CounterACT® Reports Plugin
Configuration Guide

Version 4.1.8 and Above
Table of Contents

About the Reports Plugin ................................................................. 3
Requirements ...................................................................................... 3
Supported Browsers .............................................................................. 3
Accessing the Reports Portal ............................................................... 5
Saving Reports and Creating Report Schedules ................................. 7
Managing Reports .............................................................................. 8
  Tracking Reports .............................................................................. 8
  Filter and Find ................................................................................. 9
  Simultaneously Manage Multiple Reports ......................................... 9
  Additional Report Management Tools ............................................. 9
    Configure Date/Time Format for Report Output ............................. 10
Report Templates ............................................................................ 10
  Assets Inventory ........................................................................... 10
  Working with Tables ...................................................................... 16
  Vulnerability ................................................................................ 16
  Policy Trend .................................................................................. 19
  Policy Status ............................................................................... 21
  Policy Details .............................................................................. 23
  Compliance Status ....................................................................... 25
  Device Details .............................................................................. 30
  Registered Guest Analysis ............................................................. 32
  Registered Guests ....................................................................... 38
Selecting Properties to Display .......................................................... 40
Backing up Reports .......................................................................... 41
Changing CounterACT User Passwords ............................................ 42
About the Reports Plugin

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.

Requirements

- JavaScript must be enabled on your Internet browser in order to work with the Reports Plugin.
- You must install CounterACT Service Pack 2.0.2 or above to work with this release.

Supported Browsers

The following browsers are supported:

- Internet Explorer 9 and higher
- Firefox 4.0 and higher
- Chrome 40 and higher

To enable JavaScript on Internet Explorer browsers:

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.
To enable JavaScript on Firefox:

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

In some operating systems, you may not be prompted for all the login steps described here.

To access the Reports portal:

1. Do one of the following:
   – In the Console toolbar, select Reports from the menu or select the Reports icon.
   – Browse to the following URL:
     http://<Device_IP>/report
     Where <Device_IP> is the IP address of the Enterprise Manager or an Appliance.
     A login page opens.

   When you access the portal from the Console, you may not be prompted to log in. Continue with step 4. For more information see “Separate Login to Each CounterACT Web-Based Portal” in the Console User Guide.

2. Enter the User Name and Password of a user that can access the portal. Typically the credentials you use to access the Console also grant access to the portal. For more information, see “Creating Users and User Groups” in the Console User Guide.

3. (Optional) When Service Pack 2.2.0 or above is installed in your environment, you may be able to use a Smart Card for authentication:
   a. Select the Login with Smart Card link. The Select a Certificate dialog box opens.
b. Select a certificate and then select **OK**. A PIN dialog box may open.

c. Enter a PIN code and then select **OK**.

4. The Reports home page opens.

5. Select **Add**. The Template Reports screen opens.
6. Select a report template and then select **Next** to begin generating a report. See [Configure Date/Time Format for Report Output](#).

### 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 also available to manage these reports, for example 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. Define report values.
3. Create a schedule if required, or select **None** in the Schedule section.
4. Select **Save**. Saved reports appear on the home page, showing basic settings, for example the format in which the report will be created.

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.

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 on the Reports home page to display reports that are 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.

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 Enterprise Manager as root.
2. Issue the following command:
   \[ \text{fstool set\_property msg\_report\_date\_format\_standart} \ "<expression>" \]
   Where \(<expression>\) is a legal formatting expression as described in the java.text.SimpleDateFormat class. For example, the following command generates the timestamp \textbf{12:08 PM}:
   \[ \text{fstool set\_property msg\_report\_date\_format\_standart} \ "h:mm a" \]
   All reports are generated using the specified date/time format.

Report Templates

Report templates include:
- 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, applications installed, processes and services running, open ports, external devices, operating systems and more.

This report is available to CounterACT version 6.3.4.0 and higher users only.

Assets Inventory report information is based on Console, Inventory detections. Refer to the Console, Online Help for information about working in the Inventory view.
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.

- 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.

<table>
<thead>
<tr>
<th>Segments</th>
<th>Subnets/Functions</th>
<th>MAC Addresses</th>
<th>Net Vendor</th>
</tr>
</thead>
<tbody>
<tr>
<td>000</td>
<td>Access Port</td>
<td>000000000001</td>
<td>3C09 Corporation</td>
</tr>
<tr>
<td>003</td>
<td>Management Area</td>
<td>000000000002</td>
<td>3C09 Corporation</td>
</tr>
<tr>
<td>005</td>
<td>Open Port</td>
<td>000000000003</td>
<td>3C09 Corporation</td>
</tr>
<tr>
<td>007</td>
<td>Closed Port</td>
<td>000000000004</td>
<td>3C09 Corporation</td>
</tr>
<tr>
<td>009</td>
<td>Other Port</td>
<td>000000000005</td>
<td>3C09 Corporation</td>
</tr>
</tbody>
</table>
To create an Assets Inventory report:

1. In the Reports home page, select Add. The Add Report Template dialog opens.

2. In the dialog, select Assets Inventory and then select Next. The report parameters page opens.

### 1. Header

- **Name:**
  - Assets Inventory

- **Description:**
  - Show an inventory of selected assets.

- **Report Footer:**
  - [Optional fields]

- **Generated by:**
  - [Field for administrator name]

### 2. Scope

**IP ranges:**

- **All IPs**
- **Range**
- **Segment(s) summary in footer**

- **Unknown IP addresses**

**Group By:**

- **Users**

**Filter By:**

**3. Display**

- **Select charts:**
  - [Optional choices]

- **Select inventory item column:**
  - [Optional choices]

**4. Schedule**

- **Schedule the report:**
  - None
  - Daily At [specific time]
  - Every [frequency and specific time]

- **Send Report To:** [Field for email address]
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 define the following:
   - In the **IP Ranges** section, select the host IP range or 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 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.

5. 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.
− 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 host details

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.

### Select report format

In the **Select report format** section, specify whether to create the report as a PDF or CSV file.

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.

**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.

**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.

3. In the dialog, select **Vulnerability** and then select **Next**. The report parameters page opens.
4. 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.

5. In the **Scope** section, select the host IP range or 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.

6. 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.

7. 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.
8. Take either of the following actions:

   - Select **Run**, [Run](#), to generate the defined report.
   - Select **Save**, [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.

2. In the dialog, select **Policy Trend** and then select **Next**. The report parameters page opens.
3. **Header**

   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. **Scope**

   In the **Scope** section:
   
   - Select the host IP range or segment 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.
5. 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.

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.

   *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 Status Report Example](image)

To create a Policy Status report:

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

2. In the dialog, select **Policy Status** and then 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:
   - Specify the scope by selecting the host IP range or segment 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:
     - ![Stopped]

5. 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.

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 Details

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

For example, create an Asset 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.

2. In the dialog, select Policy Details and then 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 the host IP range or segment 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.

5. In the **Display** section, define display requirements.
   - A pie chart is included in the report. Use 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.

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.

**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-compliant endpoints for each compliance policy. This information lets you quickly pinpoint compliance issues in your organization.

- Tables listing compliant and non-compliant host details, for example MAC and IP addresses, Domain and NetBIOS names, connected switch and User Directory information.
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.

2. In the dialog, select **Compliance Status** and then select Next. The report parameters page opens.
CounterACT Reports Plugin

Configuration Guide

1. Header
Name: Compliance Status
Description: Show the compliance status of selected hosts.
Report Footer: 
Generated by: admin

2. Scope
IP ranges:
- All IPs
- Range
- Segment
- Unknown IP addresses
Compliance Policies:
- All Compliance Policies
  - Antivirus Compliance
  - Instant Messaging Compliance
  - Peer-to-peer Compliance
  - Personal Firewall Compliance
  - Windows Update Compliance

3. Display
Select pie chart title: Total Compliance
Select Compliant label: Compliant
Select Not Compliant label: Not Compliant
Select Not Compliant bar chart title: Not Compliant breakdown
Details table display:
- Show Not Compliant details
- Show Compliant details
Select table columns:

<table>
<thead>
<tr>
<th>IP Address</th>
<th>MAC Address</th>
<th>DNS Name</th>
<th>NetBIOS Hostname</th>
<th>User</th>
<th>Display Name</th>
<th>NIC Vendor</th>
</tr>
</thead>
</table>

Select report format:

4. Schedule
Schedule the report:
- None
- Daily At
- Every
Send Report to: 

Version 4.1.8 and Above
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:
   - In the IP ranges section, specify the range of endpoint IP addresses or 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.

5. 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.

6. (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.

7. 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.
2. In the dialog, select Device Details and then 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 the host IP range or 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 host properties 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.

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.

## 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.

**Sample - Contact Person Report**

![Sample - Contact Person Report](image)

**Sample - Company Report**

![Sample - Company Report](image)
The **full names, companies and contact persons** information is extracted from the Guest Registration web page. Refer to the Console, Online help for more information about this feature.

**Requirements**

- Verify that you have installed the User Directory Plugin version 5.11020 or higher.
- Verify that you are working with a policy to handle network guest, for example you have run the **Corporate/Guest Template**. Refer to the Console, Online help for details.
- Verify that you are working with CounterACT version 6.3.4.0 or higher.

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.

2. In the dialog, select Registered Guest Analysis and then 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 define the following:
In the **IP Ranges** section, select the host IP range or 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:

- **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.
CounterACT Reports Plugin  Configuration Guide

- 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.

5. 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.

   ![Select guest item column](image)

   - 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 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](image)
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.

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.

**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.

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.

2. In the dialog, select Registered Guests and then 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 the host IP range or 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.
– 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.

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.

Selecting Properties to Display

The Vulnerability, Policy Compliance Details and Device Details, Asset 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 CounterACT 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.
3. Select **Edit**. The window is expanded.

![Show host details](image)

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.

```
<table>
<thead>
<tr>
<th>No.</th>
<th>Name</th>
<th>Sorted By</th>
<th>Items</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>IP Address</td>
<td>Ascending</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>NetBIOS Hostname</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

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**.

### Backing up Reports

Backup and restore procedures allow you to save many system settings, including scheduled or saved Web reports that you can later restore to the Enterprise Manager/Appliance. This feature should be used in cases of Appliance/Enterprise Manager hard drive failures or when data may be lost for another reason.

The restore procedure requires that you reinstall CounterACT. See *Backup and Restore* in the *CounterACT Installation Guide*. 
To perform a one-time backup:

1. Select **Options** from the **Tools** menu.
2. Select **CounterACT Devices** and the report that you want to backup.
3. Select **Backup**. By default the address, version number, date, and time appear as the name of the backup file.
4. Select the folder in which you want to save the backup file.
5. Select **Open** and then **Save**.

## 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 CounterACT logins, for example 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 *CounterACT Console User Manual* 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**.
Legal Notice

Copyright © ForeScout Technologies, Inc. 2000-2017. All rights reserved. The copyright and proprietary rights in this document belong to ForeScout Technologies, Inc. (“ForeScout”). It is strictly forbidden to copy, duplicate, sell, lend or otherwise use this document in any way, shape or form without the prior written consent of ForeScout. All other trademarks used in this document are the property of their respective owners.

These products are based on software developed by ForeScout. The products described in this document are protected by U.S. patents #6,363,489, #8,254,286, #8,590,004 and #8,639,800 and may be protected by other U.S. patents and foreign patents.

Redistribution and use in source and binary forms are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials and other materials related to such distribution and use acknowledge that the software was developed by ForeScout.

Unless there is a valid written agreement signed by you and ForeScout that governs the below ForeScout products and services:

- If you have purchased any ForeScout products, your use of such products is subject to your acceptance of the terms set forth at [http://www.forescout.com/eula/](http://www.forescout.com/eula/);
- If you have purchased any ForeScout products, your use of such products is subject to your acceptance of the terms set forth at [http://www.forescout.com/eula/](http://www.forescout.com/eula/);

If you have purchased any ForeScout support service (“ActiveCare”), your use of ActiveCare is subject to your acceptance of the terms set forth at [http://www.forescout.com/activecare-maintenance-and-support-policy/](http://www.forescout.com/activecare-maintenance-and-support-policy/);

- If you have purchased any ForeScout products, your use of such products is subject to your acceptance of the terms set forth at [http://www.forescout.com/eula/](http://www.forescout.com/eula/);
- If you are evaluating ForeScout’s products, your evaluation is subject to your acceptance of the applicable terms set forth below:
  - If you have requested a General Availability Product, the terms applicable to your use of such product are set forth at [http://www.forescout.com/evaluation-license/](http://www.forescout.com/evaluation-license/).
  - If you have requested an Early Availability Product, the terms applicable to your use of such product are set forth at [http://www.forescout.com/early-availability-agreement/](http://www.forescout.com/early-availability-agreement/).
  - If you have requested a Beta Product, the terms applicable to your use of such product are set forth at [http://www.forescout.com/beta-test-agreement/](http://www.forescout.com/beta-test-agreement/).
  - If you have purchased any ForeScout Not For Resale licenses, such license is subject to your acceptance of the terms set forth at [http://www.forescout.com/nfr-license/](http://www.forescout.com/nfr-license/).

Send comments and questions about this document to: documentation@forescout.com

2017-07-02 15:49