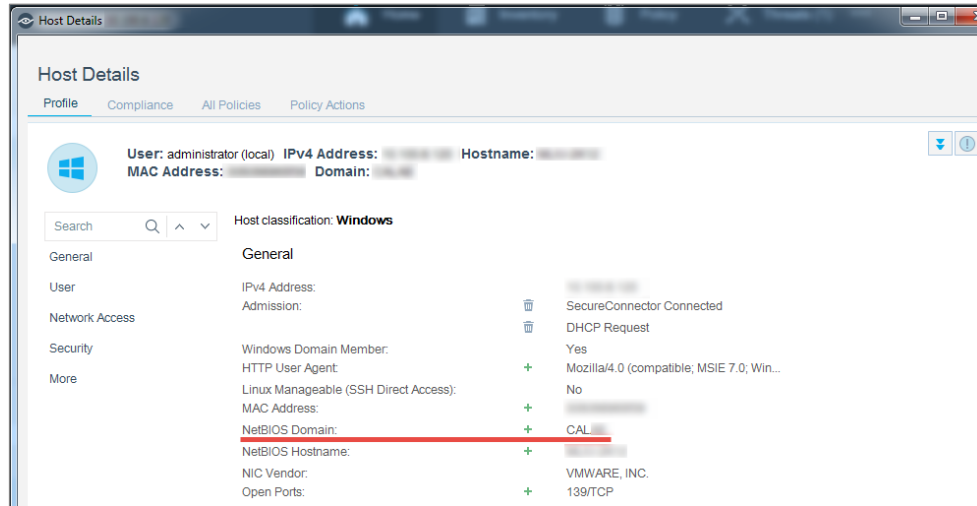
3. Right-click the detections of importance to you and select **Send Command**, select **CounterACT** and then select **Add new property to CounterACT**.



IP Address	Indicates the IP address the command applies to.																
CounterACT Property Name	<p>The name that the Forescout platform associates with the Forescout platform host property.</p> <p>Enter a new host property. The following table has examples.</p> <table border="1"> <thead> <tr> <th>CounterACT Property Name (also known as tag)</th><th>Definition</th></tr> </thead> <tbody> <tr> <td>Va_netfunc</td><td>Windows, Linux, Apple mac/OS</td></tr> <tr> <td>mac</td><td><Mac Address> Example: 010203040506</td></tr> <tr> <td>user</td><td><Windows user> Example: windows_qa</td></tr> <tr> <td>linux_logged_users</td><td><Linux user> Example: linux_qa</td></tr> <tr> <td>mac_logged_users</td><td><Mac user> Example: mac_qa</td></tr> <tr> <td>nbtomain</td><td><network domain name> Example: fsd or qalab</td></tr> <tr> <td>segment</td><td><network segment user defined field> Example: IT network or QA network</td></tr> </tbody> </table> <p>For example purposes, <i>nbtomain</i> was entered in this field.</p>	CounterACT Property Name (also known as tag)	Definition	Va_netfunc	Windows, Linux, Apple mac/OS	mac	<Mac Address> Example: 010203040506	user	<Windows user> Example: windows_qa	linux_logged_users	<Linux user> Example: linux_qa	mac_logged_users	<Mac user> Example: mac_qa	nbtomain	<network domain name> Example: fsd or qalab	segment	<network segment user defined field> Example: IT network or QA network
CounterACT Property Name (also known as tag)	Definition																
Va_netfunc	Windows, Linux, Apple mac/OS																
mac	<Mac Address> Example: 010203040506																
user	<Windows user> Example: windows_qa																
linux_logged_users	<Linux user> Example: linux_qa																
mac_logged_users	<Mac user> Example: mac_qa																
nbtomain	<network domain name> Example: fsd or qalab																
segment	<network segment user defined field> Example: IT network or QA network																
CounterACT Property Value	<p>If you entered a value into the CounterACT Property Name field, then what you enter in this field is displayed in the NetBIOS Domain field in the Detections pane in the Console.</p> <p>For example purposes, <i>arcsight_lab</i> was entered in this field.</p>																

4. Select **OK**.

5. In the Detections pane of the Home tab in the Console, search for the IP address you just made a change to.
6. Double-click the item to open it and view the Profile tab. In the example below, the NetBIOS Domain field lists the changed name, arcsight_lab.



Health Monitoring

This section covers the health monitoring of Forescout eyeExtend for ArcSight.

SNMP MIB for Forescout eyeExtend for ArcSight

Forescout eyeExtend for ArcSight provides a Management Information Base (MIB) that enables remote monitoring of module health – operational status and changes in configuration, performance and status. The MIB makes the following SNMP information available:

- [ArcSight MIB Table Attributes](#) – attributes that provide operational status information about the interaction between the module and its ArcSight server peer. It is assumed that external management systems query the Enterprise Manager for module status information.
- [SNMP Trap Notifications](#) – trap notifications, resulting from the occurrence of status, configuration and performance changes, are issued by the module. Each trap notification provides details about the specific change event that occurred. Trap notifications, issued by CounterACT Appliances and their modules, are forwarded to the Enterprise Manager and can be listened for/monitored by external management systems.

To enable query of the SNMP MIB and SNMP trap notifications:

1. Enable SNMP in each CounterACT Appliance that runs Forescout eyeExtend for ArcSight. By default, the Forescout platform SNMP agent is disabled. When upgrading the version of either the CounterACT Appliance or this module, existing settings are retained. Refer to the *Forescout Administration Guide* or *Console Online Help, Chapter 8, section SNMP Integration*.

2. Obtain the module MIB file, **ForeScoutArcSight-MIB**, from the location `/usr/local/forescout/etc/plugin/arcsight/snmp/ForeScoutArcSight-MIB`.
3. Load the **ForeScoutArcSight-MIB** file in your external management system.

ArcSight MIB Table Attributes

The Forescout eyeExtend for ArcSight MIB provides the following objects:

arcSightServerTable

OID: .1.3.6.1.4.1.11789.4.4.90.1

This object contains a table of ArcSight servers interfacing with CounterACT Appliances. When querying the Enterprise Manager (EM), this table lists the administrator configured ArcSight servers and their respective connector health status. When querying any one of the standalone appliances (or EM managed appliance) this table would contain entries representing the status of the ArcSight servers interfacing with this host. Anytime the operator adds or removes an ArcSight server from the Forescout platform module configuration, a trap notification would be generated indicating the configuration change.

arcSightServerName

OID: .1.3.6.1.4.1.11789.4.4.90.1.1.2

Forescout platform user-provided name for the ArcSight server.

arcSightServerDescription

OID: .1.3.6.1.4.1.11789.4.4.90.1.1.3

Forescout platform user-provided comment or description for the ArcSight server.

arcSightServerAddress

OID: .1.3.6.1.4.1.11789.4.4.90.1.1.1

This object indicates the ArcSight server IP address or DNS name. This attribute also identifies the peer ArcSight server with trap notifications sent from the Forescout platform on the interfacing connector state and health status and configuration changes.

arcSightServerPort

OID: .1.3.6.1.4.1.11789.4.4.90.1.1.4

This object indicates the Forescout platform user-defined ArcSight server port used by the Forescout platform to interface with its ArcSight server peer.

arcSightAssignedAppliancePeer

OID: .1.3.6.1.4.1.11789.4.4.90.1.1.5

This object identifies the CounterACT Appliance responsible for interfacing with this ArcSight server. This appliance also serves as a focal appliance for other CounterACT Appliances associated with this appliance.

arcSightConnectingAppliances

OID: .1.3.6.1.4.1.11789.4.4.90.1.1.6

This object indicates the list of CounterACT Appliances that indirectly interface with this ArcSight server. These Appliances use the focal Appliance defined for this server to send endpoint property values to ArcSight and to receive action requests.

arcSightIsDefaultServer

OID: .1.3.6.1.4.1.11789.4.4.90.1.1.7

This object indicates if this ArcSight server is used by newly added CounterACT Appliances. The default server is also used by CounterACT Appliances that were not explicitly associated with an ArcSight Server. Bind identifies servers that require administrator managed CounterACT Appliance association. Possible values are:

Default (1)

Bind (2)

arcSightIncomingMessageTransportState

OID: .1.3.6.1.4.1.11789.4.4.90.1.1.8

This object indicates if the ArcSight connector incoming action message-transport state. Possible states for the ArcSight connector are:

arcSightIncomingActionsConnected (1) CounterACT Appliance can receive policy driven action messages from its peer ArcSight server connector.

arcSightIncomingActionsDisconnected (2) ArcSight server incoming message transport is down or unresponsive; check the ArcSight device status and its network connectivity.

arcSightIncomingActionConnectivityUnknown (3) ArcSight server incoming action message transport status cannot be determined at this time (for example if the CounterACT Appliance is down or unreachable).

arcSightIncomingMessageQueueSize

OID: .1.3.6.1.4.1.11789.4.4.90.1.1.9

This object indicates the number of incoming message in the ArcSight connector queue. The Forescout platform module configuration provides an administrator-defined threshold for Forescout platform bound and lower bound settings that trigger trap notification when these thresholds are crossed.

arcSightIncomingConnectorState

OID: .1.3.6.1.4.1.11789.4.4.90.1.1.10

This object indicates the status of the ArcSight incoming connector operational state. Possible states for the ArcSight connector are:

arcSightIncomingConnectorResponsive (1) CounterACT Appliance can interface with the peer ArcSight server.

arcSightIncomingConnectorNotResponding (2) ArcSight server is disconnected, down or unresponsive; check the ArcSight device status and its network connectivity.

arcSightIncomingConnectorStateUnknown (3) ArcSight server incoming connector state status cannot be determined at this time (for example if the CounterACT Appliance is down or unreachable).

arcSightOutgoingMessageTransportState

OID: .1.3.6.1.4.1.11789.4.4.90.1.1.11

This object indicates the ArcSight connector outgoing host property message- transports state. Possible states for the ArcSight connector are:

arcSightOutgoingPropertiesConnected (1) The CounterACT Appliance can send host property update-messages to its peer ArcSight server connector.

arcSightOutgoingPropertiesDisconnected (2) ArcSight server outgoing message transport is down or unresponsive; check the ArcSight device status and its network connectivity.

arcSightOutgoingPropertiesConnectivityUnknown (3) ArcSight server outgoing message transport status cannot be determined at this time (for example if the CounterACT Appliance is down or unreachable).

arcSightOutgoingMessageQueueSize

OID: .1.3.6.1.4.1.11789.4.4.90.1.1.12

This object indicates the number of host property status in the ArcSight outgoing-connector message queue. The Forescout platform module configuration provides an administrator-defined threshold for upper bound and lower bound settings that trigger trap notification when these thresholds are crossed.

arcSightOutgoingConnectorState

OID: .1.3.6.1.4.1.11789.4.4.90.1.1.13

This object indicates the status of the ArcSight outgoing connector operational state. Possible states for the ArcSight connector are:

arcSightOutgoingConnectorResponsive (1) CounterACT Appliance can interface with the peer ArcSight server.

arcSightOutgoingConnectorNotResponding (2) ArcSight server is disconnected, down or unresponsive; check the ArcSight device status and its network connectivity.

arcSightOutgoingConnectorStateUnknown (3) ArcSight server incoming connector state status cannot be determined at this time (for example if the CounterACT Appliance is down or unreachable).

statsDeviceActionsOnHoldStatus

OID: .1.3.6.1.4.1.11789.4.3.1.14

This object indicates of the CounterACT Appliance pending actions queue status; it indicates if there are policy driven actions that were blocked because of the number of pending actions exceeded the administrator-defined queue size. Possible states are:

actionsOk (1) Policy actions are within the administrator-defined thresholds, and there are no policy driven actions in a blocked state.

actionsBlockedOnExceedingTreshold (2) Policies have created a queue of actions that exceeds the administrator-defined threshold. The Forescout operator should manually commit or delete the blocked actions in the queue.

actionsBlockStatusUnknown (3) Queue status cannot be verified (for example if the CounterACT Appliance is down or unreachable).

ctDeviceChannelStatus

OID: .1.3.6.1.4.1.11789.4.3.1.15

Indicates of the status of the CounterACT Appliance packet engine monitored traffic (channel) status; it indicates if there are policy driven actions that were blocked because of the number of pending actions exceeded the administrator-defined queue size. Possible states are:

channelsOk (1) CounterACT Appliance is currently monitoring network traffic.

channelsWarning (2) CounterACT Appliance has degraded ability to monitor network traffic and/or is temporarily limited in its ability to enforce (for example with actions such as virtual firewall).

channelsError (3) CounterACT Appliance is unable to monitor network traffic and or unable to enforce (for example with actions like virtual firewall).

channelsStatusIsUnknown (4) Traffic mirroring status cannot be verified at this time (for example if the CounterACT Appliance is down or unreachable).


channelsStatusNotApplicable (5) Network interfaces for traffic mirroring are not configured, or are administratively disabled.

SNMP Trap Notifications

The Forescout eyeExtend for ArcSight SNMP MIB provides SNMP trap notifications that the module issues due to configuration, status and performance changes. Trap notifications, issued by CounterACT Appliances and their modules, are forwarded to the Enterprise Manager and can be listened for/monitored by external management systems.

The module SNMP trap notifications include *varbinds*, as follows:

- [Common Trap Notification Varbinds](#)
- [Configuration Change Varbinds](#)

 *In future releases, SNMP MIB and trap notification information might change. For the latest information, refer to the latest Forescout Release Notes.*

Additionally, several resource properties of the module have performance thresholds that must be configured. The module monitors these resource properties as threshold crossing alarms (TCA) and issues trap notifications when specific threshold crossing conditions occur. See [Define Performance Thresholds](#).

The following table lists the trap notifications for Forescout eyeExtend for ArcSight:

ctConfigurationChangedTrap

OID: .1.3.6.1.4.1.11789.0.14

Trap notification issued due to a configuration change. Trap attributes indicate the module name of the service whose configuration was changed. This trap notification provides other configuration change information, including the changed property.

For varbind information provided in this trap notification, see [Configuration Change Varbinds](#).

arcSightServerAddedTrap

OID: .1.3.6.1.4.1.11789.4.4.90.0.1

Trap notification indicating that a new ArcSight server was added to the Forescout platform configuration.

arcSightServerRemovedTrap

OID: .1.3.6.1.4.1.11789.4.4.90.0.2

Trap notification indicating that an ArcSight server was removed from the Forescout platform configuration.

arcSightIncomingMessageTransportStateChangedTrap

OID: .1.3.6.1.4.1.11789.4.4.90.0.4

Trap notification indicating that the ArcSight incoming action message transport status has changed. In addition to the standard attributes provided by the Forescout platform on its trap notifications (like ArcSight server IP address) the severity attribute of the trap relays on the incoming action message transport state:

arcSightIncomingActionsConnected(1) severity is cleared(1)

arcSightIncomingActionsDisconnected (2) severity is major(4) indicating that incoming message transport is down.

arcSightIncomingActionConnectivityUnknown(3) severity is indeterminate(2) indicating that the ArcSight server incoming action message transport status cannot be determined at this time (for example if the CounterACT Appliance is down or unreachable).

arcSightIncomingMessageQueueHighCapacityTrap

OID: .1.3.6.1.4.1.11789.4.4.90.0.5

Trap notification sent by CounterACT Appliance if the number of incoming messages in the ArcSight connector queue exceeded the administrator-defined upper bound threshold, indicating that the ArcSight server is either responding slower than expected, down or unresponsive to the Forescout platform calls.

arcSightIncomingMessageQueueNormalCapacityTrap

.1.3.6.1.4.1.11789.4.4.90.0.6

Trap notification sent by CounterACT Appliance when the number of messages in the queue dropped below the administrator-defined lower bound threshold indicating that the message queue has returned to normal state.

arcSightIncomingConnectorStateChangedTrap

OID: .1.3.6.1.4.1.11789.4.4.90.0.3

Trap notification indicating that the ArcSight outgoing message-transport status has changed. In addition to the standard attributes provided by the Forescout platform on its trap notifications (like ArcSight server IP address), the severity attribute of the trap relays on the incoming action message transport state is as follows:

arcSightIncomingConnectorResponsive (1) severity is cleared.

arcSightIncomingConnectorNotResponding (2) severity is major(4) indicating that the incoming message transport is down.

arcSightIncomingConnectorStateUnknown (3) severity is indeterminate(2) indicating that the ArcSight server incoming action message transport status cannot be determined at this time (for example if the CounterACT Appliance is down or unreachable).

arcSightOutgoingMessageTransportStateChangedTrap

OID: .1.3.6.1.4.1.11789.4.4.90.0.8

Trap notification indicating that the ArcSight outgoing message-transport status has changed. In addition to the standard attributes provided by the Forescout platform on its trap notifications (like ArcSight server IP address), the severity attribute of the trap relays on the incoming action message transport state is as follows:

arcSightOutgoingPropertiesConnected (1) severity is cleared(1).

arcSightOutgoingPropertiesDisconnected (2) severity is major(4) indicating that the incoming message transport is down.

arcSightOutgoingPropertiesConnectivityUnknown (3) severity is indeterminate(2) indicating that the ArcSight server incoming action message transport status cannot be determined at this time (for example if the CounterACT Appliance is down or unreachable).

arcSightOutgoingMessageQueueHighCapacityTrap

OID: .1.3.6.1.4.1.11789.4.4.90.0.9

Trap notification sent by CounterACT Appliance if the number of messages in the ArcSight outgoing connector message queue exceeded the administrator-defined upper bound threshold. This could possibly indicate that the ArcSight server is either responding slower than expected, down or unresponsive to the Forescout platform calls.

arcSightOutgoingMessageQueueNormalCapacityTrap

OID: .1.3.6.1.4.1.11789.4.4.90.0.10

Trap notification sent by CounterACT Appliance if the number of outgoing messages in the ArcSight outgoing connector queue dropped below the administrator-defined lower bound threshold, indicating that the ArcSight server outgoing connector has returned to normal state.

arcSightOutgoingConnectorStateChangedTrap

OID: .1.3.6.1.4.1.11789.4.4.90.0.7

Trap notification indicating that the ArcSight outgoing connector status has changed. In addition to the standard attributes provided by the Forescout platform on its trap notifications (like ArcSight server IP address), the severity attribute of the trap relays on the incoming action message transport state is as follows:

arcSightOutgoingConnectorResponsive (1) severity is cleared(1).

arcSightOutgoingConnectorNotResponding (2) severity is major(4) indicating that the outgoing ArcSight connector is down.

arcSightOutgoingConnectorStateUnknown (3) severity is indeterminate(2) indicating that the ArcSight server incoming action message transport status cannot be determined at this time (for example if the CounterACT Appliance is down or unreachable).


Common Trap Notification Varbinds

SNMP trap notifications issued by Forescout eyeExtend for ArcSight always include a sequence of variable bindings (varbinds). A varbind is an SNMP key-value attribute pair, composed of the varbind OID (key) and its assigned value. For example, the trap notification *arcSightOutgoingConnectorStateChangedTrap* always includes the following varbind:

`.1.3.6.1.4.1.11789.3.21 = 1`, where:

`.1.3.6.1.4.1.11789.3.21` is the OID of varbind **fsTrapSeverity**

1 is the severity value assigned to this OID. The following, common varbinds are provided in all SNMP trap notifications for Forescout eyeExtend for ArcSight:

 *In future releases, SNMP MIB and trap notification information might change. For the latest information, refer to the latest Forescout Release Notes.*

ctDeviceId

OID: `.1.3.6.1.4.1.11789.4.3.1.1`

The unique identifier used to identify a managed CounterACT Appliance. This internally-defined value is commonly used with trap notifications providing consistent reference to the appliance throughout its life and for as long as it is associated with the Enterprise Manager.

ctDeviceIpAddress

OID: `.1.3.6.1.4.1.11789.4.3.1.2`

Unique IP address of the CounterACT Appliance or the Enterprise Manager that issued the SNMP trap notification.

ctDeviceIpAddressType

OID: `.1.3.6.1.4.1.11789.4.3.1.3`

The type of IP address. For example, an IPv4 address type or an IPv6 address type. Value that represents a type of Internet address. Possible values:

ipv4(1) indicates an IPv4 address, as defined by the *InetAddressIPv4* textual convention.

ipv6(2) indicates an IPv6 address, as defined by the *InetAddressIPv6* textual convention.

fsTrapSeverity

OID: `.1.3.6.1.4.1.11789.3.21`

The assigned event severity. The following are the possible severity level assignments:

Cleared (1): Indicates the clearing of one or more previously reported alarms. This alarm clears all alarms for this managed object that have the same Alarm type, Probable cause and Specific problems (if given).

Indeterminate (2): Indicates that the severity level cannot be determined.

Critical (3): Indicates that a service affecting condition has occurred and an immediate corrective action is required. Such a severity can be reported, for example, when a managed object becomes totally out of service and its capability must be restored.

Major (4): Indicates that a service affecting condition has developed and an urgent corrective action is required. Such a severity can be reported, for example, when there is a severe degradation in the capability of the managed object and its full capability must be restored.

Minor (5): Indicates the existence of a non-service affecting fault condition and that corrective action should be taken in order to prevent a more serious (for example, service affecting) fault. Such a severity can be reported, for example, when the detected alarm condition is not currently degrading the capacity of the managed object.

Warning (6): Indicates the detection of a potential or impending service affecting fault, before any significant effects have been felt. Action should be taken to further diagnose (if necessary) and correct the problem in order to prevent it from becoming a more serious service affecting fault.

Informational (7): Provided for informational purposes only.

With the exception of the Informational severity, all the other severity levels are defined in the CCITT standard X.733.

fsTrapTime

OID: .1.3.6.1.4.1.11789.3.21

Date and time that the event occurred in the Appliance, provided in the format of the *DateAndTime* field, which is specified in the SNMPv2-Textual Conventions standard.

fsTrapId


OID: .1.3.6.1.4.1.11789.3.21

The unique identifier for each issued, trap notification. The ID is a counter-based number representing a non-negative integer which monotonically increases until the assigned ID reaches its maximum value. When reaching its maximum, assigned value, the ID wraps around and begins increasing again from zero.

Based on an organization's network configuration (UDP), it is possible that the trap receiver may receive multiple copies of the same trap. In such a case, the Trap ID and Trap Time taken together can be used to identify duplicate instances of the same trap notification.

Configuration Change Varbinds

The SNMP trap notification `ctConfigurationChangedTrap`, which Forescout eyeExtend for ArcSight issues due to a configuration change, provides the following, additional varbinds:

-  *In future releases, SNMP MIB and trap notification information might change. For the latest information, refer to the latest Forescout Release Notes.*

fsFieldOid

OID: .1.3.6.1.4.1.11789.3.24

The OID of the changed attribute. For example, if the Forescout operator changed the ArcSight server name, this varbind contains the OID of the `arcSightServerName`.

fsOldValue

OID: .1.3.6.1.4.1.11789.3.25

The former value of the MIB attribute, that is, the attribute value before making the configuration change.

fsNewValue

OID: .1.3.6.1.4.1.11789.3.26

The updated value of the MIB attribute, that is, the attribute value after making the configuration change.

Additional Forescout Documentation

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

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

Documentation Downloads

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

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

-  *Software downloads are also available from these portals.*

To identify your licensing mode:

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

Technical Documentation Page

The Forescout Technical Documentation page provides a link to the searchable, web-based [Documentation Portal](#), as well as links to a wide range of Forescout technical documentation in PDF format.

To access the Technical Documentation page:

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

Product Updates Portal

The Product Updates Portal provides product and documentation downloads for Forescout platform releases, Base Modules, Content Modules, and eyeExtend modules. The portal also provides additional documentation.

To access the Product Updates Portal:

- Go to <https://updates.forescout.com/support/index.php?url=counteract> and select the version you want to discover.

Customer Support Portal

The Downloads page on the Forescout Customer Support Portal provides product and documentation downloads for Forescout platform releases, Base Modules, Content Modules, and eyeExtend modules. Software and related documentation only appear on the Downloads page if you have a license entitlement for the software.

To access documentation on the Customer Support Portal:

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

Documentation Portal

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

To access the Documentation Portal:

- Go to https://updates.forescout.com/support/files/counteract/docs_portal/

Forescout Help Tools

You can access individual documents, as well as the [Documentation Portal](#), directly from the Console.

Console Help Buttons

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

Forescout Administration Guide

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

Plugin Help Files

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

Content Module, eyeSegment Module, and eyeExtend Module Help Files

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

Documentation Portal

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