Table of Contents

About the HPE ArcSight Integration ............................................................. 4
  Use Cases ................................................................................................... 4
    Send Endpoint Status, Compliance, or Property Changes from CounterACT to ArcSight ................................................................. 5
    SmartConnector Health and Compliance for Windows ................................................. 5
    Dynamically Update HPEArcSight Asset Inventory ........................................... 5
    Trigger a CounterACT Policy and/or Action from ArcSight Correlation Rule ...... 6
  HPE ArcSight Network Integration Flow ........................................................... 6
  SNMP Management Information Base (MIB) and Trap Notifications ............... 8
  What to Do .................................................................................................. 8

Requirements ............................................................................................... 9
  CounterACT Software Requirements ............................................................ 9
  3rd Party Vendor Requirements ..................................................................... 9
  ForeScout Module License Requirements ....................................................... 9
    Requesting a License ............................................................................... 10
    More License Information ........................................................................ 10
  Install the ArcSight Module ........................................................................ 11

Configure the ArcSight Module ................................................................... 11
  Register CounterACT Devices with ArcSight ................................................. 12
  Test the Module ....................................................................................... 16
  Verify SmartConnectors are Running ......................................................... 16
    Troubleshoot Registration at the ArcSight Server ....................................... 17
  Define Performance Thresholds ................................................................. 19

Run ArcSight Policy Templates ..................................................................... 20
  ArcSight Action on Disposition Template .................................................... 21
  ArcSight Send SIEM Updates Template ......................................................... 25
  ArcSight SmartConnector Compliance Template ......................................... 30

Create Custom ArcSight Policies ................................................................. 34
  Detecting ArcSight Devices – Policy Properties ........................................... 35
  Managing ArcSight Devices – Policy Actions ............................................... 36
    Send Host and Policy Data from CounterACT to ArcSight ......................... 36

Using ArcSight ............................................................................................ 38
  ArcSight Action Connector Commands and CounterACT ......................... 38
    Sending an ArcSight Action Connector Command to CounterACT ............ 38
    Adding a New Host Property to CounterACT ........................................... 41
  Health Monitoring of the ArcSight Module ................................................. 43
    ArcSight Module SNMP MIB ..................................................................... 43
    ArcSight MIB Table Attributes ............................................................... 44
SNMP Trap Notifications ................................................................. 47

Additional CounterACT Documentation ................................. 52
  Documentation Portal ............................................................. 52
  Customer Support Portal ......................................................... 53
  CounterACT Console Online Help Tools .................................. 53
# About the HPE ArcSight Integration

CounterACT® integrates with *HPE ArcSight Enterprise Security Manager (ESM)* ("ArcSight") 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.

Hewlett Packard Enterprise's ArcSight ESM is a product designed for security information and event management (SIEM). HPE's 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)

![Diagram](image)

## Use Cases

This section describes important use cases supported by this module.

- **Send Endpoint Status, Compliance, or Property Changes from CounterACT to ArcSight**
- **SmartConnector Health and Compliance for Windows**
- **Dynamically Update HPE ArcSight Asset Inventory**
- **Trigger a CounterACT Policy and/or Action from ArcSight Correlation Rule**

**Send Endpoint Status, Compliance, or Property Changes from CounterACT to ArcSight**

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

By sending updates from CounterACT 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 HPE 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 HPE ArcSight to collect event logs. For more information, see [Verify SmartConnectors are Running](#) or the ArcSight User Guide.

**Dynamically Update HPE ArcSight Asset Inventory**

The Asset Model 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 CounterACT rules, actions, etc. This is a powerful and unique integration with ArcSight where you can effectively replicate the host profile record in CounterACT from the ForeScout Extended Module via the Assets tab of the Navigator in the ArcSight Console.
Trigger a CounterACT 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 HPE ArcSight SIEM to collect and aggregate logs from ForeScout CounterACT, firewall, and web applications. When HPE 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 CounterACT 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 the ArcSight Action Connector Commands and CounterACT and Sending an ArcSight Action Connector Command to CounterACT.

HPE 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 CounterACT, 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 CounterACT. 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 CounterACT to ArcSight

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

1. ForeScout Extended Module for ArcSight
2. ArcSight SmartConnector, sending host properties (p)
3. ArcSight server

### From ArcSight to CounterACT

The ArcSight server sends data flow to CounterACT in this order:

1. ArcSight server
2. ArcSight SmartConnector, sending action commands (a)
3. ForeScout Extended Module for ArcSight
SNMP Management Information Base (MIB) and Trap Notifications

The ArcSight Module 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 CounterACT 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 CounterACT Enterprise Manager and can be listened for/monitored by external management systems.

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 CounterACT. See Register CounterACT Devices with ArcSight and Define Performance Thresholds.
Requirements

This section describes:
- CounterACT Software Requirements
- 3rd Party Vendor Requirements
- ForeScout Module License Requirements

CounterACT continuously supports newly released ArcSight versions. Refer to the Release Notes for the most updated list.

CounterACT Software Requirements

The following CounterACT releases can work with this module:
- CounterACT version 7.0.0 with Service Pack 2.3.3 and above. It is recommended to install the latest service pack.
- Operating System Update Pack (OSUP) 1.2.0 and above.
- A module license for the ForeScout Extended Module for HPE ArcSight.
- An active Maintenance Contract for the licensed Module is required.

3rd Party Vendor Requirements

The following 3rd-Party vendor packages are required to install this release:
- HPE ArcSight 6.9.1.c
- A module license for the HPE ArcSight Module

ForeScout Module License Requirements

This ForeScout Module requires a module license. The installation package for the module is in the form of a CounterACT plugin. When installing the plugin you are provided with a 90-day demo module 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.

When the demo period expires, you will be required to purchase a permanent module license. In order to continue working with the module, you must purchase the license.

Demo license extension requests and permanent license requests are made from the CounterACT Console.
**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 CounterACT. 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 CounterACT, Console Modules pane.

![License Request Wizard](image)

**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.

![Views Pane](image)

**More License Information**

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

The installation package for the module is in the form of a CounterACT plugin.

To install the plugin:

1. Navigate to the Customer Support, ForeScout Modules page and download the plugin .fpi file.
2. Save the file to the machine where the CounterACT Console is installed.
3. Log into the CounterACT Console and select Options from the Tools menu.
5. Select Install. The Open dialog box opens.
6. Browse to and select the saved plugin .fpi file.
7. Select Install.
8. If you have not yet purchased a permanent module license, a message appears indicating that the plugin will be installed with a demo module license. Select Yes and then select Install.
9. An installation or upgrade information dialog box and an End User License Agreement will open. Accept the agreement to proceed with the installation.
10. When the installation completes, select Close. The plugin is displayed in the Plugins pane. The Module Status column indicates the status of your license. See ForeScout Module License Requirements or the CounterACT Console User Manual for details on requesting a permanent license or a demo license extension.
11. Select the plugin and select Start. The Select Appliances dialog box opens.
12. Select the CounterACT devices on which to start the plugin.
13. Select OK. The plugin runs on the selected devices.

Configure the ArcSight Module

This section describes how to configure the ArcSight Module, 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 the ArcSight Module in CounterACT:

1. In the Options pane, select Plugins.
2. In the Plugins pane, select ArcSight and then select Start. The ArcSight Module and its SmartConnectors will be started.

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 setup, un-check the Verify Server Certificate box.
1. In the ArcSight Servers tab, select **Add**. The Policy Wizard opens.

![Add ArcSight Server - Step 1 of 2](image)

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, verify the password of the user logging into the ArcSight server.
   - (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.
− 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, deselect the **Verify Server Certificate** box.

  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 CounterACT using the Browse option.

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

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

3. Select **Next**. The Assigned CounterACT devices pane opens.
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 appears 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 **Plugins**.

9. In the Plugins pane, select **ArcSight** and select **Start**.

10. Select each CounterACT device selected in step 7 to communicate with an ArcSight server, and select **OK**. The ArcSight module 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 ArcSight Module configurations:**

1. In the Options pane, select **Plugins** and then select **ArcSight**.

2. Select an item in the ArcSight Servers tab and then select **Test**. Using configured settings, CounterACT attempts to connect with the ArcSight server and to retrieve endpoint property values for the specified device.

3. The test results display.

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**. You should see two SmartConnectors listed in blue font:
   - `<your prefix>-a-XXXX(running), where a = Action.
   - `<your prefix>-p-XXXX(running), where p = Properties`
4. If you do not see the two SmartConnectors, refer to 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 CounterACT 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 CounterACT 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 CounterACT connector.

### Define Performance Thresholds

The ArcSight Module 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 CounterACT Console, select **Tools** and then select Options. The Options dialog box opens.
- Under Plugins, select the **ArcSight** folder.
- Select the **Performance Thresholds** tab.

**Run ArcSight Policy Templates**

CounterACT 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 find 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, see the CounterACT Templates and the Policy Management chapters in the Console User Guide.

For more information on how these templates work in ArcSight, see Using ArcSight

**ArcSight Action on Disposition Template**

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

CounterACT 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 the ArcSight Extended Module, CounterACT policies can include notification messages to ArcSight servers as an action.

To implement ArcSight reporting, define a CounterACT 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, CounterACT 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 CounterACT 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 CounterACT Console and select the **Policy** tab.
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**. The Name pane opens.

**Name the Policy**

The Name pane lets you define a unique policy name and useful policy description. Policy names appear in the Policy Manager, the Views pane, NAC Reports and in other features. Precise names make working with policies and reports more efficient.
5. Define a unique name for the policy you are creating based on this template, and enter a description.

- 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.


**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 for defining a scope:

   - **All IPs**: Include all addresses in the Internal Network. The Internal Network was defined when CounterACT was set up.
   - **Segment**: Select a previously defined segment of the network. To specify multiple segments, select **OK** to close the IP Address Range dialog box, and select **Segments** from the Scope pane.
   - **IP Range**: Define a range of IP addresses. These addresses must be within the Internal Network.
   - **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address. Not applicable for this policy template.

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

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

9. Select **Next**. 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 CounterACT 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 CounterACT received a disposition event message from ArcSight.

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. On the CounterACT 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 CounterACT Console and select the Policy tab.
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. The Name pane opens.
**Name the Policy**

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

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

   - 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**. The Scope pane and IP Address Range dialog box opens.

**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 for defining a scope:

   - **All IPs**: Include all addresses in the Internal Network. The Internal Network was defined when CounterACT was set up.
   - **Segment**: Select a previously-defined segment of the network. To specify multiple segments, select **OK** to close the IP Address Range dialog box, and select **Segments** from the Scope pane.
   - **IP Range**: Define a range of IP addresses. These addresses must be within the Internal Network.
   - **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address. Not applicable for this policy template.

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

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

9. Select **Next**. 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 CounterACT 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.
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. On the CounterACT Console, select **Apply** to save the policy.

**ArcSight SmartConnector Compliance Template**

Use this template to create a CounterACT 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 CounterACT Console and select the Policy tab.
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. The Name pane opens.

Name the Policy

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

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

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 for defining a scope:

- **All IPs**: Include all addresses in the Internal Network. The Internal Network was defined when CounterACT was set up.
- **Segment**: Select a previously-defined segment of the network. To specify multiple segments, select **OK** to close the IP Address Range dialog box, and select **Segments** from the Scope pane.
- **IP Range**: Define a range of IP addresses. These addresses must be within the Internal Network.
- **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address. Not applicable for this policy template.

Filter the range by including only certain CounterACT groups and/or by excluding certain endpoints or users or groups when using this policy.
8. Select OK. The added range appears in the Scope pane.

**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 CounterACT 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 CounterACT 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.

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

**Properties**

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

**Actions**

CounterACT policy actions let you instruct CounterACT 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 CounterACT 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.

**Detecting ArcSight Devices – Policy Properties**

The following properties contain data reported by the CounterACT ArcSight Module. The ArcSight Messages property is available when you install the CounterACT ArcSight Module.

**To set an ArcSight message event in a CounterACT 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 displays.
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**.

### Managing ArcSight Devices – Policy Actions

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

#### 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 HPE ArcSight Asset Connector**. The Content tab opens.

![Send Updates to HPE ArcSight Asset Connector](image)

3. Select the **Send host property results** check box to instruct CounterACT 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 CounterACT policy status (match/unmatch/pending/irresolvable).

4. Select the **Trigger** tab. Use the options to indicate when to initiate updates to the ArcSight server. Later you can use the options in the Schedule tab to further customize your event delivery strategy.

Select the following options:
− Select **Send when 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.
Using ArcSight

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

**ArcSight Action Connector Commands and CounterACT**

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.

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

- 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.

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

**Sending an ArcSight Action Connector Command to CounterACT**

To send an ArcSight Action Connector Command to CounterACT:

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 CounterACT host properties from one or more target hosts with the pre-defined IP addresses. For more information, refer to [Adding a New Host Property to CounterACT](#).

4. The Command Parameters dialog box opens displaying 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 CounterACT. This event appears with other information, for example, host information listed in the Host Details Profile tab.
To automatically update endpoint properties through the correlation rule:

- See 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.
4. The Attributes tab displays.

5. Select a condition, right-click and then select Execute Connector Command.
7. In the **Connector** field, navigate to and select your ForeScout Action (a) SmartConnector and then select **OK**.

8. In the **Command** field, select **counteract.Add ArcSight Message event**.

9. Enter information into the **IP Address** and **Message** fields.

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

10. Select **OK**.

    For advanced use cases, there is an option to update or change CounterACT endpoint properties through the ArcSight console. For more information, see **Adding a New Host Property to CounterACT**.

### Adding a New Host Property to CounterACT

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

**To add a new host property to CounterACT:**

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**.

4. The Command Parameters dialog box opens.

![Command Parameters dialog box](image)

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Indicates the IP address the command applies to.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CounterACT Property Name</strong></td>
<td>The name that CounterACT associates with the CounterACT host property. Enter a new host property - refer to the table for examples.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>CounterACT Property Name</strong> (also known as tag)</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Va_netfunc</td>
<td>Windows, Linux, Apple mac/OS</td>
</tr>
</tbody>
</table>
| 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 |
| nbtdomain | <network domain name>  
Example: fsd or qalab |
| segment | <network segment user defined field>  
Example: IT network or QA network |

For example purposes, `nbtdomain` was entered in this field.

| **CounterACT Property Value** | If you entered a value into the **CounterACT Property Name** field, then what you enter in this field displays in the NetBIOS Domain field in the Detections pane in the CounterACT Console.  
For example purposes, `arcsight_lab` was entered in this field. |
|-------------------------------|--------------------------------------------------|
5. Select **OK**.

6. In the Detections pane of the Home tab in the CounterACT Console, search for the IP address you just made a change to.

7. Double-click the item to open it and view the Profile tab. In the example below, the NetBIOS Domain field displays the changed name, arcsight_lab.

![Host Details](image)

**Health Monitoring of the ArcSight Module**

This section covers the health monitoring of the ArcSight module.

**ArcSight Module SNMP MIB**

The ArcSight Module 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 CounterACT 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 CounterACT Enterprise Manager and can be listened for/monitored by external management systems.
To enable query of the ArcSight Module SNMP MIB and SNMP trap notifications:

1. Enable SNMP in each CounterACT Appliance that runs the ArcSight Module. By default, the CounterACT SNMP agent is disabled. When upgrading the version of either the CounterACT Appliance or this module, existing settings are retained. Refer to the CounterACT Console User Manual 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 ArcSight Module 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 CounterACT 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 CounterACT 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

CounterACT user-provided name for the ArcSight server.

arcSightServerDescription

OID: .1.3.6.1.4.1.11789.4.4.90.1.1.3

CounterACT user-provided comment or description for the ArcSight server.

arcSightServerAddress

OID: .1.3.6.1.4.1.11789.4.4.90.1.1.4

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

arcSightServerPort

OID: .1.3.6.1.4.1.11789.4.4.90.1.1.5

This object indicates the CounterACT user-defined ArcSight server port used by CounterACT to interface with its ArcSight server peer.
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 CounterACT module configuration provides an administrator-defined threshold for upper 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-transport 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. CounterACT 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 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.

**actionsBlockedOnExceedingThreshold (2)** Policies have created a queue of actions that exceeds the administrator-defined threshold. The CounterACT 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 ArcSight Module 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 CounterACT 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, always refer to the latest CounterACT Service Pack 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 ArcSight Module trap notifications:
**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 CounterACT 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 CounterACT 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 CounterACT 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 CounterACT calls.

**arcSightIncomingMessageQueueNormalCapacityTrap**

**OID:** 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 CounterACT 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 CounterACT 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 CounterACT 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 CounterACT 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 the ArcSight Module 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 ArcSight Module SNMP trap notifications:

  In future releases, SNMP MIB and trap notification information might change. For the latest information, always refer to the latest CounterACT Service Pack 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 CounterACT 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.

\textit{fsTrapSeverity}\texttt{\textbackslash O\textbackslash D:} .1.3.6.1.4.1.11789.3.21

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

\textit{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).

\textit{Indeterminate (2)}: Indicates that the severity level cannot be determined.

\textit{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.

\textit{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.

\textit{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.

\textit{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.

\textit{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.

\textit{fsTrapTime}\texttt{\textbackslash O\textbackslash D:} .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 \textit{DateAndTime} field, which is specified in the SNMPv2-Textual Conventions standard.

\textit{fsTrapId}\texttt{\textbackslash O\textbackslash D:} .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 an ArcSight Module 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, always refer to the latest CounterACT Service Pack Release Notes.

**fsFieldOid**

**OID:** .1.3.6.1.4.1.11789.3.24

The OID of the changed attribute. For example, if the CounterACT 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 CounterACT Documentation**

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

- [Documentation Portal](#)
- [Customer Support Portal](#)
- [CounterACT Console Online Help Tools](#)

**Documentation Portal**

The ForeScout Documentation Portal is a Web-based library containing information about CounterACT tools, features, functionality and integrations.
To access the Documentation Portal:
2. Use your customer support credentials to log in.
3. Select the CounterACT version you want to discover.

Customer Support Portal
The Customer Support Portal provides links to CounterACT version releases, service packs, plugins and modules as well as related documentation. The portal also provides a variety of How-to Guides, Installation Guides and more. To access the Customer Support Portal, go to:

To access the Customer Support Portal:
2. Select the CounterACT version you want to discover.

CounterACT Console Online Help Tools
Access information directly from the CounterACT Console.

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

Console User Manual
Select CounterACT Help from the Help menu.

Plugin Help Files
1. After the plugin is installed, select Options from the Tools menu and then select Plugins.
2. Select the plugin and then select Help.

Documentation Portal
Select Documentation Portal from the Help menu.
Legal Notice

Copyright © ForeScout Technologies, Inc. 2000-2017. All rights reserved. The copyright and proprietary rights in this document belong to ForeScout Technologies, Inc. ("ForeScout"). It is strictly forbidden to copy, duplicate, sell, lend or otherwise use this document in any way, shape or form without the prior written consent of ForeScout. All other trademarks used in this document are the property of their respective owners.

These products are based on software developed by ForeScout. The products described in this document may be protected by one or more of the following U.S. patents: #6,363,489, #8,254,286, #8,590,004, #8,639,800 and #9,027,079 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.

Unless there is another valid written agreement executed by you and ForeScout that governs the ForeScout products and services:

- If you have purchased any ForeScout products or services, your use of such products or services is subject to your acceptance of the terms set forth at http://www.forescout.com/eula/;
- If you have purchased any ForeScout support service ("ActiveCare"), your use of ActiveCare is subject to your acceptance of the terms set forth at http://www.forescout.com/activecare-maintenance-and-support-policy/;
- If you are evaluating ForeScout’s products, your evaluation is subject to your acceptance of the applicable terms set forth below:
  - If you have requested a General Availability Product, the terms applicable to your use of such product are set forth at: http://www.forescout.com/evaluation-license/.
  - If you have requested a Beta Product, the terms applicable to your use of such product are set forth at: http://www.forescout.com/beta-test-agreement/.
  - If you have purchased any ForeScout Not For Resale licenses, such license is subject to your acceptance of the terms set forth at http://www.forescout.com/nfr-license/.

Send comments and questions about this document to: documentation@forescout.com

2017-10-02 11:25