ForeScout CounterACT®

ARF Reports Module

Configuration Guide

Version 1.0.3

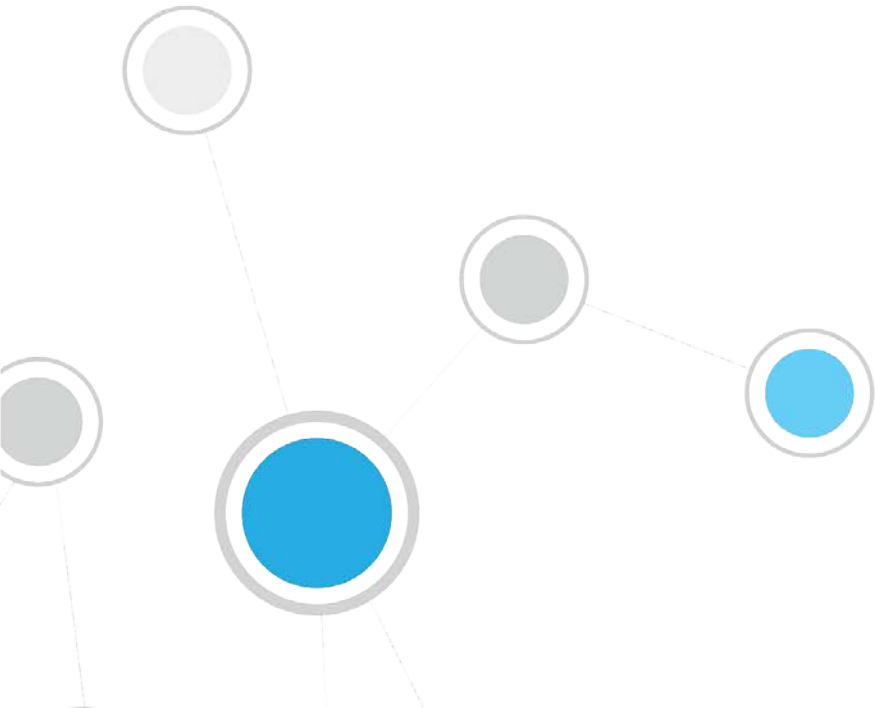


Table of Contents

About the ARF Reports Module

The ForeScout CounterACT ARF Reports Module 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.

ARF Reports are generated in XML format 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 Core Extensions Module 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 Module to report operating system CPE information, these endpoints must be managed by Remote Inspection or by the SecureConnector. The ARF Reports Module 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 ***reports*** section appears following the XML ***assets*** section. The Module 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 Module requires the following CounterACT releases and other CounterACT components:

- CounterACT 8.0
- Core Extensions Module version 1.0 with the Reports Plugin running.
- If you want the ARF Reports Module to provide CPE information about Windows endpoints, install the Windows Applications Content Module, version 2.1.4.
- If you want ARF Reports Module to provide CPE information about Macintosh and Linux endpoints, you must have Endpoint Module version 1.0 with the following components running:
  - Linux Plugin, if there are Linux endpoints in your environment
  - OS X Plugin, if there are macOS/OS X endpoints in your environment
- An active Maintenance Contract for CounterACT devices is required.

Install the Module

To install the module:

1. Navigate to one of the following ForeScout portals, depending on the licensing mode your deployment is using:
   - Product Updates Portal - ***Per-Appliance Licensing Mode***
   - Customer Portal, Downloads Page - ***Centralized Licensing Mode***

   To find out which licensing mode your deployment is working with, see Identifying Your Licensing Mode in the Console.
2. Download the module **`.fpi`** file.
3. Save the file to the machine where the CounterACT Console is installed.
4. Log into the CounterACT Console and select **Options** from the **Tools** menu.
5. Select **Modules**. The Modules pane opens.
6. Select **Install**. The Open dialog box opens.
7. Browse to and select the saved module **`.fpi`** file.
8. Select **Install**. The Installation wizard opens.
9. Select **I agree to the License Agreement**, and select **Install**. The installation will not proceed if you do not agree to the license agreement.

   Make sure you have selected the correct module to install. The installation will begin immediately after selecting Install, and cannot be interrupted or canceled.

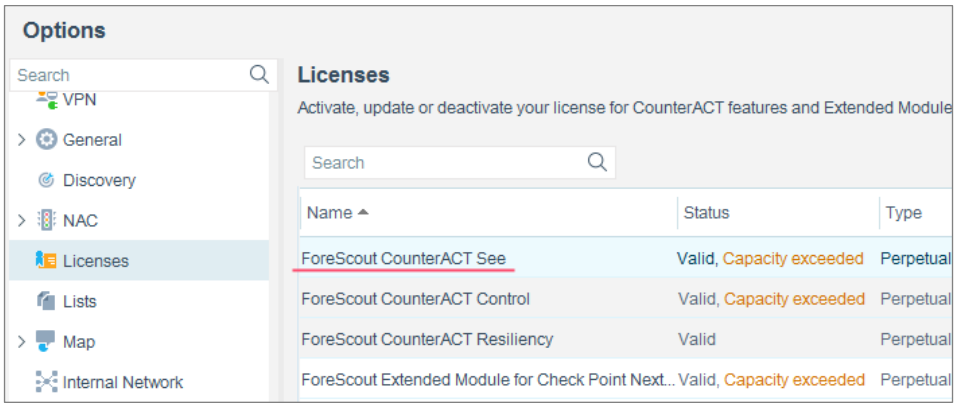
   In modules that contain more than one component, the installation proceeds automatically one component at a time.

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

Identifying Your Licensing Mode in the Console

If your Enterprise Manager has a *ForeScout CounterACT See* license listed in the Console, your deployment is operating in Centralized Licensing Mode. If not, your deployment is operating in Per-Appliance Licensing Mode.

Select **Options > Licenses** to see whether you have a *ForeScout CounterACT See* license listed in the table.



Contact your ForeScout representative if you have any questions about identifying your licensing mode.

Configure the Module

This Module does not require any configuration.

Verify That the Module Is Running

After configuring the module, verify that it is running.

To verify:

1. Select **Tools**>**Options** and then select **Modules**.
2. Navigate to the module and select **Start** if the module is not running.

Working with the ARF Report Template

Use the **ARF Report** template to define reports that provide property information about CounterACT-detected assets. Module 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 *ForeScout CounterACT Core Extensions Module 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

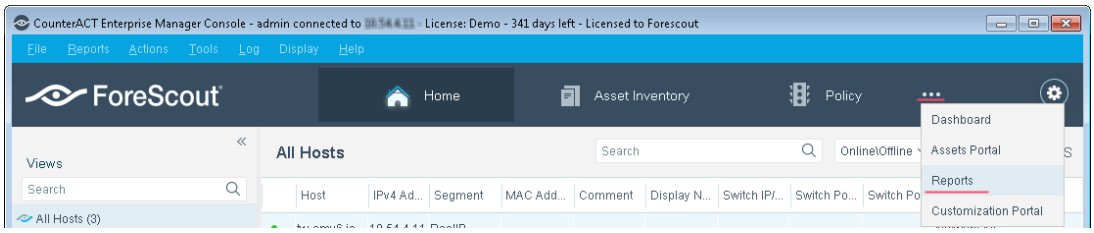
  arf_report_template_Forescout_report_<Day_Month_Date>_<HH_MM_SS>_<Time Zone>_<Year>-<count>.xml. For details about the file name format, see Immediate Report Generation.

- 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.

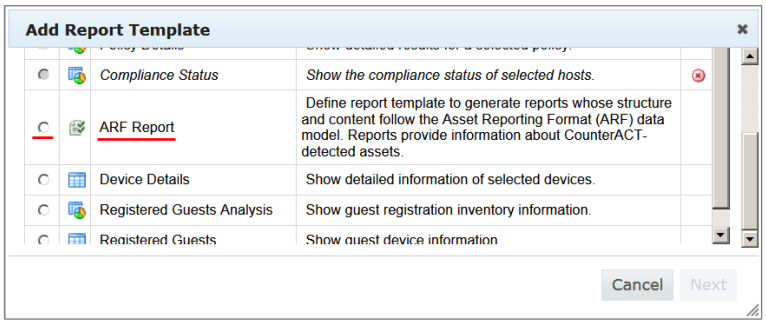
Creating an ARF Report

To create an ARF Report:

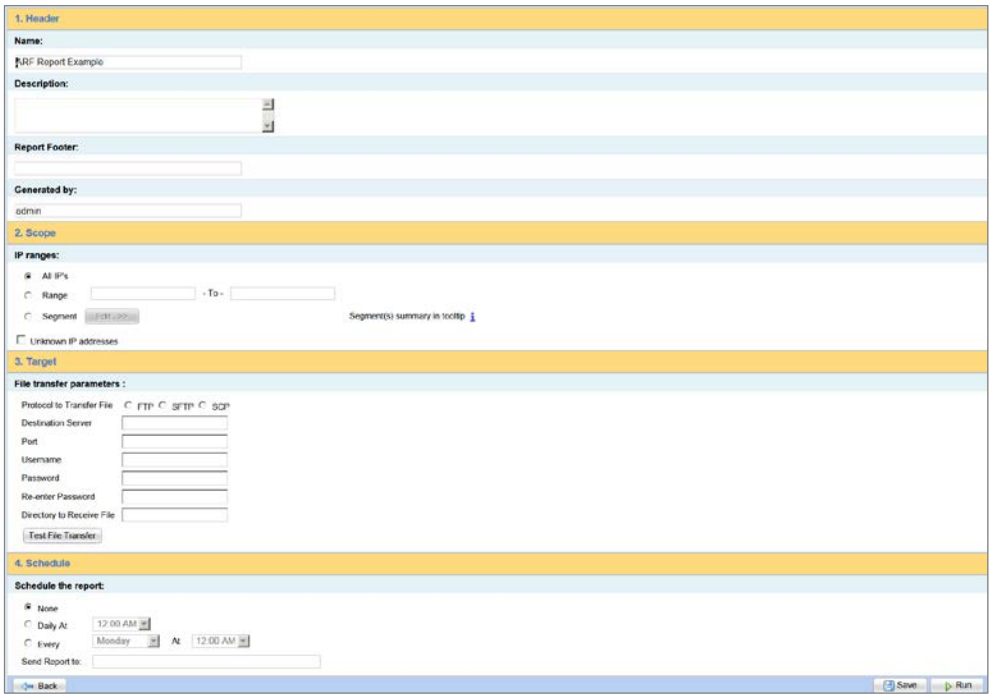
1. Select the **Ellipsis icon** ••• from the **Toolbar** menu and select **Reports** from the dropdown menu. The Reports page opens in a browser.



2. In the **Reports** 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.

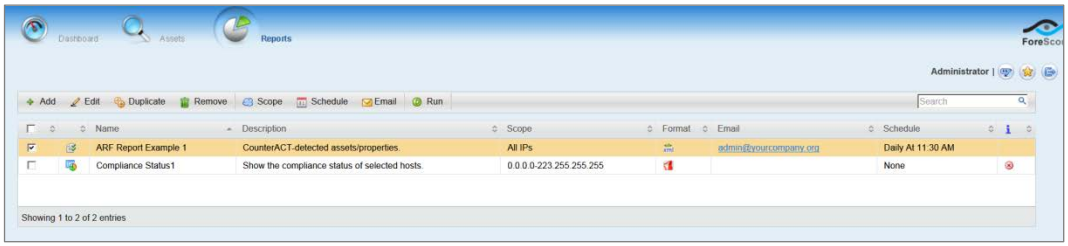
   When an ARF report is generated, the information defined in the **Header** section is not included in the report, since this information is not part of the ARF data model standard. The sole purpose of the information provided in these fields is to support the user of the ARF Report template.

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** page.



Additional CounterACT Documentation

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

- Documentation Downloads
- Documentation Portal
- CounterACT Help Tools

Documentation Downloads

Documentation downloads can be accessed from one of two ForeScout portals, depending on which licensing mode your deployment is using.

- ***Per-Appliance Licensing Mode*** - Product Updates Portal
- ***Centralized Licensing Mode*** - Customer Portal

Software downloads are also available from these portals.

To learn which licensing mode your deployment is using, see Identifying Your Licensing Mode in the Console.

Product Updates Portal

The Product Updates Portal provides links to CounterACT version releases, Base and Content Modules, and Extended Modules, as well as related documentation. The portal also provides a variety of additional documentation.

To access the Product Updates Portal:

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

Customer Portal

The Downloads page on the ForeScout Customer Portal provides links to purchased CounterACT version releases, Base and Content Modules, and Extended Modules, as well as related documentation. Software and related documentation will only appear on the Downloads page if you have a license entitlement for the software. The Documentation page on the portal provides a variety of additional documentation.

To access documentation on the ForeScout Customer Portal:

1. Go to https://forescout.force.com/support/.
2. Select **Downloads** or **Documentation**.

Documentation Portal

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

If your deployment is using Centralized Licensing Mode, you may not have credentials to access this portal.

To access the Documentation Portal:

1. Go to www.forescout.com/docportal.
2. Use your customer support credentials to log in.
3. Select the CounterACT version you want to discover.

CounterACT 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.

CounterACT Administration Guide

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 **Modules**.
2. Select the plugin and then select **Help**.

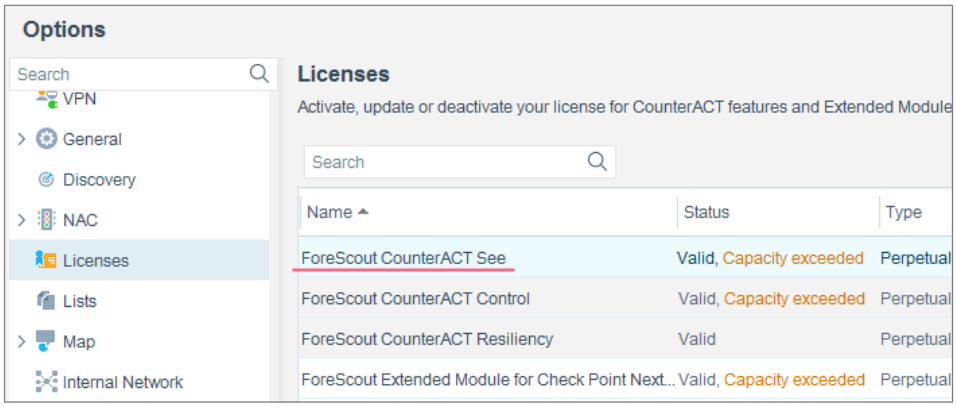
Documentation Portal

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

Identifying Your Licensing Mode in the Console

If your Enterprise Manager has a *ForeScout CounterACT See* license listed in the Console, your deployment is operating in Centralized Licensing Mode. If not, your deployment is operating in Per-Appliance Licensing Mode.

Select **Options > Licenses** to see whether you have a *ForeScout CounterACT See* license listed in the table.



Contact your ForeScout representative if you have any questions about identifying your licensing mode.

Legal Notice

2018-04-10 09:21