



---

## *Avenda Insight – Jumpstart Guide*

DOC: ISTV1.3

## Table of Contents

1	Overview .....	3
2	Getting Started with Insight.....	4
2.1	Gaining access .....	4
2.2	Logging into Avenda Insight .....	4
2.3	Navigating Avenda Insight.....	5
3	Configuring Insight.....	6
3.1	Data Sources .....	6
3.2	Configuring Messaging Options .....	8
3.3	Configuring Reports .....	9
3.4	Configuring Alerts.....	12
4	Insight Analytics.....	14
4.1	Insight Dashboard .....	15
4.2	Alert Viewer .....	22
5	Summary.....	23

# 1 Overview

Avenda Insight is an advanced application for use with the eTIPS Identity platform to deliver enhanced analytics, in-depth reporting, and significant gains when addressing compliance and regulatory overhead. The goal of this guide is to illustrate how easy it is for network managers to analyze authentication information captured from eTIPS in order to generate customized reports.

Custom report templates provide the ability to track detailed authentication records, audit trails, systematic reports on network-access trends, and generate reports that are compliant with regulatory and corporate requirements.

Insight addresses the following criteria for reporting and compliance.

## **1. Consolidated reporting on various sources of data**

Insight is capable of aggregating data from multiple eTIPS appliances, or, external stores containing archived network access logs. It presents a powerful combination of near real-time analytics, as well as the ability to look into the past to satisfy historical analysis and compliance needs.

## **2. In-depth analytics to mine data and generate trending reports**

Insight uses a powerful analytics engine that mines network access logs in order to generate trending report on various parameters. Network managers can utilize these trends to get an overview of authentication and access activity, elaborate client access distribution, load-averages, and analyze authentication traffic flow through various network devices

## **3. Ready-to-use templates that generate detailed network access reports**

Insight includes several ready-to-use templates that help reduce the time associated with creating custom reports. The templates guide users through the process of capturing data for a number of use-cases with minimal configuration.

## **4. Generate Alerts upon detecting anomalous network activity**

Insight also generates near real-time alerts on anomalous network activity. Network managers can configure alerts based on a number of various parameters; alerts generate SMS or e-mail notifications to multiple recipients to prompt action.

## 2 Getting Started with Insight

### 2.1 Gaining access

Insight uses a Web-Based management interface.

Supported Web Browsers include:

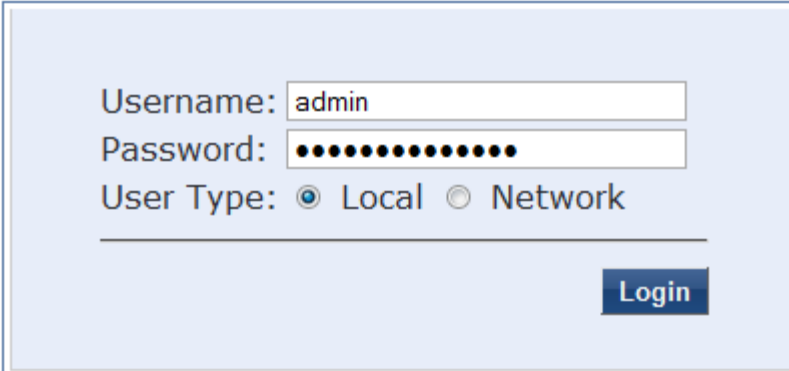
- Mozilla Firefox 3.0 +
- Microsoft Internet Explorer 7.0+
- Google Chrome 1.0

To reach the Insight interface, use one of the following methods

- Point the web-browser to <https://<etips-host-name>/Insight>
- Access eTIPS via <https://<etips-host-name>/tips> , click the “Avenda Insight” link on the page
- Launch the eTIPS Dashboard at <https://<etips-host-name>/tips>, use the “Applications” widget to click on “Avenda Insight”

### 2.2 Logging into Avenda Insight

On the login screen, use the default User Name/Password [admin/eTIPS123] and click “Login” to launch the user interface.



Username:

Password:

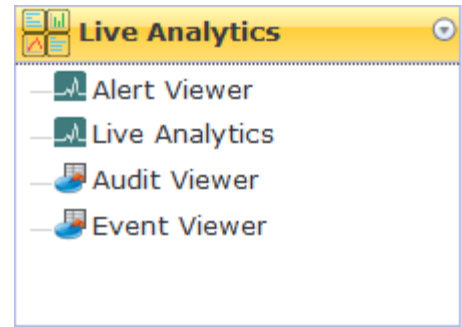
User Type:  Local  Network

## 2.3 Navigating Avenda Insight

Navigation links are located on the left side of the screen. The menu contains three sections described below:

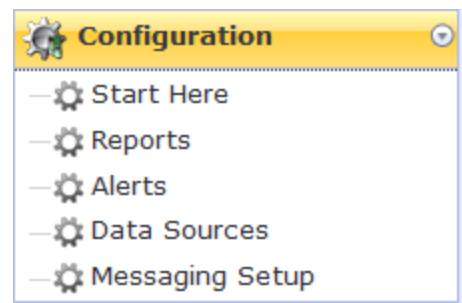
- **Live Analytics**

- Alert Viewer – Analyze alerts generated on network access information
- Live Analytics – Analyze trends; Slice and Dice data; Download reports
- Audit Viewer – View detailed audit trails
- Event Viewer – Monitor Insight Events



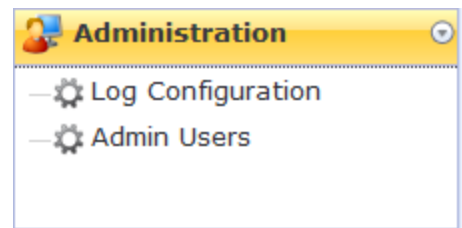
- **Configuration**

- Start Here – Selection of Insight Templates bundled with the product
- Reports – A list of Reports allowing the user to add/edit/delete Reports
- Alerts – A list of Alerts allowing the user to add/edit/delete Alerts
- Data Sources -A list of Data Sources allowing the user to add/edit/delete Data Sources



- **Administration**

- Log Configuration – Change logging options on Insight
- Admin Users – Edit User Name/Password of the default administrative user




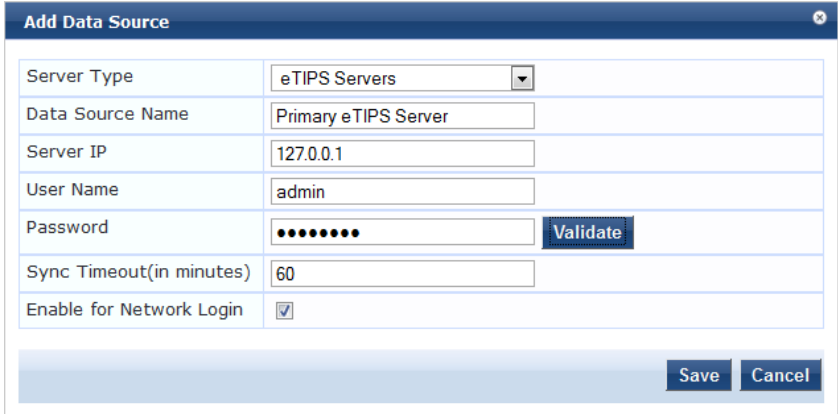
### 3 Configuring Insight

#### 3.1 Data Sources

Insight runs analytics on network access logs provided by an eTIPS server or external Insight archive server.

To setup a new data source, navigate to “Data Sources” under “Configuration” menu and click on the “Add” link.

**Adding eTIPS servers as a data source**

Configuration Steps	
<p><b>To create a new Data Source click on the following:</b></p> <ul style="list-style-type: none"> <li>• <b>Data Sources &gt;</b></li> <li>• <b>Click Add</b></li> </ul>	
<p><b>Configure data source parameters:</b></p> <ul style="list-style-type: none"> <li>• Select Type <b>eTIPS Servers</b></li> <li>• Enter <b>Data Source Name</b></li> <li>• Enter eTIPS <b>Server IP</b> address</li> <li>• Enter the <b>eTIPS administrative</b> user name</li> <li>• Enter <b>password</b> for the user configured in the previous step</li> <li>• Click <b>Save</b> when done</li> </ul>	

**Adding an external Insight archive server as a data source**

<p><b>Configuration Steps</b></p> <p>To create a new Data Source click on the following:</p> <ul style="list-style-type: none"> <li>• <b>Data Sources &gt;</b></li> <li>• <b>Click Add</b></li> </ul>	
<p><b>Configure data source parameters:</b></p> <ul style="list-style-type: none"> <li>• Select type <b>External Servers</b></li> <li>• Enter <b>Data Source Name</b></li> <li>• Enter external <b>Server's IP</b></li> <li>• Enter the <b>User Name</b> used for the external server</li> <li>• Enter <b>password</b> for the user configured in the previous step</li> <li>• Specify the <b>Cluster Name</b> for the eTIPS cluster as configured on the external server</li> <li>• Specify a <b>Record Begin Date &amp; Record End Date</b></li> <li>• Click <b>Save</b> when done</li> </ul>	

Once registered, Insight automatically updates itself and queries the data source for access logs. You can monitor update progress by selecting the Data Source and clicking the “Show Status” button

#	Name	Server IP	Server Type	Sync Timeout
1.	localhost	127.0.0.1	eTIPS	60 Minutes

Server:	localhost
Status:	True
Sync Timestamp:	Nov 18, 2009 18:49:00 PST
Backup Timestamp:	Nov 13, 2009 14:53:43 PST
Number of Failures:	0
Errors (if any):	

## 3.2 Configuring Messaging Options

### Configure email and SMS options

#### Configuration Steps

**To configure Email Messaging click on:**

- **Messaging >**
- Enter SMTP details:
  - **Server name**
  - **SSL Configuration**
  - **User name**
  - **Password**
  - **Connection timeout**

**Configure Short Messaging Service (SMS):**

- Use the **Copy to SMS Setup** button to copy e-mail configuration, or, provide details on another SMTP server
- Click Save when done

Configuration > Messaging Setup

#### Messaging

Configure the SMTP mail servers for email and SMS notifications :

**SMTP Servers**   **Mobile Service Providers**

Email

SMTP server for email notifications

Server name: <input type="text" value="mysmp.myserver.com"/>	<input type="checkbox"/> Use SSL
User Name: <input type="text" value="smpUserName"/>	Port: <input type="text" value="25"/>
Password: <input type="password" value="*****"/> <input type="checkbox"/> Clear text	Connection timeout: <input type="text" value="30"/> seconds

Short-Messaging Service (SMS)

SMTP server for SMS notifications

Server name: <input type="text" value="mysmp.myserver.com"/>	<input type="checkbox"/> Use SSL
User Name: <input type="text" value="smpUserName"/>	Port: <input type="text" value="25"/>
Password: <input type="password" value="*****"/> <input type="checkbox"/> Clear text	Connection timeout: <input type="text" value="30"/> seconds



### 3.3 Configuring Reports

The “Start Here” page provides network managers with a launch pad for creating reports. This page lists various templates, each tailored for specific network access data. Modifying the templates allows each report to meet exact requirements.

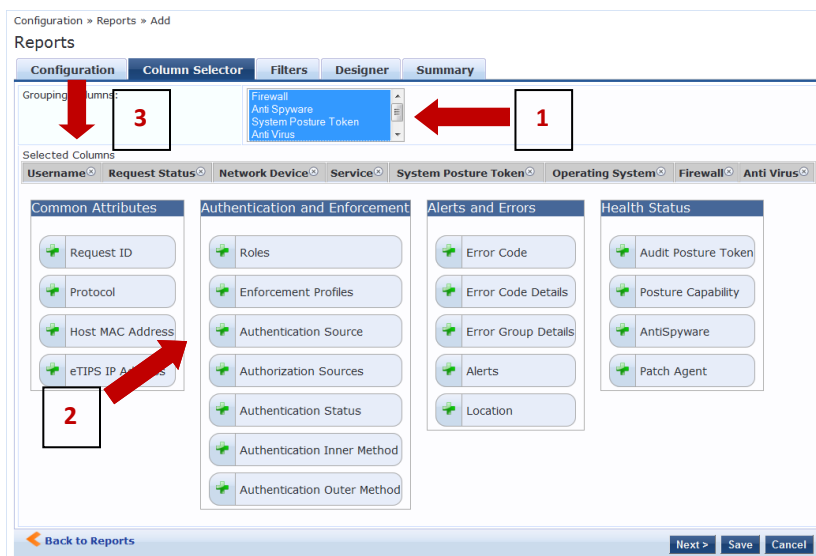
There are five (5) tabs and associated steps.

**Configure a daily report to provide data and analytics on “Client Posture Status”**

Configuration Steps	
<p><b>To add a new Posture Report click on:</b></p> <ul style="list-style-type: none"> <li>• <b>Start Here &gt;</b></li> <li>• Click <b>Posture</b> template</li> </ul>	<p>Configuration &gt; Start Here Start Here</p> <p>Select a template type to configure a report</p> <ul style="list-style-type: none"> <li><b>RADIUS Authentication</b> Report Fields: Username, Request Status, Service, Network Device, Authentication Source, Roles</li> <li><b>RADIUS Failed Authentication</b> Report Fields: Username, Host MAC Address, Network Device, Service, Error Code Details, Alerts</li> <li><b>WEBAUTH</b> Report Fields: Username, Service, Network Device, Authentication Source, Roles</li> <li><b>WEBAUTH Failed Authentication</b> Report Fields: Username, Host MAC Address, Network Device, Service, Error Code Details, Alerts</li> <li><b>Posture</b> Report Fields: Username, Request Status, Network Device, Service, System Posture Token, OS Type, Firewall, AntiVirus, AntiSpyware</li> <li><b>Failed Posture</b> Report Fields: Username, Request Status, Network Device, Service, System Posture Token, OS Type, Firewall, AntiVirus, AntiSpyware</li> </ul>
<p><b>Configure report parameters:</b></p> <ul style="list-style-type: none"> <li>• Name report <b>Daily Posture Status Report</b></li> <li>• Enter <b>Description</b></li> <li>• <b>Private</b> is unchecked (makes the report visible to other users)</li> <li>• Enter <b>e-mail addresses</b> for people that will receive reports and status information</li> <li>• Select target <b>Data Source</b></li> <li>• Enter <b>scheduling information</b> – Choose to run this report daily, at 1 AM</li> <li>• Click Next when done</li> </ul>	<p>Configuration &gt; Reports &gt; Add Reports</p> <p>Configuration   Column Selector   Filters   Designer   Summary</p> <p>Select Template: Posture</p> <p>Name: Daily Posture Status Report</p> <p>Description: Report on Client Posture Status</p> <p>Private?: <input type="checkbox"/> Yes</p> <p>Enable Data in PDF Reports?: <input checked="" type="checkbox"/> Yes</p> <p>e-mail: Messaging not configured</p> <p>Data Source: localhost</p> <p>Mode: Date Range <input type="radio"/> Scheduled <input checked="" type="radio"/></p> <p>Run this report: DAILY At 1 AM</p> <p>Back to Reports   Next &gt;   Save   Cancel</p>

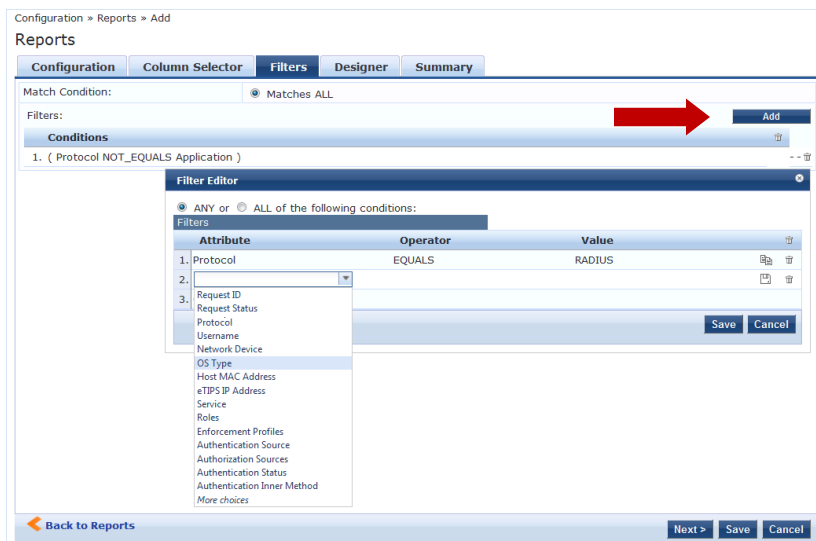
**Select data fields to populate report:**

- **1** -Select all of the available fields (reports are grouped using multiple fields, each presenting a unique analysis of network access data)
- **2**- Drag and Drop desired data types from the available list to **3 - Selected Columns**
- Click Next when done



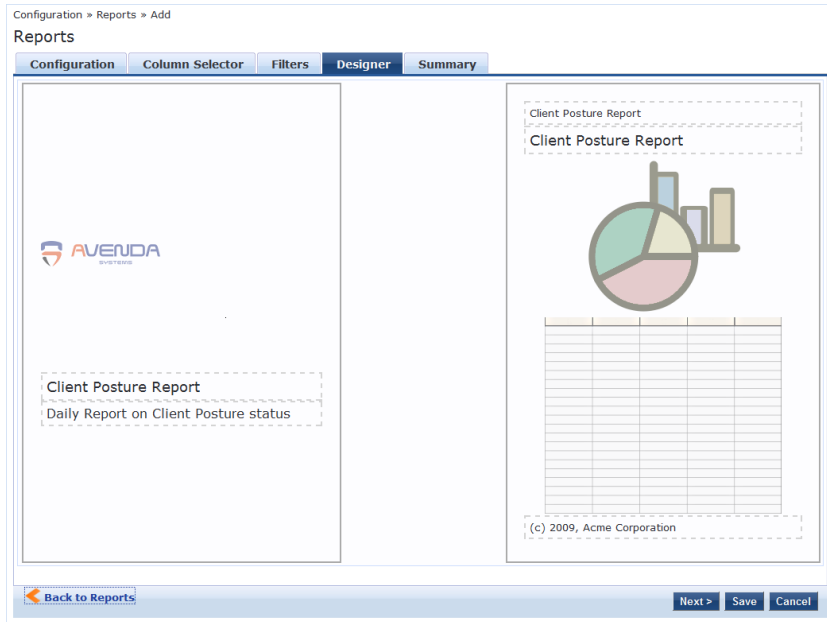
**To customize filters if needed:**

- From the filters tab click the **Add** button to launch the editor (the editor is context-aware; suggested prompts appear to assist configuration)
- Click Next when done



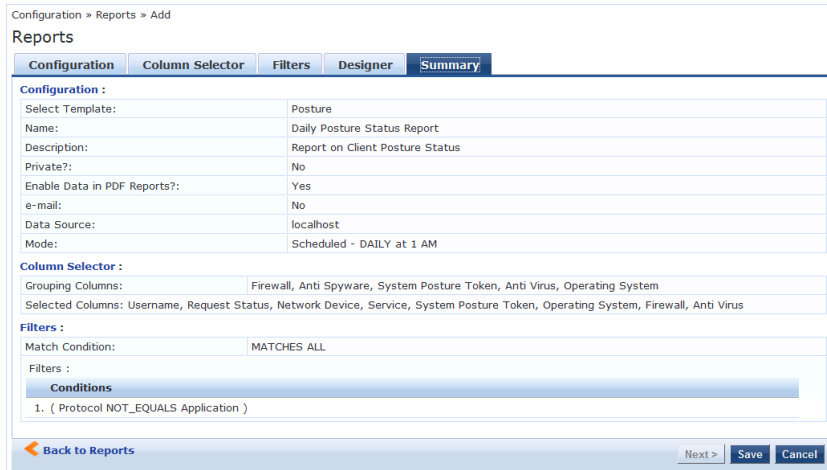
**To customize the layout of a report:**

- The report Designer is split into two areas:
  - The Cover Page:
    - Click the image to change the logo
    - Click the dotted area on the cover page to edit the report title and description
  - The Report Page(s):
    - Click the dotted area to edit the header and footer
- Click Next when done



**The last step:**

- The summary tab displays all of the configuration elements
- Review configuration elements
- Click Save when done



**Insight Notes:**

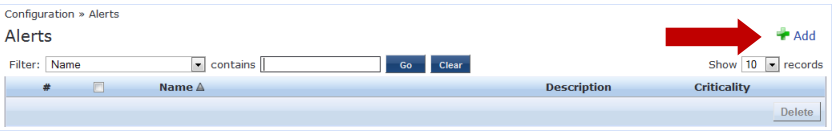
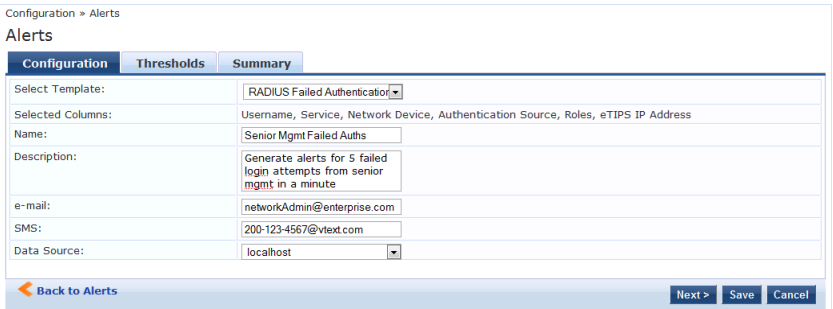
- Reports can run in a “Date Range” mode, where in Insight only extracts data for a specified date range. This option is available in the “Schedule” section found under the “Configuration” tab.
- Over thirty templates are included which segregate data by Protocol, Authentication, Client , Posture, Device Administration and eTIPS specific Audit/System events

### 3.4 Configuring Alerts

Alerts provide network managers with near real-time messages on anomalous network activity. Such activity could constitute:

- Irregular authentication activity
- Irregular Network Device access activity
- Users attempting privileged commands on network devices
- Irregular activity on the eTIPS Servers

As with Reports, Alerts include templates keyed to ease configuration. These templates allow managers to quickly configure and monitor such activity. In addition to e-mail notification, you can send alerts to mobile devices via SMS, thus providing the capability to receive mission-critical information on the go.

<p><b>Configuration Steps</b></p>									
<p><b>To add a new Alert:</b></p> <ul style="list-style-type: none"> <li>• Alerts &gt;</li> <li>• Click Add</li> </ul>	 <p>Configuration » Alerts Alerts</p> <p>Filter: Name contains Go Clear Show 10 records</p> <table border="1"> <thead> <tr> <th>#</th> <th>Name</th> <th>Description</th> <th>Criticality</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table> <p>Delete</p>	#	Name	Description	Criticality				
#	Name	Description	Criticality						
<p><b>Configure Alert Parameters:</b></p> <ul style="list-style-type: none"> <li>• Select <b>RADIUS Failed Authentications</b> template</li> <li>• Enter a <b>name</b> for the Alert</li> <li>• Provide a <b>description</b> for the same</li> <li>• Provide an <b>e-mail address</b> to which alerts are dispatched</li> <li>• Provide an <b>SMS address</b> to which alerts are dispatched (A list of Mobile service providers is available on the Messaging Setup page)</li> <li>• Click Next when done</li> </ul>	 <p>Configuration » Alerts Alerts</p> <p>Configuration Thresholds Summary</p> <p>Select Template: RADIUS Failed Authenticator</p> <p>Selected Columns: Username, Service, Network Device, Authentication Source, Roles, eTIPS IP Address</p> <p>Name: Senior Mgmt Failed Auths</p> <p>Description: Generate alerts for 5 failed login attempts from senior mgmt in a minute</p> <p>e-mail: networkAdmin@enterprise.com</p> <p>SMS: 200-123-4567@vtext.com</p> <p>Data Source: localhost</p> <p>Back to Alerts Next &gt; Save Cancel</p>								

**Configure Alert Thresholds:**

- Conditions: Specify **filters** to trigger alerts
- Threshold: Specify the **number of times** this condition must occur to trigger an alert
- Time: Specify a **window of time** in which the above set of conditions must occur to trigger an alert
- Alert Level: Specify a **Criticality for the Alert**

Configuration » Alerts  
Alerts

Configuration   **Thresholds**   Summary

Match Condition:  Matches ALL

Filters: Add

**Conditions**

1. ( Protocol EQUALS RADIUS )
2. ( Request Status EQUALS Failure )
3. ( Roles CONTAINS Senior\_Mgmt )

Threshold Value:

Threshold Time:  Minutes  Hours  Days

Alert Level:

[Back to Alerts](#) Next > Save Cancel

**The last step:**

- Review configuration elements
- Click Save when done

Configuration » Alerts  
Alerts

Configuration   **Thresholds**   Summary

**Configuration :**

Select Template: RADIUS Failed Authentication

Selected Columns: Username, Service, Network Device, Authentication Source, Roles, eTIPS IP Address

Name: Senior Mgmt Failed Auths

Description: Generate alerts for 5 failed login attempts from senior mgmt in a minute

e-mail: networkAdmin@enterprise.com

SMS: 200-123-4567@vtext.com

Data Source: localhost

**Thresholds :**

Match Condition: MATCHES ALL

Filters :

**Conditions**

1. ( Protocol EQUALS RADIUS )
2. ( Request Status EQUALS Failure )
3. ( Roles CONTAINS Senior\_Mgmt )

Threshold Value: 5

Threshold Time: 1 minutes, 0 hours, 0 days

Alert Level: CRITICAL

[Back to Alerts](#) Next > Save Cancel

**Insight Notes:**

- Alerts are generated when a particular condition is met, a given number of times in a specific window of time. These components are reflected in the Thresholds section:

## 4 Insight Analytics

Insight empowers network managers to make critical network policy decisions based on authentication and access traffic. It provides trending on network access activity, multi-tiered data and charts, enhanced slice-and-dice capabilities, and single point of access for troubleshooting.

### Launch Insight Analytics:

1. Select the report from the Reports screen, click the “Show Status” button

#	Name	Description	Private	Mode	Status
1.	Daily Posture Status Report	Report on Client Posture Status	false	Scheduled	SCHEDULED

OR

2. Click the report on the Live Analytics screen

#	Name	Description	Private	Mode	Status
1.	Daily Posture Status Report	Report on Client Posture Status	false	Scheduled	SCHEDULED

3. This launches the Insight Analytics Dashboard for the report

Success Rate	100%
Last Success	Nov 20, 2009 01:00:46 UTC
Last Failure	Nov 20, 2009 01:00:46 UTC
Begin Record Time	Nov 19, 2009 18:38:38 UTC
End Record Time	Nov 20, 2009 00:38:54 UTC
Number of records selected	4141

Date	Request Count
Nov 13	~150
Nov 14	~200
Nov 15	~120
Nov 16	~150
Nov 17	~150
Nov 18	~150
Nov 19	~80

Grouping Field	Count
iptables	~900
None	~900

Username	Request Status	Network Device	Service
testradius	Failure	192.168.5.214	...
testradius	Failure	192.168.5.214	...
trent	Success	192.168.5.214	Avend. Service
testradius	Failure	192.168.5.214	...
testradius	Failure	192.168.5.214	...
testradius	Failure	192.168.5.214	...

Date	File Name	Downloaded
2009-11-19	report.csv	Nov 19, 2009 19:53:29 UTC
	report.pdf	

## 4.1 Insight Dashboard

### Informational Notes: Dashboard component views

#### Monitor the status of current report:

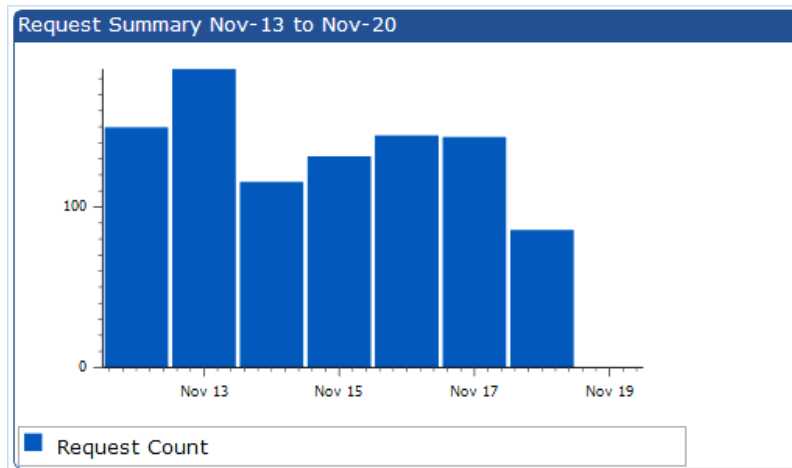
- Date/time
- Number of records selected
- Failures (if any)
- Click the **more** link to see advanced diagnostic messages

Report Status - Daily Posture Status Report	
	Success Rate 50%
	Last Success Nov 20, 2009 01:00:46 UTC
	Last Failure Nov 20, 2009 01:00:46 UTC
Begin Record Time	Nov 19, 2009 18:38:38 UTC
End Record Time	Nov 20, 2009 00:38:54 UTC
Number of records selected 0	
more...	

Report Run Details	
Run Time	Nov 19, 2009 19:53:29 UTC
Report Run Date	Nov 19, 2009 19:53:29 UTC
Begin Record Time	Feb 01, 2006 18:46:59 UTC
End Record Time	Nov 19, 2009 18:38:38 UTC
Status	true
Number of Records Selected	0
Errors	No records matching filter

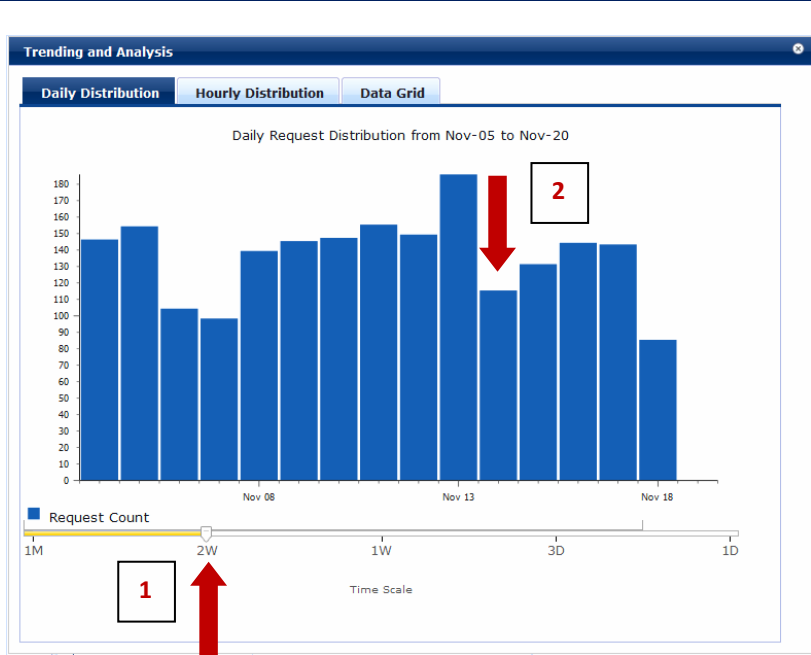
#### Analyze access distribution by day:

- Request access data is represented for the latest seven days
- Mouse-over a **bar** to see the number of requests processed
- Click on the **graph** to launch the advanced analysis window



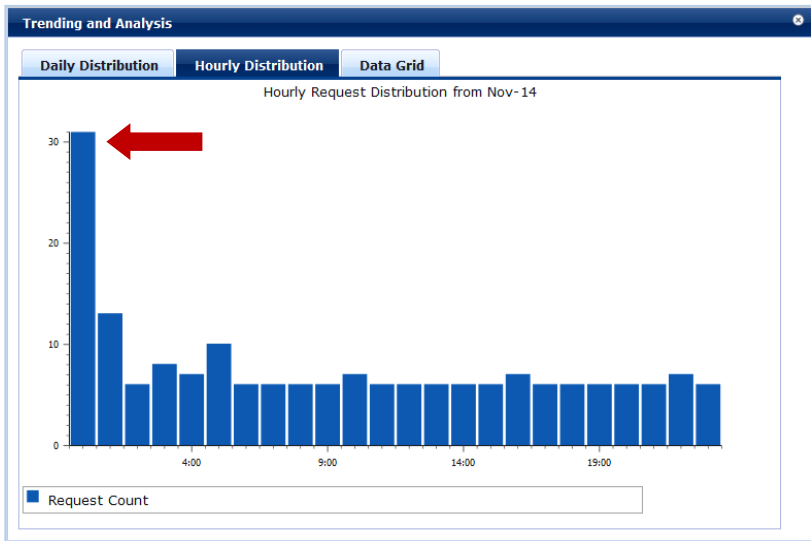
**See access request data by day:**

- **1** - Drag the **slider** to change the time-scale and associated data
- Mouse-over a **bar** to see the exact count for a given day
- **2** - Click the **bar** to launch access request distribution by hour



**See access request data by the hour:**

- Mouse-over a **bar** to see the number of requests processed
- Click a **bar** to see relevant data for access requests





**Details for previous step:**

- **1** - Browse records using the paging widget at the base of the window
- **2** - Click **Apply Filters** to add further constraints on this data

The screenshot shows a window titled "Trending and Analysis" with three tabs: "Daily Distribution", "Hourly Distribution", and "Data Grid". The "Data Grid" tab is active, displaying a table with the following data:

Username	Request Status	Network Device	Service	System Posture Token
pattabhi	Failure	192.168.5.219	Avenda Wireless Service	UNKNOWN
pattabhi	Failure	192.168.5.219	Avenda Wireless Service	UNKNOWN
001644b19320	Success	192.168.5.219	Avenda Unmanaged Hosts	UNKNOWN
pattabhi	Failure	192.168.5.219	Avenda Wireless Service	UNKNOWN
ron	Success	192.168.5.214	Avenda Wired Service	HEALTHY
pattabhi	Failure	192.168.5.219	Avenda Wireless Service	UNKNOWN
tetradius	Failure	192.168.5.214	...	UNKNOWN
pattabhi	Failure	192.168.5.219	Avenda Wireless Service	UNKNOWN
pattabhi	Failure	192.168.5.219	Avenda Wireless Service	UNKNOWN
			Avenda Wirel...	

At the bottom of the grid, there is a paging widget that says "Showing 1 - 26 of 31". A red arrow labeled "1" points to this widget. Another red arrow labeled "2" points to the "Apply Filters" button located at the top right of the grid area.

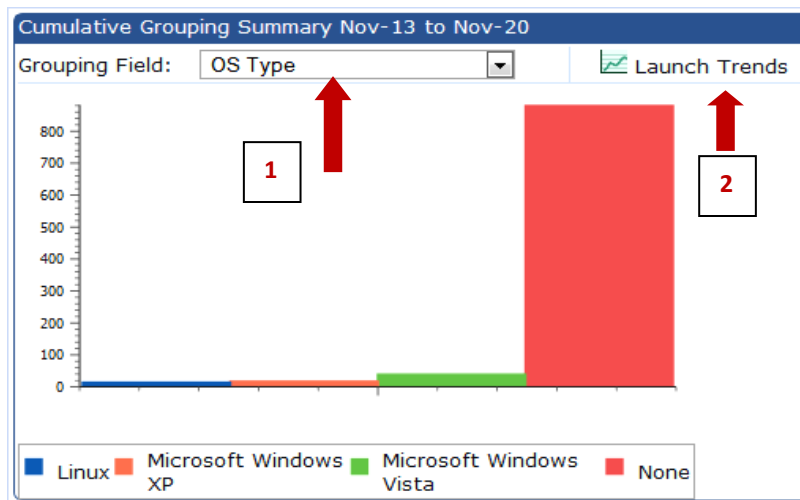
**Insight Notes:**

- Right-Click the header to show/hide columns
- Drag and drop columns to rearrange the grid

**Group Summary for Trends Distribution**

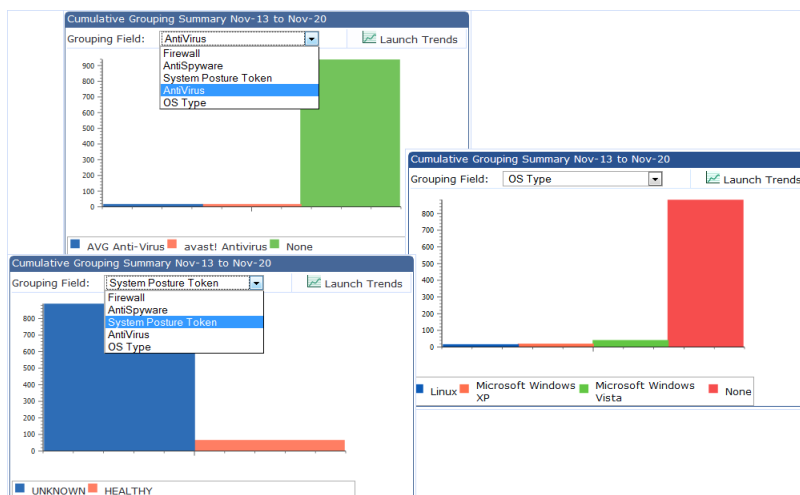
**Analyze trends on selected fields:**

- Analyze data based on fields selected for the report
- Mouse-over a **bar** to see specific data for the selected field
- **1** - Change **drop-down value** to see data for different fields
- **2** - Click **Launch Trends** to launch a time-based trend for this field (see *Time-based example on page 35 for screen details*)
- Click **anywhere** on graph to launch an advanced analysis window



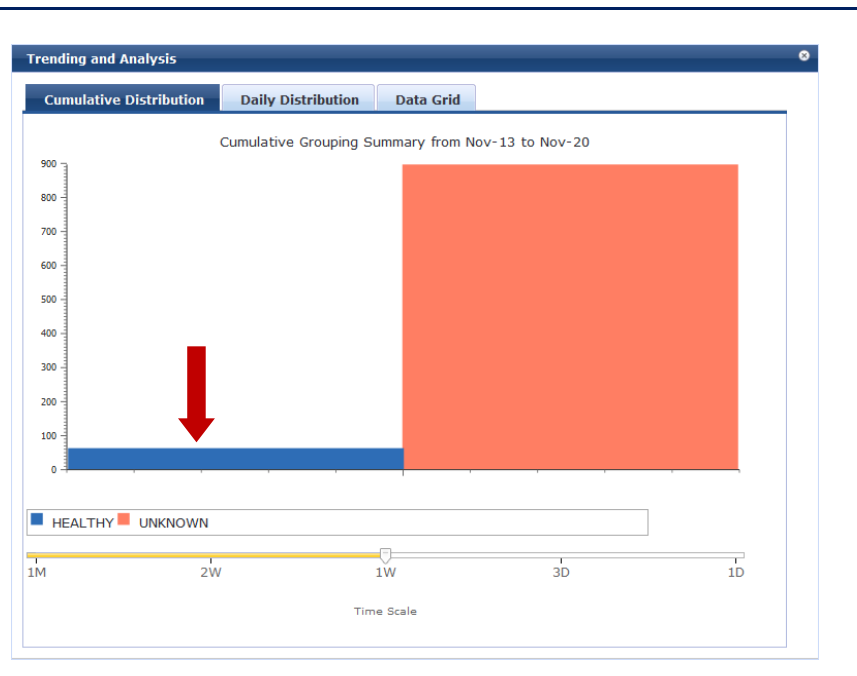
**View data by data field:**

- Select a different field from the **drop-down** to cycle through trending data



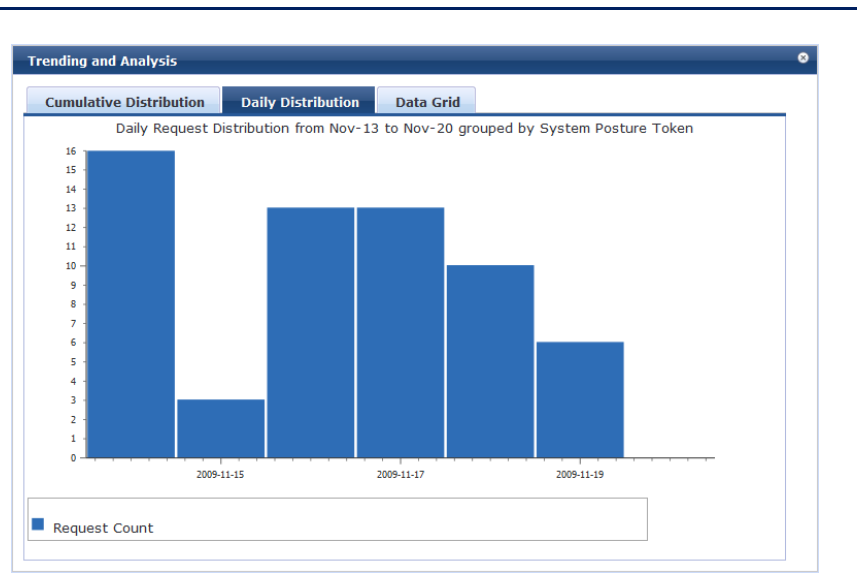
**Launch advanced analysis:**

- Mouse-over a **bar** to see the number of requests
- Click on a **bar** to see relevant data



**View daily details for the selected value in previous step:**

- Mouse-over a **bar** to see the number of requests processed
- Click on the **graph** to see relevant access requests



**Group Summary for Time-base Trending Analysis**

**Launch trends for a specific field**

- Mouse-over a **data point** to see the data for a given day
- Click the **data point** to see relevant access requests



**Dashboard view of Data grid section**

**Analyze live report data using Data Grid:**

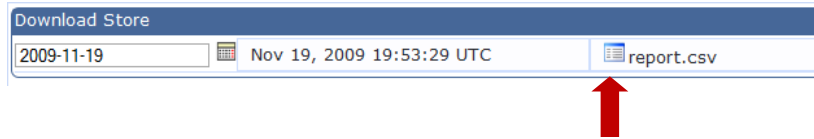
- Right-click the **headers** to Show/Hide columns
- **Drag and Drop** columns to rearrange the grid

Username	Request Status	Network Device	Service
testradius	Failure	192.168.5.214	...
testradius	Failure	192.168.5.214	...
trent	Success	192.168.5.214	Avend. Service
testradius	Failure	192.168.5.214	...
testradius	Failure	192.168.5.214	...
testradius	Failure	192.168.5.214	...

**Dashboard view of the Download Store**

**Download reports:**

- Select a **date** on the calendar to retrieve the list of reports
- Click on the **.CSV/PDF** icon to download the report

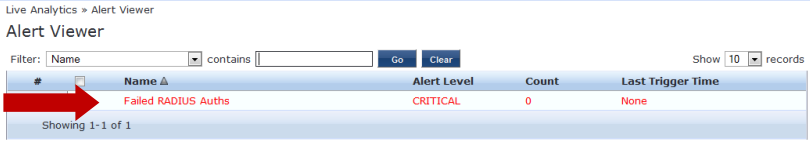
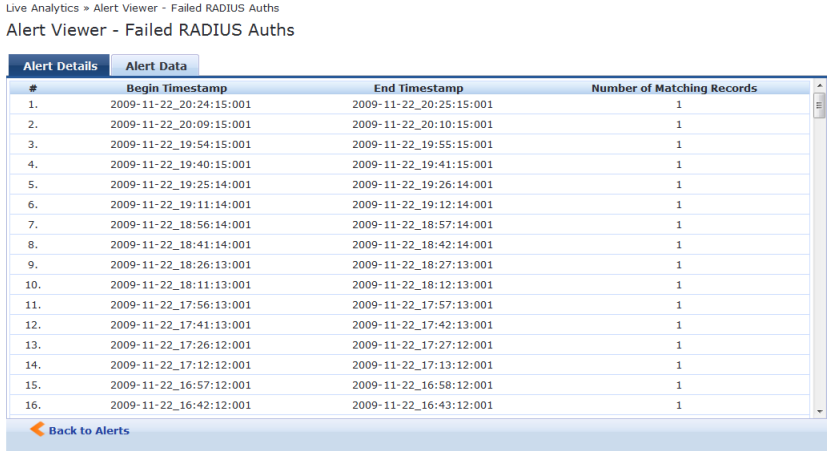
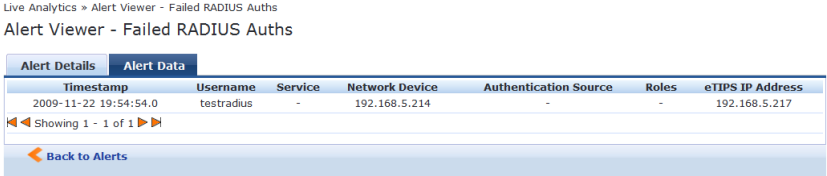
**Insight Notes:**

The Insight Dashboard is drill-down enabled. Click on any of the components to launch an advanced analysis window that lets you run complex filters on live data, that you can slice and dice to analyze trends for varying lengths of time.

## 4.2 Alert Viewer

Insight generates alerts whenever it synchronizes with its data source. A record of alerts reside in the Alert Viewer, which contains information such as a time-window in which the alert triggered, a count, and the severity as configured by the administrator.

### Viewing Alerts

<p><b>Start the alert viewer:</b></p> <ul style="list-style-type: none"> <li>Click on <b>alert</b> to launch (Alert details are launched only if the count is not zero)</li> </ul>	 <p>Live Analytics » Alert Viewer Alert Viewer</p> <p>Filter: Name [ ] contains [ ] Go Clear Show 10 records</p> <table border="1"> <thead> <tr> <th>#</th> <th>Name</th> <th>Alert Level</th> <th>Count</th> <th>Last Trigger Time</th> </tr> </thead> <tbody> <tr> <td></td> <td>Failed RADIUS Auths</td> <td>CRITICAL</td> <td>0</td> <td>None</td> </tr> </tbody> </table> <p>Showing 1-1 of 1</p>	#	Name	Alert Level	Count	Last Trigger Time		Failed RADIUS Auths	CRITICAL	0	None																																																										
#	Name	Alert Level	Count	Last Trigger Time																																																																	
	Failed RADIUS Auths	CRITICAL	0	None																																																																	
<p><b>Launch alert details:</b></p> <ul style="list-style-type: none"> <li>All triggered instances of this alert are shown here</li> <li>Each row displays the time window in which this alert was triggered, along with the number of access requests/events</li> <li>Click a <b>row</b> to view relevant access/event details</li> </ul>	 <p>Live Analytics » Alert Viewer - Failed RADIUS Auths Alert Viewer - Failed RADIUS Auths</p> <p>Alert Details   Alert Data</p> <table border="1"> <thead> <tr> <th>#</th> <th>Begin Timestamp</th> <th>End Timestamp</th> <th>Number of Matching Records</th> </tr> </thead> <tbody> <tr><td>1.</td><td>2009-11-22_20:24:15:001</td><td>2009-11-22_20:25:15:001</td><td>1</td></tr> <tr><td>2.</td><td>2009-11-22_20:09:15:001</td><td>2009-11-22_20:10:15:001</td><td>1</td></tr> <tr><td>3.</td><td>2009-11-22_19:54:15:001</td><td>2009-11-22_19:55:15:001</td><td>1</td></tr> <tr><td>4.</td><td>2009-11-22_19:40:15:001</td><td>2009-11-22_19:41:15:001</td><td>1</td></tr> <tr><td>5.</td><td>2009-11-22_19:25:14:001</td><td>2009-11-22_19:26:14:001</td><td>1</td></tr> <tr><td>6.</td><td>2009-11-22_19:11:14:001</td><td>2009-11-22_19:12:14:001</td><td>1</td></tr> <tr><td>7.</td><td>2009-11-22_18:56:14:001</td><td>2009-11-22_18:57:14:001</td><td>1</td></tr> <tr><td>8.</td><td>2009-11-22_18:41:14:001</td><td>2009-11-22_18:42:14:001</td><td>1</td></tr> <tr><td>9.</td><td>2009-11-22_18:26:13:001</td><td>2009-11-22_18:27:13:001</td><td>1</td></tr> <tr><td>10.</td><td>2009-11-22_18:11:13:001</td><td>2009-11-22_18:12:13:001</td><td>1</td></tr> <tr><td>11.</td><td>2009-11-22_17:56:13:001</td><td>2009-11-22_17:57:13:001</td><td>1</td></tr> <tr><td>12.</td><td>2009-11-22_17:41:13:001</td><td>2009-11-22_17:42:13:001</td><td>1</td></tr> <tr><td>13.</td><td>2009-11-22_17:26:12:001</td><td>2009-11-22_17:27:12:001</td><td>1</td></tr> <tr><td>14.</td><td>2009-11-22_17:12:12:001</td><td>2009-11-22_17:13:12:001</td><td>1</td></tr> <tr><td>15.</td><td>2009-11-22_16:57:12:001</td><td>2009-11-22_16:58:12:001</td><td>1</td></tr> <tr><td>16.</td><td>2009-11-22_16:42:12:001</td><td>2009-11-22_16:43:12:001</td><td>1</td></tr> </tbody> </table> <p>Back to Alerts</p>	#	Begin Timestamp	End Timestamp	Number of Matching Records	1.	2009-11-22_20:24:15:001	2009-11-22_20:25:15:001	1	2.	2009-11-22_20:09:15:001	2009-11-22_20:10:15:001	1	3.	2009-11-22_19:54:15:001	2009-11-22_19:55:15:001	1	4.	2009-11-22_19:40:15:001	2009-11-22_19:41:15:001	1	5.	2009-11-22_19:25:14:001	2009-11-22_19:26:14:001	1	6.	2009-11-22_19:11:14:001	2009-11-22_19:12:14:001	1	7.	2009-11-22_18:56:14:001	2009-11-22_18:57:14:001	1	8.	2009-11-22_18:41:14:001	2009-11-22_18:42:14:001	1	9.	2009-11-22_18:26:13:001	2009-11-22_18:27:13:001	1	10.	2009-11-22_18:11:13:001	2009-11-22_18:12:13:001	1	11.	2009-11-22_17:56:13:001	2009-11-22_17:57:13:001	1	12.	2009-11-22_17:41:13:001	2009-11-22_17:42:13:001	1	13.	2009-11-22_17:26:12:001	2009-11-22_17:27:12:001	1	14.	2009-11-22_17:12:12:001	2009-11-22_17:13:12:001	1	15.	2009-11-22_16:57:12:001	2009-11-22_16:58:12:001	1	16.	2009-11-22_16:42:12:001	2009-11-22_16:43:12:001	1
#	Begin Timestamp	End Timestamp	Number of Matching Records																																																																		
1.	2009-11-22_20:24:15:001	2009-11-22_20:25:15:001	1																																																																		
2.	2009-11-22_20:09:15:001	2009-11-22_20:10:15:001	1																																																																		
3.	2009-11-22_19:54:15:001	2009-11-22_19:55:15:001	1																																																																		
4.	2009-11-22_19:40:15:001	2009-11-22_19:41:15:001	1																																																																		
5.	2009-11-22_19:25:14:001	2009-11-22_19:26:14:001	1																																																																		
6.	2009-11-22_19:11:14:001	2009-11-22_19:12:14:001	1																																																																		
7.	2009-11-22_18:56:14:001	2009-11-22_18:57:14:001	1																																																																		
8.	2009-11-22_18:41:14:001	2009-11-22_18:42:14:001	1																																																																		
9.	2009-11-22_18:26:13:001	2009-11-22_18:27:13:001	1																																																																		
10.	2009-11-22_18:11:13:001	2009-11-22_18:12:13:001	1																																																																		
11.	2009-11-22_17:56:13:001	2009-11-22_17:57:13:001	1																																																																		
12.	2009-11-22_17:41:13:001	2009-11-22_17:42:13:001	1																																																																		
13.	2009-11-22_17:26:12:001	2009-11-22_17:27:12:001	1																																																																		
14.	2009-11-22_17:12:12:001	2009-11-22_17:13:12:001	1																																																																		
15.	2009-11-22_16:57:12:001	2009-11-22_16:58:12:001	1																																																																		
16.	2009-11-22_16:42:12:001	2009-11-22_16:43:12:001	1																																																																		
<p><b>View access request/event details for the selected alert:</b></p> <ul style="list-style-type: none"> <li>Browse records using the <b>paging widget</b> at the base of the window</li> <li>Logout when done</li> </ul>	 <p>Live Analytics » Alert Viewer - Failed RADIUS Auths Alert Viewer - Failed RADIUS Auths</p> <p>Alert Details   Alert Data</p> <table border="1"> <thead> <tr> <th>Timestamp</th> <th>Username</th> <th>Service</th> <th>Network Device</th> <th>Authentication Source</th> <th>Roles</th> <th>eTIPS IP Address</th> </tr> </thead> <tbody> <tr> <td>2009-11-22 19:54:54.0</td> <td>testradius</td> <td>-</td> <td>192.168.5.214</td> <td>-</td> <td>-</td> <td>192.168.5.217</td> </tr> </tbody> </table> <p>Showing 1 - 1 of 1</p> <p>Back to Alerts</p>	Timestamp	Username	Service	Network Device	Authentication Source	Roles	eTIPS IP Address	2009-11-22 19:54:54.0	testradius	-	192.168.5.214	-	-	192.168.5.217																																																						
Timestamp	Username	Service	Network Device	Authentication Source	Roles	eTIPS IP Address																																																															
2009-11-22 19:54:54.0	testradius	-	192.168.5.214	-	-	192.168.5.217																																																															

## 5 Summary

In this Jumpstart guide, you have configured and viewed the most common components of Avenda Insight advanced reporting application:

- Package configuration
- Configuration of attributes
- End user deployment

You are now capable of administering an 802.1X deployment to endpoints of any type in a short timeframe, across a wide geographic area. Subsequent configuration updates can also be “pushed” to the user community with minimal IT helpdesk involvement.

## Notes:

### **Avenda Systems**

3255 Scott Blvd, B2, Suite 102

Santa Clara, CA 95054

Phone: 408.748.0902

Fax: 408.748.0906

[www.avendasys.com](http://www.avendasys.com)

Copyright © 2010 Avenda Systems, Inc. All rights reserved worldwide. Avenda Systems, its product and program names and design marks are trademarks of Avenda Systems, Inc. All other trademarks mentioned in this document are the property of their respective owners.