# Table of Contents

**About Splunk Module** ................................................................................................. 4  
  Support for Splunk Adaptive Response ................................................................. 5  
  Use Cases ............................................................................................................. 6  
    Data Mining and Trend Analysis of CounterACT Data .................................... 6  
    Continuous Posture Tracking Based on a Broad Range of CounterACT Data .... 6  
    Response Actions Triggered by Splunk Data Correlation ............................. 7  
  Additional Splunk Documentation ...................................................................... 7

**About This Module** ................................................................................................. 7  
  How It Works ....................................................................................................... 8  
  Supported Splunk Versions ............................................................................. 8  
  What to Do ....................................................................................................... 8

**Requirements** ...................................................................................................... 10  
  CounterACT Requirements ............................................................................... 10  
  Secured Messaging from CounterACT Splunk Module to the ForeScout Splunk App 10  
  License Requirements ........................................................................................ 11  
    Requesting a License .................................................................................... 11  
    More License Information .......................................................................... 12

**Install the Module** ............................................................................................... 13

**Configure the Module** ......................................................................................... 14  
  Configure the Module to Use Syslog Messaging .............................................. 17  
  Configure the Plugin to Use REST Messaging ................................................. 19

**Run Splunk Policy Templates** ............................................................................. 22  
  Send Endpoint and Policy Details to Splunk ............................................... 23  
    Run the Template ....................................................................................... 23  
    How Devices are Detected and Handled .................................................... 25  
  Stage 1 – Add to HTTP Notification Action Group ....................................... 26  
    Run the Template ....................................................................................... 26  
    How Devices are Detected and Handled .................................................... 28  
  Stage 2 - Execute HTTP Notification Action ................................................. 30  
    Run the Template ....................................................................................... 30  
    How Devices are Detected and Handled .................................................... 33

**Create Custom Splunk Policies** .......................................................................... 34  
  Detecting Endpoints – Policy Properties ....................................................... 39  
  Splunk Alerts .................................................................................................... 39  
  Managing Splunk Devices – Policy Actions ..................................................... 40  
    Splunk: Send Custom Notification Action ................................................... 41  
    Splunk: Send Update from CounterACT Action ....................................... 42

**Appendix A: Default Communication Settings** ............................................... 45
Mapping CounterACT Data to the CIM Model................................. 45
Certificates.................................................................................... 45
Compute_Inventory: CPU................................................................. 46
Compute_Inventory: Network.......................................................... 46
Compute_Inventory: Memory............................................................ 46
Compute_Inventory: Storage............................................................ 46
Blocked_Malware ......................................................................... 47
Subset of Core Properties.............................................................. 47

Additional CounterACT Documentation ........................................ 48
Documentation Portal ................................................................. 48
Customer Support Portal ............................................................ 48
CounterACT Console Online Help Tools......................................... 49
About Splunk Module

Splunk Enterprise data analytics help organizations:

- Leverage the data that their infrastructure and security tools provide
- Understand their security posture
- Pinpoint and investigate risks
- Create alerts and reports.

However, IT staff must then respond to any identified threats, violations and attacks. Any delay in response can result in significant security risks.

By combining ForeScout dynamic endpoint visibility, access and security capabilities with Splunk Enterprise’s data mining capabilities, security managers can:

- Achieve a broader understanding of their security posture
- Visualize key control metrics
- Respond more quickly to mitigate a range of security issues.

Integration is bi-directional – CounterACT sends property, policy, and event information to Splunk, and Splunk sends alerts and notification messages to CounterACT.

The result is enhanced threat insight, automated control, and greater operational efficiency.
Support for Splunk Adaptive Response

Splunk’s Adaptive Response Framework describes a complete action flow, which includes requesting an action be applied to an endpoint, and tracking the status of the action taken.

This integration supports the Splunk Adaptive Response workflow as follows:

- The ForeScout App for Splunk maintains a list of available actions from CounterACT. Splunk can instruct CounterACT to respond to potential threats by applying any of these actions to endpoints that match search/trend criteria.
- To complete the action flow, CounterACT reports the status of actions applied to endpoints.
Use Cases

This section describes important use cases supported by this module. To understand how this module helps you achieve these goals, see About This Module.

- Data Mining and Trend Analysis of CounterACT Data
- Continuous Posture Tracking Based on a Broad Range of CounterACT Data
- Response Actions Triggered by Splunk Data Correlation

Data Mining and Trend Analysis of CounterACT Data

Splunk’s strength is storing and indexing data over long periods of time. To complement CounterACT’s real-time monitoring and management tools, Splunk provides long term data storage and in-depth history and trend analysis tools as standard options.

Continuous Posture Tracking Based on a Broad Range of CounterACT Data

Integration with Splunk includes a dedicated ForeScout App for Splunk with custom dashboards that let security managers quickly monitor the current operational/security posture. With this release, CounterACT reports a wider range of data to Splunk, and the dashboards display real-time metrics derived from this information, such as:

- Endpoint compliance status summaries
- Patterns of network access over time
- Trends in CounterACT policies
- Significant changes in endpoint processes and applications
- Endpoint system health information including hardware and certificate information
Experienced Splunk users can customize the searches and dashboards provided with the ForeScout App, or combine CounterACT information with other data sources in the Splunk environment.

**Response Actions Triggered by Splunk Data Correlation**

The results of Splunk’s intuitive search and reporting tools can generate notification messages which are sent to CounterACT. Based on alert data received from Splunk, CounterACT policies can automatically apply remediation actions, isolate breached systems, or invoke additional management steps such as security scans.

For example, if Splunk determines that a set of endpoints have a material security issue, CounterACT can automatically initiate remediation that targets the specific problem identified by Splunk and report back on the status of the action taken.

**Additional Splunk Documentation**

Refer to online documentation for more information about the Splunk solution:

http://docs.splunk.com/Documentation/Splunk

**About This Module**

This module works with the ForeScout App for Splunk to integrate CounterACT and Splunk so that you can:

- Use policies and actions provided by the Splunk Module to regularly push endpoint data to Splunk. See details of the [Send Endpoint and Policy Details to Splunk](#) policy template and the [Splunk: Send Update from CounterACT Action](#).

- In the ForeScout App for Splunk, view CounterACT data in a dedicated, customizable Splunk dashboard. See the [ForeScout App for Splunk How-to Guide](#) for details.

- Define CounterACT policies that respond to Splunk alerts. See [Run Splunk Policy Templates](#).

- In the ForeScout App for Splunk, configure Splunk to send alerts to CounterACT based on custom search or report results. Searches can combine data from multiple sources.

- Send Update from CounterACT Action - This action submits endpoint data to Splunk. This action is the primary method of transmitting data from CounterACT to Splunk. In addition to the specified host properties, each update message sent to Splunk includes the following information for each endpoint:
  - MAC Address
  - NetBIOS Hostname
  - NetBIOS Domain
  - User
The Splunk Module and the ForeScout App for Splunk work together to support communication between CounterACT and Splunk. You must install and configure both components to work with the features described in this document. For example, CounterACT policies and actions provided by the Splunk Module are used to populate Splunk with CounterACT data. Read this document together with the ForeScout App for Splunk How-to Guide.

To use the module, you should have a solid understanding of how CounterACT policies work and understand basic Splunk concepts, functionality and terminology.

To access the ForeScout App for Splunk How-to Guide:

1. Go to https://splunkbase.splunk.com/ and conduct a search on “ForeScout App for Splunk” and select it.

   If you have already installed the ForeScout App for Splunk, you can read documentation in Splunkbase.

2. Select the Details tab and then download the ForeScout App for Splunk How-To-Guide (v 2.5.0).

How It Works

Two components are installed to support this integration:

- The Splunk Module is installed in CounterACT.
- The ForeScout App for Splunk is installed in Splunk.

The result is comprehensive bi-directional integration – CounterACT can send a dynamic list of property, policy, and event information to Splunk, and Splunk can send alerts and other messages to CounterACT.

Splunk search uses data from CounterACT and other sources to detect patterns that indicate threats.

The ForeScout App submits alerts generated by Splunk to CounterACT, where the Splunk Module parses the alert into host properties.

CounterACT policies examine these properties to identify endpoints in need of remediation, and apply the requested action.

Supported Splunk Versions

This release supports Splunk Enterprise version 6.4.x and 6.5.0.

What to Do

This section lists the steps you should take to set up your system when integrating with Splunk.

The Splunk Module and the ForeScout App for Splunk work together to support communication between CounterACT and Splunk. You must install and configure both components to work with the features described in this document. For example,
CounterACT policies and actions provided by the Splunk Module are used to populate Splunk with CounterACT data. As you plan deployment, read this document together with the *ForeScout App for Splunk How-to Guide*.

<table>
<thead>
<tr>
<th>In the CounterACT Console</th>
<th>On the Splunk Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Review the ForeScout App How-to Guide and this Configuration Guide. Choose protocol(s) for CounterACT messaging to Splunk. See Configure the Module.</td>
<td></td>
</tr>
<tr>
<td>2. Verify that CounterACT requirements are met. See Requirements. Install the Module.</td>
<td>3. Verify that the Splunk server contains a user with the required permissions to work with the ForeScout App for Splunk. Download and Install the ForeScout App for Splunk from Splunkbase.splunk.com</td>
</tr>
<tr>
<td>4. Configure Splunk Communication with CounterACT.</td>
<td></td>
</tr>
<tr>
<td>5. Configure Splunk to receive messages from CounterACT: - Configure a CounterACT User for the Splunk REST API - Configure Data Inputs from CounterACT</td>
<td></td>
</tr>
<tr>
<td>6. Configure the</td>
<td></td>
</tr>
<tr>
<td>7. Create a CounterACT policy that sends information to Splunk. See Run Splunk Policy Templates Tune the frequency of data reporting based on your network conditions and the volume of data you want to work with in Splunk. Create Custom Splunk Policies</td>
<td>Required for configuration: Splunk Server IP Custom Port/Protocol REST Account Credentials Event Collector Authorization Token (from Data Inputs)</td>
</tr>
</tbody>
</table>
Requirements

This section describes system requirements, including:

- CounterACT Requirements
- Secured MessagingLicense Requirements

CounterACT Requirements

The module requires the following CounterACT releases and other CounterACT components:

- The ForeScout App for Splunk interacts with a CounterACT Enterprise Manager running 7.0.0 and above.
- Service Pack 2.2.0 or above ( SP 2.3.2 recommended)
- Verify that the following policies are active:
  - Classification
  - Compliance

Host information determined by these policies is reported to Splunk and used in standard dashboards of the ForeScout App for Splunk. Similarly, host information determined by other policies categorized as Classification or Compliance policies is reported to Splunk.

To categorize policies:

1. Select a policy for categorization from the Console, Policy tab and then select Categorize. The Categorize dialog box opens.
2. Select the category you need.

If you plan to send system health and network data, install and enable Hardware Inventory Plugin (v 1.0.1) and NetFlow Plugin (v 1.1.0).

Secured Messaging from CounterACT Splunk Module to the ForeScout Splunk App

CounterACT Splunk Module updates messages sent to the Splunk server via HTTP Event Collector or HTTP REST. It can also use HTTPS. If the Splunk server is configured to use SSL (HTTPS) over Splunk Web:

- By default Splunk 6.4.x generates a self-signed certificate that it uses for HTTPS messaging. Because this certificate is not signed by any certificate authority, CounterACT does not validate SSL handshakes based on this certificate.
Possible solutions include:

- Downloading the Splunk Web Public Certificate and installing it in the CounterACT trusted certificate store.
- Generating a valid signed certificate which can be validated by CounterACT and installing it on Splunk Web.

It is recommended to use trusted (on both CounterACT and Splunk) certificates to ensure the Enable Certificate Verification option in Splunk is valid.

For more information about HTTPS configuration in Splunk, refer to the Splunk knowledge base.

License Requirements

This module is packaged as a ForeScout Module, and requires a module license. When installing the module 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.

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.

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 for more information.
Install the Module

This section describes how to download the module from the ForeScout Web site and install it on the Console.

This module interacts with the ForeScout App for Splunk. If you install only this module, you can send CounterACT information to Splunk. However, you must install and configure both components to work with all the features described in this document, including bidirectional interaction with Splunk.

To install the module:

1. Acquire a copy of the module in either one of the following ways:
   - If you are installing a Beta release of this module, acquire the .fpi file from your ForeScout representative or contact beta@forescout.com.
   - Otherwise, navigate to the Customer Support, ForeScout Modules page and download the .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 .fpi file.
7. Select Install.
8. If you have not yet purchased a permanent module license, a message appears indicating that the module 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. Once the installation is complete, select Close. The module is listed in the Plugins pane. The Module Status column indicates the status of your license. See License Requirements and the CounterACT Console User Manual for information on requesting a permanent license or a demo license extension.

11. Select the module and select Start. The Select Appliances dialog box opens.

12. Select the CounterACT devices on which to start the module.

13. Select OK. The module runs on the selected devices.

### Configure the Module

Configure the module to ensure that CounterACT can communicate with Splunk.

*Perform this procedure after the ForeScout App for Splunk is installed on your Splunk server.*

To complete configuration of some of these connections, you must perform corresponding configuration steps on the Splunk server.

The following protocols can be used by CounterACT to send information to Splunk:

- Using Splunk Event Collector messages. This is the recommended protocol. Event Collector is a proprietary Splunk HTTP(S) channel introduced in Splunk 6.3. Follow the procedure described in this section to use Event Collector Messages.

- Using Syslog messaging. To use Syslog, define one or more Splunk server targets as described in Configure the Module to Use Syslog Messaging.

- Using HTTPS POST messages to the Splunk REST API. Define server targets as described in Configure the Plugin to Use REST Messaging.

**To configure the module:**

1. In the CounterACT Console, select Options from the Tools menu. The Options dialog box opens.

2. Navigate to and select the Plugins folder.

3. In the Plugins pane, select Splunk, and select Configure. The Splunk pane opens.
4. Define one or more Splunk servers that receive update messages from CounterACT:

   a. Select the Splunk HTTP Targets tab, and select **Add**. The Add Splunk Syslog Target dialog box opens.

   b. In the Splunk HTTP Type drop down, select **Event Collector**. This is a Splunk-specific message type used to report event and endpoint data. The default port in Splunk for these messages is 8088.

   c. Enter the following information and Select **OK**. The server appears in the Splunk HTTP Targets tab.

      **POST to URL**: The target URL that appears in the POST message header. In most cases the URL takes the form of the example shown. Replace **my.splunk.com** with the IP address of your Splunk server. If the Splunk server uses a different port from the default, specify the actual port used. See **Appendix A: Default Communication Settings**.

      **Comment**: Optional text that indicates the location or other information that identifies the server.

      **Authorization Token**: CounterACT includes this string in the HTTP message header of event collector messages, and Splunk uses it to authorize these messages. Copy the Token Value created by Splunk for the Event Collector data input. Refer to the **ForeScout App for Splunk How-to Guide**.
d. Repeat these steps to define additional Event Collector/HTTP targets.
e. To modify Splunk server information, select the server, then select **Edit**.

Verify that data inputs defined on the Splunk server use the port and other settings you define here. Refer to the ForeScout App for Splunk How-to Guide.

5. Select the General Settings tab.

<table>
<thead>
<tr>
<th>Splunk Syslog Targets</th>
<th>Splunk HTTP Targets</th>
<th>General Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syslog Message Defaults</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identity</td>
<td>CounterACT</td>
<td></td>
</tr>
<tr>
<td>Facility</td>
<td>local4</td>
<td></td>
</tr>
<tr>
<td>Priority</td>
<td>info</td>
<td></td>
</tr>
<tr>
<td><strong>CounterACT Data Submission Settings</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Send Property Titles (longer)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Splunk Alert Message Settings</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>List of Supported IP fields:</td>
<td>ip,dest_ip,dest_host,dest_name,dest</td>
<td></td>
</tr>
<tr>
<td>Alert Service Authorization Token:</td>
<td>78ED03BD-A362-4F2F-988E-BB75BB1B94EB</td>
<td></td>
</tr>
</tbody>
</table>

The following options and fields are relevant when Event Collector messaging is used to report data to Splunk:

| **Send Property Titles** | CounterACT sends host property information to Splunk as **Field:Value** pairs in JSON format. By default, the **Field** label is the internal property tag of each property. Select this option to send two sets of property value information to Splunk:
Using the property tag as the **Field** label:
*va_os : Windows 8.1 64-bit Pro*
Using the property's full name as the **Field** label:
*Windows Version : Windows 8.1 64-bit Pro*

| **List of Supported IP fields** | In alert messages sent by Splunk to CounterACT, fields with these tags are parsed for IP Address information. CounterACT evaluates the fields in the order shown in this list: the first IP address found is used to identify the endpoint to which the alert applies. In Splunk, alert messages must be triggered by search queries that reference/evaluate one of these fields. Refer to the *ForeScout App for Splunk How-to Guide.* |

| **Alert Service Authorization Token** | This string is used in the HTTP message header of alert messages sent to CounterACT by the ForeScout App for Splunk. |

6. In the Splunk pane, select **Apply**. A confirmation dialog box opens.
7. Select **Yes** to save the configuration, and then select **Close**.
Configure the Module to Use Syslog Messaging

(Optional) Use the following procedure to configure the module to send information to Splunk using Syslog messages instead of Splunk Event Collector messages.

To configure:

1. In the CounterACT Console, select **Options** from the **Tools** menu. The Options dialog box opens.
2. Navigate to and select the **Plugins** folder.
3. In the **Plugins** pane, select **Splunk**, and select **Configure**. The Splunk pane opens.

4. Define one or more Splunk servers that receive update messages from CounterACT in Syslog format:
   a. In the Splunk Syslog Targets tab, select **Add**. The Add Splunk Syslog Target dialog box opens.
   b. Enter the following information and Select **OK**. The server appears in the Splunk Syslog Targets tab.

<table>
<thead>
<tr>
<th>Address</th>
<th>The hostname or IP address of the Splunk server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP/UDP</td>
<td>The protocol used for Syslog messaging with the server.</td>
</tr>
</tbody>
</table>
Port
The port on the server that is used for Syslog messaging. If the Splunk server uses a different port from the default, specify the actual port used. See Appendix A: Default Communication Settings.

Comment
Optional text that indicates the location or other information that identifies the server.

c. If you need to send data to several Splunk servers, such as servers at different locations, repeat these steps to define additional Syslog targets.

d. To modify the comment, select the server, then select Edit.

- Verify that data inputs defined on the Splunk server use the port and other settings you define here. Refer to the ForeScout App for Splunk How-to Guide.

5. Select the General Settings tab.

<table>
<thead>
<tr>
<th>Splunk Syslog Targets</th>
<th>Splunk HTTP Targets</th>
<th>General Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure Splunk Plugin:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Syslog Message Defaults:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identity: CounterACT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Facility: local4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Priority: info</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CounterACT Data Submission Settings:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Send Property Titles (longer):</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Splunk Alert Message Settings:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>List of Supported IP fields: ip,dest_ip,dest_host,dest_name,dest</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alert Service Authorization Token: 73ED05D8-A363-4F2F-998E-BB73D31B94EB</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Configure default values for Syslog message header fields in the Syslog Message Defaults section. These values override default message settings of the Syslog Plugin, but only for messages sent to Splunk.

- Verify that settings on the Splunk server match the settings you define here. Refer to the ForeScout App for Splunk How-to Guide.

6. This tab also contains the following options and fields:

| Send Property Titles | CounterACT sends host property information to Splunk as Field:Value pairs. By default, the Field: label is the internal property tag of each property. Select this option to send two sets of property value information to Splunk: Using the property tag as the Field: label: va_os : Windows 8.1 64-bit Pro Using the property’s full name as the Field: label: Windows Version : Windows 8.1 64-bit Pro |

Version 2.5.0
List of Supported IP fields

In alert messages sent by Splunk to CounterACT, fields with these tags are parsed for IP Address information. CounterACT evaluates the fields in the order shown in this list: the first IP address found is used to identify the endpoint to which the alert applies.

In Splunk, alert messages must be triggered by search queries that reference/evaluate one of these fields. Refer to the ForeScout App for Splunk How-to Guide.

Alert Service Authorization Token

This string is used in the HTTP message header of alert messages sent to CounterACT by the ForeScout App for Splunk.

7. In the Splunk pane, select Apply. A confirmation dialog box opens.
8. Select Yes to save the configuration, and then select Close.

Configure the Plugin to Use REST Messaging

(Optional) Use the following procedure to configure the plugin to send information to Splunk using HTTP REST messages instead of Splunk Event Collector messages.

To configure the plugin to use REST messaging:
1. In the CounterACT Console, select Options from the Tools menu. The Options dialog box opens.
2. Navigate to and select the Plugins folder.
3. In the Plugins pane, select Splunk, and select Configure. The Splunk pane opens.
4. Define one or more Splunk servers that receive update messages from CounterACT in HTTP POST format:
   a. Select the Splunk HTTP Targets tab, and select Add. The Add Splunk Syslog Target dialog box opens.
   b. In the Splunk HTTP Type drop down, select one of the following:
REST API – used to submit data or queries to the Splunk API. By default, these messages use port 8089 in Splunk.

Event Collector – a Splunk-specific message type used to report event and endpoint data. The default port in Splunk for these messages is 8088.

c. Enter the following information and Select OK. The server appears in the Splunk Syslog Targets tab.

| POST to URL | The target URL that appears in the POST message header. In most cases the URL takes the form of the example shown. Replace my.splunk.com with the IP address of your Splunk server. If the Splunk server uses a different port from the default, specify the actual port used. See Appendix A: Default Communication Settings. |
| Comment | Optional text that indicates the location or other information that identifies the server. |
| REST User Name | The credentials CounterACT uses to access the API on Splunk. Enter the credentials of the account created in Splunk for CounterACT. Refer to the ForeScout App for Splunk How-To Guide. |
| Rest Password |

d. Repeat these steps to define additional HTTP targets.

e. To modify Splunk server information, select the server, then select Edit.

 Verify that data inputs defined on the Splunk server use the port and other settings you define here. Refer to the ForeScout App for Splunk How-to Guide.

5. Select the General Settings tab.
The following options and fields are relevant when REST/HTTP messaging is used to report data to Splunk:

| Send Property Titles | CounterACT sends host property information to Splunk as Field:Value pairs in JSON format. By default, the Field: label is the internal property tag of each property. Select this option to send two sets of property value information to Splunk:
Using the property tag as the Field: label:
va_os: Windows 8.1 64-bit Pro
Using the property’s full name as the Field: label:
Windows Version: Windows 8.1 64-bit Pro |
| List of Supported IP fields | In alert messages sent by Splunk to CounterACT, fields with these tags are parsed for IP Address information. CounterACT evaluates the fields in the order shown in this list: the first IP address found is used to identify the endpoint to which the alert applies. In Splunk, alert messages must be triggered by search queries that reference/evaluate one of these fields. Refer to the ForeScout App for Splunk How-to Guide. |
| Alert Service Authorization Token | This string is used in the HTTP message header of alert messages sent to CounterACT by the ForeScout App for Splunk. |

6. In the Splunk pane, select **Apply**. A confirmation dialog box opens.
7. Select **Yes** to save the configuration, and then select **Close**.
Run Splunk Policy Templates

This module provides the following policy templates used to detect, manage and remediate endpoints based on the Splunk integration.

- The **Send Endpoint and Policy Details to Splunk** template generates a policy that sends endpoint and policy information to Splunk.
- Splunk Stage 1 – Add to HTTP Notification Action Group and Stage 2 - Execute HTTP Notification Action templates provide an example of group-based handling of action request messages received from Splunk.
  - Splunk **Stage 1 - Add to HTTP Notification Action Group** template generates a policy that detects messages that request the HTTP Notification action, and places them in the Splunk HTTP Notification group. Use this as a reference and follow the correct action group based on the action requested from Splunk.
  - Splunk **Stage 2 - Execute HTTP Notification Action** template generates a policy that executes the HTTP Notification action for endpoints in the HTTP Notification Action Group.

Before applying the templates, it is recommended that you have a basic understanding of CounterACT policies before working with the templates. See the CounterACT Templates and Policy Management chapters of the Console User Guide.
Send Endpoint and Policy Details to Splunk

Create policies based on this template to send endpoint properties, classification, and policy information to Splunk.

Run the Template

This section describes how to create a policy from the policy template. For details about how the policy works, see Run Splunk Policy Templates.

To run the template:
1. Log in to the CounterACT Console and select the Policy tab.
2. Select Add from the Policy Manager. The Policy Wizard opens.
3. Expand the Splunk folder and select Send Endpoint and Policy Details to Splunk.
4. Select Next. The Name page of the Policy Wizard opens.

Name the Policy

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

**Naming Tips**

− Make sure names are accurate and clearly reflect what the policy does. For example, do not use a generic name such as My_Compliance_Policy.
− 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 Hosts will be Inspected - Policy Scope**

The Scope pane and IP Address Range dialog box let you define a range of endpoints to be inspected for this policy.

7. Use the IP Address Range dialog box to define which endpoints are inspected. The following options are available for defining a scope:

− **All IPs**: Include all addresses in the Internal Network. The Internal Network was defined when CounterACT was set up.
- **Segment**: Select a previously defined segment of the network. To specify multiple segments, select OK to close the IP Address Range dialog box, and select Segments from the Scope page.

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

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

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

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

9. Select Next. The Main Rule pane opens. See How Devices are Detected and Handled for details of default policy logic.

10. Select Next. The Sub-rules pane opens. See How Devices are Detected and Handled for details of default policy logic.

11. Select Finish. The policy is created.

**How Devices are Detected and Handled**

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

Endpoints that match the Main Rule are included in policy sub-rule inspection. When endpoints do not match the Main Rule, policy evaluation ends. Sub-rules are not evaluated for these endpoints.
Sub-rules are evaluated in order until a match is found. When an endpoint matches the conditions of a sub-rule, the actions of that sub-rule are applied to the endpoint and policy evaluation ends. If the host does not match the conditions of the sub-rule, evaluation moves to the next sub-rule.

**Main Rule**

The main rule of this policy applies no filtering conditions: it includes all endpoints detected by CounterACT within the specified policy scope.

The [Splunk: Send Update from CounterACT Action](#) can send the following information to Splunk for each detected endpoint:

- Selected host properties – by default, the policy sends all host properties.
- Compliance policy status – by default, the policy sends information for all active Compliance policies.
- General policy status – by default, the policy sends all active policy information to Splunk.

For details about specifying the information that is sent to Splunk and for other information about other action options, see [Splunk: Send Update from CounterACT Action](#).

**Sub-Rules**

There are no sub-rules in this policy.

**Stage 1 – Add to HTTP Notification Action Group**

Create policies based on this template to detect messages that request the HTTP Notification action, and place them in the Splunk HTTP Notification group. Use this as a reference and follow the correct action group based on the action requested from Splunk.

**Run the Template**

This section describes how to create a policy from the policy template. See [How Devices are Detected and Handled](#) for details of default policy logic.

**To run the template:**

1. Log in to the CounterACT Console and select the **Policy** tab.
2. Select **Add** from the Policy Manager. The Policy Wizard opens.
3. Expand the **Splunk** folder and select the Execute HTTP Notification Action Group template.
4. Select **Next**. The **Name** page of the policy creation wizard opens.
Name the Policy

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

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

Naming Tips

- Make sure names are accurate and clearly reflect what the policy does. For example, do not use a generic name such as My_Compliance_Policy.
- 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 Hosts will be Inspected - Policy Scope

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

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

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

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

9. Select Next. The Main Rule pane opens. See **How Devices are Detected and Handled** for details of default policy logic.

10. Select Finish. The policy is created.

**How Devices are Detected and Handled**

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

Endpoints that match the Main Rule are included in policy sub-rule inspection. When endpoints do not match the Main Rule, policy evaluation ends. Sub-rules are not evaluated for these endpoints.

Sub-rules are evaluated in order until a match is found. When an endpoint matches the conditions of a sub-rule, the actions of that sub-rule are applied to the endpoint and policy evaluation ends. If the host does not match the conditions of the sub-rule, evaluation moves to the next sub-rule.
**Main Rule**

The main rule captures all Splunk action requests associated with a specific action group.

**Sub-Rules**

The first sub-rule of the policy adds an endpoint to HTTP Notification Action group when an HTTP Notification Action request is received from Splunk. The endpoint is part of the group for a day (default.)

The second sub-rule detects all other endpoints that do not match the action request within a day (default).

**To define the action:**

1. Select **Splunk Alerts** from the Sub-rules, Condition dialog box.
2. Select **Edit**.
3. Select **Splunk Alert Action Group** and then select **Meets the following criteria**.
4. Use the drop-downs to specify the criteria for meeting the Action Group alert.
5. Select **Splunk Alert Action** and then select **Meets the following criteria**.
6. Select Notify – HTTP Notification and then select OK.

Stage 2 - Execute HTTP Notification Action

Create policies based on this template to instruct CounterACT how to handle action request alerts sent to CounterACT from Splunk. The policy detects endpoints for which Splunk has requested the HTTP Notification action and then adds these endpoints to the Splunk HTTP Notification Alerts group.

To support Splunk action request alert messages, create a companion policy based on this template. The policy will then add endpoints to the Splunk HTTP Notification Alerts group when Splunk alert messages request this action for the endpoint.
To implement other actions requested by Splunk, create and modify policies based on this template.

**Run the Template**

This section describes how to create a policy from the policy template. See How Devices are Detected and Handled for details of default policy logic.

**To run the template:**

1. Log in to the CounterACT Console and select the Policy tab.
2. Select Add from the Policy Manager. The Policy Wizard opens.
3. Expand the Splunk folder and select the Execute HTTP Notification Action template.
4. Select Next. The Name page of the policy creation wizard opens.

**Name the Policy**

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

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

**Naming Tips**

- Make sure names are accurate and clearly reflect what the policy does. For example, do not use a generic name such as My_Compliance_Policy.
- 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 Hosts will be Inspected - Policy Scope**

The Scope pane and IP Address Range dialog box let you define a range of endpoints to be inspected for this policy.

7. Use the IP Address Range dialog box to define which endpoints are inspected. The following options are available for defining a scope:

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

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

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

9. Select Next. The Main Rule pane opens. See How Devices are Detected and Handled for details of default policy logic.

10. Select Finish. The policy is created.

The CounterACT Splunk Module tracks the progress of actions requested by Splunk alerts, and reports the final status of the action. This is called the asynchronous response to the alert message. By default, this report is generated 8 hours after the alert message is received.
The following action status values displayed in the Dashboard are reported by CounterACT.

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>The action completed without failure.</td>
</tr>
<tr>
<td>Failure</td>
<td>The action completed with a failure, or timed out.</td>
</tr>
<tr>
<td>Pending</td>
<td>At the time the report is generated, the action is not yet complete. For example, HTTP redirection actions may be waiting for user interaction to complete.</td>
</tr>
<tr>
<td>Init</td>
<td>The action is in Initializing state, and not yet complete.</td>
</tr>
</tbody>
</table>

No Status

No status can be reported for one of the following reasons:

- No active policy detects the relevant Splunk Last Alert property, or applies the requested action.
- The endpoint has been deleted from CounterACT.
- Even though the IP address of the endpoint is within CounterACT’s network scope, the endpoint has not been detected by CounterACT.
- Scheduled CounterACT data purges clear action data before reports are generated.

Invalid

- The endpoint IP is outside the network scope defined in CounterACT.
- An unspecified internal error occurred.

Note that:

- For HTTP Redirection actions, the module can only report either Pending or No Status. The module cannot report Success for these actions.
- If CounterACT users or other CounterACT policies apply the same action to an endpoint that was requested by a Splunk alert, CounterACT will report the result of the most recent application of the action. The report cannot distinguish between the triggers that applied the action to an endpoint.

How Devices are Detected and Handled

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

Endpoints that match the Main Rule are included in policy sub-rule inspection. When endpoints do not match the Main Rule, policy evaluation ends. Sub-rules are not evaluated for these endpoints.

Sub-rules are evaluated in order until a match is found. When an endpoint matches the conditions of a sub-rule, the actions of that sub-rule are applied to the endpoint and policy evaluation ends. If the host does not match the conditions of the sub-rule, evaluation moves to the next sub-rule.

Main Rule

The main rule looks for an endpoint that is part of a specific group and when it finds a match, applies a defined action. The conditions defined in the Criteria section are re-checked every 8 hours (default.)
Sub-Rules
There are no sub-rules in this policy.

Create Custom Splunk Policies

You may need to create a custom policy to capture Splunk action requests supported by this integration but not covered in the policy templates provided with this module. In addition to the bundled CounterACT properties and actions available for detecting and handling endpoints, you can work with properties and actions provided by this module to create custom policies.

To ensure all conditional properties for responding to an action requests are adequately fulfilled, it is best to create this custom policy out of Stage 1 and Stage 2 policy templates provided with CounterACT.

For more information about working with policies, select Help from the Policy Wizard.

To create a custom Splunk Stage 1 policy:

1. Log in to the CounterACT Console.
2. On the Console toolbar, select the Policy tab. The Policy Manager opens.
3. Select Add to create a policy.
4. Select Splunk Stage 1: Add to HTTP Notification Action Group template and select Next.
5. Change the name of the policy to a custom name and then select **Next**.

6. Select an appropriate scope and then select **Next**.

7. Edit the main rule to specify the desired Splunk Alert Action Group. Select **Next**. The Add to Switch Block Action group dialog box displays.

8. In the Condition section, **Edit** the first Sub-Rule and give it a custom name.
9. In the Actions section, **Add** or **Edit** the desired Splunk Alert Action. The Splunk Alert Action Group should be the same as the one specified in the main rule.

10. **Select OK**. The Condition page displays.

11. In the Splunk Alert Action section, select the **Splunk Alert Action** that is to be associated with the custom policy. **Select OK**. The Action dialog box displays.
12. The second sub-rule does not need to be edited. Select Finish.

To Create a Custom Splunk Stage 2 Policy:

1. Log in to the CounterACT Console.
2. On the Console toolbar, select the Policy tab. The Policy Manager opens.
3. Select Add to create a policy. The Policy Wizard displays.
4. Select Splunk Stage 2: Execute HTTP Notification Action template and select **Next**.

5. Change the name of the policy to a custom name and then select **Next**.

6. Select an appropriate scope and then select **Next**. The Condition dialog box displays.
7. In the Condition section, select the “Member of Group” item and **Edit** the main rule condition to specify the group from the Stage 1 policy template.

8. In the Actions section, **Add** or **Edit** the Action in the main-rule to the action for the custom policy.

9. Select **OK**.

**Detecting Endpoints – Policy Properties**

As part of the custom policy you created, the endpoints need to be configured.

**Splunk Alerts**

Splunk alerts messages are sent to CounterACT to request an action to an endpoint.

There are three aspects for every Splunk alert check: Splunk Alert Action Group, Splunk Alert Action, and Splunk Alert Action Server.

**To configure Splunk Alerts:**

1. In the ForeScout Splunk App, search for “Splunk Alerts”. Select it. The Condition pane displays the configurations for Splunk Alerts.
2. The **Splunk Alert Action Group** field maps to an action group in CounterACT. In the Condition pane, select the Action Group values.

3. The **Splunk Alert Action** field maps the action(s) the selected group. If the group meets or does not meet the selected criteria, a request for action (alert) will be sent to CounterACT.

4. The **Splunk Alert Action Server** – Enter the IP address of the server that triggers the alert action request.

5. Select **OK**.

### Managing Splunk Devices – Policy Actions

This section describes the actions that are made available when the Splunk module is installed.

**To access Splunk Actions:**

1. Navigate to the Actions tree from the Policy Actions dialog box.
2. Expand the Audit folder in the Actions tree.
3. The following actions are available:
   - Splunk: Send Custom Notification Action
   - Splunk: Send Update from CounterACT Action

**Splunk: Send Custom Notification Action**

Use this action to send a text message to one or more Splunk servers. This message can include varied information, such as:

- Standard event or error strings that are reported by other components of your security environment.
- Information not included in regular updates of host property and policy information that CounterACT sends to Splunk. For example: add this action to policies that apply or remove the **Switch Block** action to track port blocking in Splunk.

**To use this action:**

1. Select the Send Using Syslog Messages and/or the **Send using HTTP POST** options to determine how CounterACT submits the message to Splunk.

2. For each message type you selected, do one of the following:
   - Select the **Send to All...** option to send the message to all Splunk server targets defined in CounterACT.
   - Select the **Send to Selected...** option to send the message to a subset of Splunk server targets defined in CounterACT.

3. Compose the message text. You can use property tags to include endpoint-specific or user-specific values in this field. See the **Console User Manual** for details.
4. Use the options of the Schedule tab to specify when the action is applied, to delay application of the action, or to specify repeat application of the action.

Splunk: Send Update from CounterACT Action

When sending update messages from the ForeScout Splunk Module to the Splunk server, the update messages contains the IP Address, MAC Address, NetBIOS Host, NetBIOS Domain and Username. If none of these parameters are available, the fields are removed from the update message. If, for a given device, one or more of these attributes cannot be resolved, then the update messages will contain only the ones that have been successfully resolved.

This action submits endpoint data to Splunk. This action is the primary method used for transmitting data from CounterACT to Splunk.

Typically action and policy schedule settings are configured to regularly update Splunk with data for all endpoints detected by CounterACT. For example, see the Send Endpoint and Policy Details to Splunk policy template provided with the module.

Content Sent Tab

Specify the data that is included in the message sent to Splunk.

- Select the **Policy status** option to include the most recent results of policy-based evaluation of the endpoint. CounterACT reports whether the endpoint matches each rule of all active policies.

- Select the **Compliance status** option to include the aggregate Compliance status of the endpoint, based on the Compliance properties.

- Select the **Host Properties** option to include host property values for the endpoint. Do one of the following:
  
  Select the **All Properties** option to include all host property values.
  
  Select the **Selected Properties** option and select properties you want to include. Use the Search field to quickly locate properties.
By default, the Field: label is the internal property tag of each property. You can configure the module to use the full name of each property as the Field: label. See Configure the Module.

**Splunk Server Target Tab**

Select the **Send Using Syslog Messages** and/or the **Send using HTTP POST** options to determine how CounterACT submits the message to Splunk.

For each message type you selected, do one of the following:

- Select the **Send to All...** option to send the message to all Splunk server targets defined in CounterACT.
- Select the **Send to Selected...** option to send the message to a subset of Splunk server targets defined in CounterACT.
Trigger Tab

Specify one or more triggers that send the specified information to Splunk.

- Select the **Send when this action starts** option to send a message when the endpoint matches the conditions of a policy rule that invokes this action.
- Select the **Send whenever information is updated** option to send a message when the specified information changes. For example, if a previously compliant endpoint no longer satisfies Compliance policies, the message is sent.
- Select the **Send periodically** option to repeatedly send the message at the time interval you specify, with updated information. Messages are sent periodically as long as the endpoint satisfies the conditions of the policy rule that invokes this action.

Schedule Tab

Use the options of the Schedule tab to specify when the action is applied, to delay application of the action, or to specify repeat application of the action.
Appendix A: Default Communication Settings

The following table lists default settings for the communication between Splunk and CounterACT.

<table>
<thead>
<tr>
<th>Name</th>
<th>Direction</th>
<th>Protocol</th>
<th>Port</th>
<th>To customize</th>
</tr>
</thead>
<tbody>
<tr>
<td>REST</td>
<td>To Splunk</td>
<td>HTTPS</td>
<td>8089</td>
<td>Enter custom port/URL in the POST to URL field when you Configure the Module.</td>
</tr>
<tr>
<td>Event Collector</td>
<td>To Splunk</td>
<td>HTTPS</td>
<td>8088</td>
<td></td>
</tr>
</tbody>
</table>
| Syslog          | To Splunk     | TCP/UDP    | 515  | 1. In Splunk: clone the Data Input, and customize port.  
                                        |               |           | 2. In CounterACT: customize Port and TCP/UDP fields when you Configure the Module. |
| Alert API       | To CounterACT | HTTP       | 80   | In Splunk: edit the URL of the built in Alerts. |

Mapping CounterACT Data to the CIM Model

This section describes mapping of CounterACT host properties to the CIM model.

Certificates

**Tags:** certificate

Splunk Reference:  
[http://docs.splunk.com/Documentation/CIM/4.5.0/User/Certificates](http://docs.splunk.com/Documentation/CIM/4.5.0/User/Certificates)

<table>
<thead>
<tr>
<th>Data Model Field</th>
<th>CounterACT Field Tag</th>
</tr>
</thead>
<tbody>
<tr>
<td>ssl_name</td>
<td>Name</td>
</tr>
<tr>
<td>ssl_serial</td>
<td>Serial_Number</td>
</tr>
<tr>
<td>ssl_is_valid</td>
<td>Status</td>
</tr>
<tr>
<td>ssl_issuer_common_name</td>
<td>CN</td>
</tr>
<tr>
<td>ssl_subject_unit</td>
<td>OU</td>
</tr>
<tr>
<td>ssl_subject_locality</td>
<td>L</td>
</tr>
<tr>
<td>ssl_subject_state</td>
<td>S</td>
</tr>
<tr>
<td>sslIssuer</td>
<td>Issuer</td>
</tr>
<tr>
<td>ssl_start_time</td>
<td>Not_Before</td>
</tr>
<tr>
<td>ssl_end_time</td>
<td>Not_After</td>
</tr>
</tbody>
</table>
Compute_Inventory: CPU

**Tags:** cpu

Splunk Reference: [http://docs.splunk.com/Documentation/CIM/4.5.0/User/ComputeInventory](http://docs.splunk.com/Documentation/CIM/4.5.0/User/ComputeInventory)

<table>
<thead>
<tr>
<th>Data Model Field</th>
<th>CounterACT Field Tag</th>
</tr>
</thead>
<tbody>
<tr>
<td>cpu_cores</td>
<td>Number_Of_Cores</td>
</tr>
<tr>
<td>family</td>
<td>Family</td>
</tr>
<tr>
<td>cpu_load_percent</td>
<td>Load_Percentage</td>
</tr>
</tbody>
</table>

Compute_Inventory: Network

**Tags:** network

Splunk Reference: [http://docs.splunk.com/Documentation/CIM/4.5.0/User/ComputeInventory](http://docs.splunk.com/Documentation/CIM/4.5.0/User/ComputeInventory)

<table>
<thead>
<tr>
<th>Data Model Field</th>
<th>CounterACT Field Tag</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip</td>
<td>IP_Address</td>
</tr>
<tr>
<td>dns</td>
<td>DNS_HostName</td>
</tr>
<tr>
<td>mac</td>
<td>MAC_Address</td>
</tr>
</tbody>
</table>

Compute_Inventory: Memory

**Tags:** memory

Splunk Reference: [http://docs.splunk.com/Documentation/CIM/4.5.0/User/ComputeInventory](http://docs.splunk.com/Documentation/CIM/4.5.0/User/ComputeInventory)

<table>
<thead>
<tr>
<th>Data Model Field</th>
<th>CounterACT Field Tag</th>
</tr>
</thead>
<tbody>
<tr>
<td>mem</td>
<td>Capacity</td>
</tr>
</tbody>
</table>

Compute_Inventory: Storage

**Tags:** storage

Splunk Reference: [http://docs.splunk.com/Documentation/CIM/4.5.0/User/ComputeInventory](http://docs.splunk.com/Documentation/CIM/4.5.0/User/ComputeInventory)

<table>
<thead>
<tr>
<th>Data Model Field</th>
<th>CounterACT Field Tag</th>
</tr>
</thead>
<tbody>
<tr>
<td>storage</td>
<td>Size__Megabytes_</td>
</tr>
<tr>
<td>storage_free</td>
<td>Free_Space__Megabytes_</td>
</tr>
</tbody>
</table>
**Blocked_Malware**

*Tags:* malware, attack

Splunk Reference: [http://docs.splunk.com/Documentation/CIM/4.5.0/User/Malware](http://docs.splunk.com/Documentation/CIM/4.5.0/User/Malware)

<table>
<thead>
<tr>
<th>Data Model Field</th>
<th>CounterAct Field Tag</th>
</tr>
</thead>
<tbody>
<tr>
<td>file_hash</td>
<td>Threat_File_MD5</td>
</tr>
<tr>
<td>file_name</td>
<td>Threat_File_Name</td>
</tr>
<tr>
<td>sender</td>
<td>host</td>
</tr>
</tbody>
</table>

**Subset of Core Properties**

Additionally, the following subset of core properties has been mapped to tags in the CIM model.

<table>
<thead>
<tr>
<th>CounterACT Property (Name and Tag)</th>
<th>Splunk Tag</th>
<th>Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address {ip}</td>
<td>dest, dest_ip</td>
<td>All</td>
</tr>
<tr>
<td>Windows Processes Running {process_no_ext}</td>
<td>process</td>
<td>Application State</td>
</tr>
<tr>
<td>Linux Processes Running {linux_process_running}</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Macintosh Processes Running {mac_process_running}</td>
<td></td>
<td></td>
</tr>
<tr>
<td>User {user}</td>
<td>user</td>
<td>All</td>
</tr>
<tr>
<td>Windows Services Running {service}</td>
<td>service</td>
<td>Application State / Services</td>
</tr>
<tr>
<td>Windows Services Installed {service_installed}</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NetBIO Domain {nbtdomain}</td>
<td>dest_nt_domain</td>
<td>Malware</td>
</tr>
<tr>
<td>Malicious Event {malic}</td>
<td>ids_type=host category, signature</td>
<td>Intrusion Detection</td>
</tr>
<tr>
<td>Appliance</td>
<td>dvc, dvc_ip</td>
<td>Intrusion Detection</td>
</tr>
</tbody>
</table>
Additional CounterACT Documentation

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

- Documentation Portal
- 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 and 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:
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

1. Select CounterACT Help from the Help menu.

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

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

Copyright © ForeScout Technologies, Inc. 2000-2016. 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 are protected by 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 a valid written agreement signed by you and ForeScout that governs the below ForeScout products and services:

- If you have purchased any ForeScout products, your use of such products 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 have purchased any ForeScout Professional Services, the provision of such services is subject to your acceptance of the terms set forth at http://www.forescout.com/professional-services-agreement/;
- 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 an Early Availability Product, the terms applicable to your use of such product are set forth at: http://www.forescout.com/early-availability-agreement/.
  - 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

2016-11-09 16:07