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

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 Reports

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

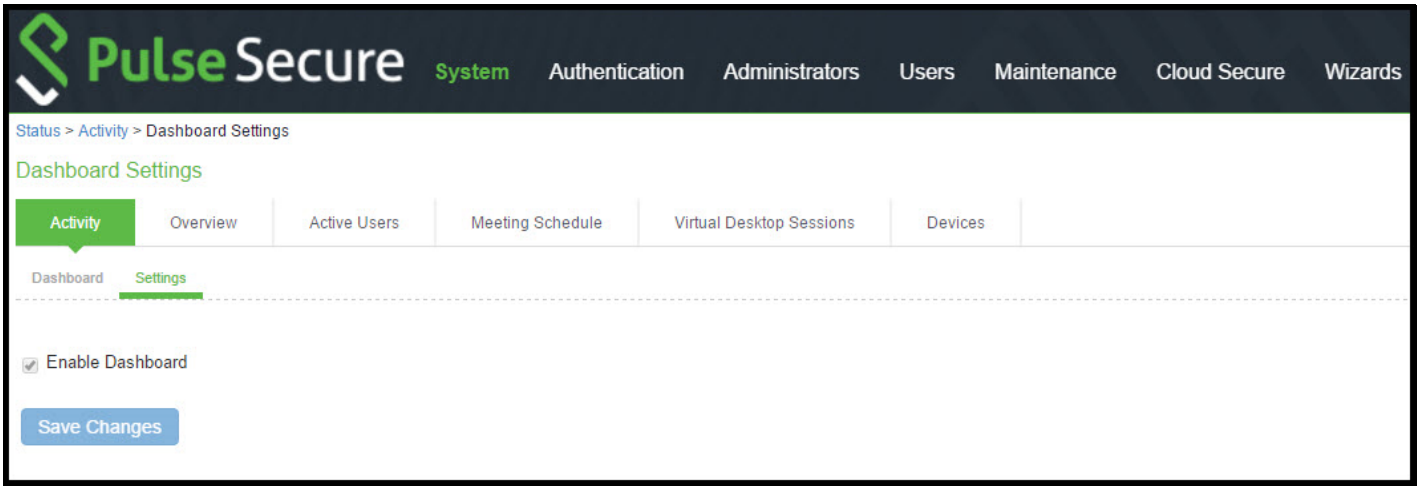


Figure 2 shows the available system reports through the dashboard for Pulse Connect Secure.

Figure 2 Dashboard

Using the Dashboard

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

Dashboard Overview

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
Connect Secure	
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

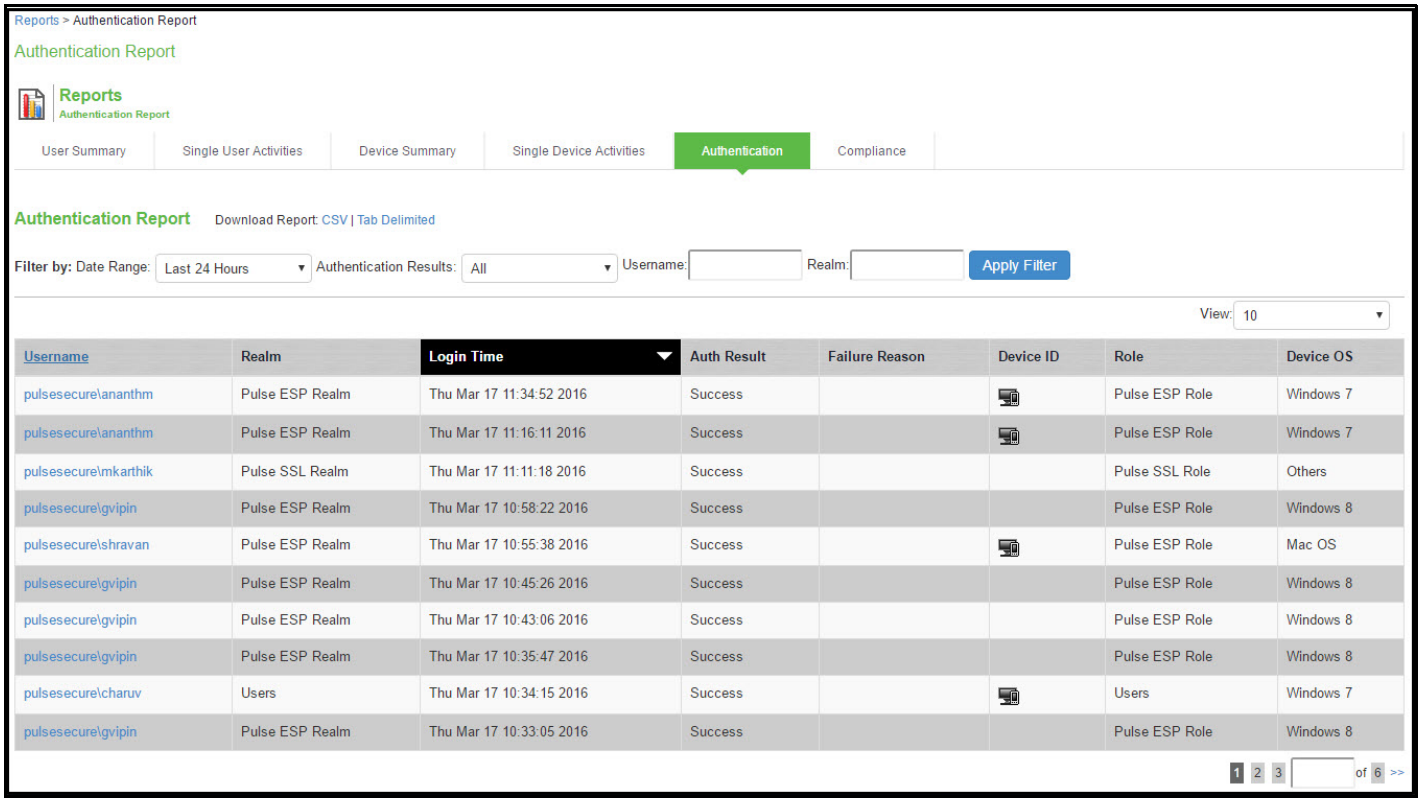
Drilling Down to Detailed Reports

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



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

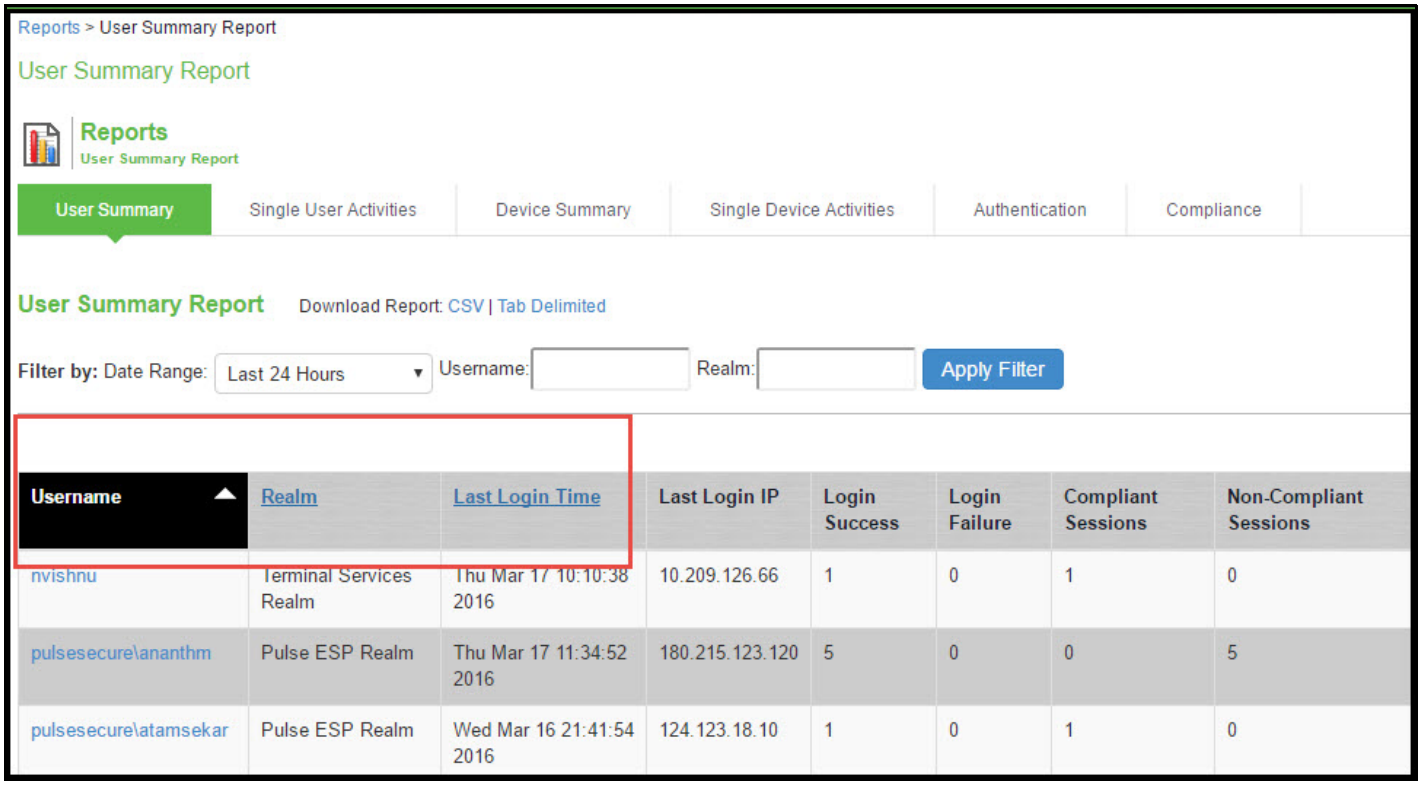


Table 4 describes the columns on the user summary report.

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.

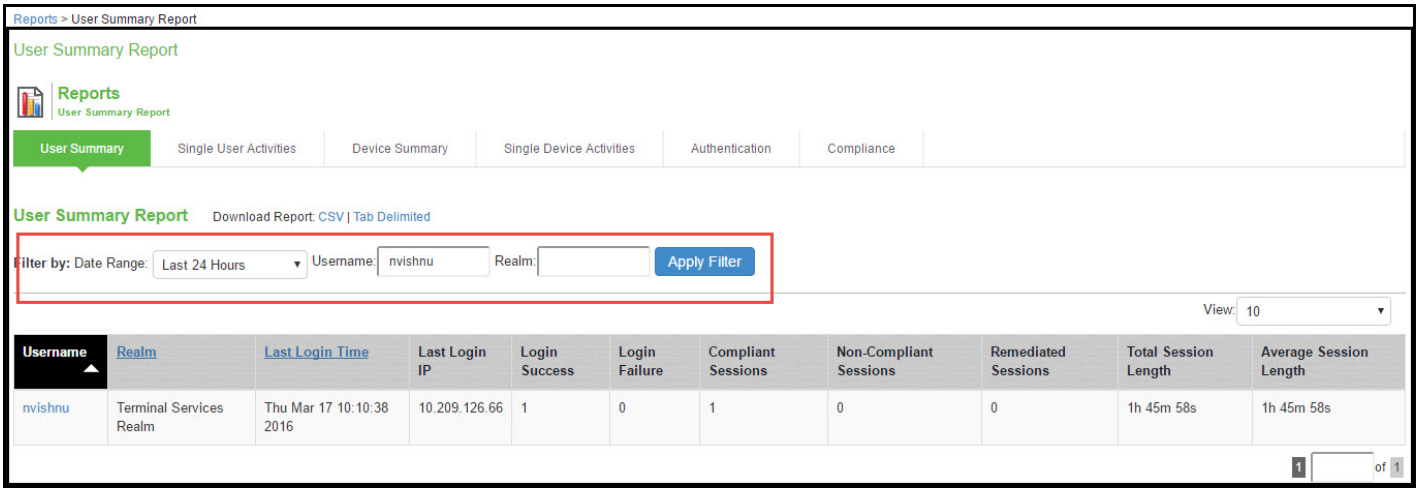
Applying Data Filters

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



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:

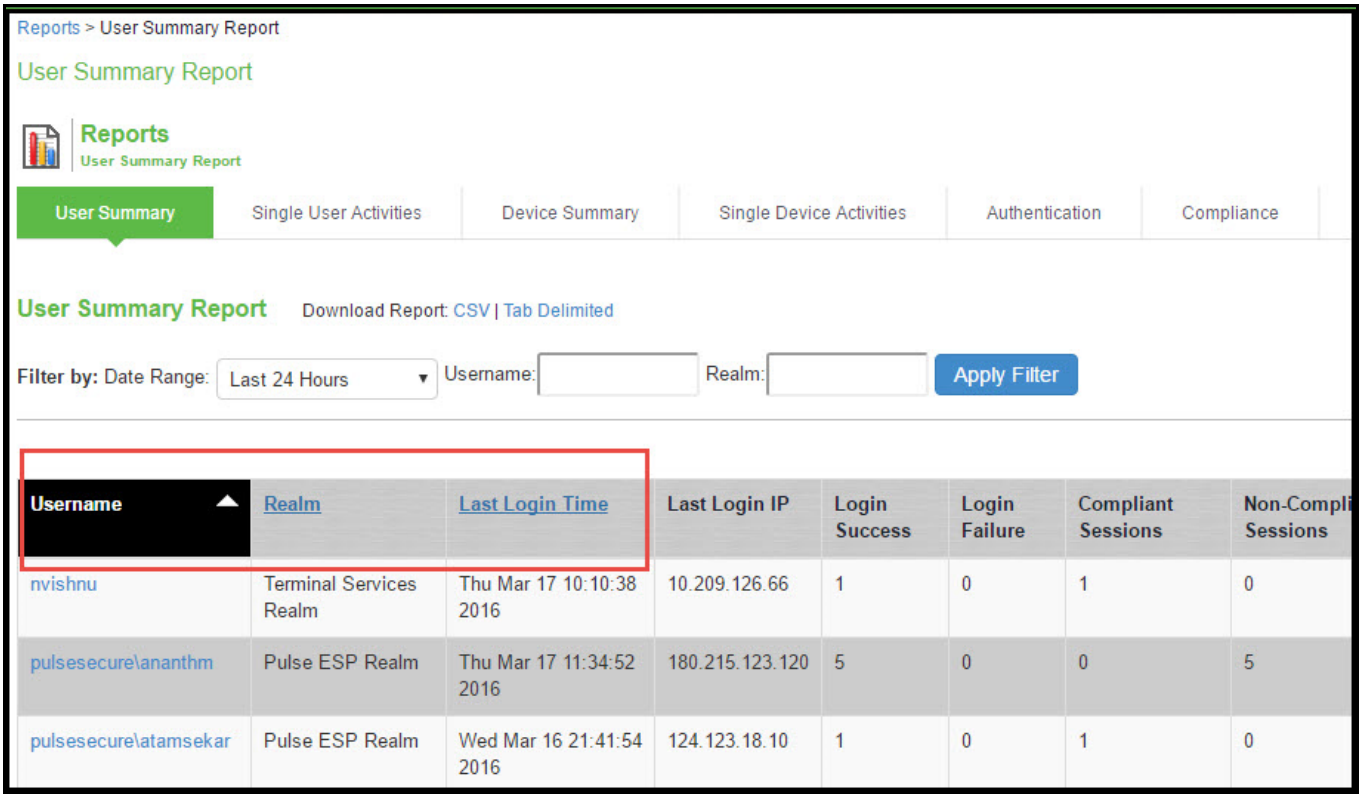
1. Select **System > Reports > User Summary.**
2. Select one of the following columns from the user summary report table and click either the ascending or descending order icon.
   - Username
   - Realm

- 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



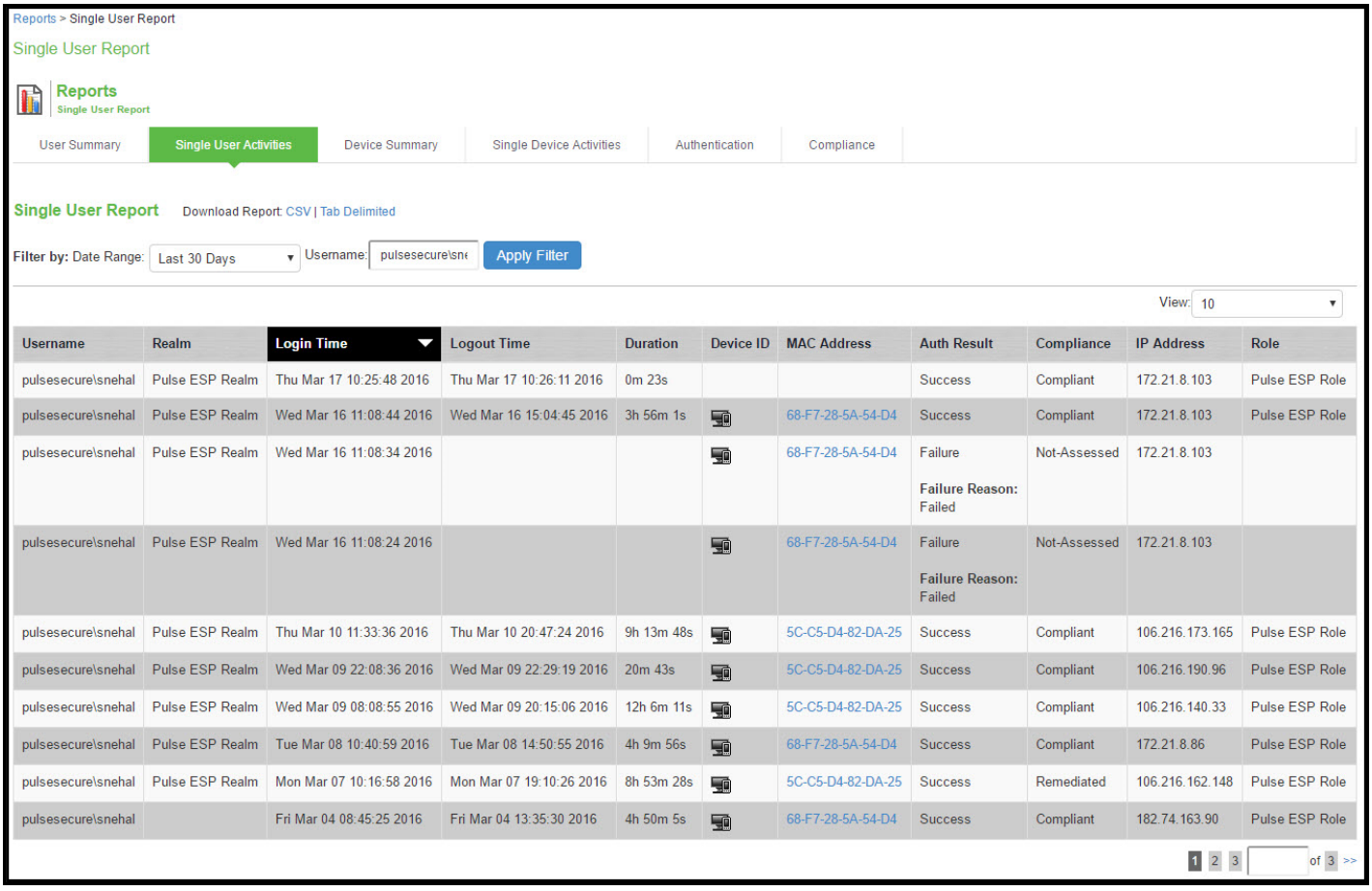
Drilling Down to the Single User Report

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



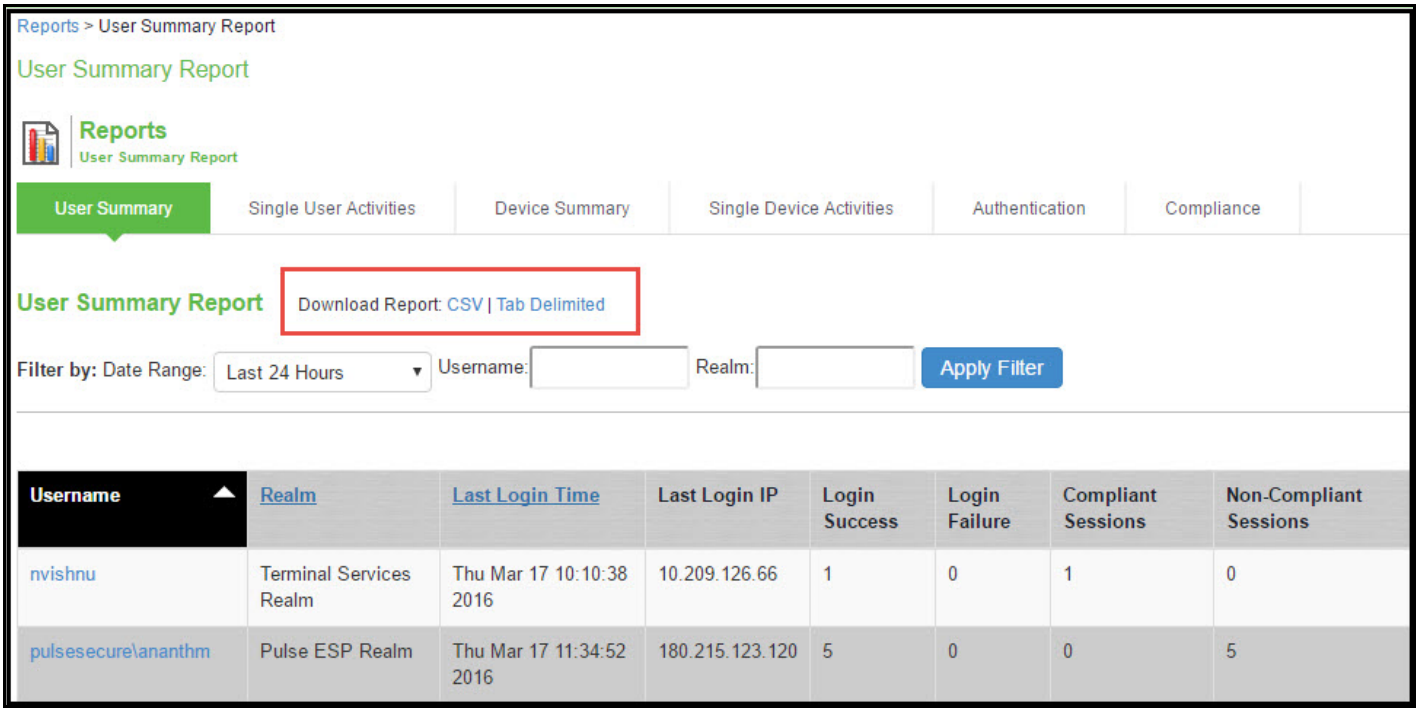
Exporting User Summary Report

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



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

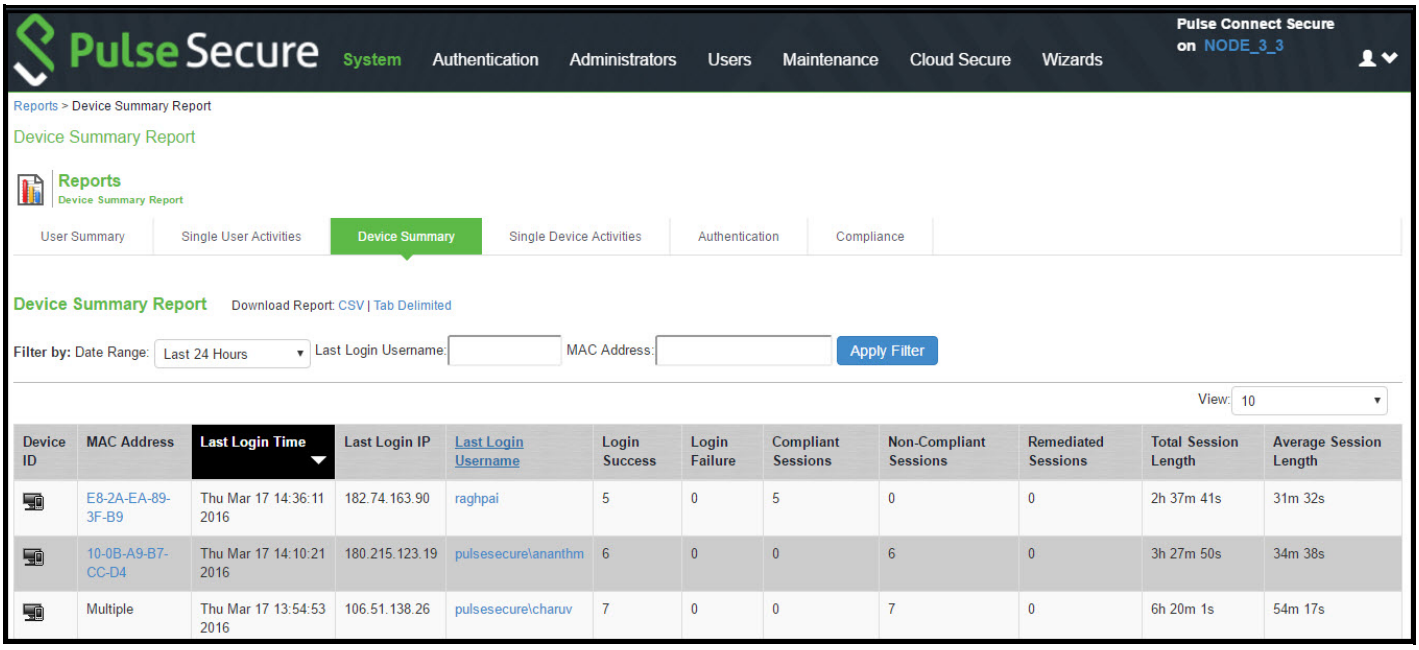


Table 5 describes the columns on the device summary report.

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.

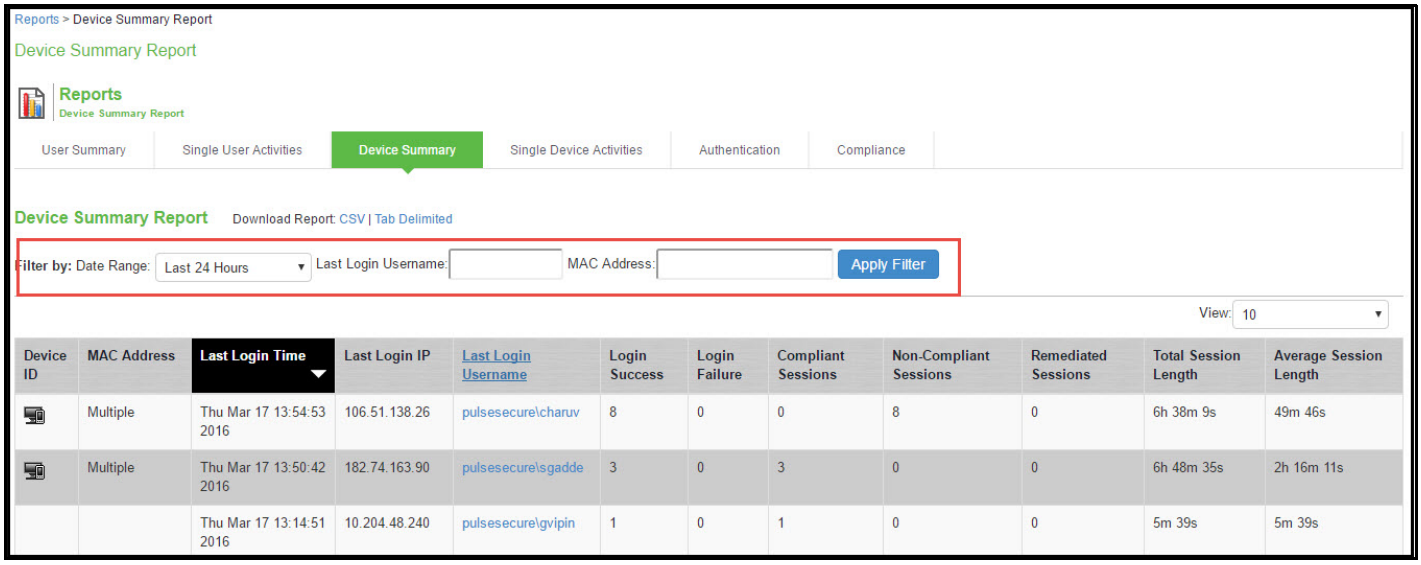
Applying Data Filters

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



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.

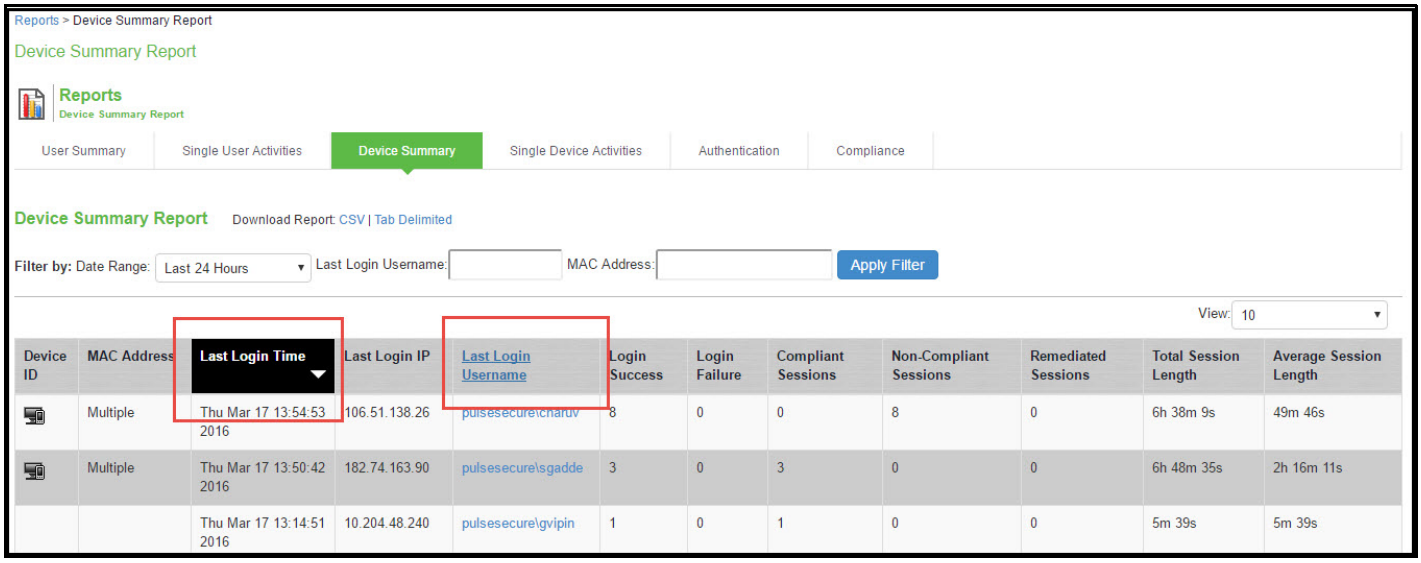
To sort the device summary report:

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



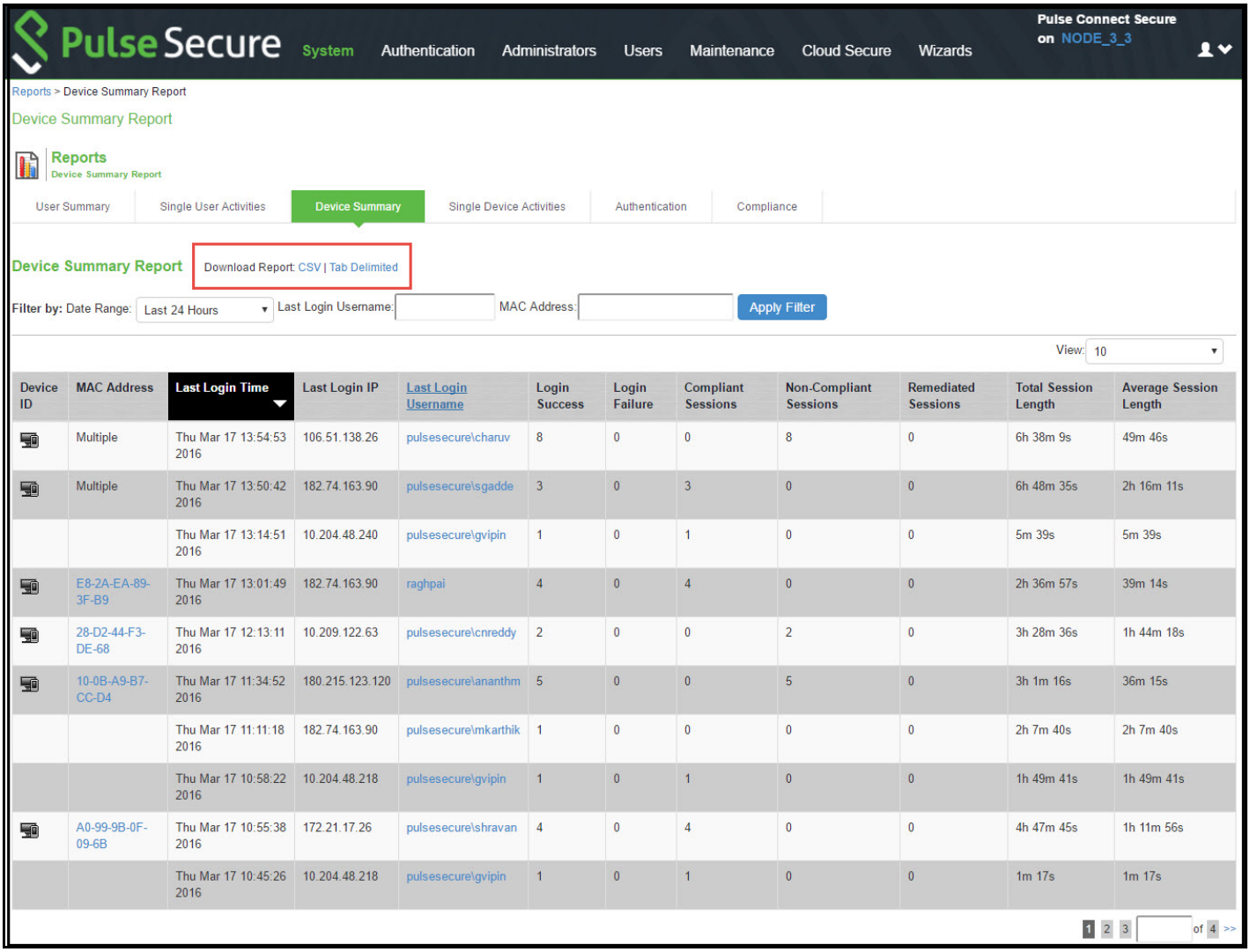
Exporting Device Summary Report

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



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

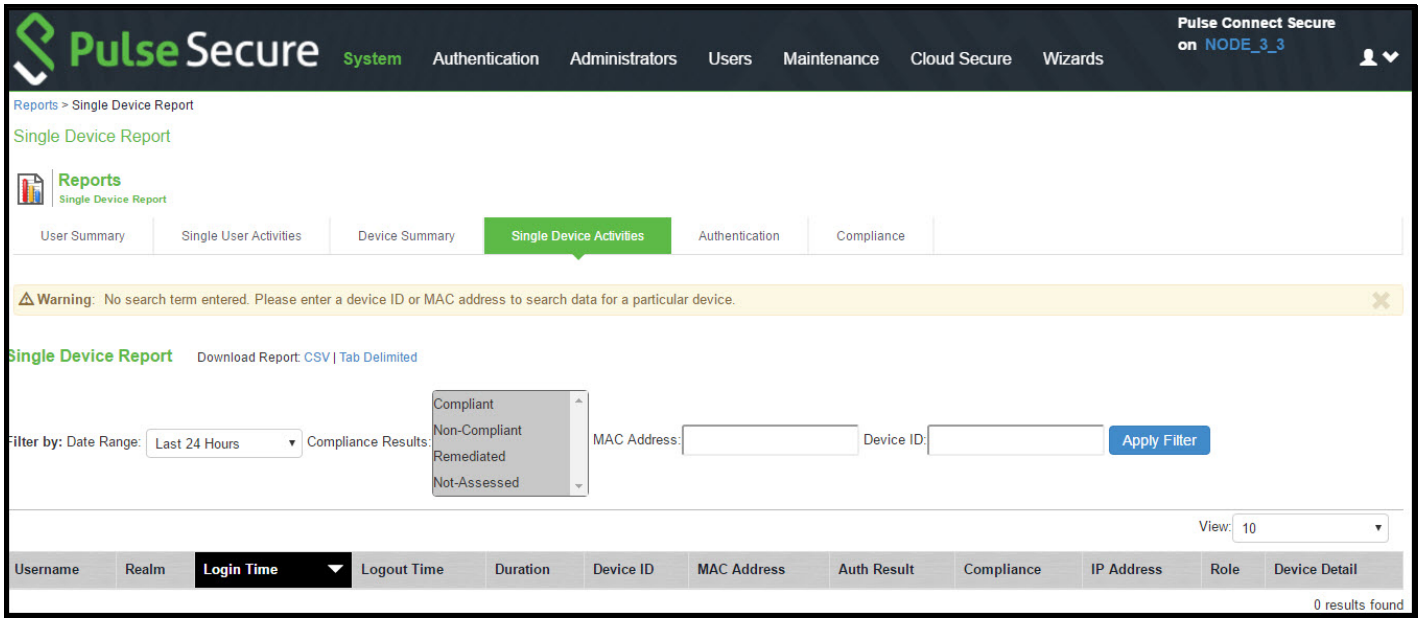


Table 6 describes the columns on the single device report.

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.

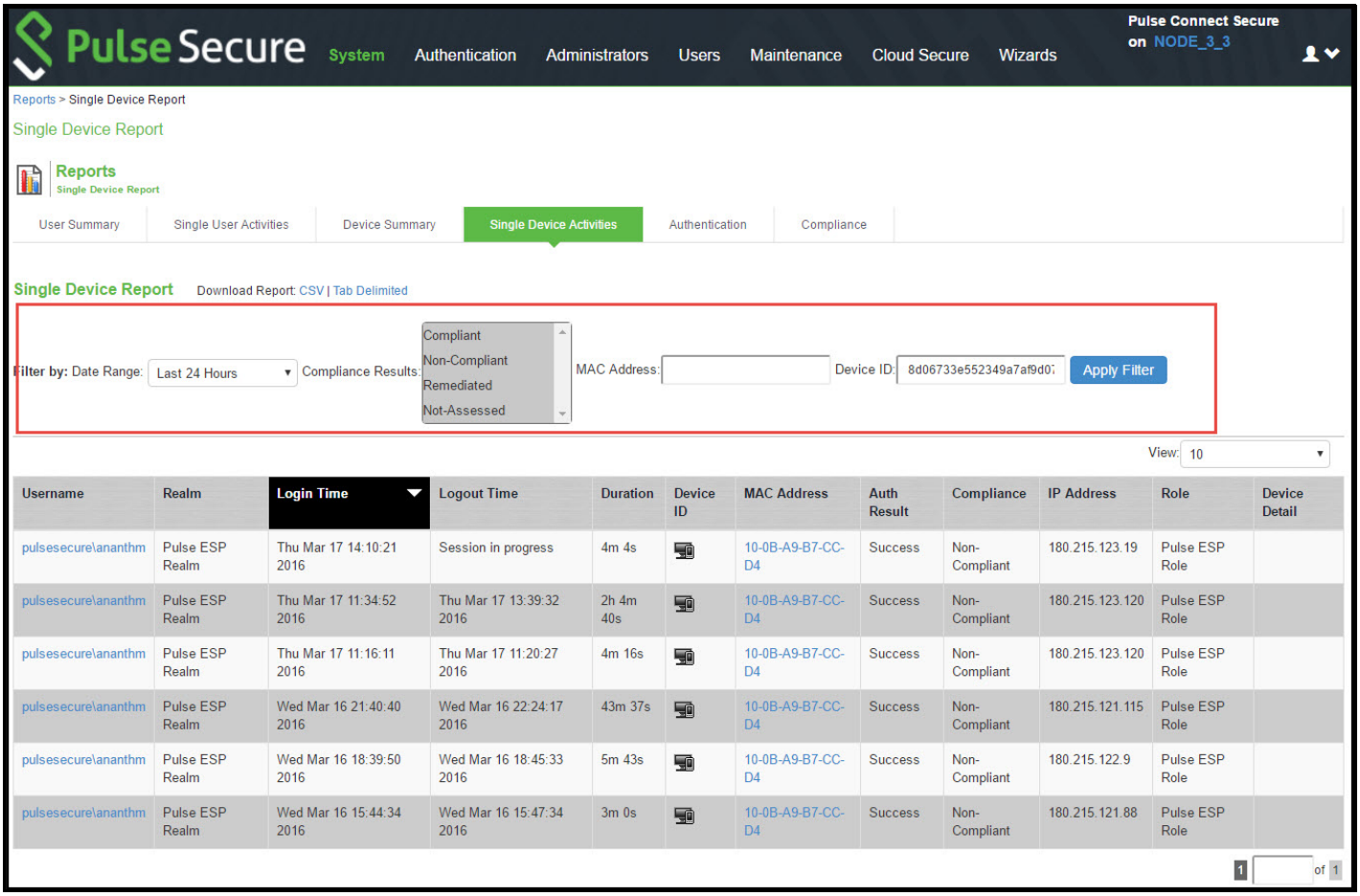
Applying Data Filters

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



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.

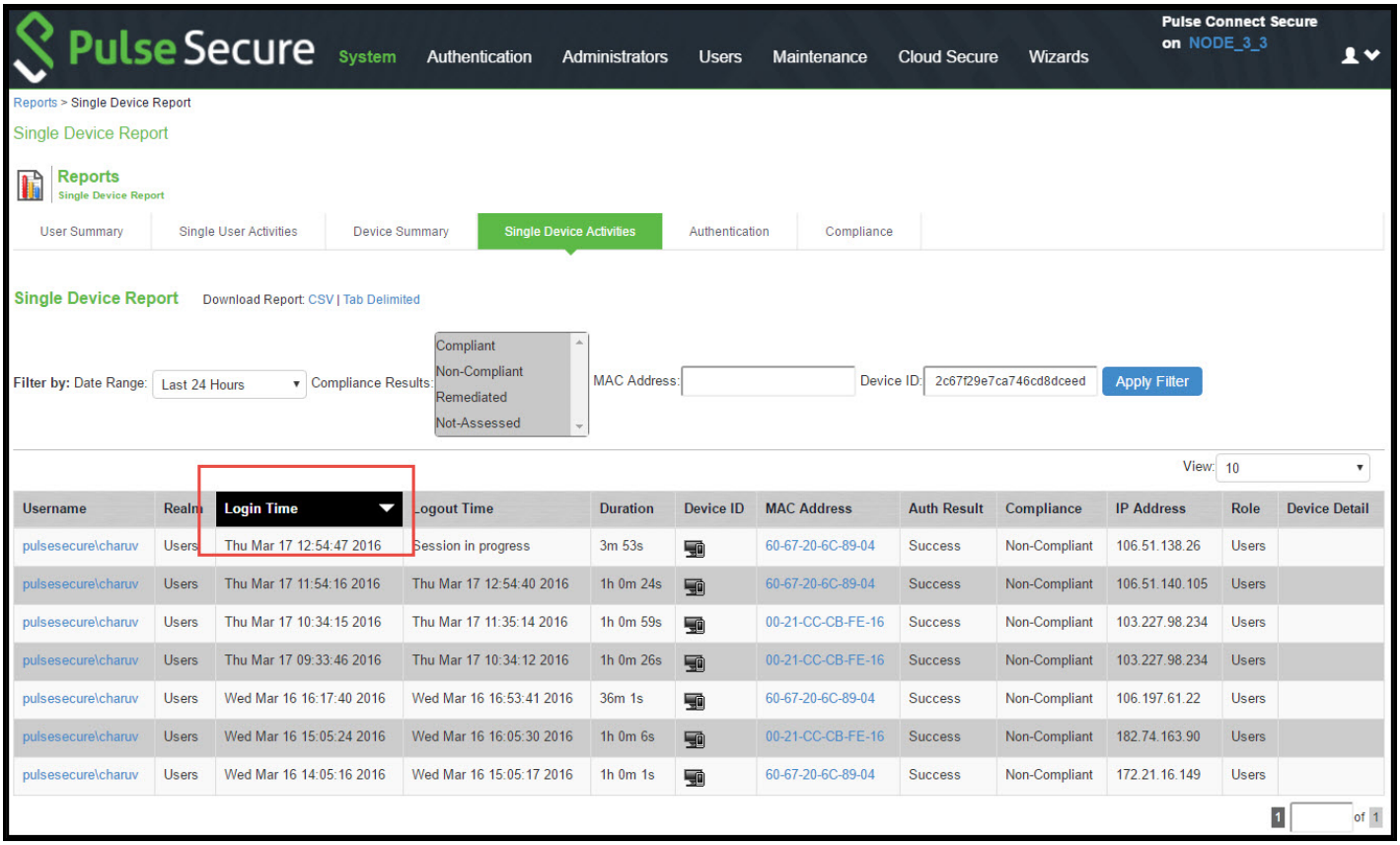
To sort the single device activities report:

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



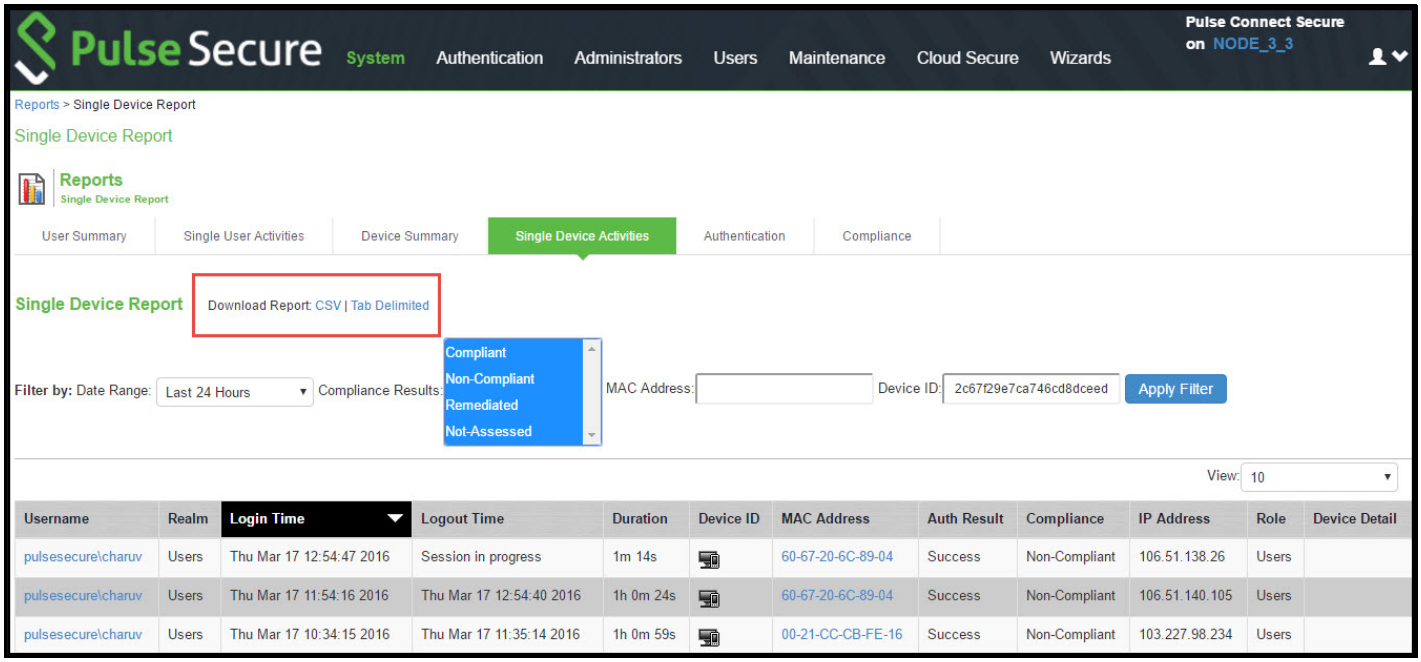
Exporting Single Device Activities Report

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



Using the Authentication Report

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

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

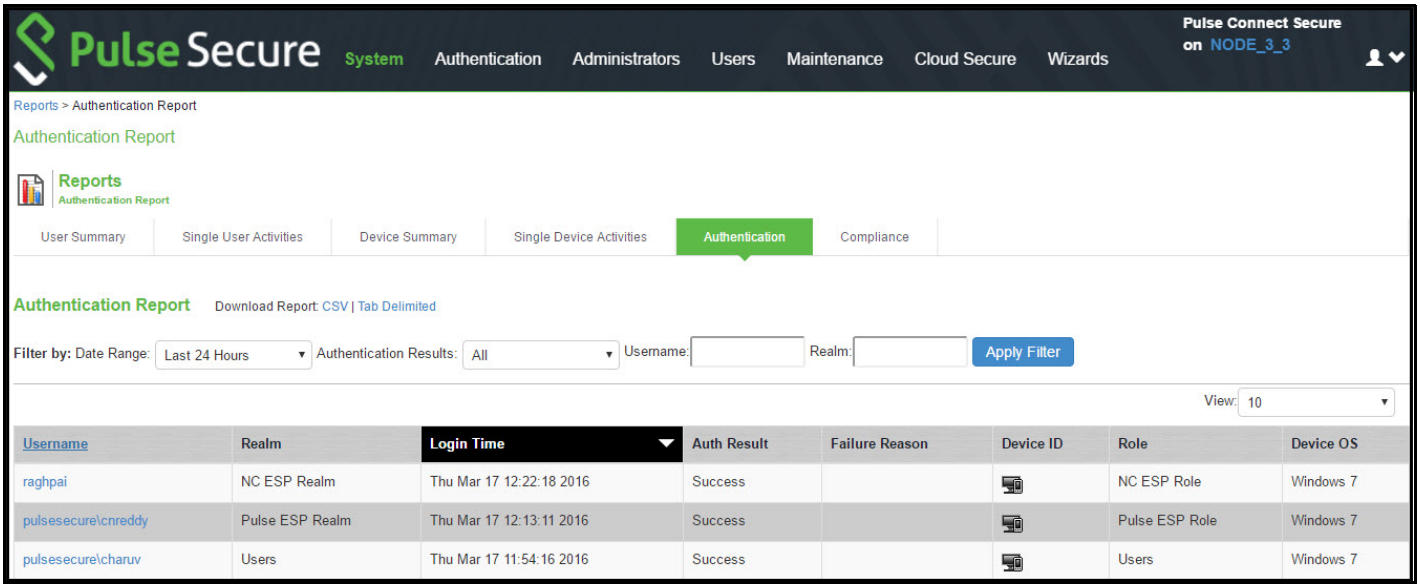


Table 7 describes the columns on the authentication report.

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:

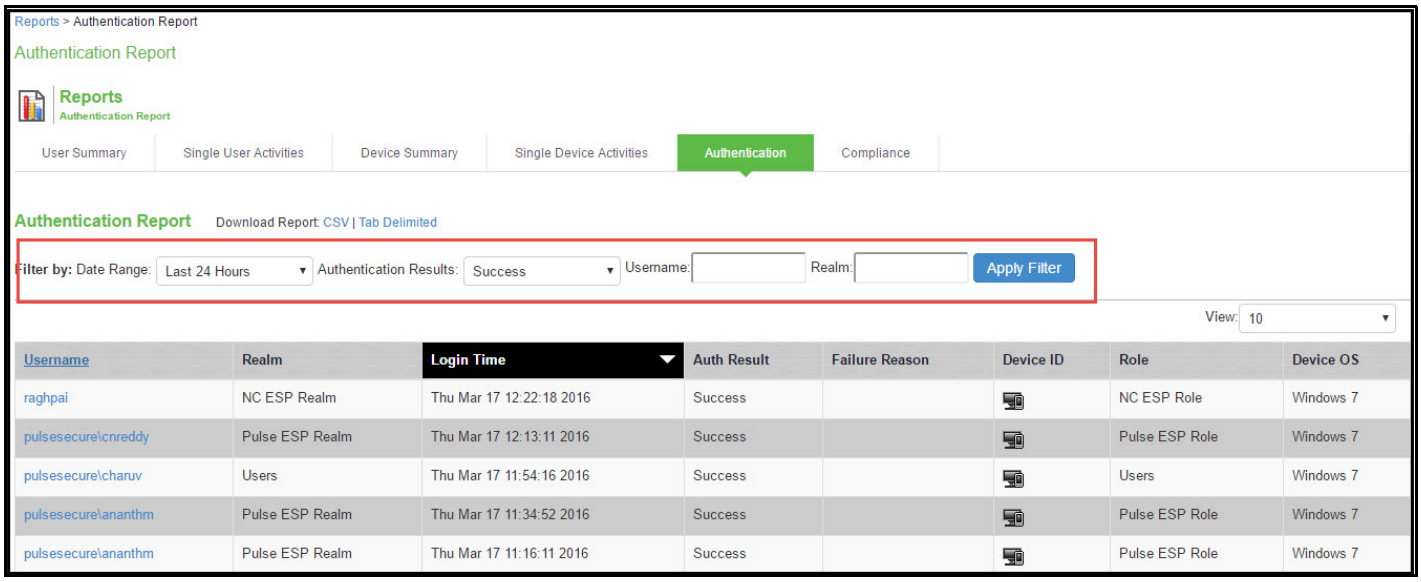
1. Select **System > Reports > Authentication.**
2. Select one of the following periods from the **Filter by: Date Range** list box:
   - **Last 24 Hours** - (Default) Refers to the last 24 hours from the current hour.

- **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



Sorting Records

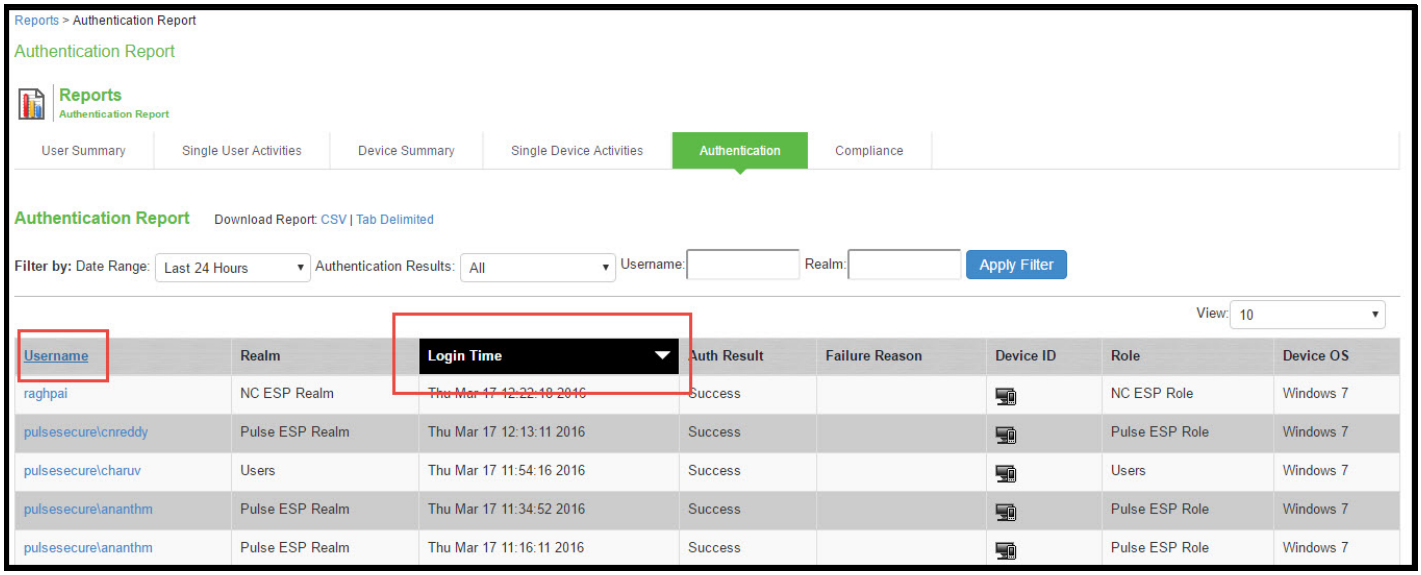
The data source determines the default sort order of the data rows in the report. Typically, data appears randomly, so sorting is an important task in creating a useful report. You can sort single data column.

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



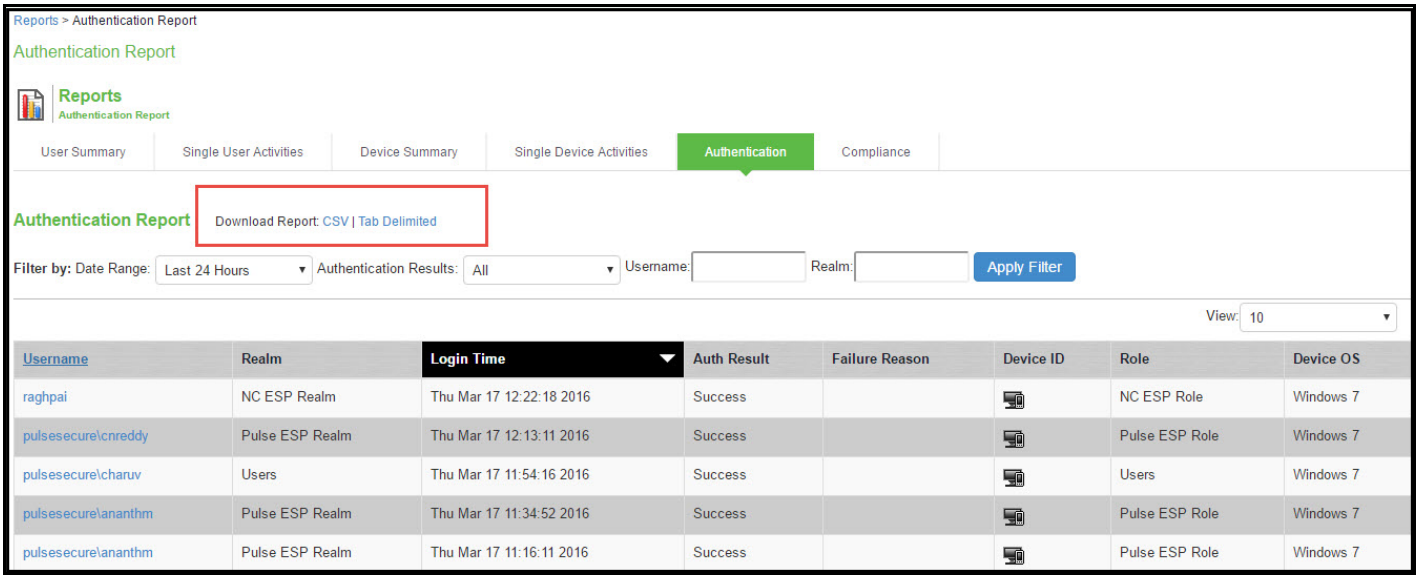
Exporting Authentication Report

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



Using the Compliance Report

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

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

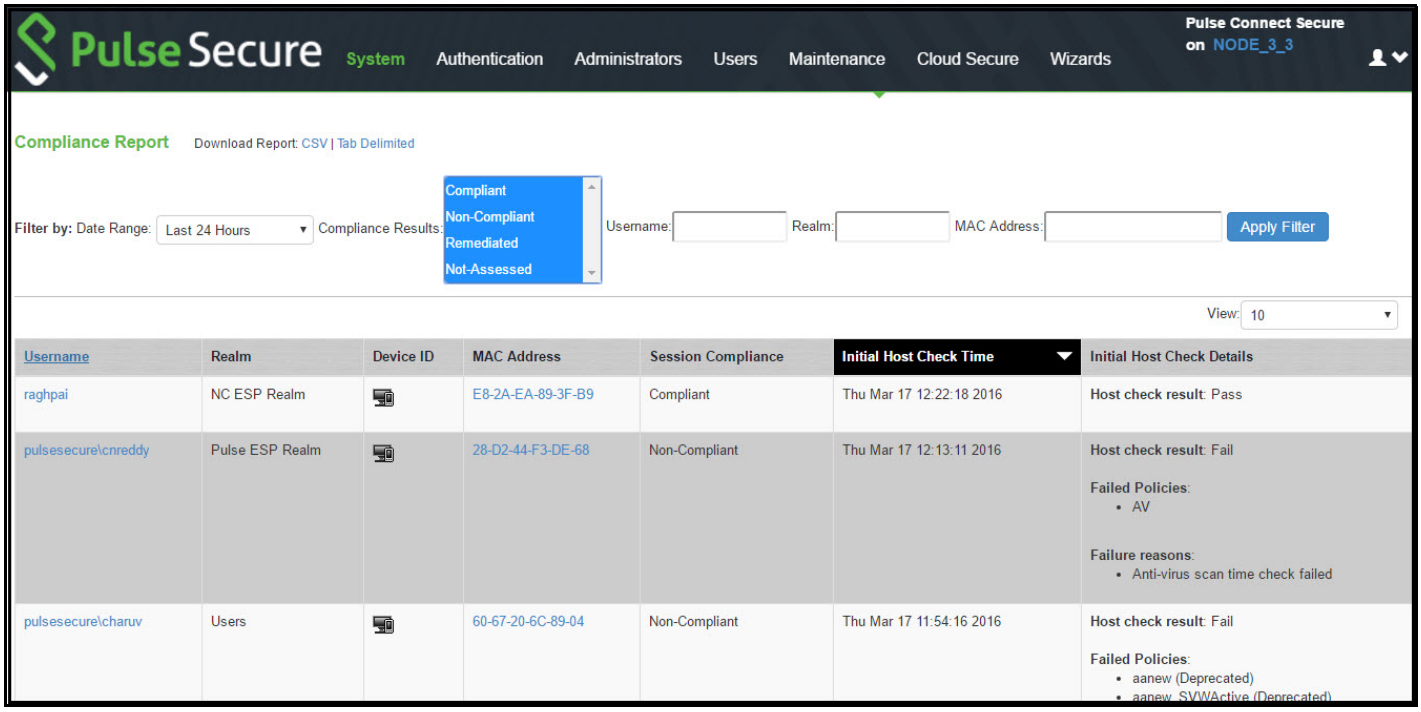


Table 8 describes the different columns on the compliance report.

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

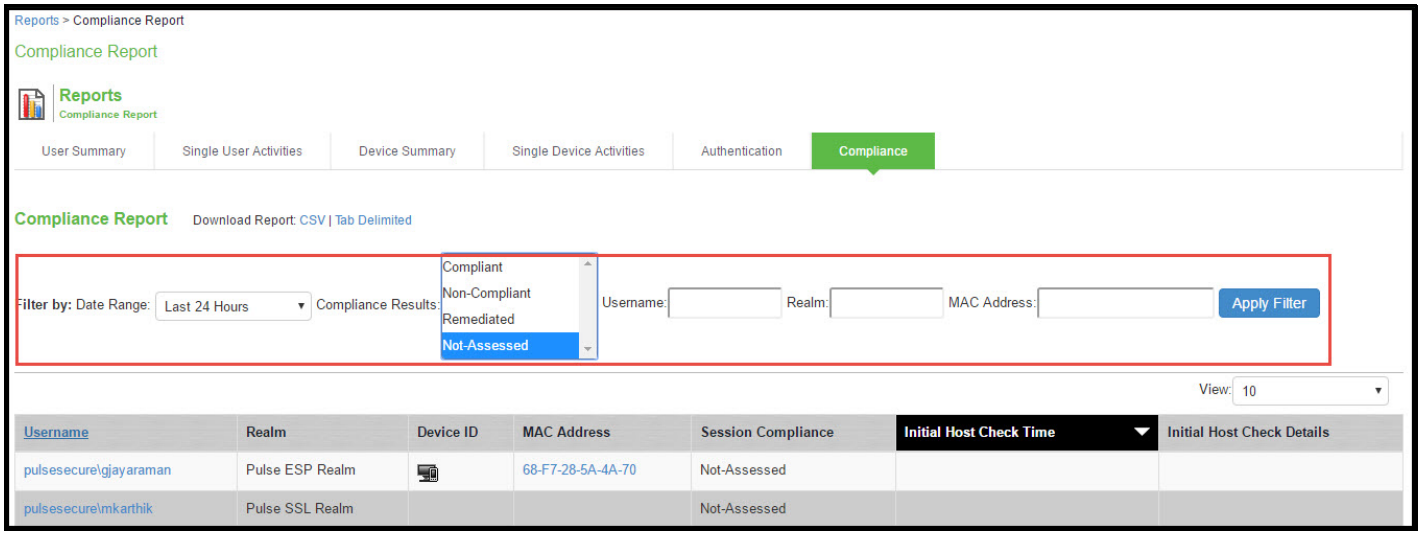
To apply a data filter:

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



Sorting Records

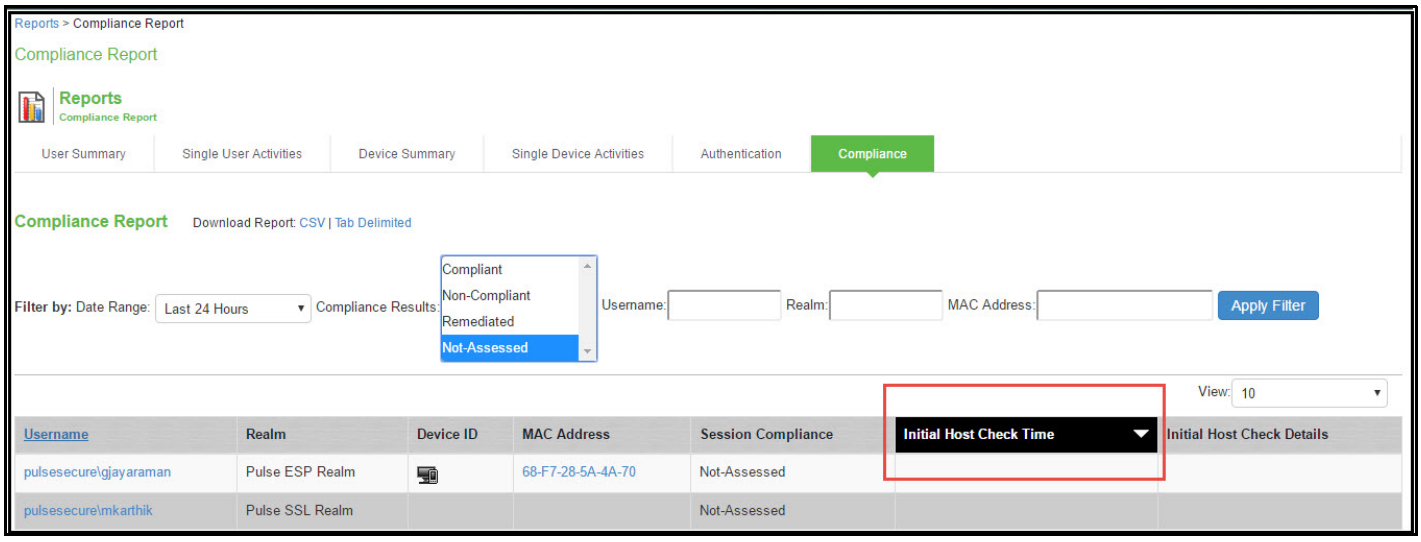
The data source determines the default sort order of the data rows in the report. Typically, data appears randomly, so sorting is an important task in creating a useful report. You can sort single data column.

To sort the compliance:

1. Select S**ystem > Reports > Compliance.**
2. Select I**nitial 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



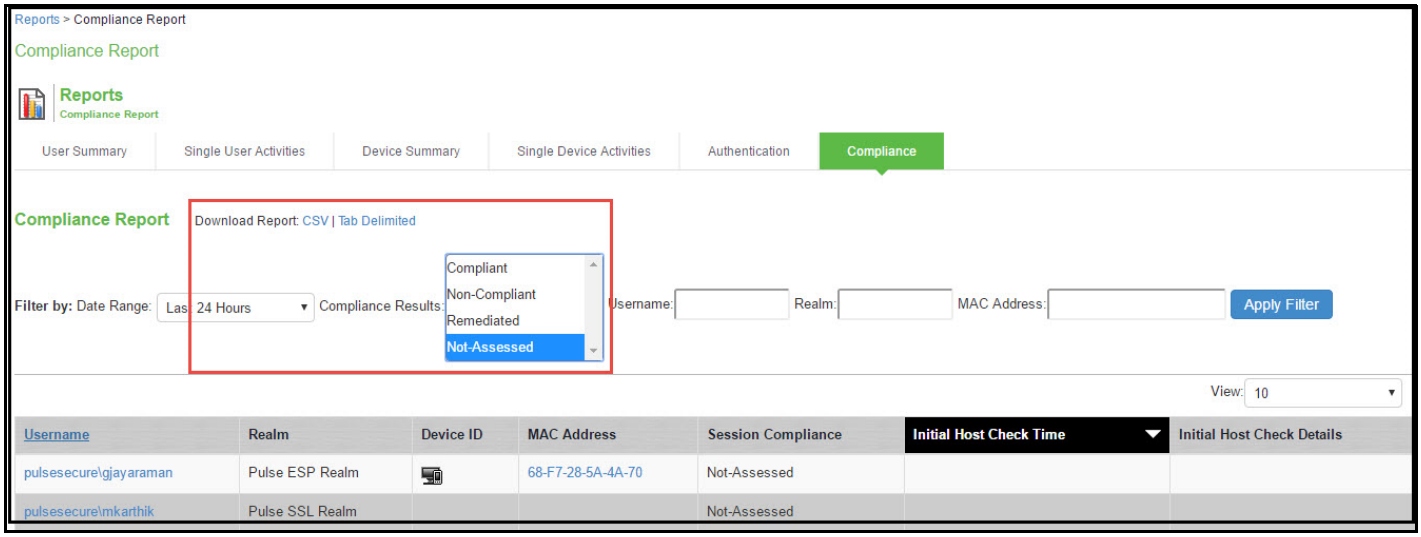
Exporting Compliance Report

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



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.