FORESCOUT

Forescout

ARF Reports Module

Configuration Guide

Version 1.0.4

Contact Information

Forescout Technologies, Inc.

190 West Tasman Drive

San Jose, CA 95134 USA

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

Toll-Free (US): 1.866.377.8771

Tel (Intl): 1.408.213.3191

Support: 1.708.237.6591

About the Documentation

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

Legal Notice

2020-06-17 19:27

Table of Contents

About the ARF Reports Module

The Forescout® ARF Reports Module provides users with the **ARF Report** template, which is available in the Forescout **Reports Portal**. Working with this report template, users define and generate reports that provide information about assets detected by the Forescout platform.

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 Forescout **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 Forescout 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 detected asset. The report lists each 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.
  - 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 detected asset. For example, if a 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.

ARF Reports Module Requirements

The Module requires the following components:

- CounterACT 8.0, Forescout 8.1.x, Forescout 8.2 or Forescout interim release 8.2.1
- The Core Extensions Module with the Reports Plugin running -
  - Core Extensions Module version 1.0.1 (CounterACT 8.0)
  - Core Extensions Module version 1.1.3 (Forescout 8.1.x)
  - Core Extensions Module version 1.2 (Forescout 8.2)
  - Core Extensions Module version 1.2.1 (Forescout interim release 8.2.1)
- If you want the ARF Reports Module to provide CPE information about Windows endpoints, install the Content Module Windows Applications version 20.0.2

- If you want the ARF Reports Module to provide CPE information about Macintosh and Linux endpoints, you must have the Endpoint Module –
  - Endpoint Module version 1.0.1 (CounterACT 8.0)
  - Endpoint Module version 1.1.3 (Forescout 8.1.x)
  - Endpoint Module version 1.2 (Forescout 8.2)
  - Endpoint Module version 1.2.1 (Forescout interim release 8.2.1)

  with the following components running:
  - The Linux Plugin, if Linux endpoints access your network
  - The OS X Plugin, if macOS/OS X endpoints access your network

Install the Module

To install the module:

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

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

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

   In modules that contain more than one component, the installation proceeds automatically one component at a time.
10. When the installation completes, select **Close** to close the window. The installed module is displayed in the Modules pane.

    Some components are not automatically started following installation.

Configure the Module

This 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 detected assets. Module generated ARF reports are in XML format. As with other reports provided by the Forescout Reports Portal, 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 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

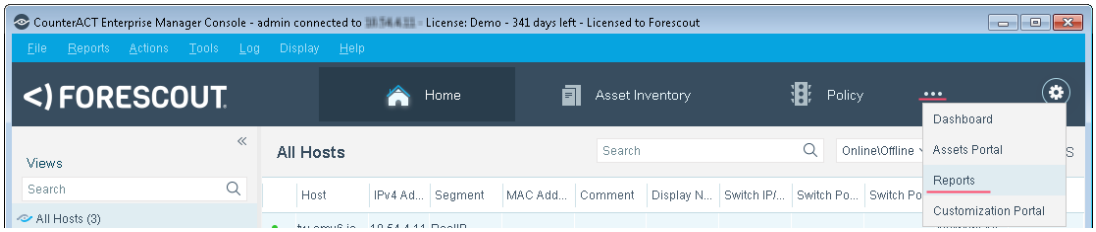
  `arf_report_template_Forescout_report_<Day_Month_Date>_<HH_MM_SS>_<Time Zone>_<Year>-<count>.xml`. For details about the file name format, see Immediate Report Generation.

- 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.

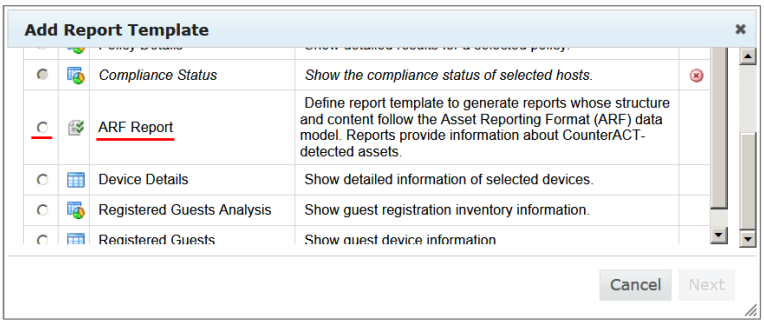
Creating an ARF Report

To create an ARF Report:

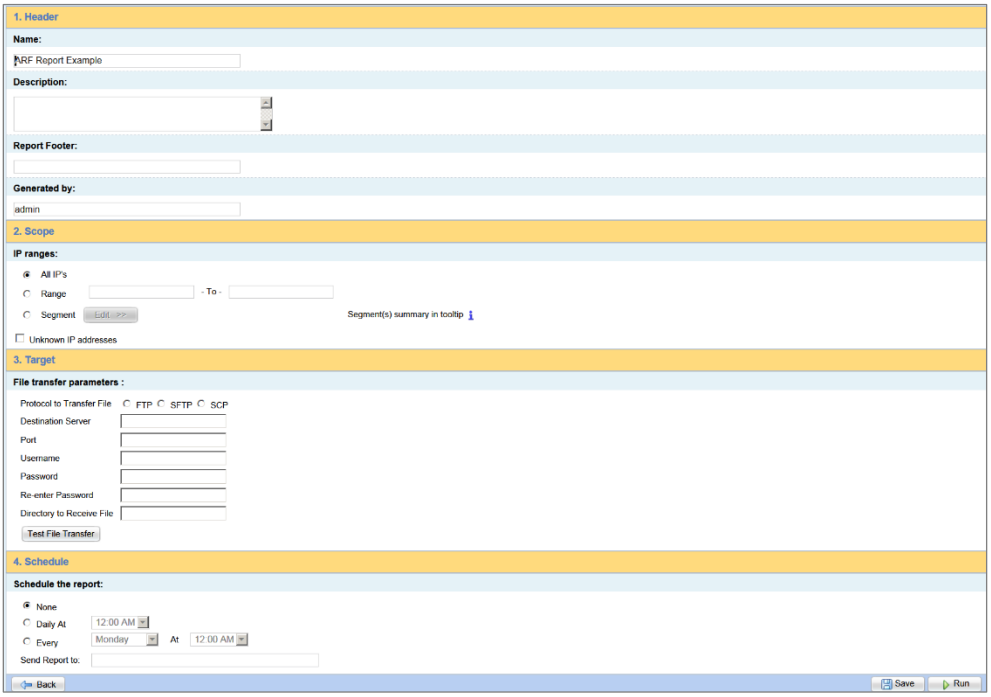
1. Select the **Ellipsis icon** ••• from the **Toolbar** menu and select **Reports** from the dropdown menu. The Reports page opens in a browser.



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.



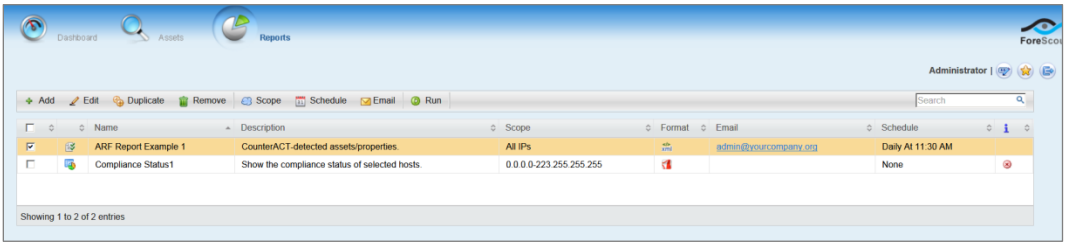
4. In the **Header** section:
   - In the **Name** field, enter a report name (*required*). Maximum length is 60 characters. The following characters cannot be used in this field:
     & # : / ' ` "
   - In the **Description** field, enter descriptive text (*optional*).
   - In the **Generated by** field, 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 Forescout Documentation

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

- Documentation Downloads
- Documentation Portal
- Forescout Help Tools

Documentation Downloads

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

- ***Per-Appliance Licensing Mode*** – Product Updates Portal
- ***Flexx Licensing Mode*** – Customer Support Portal

Software downloads are also available from these portals.

To identify your licensing mode:

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

Technical Documentation Page

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

To access the Technical Documentation page:

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

Product Updates Portal

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

To access the Product Updates Portal:

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

Customer Support Portal

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

To access documentation on the Customer Support Portal:

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

Documentation Portal

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

To access the Documentation Portal:

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

Forescout Help Tools

You can access individual documents, as well as the Documentation Portal, directly from the Console.

Console Help Buttons

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

Forescout Administration Guide

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

Plugin Help Files

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

Content Module, eyeSegment Module, and eyeExtend Product Help Files

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

Documentation Portal

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