CounterACT ARF Reports Plugin

Configuration Guide

Version 1.0.2 and Above

Table of Contents

About the ARF Reports Plugin

The ARF Reports Plugin provides CounterACT users with the **ARF Report** template, which is available in the CounterACT **Reports Portal**. Working with this report template, users define and generate reports that provide information about CounterACT-detected assets.

The structure and content of these reports follow the Asset Reporting Format (ARF) data model, which is a component of the Security Content Automation Protocol (SCAP). ARF is a standard for compiling IT asset information. Information that is compiled using this standard can be easily shared with third-party systems.

Plugin generated ARF Reports are XML formatted into a file that is then transferred to a remote server, which is specified by the user.

All features provided by the CounterACT **Reports Portal** are available for use with the **ARF Report** template. These include accessing reports, scheduling reports, saving reports and managing reports. For feature information available with the **Reports Portal**, refer to the *CounterACT Reports Plugin Configuration Guide*.

Report Content

ARF reports contain the following XML sections:

- Assets
- Reports

Assets

The XML section **assets** provides the **computing-device** properties for each CounterACT-detected asset. The report lists each CounterACT-detected asset by an assigned **asset-id**. Properties reported per asset are:

- Common Platform Enumeration (CPE): IT product and platform information encoded in a standard, machine-readable format. CPE information is reported for Windows, Macintosh and Linux endpoints.
  - In order for the plugin to report operating system CPE information, these endpoints must be managed by either Remote Inspection or SecureConnector. The ARF Reports Plugin obtains operating system CPE information about these endpoints from the resolved OS CPE Format property.

  CPE information examples:

  - Windows: **`cpe:2.3:o:microsoft:Windows_Server_2008_64-bit_R2:-:Service_Pack_1:-:*:Enterprise_Edition`**
  - Macintosh: **`cpe:2.3:o:apple:mac_os_x:10.8.0:*:*:*:*:*:*:*`**
  - Linux: **`cpe:2.3:o:centos:centos:6.1:*:*:*:*:*:*:*`**
- Connections:
  - IP address
  - MAC address
- Fully Qualified Domain Name (FQDN)
- Host Name

When no information is available to report about a property, that property is not listed for the CounterACT-detected asset. For example, if a CounterACT-detected asset has no FQDN, there will be no **fqdn** entry for the asset listed in the report.

Reports

The XML section ***reports*** appears following the XML section ***assets***. The plugin does not provide any information in this section. This section can be ignored.

Report File Transfer

Definition of an **ARF Report** template includes a remote server location to where the generated report is transferred (a server location that should be accessible to report consumers). The following data transfer protocols are available:

- FTP
- SFTP
- SCP

Example:

Define an ARF report that is generated daily at 5:00 am and transferred via SFTP to your Enterprise GRC system.

Requirements

The following CounterACT releases must be installed to run the ARF Reports Plugin:

- CounterACT 7.0.0, Service Pack 2.0.1 or above
- Reports Plugin, version 4.1.3 or above
- If you want the ARF Reports Plugin to provide CPE information about Windows endpoints, install the HPS Applications Plugin, version 2.0.2 or above
- If you want ARF Reports Plugin to provide CPE information about Macintosh and Linux endpoints, install the Macintosh/Linux Property Scanner Plugin, version 6.1.9 or above

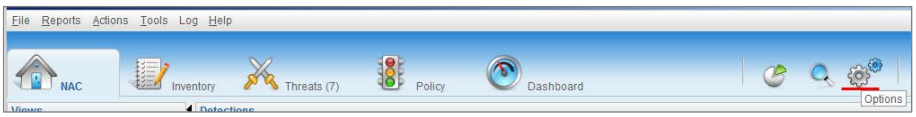
Refer to the *CounterACT Reports Plugin Configuration Guide* for all other report-related requirements.

Install the Plugin

To install the plugin:

1. Acquire a copy of the plugin in either one of the following ways, as relevant:
   a. If you are installing a Beta release of this plugin, acquire the plugin from your ForeScout representative or contact beta@forescout.com.
   b. Otherwise, navigate to the Customer Support Plugins page and download the plugin.
2. Save the plugin installation file to the machine where the CounterACT Console is installed.

3. Log in to CounterACT and select the **Options** icon from the CounterACT Console toolbar.



4. Navigate to the **Plugins** folder. The Plugins pane opens.
5. In the Plugins pane, select **Install**. The **Open** dialog box opens.
6. Navigate to the plugin save location. Select the plugin **`.fpi`**.
7. Select **Install**. An upgrade information dialog box and a license agreement dialog box open.
8. In each dialog box, select **OK.** The installation proceeds to completion.

Configure the Plugin

This plugin does not require any configuration.

Working with the ARF Report Template

Use the **ARF Report** template to define reports that provide property information about CounterACT-detected assets. Plugin generated ARF reports are in XML format. As with other CounterACT reports, an ARF report can be either immediately generated or generated on a scheduled basis.

Immediate Report Generation

With immediate report generation, the following occurs:

- The generated report is transferred in a file to a remote server location, based on the information you defined in the report template parameters page. The file name format is

  `arf_report_template_Forescout_report_<Day_Month_Date>_<HH_MM_SS>_<Time Zone>_<Year>-<count>.xml`.

  Where:

  – **`<HH_MM_SS>`** is in 24 hour format.

  – **`<count>`** is an integer value, starting at zero, that is incremented with each, subsequent, generated report. **`<count>`** resets to zero every time the Enterprise Manager is restarted.

  File name example:

  `arf_report_template_Forescout_report_Tue_Jun_10_19_55_38_CDT_2014-8.xml`.

- The generated report is displayed in a web page, using your machine's default web browser. For the list of supported browsers, refer to the *CounterACT Reports Plugin Configuration Guide*.

Scheduled Report Generation

With scheduled ARF Report generation, the following occurs:

- The generated report is transferred in a file to a remote server location, based on the file transfer information you defined in the report template parameters page. The file name format is

  `arf_report_template_Forescout_report_<Day_Month_Date>_<HH_MM_SS>_<Time Zone>_<Year>-<count>.xml`. For details about the file name format, see Immediate Report Generation.

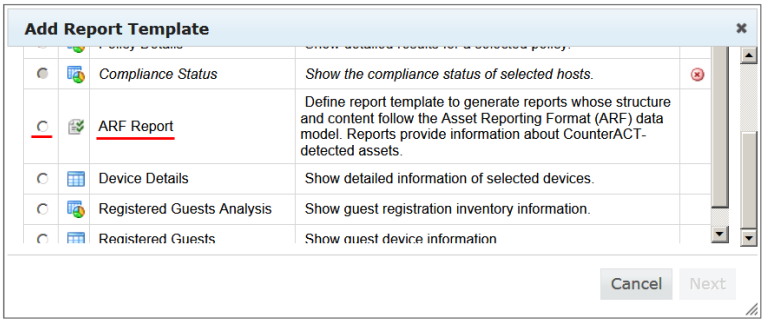
- The generated report is delivered by email to the email address you defined in the report template parameters page. It is sent in an attached file that has the same file name as the transferred file.

Creating an ARF Report

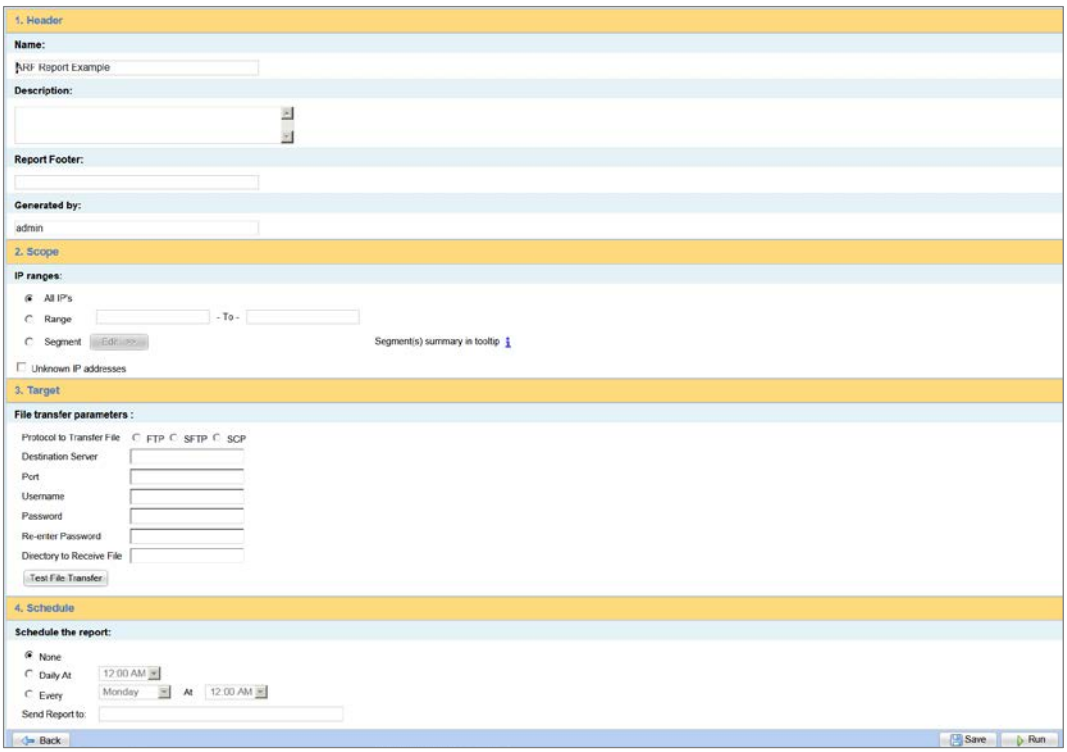
To create an ARF Report:

1. In the CounterACT Console toolbar, select the **Reports Portal** icon.

2. In the **Reports Portal** home page, select **Add**. The **Add Report Template** dialog opens.



3. Select **ARF Report** and then select **Next**. The report template parameters page opens.



4. In the **Header** section:

   – In the **Name** field, enter a report name (*required*). Maximum length is 60 characters. The following characters cannot be used in this field:

     & # : / ' ` "

   – In the **Description** field, enter descriptive text (*optional*).

   – In the **Generated by** field, enter the name of the CounterACT user generating or associated with the report (*optional*). Maximum length is 60 characters.

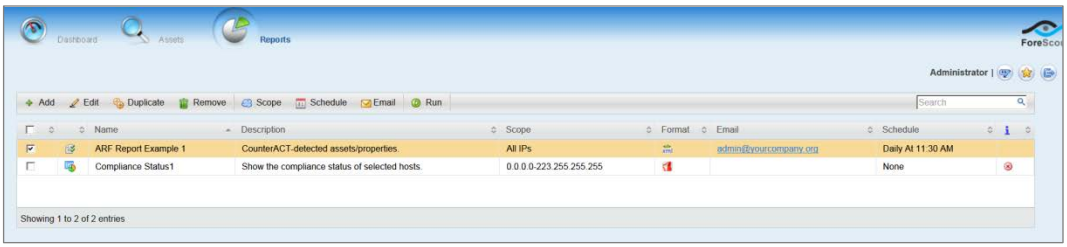
   When an ARF report is generated, the information defined in the **Header** section is not included in the report, since this information is not part of the ARF data model standard. The sole purpose of the information provided in these fields is to support the user of the ARF Report template.

5. In the **Scope** section, select either all IPs, a host IP range or the network IP segments for which to create the report. Select **Unknown IP addresses** to include hosts at which a MAC address was detected, rather than an IP address.
6. In the **Target** section, provide the following details that are used to transfer the generated ARF report to a remote server:
   - **Protocol to Transfer File**: Select the protocol that will be used to transfer the file containing the generated ARF report.
   - **Destination Server**: Specify the server to which the file will be transferred. Enter either the server IP address, the server FQDN or the server name.
   - **Port**: Specify the port number to connect to on the remote server. The default port of the selected transfer protocol automatically appears in this field.
   - **User**: Specify the username to use when logging in to the remote server.
   - **Password**: Specify the password to use when logging in to the remote server.
   - **Re-enter Password**: Verify the specified password by re-entering it in this field.
   - **Directory to Receive File**: Specify the directory to receive the transferred file.
7. In the **Target** section, select **Test File Transfer** to execute a file transfer test based on the information defined in this section.
8. In the **Schedule** section, define a report generation schedule (optional).
   - Define a schedule to generate either

     a daily recurring report (**Daily At** <*time of day*>)

     or a day of week recurring report (**Every** <*day of week*> **At** <*time of day*>).
   - In the **Send Report to** field, enter an email address to send the generated report to. You may enter multiple email addresses, separating them with commas.
9. Perform either of the following:
   - Select **Run** to generate a report using the defined report template.
   - Select **Save** to save the defined report template for later use.

     The defined report template is saved and appears in the **My Reports** table on the **Reports Portal** home page.



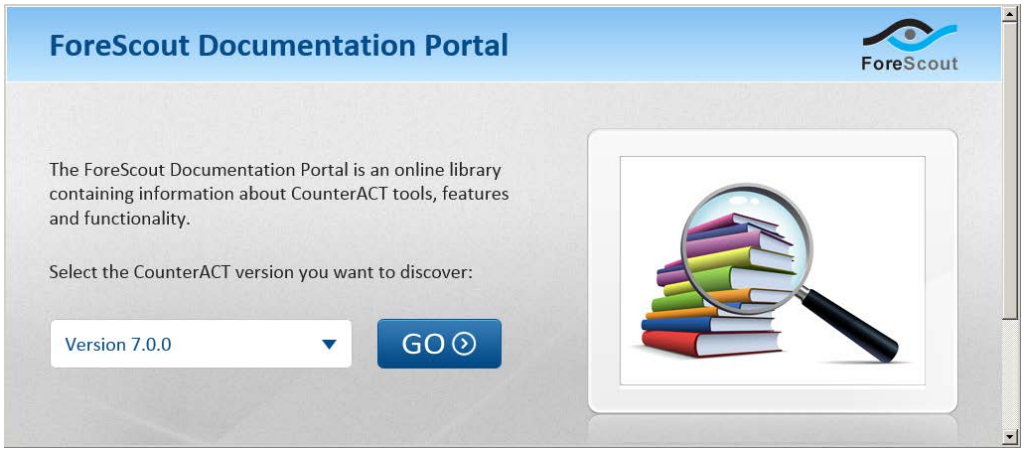
Additional CounterACT Documentation

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

- Documentation Portal
- Customer Support Portal
- CounterACT Console Help Tools

Documentation Portal

The ForeScout Documentation Portal is Web-based library containing information about CounterACT tools, features and functionality and integrations.



To access the Documentation Portal

1. Go to www.forescout.com/kb.
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, Hotfixes, Plugins and Module as well as related documentation. The portal also provides a variety of How-to Guides, Installation guides and more.

To access the Customer Portal:

1. Go to https://updates.forescout.com/support/index.php?url=counteract.
2. Select the CounterACT version you want to discover.

CounterACT Console 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. Select **Options** from the **Tools** menu and the select **Plugins**.
2. Select a plugin and then select **Help**.

Documentation Portal

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

Legal Notice