



ForeScout

Core Extensions Module: Reports Plugin

Configuration Guide

Version 5.2.1



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 Forescout Technologies, Inc. All rights reserved. Forescout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents can be found at <https://www.Forescout.com/company/legal/intellectual-property-patents-trademarks>. Other brands, products, or service names may be trademarks or service marks of their respective owners.

2020-07-09 09:31

Table of Contents

| | |
|--|-----------|
| About the Reports Plugin | 4 |
| Overlapping IP Address Support | 4 |
| Requirements | 4 |
| Forescout Requirements | 5 |
| Web Browser Requirements | 5 |
| Supported Browsers | 5 |
| Verify That the Plugin Is Running | 7 |
| Accessing the Reports Portal | 7 |
| Managing Reports | 9 |
| Saving Reports and Creating Report Schedules | 9 |
| Tracking Reports | 10 |
| Filter and Find | 11 |
| Simultaneously Manage Multiple Reports | 11 |
| Additional Report Management Tools | 12 |
| Configure Date/Time Format for Report Output | 12 |
| Report Templates | 12 |
| Assets Inventory | 13 |
| Working with Tables | 18 |
| Vulnerability | 19 |
| Policy Trend | 21 |
| Policy Status | 22 |
| Policy Details | 23 |
| Compliance Status | 24 |
| Device Details | 26 |
| Registered Guest Analysis | 27 |
| Registered Guests | 30 |
| Selecting Properties to Display | 32 |
| Changing CounterACT User Passwords | 33 |
| Core Extensions Module Information | 34 |
| Additional Forescout Documentation | 34 |
| Documentation Downloads | 35 |
| Documentation Portal | 35 |
| Forescout Help Tools | 36 |

About the Reports Plugin

The Reports Plugin is a component of the Forescout Core Extensions Module. See [Core Extensions Module Information](#) for details about the module.

The Reports Plugin lets you generate reports with real-time and trend information about policies, host compliance status, vulnerabilities, device details, assets and network guests.

Use reports to keep network administrators, executives, the Help Desk, IT teams, security teams or other enterprise teams well-informed about network activity. Reports can be used, for example, to help you understand:

- Long term network compliance progress/trends
- Immediate security needs
- Compliance with policies
- Status of a specific policy
- Network device statistics

You can create reports and view them immediately, save reports or generate schedules to ensure that network activity and detections are automatically and consistently reported.

In addition, you can use any language supported by your operating system to generate reports. Reports can be viewed and printed as either PDF or CSV files.

Overlapping IP Address Support

The Reports Plugin supports reporting information about networks that use overlapping IP addresses. For example, when preparing a report, if the selected IP address segment is assigned an IP Reuse Domain (IRD), the plugin report includes only those network devices whose IPv4 address is located within that IP Reuse Domain (IRD). For details about enabling and configuring the Forescout platform's support of overlapping IP address use in an enterprise's network, refer to the *Forescout Working with Overlapping IP Addresses How-to Guide*. See [Additional Forescout Documentation](#) for information on how to access this document.

Requirements

This section describes the requirements for configuring and running the Forescout Reports Plugin.

Forescout Requirements

The following Forescout platform and component versions must be running in your Enterprise Manager and your Appliances:

- Forescout interim release 8.2.1
- Core Extensions Module 1.2.1 with the Reports Plugin

Web Browser Requirements

The Reports Plugin requires that web browsers, with which the plugin works, have the following options configured/enabled:

- JavaScript must be enabled on your browser

Supported Browsers

The Reports Plugin supports working with following web browsers:

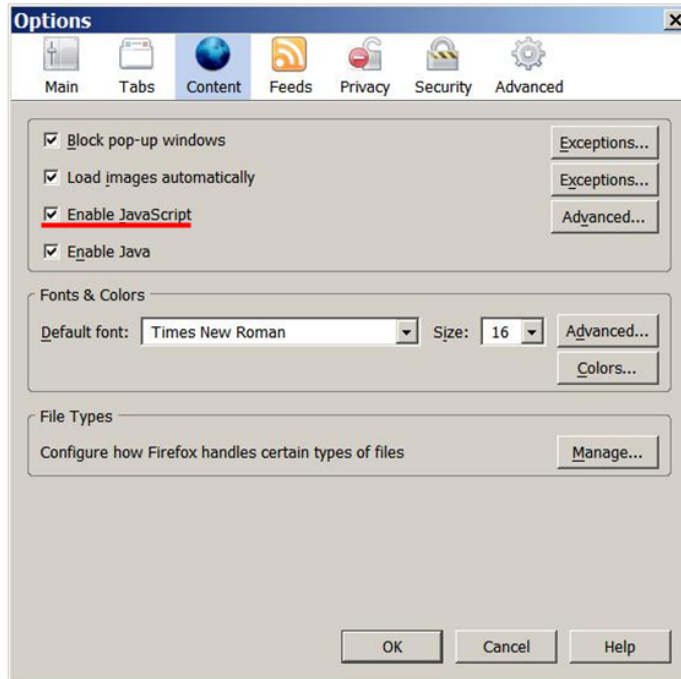
- Google Chrome 40 and higher
- Mozilla Firefox 4.0 and higher
- Microsoft Internet Explorer 9 and higher

To enable JavaScript for a Chrome browser:

1. In the extreme, upper-right of the browser tab, select the **Menu** icon (three vertical dots).
2. In the menu, select **Settings**.
3. In the page's list of topics, select **Privacy and security**.
4. In the *Privacy and security* pane, select **Site settings**.
5. In the *Site settings* pane, scroll to and select **JavaScript**.
6. In the *JavaScript* pane, enable **Allowed (recommended)**.

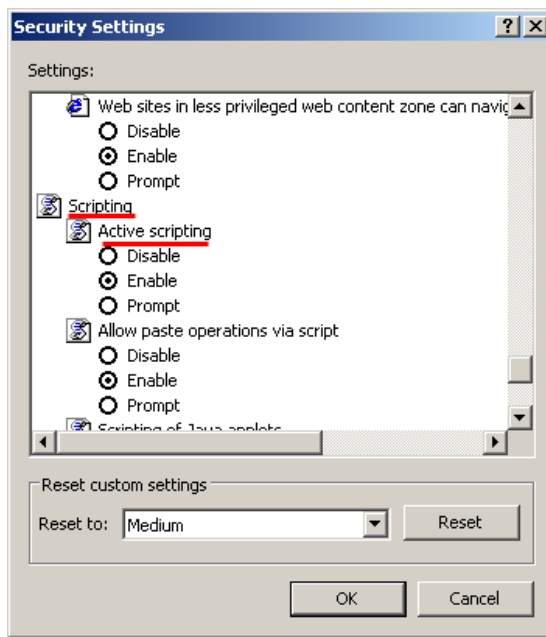
To enable JavaScript for a Firefox browser:

1. Select **Options** from the *Tools* menu and then select the **Content** tab.
2. Verify that **Enable JavaScript** is selected and then select **OK**.



To enable JavaScript for an Internet Explorer browser:

1. Select **Internet Options** from the *Tools* menu and then select the **Security** tab.
2. Select **Custom Level**.
3. Scroll down to *Scripting/Active Scripting*.
4. Verify that **Enable** is selected.



Verify That the Plugin Is Running

After configuring the plugin, verify that it is running.


To verify:

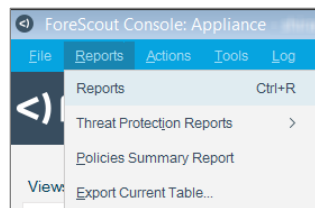
1. Select **Tools>Options** and then select **Modules**.
2. Navigate to the plugin and select **Start** if the plugin is not running.

Accessing the Reports Portal


You may be required to log in before you can access any of the Forescout web portals. If you have access to the Forescout Console, enter the same credentials you use to log in to the Console.

To access the Reports Portal:

1. To access the *Reports* portal from the Console, do one of the following:
 - Select the **More** icon  from the Console toolbar, and then select **Reports** from the dropdown menu.
 - Select **Reports** from the *Reports* menu on the Console.



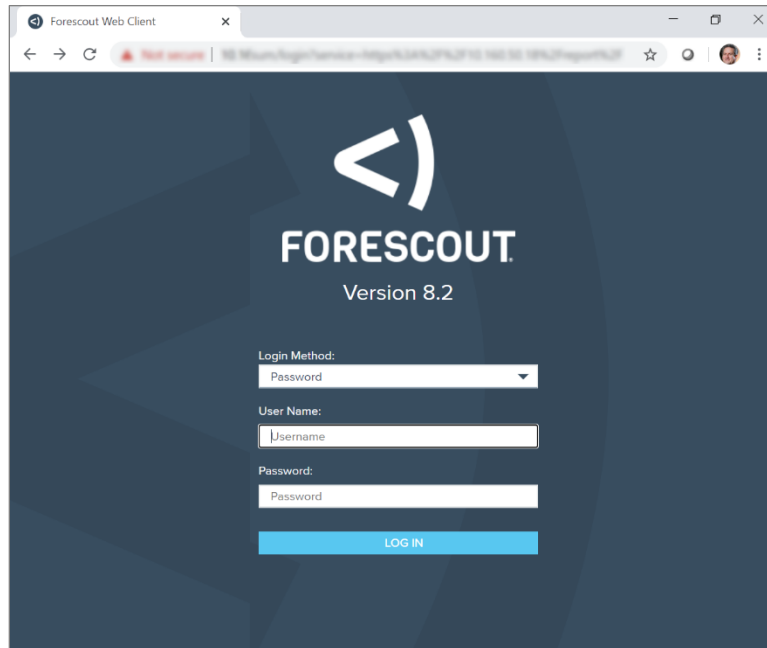
The web portal opens in a new browser window.

 *When you access the portal from the Console, you might not be prompted to log in.*

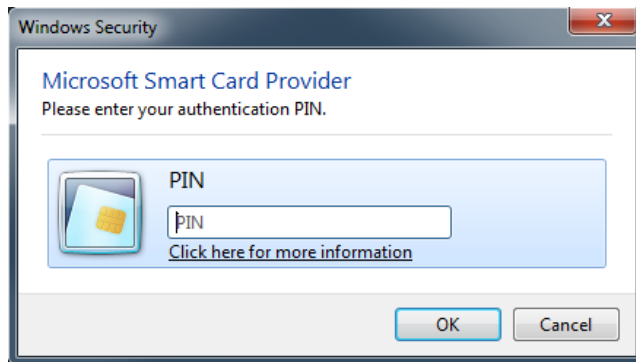
2. To log in to web portals from your web browser, enter the following URL:
http://<Device_IP>/report

Where <Device_IP> is the IP address of the Enterprise Manager or an Appliance.

If you are not already authenticated to Forescout web portals, the *Forescout Login* dialog box opens.



3. Select from the following login methods:
 - Select **Password** to perform standard authentication. Enter your user name and password.
If you have forgotten your password, contact your System Administrator or another user authorized to change your Forescout password.
 - Select **Smart Card** to allow authentication using a connected smart card. If the Smart Card contains more than one certificate, select the certificate for login to the Forescout web portals. Then enter your smart card PIN code, and select **OK**.

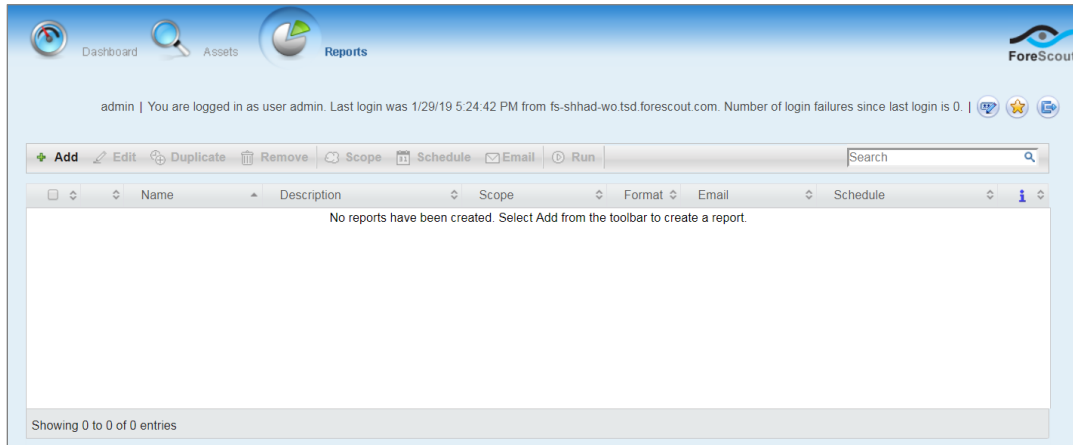


4. Select **Log In**.
5. A window may open displaying terms and conditions. To continue working, accept the terms. The login process continues.
6. If two-factor authentication is required, complete the Security Verification requirements and then select **Verify**.

Reports Home Page

The *Reports* home page opens, displaying the following login information:

- User name and IP address of your current login session
- Time and IP address of this user's last successful login
- Number of this user's recent login attempts that failed



If you think this information is incorrect, report it to your security officer.

Managing Reports

This section describes report management options, which can be applied to single reports or to several reports simultaneously. For example, run several reports together or simultaneously edit the report scope, schedule and email configurations.

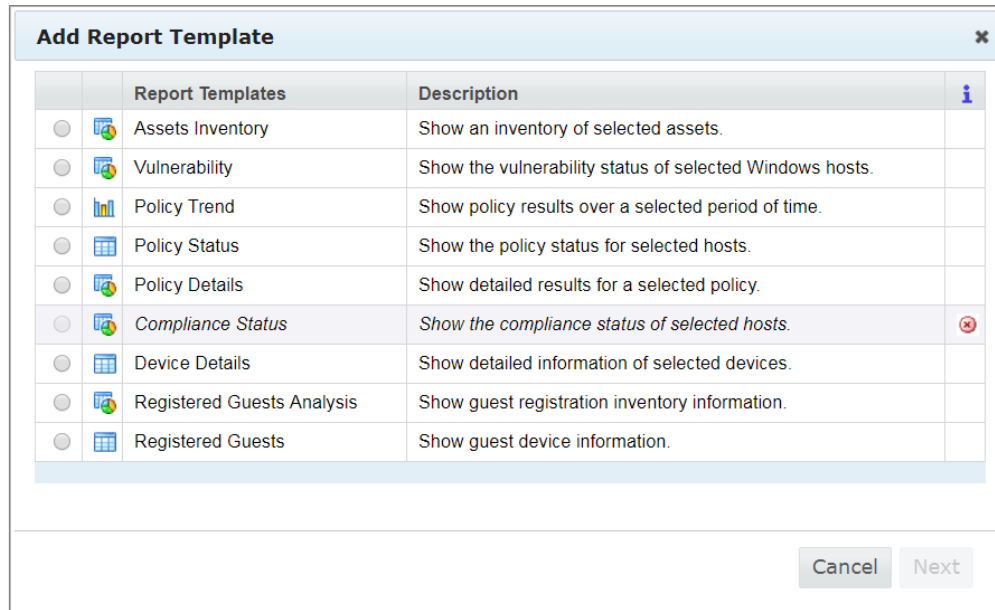
Saving Reports and Creating Report Schedules

In addition to generating reports for immediate review, you can save them for future use or create report schedules.

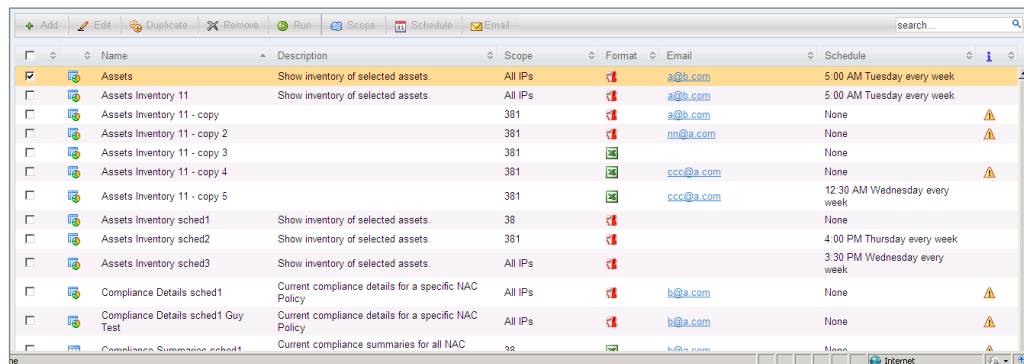
These reports appear on the Reports home page. Options are available to manage these reports, such as duplicate or edit single reports or several reports simultaneously.

To work with reports:

1. Select **Add** from the Reports Home page. The templates screen opens.

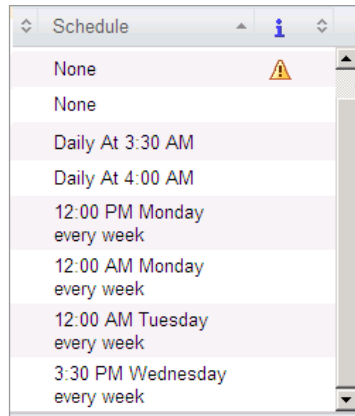


2. Select a report template and then select **Next** to begin generating a report.
3. Define report values.
4. Create a schedule if required, or select **None** in the Schedule section. See [Configure Date/Time Format for Report Output](#).
5. Select **Save**. Saved reports appear on the home page, showing basic settings, such as the format in which the report will be created.



Tracking Reports

You can easily track report schedules and reports settings such as email addresses by using the sort feature. In the example shown below, the Schedule column has been sorted to display scheduled reports in the order they will be delivered — starting with None, followed by Daily and then the days of the week.



Filter and Find

Use the search tool to filter the Reports home page to display reports that are of interest to you. For example, type in Assets to only display reports that include the name Asset, or display reports that were defined with a certain scope. In the example shown below, reports that were defined to include All IPs are displayed.

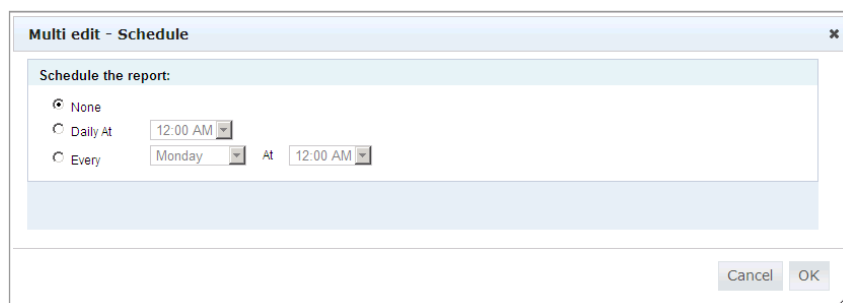
| | Name | Description | Scope | Format | Email | Schedule |
|-------------------------------------|------------------------------------|--|---------|--------|---------|------------------------------|
| <input checked="" type="checkbox"/> | Assets | Show inventory of selected assets. | All IPs | | a@b.com | Daily At 4:00 AM |
| <input checked="" type="checkbox"/> | Assets Inventory 11 | Show inventory of selected assets. | All IPs | | a@b.com | Daily At 3:30 AM |
| <input type="checkbox"/> | Assets Inventory sched3 | Show inventory of selected assets. | All IPs | | b@a.com | 3:30 PM Wednesday every week |
| <input type="checkbox"/> | Compliance Details sched1 | Current compliance details for a specific NAC Policy | All IPs | | b@a.com | None |
| <input type="checkbox"/> | Compliance Details sched1 Guy Test | Current compliance details for a specific NAC Policy | All IPs | | b@a.com | None |
| <input type="checkbox"/> | Compliance Trend sched1 | Compliance with a specific NAC Policy over time | All IPs | | | None |

Simultaneously Manage Multiple Reports

This section describes how to manage several reports simultaneously. For example, run or delete reports together, or simultaneously edit the report scope, schedule and email configurations.

To manage reports simultaneously:

1. Select the reports you want to manage.
2. Select **Scope**, **Run**, **Schedule** or **Email**. A Multi edit dialog box opens.



3. Update the values. These values are applied to all the reports you selected.

Additional Report Management Tools

- *To edit a saved report:* Select the report checkbox and then select **Edit**.
- *To delete a saved report:* Select the report checkbox, and then select **Remove**.
- *To duplicate a report:* Select the report checkbox, and then select **Duplicate**.
- *To run report:* Select the report checkbox, and then select **Run**.

Configure Date/Time Format for Report Output

Use this procedure to define the format of date and time information when reports are output to a file. For example, you can specify American or European date formats and choose a timestamp based on a 24 or 12 hour clock.

To define date and time format for report files:

1. Log in to the CounterACT device through the command-line interface (CLI) and run the following command:

```
fstool set_property msg.report.date.format.standart "<expression>"
```

Where *<expression>* is a legal formatting expression as described in the `java.text.SimpleDateFormat` class. For example, the following command generates the timestamp **12:08 PM**:

```
fstool set_property msg.report.date.format.standart "h:mm a"
```

All reports are generated using the specified date/time format.

Report Templates

The plugin provides the following report templates:

- [Assets Inventory](#)
- [Vulnerability](#)
- [Policy Trend](#)
- [Policy Status](#)
- [Policy Details](#)
- [Compliance Status](#)
- [Device Details](#)
- [Registered Guest Analysis](#)
- [Registered Guests](#)

Assets Inventory

Create a report that tracks network asset statistics. For example, installed applications, running processes and services, open ports, external devices, operating systems, and more.

Assets Inventory report information is based on Console Inventory detections. Refer to the ForeScout Help for information about working in the *Asset Inventory* view.

The screenshot shows the ForeScout Enterprise Manager Console interface. The top navigation bar includes 'File', 'Reports', 'Actions', 'Tools', 'Log', 'Display', and 'Help'. The main header shows 'ForeScout' and navigation links for 'Home', 'Asset Inventory', 'Policy', and a settings icon. The left sidebar contains a 'Views' section with a search bar and a tree view showing 'User Directory', 'Open Ports', 'Windows' (expanded), 'Windows Processes Running' (selected), 'Windows SecureConnector Version', 'Windows Services Running', and 'Windows Version'. Below this is a 'Filters' section with a search bar and a list of filters: 'All', 'Segments (77)', 'Organizational Units', 'Default Groups', and 'Groups'. The main content area is titled 'Windows Processes Running' and contains a table with columns: 'Windows Processes Running', 'No. of Hosts', 'Last Update', and 'Last Host'. The table lists several processes: 'tsprocsvc' (3 hosts), 'googletalk' (1 host), 'lgfxUIService' (1 host), 'lgfxEM' (1 host), 'lgfxHK' (1 host), 'lgfxTray' (1 host), 'jucheck' (1 host), and 'lusrched' (1 host). Below this table is a 'Hosts' section titled 'Windows Processes Running: tsprocsvc' showing '3 OF 79 HOSTS'. It contains a table with columns: 'Host', 'Host IP', 'Segment', 'MAC Address', and 'Function'. The hosts listed are 'COMBINGWIN' (IP: 10.36.2.84, Segment: Main 36 34, MAC: 8254100072ab, Function: Computer), 'COMBINGWINIPRO32-2' (IP: 10.36.2.81, Segment: 36, MAC: 000000000000, Function: Computer), and 'COMBINGWINIPRO64-1' (IP: 10.36.1.88, Segment: Main 36 34, MAC: 000000000000, Function: Unknown). The bottom status bar shows a green checkmark, a red X, a yellow warning, and the time '7/9/17 1:38:19 PM'.

To gain a comprehensive understanding of your network assets, you can display this information in a variety of formats, for example:

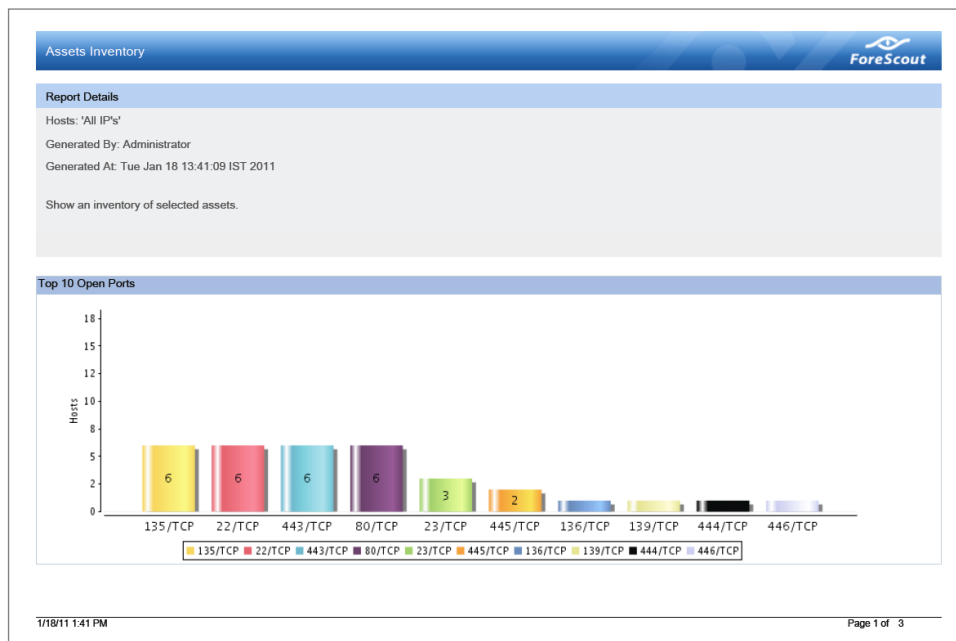
- Generate a table of applications installed on your network. The report includes the application name and version, as well as related information — such as the number of endpoints that have installed the application.

| Assets Inventory | | | | | |
|--|----------------|-------|--------------|---------------------|-----------|
| Report Details | | | | | |
| Hosts: 'All IPs' | | | | | |
| Generated By: Administrator | | | | | |
| Generated At: Mon Nov 22 12:38:47 IST 2010 | | | | | |
| Show inventory of selected assets. | | | | | |
| Name | Version | Lists | No. of Hosts | Last Update | Last Host |
| Java(TM) 6 Update 10 | 6.0.100 | | 1 | Mon Nov 22 12:00:01 | 10.36.1.1 |
| Directory Server | | | 1 | Mon Nov 22 12:00:01 | 10.36.1.1 |
| Microsoft Baseline Security Analyzer 2.1 | 2.1.0000 | | 1 | Mon Nov 22 12:00:01 | 10.36.1.1 |
| Windows Server 2003 Service Pack 1 Administration Tools Pack | 5.2.3790.1830 | | 1 | Mon Nov 22 12:00:01 | 10.36.1.1 |
| General Knowledge Base Server | | | 1 | Mon Nov 22 12:00:01 | 10.36.1.1 |
| RDC | | | 1 | Mon Nov 22 12:00:01 | 10.36.1.1 |
| WMGAPI | 1.0.0.0 | | 1 | Mon Nov 22 12:00:01 | 10.36.1.1 |
| MSXML 4.0 SP2 (KB927738) | 4.20.5941.0 | | 1 | Mon Nov 22 12:00:01 | 10.36.1.1 |
| XML Paper Specification Shared Components Pack 1.0 | | | 1 | Mon Nov 22 12:00:01 | 10.36.1.1 |
| Microsoft .NET Framework 2.0 Service Pack 1 | 2.1.12022 | | 1 | Mon Nov 22 12:00:01 | 10.36.1.1 |
| Microsoft Report Viewer | | | 1 | Mon Nov 22 12:00:01 | 10.36.1.1 |
| Redistributable 2006 | | | 1 | Mon Nov 22 12:00:01 | 10.36.1.1 |
| Windows Communication Foundation | 3.0.04056.30 | | 1 | Mon Nov 22 12:00:01 | 10.36.1.1 |
| Adobe Flash Player 9 ActiveX | 9.0.115.0 | | 1 | Mon Nov 22 12:00:01 | 10.36.1.1 |
| Windows Imaging Component | 3.0.0.0 | | 1 | Mon Nov 22 12:00:01 | 10.36.1.1 |
| Windows Presentation Foundation | 3.0.6820.0 | | 1 | Mon Nov 22 12:00:01 | 10.36.1.1 |
| Windows Internal Database (MICROSOFT#MSSEE) | 9.2.3042.00 | | 1 | Mon Nov 22 12:00:01 | 10.36.1.1 |
| Windows Internal Database | | | 1 | Mon Nov 22 12:00:01 | 10.36.1.1 |
| VMware Tools | 7.8.4.5078 | | 1 | Mon Nov 22 12:00:01 | 10.36.1.1 |
| Configuration Manager Client | 4.00.6221.1000 | | 1 | Mon Nov 22 12:00:01 | 10.36.1.1 |

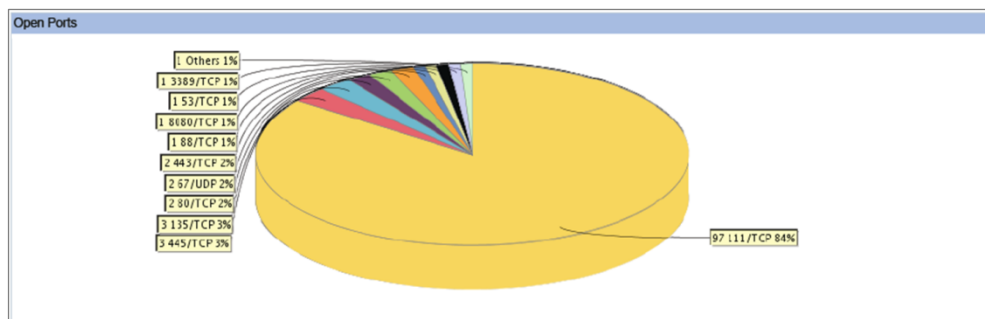
11/22/10 12:38 PM

Page 1 of 2

- Generate a bar chart displaying the top 10 open ports.



- Generate a pie chart displaying detections, in percentages.



















- Generate a report that includes host details for asset items detected. For example, if you choose to run a report on open ports in your organization you could include a table of all endpoints with each open port and could include specific host details.

| 111/TCP | | | |
|---------|----------------------|--------------|------------------|
| Segment | Network Function | MAC Address | NIC Vendor |
| 383 | Access point | 000103810131 | 3COM CORPORATION |
| 383 | Amazon Kindle | 000103810111 | 3COM CORPORATION |
| 383 | Apple Mac OS X | 000103810110 | 3COM CORPORATION |
| 383 | Apple Mac OS X | 000103810134 | 3COM CORPORATION |
| 383 | Apple Mac OS X | 000103810122 | 3COM CORPORATION |
| 383 | Apple Mac OS X | 000103810147 | 3COM CORPORATION |
| 383 | Apple Mac OS X | 000103810141 | 3COM CORPORATION |
| 383 | Apple Mac Server | 000103810117 | 3COM CORPORATION |
| 383 | CounterACT Appliance | 000103810133 | 3COM CORPORATION |
| 383 | CounterACT Appliance | 000103810121 | 3COM CORPORATION |
| 383 | CounterACT Appliance | 000103810109 | SYTEK INC. |
| 383 | FileServer | 000103810116 | 3COM CORPORATION |
| 383 | Gateway | 000103810139 | 3COM CORPORATION |
| 383 | IBM OS | 000103810115 | SYTEK INC. |
| 383 | IBM mvs | 000103810129 | 3COM CORPORATION |
| 383 | Linux Desktop/Server | 000103810102 | SYTEK INC. |
| 383 | Linux Desktop/Server | 000103810114 | 3COM CORPORATION |
| 383 | Linux Desktop/Server | 000103810118 | SYTEK INC. |
| 383 | Linux Desktop/Server | 000103810138 | 3COM CORPORATION |
| 383 | Linux Desktop/Server | 000103810132 | 3COM CORPORATION |
| 383 | Linux Desktop/Server | 000103810140 | 3COM CORPORATION |
| 383 | Linux Desktop/Server | 000103810120 | 3COM CORPORATION |
| 383 | Linux Desktop/Server | 000103810126 | 3COM CORPORATION |
| 383 | Linux Desktop/Server | 000103810154 | 3COM CORPORATION |
| 383 | Linux Desktop/Server | 000103810155 | 3COM CORPORATION |
| 383 | Linux Desktop/Server | 000103810150 | 3COM CORPORATION |
| 383 | Linux Desktop/Server | 000103810151 | 3COM CORPORATION |
| 383 | Linux Desktop/Server | 000103810162 | 3COM CORPORATION |
| 383 | Linux Desktop/Server | 000103810163 | 3COM CORPORATION |
| 383 | Linux Desktop/Server | 000103810158 | 3COM CORPORATION |
| 383 | Linux Desktop/Server | 000103810159 | 3COM CORPORATION |
| 383 | Linux Desktop/Server | 000103810146 | 3COM CORPORATION |

To create an Assets Inventory report:

- In the *Reports* home page, select **Add**. The **Add Report Template** dialog opens. Select **Assets Inventory** and select **Next**. The report parameters page opens.

| | |
|---|---|
| 1. Header | |
| Name: | Assets Inventory  |
| Description: | Show an inventory of selected assets.  |
| Report Footer: | |
| Generated by: | admin |
| 2. Scope | |
| IP ranges: | <input checked="" type="radio"/> All IP's <input type="radio"/> Segment   <input type="checkbox"/> Unknown IP addresses |
| Group By: | Users  |
| <input type="checkbox"/> Filter By: | |
| 3. Display | |
| Select charts: | <input checked="" type="checkbox"/>   |
| <input checked="" type="checkbox"/> Select inventory item column: | <div>Users </div> <div>Lists</div> <div>No. of Hosts</div> |
| |   |
| <input type="checkbox"/> Show host details: | |
| Select report format: | <input checked="" type="radio"/>    |
| 4. Schedule | |
| Schedule the report: | |
| <input checked="" type="radio"/> None <input type="radio"/> Daily At <input type="text" value="12:00 AM"/>  <input type="radio"/> Every <input type="text" value="Monday"/>  At <input type="text" value="12:00 AM"/>  | |
| Send Report to: <input type="text"/> | |

- In the **Header** section, enter a header name, a description and the name of the CounterACT user generating the report. This information appears at the top of the report. Enter optional footer text, which appears at the bottom of the report.

3. In the **Scope** section define the following:
 - In the **IP Ranges** section, select **All IPs** or specify segments for which to create the report. Select **Unknown IP addresses** to include endpoints at which a MAC address was detected, rather than an IP address. In the **Group by** section, select the inventory item for which to create the report, for example: Applications Installed, Windows Processes Running or Open Ports.
 - Select **Filter by** to define specific conditions under which results will be displayed:


☒ **Filter By:**

☐ Filter 'User' by

☐ Show 'User' if number of hosts is greater than

☐ Show 'User' if number of hosts is less than

☐ Show top hosts with 'User'




- > *Filter inventory item by:* Add specific text to search for. If the text is found, related items will be displayed. Regular expressions are allowed.

For example, filter all applications installed containing the string "windows". Entries are not case sensitive.
- > *Show inventory items if number of endpoints is greater than X:* Display results if more than a specific number of endpoints are detected with the inventory item.
- > *Show inventory items if number of endpoints is less than X:* Display results if less than a specific number of endpoints are detected.
- > For example, only display results of open ports if more than 200 endpoints, but less than 800 endpoints are detected with these open ports.
- > *Show top endpoints with inventory item.* Enter the maximum number of inventory items that should be displayed. The items displayed will be those which have the most host detections for the item. For example, if you select to show the top eight installed applications, the report will display the eight applications that are installed in the highest number of endpoints.





4. In the **Display** section, define the following:
 - In the **Select charts** section, indicate if you want to display the results as a bar chart or pie chart or both. The bar chart shows numbers of endpoints that match the item and the pie chart displays results in percentages.
 - In the **Select inventory item column** section select **Edit** to customize the display of default results in the report table.



☒ Select inventory item column:

User ▲ Lists No. of Hosts

 Edit >>

| No. | Name | Display | Sorted By | Items |
|-----|--------------|--------------|-----------|-------|
| 1 | User | User | Ascending | 1 |
| 2 | Lists | Lists | | 10 |
| 3 | No. of Hosts | No. of Hosts | | 1 |

 Add...
 Remove
 Up
 Down

- Use the **Display** option to select a label to use when displaying them. For example, choose to display open ports with the label **Open Ports/New York Branch**.
 - Use the **Sorted By** option to define the sort order of the display.
 - Use the **Items** option to indicate the maximum items to display. Limit this number if you anticipate there will be a significant number of detections and want to avoid cluttering the report.
 - Use **Up** and **Down** to change the order of the columns in the report. This is the order in which they appear from left to right.
 - **Add** and **Remove** are not available for this option.
 - Select **Show host details** to create a separate table with details about each host that was detected for the report. For example, if 50 endpoints were detected with a specific application installed, you can display an extensive range of host information regarding each host.
See [Working with Tables](#) for details.
 - Use **Up** and **Down** to change the order the columns appear in the report, (the order they appear from left to right).
 - Use **Add** and **Remove** to include and remove an extensive range of properties to display in the table report. See [Selecting Properties to Display](#) for details.
 - In the **Select report format** section, specify whether to create the report as a PDF or CSV file.
5. In the **Schedule** section, optionally create a report schedule.
- Define a schedule.
 - List an email address to send the report. You may enter multiple email addresses, separating them with commas. The report is saved in the “My Reports” table on the Reports page.
6. Take one of the following actions:
- Select **Run**, , to generate the defined report.
 - Select **Save**, , to save the defined report for later use.

Working with Tables

If you selected to show host details, host information will appear in a table. This information is linked to related information in the table that lists host details.

In the example shown below, selecting Open Port 111/TCP displays a table that lists all endpoints with port 111/TCP open and provides information about these endpoints.

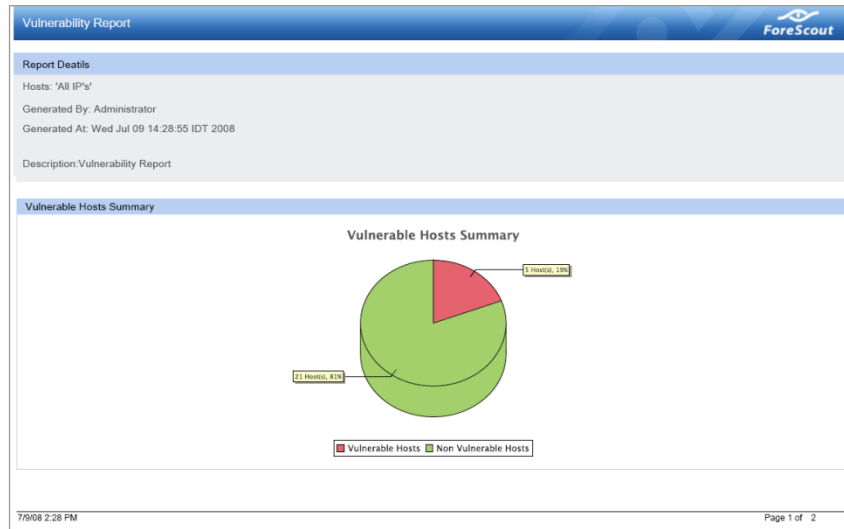
| Open Ports | Lists | No. of Hosts |
|------------|-------------|--------------|
| 21/TCP | list-manual | 1 |
| 23/TCP | | 1 |
| 53/TCP | | 1 |
| 67/UDP | | 2 |
| 80/TCP | | 2 |
| 88/TCP | list-manual | 1 |
| 111/TCP | | 16 |
| 135/TCP | | 2 |
| 139/TCP | | 1 |
| 161/UDP | | 1 |
| 445/TCP | list-manual | 3 |
| 3389/TCP | | 1 |
| 8080/TCP | | 1 |
| Total: 13 | | |

| 111/TCP | | | |
|---------|-----------------------|--------------|------------------|
| Segment | Network Function | MAC Address | NIC Vendor |
| 383 | Access point | 000103810131 | 3COM CORPORATION |
| 383 | Amazon Kindle | 000103810111 | 3COM CORPORATION |
| 383 | Apple Mac OS X | 000103810110 | 3COM CORPORATION |
| 383 | Apple Mac OS X | 000103810134 | 3COM CORPORATION |
| 383 | Apple Mac OS X | 000103810122 | 3COM CORPORATION |
| 383 | Apple Mac OS X | 000103810147 | 3COM CORPORATION |
| 383 | Apple Mac OS X | 000103810141 | 3COM CORPORATION |
| 383 | Apple Mac Server | 000103810117 | 3COM CORPORATION |
| 383 | CounterACT Appliance | 000103810133 | 3COM CORPORATION |
| 383 | CounterACT Appliance | 000103810121 | 3COM CORPORATION |
| 383 | CounterACT Appliance | 000010381019 | SYTEK INC. |
| 383 | FileServer | 000103810116 | 3COM CORPORATION |
| 383 | Gateway | 000103810139 | 3COM CORPORATION |
| 383 | IBM OS | 000010381016 | SYTEK INC. |
| 383 | Item mvs | 000103810129 | 3COM CORPORATION |
| 383 | Linux: Desktop/Server | 000010381012 | SYTEK INC. |

Vulnerability


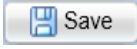
Use this report to see the vulnerability status of selected Windows endpoints. A pie chart shows the number and percentage of endpoints with vulnerabilities versus those that have no vulnerabilities. A report lists the relevant endpoints. You can show the vulnerabilities of each host by selecting **Vulnerabilities** in the Select table columns section. The report is generated as a PDF file.

Before generating the report, you need to have a Microsoft Vulnerabilities policy running with the scope and vulnerabilities that interest you. If an Appliance is down, the endpoints managed by that Appliance are not included in the report.



To create a Vulnerability report:

1. Define a Microsoft Vulnerabilities policy:
 - Set up a policy with the scope you are interested in.
 - Add the **Windows Security > Microsoft Vulnerabilities** property to the policy. Within that property, select all the vulnerabilities that interest you.
 - Run the policy.
2. In the *Reports* home page, select **Add**. The **Add Report Template** dialog opens. Select **Vulnerability** and select **Next**. The report parameters page opens.
3. In the **Header** section, enter a header name, a description and the name of the CounterACT user generating the report. This information appears at the top of the report. Enter optional footer text, which appears at the bottom of the report.
4. In the **Scope** section, select **All IPs** or specify segments for which to create the report. Select **Unknown IP addresses** to include endpoints at which a MAC address was detected, rather than an IP address.
5. In the **Display** section, define display requirements.
 - Select the titles and descriptions to appear in the pie chart.
 - Select the vulnerable and non-vulnerable descriptions.
 - Select **Edit** to add, remove and/or reorganize properties that are displayed as table column headers to appear in the report, including the default headers. You may select up to 21 properties. See [Selecting Properties to Display](#) for more information. Select **OK** when done.
 - Select whether you want the report to show a summary of vulnerabilities next to each host.
 - Select whether or not you want the report to include endpoints with/without vulnerabilities.
6. In the **Schedule** section, optionally create a report schedule.
 - Define a schedule.

- List an email address to send the report. You may enter multiple email addresses, separating them with commas. The report is saved in the “My Reports” table on the Reports page.
7. Take either of the following actions:
- Select **Run**, , to generate the defined report.
 - Select **Save**, , to save the defined report for later use.

Policy Trend


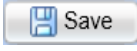

Use this report to display a graph indicating policy results over a defined period.

If you run a report for a single policy only, the report displays matched, unmatched and irresolvable endpoints. If you run a report that includes sub-policies, the results will include endpoints with matched sub-policies as well as endpoints that were unmatched or irresolvable for the parent policy. For example, show guest connection trends in your enterprise for all Windows machines.

Show all windows machines (parent policy which classifies machines) to learn how many machines are guests (sub-policy) and how many machines are corporate (sub-policy).

To create a Policy Trend report:

1. In the *Reports* home page, select **Add**. The **Add Report Template** dialog opens. Select **Policy Trend** and select **Next**. The report parameters page opens.
2. In the **Header** section, enter a header name, a description and the name of the CounterACT user generating the report. This information appears at the top of the report. Enter optional footer text, which appears at the bottom of the report.
3. In the **Scope** section:
 - Select **All IPs** or specify segments for which to create the report. Select **Unknown IP addresses** to include endpoints at which a MAC address was detected, rather than an IP address.
 - Select a policy and then adjust the policy status labels and colors presented in the report, if required, by selecting **Edit policy labels....** For example, instead of indicating that endpoints *Match* a policy you can use the term *Not compliant*, and assign a color to color-code the status results. This provides additional report customization and easier reading.
4. In the **Display** section, define display requirements.
 - Select the time period to display the results
 - Select the units in which to display the time. For example, show the trend over a month and display daily results.
5. In the **Schedule** section, optionally create a report schedule.
 - Define a schedule.

- List an email address to send the report. You may enter multiple email addresses, separating them with commas. The report is saved in the “My Reports” table on the Reports page.
6. Take either of the following actions:
- Select **Run**, , to generate the defined report.
 - Select **Save**, , to save the defined report for later use.
-  *Generating a trend report can take up to a few hours, since the historical data is retrieved from every appliance and not only from the Enterprise Manager.*

Policy Status

Use this report to display the number of matched, unmatched and irresolvable endpoints detected for each policy and sub-policy.

| Policy Compliance Summaries2 ForeScout | | | |
|---|-------|---------|--------------|
| Report Details | | | |
| Hosts: All IP's | | | |
| Generated By: Administrator | | | |
| Generated At: Wed Mar 25 10:09:17 IST 2009 | | | |
| Compliance summaries for all NAC Policies | | | |
| Policy Name | Match | Unmatch | Irresolvable |
| Policy Folders | | | |
| Asset Classification | 36 | 0 | 0 |
| NAT devices | 0 | 36 | 0 |
| Windows | 0 | 0 | 36 |
| Printers | 0 | 0 | 0 |
| Linux/Unix | 0 | 0 | 0 |
| Macintosh | 0 | 0 | 0 |
| Voice devices | 0 | 0 | 0 |
| Network devices | 0 | 0 | 0 |
| Unclassified | 0 | 0 | 0 |
| MAC/Windows/Linux | 0 | 0 | 36 |
| USB Device Compliance | 0 | 36 | 0 |
| SecureConnector not running | 0 | 0 | 0 |
| Allowed USB devices | 0 | 0 | 0 |
| Other USB devices | 0 | 0 | 0 |
| | - | - | - |


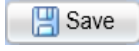
To create a Policy Status report:

1. In the *Reports* home page, select **Add**. The **Add Report Template** dialog opens. Select **Policy Status** and select **Next**. The report parameters page opens.

In the **Header** section, enter a header name, a description and the name of the CounterACT user generating the report. This information appears at the top of the report. Enter optional footer text, which appears at the bottom of the report.
2. In the **Scope** section:
 - Select **All IPs** or specify segments for which to create the report. Select **Unknown IP addresses** to include endpoints at which a MAC address was detected, rather than an IP address.
 - Select all policies or choose specific policy folders. You can choose to include or exclude policies that have been stopped. If policies are stopped,

results will be displayed as 0. Stopped policies appear as follows on this page:



3. In the **Display** section, define display requirements.
 - Review the policy status labels presented in the report and change them, if needed, by typing in new labels. For example, instead of indicating that endpoints *Match* a policy, you can use the term *Not compliant*. (Optional)
 - Choose to either create the report as a PDF or CSV file.
4. In the **Schedule** section, optionally create a report schedule.
 - Define a schedule.
 - List an email address to send the report. You may enter multiple email addresses, separating them with commas. The report is saved in the “My Reports” table on the Reports page.
5. Take either of the following actions:
 - Select **Run**, , to generate the defined report.
 - Select **Save**, , to save the defined report for later use.

Policy Details

Use this report to display policy details for endpoints detected by a specific policy.

For example, create an Primary Classification policy and then run a report to show how many Windows, Linux, NAT machines or printers are installed in your organization.

The report summarizes results in a pie chart and also provides details, for example, the IP address, DNS name and NetBIOS name of each Windows, Linux, NAT machine and printer.

To create a Policy Details report:

1. In the *Reports* home page, select **Add**. The **Add Report Template** dialog opens. Select **Policy Details** and select **Next**. The report parameters page opens.

In the **Header** section, enter a header name, a description and the name of the CounterACT user generating the report. This information appears at the top of the report. Enter optional footer text, which appears at the bottom of the report.

2. In the **Scope** section:
 - Select **All IPs** or specify segments for which to create the report. Select **Unknown IP addresses** to include endpoints at which a MAC address was detected, rather than an IP address.
 - Select a policy and then adjust the policy status labels and colors presented in the report, if required, by selecting **Edit policy labels**

For example, instead of indicating that endpoints match a policy you can use the term *Not compliant*, and assign a color to color-code the status results. This provides additional report customization and easier reading.

3. In the **Display** section, define display requirements.
 - A pie chart is included in the report. User the **Select pie chart title** section to customize the name displayed in the chart.
 - Select the table columns that will be used in the report for each host defined in the **Scope** section. Select **Edit** to add, remove and/or reorganize properties that will be displayed as table column headers in the report, including the default headers, for example, the Host name DNS name and LDAP display name.

You may select up to 21 properties. See [Selecting Properties to Display](#) for more information. Select **OK** when done.



- Select a report format, either PDF or CSV file.

4. In the **Schedule** section, optionally create a report schedule.

- Define a schedule.
- List an email address to send the report.

You may enter multiple email addresses, separating them with commas. The report is saved in the “My Reports” table on the Reports page.


5. Take either of the following actions:

- Select **Run**, , to generate the defined report.
- Select **Save**, , to save the defined report for later use.

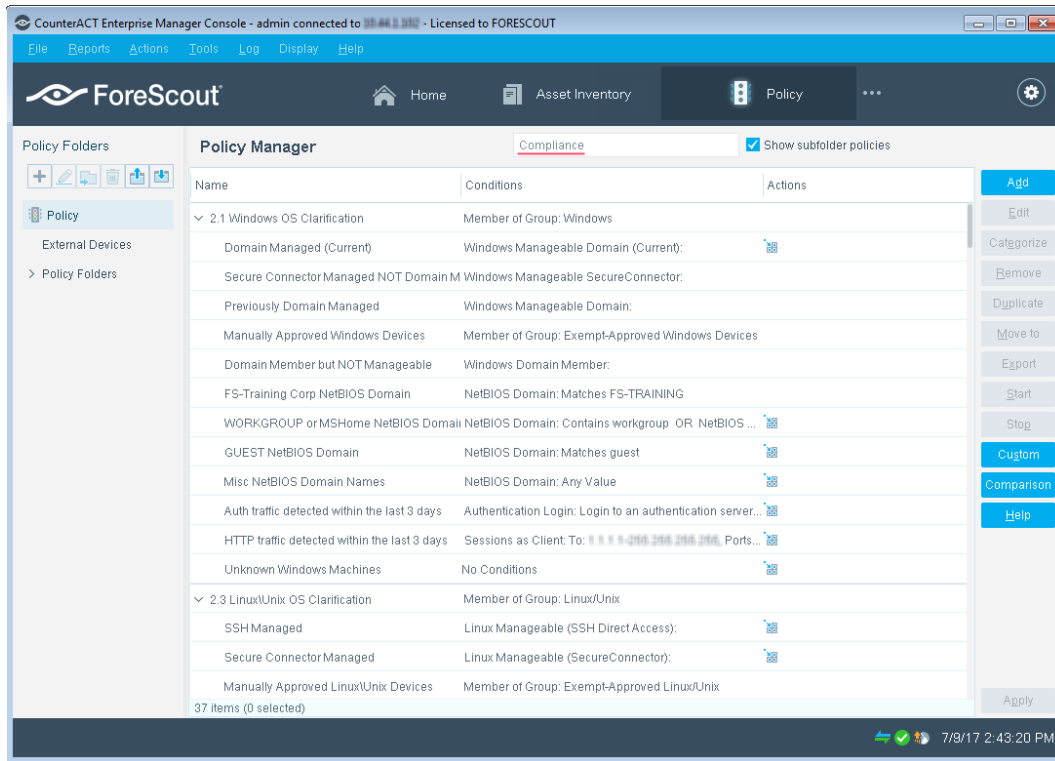
Compliance Status

Use this report to display information regarding the compliance status of endpoints in the network, including:

- A pie chart that displayed the overall distribution of compliant and non-compliant endpoints.
- A bar chart that displays the number of non-complaint endpoints for each compliance policy. This information lets you quickly pinpoint compliance issues in your organization.
- Tables listing compliant and non-compliant host details, such as MAC and IP addresses, Domain and NetBIOS names, connected switch and User Directory information.

 *To run this report at least one Compliance policy must be defined in your system.*

Endpoints displayed in this report were detected in policies categorized as *Compliance* policies in the Policy Manager. If a host is inspected by several compliance policies and is not compliant in one, the host is not compliant.




To create a Compliance Status report:

1. In the *Reports* home page, select **Add**. The **Add Report Template** dialog opens. Select **Compliance Status** and select **Next**. The report parameters page opens.

In the **Header** section, enter a header name, a description and the name of the CounterACT user generating the report. This information appears at the top of the report. Enter optional footer text, which appears at the bottom of the report.

2. In the **Scope** section:

- In the IP ranges section, select **All IPs** or specify segments for which to create the report. Select **Unknown IP addresses** to include endpoints for which a MAC address was detected, rather than an IP address.
- In the Compliance Policies section, the **All Compliance Policies** option is selected by default. Use this default setting to create a report based on all Compliance Policies.

To create a report based on a subset of policies or policy rules, clear the **All Compliance Policies** checkbox and select specific policies and sub-rules, using the  buttons.

- (Optional) Define display labels for policies or sub-rules included in the report. For example, change the *AV Not Installed* and *AV Not Running* sub-rule to *Symantec Not installed* and *Symantec Not running*, if this is the AntiVirus application that is monitored.

3. In the **Display** section:

- Define the following display options:



| | |
|---|---|
| Select pie chart title | The text displayed as the title of the pie chart |
| Select Compliant label | The text label that indicates compliant endpoints in the bar chart and the table. |
| Select Not Compliant label | The text label that indicates non-compliant endpoints in the bar chart and the table. |
| Select Not Compliant bar chart title | The text label that indicates non-compliant endpoints in the bar chart. |

- Select the table columns that will be displayed in the report. Select **Edit** to add, remove and/or reorganize properties that will be displayed as table column headers in the report, including the default headers, for example, the Host name DNS name and LDAP display name. You may select up to 21 properties. See [Selecting Properties to Display](#) for more information. Select **OK** when done.
- Select a report format, either PDF or CSV file.

4. (Optional) In the **Schedule** section, create a report generation schedule.

- Define a schedule.
- List an email address to which the report is sent. You may enter multiple email addresses, separating them with commas. The report is saved in the “My Reports” table on the NAC Reports page.

5. Do one of the following:


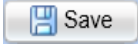
- Select **Run**  to generate the defined report.
- Select **Save**  to save the defined report for later use.

Device Details

Use this report to display information about network devices. For example, list the MAC address, related switch information or LDAP information available for selected endpoints.

To create a Device Details Report:

1. In the *Reports* home page, select **Add**. The **Add Report Template** dialog opens. Select **Device Details** and select **Next**. The report parameters page opens.
2. In the **Header** section, enter a header name, a description and the name of the CounterACT user generating the report. This information appears at the top of the report. Enter optional footer text, which appears at the bottom of the report.
3. In the **Scope** section, select **All IPs** or specify segments for which to create the report. Select **Unknown IP addresses** to include endpoints at which a MAC address was detected, rather than an IP address.

4. In the **Display** section, define display requirements.
 - Select host proprieties you want to display for each host defined in the *Scope*. Select **Edit** to add, remove and/or reorganize properties that will be displayed as table column headers in the report, including the default headers. For example, show the IP and MAC addresses and LDAP information for the endpoints defined in the scope. You may select up to 21 properties. See [Selecting Properties to Display](#) for more information. Select **OK** when done.
 - Choose to either create the report as a PDF or CSV file.
5. In the **Schedule** section, optionally create a report schedule.
 - Define a schedule.
 - List an email address to send the report. You may enter multiple email addresses, separating them with commas. The report is saved in the “My Reports” table on the Reports page.
6. Take either of the following actions:
 - Select **Run**, , to generate the defined report.
 - Select **Save**, , to save the defined report for later use.

Registered Guest Analysis

Create a report that tracks important information about guests that have registered for network access, including:

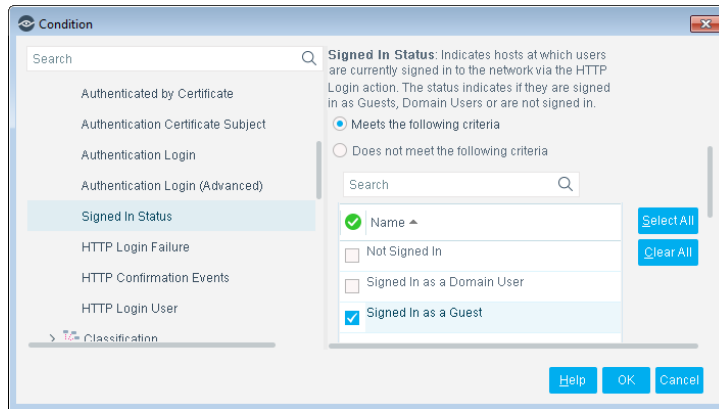
- The approval status of the guest that is registering.
- The names of corporate individuals that approved guests.
- The full names of guests registering for network access.
- The names of the companies that the registering guests are associated with.
- The names of contact persons that the registering guests are associated with.

The *full names, companies and contact persons* information is extracted from the Guest Registration web page. Refer to the Forescout Administration Guide for more information about this feature. See [Additional Forescout Documentation](#) for information on how to access the guide.

Requirements

- Authentication Module version 1.2.1 with User Directory Plugin running.
- Verify that you are working with a policy to handle network guests, for example, that you have run the **Corporate/Guest Template**. Refer to the Forescout Administration Guide for details. See [Additional Forescout Documentation](#) for information on how to access the guide.
- Verify that you are working with Forescout version 8.2.x.

The report investigates guests that have been resolved as *signed in* guests.



To create a Registered Guest Analysis report:

1. In the *Reports* home page, select **Add**. The **Add Report Template** dialog opens. Select **Registered Guest Analysis** and select **Next**. The report parameters page opens.
2. In the **Header** section, enter a header name, a description and the name of the CounterACT user generating the report. This information appears at the top of the report. Enter optional footer text, which appears at the bottom of the report.
3. In the **Scope** section define the following:
 - In the **IP Ranges** section, select **All IPs** or specify segments for which to create the report. Select **Unknown IP addresses** to include endpoints at which a MAC address was detected, rather than an IP address.
 - In the **Group By** section, select the guest registration item of interest: The report will be generated for this item.
 - › *Approved By* – the names of corporate individuals that approved guests.
 - › *Companies* – the names of the companies that the guest is associated with. This information was inserted in the Guest Registration page **Company** field when the guest registered with the network.
 - › *Contact Persons* – the names of contact people entered in the Guest Registration page **Contact Person** field when the guest registered with the network.
 - › *Guest Registration Status* – The approval status of the guest that is registering. The following results may appear in the report: *Approved*, *Declined Waiting for Approval*, or *Approved Automatically*.
 - › *Full Name* – The name entered by the guest in the **Full Name** field of the Guest Registration web page.

- Select **Filter By** to define specific conditions under which results will be displayed:

| | | |
|-------------------------------------|---|----------------------------------|
| <input checked="" type="checkbox"/> | Filter 'Guest Approved By' by | <input type="text" value="Sam"/> |
| <input type="checkbox"/> | Show 'Guest Approved By' if number of hosts is greater than | <input type="text"/> |
| <input type="checkbox"/> | Show 'Guest Approved By' if number of hosts is less than | <input type="text"/> |
| <input checked="" type="checkbox"/> | Show top hosts with 'Guest Approved By' | <input type="text" value="8"/> |

- › *Filter item by:* Add specific text to search for. If the text is found, related items will be displayed. Regular expressions are allowed. For example, if you have selected to create an *Approved By* report, you can filter the approved by item using *sam*, and all approvers with the characters *sam* will appear in the report. Entries are not case sensitive.
 - › *Show results if the number of endpoints is greater than X:* Display results if more than a specific number of endpoints are detected with the inventory item.
 - › *Show results if the number of endpoints is less than X:* Display results if less than a specific number of endpoints are detected.
 - › For example, only display results of approvers if more than 200, but less than 300 are detected.
 - › *Show top endpoints with inventory item.* Enter the maximum number of Inventory Items that should be displayed. The items displayed will be those which have the most host detections for the item. For example, if you select to show the top eight approvers, the report will display the eight approvers that are named in the most number of endpoints.

4. In the **Display** section, define the following:

- In the **Select charts** section, indicate if you want to display the results as a bar chart or pie chart or both. The bar chart shows the top ten endpoints that match the item and the pie chart displays the top ten results in percentages.
- In the **Select guest item column** section, select **Edit** to customize the display of default results in the report table.

| No. | Name | Display | Sorted By | Items |
|-----|----------------|---|--|---------------------------------|
| 1 | Guest. Company | <input type="text" value="Guest. Company"/> | <input checked="" type="radio"/> Ascending | <input type="text" value="1"/> |
| 2 | Lists | <input type="text" value="Lists"/> | <input type="radio"/> | <input type="text" value="10"/> |
| 3 | No. of Hosts | <input type="text" value="No. of Hosts"/> | <input type="radio"/> | <input type="text" value="1"/> |


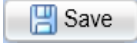
- › Use the **Display** option to select a label to use when displaying them. For example, choose to display **No. of Endpoints** with the label **Guests/New York Branch**.

- › Use the **Sort By** option to define the sort order of the display.
 - › Use the **Item** option to indicate the maximum items to display. Limit this number if you anticipate there will be a significant number of detections and want to avoid cluttering the report.
 - › Use **Up** and **Down** to change the order of the columns in the report. This is the order in which they appear from left to right.
 - › **Add** and **Remove** are disabled for this report.
- Select **Show host details** to create a separate table with details about each host that was detected for the report. For example, if 50 endpoints were detected with a specific approver, you can display an extensive range of host information regarding each host.

☒ Show host details:

| IP Address | NetBIOS Hostname | Guest Approved By | Guest Registration Status | Guest Tags | Guest: Comment | Guest: Company | Guest: Contact Person | Guest: Full Name | Guest: Location | Guest: Title |
|------------|------------------|-------------------|---------------------------|------------|----------------|----------------|-----------------------|------------------|-----------------|--------------|
|------------|------------------|-------------------|---------------------------|------------|----------------|----------------|-----------------------|------------------|-----------------|--------------|

 Edit >>

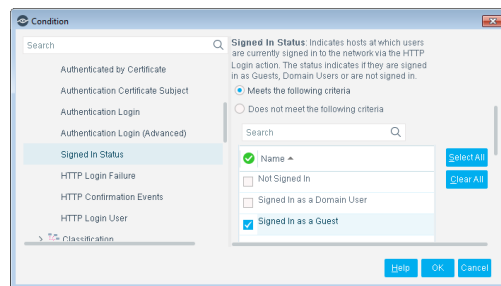
- › If you selected to show host details, host information will appear in a table. This information is linked to related information in the table that lists host details.
 - › Use **Up** and **Down** to change the order the columns appear in the report, (the order they appear from left to right).
 - › **Add** and **Remove** are disabled for this report.
 - In the **Select report format** section, specify whether to create the report as a PDF or CSV file.
5. In the **Schedule** section, optionally create a report schedule.
- Define a schedule.
 - List an email address to send the report. You may enter multiple email addresses, separating them with commas. The report is saved in the **My Reports** table on the Reports page.
6. Take either of the following actions:
- Select **Run**, , to generate the defined report.
 - Select **Save**, , to save the defined report for later use.

Registered Guests

Use this report to display information about devices used by network guests. For example, list the MAC address, related switch information or LDAP information available for selected endpoints.



| Registered Guests | | | | | |
|--|------------------|---------------------|------------|-------------------------|--|
| Report Details | | | | | |
| Hosts: 'All IPs' | | | | | |
| Generated By: Administrator | | | | | |
| Generated At: Tue Jan 11 13:51:01 IST 2011 | | | | | |
| Show guest device information. | | | | | |
| MAC Address | NetBIOS Hostname | Display Name | NIC Vendor | Network Function | Open Ports |
| 001430c0d0e | MALTA_LAP | ad_displayname-mays | INTEL | Windows Machine | |
| 0ae334c9d9d | T33DU | ad_displayname-i | INTEL | Windows Machine | 23/TCP |
| | RE | | INTEL | Windows Machine | |
| 001e1a03b107 | XP | ad_displayname-han | INTEL | Windows Machine | |
| | DANNY-LR | ad_displayname-dary | INTEL | Windows Machine | |
| 001275a4284e | SHAI | ad_displayname-sha | IBM | Printer | |
| 0465e0e01a2c | GELR | | AXIOM | Linux Desktop/Server | |
| 0059c0c0dec | YOTAMR | ad_displayname-yot | AXIOM | Linux Desktop/Server | |
| 01e064c03324 | ITAHIR | ad_displayname-i | NETRONIX | Apple Mac OS X | 23/TCP, 22/TCP, 81/TCP, 80/TCP, 443/TCP, 135/TCP, 445/TCP, 136/TCP, 22/TCP, 444/TCP, 80/TCP, 445/TCP, 443/TCP, 135/TCP, 445/TCP, 136/TCP(more) |
| | NOAM | ad_displayname-noa | NETRONIX | Linux Desktop/Server | 23/TCP, 22/TCP, 80/TCP, 443/TCP, 135/TCP, 445/TCP, 136/TCP |
| 0204ea65563c | POLY | | INTEL | Unix Server/Workstation | |
| 0124ea65563c | TIM | | INTEL | Windows Machine | 23/TCP, 80/TCP, 445/TCP, 135/TCP, 443/TCP |
| 01a4ea655644 | ROY | | INTEL | Windows Machine | 23/TCP, 80/TCP, 445/TCP, 135/TCP, 443/TCP |
| 01a4ea655677 | LI | | INTEL | Linux Desktop/Server | |
| Total: 14 | | | | | |

The report investigates guests that have been resolved as *signed in* guests.



To create a Registered Guests report:

1. In the **Reports** home page, select **Add**. The **Add Report Template** dialog opens. Select **Registered Guests** and then select **Next**. The report parameters page opens.
2. In the **Header** section, enter a header name, a description and the name of the CounterACT user generating the report. This information appears at the top of the report. Enter optional footer text, which appears at the bottom of the report.
3. In the **Scope** section, select **All IPs** or specify segments for which to create the report. Select **Unknown IP addresses** to include endpoints at which a MAC address was detected, rather than an IP address.
4. In the **Display** section, define display requirements.
 - In the **Select table columns** section: Select host properties you want to display. Select **Edit** to add, remove and/or reorganize properties that will be displayed as table column headers in the report, including the default headers. For example, show the IP and MAC addresses and LDAP information for the endpoints defined in the scope. You may select up to 21 properties. See [Selecting Properties to Display](#) for more information. Select **OK** when done.
 - In the **Select Report Format** section: Choose to either create the report as a PDF or CSV file.
5. In the **Schedule** section, optionally create a report schedule.
 - Define a schedule.

- List an email address to send the report. You may enter multiple email addresses, separating them with commas. The report is saved in the “My Reports” table on the Reports page.
6. Take either of the following actions:
- Select **Run**, , to generate the defined report.
 - Select **Save**, , to save the defined report for later use.

Selecting Properties to Display

The Vulnerability, Policy Compliance Details and Device Details, Assets Inventory and Guest Registration Reports let you choose an extensive range of properties to display in the report output. For example, the details related to device information events, switch information and more.

Several tools are available to help you choose and customize properties you want to display.

For example, you can:

- Change the display name of the property header (e.g., IP Address to Machine Address)
- Change the order in which the information is displayed (e.g., first show device information then show OS information)
- Add additional properties – up to 21.

To choose and manage properties that you display in the table columns:

1. Select **a policy**.
2. In the Display section, select **Show host details**. The default properties that will be displayed in the table columns.

| Show host details | | | | | | | | | | |
|---|------------------|-------------------|---------------------------|------------|----------------|----------------|-----------------------|------------------|-----------------|--------------|
| IP Address | NetBIOS Hostname | Guest Approved By | Guest Registration Status | Guest Tags | Guest: Comment | Guest: Company | Guest: Contact Person | Guest: Full Name | Guest: Location | Guest: Title |
|  Edit >> | | | | | | | | | | |

3. Select **Edit**. The window is expanded.
4. Select **Add**. A complete list of properties is displayed. You may include a total of 18 to 21 properties, depending on the report. If you have installed third party plugins, related properties are also available.

| Select table columns | | | |
|--|---|---|---|
| General Properties | | | |
| <input type="checkbox"/> Lists | <input type="checkbox"/> No. of Hosts | <input type="checkbox"/> User | <input type="checkbox"/> Company |
| <input type="checkbox"/> Department | <input type="checkbox"/> Open Ports | <input type="checkbox"/> Windows Processes Running | <input type="checkbox"/> Windows Services Running |
| <input type="checkbox"/> Macintosh Processes Running | <input type="checkbox"/> Macintosh Software Updates Missing | <input type="checkbox"/> Macintosh User | <input type="checkbox"/> Macintosh Version |
| <input type="checkbox"/> Linux Processes Running | <input type="checkbox"/> Linux User | <input type="checkbox"/> Linux Version | <input type="checkbox"/> Name |
| <input type="checkbox"/> Version | <input type="checkbox"/> Name | <input type="checkbox"/> Class | <input type="checkbox"/> Bus type |
| <input type="checkbox"/> Microsoft Vulnerabilities | <input type="checkbox"/> Network Function | <input type="checkbox"/> Switch IP | <input type="checkbox"/> Windows Version |
| User Directory | | | |
| <input type="checkbox"/> Account is Disabled | <input type="checkbox"/> Account is Expired | <input type="checkbox"/> Company | <input type="checkbox"/> Department |
| <input type="checkbox"/> Display Name | <input type="checkbox"/> Distinguished Name | <input type="checkbox"/> Email | <input type="checkbox"/> Employee Number |
| <input type="checkbox"/> Initials | <input type="checkbox"/> LDAP User Name | <input type="checkbox"/> Last Name | <input type="checkbox"/> Member Of |
| <input type="checkbox"/> Mobile Phone | <input type="checkbox"/> Phone | <input type="checkbox"/> Street Address | <input type="checkbox"/> Title |
| <input type="checkbox"/> User given Name | | | |
| Classification (Advanced) | | | |
| <input type="checkbox"/> Banner 139/TCP (Client) | <input type="checkbox"/> Banner 139/TCP (Server) | <input type="checkbox"/> Banner 445/TCP (Client) | <input type="checkbox"/> Banner 445/TCP (Server) |
| <input type="checkbox"/> Banner 80/TCP (Server) | <input type="checkbox"/> Classification Method | <input type="checkbox"/> Compare Network Function To (Classification Version 2) | <input type="checkbox"/> Compare OS Fingerprint To (Classification Version 2) |
| <input type="checkbox"/> HTTP User Agent | <input type="checkbox"/> HTTP User Agent (obsolete) | <input type="checkbox"/> Nmap-Banner (Ver. 4) | <input type="checkbox"/> Nmap-Banner (Ver. 5.3) |
| <input type="checkbox"/> OS 139/TCP (Client) | <input type="checkbox"/> OS 139/TCP (Server) | <input type="checkbox"/> OS 445/TCP (Client) | <input type="checkbox"/> OS 445/TCP (Server) |
| <input type="checkbox"/> OS 80/TCP (Client) | <input type="checkbox"/> OS 80/TCP (Server) | <input type="checkbox"/> OS(Engine) | <input type="checkbox"/> TCP/IP Syn Ack Fingerprint |
| <input type="checkbox"/> TCP/IP Syn Ack Fingerprint(Raw) | <input type="checkbox"/> TCP/IP Syn Fingerprint | <input type="checkbox"/> TCP/IP Syn Fingerprint(Raw) | |
| Classification | | | |
| <input type="checkbox"/> Network Function | <input type="checkbox"/> OS Fingerprint | | |
| Device Information | | | |
| <input type="checkbox"/> DHCP Server Address | <input type="checkbox"/> DNS Name | <input type="checkbox"/> Device Interfaces | <input type="checkbox"/> General Vulnerabilities |
| <input type="checkbox"/> Host is online | <input type="checkbox"/> MAC Address | <input type="checkbox"/> Member of Group | <input type="checkbox"/> NIC Vendor |

Ensure that your report can provide values for the properties selected for display by running policies that resolve the selected properties. If your running policies do not resolve either some or all of these properties, it is recommended to add new Discovery rules that are dedicated to resolving properties selected for report display. To add or edit Discovery rules, navigate to and select **Options > Discovery**.

Changing CounterACT User Passwords

You can manually change your user password using the Change Password option. The user password configured here is global and applies to all Forescout logins, such as the Console and the *Reports* portal. You can also change your user password from the Console.

This option is disabled for users connecting to the *Reports* portal through a User Directory server. For users not connecting through a User Directory server, the Change Password option is always available and cannot be disabled by an Administrator user. You can define users and how they connect to the *Reports* portal by selecting **Options > Console Users Profiles** in the Console.

The change password activity is written to the *Audit Trail*. Select **Audit Trails** from the **Log** menu in the Console to access the *Audit Trail*.

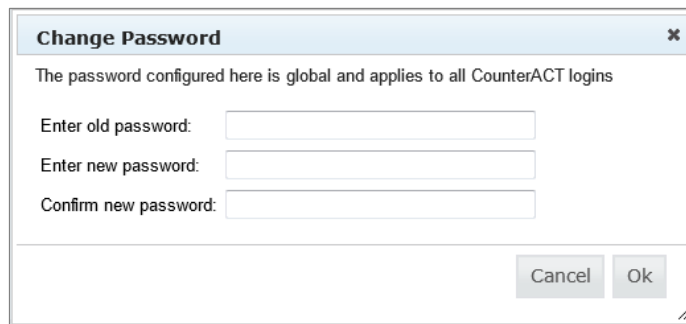
Refer to the section on Managing Users in the *Forescout Administration Guide* for more information on user passwords.

To change your CounterACT User Password:

1. In the *Administrator* section, select the **Change Password** button.



2. In the *Change Password* dialog box that opens, enter the old and new passwords and select **OK**.



The password configured here is global and applies to all CounterACT logins

Enter old password:

Enter new password:

Confirm new password:

Cancel Ok

Core Extensions Module Information

The Reports Plugin is installed with the Forescout Core Extensions Module.

The Forescout Core Extensions Module provides an extensive range of capabilities that enhance the core Forescout solution. These capabilities enhance detection, classification, reporting, troubleshooting, and more. The following components are installed with the Core Extensions Module:

| | | |
|------------------------------|----------------------------|-------------------------------|
| Advanced Tools Plugin | Device Data Publisher | IoT Posture Assessment Engine |
| CEF Plugin | DNS Client Plugin | |
| Cloud Uploader | DNS Enforce Plugin | NBT Scanner Plugin |
| DHCP Classifier Plugin | DNS Query Extension Plugin | Packet Engine |
| Dashboards Plugin | External Classifier Plugin | Reports Plugin |
| Data Publisher | Flow Analyzer Plugin | Syslog Plugin |
| Data Receiver | Flow Collector | Technical Support Plugin |
| Device Classification Engine | IOC Scanner Plugin | Web Client Plugin |

The Core Extensions Module is a Forescout Base Module. Base Modules are delivered with each Forescout release. Upgrading the Forescout version or performing a clean installation installs this module automatically.

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 modules. 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 modules. 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 Module 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.