Integrating ClearPass Policy Manager and Splunk

Intro to the Aruba ClearPass App for Splunk Enterprise

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Author</th>
<th>Revision Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>May/July 2014</td>
<td>Premraj Lourdraj/ Sohag Desai</td>
<td>Initial Revision, Updates and Review</td>
</tr>
<tr>
<td>October 2014</td>
<td>Danny Jump</td>
<td>Final updates and Published Version #1</td>
</tr>
</tbody>
</table>
# Table of Contents

Copyright ........................................................................................................................................................ 6
Open Source Code........................................................................................................................................ 6

Introduction and Overview ................................................................................................................................ 7
ClearPass, Splunk and the ClearPass Splunk App........................................................................................... 7
Assumptions....................................................................................................................................................... 7
Types of Syslog.................................................................................................................................................. 8
Syslogs based on ClearPass internal modules, RADIUS or Auth Services ........................................... 8
Syslogs based on Session Logs, Audit Records and Event Records ..................................................... 9

Network Topology and Components..................................................................................................... 10

Configuring ClearPass to Send Syslogs to Splunk.................................................................................. 11
Adding Splunk as a Syslog Target ............................................................................................................. 11
Importing ClearPass Syslog Filters........................................................................................................... 12

Configure Splunk to receive Syslogs from ClearPass.............................................................................. 14
Adding a Data Input...................................................................................................................................... 14
Installing the ClearPass Splunk App on Splunk...................................................................................... 17
Uploading the ClearPass Splunk App package......................................................................................... 17

Configuring Error Code to Error String Lookup Settings .................................................................... 19
Configuring EMM/MDM Data Polling Script............................................................................................. 21

ClearPass Splunk App Dashboard Elements ........................................................................................... 24
Overview........................................................................................................................................................... 24
Authentications.................................................................................................................................................. 25
Authentication Overview............................................................................................................................. 25
Failure by Error Types................................................................................................................................ 26
Failure Distribution....................................................................................................................................... 28
Search ............................................................................................................................................................ 50
Syslog Raw Data .................................................................................................................................................... 50
Failed Authentication Raw Data .......................................................................................................................... 50
Successful Authentication Raw Data .................................................................................................................... 51
Event Log Raw Data ............................................................................................................................................. 51
Audit Log Raw Data ............................................................................................................................................. 51
Caveats ................................................................................................................................................................... 51
Checking Splunk is receiving Syslog Data from CPPM ....................................................................................... 52

Table of Figures
Figure 1 - Example of Syslogs based on internal ClearPass modules ................................................................. 8
Figure 2 - Example of Syslog: Session Logs ......................................................................................................... 9
Figure 3 - Example of Syslog: Audit Records ...................................................................................................... 9
Figure 4 - Example of Syslog: System Events ..................................................................................................... 9
Figure 5 - Network Topology and Component Interaction .................................................................................. 10
Figure 6 - Adding Syslog Targets to ClearPass ................................................................................................. 11
Figure 7 - Importing Syslog Export Filters into ClearPass ................................................................................. 12
Figure 8 - List of Syslog Export Filters after Import ......................................................................................... 13
Figure 9 - Splunk Data Input Page ................................................................................................................... 14
Figure 10 - Splunk UDP Data Input Page ........................................................................................................ 15
Figure 11 - Splunk Data Input UDP Add new Page .......................................................................................... 15
Figure 12 - Splunk UDP Summary Table Page .............................................................................................. 16
Figure 13 - Splunk Manage Apps Page ........................................................................................................... 17
Figure 14 - Splunk Upload App Page ................................................................................................................ 18
Figure 15 - Splunk Upload App Page (after upload) ....................................................................................... 18
Figure 41 - System > System Monitor ................................................................. 42
Figure 42 - System > System Events ................................................................. 43
Figure 43 - System > Audit Records ................................................................. 44
Figure 44 - System > License Usage > Policy Manager License Indicator ........ 45
Figure 45 - System > License Usage > Guest License Indicator ..................... 46
Figure 46 - Search > Generic Query Textbox ................................................... 47
Figure 47 - Search > Generic Query Dropdown .............................................. 49
Figure 48 - Search > Search ......................................................................... 50
Figure 49 - Splunk Event Dashboard Element Showing Incomplete Description Field .................................................. 52
Figure 50 - Checking Syslog events are being received by Splunk .................. 52

Copyright
© 2014 Aruba Networks, Inc. Aruba Networks’ trademarks include Aruba Networks®,
Aruba The Mobile Edge Company® (stylized), Aruba Mobility-Defined Networks™, Aruba
Mobility Management System®, People Move Networks Must Follow®, Mobile Edge
Architecture®, RFProtect®, Green Island®, ETips®, ClientMatch™, Virtual Intranet
Access™, ClearPass Access Management Systems™, Aruba Instant™, ArubaOSTM,
xSecTM, ServiceEdge™, Aruba ClearPass Access Management System™, Airmesh™,
AirWave™, Aruba Central™, and “ARUBA@WORK™. All rights reserved. All other
trademarks are the property of their respective owners.

Open Source Code
Certain Aruba products include Open Source software code developed by third parties,
including software code subject to the GNU General Public License (GPL), GNU Lesser
General Public License (LGPL), or other Open Source Licenses. The Open Source code used
can be found at this site: http://www.arubanetworks.com/open_source
Introduction and Overview

This document describes how to integrate ClearPass Policy Manager with Splunk and install the add-on Aruba ClearPass App for Splunk in order to extract maximum efficiency from both applications. Specifically, it provides information on:

- How to configure ClearPass to send Syslog output to an instance of Splunk
- How to configure Splunk to receive data from one or more ClearPass servers
- How to install and configure the ClearPass Splunk App on Splunk

After completion of these steps, the ClearPass Splunk App will display charts and tables showing ClearPass events captured from Syslog messages sent by ClearPass Policy Manager. The document also provides screenshots of every menu item and dashboard element and explains what they represent.

**Note:** Where you see a red-chili this is to signify a ‘hot’ important point and highlights that this point is to be taken as a best-practice recommendation.

ClearPass, Splunk and the ClearPass Splunk App

ClearPass Policy Manager is an Access security solution used extensively in small, midrange and large enterprises. ClearPass provides the capability to send various kinds of Authentication, Authorization and Accounting events as RFC 5424 compliant Syslog messages to any Syslog receiver when endpoints authenticate to the network.

Splunk is a log management/SIEM solution that can receive Syslog messages from multiple sources. These messages are stored within Splunk and then can be correlated, searched, analyzed and displayed using its graphical user interface.

Splunk is also a platform that runs mini-applications (Apps) as add-ons to Splunk, which are customized for specific external applications or products which send Syslogs. The App provides visualization of the received data without requiring the user to run complex searches within Splunk.

These apps typically consist of a number of dashboard elements like charts, tables and graphs that are accessible via a menu structure contained within the app, which are based on pre-defined searches. The ClearPass Splunk App is such an App and was developed by Aruba for visualizing a Syslog feed from ClearPass Policy Manager.

Assumptions

The audience for this document is assumed to be familiar with the administration and use of ClearPass Policy Manager and Splunk applications.
Types of Syslog

ClearPass can generate two different types of Syslog feeds:

1. **Syslogs based on logs generated by internal ClearPass modules.** This can be configured by clicking on **Administration >> Server Manager >> Log Configuration** in ClearPass.
   - These are logs from ClearPass internal modules like the RADIUS Server or ClearPass Authentication Request services.

2. **Syslogs based on Access Tracker events, System events and Audit records.** These can be configured by clicking on **Administration >> External Servers >> Syslog Export Filters** in ClearPass.
   - These are the logs defined in Data Filters, which will be discussed later in this document.

### Syslogs based on ClearPass internal modules, RADIUS or Auth Services

While you can setup Splunk to receive Syslog messages based on ClearPass internal modules, we are going to ignore them in this document as they are not particularly useful for admin users. Here are some examples of these types of Syslog messages:

```
Mar 27 12:01:40 10.17.6.54 2014-03-27 12:00:15,315 [main] DEBUG RadiusServer.Radius - Module: Loaded SQL
Mar 27 12:01:40 10.17.6.54 2014-03-27 12:00:15,315 [main] DEBUG RadiusServer.Radius - sql: driver = "rlm_sql_unixodbc"
Mar 27 12:01:40 10.17.6.54 2014-03-27 12:00:15,316 [main] DEBUG RadiusServer.Radius - sql: driver = "PostgreSQL"
Mar 27 12:01:40 10.17.6.54 2014-03-27 12:00:15,316 [main] DEBUG RadiusServer.Radius - sql: login = "appuser"
Mar 27 12:01:40 10.17.6.54 2014-03-27 12:00:15,316 [main] DEBUG RadiusServer.Radius - sql: password = "(encstring)"
```

---

Figure 1 - Example of Syslogs based on internal ClearPass modules
Syslogs based on Session Logs, Audit Records and Event Records

For the purposes of this document, we will only discuss integration of ClearPass Syslog data based on:

- Session logs – these can be seen in the ClearPass Access Tracker
- Audit records – these can be seen in the ClearPass Audit Viewer
- Event records – these can be seen in the ClearPass Event Viewer

Figure 2, 3 and 4 show examples of these three log types. Note that the Syslog payload is sent as name/value pairs.

This document will explain how to configure ClearPass to send these three types of log messages; namely, Session logs, Audit records and System events, to Splunk.
Network Topology and Components

Figure 5 shows some examples of network components that interact with Splunk. ClearPass (with Syslog Filters configured) is shown as one of the Syslog senders.

To integrate ClearPass with Splunk, three major tasks which are covered in the next three sections must be performed:

1. Configure ClearPass to send Syslogs to Splunk
2. Configure Splunk to receive Syslog data feed from ClearPass
3. Install and configure the ClearPass Splunk App on a Splunk Server
Configuring ClearPass to Send Syslogs to Splunk

**Note:** The configuration steps described in this section were tested using ClearPass 6.3.2 & 6.4.1. However these steps should work for any 6.3 or 6.4 version of ClearPass.

Configuration consists of the following steps:

- Adding a Splunk Server as a Syslog Target.
- Importing the ClearPass Syslog Export Filters defined for the ClearPass Splunk App into ClearPass, after modifying them first to use the Splunk Server hostname or IP address.

### Adding Splunk as a Syslog Target

First, add an instance of Splunk to ClearPass as a Syslog target. To do this, add the Splunk IP address or hostname and port number at the appropriate place in the ClearPass administrative interface.

1. Navigate to **Administration >> External Servers >> Syslog Targets** and click on **Add**.
2. In the popup window, enter the requested details, namely:
   - **Host Address:** Splunk server IP address or hostname
   - **Description:** (Optional) Description of the Splunk device
   - **Protocol:** Syslog protocol type (UDP/TCP)
   - **Server Port:** 514

   The protocol type (UDP/TCP) and the port number (514) should match the values that you will set in Splunk (see the next section).

3. Click on **Save** and verify that your settings have been saved correctly.

![Figure 6 - Adding Syslog Targets to ClearPass](image)
Importing ClearPass Syslog Filters

Next, import the export filters provided in the *SyslogExportData_for_Splunk.xml* file, which is part of the ClearPass Splunk App bundle into ClearPass. It is also available to download from the Aruba support site [here](#).

1. Extract the file *SyslogExportData_for_Splunk.xml* from the ClearPass Splunk App bundle or download it from the above link and save it to your local disk.
2. Using a text editor, locate all instances of *Change.me* in the extracted file and replace them with the hostname or IP address of the Splunk server configured on ClearPass and save it.
4. In the popup window, click on the Choose File button, browse to the location where you saved the *SyslogExportData_for_Splunk.xml* file, suitably modified as mentioned in step 2, and select the file.

![Figure 7 - Importing Syslog Export Filters into ClearPass](image)

Figure 7 - Importing Syslog Export Filters into ClearPass
5. **Click on Import** and verify that the following Syslog filters have been imported correctly – see Figure 8:

![List of Syslog Export Filters after Import](image)

**Figure 8 - List of Syslog Export Filters after Import**
Configure Splunk to receive Syslogs from ClearPass

**Note:** The configuration steps described in this section were tested on Splunk 6.1.1, we are currently testing our application with Splunk 6.2 and will update the documentation and app as appropriate.

Configuring Splunk consists of the following, performed in order:

- Adding a TCP or UDP Data Input to Splunk while ensuring that:
  - Port number matches the value entered in ClearPass when adding Splunk as a Syslog target
  - Source Type is set to Aruba:CPPM:Syslog
- Installing the ClearPass Splunk App on your Splunk server
- Configuring error-code-to-error-string lookup settings

### Adding a Data Input

1. Navigate to Settings >> Data >> Data Input. Click on the link UDP (or TCP).

![Figure 9 - Splunk Data Input Page](image)
2. From the UDP (or TCP) page, click on the **New** button.

![Figure 10 - Splunk UDP Data Input Page](image)

3. From the **Add new** page, enter the requested details, namely:
   - **UDP Port**: Enter 514 or the same port as you entered in ClearPass when adding Splunk
   - **Source name override**: Leave this field blank
   - **Set sourcetype**: Select **Manual** from the dropdown list
   - **Source type**: Enter **Aruba:CPPM:Syslog**

![Figure 11 - Splunk Data Input UDP Add new Page](image)

4. Click **Save** and verify that your details appear correctly in the **Data inputs > UDP** table.
Figure 12 - Splunk UDP Summary Table Page

This concludes the required configuration of Splunk for integration with ClearPass for receiving all Syslog information fields from ClearPass.
Installing the ClearPass Splunk App on Splunk

**Note:** The steps described in this section were tested on Splunk 6.1.1.

Installing the Clear Pass Splunk App consists of:

- Uploading the ClearPass Splunk App package from your computer into Splunk
- Restarting your Splunk server

**Uploading the ClearPass Splunk App package**

1. Navigate to **Apps >> Manage Apps**. Click on the **Install app from file** button.

![Figure 13 - Splunk Manage Apps Page](image)

2. From the **Upload app** page, click on **Choose File**. Locate the file `ClearPassOnSplunk_1.2.tar.gz` (assuming the version of the ClearPass Splunk app is 1.2), on your computer and select it. Click the **Upload** button.

**Note:** If you are upgrading your ClearPass Splunk app to a later version, select the checkbox labelled **Upgrade app**.

**Note:** If the version of app is different from 1.2, locate and select the appropriate file.
3. Restart Splunk to complete the install. Click on the **Restart Splunk** button.

After restarting and logging in to Splunk again, the ClearPass Splunk App will appear in the Splunk Home page (see Figure 16).
Configuring Error Code to Error String Lookup Settings

As a part of the ClearPass Splunk application, we have included an error file lookup table. This allows Splunk to translate to the user an error_string rather than a basic error-code. An error code of ‘6204’ is quite meaningless, but through this section of configuration we would return to the user ‘No enforcement profiles matched to perform command authorization’.

1. Navigate to Settings >> Knowledge >> Lookups. Click on Automatic lookups.

2. From the Automatic lookups page, from the App context dropdown list, select Splunk for ClearPass (assuming the version number of the App is 2.0). Click on New.
3. From the Add new page enter the following and then click the Save button:
   - **Name**: Enter [relevant name] i.e. ClearPass on Splunk
   - **Lookup table**: Select error_code_lookup from the dropdown list
   - **Apply to**: Select sourcetype from the dropdown list
   - **Named**: Enter Aruba:CPPM:Syslog
   - **Lookup input fields**: Enter error_code = error_code
   - **Lookup output fields**: Enter error_code_str = error_code_str

As an example, see below for an error-code-str where we display the message ‘Access denied by Policy’, rather than an error code of ‘206’.

This concludes the configuration of the error-code-to-error-string-lookup settings.
Configuring EMM/MDM Data Polling Script

Where a customer is ingesting EMM/MDM endpoint attributes into ClearPass we can export some of this valuable information into our Splunk ClearPass application, to allow the end-user to leverage the reporting power of Splunk.

To configure this feature follow this next section. If the enduser does not utilize EMM/MDM within their ClearPass deployment this section can be ignored.

During the installation of the ClearPass application Splunk extracts a shell script that we can utilize to have Splunk ingest these additional endpoint attributes. However prior to point Splunk at the script, we need to modify the default script to provide it with the IP address of the ClearPass Publisher and provide some credentials the script can use to access a ClearPass Publisher.

For Linux the script is located generally in the following location. This will vary based upon where you installed Splunk. For our installation and as to provide an example you need to edit the mdm.sh file located here `/opt/splunk/etc/apps/ClearPassOnSplunk_2/bin/mdm.sh`

Use your favorite editor and edit the following lines. **Make a copy of the file before you edit it.**

```
# List of ClearPass servers
# svrs="changeme_servers_list"
svrs="10.2.100.150 10.2.100.151"

for cphost in $svrs
do

# wget  -q -O $of  --http-password=passwd_here --http-user=apisplunk –
# no-check-certificate https://$cphost/tipsapi/config/fetch/Endpoint

wget -q -O $of  --http-password=password_here --http-user=apisplunk --
no-check-certificate https://$cphost/tipsapi/config/fetch/Endpoint
```

**Figure 21 - Editing mdm.sh to add ClearPass Publisher details**

We are only interested in the highlighted **red** lines above. Copying these lines as a reference is good practice as shown above.

Ensure that the IP address’s of svrs is enclosed in double literals. Notice, in our example above we provided two IP addresses for the ClearPass servers. If you have multiple nodes you want to ingest data from ensure they are listed and separated by a space.

**Note:** For nodes in the same cluster, only the Publisher needs to be added.
Also for the two highlighted attributes on the wget command, the user apisplunk must be created within the ClearPass system. We recommend that you create a RO Admin account under Administration-> Users and Privileges -> Admin Users

**Note:** You can use any name you want, we just recommend creating a new RO account and not using the built in admin account.

![Creating a RO Admin user 'apisplunk' on ClearPass](image)

Once the shell script file has been edited as shown above, the script needs to be configured within Splunk, so Splunk can begin to ingest the data from the ClearPass Publisher using the configuration just configured in the script file.

Go to **Settings -> Data inputs -> Scripts**

![Adding a shell script to Splunk to ingest EMM data from ClearPass](image)
Click on ‘Scripts’ as highlighted above, then New from the next screen to display the below input screen.

![Figure 24 - Adding the MDM polling script to the ClearPass Splunk application](image)

Under the **Source: Command** enter `/opt/splunk/etc/apps/ClearPassOnSplunk_2/bin/mdm.sh`

**Note:** The data path entered above applies specifically to Linux and particular because we installed Splunk in the `/opt` directory. This will differ for HP-UX/Windows etc. Please locate the `mdm.sh` file location as appropriate to your Splunk platform and installation directory.

Under the **Source: Interval** enter the period of time which matches the polling duration of CPPM with the EMM provider.

This is configured under the Cluster Wide Parameters. If this is unknown, it’s recommended to set this value initially to 3,600 which is 1-hour. This value can be modified later as required.

**Note:** The polling period in the cluster-wide settings is in minutes the setting here is in seconds.

Under the **Source type: Set sourcetype** change this to Manual from the drop down list.
Under the **Source type: Source type** enter Aruba:CPPM:MDM

That completes the configuration of the EMM/MDM section. EMM data records should begin appearing within the ClearPass Splunk app very soon.
ClearPass Splunk App Dashboard Elements

This section describes the ClearPass Splunk App menu items and dashboard elements.

Overview

Figure 25 - Overview Dashboard

Note: All data points shown pertain to the selected time period in the upper left area of the dashboard as well as the ClearPass server selection (i.e. “All” or a specific ClearPass server).

The Overview dashboard consists of the following dashboard elements:

First Row:
- **Failed Attempts**: Number of failed authentications
- **Endpoints Authenticated**: Number of unique endpoints authenticated
- **NAS Devices**: Number of Network Access Servers configured to use ClearPass Servers (integrated with Splunk and sending Syslogs) as AAA servers
- **ClearPass Servers**: Number of ClearPass servers integrated with Splunk to send Syslogs

Second Row:
- **Incoming Requests**: Line chart of all authentication requests broken out by outcome (i.e. green = Accepts, red = Rejects, yellow = timeouts), received by ClearPass server(s) currently selected
• **Auth rate per Min:**
  
  per Server
  
  Gauge showing authentication rate averaged over prior minute for all authentication requests received by all ClearPass server(s) currently selected

Third Row:

• **Last 10 Auth Requests:**  Service details on ten most recent authentication requests

• **Last 10 Auth Failures:**  Error details on ten most recent authentication failures

• **Last 10 Auth Alerts:**  Alert details on ten most recent authentication alerts

### Authentications

#### Authentication Overview

![Authentication Overview Dashboard](image)

**Figure 26 - Authentication Overview**

**Note:** All the counts and data shown pertain to the selected time period in the upper left area of the dashboard as well as the ClearPass server selection (i.e. either “All” or a specific ClearPass server).

The Authentication Overview dashboard consists of the following dashboard elements:

First Row:

• **Total Auths:**  Number of total authentications, successful and unsuccessful

• **Total Successful Auths:**  Number of total successful authentications

• **Total Users:**  Number of unique users (duplicates removed across all ClearPass servers selected)

• **Total Endpoints:**  Number of unique endpoints (duplicates removed across all ClearPass servers selected)
• **Total Services:** Number of unique services matched for successful auths
• **NAS Used:** Number of NAS devices configured to use ClearPass Servers (integrated with Splunk and sending Syslogs) as AAA servers

**Second Row:**
• **Incoming Auth Requests:** Line chart of incoming authentication requests over time
• **Auth Failures:** Bar chart of incoming authentication failures over time
• **Service Categorization:** Pie chart breakdown of matched services for successful authentications

**Third Row:**
• **Top 10 User Auths:** Table displaying top ten most frequent user auths
• **Top 10 Services Used:** Table displaying top ten most frequent services hit for authentication
• **Top 10 Alerts Raised:** Table displaying top ten most frequent alerts raised
• **Top 10 Incoming Client MAC:** Table displaying top ten most frequent unique client MAC addresses authenticated
• **Top 10 IP Used:** Details of top ten most frequent IP addresses seen for authentications

**Failure by Error Types**

![Graph showing authentication failure by error type](image)

**Figure 27 - Authentication Failure by Error Type**

**Note:** All the counts and data shown pertain to the selected time period in the upper left area of the dashboard as well as the ClearPass server selection (i.e., either “All” or a specific ClearPass server).
The Failure by Error Types dashboard consists of the following dashboard elements:

**First Row:**
- **Request Timed Out:** Number of authentication failures due to time out
- **Denied by Policy:** Number of authentication failures denied due to non-compliance to policy
- **User Authentication Failed:** Number of authentication failures due to incorrect password
- **Internal RADIUS Error:** Number of authentication failures due to an internal error in the ClearPass RADIUS server
- **User Not Found:** Number of authentication failures due to username not found in any of the configured authentication sources
- **Wrong Shared Secret:** Number of authentication failures due to incorrect shared secret

**Second Row:**
- **Timeout by Controller:** Breakdown of authentication timeout by controller (pie)
- **Denied by Policy by Server:** Breakdown of authentication failures denied by policy by ClearPass server (pie)
- **User Authentication Failed by Server:** Breakdown of authentication failures due to incorrect password
- **Internal RADIUS Error by Server:** Breakdown of authentication failures due to internal error in ClearPass RADIUS server (pie)
- **User Not Found by Server:** Breakdown of authentication failures due to user not found by ClearPass server (pie)
- **Wrong Shared Secret by Controller:** Breakdown of authentication failures due to incorrect shared secret by controller (pie)

**Third Row:**
- **Timeout by Controller:** Bar chart version of corresponding data (see above)
- **Denied by Policy by Server:** Bar chart version of corresponding data (see above)
- **User Authentication Failed by Server:** Bar chart version of corresponding data (see above)
- **Internal RADIUS Error by Server:** Bar chart version of corresponding data (see above)
- **User Not Found by Server:** Bar chart version of corresponding data (see above)
- **Wrong Shared Secret by Controller:** Bar chart version of corresponding data (see above)
Fourth Row:
- **Timeout by User:** By user breakdown of corresponding data (see above)
- **Denied by Policy:** By user breakdown of corresponding data (see above)
- **User Authentication:** By user breakdown of corresponding data (see above)
- **Internal RADIUS Error:** By user breakdown of corresponding data (see above)
- **User Not Found by User:** By user breakdown of corresponding data (see above)
- **Wrong Shared Secret:** By user breakdown of corresponding data (see above)

Fifth Row:
- **Failed Requests:** Top ten most frequent failed requests by error type (bar)
- **Failed Requests:** Top ten most frequent failed requests by error type (pie)

Sixth Row:
- **Successful vs Failed:** Number of successful and failed requests per hour (line)
- **Successful vs Failed:** Proportion of accepted, rejected and timed out requests (pie)

**Failure Distribution**

![Failure Distribution Diagram](image)

Figure 28 - Authentications > Failure Distribution
**Note:** All data shown pertain to the selected time period in the upper left area of the dashboard and the ClearPass server selection (i.e., either “All” or a specific ClearPass server) filtered by the Failure Type (i.e. Request Timed Out, User Not Found, Wrong Shared Secret, etc.) selection.

The Failure Distribution dashboard consists of the following dashboard elements:

**First Row:**
- **Total Failed Attempts:** Number of total failed authentication attempts
- **Users Failed:** Number of total unique user who had failed authentications
- **Endpoints Failed:** Number of total unique endpoints with failed authentications

**Second Row:**
- **Authentication Failure:** Breakdown of failed authentications by controller / NAS device
  - by Network Device
- **Top 10 Failed Attempts:** Breakdown of failed authentications by user
  - by Users
- **Top 10 Failed Attempts:** Breakdown of failed authentications by endpoint
  - by Endpoints

**Third Row:**
- **Authentication Failure:** Table displaying failed authentications by NAS device
  - by NAS Device
- **Top 10 Failed Attempts:** Table displaying failed authentications by user
  - by Users
- **Top 10 Failed Attempts:** Table displaying failed authentications by endpoint
  - by Endpoints
Authentication Trends

Figure 29 - Authentications > Authentication Trends

**Note:** All the information displayed on this dashboard is based on the time period selected as well as the ClearPass server(s) and NAS device(s) selected. Additionally, you can filter the data by Authentication Status and Syslog field (e.g. `req_source`, `user_name`, `error_code`, `mac_address`, `service_name`, `session_id`).

**Note:** Before any data can be displayed, you must first make your selections and click the Submit button.

The Authentication Trends dashboard consists of the following dashboard elements:

**First Row:**
- **Logins Today:** Number of successful authentications for current day
- **Logins Yesterday:** Number of successful authentications for previous day
- **Logins 7-Days Ago:** Number of successful authentications seven days prior
- **Logins Last Week Avg:** Average number of successful authentications seven days prior
- **Logins Last Month Avg:** Average number of successful authentications thirty days prior

**Second Row:**
- **Login Compare:** Comparison of total logins per hour for current day versus previous day
  - **Today vs Yesterday**
  - **Today vs 7 Days Ago**
Third Row:
- **Login Trend:** Comparison of total logins per hour for current day versus logins per hour averaged over last week

Fourth Row:
- **Login Trend:** Comparison of total logins per hour for current day versus logins per hour averaged over last thirty days

Fifth Row:
- **Logins:** Comparison of total logins per hour for current day versus logins per hour averaged over selected date range

**Policy Enforcement**

![Policy Enforcement Dashboard](image)

**Figure 30 - Authentications > Policy Enforcement**

**Note:** All the counts and data shown pertain to the selected time period in the upper left area of the dashboard as well as the ClearPass server selection (i.e., either “All” or a specific ClearPass server).

The Policy Enforcement dashboard consists of the following dashboard elements:

First Row:
- **Total Policy Enforcements:** Number of total number of policy enforcements applied
- **Total Enforcement Profiles:** Number of total number of enforcement profiles applied
- **Total Roles:** Number of total number of roles assigned
- **Unhealthy Sessions:** Number of total number of sessions in which posture is UNKNOWN or QUARANTINE
**Second Row:**

- **Top 10 Roles Assigned:** Top ten most frequent roles assigned
- **Top 10 Enforcement Profiles:** Top ten most frequent enforcement profiles applied
- **Health Status:** Breakdown of posture / health by type: HEALTHY, UNKNOWN and QUARANTINE

**Third Row:**

- **Policy Enforcement:** Line chart of number of enforcements per hour

---

**Endpoints**

**Endpoint Categories**

![Endpoint Categories Dashboard](image)

**Figure 31 - Endpoints > Endpoint Categories**

**Note:** All the information displayed on this dashboard is based on the time period selected as well as the ClearPass server(s) and endpoint category (e.g. VoIP phone, SmartDevice, Computer, etc.) and device family (e.g. device vendor) selected. Additionally, you can filter the data by HTTP User Agent (sent by HTTP browsers).

The Endpoint Categories dashboard consists of the following dashboard elements:

**First Row:**

- **All Device Categories:** Breakdown of device categories (e.g. SmartDevice, VoIP Phone, Computer, Access Points) [based on ClearPass dictionary]
• **Device Family by:**
  **Selected Category**
  For selected category, breakdown of device family (e.g. Aastra, Android, Apple, Windows, etc.) [based on ClearPass dictionary]

• **Device Vendor by:**
  **MACs in selected Category**
  For selected category, breakdown of vendor [based on MAC OUI only]

**Second Row:**
• **Endpoints Matching:**
  **Category/Family/UserAgent**
  Table displaying endpoint details including hostname, device name, device family, device category, IP address and MAC vendor

---

**Endpoint Profiles**

![Endpoint Profiles dashboard](image)

**Figure 32 - Endpoints > Endpoint Profiles**

**Note:** All the information displayed on this dashboard is based on the time period selected as well as the ClearPass server(s) and endpoint Hostname. Additionally, you can filter the results using any search string. Click the **Submit** button if you enter a value in the **Search String** field.

The Endpoint Profiles dashboard consists of the following dashboard elements:

**First Row:**
• **Endpoint Profiles:**
  Table displaying endpoint details including hostname, device name, device family, device category, IP address and DHCP fingerprint

**Second Row:**
• **Endpoint Locations:**
  Breakdown of geographic location of endpoints based on IP address
MDM

MDM - Category Charts

Figure 33 – Detailed MDM Endpoint Categories

**Note:** All the information displayed on this dashboard is based on the time period selected as well as the ClearPass server. The MDM Category dashboard consists of the following dashboard elements:

**First Row:**

**Distribution by Ownership:** Breakdown of Endpoint by Ownership, Employee, Corporate, Shared etc.

**Compromised Devices:** Breakdown of endpoint by Compromised status. Note that compromised status can be reported as false or False, note upper case first character in False.

**Encryption Enabled:** Breakdown of endpoint by Encryption status. Note that encryption status can be reported as false or False, note upper case first character in False.
Second Row:

**Distribution by Model:** Breakdown of Endpoint by device model, i.e. iPhone4S, iPhone5, Apple TV, Nexus 7.

**Distribution by Manufacture:** Breakdown of Endpoint by device manufacture, i.e. Apple, Samsung, HTC, Asus

**Distribution by OS Version:** Breakdown of Endpoint by OS Version, i.e. iOS 8.1, iOS 7.0, Android 4.1, Android 4.2

**MDM - Category Stats**

![MDM Category Stats](image)

**Figure 34 - MDM Endpoint Categories Tables**

**Note:** All the information displayed on this dashboard is based on the time period selected as well as the ClearPass server(s). The above tables are copies of the previous section where data was presented in charts.

First Row:

**Distribution by Ownership:** Table of Endpoint by Ownership, Employee, Corporate, Shared etc.

**Compromised Devices:** Table of endpoint by Compromised status. Note that compromised status can be reported as false or False, note upper case first character in False.
**Encryption Enabled:** Table of endpoint by Encryption status. Note that encryption status can be reported as false or False, note upper case first character in False.

**Second Row:**

**Distribution by Model:** Table of Endpoint by device model, i.e. iPhone4S, iPhone5, Apple TV, Nexus 7.

**Distribution by Manufacture:** Table of Endpoint by device manufacture, i.e. Apple, Samsung, HTC, Asus

**Distribution by OS Version:** Table of Endpoint by OS Version, i.e. iOS 8.1, iOS 7.0, Android 4.1, Android 4.2

**MDM - Category List**

![MDM List by Ownership](image)

**Figure 35 - MDM List by Ownership**

**Note:** All the information displayed on this dashboard is based on the time period selected as well as the ClearPass server(s). The bottom of the windows displays detailed level data on the endpoint.

**First Row:**

**Number of MDM Records:** Total number of MDM records, can be sub-divided by choosing Ownership and selecting a category.

**Number of Corporate Devices:** Total number of Corporate devices

**Number of Non-Corporate Devices:** Total number of Non-Corporate devices
Second Row:

**List of MDM Devices:**
List displays detailed attributes by All devices or by category selected in drop-down, i.e. Corporate, Employee

**MDM - Search**

![MDM Search](image)

**Figure 36 - Search for an MDM Endpoint**

**Note:** All the information displayed on this dashboard is based on the time period selected as well as the ClearPass server(s). The bottom of the windows displays detailed level data on the endpoint you select using the below criteria.

**Search for an MDM endpoint by criteria**
Ownership, Owner, IMEI, Phone Number, UDID, Model or Manufacturer. Note that if you wanted to search for iPhone 4S you need to enclose the string in literals "iPhone 4S"
**Sessions**

**Session Details**

![Session Details Dashboard]

Figure 37 - Sessions > Session Details

**Note:** All the information displayed on this dashboard is based on the time period selected as well as the ClearPass server selection (i.e., either “All” or a specific ClearPass server). Additionally, you can filter the results by Username. Click the **Submit** button if you select a value other than **All** in the **Username** field.

The Session Details dashboard consists of the following dashboard elements:

**First Row:**
- **Sessions:** Number of total number of RADIUS sessions started
- **Accounting Started:** Number of total number of RADIUS sessions with RADIUS Accounting enabled started
- **Accounting Stopped:** Number of total number of RADIUS sessions with RADIUS Accounting enabled stopped
- **Input Volume MB:** Volume of input octets received from the endpoint during all completed RADIUS sessions in MBs
- **Output Volume MB:** Volume of input octets sent to the endpoint during all completed RADIUS sessions in MBs

**Second Row:**
- **Session Locations:** Table displaying session location details: City, Region, Country with session ID, session time, username, host ID and errors (if any)
Third Row:
• **Session Policy Details:** Table displaying session policy details: service name, authentication method, authentication source with session ID, session time, username, host ID and errors (if any)

Fourth Row:
• **Session Start/Stop:** Table displaying session details: start time, stop time, NAS port type with session ID, session time, username and host IP address

Fifth Row:
• **Session Usage:** Table displaying session usage details: input octets, output octets, with session ID, session time, username and host IP address

**Bandwidth Usage**

![Bandwidth Usage Dashboard](image)

**Figure 38 - Sessions > Bandwidth Usage**

**Note:** All the information displayed on this dashboard is based on the time period selected as well as the ClearPass server selection (i.e., either “All” or a specific ClearPass server).

The Bandwidth Usage dashboard consists of the following dashboard elements:

First Row:
• **KBPS:** Rate of data throughput (input octets and output octets) in kilobytes per second for the selected time period
• **Input in MB:** Volume of input octets received from the endpoint during all completed RADIUS sessions in MBs
• **Output in MB:** Volume of output octets received from the endpoint during all completed RADIUS sessions in MBs
Second Row:
- **Top Bandwidth Users:** Top ten endpoints with highest total volume of data throughput in MBs

Third Row:
- **Bandwidth Usage:** Chart of data volume throughput over time for top ten endpoints

### Comparison

#### Compare Servers

![Image of Compare Servers dashboard](image)

**Figure 39 - Comparison > Compare Servers**

**Note:** All the information displayed on this dashboard is based on the time period selected as well as the ClearPass server(s) selected. Before any data can be displayed, you must first select your ClearPass server(s).

The Compare Servers dashboard consists of the following dashboard elements:

**First Row:**
- **Logins by Server:** Breakdown of successful authentications by ClearPass server
- **Failures by Server:** Breakdown of failed authentications by ClearPass server
- **Protocol by Server:** Bar chart of authentication protocols used per ClearPass server
- **Services by Server:** Table displaying ClearPass server, service hit and count
Second Row:

- **Health Status by Server:** Table displaying ClearPass server, health posture (HEALTHY/QUARANTINE/UNKNOWN) and count
- **NAS Devices by Server:** Breakdown of NAS devices per ClearPass server
- **Unique MACs by Server:** Breakdown of unique endpoints per ClearPass server
- **Unique Users by Server:** Breakdown of unique users per ClearPass server

## Compare NAS Devices

![Figure 40 - Comparisons > Compare NAS Devices](image)

**Note:** All the information displayed on this dashboard is based on the time period selected as well as the NAS device(s) selected. Before any data can be displayed, you must first select your NAS device(s) and click the **Submit** button.

The Compare NAS Devices dashboard consists of the following dashboard elements:

**First Row:**
- **Logins by NAS Devices:** Breakdown of successful authentications by NAS device
- **Failures by NAS Device:** Breakdown of failed authentications by NAS device
- **Protocol by NAS Device:** Bar chart of authentication protocols used per NAS device
- **Services by NAS Device:** Table displaying NAS device, service hit and count

**Second Row:**
- **Auth Source by NAS Device**
  - Table displaying NAS device, authentication source and count
• **Auth Method:** Table displaying NAS device, authentication method (PAP, MSCHAP, MAC_AUTH, EAP-TLS, EAP/PEAP, etc.) and count
• **NAS Port Type:** Breakdown of type of port (Ethernet, FastEthernet, GigabitEthernet, Wireless, etc.) by NAS device
• **Service Type:** Breakdown of RADIUS service type (e.g. Login, Framed, Outbound, Administrative, NAS Prompt, Call Check, etc.) by NAS device.

Third Row:
• **ClearPass Servers:** Breakdown of ClearPass servers by NAS device
• **Unique MACs:** Breakdown of unique endpoint MAC addresses by NAS device
• **Unique Users:** Breakdown of unique users by NAS device

**System**

**System Monitor**

![System Monitor Dashboard](image)

**Figure 41 - System > System Monitor**

**Note:** All the information displayed on this dashboard is based on the time period selected.

The System Monitor dashboard consists of the following dashboard elements:
First Row:

- **Server Status:**
  - Table displaying details of server uptime: hostname, uptime, data interface status, management interface status
- **CPU Usage:**
  - Table displaying details of server CPU usage: hostname, CPU usage graph, percentage CPU used
- **CPU Available:**
  - Table displaying details of server CPU idle time: hostname, CPU idle time graph, percentage CPU idle

Second Row:

- **Memory Usage:**
  - Table displaying details of server memory usage: hostname, memory usage graph, MBs of memory used
- **Memory Available:**
  - Table displaying details of memory available: hostname, memory availability graph, MBs of memory available
- **Swap Size Usage:**
  - Table displaying details of swap space used: hostname, swap space used graph, KBs used
- **Swap Size Available:**
  - Table displaying details of swap space available: hostname, swap size availability graph, KBs available

**System Events**

![System Events Dashboard](image)

**Figure 42 - System > System Events**

**Note:** All the information displayed on this dashboard is based on the time period selected as well as the ClearPass server(s) selected. Before any data can be displayed, you must first select your ClearPass server(s).

The System Events dashboard consists of the following dashboard elements:
First Row:
- **Failed Events:** Details of failed events: category, description, count
- **Latest Events:** Details of most recent events: level, category, description, count

Second Row:
- **ClearPass Logins:** Details of logins to ClearPass servers: timestamp, host, description, action key
- **AV Updates:** Details of antivirus updates to ClearPass servers: timestamp, host, description, action key

Third Row:
- **User Agent Updates:** Details of user agent updates to ClearPass servers: host, description, action key
- **Hotfixes Updates:** Details of hotfix updates to ClearPass servers: host, description, action key

**Audit Records**

![Audit Records Dashboard](image)

**Figure 43 - System > Audit Records**

**Note:** All the information displayed on this dashboard is based on the time period selected as well as the ClearPass server(s) selected. Before any data can be displayed, you must first select your ClearPass server(s).

The Audit Records dashboard consists of the following dashboard elements:

**First Row**
- **Audit Records:** Details of changes made to attributes of ClearPass-managed entities such as endpoints, guest users, applications, profile definitions, etc.: timestamp, source ID (i.e. ID of entity on which changes are being made), type of change, entity category, user who made the change
License Indicator

Figure 44 - System > License Usage > Policy Manager License Indicator

Note: All the information displayed on this dashboard is based on the ClearPass server(s) selected. Before any data can be displayed, you must first select your ClearPass server(s) and click the Submit button.

The License Indicator dashboard consists of the following dashboard elements:

First Row:
- **Today’s Unique:** Number of unique MAC addresses (duplicates removed across all selected ClearPass servers) seen on current date
- **7-Day Unique:** Number of unique MAC addresses (duplicates removed across all selected ClearPass servers) seen over prior seven day period
- **7-Day Unique:** Number of unique MAC addresses (duplicates removed across all selected ClearPass servers) seen over prior seven day period averaged over thirty days

Second Row:
- **Past Week Unique:** Bar chart of cumulative count of unique MAC addresses (duplicates removed across all selected ClearPass servers) seen over prior seven days
- **Past Week Unique:** Table displaying cumulative count of unique MAC addresses (duplicates removed across all selected ClearPass servers) seen over prior seven days

Third Row:
- **30 DAY AVG Unique:** Line chart showing two quantities: a running average from 36
MAC Count – Chart

• **30 DAY AVG Unique:**

MAC Count – Table

Table displaying the same information as above in a tabular form

Guest License Indicator

![Image of Guest License Indicator dashboard](image)

Figure 45 - System > License Usage > Guest License Indicator

**Note:** All the information displayed on this dashboard is based on the ClearPass server(s) selected. Before any data can be displayed, you must first select your ClearPass server(s) and click the **Submit** button.

The Guest License Indicator dashboard consists of the following dashboard elements:

**First Row:**
- **Guest Sessions Today:** Number of guest sessions initiated on current date
- **Unique Guest:** Number of unique guest MAC addresses (duplicates removed across all selected ClearPass servers) seen on current date
- **Unique Guest:** Number of unique guest MAC addresses (duplicates removed across all selected ClearPass servers) averaged over a 30 day period

**Second Row:**
- **Unique Guest:** Line chart of unique guest MAC addresses (duplicates removed across all ClearPass servers) seen on current date

**Third Row:**
- **30 DAY AVG/TOT:** Line chart showing two quantities: an average over the last 30
Unique Guest MAC Count – Chart  days prior of unique guest MAC address count; and the total number of unique MAC addresses over the last 30 days

- **30 DAY Guest: MAC Details – Table:**  Table displaying details of guest MAC addresses over the last 30 days: average unique guest MACs, days unique guest MACs, average (non-unique) guest MACs, days (non-unique) guest MACs, total unique guest MACs (cumulative), total (non-unique) Guest MACs (cumulative), timestamp

### Search

#### Generic Query Textbox

![Generic Query Textbox](image)

**Figure 46 - Search > Generic Query Textbox**

**Note:** All the information displayed on this dashboard is based on the time period selected as well as the ClearPass server(s) selected. Additionally, you can filter the display using the following search fields: Username, Hostname, MAC Address, IP Address, NAS Port Type and any other search string. Before any data can be displayed, you must first select your ClearPass server(s) and click the **Submit** button.

The Generic Query Textbox dashboard consists of the following dashboard elements:

- **First Row:**
  - **Dashboard:**  Table displaying the following details: authentication session ID, time stamp, user name, service name, NAS IP address, NAS port, MAC Address, login status, request source, connection status, error code.
Second Row:
- **RADIUS:**

  **Session**

  Table displaying the following details: authentication session ID, time stamp, user name, end host ID, service name, NAS IP address, authentication method, NAS port, MAC Address, login status, request source, count of alerts present, connection status, error code.

Third Row:
- **RADIUS:**

  **Accounting**

  Table displaying the following: RADIUS authentication session ID, sequence number, RADIUS accounting session ID, time stamp, user name, hostname, endpoint, IP address, NAS IP address, NAS port type, called station MAC address, calling station MAC address, accounting status type, accounting session time, accounting delay time, accounting input octets, accounting input packets, accounting output octets, accounting output packets

Fourth Row:
- **RADIUS:**

  **Accounting**

  **Detail**

  Table displaying the following: RADIUS authentication session ID, RADIUS accounting session ID, type of authentication session, database row ID, RADIUS attribute name, RADIUS attribute value

Fifth Row:
- **Endpoint:**

  **Profiles**

  Table displaying the following: time stamp, endpoint hostname, endpoint MAC Address, endpoint IP address, MAC vendor (based on OUI), Boolean value to indicate whether the IP address is static, time when endpoint was added, time when endpoint was updated, DHCP fingerprint, endpoint name, endpoint family, endpoint category

Sixth Row:
- **Additional:**

  **Search Output**

  Table displaying the following: raw Syslog message, time stamp, ClearPass server IP address, Syslog sender IP address, index, Number of lines in Syslog message, Syslog source port, Splunk sourcetype, Splunk server hostname / IP address to which Syslog was sent
ClearPass Application

Generic Query Dropdown

![Generic Query Dropdown](image)

**Figure 47 - Search > Generic Query Dropdown**

**Note**: All the information displayed on this dashboard is based on the time period selected as well as the ClearPass server(s) selected. Additionally, you can filter the display using the following search dropdown lists: Username, Hostname, MAC Address, IP Address, NAS Port Type and any other search string. Display using the following: search Address, NAS Port Type and any other search string. Before any data can be displayed, you must first select your ClearPass server(s) and click the Submit button.

This next dashboard displays data that is identical to the previous dashboard (Generic Query Textbox), except the selection fields are dropdown lists.

The Generic Query dropdown dashboard consists of the following dashboard elements:

- **First Row**:
  - **Dashboard**: See above – identical to information displayed for previous dashboard

- **Second Row**:
  - **RADIUS**:
    - **Session**: See above – identical to information displayed for previous dashboard

- **Third Row**:
  - **RADIUS**:
    - **Accounting**: See above – identical to information displayed for previous dashboard

- **Fourth Row**:
  - **RADIUS**:
    - **Accounting Detail**: See above – identical to information displayed for previous dashboard
Fifth Row:
- **Endpoint:** See above – identical to information displayed for previous dashboard

Sixth Row:
- **Generic:** See above – identical to information displayed for previous dashboard

**Search**

![Search Dashboard](image)

**Figure 48 - Search > Search**

This dashboard is the generic Splunk search dashboard. You can enter any search string or event type. The Splunk UI will prompt you to select any values that are contextually relevant.

**Syslog Raw Data**

Here are examples of the raw Syslog data received from ClearPass for different types of events. Note the column names that are returned for these events.

**Failed Authentication Raw Data**

```plaintext
```
Successful Authentication Raw Data

```
```

Event Log Raw Data

```
```

Audit Log Raw Data

```
<143>2014-03-28 16:47:14,250 10.17.6.54 All Audits 30 1 0 Timestamp=Mar 28, 2014 16:46:59 IST,Source=All Audits,Category=Syslog Export Data,Action=MODIFY,User=admin
```

Caveats

The following caveats exist when using ClearPass and Splunk as described in this document:

1. If the value of any field in the Syslog message payload sent by ClearPass contains a comma (,) then only the value that is before the comma will be used as the value of the field.

   For example, if the name/value pair in ClearPass is:

   ```
   ClearPass: Common.Roles="[Employee], [User Authenticated]"
   ```

   then Splunk will only capture the first value:

   ```
   Splunk: Common.Roles="[Employee]"
   ```

2. If the value of any field in the Syslog message payload sent by ClearPass contains an ‘=' sign then only the value that is before the ‘=' sign will be used in Splunk.

   For example, if the payload in the ClearPass Syslog message is:
ClearPass Application  ClearPass App for Splunk Enterprise

Jun 3 13:08:36 10.17.6.54 2014-06-03 13:07:14,536 10.17.6.54 CPPM_System_Events 973 1 0
event_source=SnmpService,level=ERROR,category=Trap,description=Switch IP=10.17.8.67.
Ignore v2c trap. Bad security name in trap,action_key=Failed,timestamp=2014-06-03
13:05 :30.023+05:30

Note that the description field has a string with an embedded ‘=’ sign. Splunk will only
capture the value before the ‘=’ sign as below:

Splunk description: Switch

<table>
<thead>
<tr>
<th>Latest Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>level</td>
</tr>
<tr>
<td>------</td>
</tr>
<tr>
<td>ERROR</td>
</tr>
<tr>
<td>ERROR</td>
</tr>
<tr>
<td>ERROR</td>
</tr>
<tr>
<td>INFO</td>
</tr>
<tr>
<td>INFO</td>
</tr>
<tr>
<td>INFO</td>
</tr>
<tr>
<td>INFO</td>
</tr>
<tr>
<td>WARN</td>
</tr>
</tbody>
</table>

Figure 49 - Splunk Event Dashboard Element Showing Incomplete Description Field

Checking Splunk is receiving Syslog Data from CPPM

To check that syslog data is being received by Splunk, go to Splunk -> Apps -> Search & Reporting and ensure that see that data events are being received as shown below. Also specifically look at the Latest Event counter to see when the last event was received.

Figure 50 - Checking Syslog events are being received by Splunk