



# Dashboard and Reports Configuration Guide

Published **August 2020**

Document Version **1.0**

Pulse Secure, LLC  
2700 Zanker Road,  
Suite 200 San Jose  
CA 95134

[www.pulsesecure.net](http://www.pulsesecure.net)

© 2020 by Pulse Secure, LLC. All rights reserved.

Pulse Secure and the Pulse Secure logo are trademarks of Pulse Secure, LLC in the United States. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Pulse Secure, LLC assumes no responsibility for any inaccuracies in this document. Pulse Secure, LLC reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

*Dashboard and Reports Configuration Guide*

The information in this document is current as of the date on the title page.

## **END USER LICENSE AGREEMENT**

The Pulse Secure product that is the subject of this technical documentation consists of (or is intended for use with) Pulse Secure software. Use of such software is subject to the terms and conditions of the End User License Agreement (“EULA”) posted at <http://www.pulsesecure.net/support/eula/>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

# Contents

---

DASHBOARD AND REPORT OVERVIEW .....	5
ENABLING THE DASHBOARD.....	5
USING THE DASHBOARD .....	7
DASHBOARD OVERVIEW .....	8
ABOUT THE DASHBOARD .....	8
ABOUT THE DASHBOARD DATABASE .....	8
DISPLAYING THE DASHBOARD.....	9
SELECTING A DATA TIMEFRAME .....	10
REFRESHING DATA .....	12
DRILLING DOWN TO DETAILED REPORTS.....	13
USING THE USER SUMMARY REPORT.....	14
ABOUT THE USER SUMMARY REPORT.....	14
DISPLAYING THE USER SUMMARY REPORT .....	14
APPLYING DATA FILTERS.....	16
SORTING RECORDS .....	16
DRILLING DOWN TO THE SINGLE USER REPORT .....	17
EXPORTING USER SUMMARY REPORT .....	18
USING THE DEVICE SUMMARY REPORT .....	19
ABOUT THE DEVICE SUMMARY REPORT .....	19
DISPLAYING THE DEVICE SUMMARY REPORT.....	19
APPLYING DATA FILTERS.....	21
SORTING RECORDS .....	22
EXPORTING DEVICE SUMMARY REPORT .....	23
USING THE SINGLE DEVICE REPORT.....	24
ABOUT THE SINGLE DEVICE ACTIVITIES REPORT.....	24
DISPLAYING THE SINGLE DEVICE ACTIVITIES REPORT.....	25
APPLYING DATA FILTERS.....	26
SORTING RECORDS .....	27
EXPORTING SINGLE DEVICE ACTIVITIES REPORT .....	28
USING THE AUTHENTICATION REPORT.....	29
ABOUT THE AUTHENTICATION REPORT.....	29
DISPLAYING THE AUTHENTICATION REPORT.....	29
APPLYING DATA FILTERS.....	30
SORTING RECORDS .....	31
EXPORTING AUTHENTICATION REPORT .....	32
USING THE COMPLIANCE REPORT.....	33
ABOUT THE COMPLIANCE REPORT.....	33
DISPLAYING THE COMPLIANCE REPORT .....	33

APPLYING DATA FILTERS.....	35
SORTING RECORDS .....	36
EXPORTING COMPLIANCE REPORT.....	37
TROUBLESHOOTING A TOP ROLES CHART FROM THE DASHBOARD .....	37

# Dashboard and Reports

---

- [Dashboard and Report Overview](#) ..... 5
- [Enabling the Dashboard](#) ..... 5
- [Using the Dashboard](#) ..... 7
- [Using the User Summary Report](#) ..... 14
- [Using the Device Summary Report](#) ..... 19
- [Using the Single Device Report](#) ..... 24
- [Using the Authentication Report](#) ..... 29
- [Using the Compliance Report](#) ..... 33
- [Troubleshooting a Top Roles Chart from the Dashboard](#) ..... 37

## Dashboard and Report Overview

A dashboard is an interface used to manage the Pulse Secure access management framework. It provides an integrated view of all devices and users accessing the network, their device profile information, authentication methods used to gain access, device posture compliance and so on.

A report is an element of a dashboard used to convey complex data in simplified formats. Pulse Secure access management framework collects log and configuration data from across your network, and it then aggregates the data into reports for you to view and analyze. It provides a standard set of predefined reports that you can use and customize to fit your needs. The reports are grouped into logical categories for information related to authentication, session traffic, device administration, configuration and administration, and troubleshooting.

You can use the system dashboard and reports to analyze system utilization.

**Note:** When there is no data available for some duration:

- the new UI shows this data with '0' value
- the classical UI skips showing this data

An investigation is required only if any one of the graphs shows a drop for some duration in both new UI and classical UI.

## Enabling the Dashboard

You can use the admin console to enable or disable the dashboard.

To enable the dashboard.

1. Select **System > Status > Activity > Settings**.
2. Select **Enable Dashboard**.

**Note:** The dashboard is enabled by default.

**Figure 1** shows the Dashboard Settings for Pulse Connect Secure.

Figure 1 Dashboard Settings - Pulse Connect Secure

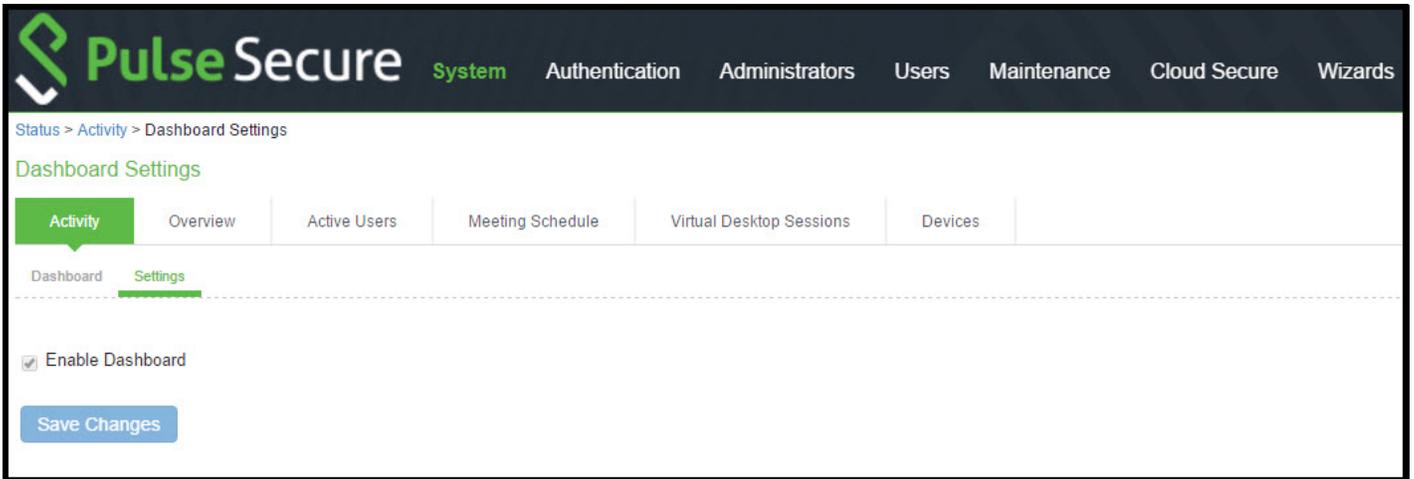


Figure 2 shows the available system reports through the dashboard for Pulse Connect Secure.

Figure 2 Dashboard



## Using the Dashboard

This topic describes the dashboard. It includes the following information:

- [“Dashboard Overview” on page 8](#)
- [“Displaying the Dashboard” on page 9](#)
- [“Selecting a Data Timeframe” on page 10](#)
- [“Drilling Down to Detailed Reports” on page 13](#)

## Dashboard Overview

- [“About the Dashboard” on page 8](#)
- [“About the Dashboard Database” on page 8](#)

### About the Dashboard

The dashboard contains six default graphic reports focused on security, network activity, application activity, system monitoring, and compliance.

**Table 1** describes the dashboard status bar for Pulse Connect Secure.

Table 1 Dashboard Status Bar

Metric	Description
<b>Connect Secure</b>	
Total Users	The total number of unique users logged in over the past 1, 7, or 30 days. (The count is based on the chart time period setting. The pertinent time period, for example, 1, 7, or 30 days, is shown within brackets along with the number of users.)
Active Users	The number of unique users currently logged in.
Current SSL Sessions	The total number of current SSL sessions.
Auth Only Sessions	The total number of authentication-only user sessions.
ActiveSync Device Count	The total number of active synchronization devices.

**Table 2** describes the default dashboard charts.

Table 2 Dashboard Charts

Metric	Description
Authentication Success	The number of successful authentications over the selected time period (1, 7, or 30 days).
Authentication Failure	The number of failed authentications over the selected time period (1, 7, or 30 days).
Session OS Count	Pie chart showing the number of the successful sessions per operating system.
Top Roles	Pie chart showing the number of top user roles assigned during the selected time period.
Compliance Results	Pie chart showing Host Checker posture assessment results: Compliant, Not Compliant, Not Assessed, or Remediated. Compliance results are reported for all instances in which Host Checker is run.
Posture Assessment	Pie chart showing Host Checker policy violations. Policy violations are reported only for instances in which Host Checker is run at initial sign in.

### About the Dashboard Database

The dashboard monitoring service collects and stores data in a database for 30 days. The total number of records stored in the database can be up to 300,000 records.

The dashboard database is created only after enabling the dashboard option. Note that only new sessions are added to the database and changing the Timeframe filter or clicking refresh sends queries to the database. The data is collected only when the dashboard option is enabled.

**Table 3** describes the different actions and their results.

Table 3 Dashboard Database

Action	Description
Disable and then reenable the dashboard.	The data collection stops when your dashboard is disabled.
Restore the data from backup, snapshot, or import config.	The data is not exported, and the data is retained during upgrades.

## Displaying the Dashboard

To display the dashboard, select **System > Status > Activity > Dashboard**.

**Figure 3** shows the dashboard for Pulse Connect Secure.

Figure 3 Dashboard - Pulse Connect Secure



## Selecting a Data Timeframe

To select a data timeframe:

1. Select **System > Status > Activity > Dashboard**.
2. Select one of the following periods from the **Timeframe** list box:
  - **Last 24 Hours** - (Default) Refers to the last 24 hours from the current hour.
  - **Last 7 Days** - Refers to current day and the previous last 6 days.
  - **Last 30 Days** - Refers to current day and the previous last 29 days.

**Note:** Access records are kept for 30 days. Older records are removed and not included in dashboard charts and reports.

Figure 4 shows the dashboard for a timeframe of 30 days.

Figure 4 Dashboard Showing a 30-Day Timeframe



Figure 5 shows the dashboard for a timeframe of 7 days.

Figure 5 Dashboard Showing a 7-Day Timeframe



## Refreshing Data

To refresh data:

1. Select **System > Status > Activity > Dashboard**.
2. Select one of the following refresh rates from the **Refresh** list box:
  - Disabled
  - 5 Minutes
  - 10 Minutes
  - 30 Minutes

- 60 Minutes

Figure 6 shows the dashboard with a refresh rate of 5 minutes.

Figure 6 Dashboard Showing a 5-Minute Refresh Rate



## Drilling Down to Detailed Reports

To drill down to view detailed reports:

1. Select **System > Status > Activity > Dashboard**.

1. Click the search icon  to display the corresponding tabular report with predefined search filters.

Figure 7 shows the detailed authentication report. The Authentication Results filter is set to **Success**.

Figure 7 Detailed Authentication Report

Reports > Authentication Report

Authentication Report

Reports  
Authentication Report

User Summary | Single User Activities | Device Summary | Single Device Activities | **Authentication** | Compliance

Authentication Report Download Report: CSV | Tab Delimited

Filter by: Date Range: Last 24 Hours Authentication Results: All Username: Realm: Apply Filter

View: 10

Username	Realm	Login Time	Auth Result	Failure Reason	Device ID	Role	Device OS
pulsesecure\ananthm	Pulse ESP Realm	Thu Mar 17 11:34:52 2016	Success			Pulse ESP Role	Windows 7
pulsesecure\ananthm	Pulse ESP Realm	Thu Mar 17 11:16:11 2016	Success			Pulse ESP Role	Windows 7
pulsesecure\mkarthik	Pulse SSL Realm	Thu Mar 17 11:11:18 2016	Success			Pulse SSL Role	Others
pulsesecure\gvipin	Pulse ESP Realm	Thu Mar 17 10:58:22 2016	Success			Pulse ESP Role	Windows 8
pulsesecure\shravan	Pulse ESP Realm	Thu Mar 17 10:55:38 2016	Success			Pulse ESP Role	Mac OS
pulsesecure\gvipin	Pulse ESP Realm	Thu Mar 17 10:45:26 2016	Success			Pulse ESP Role	Windows 8
pulsesecure\gvipin	Pulse ESP Realm	Thu Mar 17 10:43:06 2016	Success			Pulse ESP Role	Windows 8
pulsesecure\gvipin	Pulse ESP Realm	Thu Mar 17 10:35:47 2016	Success			Pulse ESP Role	Windows 8
pulsesecure\charuv	Users	Thu Mar 17 10:34:15 2016	Success			Users	Windows 7
pulsesecure\gvipin	Pulse ESP Realm	Thu Mar 17 10:33:05 2016	Success			Pulse ESP Role	Windows 8

1 2 3 of 6 >>

## Using the User Summary Report

This topic describes the user summary report. It includes the following information:

- [“About the Device Summary Report” on page 19](#)
- [“Displaying the Device Summary Report” on page 19](#)
- [“Applying Data Filters” on page 21](#)
- [“Sorting Records” on page 16](#)
- [“Drilling Down to the Single User Report” on page 17](#)
- [“Exporting User Summary Report” on page 18](#)

## About the User Summary Report

The user summary report displays user statistics such as realm, username, last login time, last login IP, successful login, and so on for each user based on the user activity in the selected time range.

## Displaying the User Summary Report

To display the user summary report, select **System > Reports > User Summary**.

[Figure 8](#) shows the user summary report for Pulse Connect Secure.

Figure 8 User Summary Report - Pulse Connect Secure

Reports > User Summary Report

### User Summary Report

Reports  
User Summary Report

User Summary | Single User Activities | Device Summary | Single Device Activities | Authentication | Compliance

User Summary Report Download Report: CSV | Tab Delimited

Filter by: Date Range: Last 24 Hours Username: Realm: Apply Filter

Username	Realm	Last Login Time	Last Login IP	Login Success	Login Failure	Compliant Sessions	Non-Compliant Sessions
nvishnu	Terminal Services Realm	Thu Mar 17 10:10:38 2016	10.209.126.66	1	0	1	0
pulsesecure\ananthm	Pulse ESP Realm	Thu Mar 17 11:34:52 2016	180.215.123.120	5	0	0	5
pulsesecure\latamsekar	Pulse ESP Realm	Wed Mar 16 21:41:54 2016	124.123.18.10	1	0	1	0

Table 4 describes the columns on the user summary report.

Table 4 User Summary Report Columns

Column	Description
Username	Specifies the name of the user.
Realm	Specifies the realm.
Last Login Time	Specifies the last time the user logged in.
Last Login IP	Specifies the last IP that the user logged in with.
Login Success	Specifies the number of successful logins.
Login Failure	Specifies the number of failed logins.
Compliant Sessions	Specifies the number of compliant sessions.
Non Compliant Sessions	Specifies the number of non compliant sessions.
Remediated Sessions	Specifies the number of remediated sessions.
Total Session Length	Specifies the total length of the sessions.
Average Session Length	Specifies the average length of the sessions.

## Applying Data Filters

To apply a data filter:

1. Select **System > Reports > User Summary**.
2. Select one of the following periods from the **Date Range** list box:
  - **Last 24 Hours** - (Default) Refers to the last 24 hours from the current hour.
  - **Last 7 Days** - Refers to current day and the previous last 6 days.
  - **Last 30 Days** - Refers to current day and the previous last 29 days.
3. Enter search criteria in one or more of the following attribute columns:
  - Username
  - Realm
4. Click **Apply Filter**.

Figure 9 shows the user summary report filtered by username for Pulse Connect Secure.

Figure 9 Filter User Summary Report

The screenshot shows the 'User Summary Report' interface. At the top, there are navigation tabs: 'User Summary' (selected), 'Single User Activities', 'Device Summary', 'Single Device Activities', 'Authentication', and 'Compliance'. Below the tabs, there is a 'Filter by:' section with a 'Date Range' dropdown set to 'Last 24 Hours', a 'Username' text box containing 'nvishnu', and an empty 'Realm' text box. An 'Apply Filter' button is to the right of these fields. Below the filter section is a table with the following columns: Username, Realm, Last Login Time, Last Login IP, Login Success, Login Failure, Compliant Sessions, Non-Compliant Sessions, Remediated Sessions, Total Session Length, and Average Session Length. The table contains one row for the user 'nvishnu' from the 'Terminal Services Realm'. The 'View:' dropdown is set to '10'.

Username	Realm	Last Login Time	Last Login IP	Login Success	Login Failure	Compliant Sessions	Non-Compliant Sessions	Remediated Sessions	Total Session Length	Average Session Length
nvishnu	Terminal Services Realm	Thu Mar 17 10:10:38 2016	10.209.126.66	1	0	1	0	0	1h 45m 58s	1h 45m 58s

## Sorting Records

The data source determines the default sort order of the data rows in the report. Typically, data appears randomly, so sorting is an important task in creating a useful report. You can sort single data columns or multiple columns.

To sort the user summary report:

1. Select **System > Reports > User Summary**.
2. Select one of the following columns from the user summary report table and click either the ascending or descending order icon.
  - Username
  - Realm

- Last Login Time

**Note:** The username column is sorted in ascending order by default.

Figure 10 shows the user summary report sorted by username for Pulse Connect.

Figure 10 Sort User Summary Report - Pulse Connect Secure

Reports > User Summary Report

User Summary Report

Reports  
User Summary Report

User Summary | Single User Activities | Device Summary | Single Device Activities | Authentication | Compliance

User Summary Report Download Report: CSV | Tab Delimited

Filter by: Date Range: Last 24 Hours Username: Realm: Apply Filter

Username	Realm	Last Login Time	Last Login IP	Login Success	Login Failure	Compliant Sessions	Non-Compliant Sessions
nvishnu	Terminal Services Realm	Thu Mar 17 10:10:38 2016	10.209.126.66	1	0	1	0
pulsesecure\ananthm	Pulse ESP Realm	Thu Mar 17 11:34:52 2016	180.215.123.120	5	0	0	5
pulsesecure\atamsekar	Pulse ESP Realm	Wed Mar 16 21:41:54 2016	124.123.18.10	1	0	1	0

## Drilling Down to the Single User Report

To drill down to a single user report:

1. Select **System > Reports > User Summary**.
2. Click the username to view the single user report.

Figure 11 shows the single user report displayed for Pulse Connect Secure.

Figure 11 Detailed Single User Report - Pulse Connect Secure

Reports > Single User Report

Single User Report

Reports  
Single User Report

User Summary **Single User Activities** Device Summary Single Device Activities Authentication Compliance

Single User Report Download Report: CSV | Tab Delimited

Filter by: Date Range: Last 30 Days Username: pulsesecure\snehal Apply Filter

View: 10

Username	Realm	Login Time	Logout Time	Duration	Device ID	MAC Address	Auth Result	Compliance	IP Address	Role
pulsesecure\snehal	Pulse ESP Realm	Thu Mar 17 10:25:48 2016	Thu Mar 17 10:26:11 2016	0m 23s			Success	Compliant	172.21.8.103	Pulse ESP Role
pulsesecure\snehal	Pulse ESP Realm	Wed Mar 16 11:08:44 2016	Wed Mar 16 15:04:45 2016	3h 56m 1s		68-F7-28-5A-54-D4	Success	Compliant	172.21.8.103	Pulse ESP Role
pulsesecure\snehal	Pulse ESP Realm	Wed Mar 16 11:08:34 2016				68-F7-28-5A-54-D4	Failure Failure Reason: Failed	Not-Assessed	172.21.8.103	
pulsesecure\snehal	Pulse ESP Realm	Wed Mar 16 11:08:24 2016				68-F7-28-5A-54-D4	Failure Failure Reason: Failed	Not-Assessed	172.21.8.103	
pulsesecure\snehal	Pulse ESP Realm	Thu Mar 10 11:33:36 2016	Thu Mar 10 20:47:24 2016	9h 13m 48s		5C-C5-D4-82-DA-25	Success	Compliant	106.216.173.165	Pulse ESP Role
pulsesecure\snehal	Pulse ESP Realm	Wed Mar 09 22:08:36 2016	Wed Mar 09 22:29:19 2016	20m 43s		5C-C5-D4-82-DA-25	Success	Compliant	106.216.190.96	Pulse ESP Role
pulsesecure\snehal	Pulse ESP Realm	Wed Mar 09 08:08:55 2016	Wed Mar 09 20:15:06 2016	12h 6m 11s		5C-C5-D4-82-DA-25	Success	Compliant	106.216.140.33	Pulse ESP Role
pulsesecure\snehal	Pulse ESP Realm	Tue Mar 08 10:40:59 2016	Tue Mar 08 14:50:55 2016	4h 9m 56s		68-F7-28-5A-54-D4	Success	Compliant	172.21.8.86	Pulse ESP Role
pulsesecure\snehal	Pulse ESP Realm	Mon Mar 07 10:16:58 2016	Mon Mar 07 19:10:26 2016	8h 53m 28s		5C-C5-D4-82-DA-25	Success	Remediated	106.216.162.148	Pulse ESP Role
pulsesecure\snehal		Fri Mar 04 08:45:25 2016	Fri Mar 04 13:35:30 2016	4h 50m 5s		68-F7-28-5A-54-D4	Success	Compliant	182.74.163.90	Pulse ESP Role

1 2 3 of 3 >>

## Exporting User Summary Report

To export device summary report:

1. Select **System > Reports > User Summary**.
2. Select a Download Report option.
  - **CSV** - Exports the report in CSV format.
  - **Tab Delimited** - Exports the report in tab-delimited format.

Figure 12 shows the export user summary report for Pulse Connect Secure is similar.

Figure 12 Export User Summary Report - Pulse Connect Secure

Reports > User Summary Report

User Summary Report

Reports  
User Summary Report

User Summary | Single User Activities | Device Summary | Single Device Activities | Authentication | Compliance

User Summary Report [Download Report: CSV | Tab Delimited](#)

Filter by: Date Range: Last 24 Hours Username: Realm: [Apply Filter](#)

Username	Realm	Last Login Time	Last Login IP	Login Success	Login Failure	Compliant Sessions	Non-Compliant Sessions
nvishnu	Terminal Services Realm	Thu Mar 17 10:10:38 2016	10.209.126.66	1	0	1	0
pulsesecure\ananthm	Pulse ESP Realm	Thu Mar 17 11:34:52 2016	180.215.123.120	5	0	0	5

## Using the Device Summary Report

This topic describes the device summary report. It includes the following information:

- [“About the User Summary Report” on page 14](#)
- [“Displaying the User Summary Report” on page 14](#)
- [“Applying Data Filters” on page 16](#)
- [“Sorting Records” on page 22](#)
- [“Exporting Device Summary Report” on page 23](#)

## About the Device Summary Report

The device summary report displays device information such as device detail, MAC address, last login time, last login IP, login successful, and so on for each user based on device activity in the selected time range.

## Displaying the Device Summary Report

To display the device summary report:

1. Select **System > Reports > Device Summary**.
2. Select one of the following periods from the **Date Range** list box:
  - **Last 24 Hours** - (Default) Refers to the last 24 hours from the current hour.
  - **Last 7 Days** - Refers to current day and the previous last 6 days.

- **Last 30 Days** - Refers to current day and the previous last 29 days.
3. Enter search criteria in one or more of the following columns:
    - Last Login Username
    - MAC Address
  4. Click **Apply Filter**.

Figure 13 shows the device summary report for Connect Secure.

Figure 13 Device Summary Report - Connect Secure

Device ID	MAC Address	Last Login Time	Last Login IP	Last Login Username	Login Success	Login Failure	Compliant Sessions	Non-Compliant Sessions	Remediated Sessions	Total Session Length	Average Session Length
	E8-2A-EA-89-3F-B9	Thu Mar 17 14:36:11 2016	182.74.163.90	raghpai	5	0	5	0	0	2h 37m 41s	31m 32s
	10-0B-A9-B7-CC-D4	Thu Mar 17 14:10:21 2016	180.215.123.19	pulsesecure\ananthm	6	0	0	6	0	3h 27m 50s	34m 38s
	Multiple	Thu Mar 17 13:54:53 2016	106.51.138.26	pulsesecure\charuv	7	0	0	7	0	6h 20m 1s	54m 17s

Table 5 describes the columns on the device summary report.

Table 5 Device Summary Report Columns

Column	Description
Device ID	Specifies a unique identifier to identify the endpoint. Click the device ID icon to view a single device report.
MAC Address	Specifies the MAC address of the device. Click the MAC address to view a single device report.
Last Login Time	Specifies the last time the device was logged in.
Last Login IP	Specifies the last IP that the device logged in with.
Last Login Username	Specifies the username that the user logged in with.
Login Success	Specifies the number of successfully logins.
Login Failure	Specifies the number of failed logins.

Column	Description
Compliant Sessions	Specifies the number of compliant sessions.
Non-Compliant Sessions	Specifies the number of non-compliant sessions.
Remediated Sessions	Specifies the number of remediated sessions.
Total Session Length	Specifies the total session length.
Average Session Length	Specifies the average session length.

**Note:** If a device has more than one MAC address in a session, then the value appearing in the MAC Address column will be multiple instead of the actual MAC addresses. Note that the value multiple is not hyperlinked.

## Applying Data Filters

To apply a data filter:

1. Select **System > Reports > Device Summary**.
2. Select one of the following periods from the **Date Range** list box:
  - **Last 24 Hours** - (Default) Refers to the last 24 hours from the current hour.
  - **Last 7 Days** - Refers to current day and the previous last 6 days.
  - **Last 30 Days** - Refers to current day and the previous last 29 days.
3. Enter search criteria in one or more of the following columns:
  - Last Login Username
  - Mac Address
4. Click **Apply Filter**.

Figure 14 shows the device summary report for Pulse Connect Secure.

Figure 14 Filter Device Summary Report - Pulse Connect Secure

Reports > Device Summary Report

Device Summary Report

Reports  
Device Summary Report

User Summary | Single User Activities | **Device Summary** | Single Device Activities | Authentication | Compliance

Device Summary Report Download Report: CSV | Tab Delimited

Filter by: Date Range: Last 24 Hours Last Login Username: [input] MAC Address: [input] Apply Filter

View: 10

Device ID	MAC Address	Last Login Time	Last Login IP	Last Login Username	Login Success	Login Failure	Compliant Sessions	Non-Compliant Sessions	Remediated Sessions	Total Session Length	Average Session Length
[icon]	Multiple	Thu Mar 17 13:54:53 2016	106.51.138.26	pulsesecure\charuv	8	0	0	8	0	6h 38m 9s	49m 46s
[icon]	Multiple	Thu Mar 17 13:50:42 2016	182.74.163.90	pulsesecure\sgadde	3	0	3	0	0	6h 48m 35s	2h 16m 11s
		Thu Mar 17 13:14:51 2016	10.204.48.240	pulsesecure\gvipin	1	0	1	0	0	5m 39s	5m 39s

## Sorting Records

The data source determines the default sort order of the data rows in the report. Typically, data appears randomly, so sorting is an important task in creating a useful report. You can sort single data columns or multiple columns.

To sort the device summary report:

1. Select **System > Reports > Device Summary**.
2. Select any one of the following columns and click either the ascending or descending order icon.
  - Last Login Time
  - Last Login Username

**Note:** You can sort the column in either ascending order or descending order.

Figure 15 shows the device summary report sorted by last login time for Pulse Connect Secure.

Figure 15 Sort Records in Device Summary Report

Reports > Device Summary Report

Device Summary Report

Reports  
Device Summary Report

User Summary | Single User Activities | **Device Summary** | Single Device Activities | Authentication | Compliance

Device Summary Report Download Report: CSV | Tab Delimited

Filter by: Date Range: Last 24 Hours Last Login Username: MAC Address: Apply Filter

View: 10

Device ID	MAC Address	Last Login Time	Last Login IP	Last Login Username	Login Success	Login Failure	Compliant Sessions	Non-Compliant Sessions	Remediated Sessions	Total Session Length	Average Session Length
	Multiple	Thu Mar 17 13:54:53 2016	106.51.138.26	pulsesecure\charuv	8	0	0	8	0	6h 38m 9s	49m 46s
	Multiple	Thu Mar 17 13:50:42 2016	182.74.163.90	pulsesecure\sgadde	3	0	3	0	0	6h 48m 35s	2h 16m 11s
		Thu Mar 17 13:14:51 2016	10.204.48.240	pulsesecure\gvipin	1	0	1	0	0	5m 39s	5m 39s

## Exporting Device Summary Report

To export device summary report:

1. Select **System > Reports > Device Summary**.
2. Select a Download Report option.
  - **CSV** - Exports the report in CSV format.
  - **Tab Delimited** - Exports the report in tab-delimited format.

Figure 16 shows the export device summary report Pulse Connect Secure.

Figure 16 Export Device Summary Report

Reports > Device Summary Report

Device Summary Report

Reports  
Device Summary Report

User Summary | Single User Activities | **Device Summary** | Single Device Activities | Authentication | Compliance

Device Summary Report [Download Report: CSV | Tab Delimited](#)

Filter by: Date Range: Last 24 Hours | Last Login Username: | MAC Address: | [Apply Filter](#)

View: 10

Device ID	MAC Address	Last Login Time	Last Login IP	Last Login Username	Login Success	Login Failure	Compliant Sessions	Non-Compliant Sessions	Remediated Sessions	Total Session Length	Average Session Length
	Multiple	Thu Mar 17 13:54:53 2016	106.51.138.26	pulsesecure\charuv	8	0	0	8	0	6h 38m 9s	49m 46s
	Multiple	Thu Mar 17 13:50:42 2016	182.74.163.90	pulsesecure\sgadde	3	0	3	0	0	6h 48m 35s	2h 16m 11s
		Thu Mar 17 13:14:51 2016	10.204.48.240	pulsesecure\gvipin	1	0	1	0	0	5m 39s	5m 39s
	E8-2A-EA-89-3F-B9	Thu Mar 17 13:01:49 2016	182.74.163.90	raghpal	4	0	4	0	0	2h 36m 57s	39m 14s
	28-D2-44-F3-DE-68	Thu Mar 17 12:13:11 2016	10.209.122.63	pulsesecure\cnreddy	2	0	0	2	0	3h 28m 36s	1h 44m 18s
	10-0B-A9-B7-CC-D4	Thu Mar 17 11:34:52 2016	180.215.123.120	pulsesecure\ananthm	5	0	0	5	0	3h 1m 16s	36m 15s
		Thu Mar 17 11:11:18 2016	182.74.163.90	pulsesecure\mkarthik	1	0	0	0	0	2h 7m 40s	2h 7m 40s
		Thu Mar 17 10:58:22 2016	10.204.48.218	pulsesecure\gvipin	1	0	1	0	0	1h 49m 41s	1h 49m 41s
	A0-99-9B-0F-09-6B	Thu Mar 17 10:55:38 2016	172.21.17.26	pulsesecure\shravan	4	0	4	0	0	4h 47m 45s	1h 11m 56s
		Thu Mar 17 10:45:26 2016	10.204.48.218	pulsesecure\gvipin	1	0	1	0	0	1m 17s	1m 17s

1 2 3 of 4 >>

## Using the Single Device Report

This topic describes the single device report. It includes the following information:

- [“About the Single Device Activities Report” on page 24](#)
- [“Displaying the Single Device Activities Report” on page 25](#)
- [“Applying Data Filters” on page 26](#)
- [“Sorting Records” on page 31](#)
- [“Exporting Single Device Activities Report” on page 28](#)

## About the Single Device Activities Report

The single device activities report displays the device activity information such as username, realm, login time, logout time, device detail, MAC address, authentication mechanism, authentication result, compliance, IP address, role and so on for each device.

## Displaying the Single Device Activities Report

To display the single device activities report, select **System > Reports > Single Device Activities**.

Figure 17 shows the single device activities report for Pulse Connect Secure.

Figure 17 Single Device Activities Report - Pulse Connect Secure

Table 6 describes the columns on the single device report.

Table 6 Single Device Report Columns

Column	Description
Username	Specifies the name of the user.
Realm	Specifies the realm.
Login Time	Specifies the time the user logged in.
Logout Time	Specifies the time the user logged out.
Duration	Specifies the total duration of the user session.
Device ID	Specifies a unique identifier used to identify an end point. Click the device ID icon to view a single device report.
MAC Address	Specifies the MAC address of the device.
Auth Mechanism	Specifies the authentication mechanism: 802.1x, Layer 3, MAC address. It applies to Policy Secure only.
Auth Result	Specifies the authentication result.
Compliance	Specifies the Host Checker posture assessment results: Compliant, Not Compliant, Not Assessed, or Remediated.

Column	Description
IP Address	Specifies the IP that the user logged in with.
Role	Specifies the role of the user.
Device Detail	Displays the URL that is used for connecting to the MDM server.

## Applying Data Filters

To apply a data filter:

1. Select **System > Reports > Single Device Activities**.
2. Select one of the following periods from the **Filter by: Date Range** list box:
  - **Last 24 Hours** - (Default) Refers to the last 24 hours from the current hour.
  - **Last 7 Days** - Refers to current day and the previous last 6 days.
  - **Last 30 Days** - Refers to current day and the previous last 29 days.
3. Enter search criteria in one or more of the following columns:
  - Compliance Results
  - MAC Address
  - Device ID
  - Authentication Mechanism. It applies only to Policy Secure.
4. Click **Apply Filter**.

Figure 18 shows the single device activities report for Pulse Connect Secure.

Figure 18 Filter Single Device Activities Report

Pulse Secure System Authentication Administrators Users Maintenance Cloud Secure Wizards Pulse Connect Secure on NODE\_3\_3

Reports > Single Device Report

Single Device Report

Reports Single Device Report

User Summary Single User Activities Device Summary **Single Device Activities** Authentication Compliance

Single Device Report Download Report: CSV | Tab Delimited

Filter by: Date Range: Last 24 Hours Compliance Results: Compliant, Non-Compliant, Remediated, Not-Assessed MAC Address: Device ID: 8d06733e552349a7af9d0 Apply Filter

View: 10

Username	Realm	Login Time	Logout Time	Duration	Device ID	MAC Address	Auth Result	Compliance	IP Address	Role	Device Detail
pulsesecure\anathm	Pulse ESP Realm	Thu Mar 17 14:10:21 2016	Session in progress	4m 4s		10-0B-A9-B7-CC-D4	Success	Non-Compliant	180.215.123.19	Pulse ESP Role	
pulsesecure\anathm	Pulse ESP Realm	Thu Mar 17 11:34:52 2016	Thu Mar 17 13:39:32 2016	2h 4m 40s		10-0B-A9-B7-CC-D4	Success	Non-Compliant	180.215.123.120	Pulse ESP Role	
pulsesecure\anathm	Pulse ESP Realm	Thu Mar 17 11:16:11 2016	Thu Mar 17 11:20:27 2016	4m 16s		10-0B-A9-B7-CC-D4	Success	Non-Compliant	180.215.123.120	Pulse ESP Role	
pulsesecure\anathm	Pulse ESP Realm	Wed Mar 16 21:40:40 2016	Wed Mar 16 22:24:17 2016	43m 37s		10-0B-A9-B7-CC-D4	Success	Non-Compliant	180.215.121.115	Pulse ESP Role	
pulsesecure\anathm	Pulse ESP Realm	Wed Mar 16 18:39:50 2016	Wed Mar 16 18:45:33 2016	5m 43s		10-0B-A9-B7-CC-D4	Success	Non-Compliant	180.215.122.9	Pulse ESP Role	
pulsesecure\anathm	Pulse ESP Realm	Wed Mar 16 15:44:34 2016	Wed Mar 16 15:47:34 2016	3m 0s		10-0B-A9-B7-CC-D4	Success	Non-Compliant	180.215.121.88	Pulse ESP Role	

1 of 1

## Sorting Records

The data source determines the default sort order of the data rows in the report. Typically, data appears randomly, so sorting is an important task in creating a useful report. You can sort single data column.

To sort the single device activities report:

1. Select **System > Reports > Single Device Activities**.
2. Select **Login Time** column and click either the ascending or descending order icon.

**Note:** You can sort the column in either ascending order or descending order.

Figure 19 shows the single device activities report sorted by last login time Pulse Connect Secure.

Figure 19 Sort Records in Single Device Activities Report

Reports > Single Device Report

Single Device Report

Reports  
Single Device Report

User Summary | Single User Activities | Device Summary | **Single Device Activities** | Authentication | Compliance

Single Device Report Download Report: CSV | Tab Delimited

Filter by: Date Range: Last 24 Hours Compliance Results:   
 Compliant  
 Non-Compliant  
 Remediated  
 Not-Assessed

MAC Address: Device ID: 2c67f29e7ca746cd8dceed Apply Filter

View: 10

Username	Realm	Login Time	Logout Time	Duration	Device ID	MAC Address	Auth Result	Compliance	IP Address	Role	Device Detail
pulsesecure\charuv	Users	Thu Mar 17 12:54:47 2016	Session in progress	3m 53s		60-67-20-6C-89-04	Success	Non-Compliant	106.51.138.26	Users	
pulsesecure\charuv	Users	Thu Mar 17 11:54:16 2016	Thu Mar 17 12:54:40 2016	1h 0m 24s		60-67-20-6C-89-04	Success	Non-Compliant	106.51.140.105	Users	
pulsesecure\charuv	Users	Thu Mar 17 10:34:15 2016	Thu Mar 17 11:35:14 2016	1h 0m 59s		00-21-CC-CB-FE-16	Success	Non-Compliant	103.227.98.234	Users	
pulsesecure\charuv	Users	Thu Mar 17 09:33:46 2016	Thu Mar 17 10:34:12 2016	1h 0m 26s		00-21-CC-CB-FE-16	Success	Non-Compliant	103.227.98.234	Users	
pulsesecure\charuv	Users	Wed Mar 16 16:17:40 2016	Wed Mar 16 16:53:41 2016	36m 1s		60-67-20-6C-89-04	Success	Non-Compliant	106.197.61.22	Users	
pulsesecure\charuv	Users	Wed Mar 16 15:05:24 2016	Wed Mar 16 16:05:30 2016	1h 0m 6s		00-21-CC-CB-FE-16	Success	Non-Compliant	182.74.163.90	Users	
pulsesecure\charuv	Users	Wed Mar 16 14:05:16 2016	Wed Mar 16 15:05:17 2016	1h 0m 1s		60-67-20-6C-89-04	Success	Non-Compliant	172.21.16.149	Users	

1 of 1

## Exporting Single Device Activities Report

To export single device activities report:

1. Select **System > Reports > Single Device Activities**.
2. Select a Download Report option.
  - **CSV** - Exports the report in CSV format.
  - **Tab Delimited** - Exports the report in tab-delimited format.

Figure 20 shows the single device activities report for Pulse Connect Secure.

Figure 20 Export Single Device Activities Report

Single Device Report

Download Report: CSV | Tab Delimited

Filter by: Date Range: Last 24 Hours Compliance Results: Compliant, Non-Compliant, Remediated, Not-Assessed

MAC Address: Device ID: 2c67f29e7ca746cd8dceed Apply Filter

View: 10

Username	Realm	Login Time	Logout Time	Duration	Device ID	MAC Address	Auth Result	Compliance	IP Address	Role	Device Detail
pulsesecure\charuv	Users	Thu Mar 17 12:54:47 2016	Session in progress	1m 14s		60-67-20-6C-89-04	Success	Non-Compliant	106.51.138.26	Users	
pulsesecure\charuv	Users	Thu Mar 17 11:54:16 2016	Thu Mar 17 12:54:40 2016	1h 0m 24s		60-67-20-6C-89-04	Success	Non-Compliant	106.51.140.105	Users	
pulsesecure\charuv	Users	Thu Mar 17 10:34:15 2016	Thu Mar 17 11:35:14 2016	1h 0m 59s		00-21-CC-CB-FE-16	Success	Non-Compliant	103.227.98.234	Users	

## Using the Authentication Report

This topic describes the authentication report. It includes the following information:

- [“About the Authentication Report” on page 29](#)
- [“Displaying the Authentication Report” on page 29](#)
- [“Applying Data Filters” on page 30](#)
- [“Sorting Records” on page 31](#)
- [“Exporting Authentication Report” on page 32](#)

## About the Authentication Report

The authentication report displays the authentication result for each user based on the device activity in the selected time range.

## Displaying the Authentication Report

To display the authentication report, select **System > Reports > Authentication**.

[Figure 21](#) shows the authentication report for Pulse Connect Secure.

Figure 21 Authentication Report - Pulse Connect Secure

Username	Realm	Login Time	Auth Result	Failure Reason	Device ID	Role	Device OS
raghpai	NC ESP Realm	Thu Mar 17 12:22:18 2016	Success			NC ESP Role	Windows 7
pulsesecure\cnreddy	Pulse ESP Realm	Thu Mar 17 12:13:11 2016	Success			Pulse ESP Role	Windows 7
pulsesecure\chanuv	Users	Thu Mar 17 11:54:16 2016	Success			Users	Windows 7

Table 7 describes the columns on the authentication report.

Table 7 Authentication Report Columns

Column	Description
Username	Specifies the name of the user.
Realm	Specifies the realm.
Login Time	Specifies the time the user logged in.
Auth Mechanism	Specifies the authentication mechanism: 802.1x, Layer 3, MAC address. It applies only to Policy Secure.
Auth Result	Specifies the authentication result.
Failure Reason	Specifies the host checker failure reason.
Device ID	Specifies a unique identifier used to identify an end point. Click the device ID icon to view a single device report.
Role	Specifies the user role.
Device OS	Specifies the operating system of the device.

## Applying Data Filters

To apply a data filter:

1. Select **System > Reports > Authentication**.
2. Select one of the following periods from the **Filter by: Date Range** list box:
  - **Last 24 Hours** - (Default) Refers to the last 24 hours from the current hour.

- **Last 7 Days** - Refers to current day and the previous last 6 days.
  - **Last 30 Days** - Refers to current day and the previous last 29 days.
3. Enter search criteria in one or more of the following columns:
    - Authentication Results
    - Username
    - Realm
  4. Click **Apply Filter**.

Figure 22 shows the authentication report for Pulse Connect Secure.

Figure 22 Filter Authentication Report

The screenshot shows the 'Authentication Report' page. At the top, there are navigation tabs: 'User Summary', 'Single User Activities', 'Device Summary', 'Single Device Activities', 'Authentication' (selected), and 'Compliance'. Below the tabs, there's a 'Filter by:' section with a 'Date Range' dropdown set to 'Last 24 Hours', an 'Authentication Results' dropdown set to 'Success', and input fields for 'Username' and 'Realm'. An 'Apply Filter' button is to the right. A 'View:' dropdown is set to '10'. Below the filter section is a table with the following data:

Username	Realm	Login Time	Auth Result	Failure Reason	Device ID	Role	Device OS
raghpai	NC ESP Realm	Thu Mar 17 12:22:18 2016	Success			NC ESP Role	Windows 7
pulsesecure\cnreddy	Pulse ESP Realm	Thu Mar 17 12:13:11 2016	Success			Pulse ESP Role	Windows 7
pulsesecure\chanuv	Users	Thu Mar 17 11:54:16 2016	Success			Users	Windows 7
pulsesecure\ananthm	Pulse ESP Realm	Thu Mar 17 11:34:52 2016	Success			Pulse ESP Role	Windows 7
pulsesecure\ananthm	Pulse ESP Realm	Thu Mar 17 11:16:11 2016	Success			Pulse ESP Role	Windows 7

## Sorting Records

The data source determines the default sort order of the data rows in the report. Typically, data appears randomly, so sorting is an important task in creating a useful report. You can sort single data column.

To sort the authentication report:

1. Select **System > Reports > Authentication**.
2. Select **Login Time** column and click either the ascending or descending order icon.

Figure 23 shows the authentication report sorted by last login time for Pulse Connect Secure.

Figure 23 Sort Records in Authentication Report

Reports > Authentication Report

Authentication Report

Reports  
Authentication Report

User Summary | Single User Activities | Device Summary | Single Device Activities | **Authentication** | Compliance

Authentication Report Download Report: CSV | Tab Delimited

Filter by: Date Range: Last 24 Hours Authentication Results: All Username: Realm: Apply Filter

View: 10

Username	Realm	Login Time	Auth Result	Failure Reason	Device ID	Role	Device OS
raghpai	NC ESP Realm	Thu Mar 17 12:22:18 2016	Success			NC ESP Role	Windows 7
pulsesecure\cnreddy	Pulse ESP Realm	Thu Mar 17 12:13:11 2016	Success			Pulse ESP Role	Windows 7
pulsesecure\charuv	Users	Thu Mar 17 11:54:16 2016	Success			Users	Windows 7
pulsesecure\ananthm	Pulse ESP Realm	Thu Mar 17 11:34:52 2016	Success			Pulse ESP Role	Windows 7
pulsesecure\ananthm	Pulse ESP Realm	Thu Mar 17 11:16:11 2016	Success			Pulse ESP Role	Windows 7

## Exporting Authentication Report

To export an authentication report:

1. Select **System > Reports > Authentication**.
2. Select a Download Report option.
  - **CSV** - Exports the report in CSV format.
  - **Tab Delimited** - Exports the report in tab-delimited format.

Figure 24 the authentication report displayed for Pulse Connect Secure.

Figure 24 Export Authentication Report

Reports > Authentication Report

Authentication Report

Reports  
Authentication Report

User Summary | Single User Activities | Device Summary | Single Device Activities | **Authentication** | Compliance

Authentication Report Download Report: CSV | Tab Delimited

Filter by: Date Range: Last 24 Hours Authentication Results: All Username: Realm: Apply Filter

View: 10

Username	Realm	Login Time	Auth Result	Failure Reason	Device ID	Role	Device OS
raghpai	NC ESP Realm	Thu Mar 17 12:22:18 2016	Success			NC ESP Role	Windows 7
pulsesecure\cnreddy	Pulse ESP Realm	Thu Mar 17 12:13:11 2016	Success			Pulse ESP Role	Windows 7
pulsesecure\charuv	Users	Thu Mar 17 11:54:16 2016	Success			Users	Windows 7
pulsesecure\ananthm	Pulse ESP Realm	Thu Mar 17 11:34:52 2016	Success			Pulse ESP Role	Windows 7
pulsesecure\ananthm	Pulse ESP Realm	Thu Mar 17 11:16:11 2016	Success			Pulse ESP Role	Windows 7

## Using the Compliance Report

This topic describes the compliance report. It includes the following information:

- “About the Compliance Report” on page 33
- “Displaying the Compliance Report” on page 33
- “Applying Data Filters” on page 35
- “Sorting Records” on page 36
- “Exporting Compliance Report” on page 37

## About the Compliance Report

The compliance report displays compliance status such as compliant, not compliant, remediated, not assessed information for each user based on the device activity in the selected time range.

## Displaying the Compliance Report

To display the compliance report, select **System > Reports > Compliance**.

Figure 25 shows the compliance report for Pulse Connect Secure.

Figure 25 Compliance Report - Pulse Connect Secure

Username	Realm	Device ID	MAC Address	Session Compliance	Initial Host Check Time	Initial Host Check Details
raghpai	NC ESP Realm		E8-2A-EA-89-3F-B9	Compliant	Thu Mar 17 12:22:18 2016	Host check result: Pass
pulsesecure\cnreddy	Pulse ESP Realm		28-D2-44-F3-DE-68	Non-Compliant	Thu Mar 17 12:13:11 2016	Host check result: Fail Failed Policies: • AV Failure reasons: • Anti-virus scan time check failed
pulsesecure\charuv	Users		60-67-20-6C-89-04	Non-Compliant	Thu Mar 17 11:54:16 2016	Host check result: Fail Failed Policies: • aanev (Deprecated) • aanev: SVMActive (Deprecated)

Table 8 describes the different columns on the compliance report.

Table 8 Compliance Report Columns

Column	Description
Username	Specifies the name of the user.
Realm	Specifies the realm.
Device ID	Specifies a unique identifier used to identify an end point. Click the device ID icon to view a single device report.
MAC Address	Specifies the MAC address of the device.
Session Compliance	Specifies the Host Checker posture assessment results: Compliant, Not Compliant, Not Assessed, or Remediated.
Initial Host Check Time	Specifies the initial host check time.
Initial Host Check Details	Specifies the host check result.

The posture assessment chart is also a part of compliance report. It is displayed based on Initial Host Checker evaluation details (Login time).

**Table 9** lists the type and the failure reasons for Host Checker.

Table 9 Host Checker Failure Reasons- Posture Assessment Chart

Type	Failure Reason
Antivirus	Anti-virus not installed Anti-virus not running Anti-virus not up to date Anti-virus scan time check failed
Firewall	Firewall not installed Firewall not running
Antimalware	Anti-malware not installed
Antispyware	Anti-spyware not installed Anti-spyware not running
OS Checks	Unsupported OS
Port	Restricted ports open Required ports not open
Process	Detected restricted processes Required processes not detected
File	Detected restricted files Required files missing
Registry	Incorrect registry settings

Type	Failure Reason
NetBIOS	Detected restricted NetBIOS names Required NetBIOS names not found
MAC Address	Detected restricted MAC address Required MAC address not present
Machine Certificate	Certificate missing
Patch management	Patches missing
Cache Cleaner	Cache cleaner failed
SVW	NA (Not considered for reporting)
SVW sub policy (.SVWActive)	Connected from non-SVW
Remote IMV	Remote IMV failure
EES	Enhanced Endpoint Security failed (no longer supported)
3rd party	NA (Not considered for reporting)
3rd party sub policy	3rd party sub policy failed
Rooting Detection	Detected rooted devices
Jail Breaking Detection	Detected jail broken devices
3rd party NHC Check	Generic failure
Statement of Health	Generic failure
Connection Control	Generic failure

## Applying Data Filters

To apply a data filter:

1. Select **System > Reports > Compliance**.
2. Select one of the following periods from the **Filter by: Date Range** list box:
  - **Last 24 Hours** - (Default) Refers to the last 24 hours from the current hour.
  - **Last 7 Days** - Refers to current day and the previous last 6 days.
  - **Last 30 Days** - Refers to current day and the previous last 29 days.
3. Enter search criteria in one or more of the following columns:
  - Compliance Results
  - Username
  - Realm
  - MAC Address

4. Click **Apply Filter**.

Figure 26 shows the compliance report for Pulse Connect Secure.

Figure 26 Filter Compliance Report

The screenshot shows the 'Compliance Report' page. At the top, there are navigation tabs: 'User Summary', 'Single User Activities', 'Device Summary', 'Single Device Activities', 'Authentication', and 'Compliance'. Below these, there's a 'Compliance Report' section with a 'Download Report: CSV | Tab Delimited' link. A filter section is highlighted with a red box, containing a 'Filter by: Date Range' dropdown set to 'Last 24 Hours', a 'Compliance Results' dropdown menu with options 'Compliant', 'Non-Compliant', 'Remediated', and 'Not-Assessed', and input fields for 'Username', 'Realm', and 'MAC Address' with an 'Apply Filter' button. Below the filter section, there's a 'View: 10' dropdown. The main table has columns: 'Username', 'Realm', 'Device ID', 'MAC Address', 'Session Compliance', 'Initial Host Check Time', and 'Initial Host Check Details'. The table contains two rows of data.

Username	Realm	Device ID	MAC Address	Session Compliance	Initial Host Check Time	Initial Host Check Details
pulsesecure\gjayaraman	Pulse ESP Realm		68-F7-28-5A-4A-70	Not-Assessed		
pulsesecure\mkarthik	Pulse SSL Realm			Not-Assessed		

## Sorting Records

The data source determines the default sort order of the data rows in the report. Typically, data appears randomly, so sorting is an important task in creating a useful report. You can sort single data column.

To sort the compliance:

1. Select **System > Reports > Compliance**.
2. Select **Initial Host Check Time** or **Username** column and click either the ascending or descending order icon.

Figure 27 shows the compliance report sorted by last login time for Pulse Connect Secure.

Figure 27 Sort Records in Compliance Report

This screenshot is similar to Figure 26 but shows the 'Initial Host Check Time' column in the table header selected for sorting, indicated by a red box around the dropdown arrow. The filter section is also visible, with the 'Compliance Results' dropdown menu open, showing 'Not-Assessed' selected.

Username	Realm	Device ID	MAC Address	Session Compliance	Initial Host Check Time	Initial Host Check Details
pulsesecure\gjayaraman	Pulse ESP Realm		68-F7-28-5A-4A-70	Not-Assessed		
pulsesecure\mkarthik	Pulse SSL Realm			Not-Assessed		

## Exporting Compliance Report

To export a compliance report:

1. Select **System > Reports > Compliance**.
2. Select a Download Report option.
  - **CSV** - Exports the report in CSV format.
  - **Tab Delimited** - Exports the report in tab-delimited format.

Figure 28 shows the export compliance report displayed for Pulse Connect Secure.

Figure 28 Export Compliance Report

Reports > Compliance Report

Compliance Report

Reports  
Compliance Report

User Summary | Single User Activities | Device Summary | Single Device Activities | Authentication | **Compliance**

Compliance Report Download Report: CSV | Tab Delimited

Filter by: Date Range: Last 24 Hours Compliance Results:   
 Compliant  
 Non-Compliant  
 Remediated  
 Not-Assessed

Username: Realm: MAC Address: Apply Filter

View: 10

Username	Realm	Device ID	MAC Address	Session Compliance	Initial Host Check Time	Initial Host Check Details
pulsesecure\jayaraman	Pulse ESP Realm		68-F7-28-5A-4A-70	Not-Assessed		
pulsesecure\mkarthik	Pulse SSL Realm			Not-Assessed		

## Troubleshooting a Top Roles Chart from the Dashboard

Problem	Description:
Environment:	
Symptoms: The same role for a selected time period appears multiple times in a top user roles report generated from the dashboard.	
Diagnosis	The same role can appear multiple times when the role was deleted but created again using the same name.

