
# VOSS Insights
# Arbitrator Administration Guide

Release 22.2

Oct 18, 2022

## Legal Information



DOCUMENT ID: 20221018103412

# Contents

# 1. What's New

## 1.1. Arbitrator Administration Guide: Release 22.2

- EKB-13343: Cannot run backup to external system. See: *Configuration*

  Added details on nfs option and new Check NFS buttons.

# 2. Getting Started

## 2.1. Introduction

Welcome to Insights Arbitrator, a powerful log analytics platform that allows multiple data sources and log formats to be consumed, extracted, analyzed, and correlated, for complete event, alarm and systems monitoring.

This guide describes how to use and administer the Arbitrator platform. You can use this guide for help with importing assets, importing scripts, configuring new correlation rules, searching logs, assigning scripts to assets to create probes, and for overall performance management of the systems monitored.

---

**Note:** This guide is aimed at system administrators and users responsible for configuring and monitoring the Correlation platform. Users should have a working knowledge of operating systems, software applications, and network elements.

---

The Arbitrator platform design allows it to be used in multiple workflows. While you won't need to follow any particular linear flow, some elements must be configured in a specific order. Those will be pointed out in each section.

This guide covers the following:

- Correlate - the main user interface, which allows you to visualize the monitored systems and to manage alerts for these systems. The views within this workspace are constantly updating with newly gathered data.
- Configuration - this is the workspace used to install and set up the platform.

## 2.2. Arbitrator Licensing

### 2.2.1. Overview

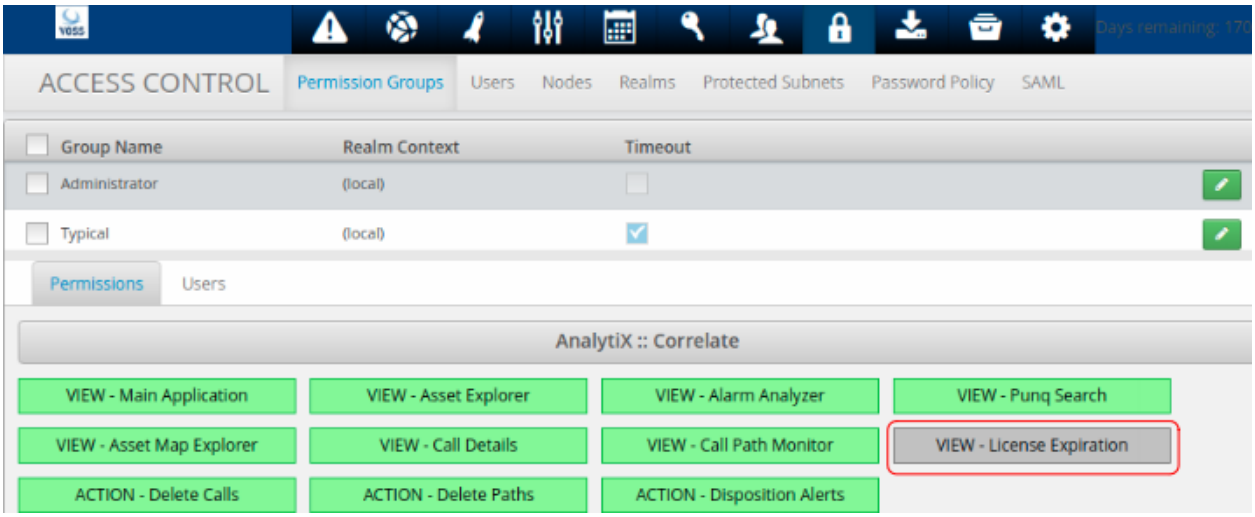
You can view the Arbitrator License remaining days in the user interface, once you log in.

This setting can be enabled (display) or disabled (hide).

### 2.2.2. Show or Hide Days Remaining from the UI

You can choose to show or hide the license days remaining from the main user interface. To do this:

1. In **ACCESS CONTROL**, select **Permission Groups**.
2. Toggle the following setting: **VIEW - License Expiration**




### 2.2.3. View License Days Remaining

To see how many days left, from the main menu, for a logged in user:

1. Choose **About**
2. Check the **DAYS LICENSED** and **DAYS REMAINING** values.

### 2.2.4. Load a License File

To load a license file:

1. Obtain the license file
2. Choose **About**
3. Click **EDIT PRODUCT KEY** and replace it with the one from the license file.

**Note:** When updating a license file, any custom theme that is applied remains active.

# 3. Correlate

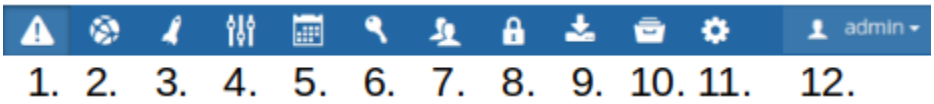
## 3.1. Correlate

### 3.1.1. Menu Bar

There are distinct functional ‘Views’ within the interface. Each will be covered in its own section of this guide.

- Policy Monitor
- Asset Map Explorer
- Asset Explorer
- Alarm Analyzer
- Event Search
- Call Path Monitor
- Call Detail Monitor

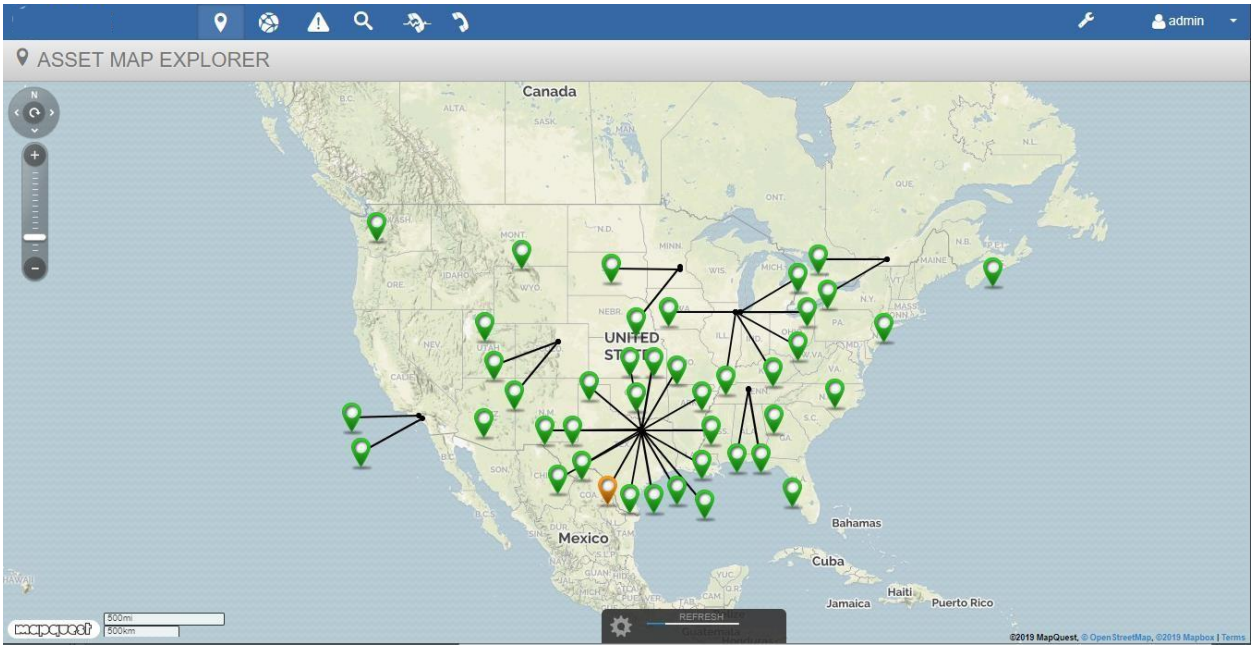
This menu is located at the top of the browser page and allows you to navigate to each of the Arbitrator views. Each are shown below:




1. Policy Configuration
2. Asset Configuration
3. Probe Configuration
4. Controls
5. Response Procedures
6. Credentials
7. Customers
8. Access Control
9. Import / Export
10. Archive Management
11. Tools
12. Admin

## 3.1.2. Assets

### Asset Map Explorer



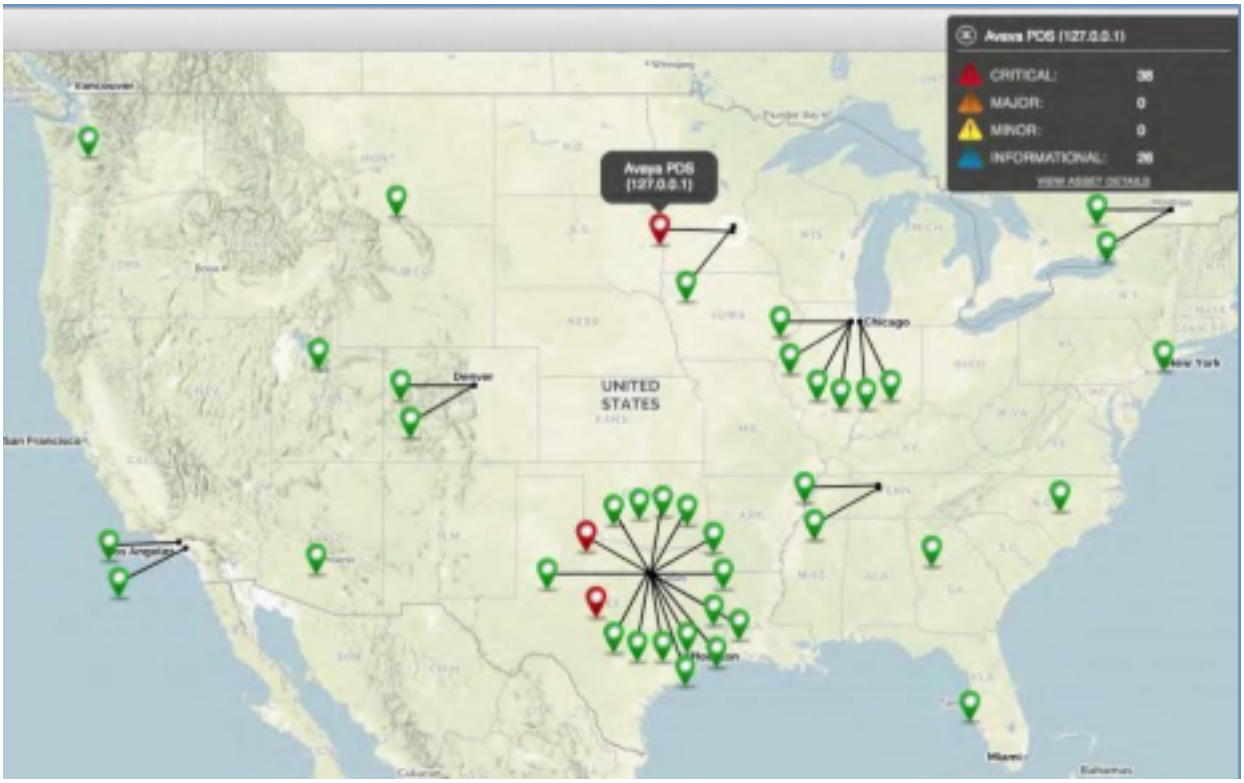

This view displays all of the defined assets in the system on a map for visual grouping according to their physical location. The location or address of the assets are input in the asset configuration section within the Configuration interface. This view is integrated with the MapQuest API (Internet access required to display the map).

Note: The system allows the ability to import a .csv file of assets and addresses.

### Asset Overview

Each Asset is colored to reflect its current Alert Status. The status colors available and their meanings are below:

- Red (Critical)
- Orange (Major)
- Yellow (Minor)
- Blue (Informational / Notification)
- Green (Healthy)




You can click on any of the assets to display the summarized alarm statistics for that asset. A box will open in the upper right corner of the screen to show the details. To see greater detail about the status of the asset, click on the underlined View Asset Details in the bottom of the box. This will take you to the Asset Details view. (See Asset Details view under the Asset Explorer Section)

### Asset Explorer

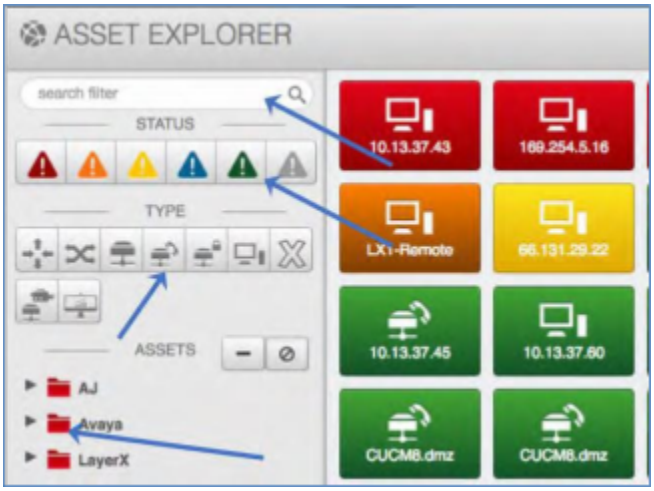
Asset Explorer gives a view into the current alarm state of the assets monitored by Arbitrator.

Only devices created as Assets in the Arbitrator system will be rendered in the view. Since Correlated events create alarms in the system, asset icon colors will change to reflect the severity level of the alert. Assets display the color of the current highest-level alert for that asset in the system.

Alert Severity Levels:

- Red (Critical)
- Orange (Major)
- Yellow (Minor)
- Blue (Informational / Notification)
- Green (Healthy)

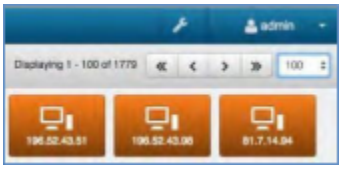

### Asset Filtering




The Assets displayed can be filtered using the filtering pane on the left. This includes:

- Filtering by Alert Severity levels
- Asset Type
- Defined Asset Groups
- Keyword

### Asset Explorer Navigation




The Asset Explorer will display up to 100 assets per page. Use the navigation button in the top right to grab the next 100 assets or the specific increment you have set.

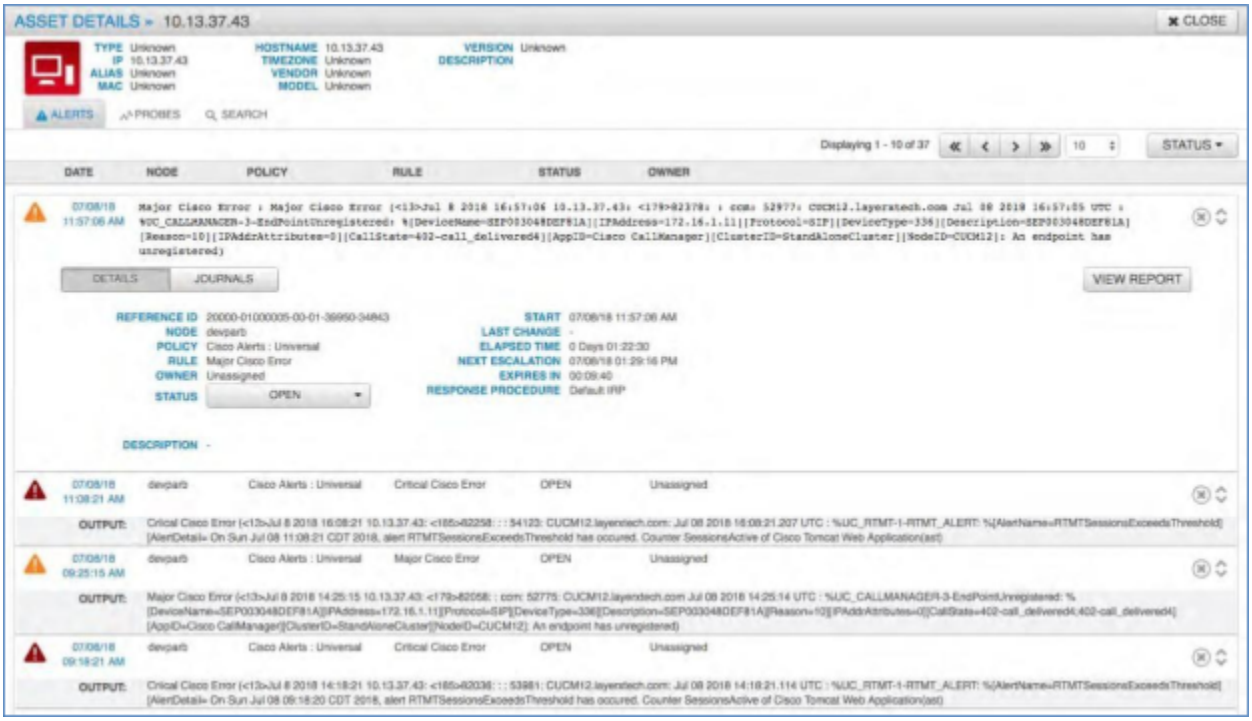
### Asset Details View

The Asset Details View is opened when you double click on any of the assets in the Asset Explorer view. Once open the view contains 3 tabs:

- Alerts
- Probes
- Search

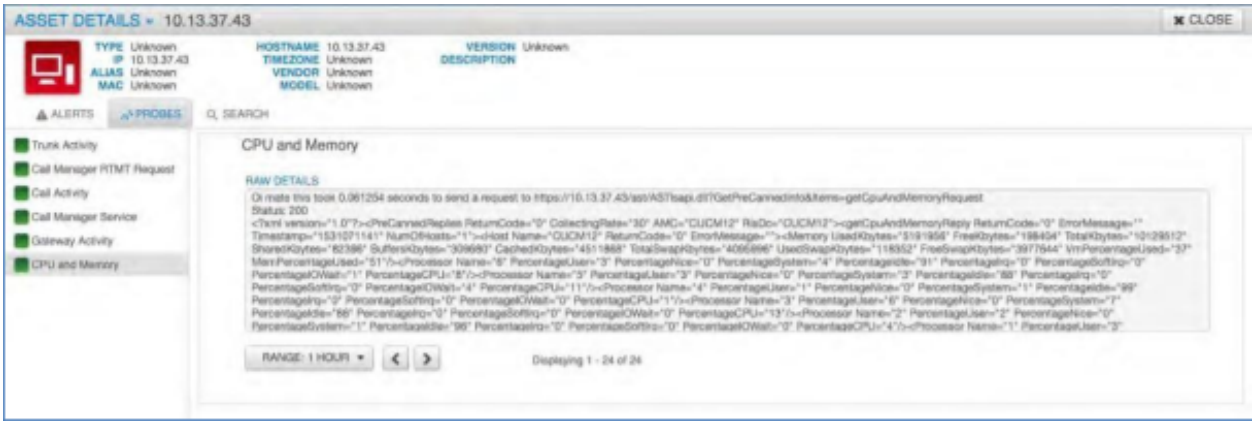
Click Close in the upper right corner of the screen to return to the Asset Explorer view.

### Asset Details: Alerts Tab




This tab displays all alerts associated with the asset and allows the user to disposition, add alert journal entries for the alert and see a report of the alert and events. (See Alert Disposition, Alert Journal and View Report within the Alert Analyzer Section)

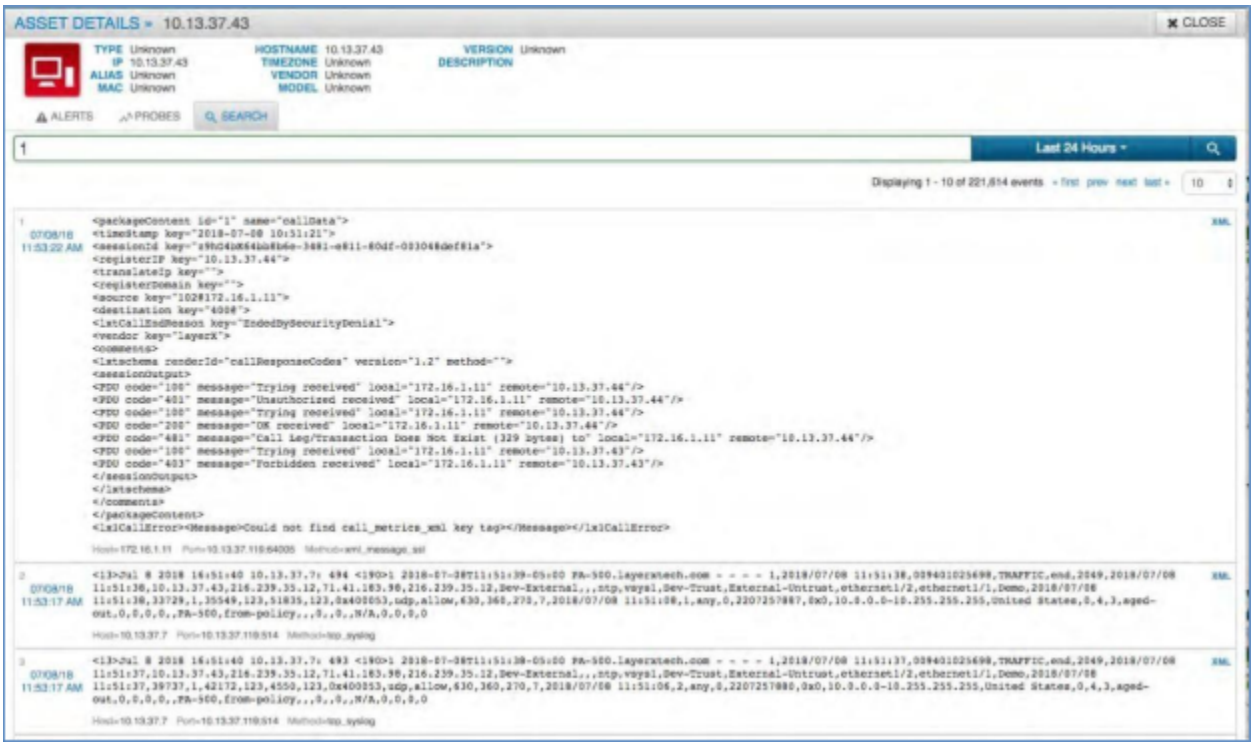
### Asset Details: Probes




This tab displays all probes associated with the asset. Clicking on each probe will display the probes output. If output is a numerical value, such as CPU usage, then a graph will be displayed of that value over time. If the probe output is non-numerical then just the last probe output will be displayed.

### Asset Details: Search

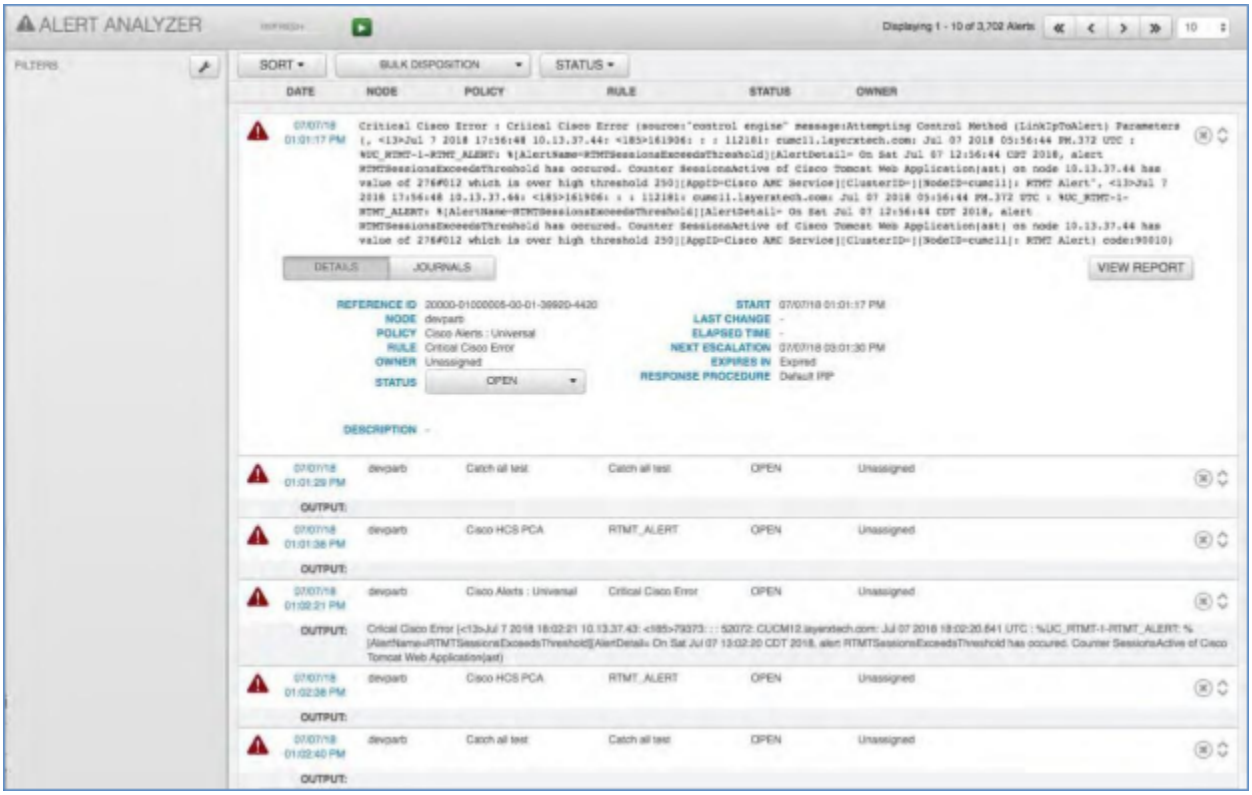
This tab contains an event search bar tied to the data only associated with this asset. This allows the user to search all logs / events by this particular asset versus the entire index data store. (See Event Search for more details)



## 3.1.3. Alerts

### Alert Analyzer

The Alert Analyzer screen displays all of the alerts coming into the system based on a first in / last out presentation. It allows the user to see the alerts as they are happening or ones that have been in existence for a period of time. It also provides the ability to disposition the alerts based on activity as well as view a report with specific details associated with the alert. There are also several filter and sort options available to apply to the view.

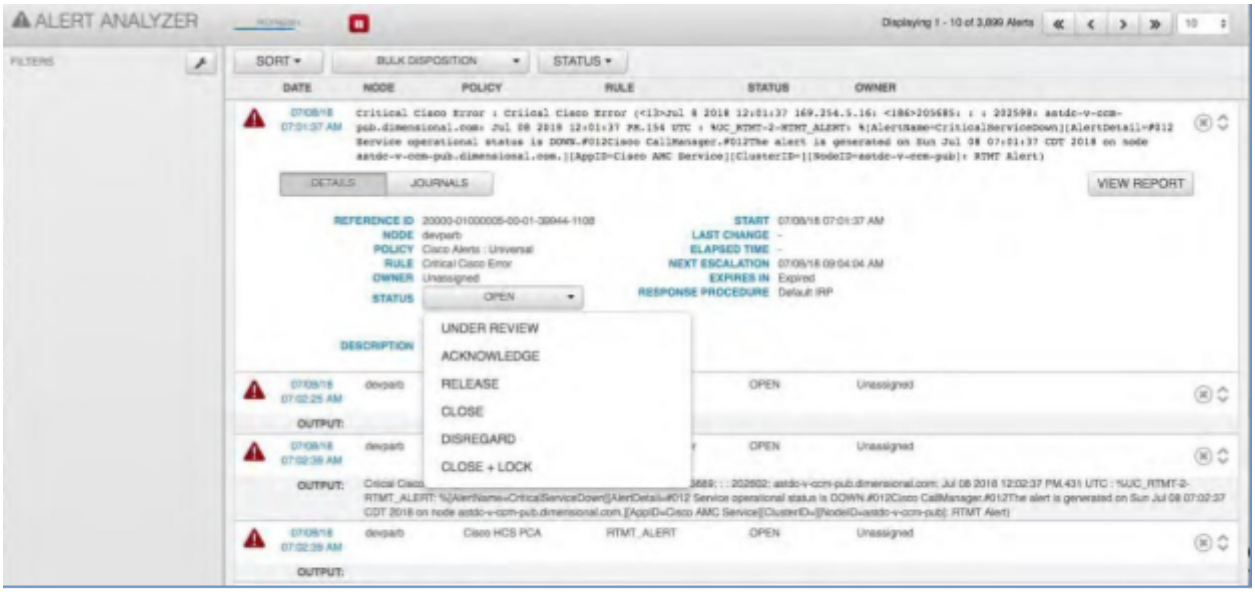



### Alert Disposition

The drop-down box allows you to set the status of each alert. The can be set one at a time or by bulk. The available options are:

- Open: This is a new alert.
- Under Review: Moved out of the open state and the alert journal can still be edited.
- Acknowledge: Moved out of the open state and the alert journal can still be edited.
- Release: Moved out of the open state and the alert journal can still be edited.
- Close: Moved out of the open state and the alert journal can still be edited.
- Disregard: The alert is deleted from the system.
- Close and Locked: Moved to a closed state and the alert journal cannot be edited.

To disposition an alert simply open the alert by expanding it (click the up and down arrows to the far right of the alert). Once open select the drop-down box next to “Status” and select the disposition state.

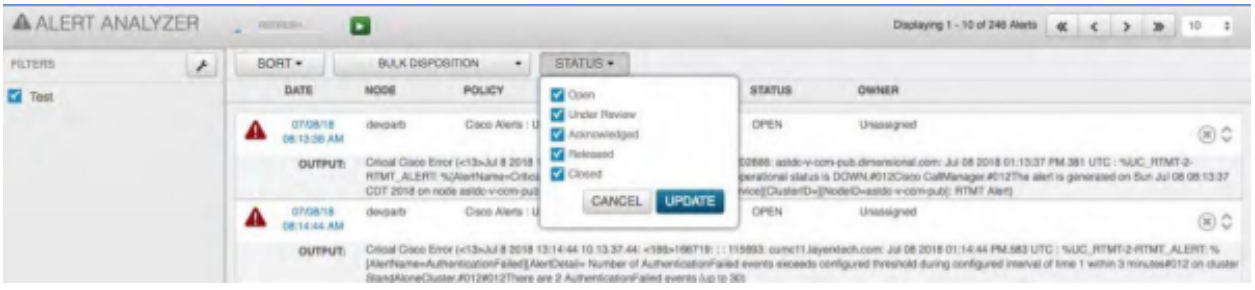




Bulk Disposition: This will allow the user to disposition a group of alerts at once. First apply the required filter to the alerts by using the Filter Manager (See Alert Filters). Once you have the group of alerts filtered then select the desired disposition state from the “Bulk Disposition” drop-down box.

### Filtering by Disposition

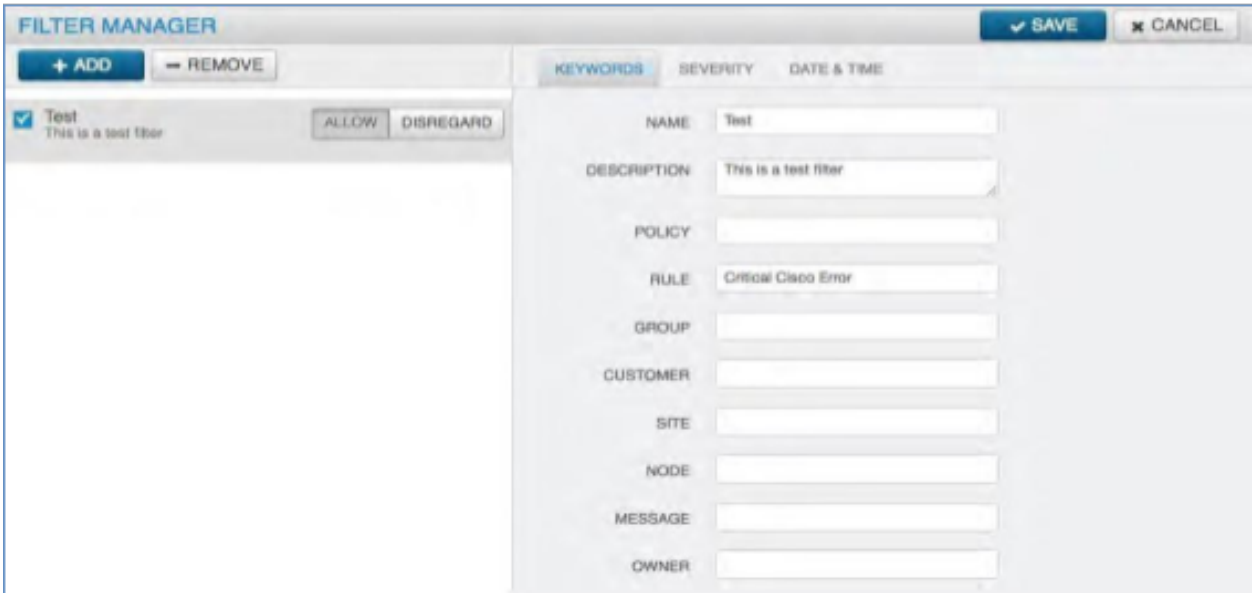
By clicking the drop-down box “Status” you can choose to see only the alerts with a specific disposition status. Once open select your choice(s) by checking the boxes and click update. The screen will show only the ones you have selected.



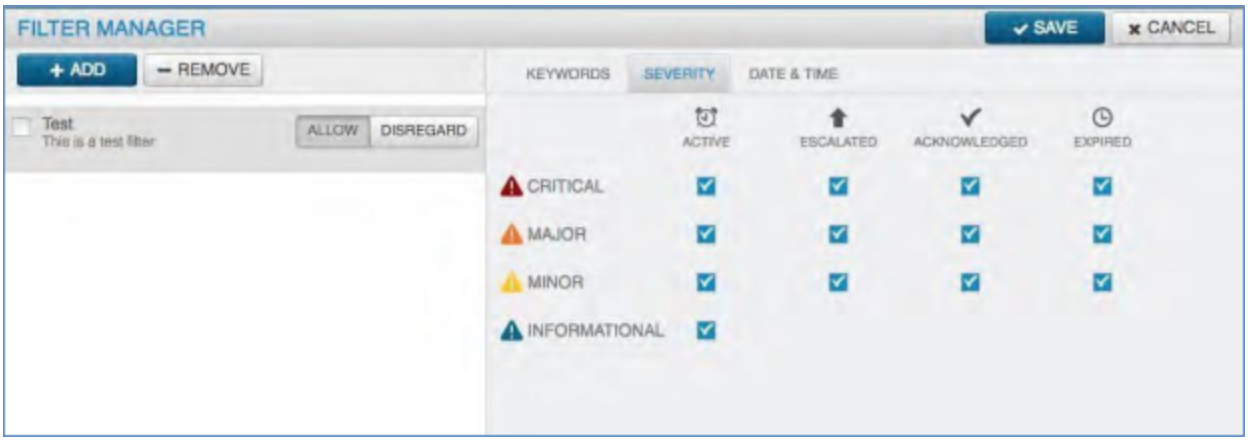
### Alert Filters

Alert Filters provide the ability to filter all of the alerts by Keywords, Severity and Date & Time. Open the “Filter Manager” by selecting the wrench icon in the top left of the screen next to the word Filters. Click the “Add” button to add a new filter.

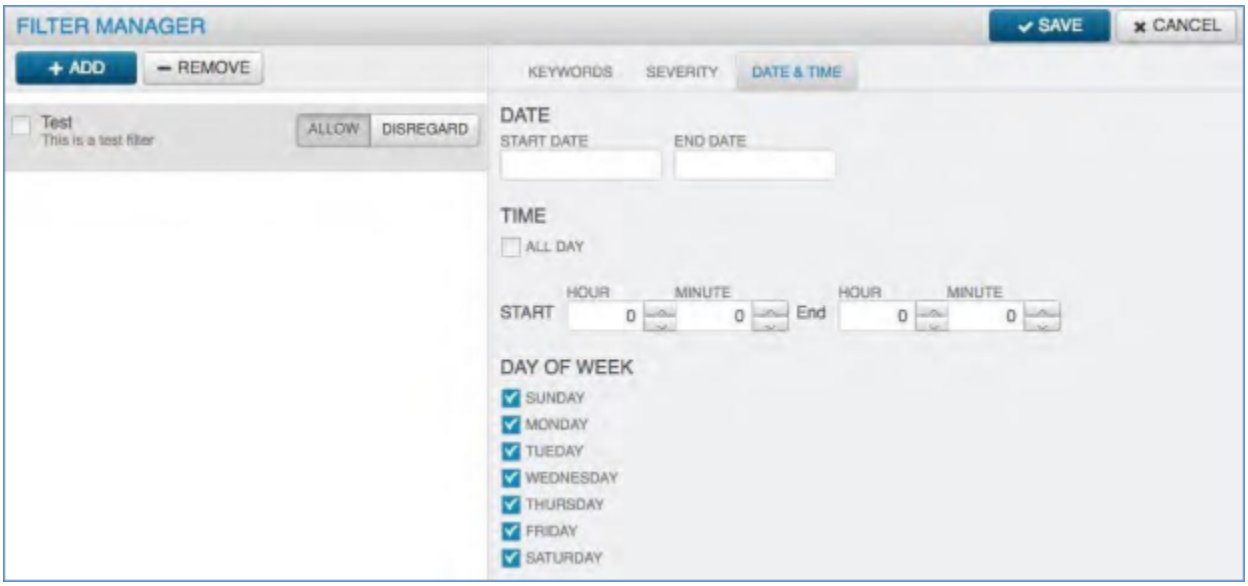
- Keywords: Fill in the detail to filter by. Choose to enter one, many or all of the criteria fields.
  - Name: Sets the name of the filter for your reference
  - Description: Description of the filter
  - Policy: Filter by the name of the correlation policy
  - Rule: Filter by the name of the correlation rule
  - Group: Filter by the name of the group
  - Customer: Filter by the name of the customer
  - Site: Filter by the site
  - Node: Filter by the node
  - Message: Filter by the message
  - Owner: Filter by the owner




- Severity: The filter can be set based on the chosen severity or severities. Additionally, the state or states can be chosen with each severity. Click the levels desired.
  - Active: Alert is currently in one of the active states
  - Escalated: Alert has been escalated based on the timer in the correlation rule
  - Acknowledged: Alert is in an acknowledged disposition state.
  - Expired: Alert has expired based on the timer set in the correlation rule




- Date & Time: The filter can be set based on a date range, by “All Day”, by a specific start and end time, by the day of the week or any combination.

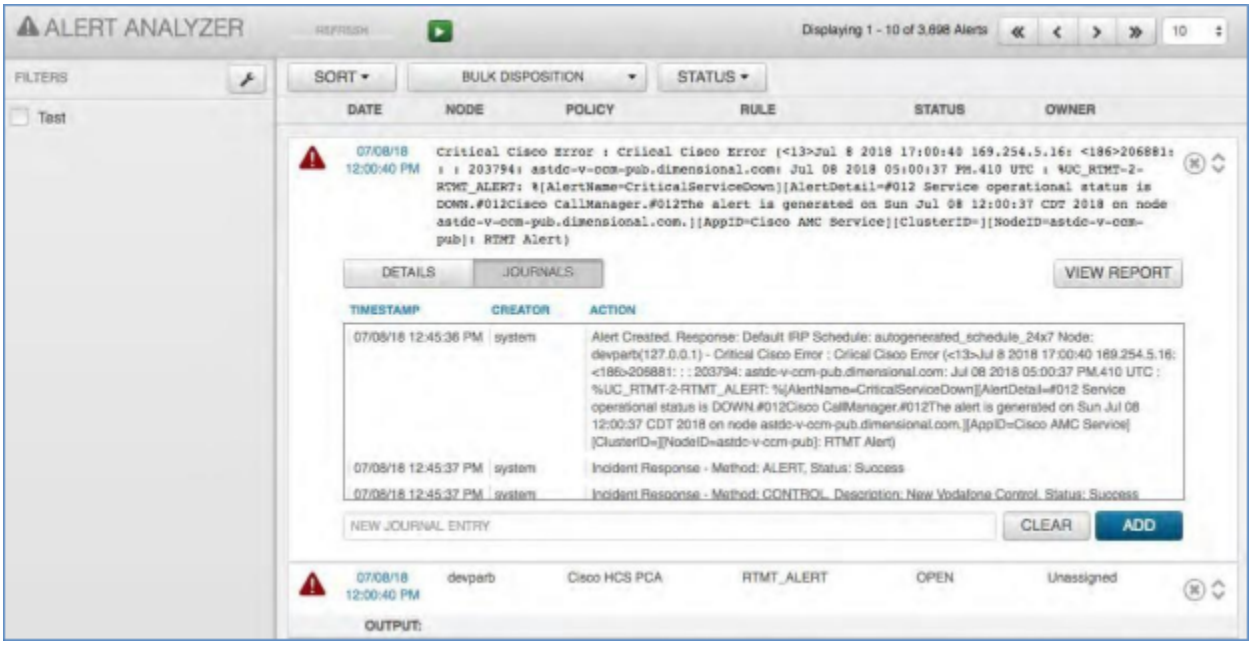



### Alert Journal

The Alert Journal will show the history of the alert and the actions taken both by the system and by the user. Additionally, a user can add a journal entry to update status or actions taken.

To add an Alert Journal:

- Click the Pause button to stop the automatic refresh
- Expand the Alert you want to add an entry to by clicking the expand icon
- Click the Journals Button
- Type the journal entry into the text box where it says NEW JOURNAL ENTRY
- When done Click Add
- Click the Play button to stop the pause and allow to refresh

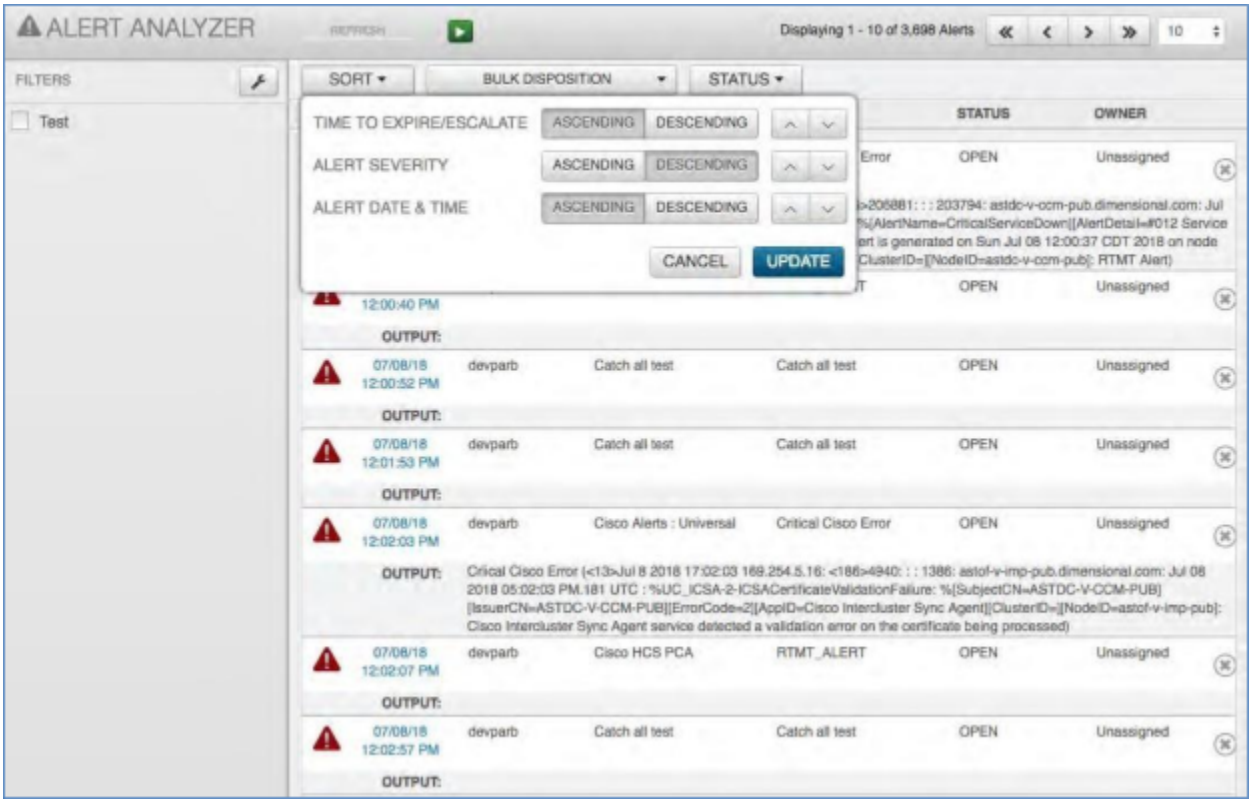



### Alert Sorting

The alerts shown on the Alert Analyzer can be sorted based on three categories:

- Time to Expire / Escalate
- Alert Severity
- Alert Date & Time

These three choices determine the sorting of the alerts on the Alert Analyzer screen. Each one can be toggled between ascending and descending order. Additionally, the order of each one will be the first to last in priority. This can be changed by clicking the down or up button next to each category.




## 3.1.4. Search

### Event Search

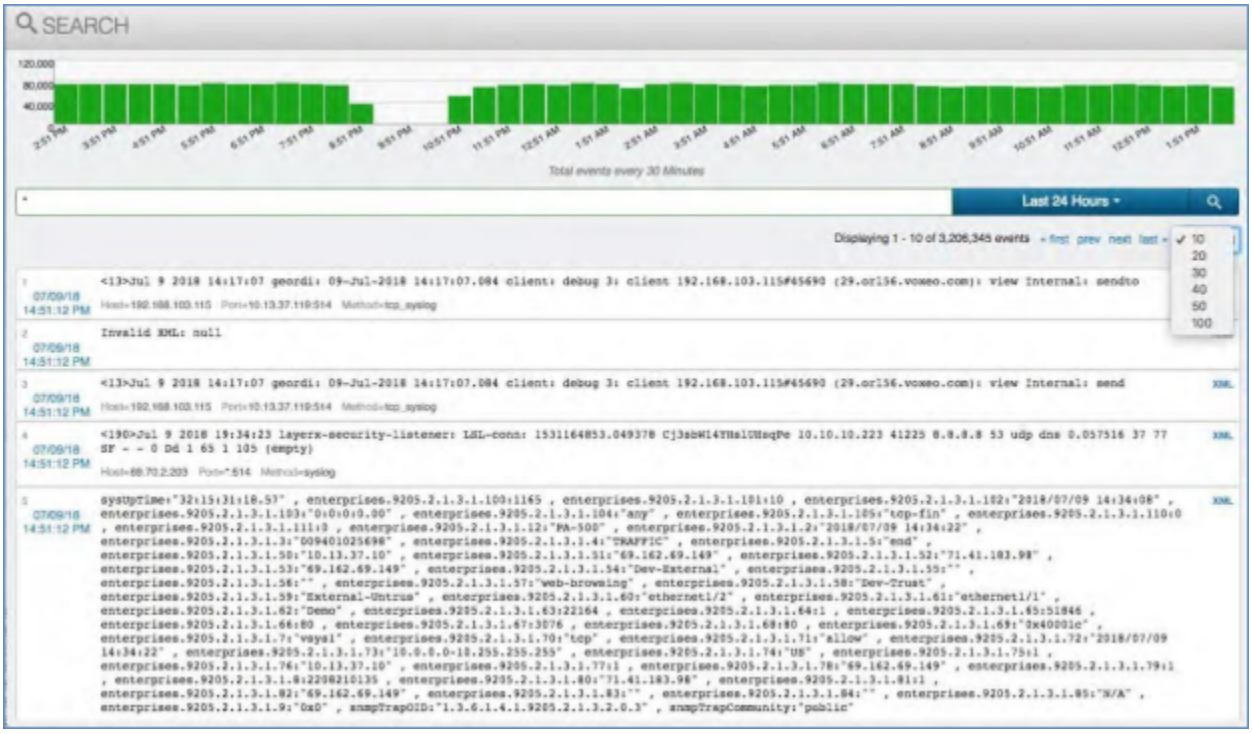
The Event search view provides access to all the raw data coming into Arbitrator Correlation and provides a simple interface to search and display it. The Arbitrator Correlation platform builds a dictionary of all of the words it has absorbed from all of the logs it has received and enables rapid search across large volumes of data. Essentially making an otherwise difficult amount of data quickly searchable and more useable.

### Simple Searching

To perform a simple search across all of the logs based on the default time of “Last 24 Hours” use the “*” wildcard character.

- In the search text input field type *
- Press Enter or click the magnifying glass icon

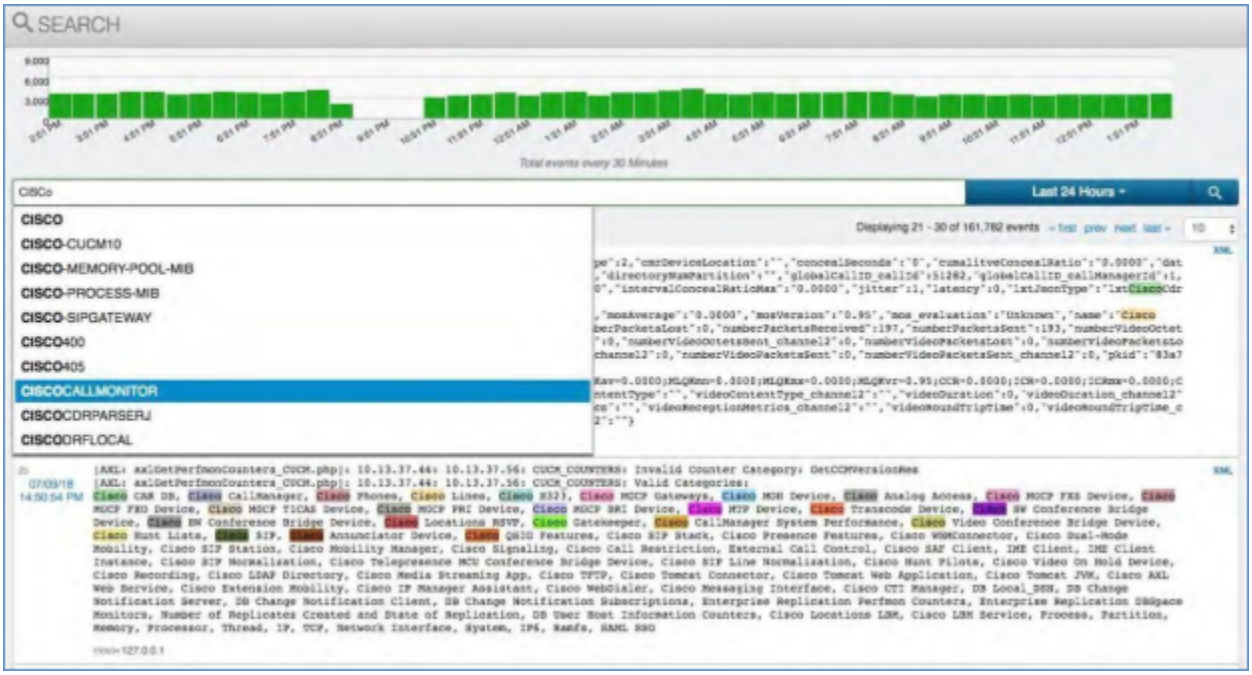
All log data received in the last 24 hours will be returned. The default number of logs per page is 10 but can be expanded by opening the drop-down box under the time bar and selecting the number desired.




### Keyword Searching

To perform a keyword search across all of the logs based on the default time of “Last 24 Hours” start by typing in the word that you know is present in your data, such as “Cisco”. As you type the word the event search will begin to auto suggest your keyword based on the data the Correlation platform has collected. Once you have finished press enter, select the word in the drop-down list or click the magnifying glass icon.

All log data that contains the keyword in the last 24 hours will be returned. The default number of logs per page is 10 but can be expanded by opening the drop-down box under the time bar and selecting the number desired.




### Utilizing Conjunctions with Searching

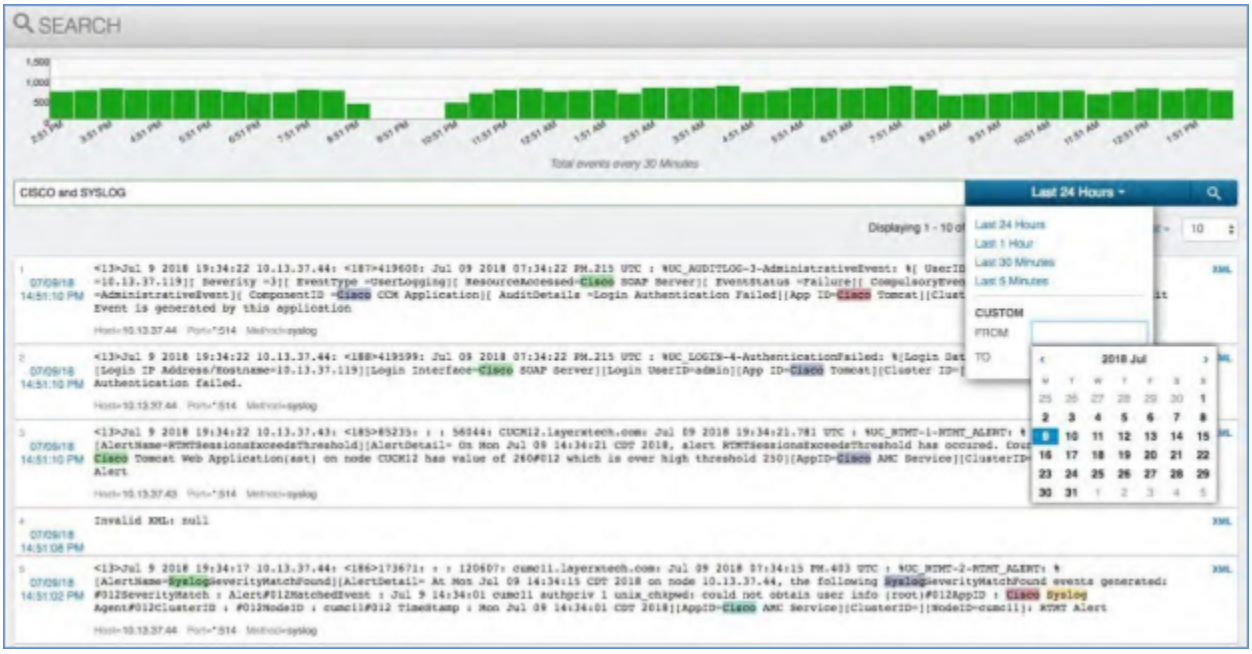
The Event Search allows the use of conjunctions to combine keywords which will assist you in being more specific in your search. The conjunctions available are AND, OR and NOT. To perform a search with conjunctions across all of the logs based on the default time of “Last 24 Hours” start by typing in the word that you know is present in your data, such as “Cisco”, followed by the conjunction then the next word. Once you have finished press enter, select the word in the drop-down list or click the magnifying glass icon.

All log data that contains the keywords in the last 24 hours will be returned. Note: when using a conjunction in the search the logic must match or no data will be returned. The default number of logs per page is 10 but can be expanded by opening the drop-down box under the time bar and selecting the number desired.


### Date Range Searching

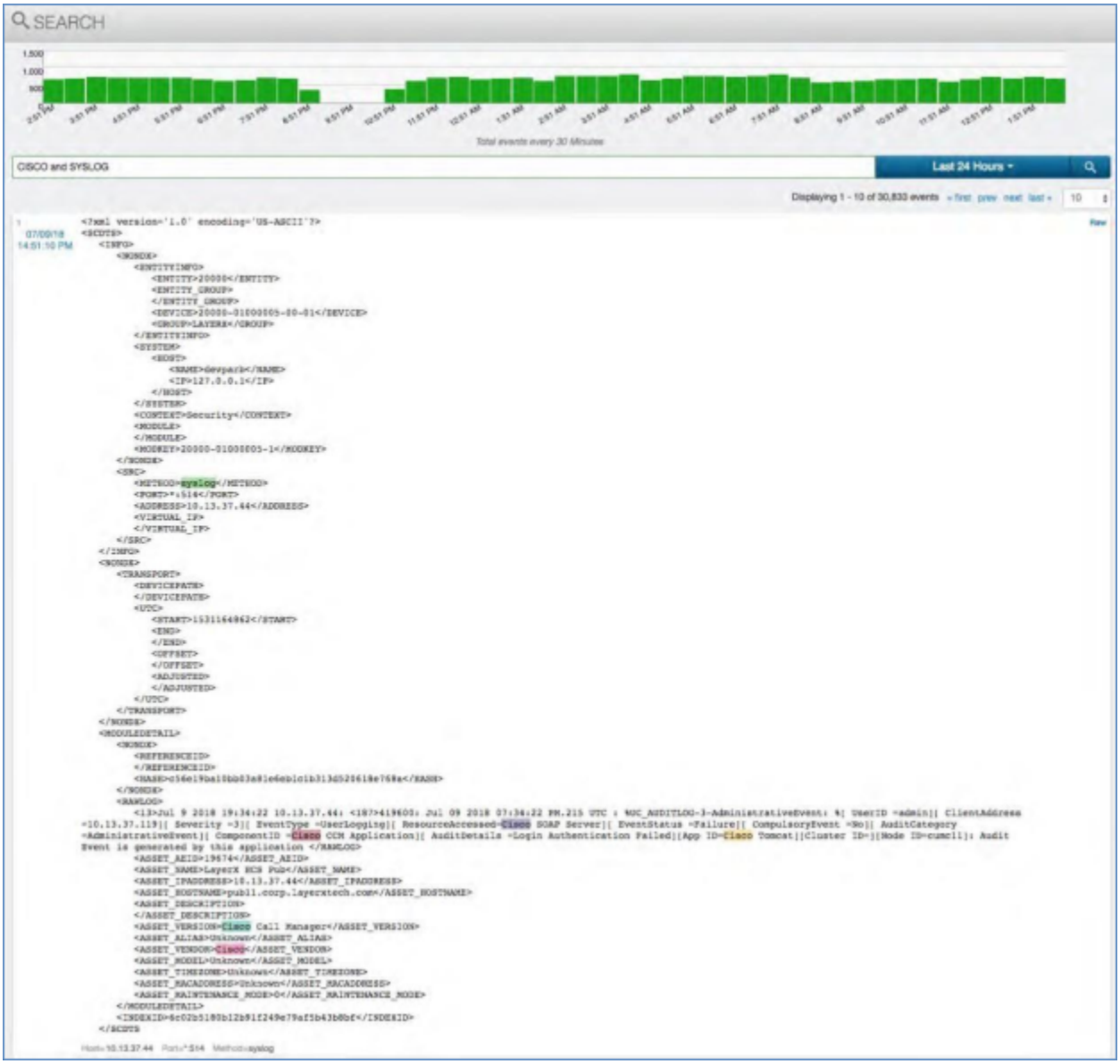
With any of the above methods the user can also select the specific date to search for the data. The default is the last 24 hours but by opening the drop-down bar several options are presented.

- Last 24 Hours: The default
- Last 1 Hour
- Last 30 Minutes
- Last 5 Minutes
- Custom date range showing from and to. Clicking in the “From” box opens up a calendar from where you can select the specific from date you desire. Clicking in the “To” box will do the same.




### Search Result Meta-Data

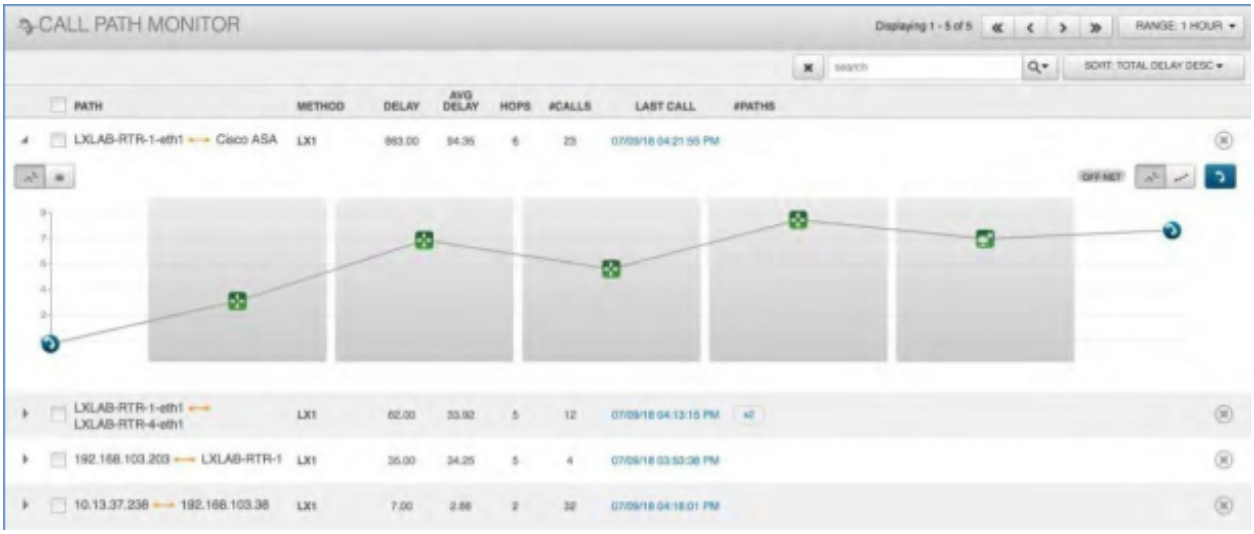
The Event Search engine utilizes the core processes of the Arbitrator Correlation platform to store, tag and manage the data. To the right of each log entry is a blue “XML”. Clicking on this will open up all of the XML representation of the data along with some very important added elements. In particular are the Entity ID’s which server as the basis for making every event unique and formulating the “Reference ID” seen in the Alert Analyzer screen. Additionally, if applicable, a hash of the raw log is available for compliance purposes. To go back to the main search screen simply click the blue “Raw”.




## 3.1.5. Call Path

### Call Path Monitor

The Call Path Monitor serves as one of the base screens for managing Unified Communications and the particular call path that a Voice over IP call takes. It will display the paths or routes that a call took from the source to the destination. Each path contains the IP Addresses, number of hops, delay and latency during the call.




### Sorting Call Paths

The screen and the represented call paths can be sorted by three variables:

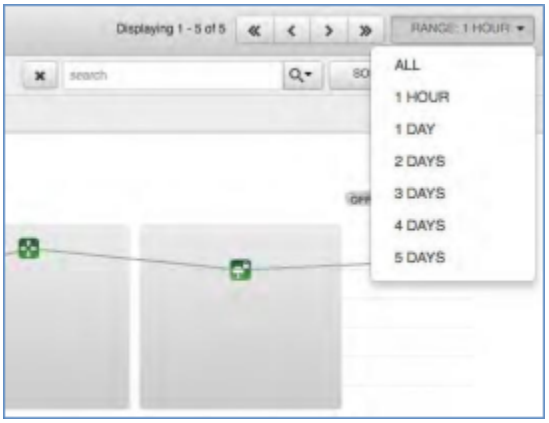
- Total Delay: The total latency on the call.
- Average Delay: The average latency on the call.
- Total Hops: The total number of layer-3 hops the call took.

Each selection also has the choice of selecting ascending or descending order.

### Time Range for Call Paths

This provides the option of selecting the time range in which to show the call paths collected. Click the "Range" drop-down button. The available options are:

- All
- 1 Day
- 2 Days
- 3 Days
- 4 Days
- 5 Days



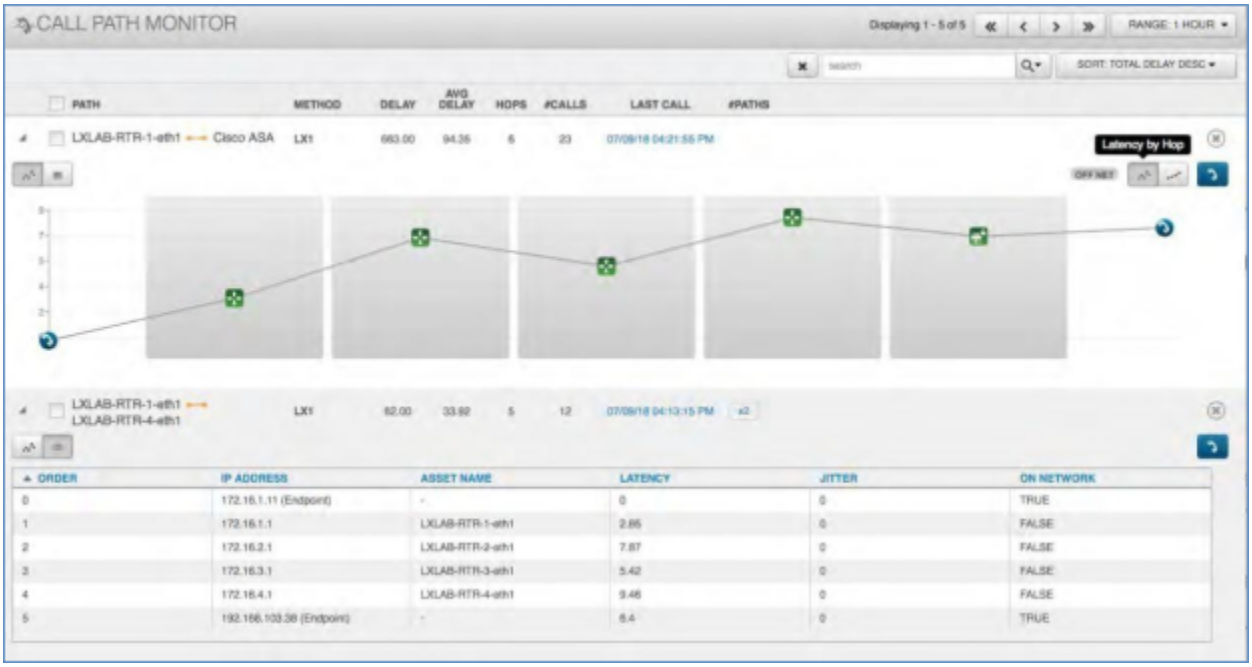

### Expanding Call Paths

Expanding a call path allows you to see the path by hop or by IP Address. In addition, it provides an option to view it by the total per hop or cumulative delay, latency, and Jitter. The expanded view also shows you whether the call was ON Network or OFF Network. The expanded view can be toggled to show in graph or table views.

To expand a call path and toggle between graph and table views:

- Click arrow icon next to the call path you want to expand

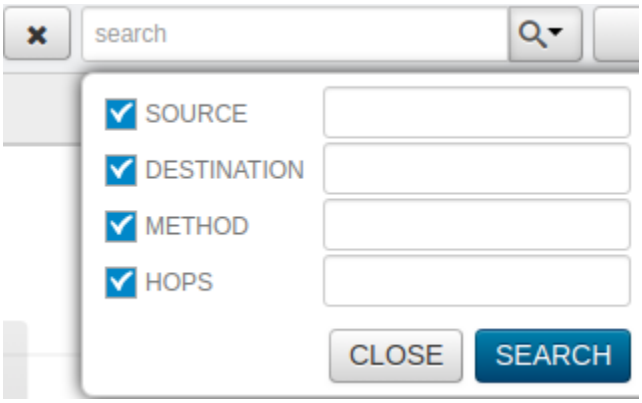
By default, the view will be in graph mode. To switch to the table view, simply choose the table view icon in the upper left corner of the now expanded call path.




### Searching Call Paths

Each Call Path has several fields you can utilize to search and filter for the call(s) that you are interested in. The fields available are:

- Source
- Destination
- Method
- Hops



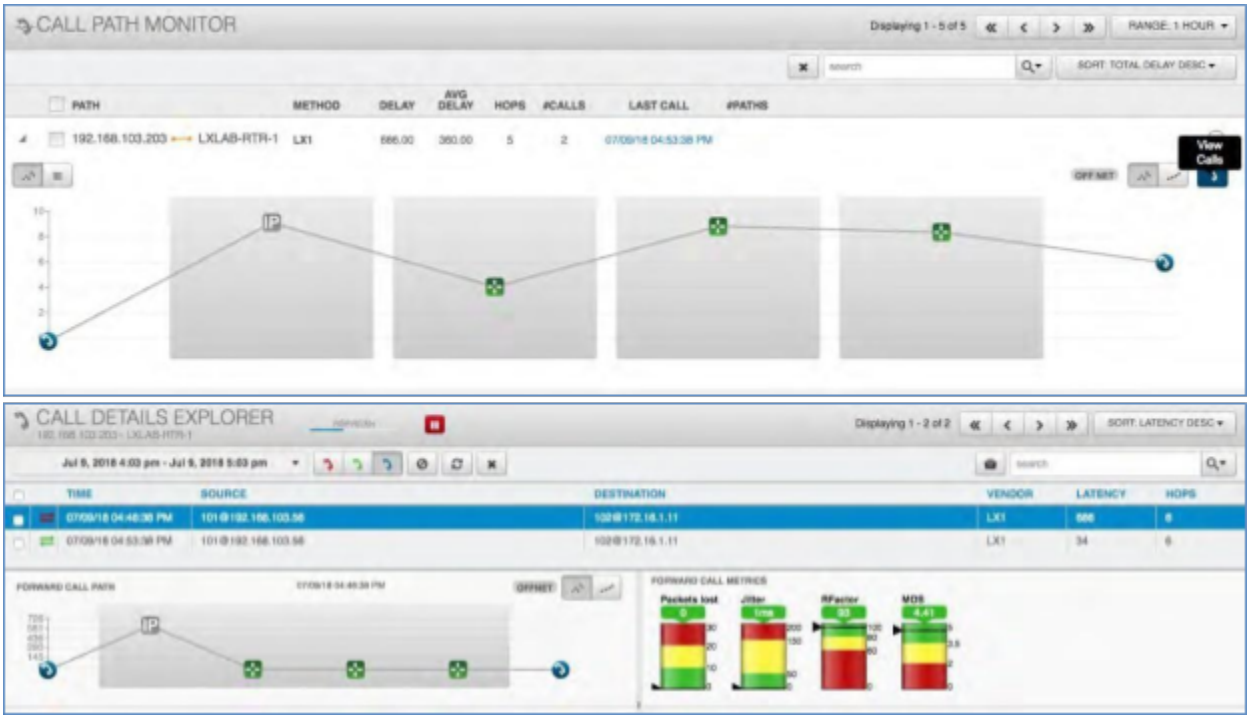
### View Call Details from the Call Path

The Call Path screen allows you to drill into the specific call details right on the chart. Simply click the blue telephone icon at the end of the path and it will take you to the Call Details Explorer view for that call path.

## 3.1.6. Call Details

### Call Details Explorer

The Call Details Explores is the main screen for managing Unified Communications and the details of a particular call path that a Voice over IP call takes. It will display the time, source destination, vendor, latency and hops along the top screen. Below will show the Call path with each hop along with the call metrics (packets lost, jitter, R-Factor and MOS).

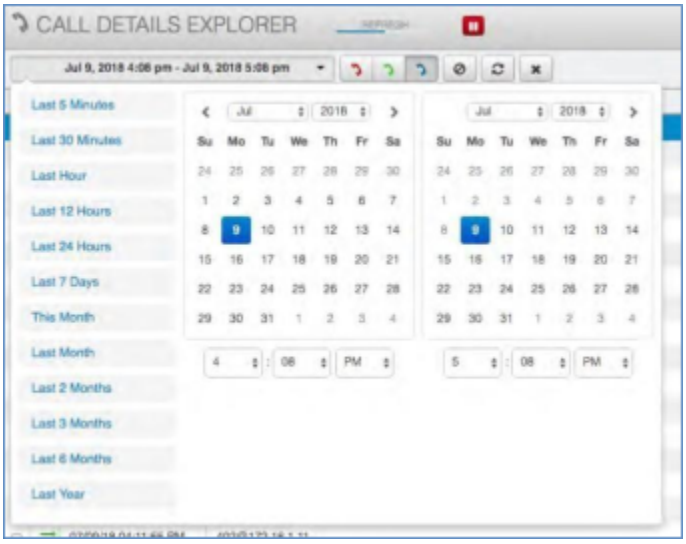



### Filter by Date and Time

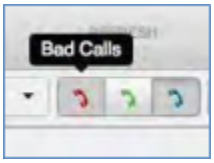
In the upper left corner there is a time bar. You can choose to search the call details by the various options presented. When you click inside the bar several options along with a calendar open up to select.

- Last 5 Minutes
- Last 30 Minutes
- Last Hour
- Last 12 Hours
- Last 24 Hours
- Last 7 Days * This Month
- Last Month

- Last 2 Months
- Last 3 Months
- Last 6 Months
- Last Year
- Specific Date and Time



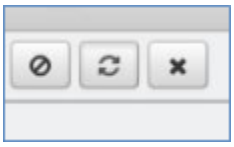

### Filter by Call Quality




Just next to the time bar are several icons that allow you to filter the call detail data by Call Quality. There are 3 options:

- Bad Calls (Red)
- Good Calls (Green)
- Bad and Good Calls (Blue)

### Clear Filter, Update and Delete Call



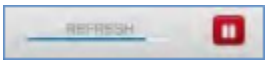
The three icons next to the call quality filters provide the functions below:

- Clear Filter: This will remove all filters set and the call details will show the default display.
- Update: The screen is pre-set with a refresh timer. Clicking this icon allows you to request new data on demand.

- Delete Call: If the check box is selected next to any call then by clicking this icon the system will delete that call.

### Refresh Pause

Selecting the pause icon in the top left of the view will stop the refresh cycle. This comes in handy as you are reviewing a specific call.

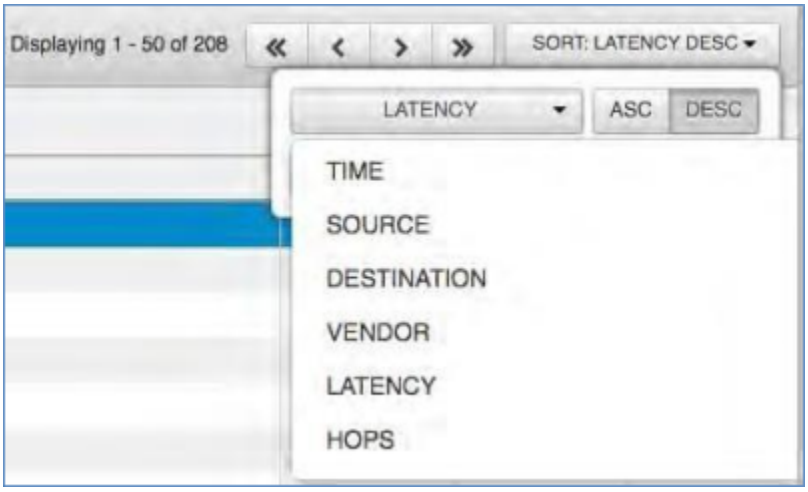


### Sorting

At the top right of the screen is a drop-down button called “Sort”. Clicking this button will open up several options for which the call details can be sorted.

- Time: The time the call was placed
- Source: The source that placed the call
- Destination: The destination of the call
- Vendor: Identifies the method that created the call. The only options are LX1 (the VOSS Raptor Call Path generator) and RTCP (Avaya specific RTCP and call path data)
- Latency: The aggregate latency recorded on the call
- Hops: The total number of hops the call took

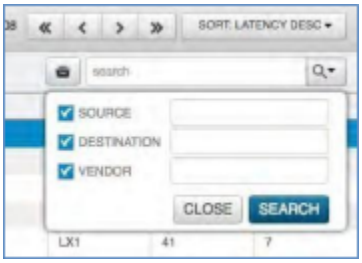
Each option allows for the choice of ascending or descending order.



### Search Call Details

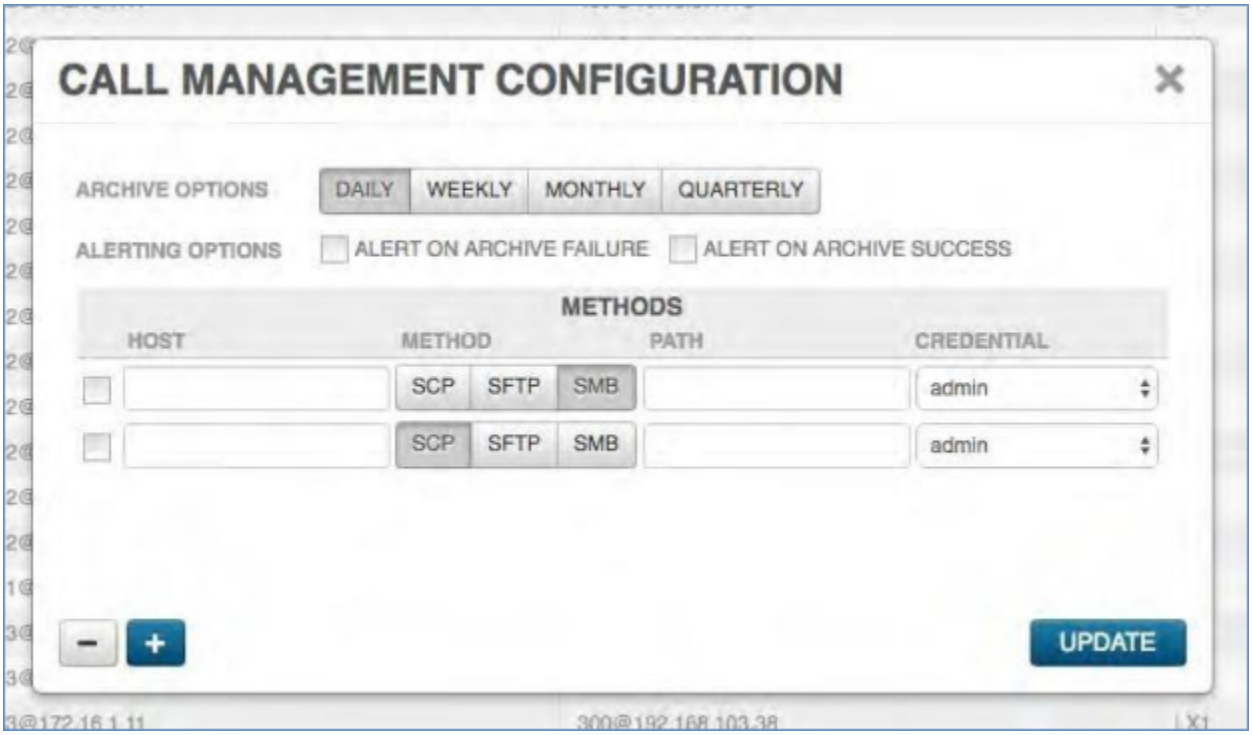
The search bar in the top right of the screen allows the user to search for specific call details. There are three options that can be utilized to search:

- Source: The source IP that made the call
- Destination: The destination IP that received the call
- Vendor: Identifies the method that created the call. The only options are LX1 (the VOSS Raptor Call Path generator) and RTCP (Avaya specific RTCP and call path data)




## 3.1.7. Call Management Configuration

In very busy or large environments it is imperative to manage the data that is being collected in the Call Detail Explorer. Have potentially 100's of thousands of calls can lead to the data becoming difficult to manage. As such there is the option to manage the configuration of the call table within the Call Detail Explorer screen. Click the file cabinet icon next to the search bar and a menu screen will pop up. This provides optional time and methods for which the call data can be archived. The choices are Daily, Weekly, Monthly or Quarterly. Be sure to toggle on "Alert on Archive Failure" and "Alert on Archive Success. The methods available for archival are SCP, SFTP or SMB. Each requires a host, path and credential. Multiple methods may be added.

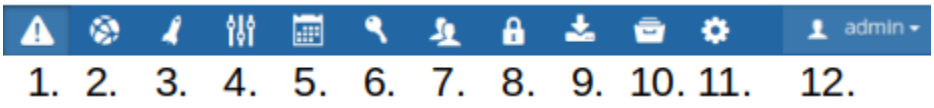


# 4. Configuration

## 4.1. Configuration

The menu bar at the top of the screen provides options to navigate to each of the configuration sections. Each will be covered in its own section of this guide.

- *Policy Configuration*
- *Asset Configuration*
- *Probe Configuration*
- *Controls*
- *Response Procedure Configuration*
- *Credential Configuration*
- *Customer Configuration*
- *Access Control*
- *Import & Export*
- *Archive Management*
- *Log Management*
- *Tools*

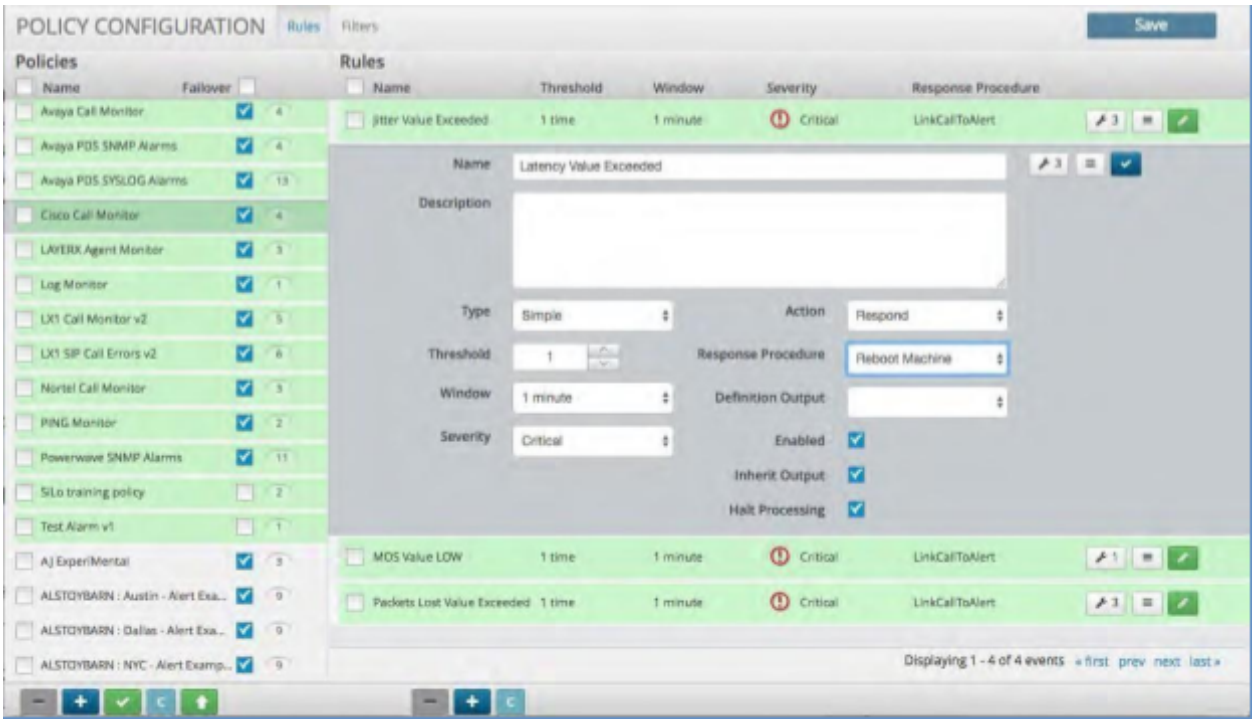



### 4.1.1. Policy Configuration

Polices are a modular groupings of correlation rules, actions and response procedures that define how to respond to certain situations that happen on the monitored systems. Policies are usually system and manufacturer specific but can contain custom scripts for actions and response procedures. Each policy will also contain several correlation rules that are designed to create Alerts based on the best practices of that particular system manufacturer. These alerts can apply to:

- Business Processes
- Infrastructure
- Security

- Applications
- Unified Communications
- Network behavior
- Metrics and Threshold Violations

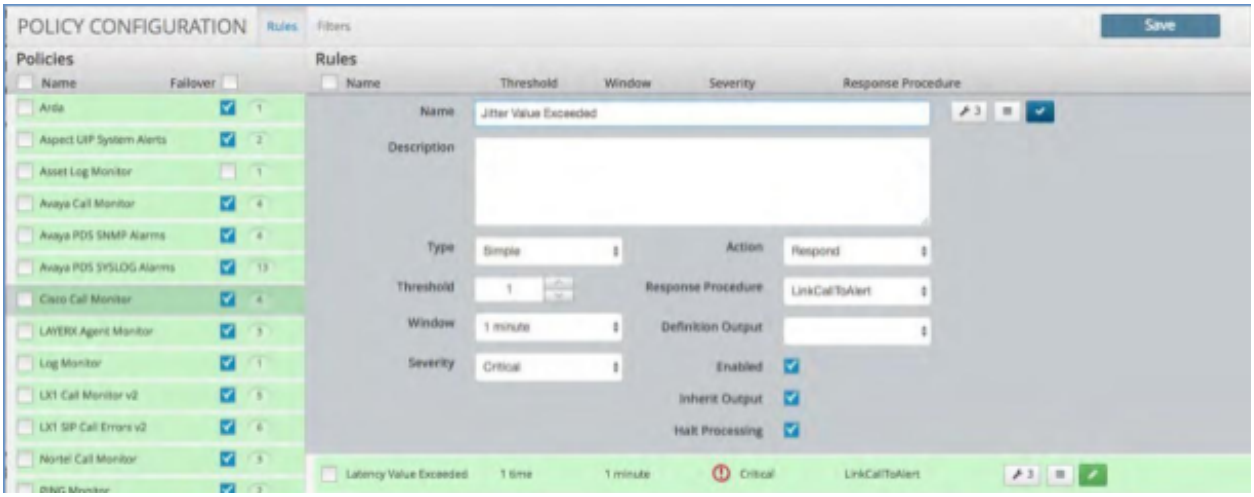



## Correlation Rules

A Correlation rule extracts data from the various sources and then defines the parameters for Alert creation within a Policy. It may contain 1 or more Correlation Definitions along with specific actions and Response Procedures. Each correlation rule consists of the following parameters:

| Parameter | Description |
|---|---|
| Name | Descriptive name for the correlation rule which will be displayed within an Alert and viewed in Alert Analyzer. |
| Description | Enter a complete description of the problem that created the alert along with any specific remediation steps that should be taken to resolve the problem. |
| Type | Simple: Select if the rule is to analyze a single log and as a result of the rule, you want to execute an action.<br>Compound: Select if the rule is to correlate more than one log, the results of another correlated event or multi-tiered rules. A compound rule can be one or more simple rules that feed into one primary rule, or it can come directly from the source.<br>Unique: Same as Simple but as a definition will be the only one. |
| Threshold | Selects how many times this rule is to match before an action occurs. |
| Window | Select the time window for the rule to match before an action occurs. |

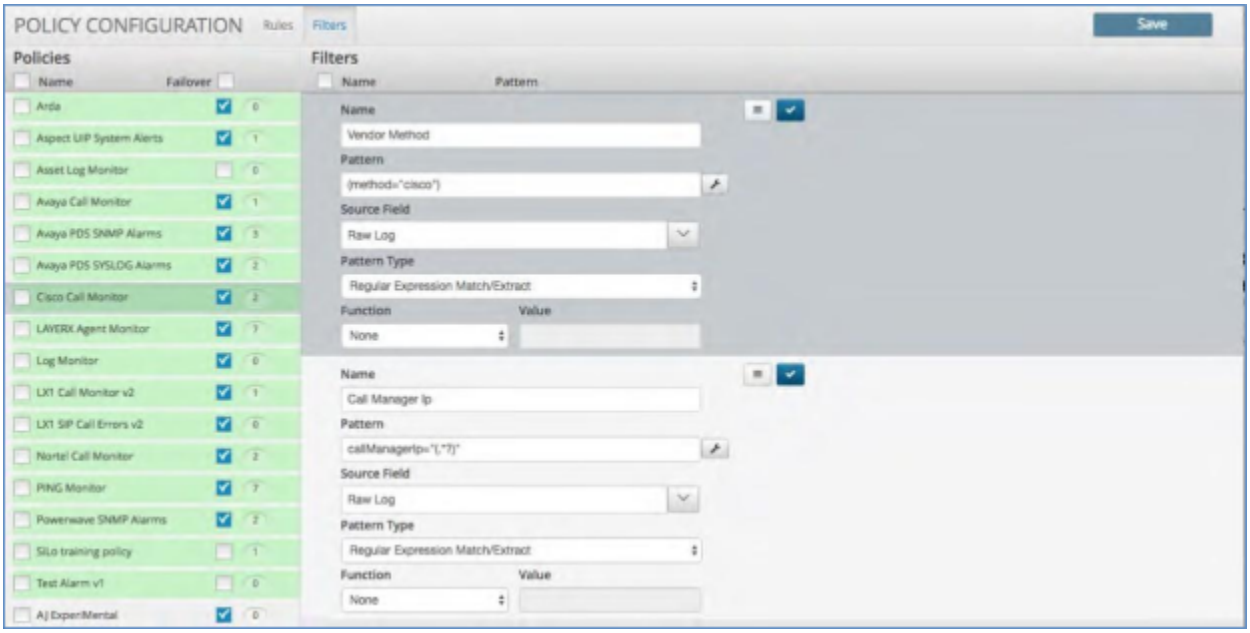
| Parameter | Description |
|---|---|
| Severity | Indicates what is to appear in the Status field on the Alert Viewer monitor.<br>Select the severity for this rule:<br>• Informational<br>• Minor<br>• Major<br>• Critical |
| Action | Choose the action that is to occur for this rule, based on the selection in the Severity field<br>• Respond - If the condition is met, set a marker and send an alert.<br>• Track - If the condition is met, track the event, but do not post it to the Alert Analyzer.<br>• Track/Respond - If the condition is met, send an alert and continue to monitor.<br>• Respond on Expire – If the condition is met, wait to send an alert until the window time has expired. If you want the policy/rule to only alert after an application does not respond, based on the setting (for example, to ping 9 times in 10 minutes), choose **Track and Respond**. For the example in this case, the alert triggers as soon as it sees 9 ping failures. This setting (Respond on Expire) does not track.<br>• Submit - Submit the results of a correlation event back into the Correlation Engine so that the behavior can be analyzed and re- correlated.<br>• Submit/Respond - Submit this alert back into the Correlation Engine so that the event can be analyzed and re-correlated. Then set a marker and send an alert. |
| Response Procedure | For any rule that is satisfied, an Incident Response Procedure occurs and an event is posted to the Alert Analyzer. Select the Response Procedure from the drop-down menu to execute when conditions have been met. |
| Definition Output | Selects a single Correlation Definition's extracted value to be displayed with the Alert. |
| Enabled | Toggle to enable/disable the rule |
| Inherit Output | Toggle to enable/disable whether the rule will include the results of the filter attached to the policy module. |
| Halt Processing | Toggle to halt processing of logs to any other rules within the policy if the rule matches. This will highlight the Policy in Green to indicate that this function is in use. |
| Correlation Definitions | Click the wrench icon where you can define one or more definitions match and or extract the required data from a log or event. See Correlation Definitions. |
| Output Order | Sets the preferred order to output the extracted data from the Correlation Definitions. |
| Done | Click the Done box when the rule is complete |
| Save | Be sure to click the Save button so your rule (or changes) are saved and committed. |




Correlation Filters provide a simple way of ensuring that all of the correlation rules within the policy are firing on the correct set of data. The engine first looks at the filter criteria, then it selects only the data that matches the criteria, and then it applies the correlation rule. You can add as many of these as required.

Each filter has the following options:

| Filter Option | Description |
|---|---|
| Name | Provide a name as close as possible to the data elements you wish to filter. This allows the output to match the name once viewed in the alert text. |
| Pattern | The extraction method used to pull a particular data point out. Click the Wrench icon adjacent to the box to launch the **Regex Wizard**, which helps you to find and extract the data.<br>The **Regex Wizard** has two sections:<br>1. Select a Log: In the top section you can search and select the log or data set you will be utilizing. That will then show up in the bottom portion under the phrase “Select log from the list above or paste log here:”. You can copy and paste a log into this section as well.<br>2. Create Regex: Once you have your log then go to this section. Here you can use the wizard to create the Regular Expression required. Close the wizard and copy this pattern the Regex into the box under Pattern. |
| Source Field | From the drop-down, choose the source from which data is extracted. |
| Pattern Type | From the drop-down, choose the type of expression you want to use:<br>• String Match<br>• Regular Expression Match<br>• Regular Expression Match/Extract (Most Often Used)<br>• Regular Expression Multi-Valued Extract |
| Function | If the extracted data is integer-based, you can apply the following functions for comparing data:<br>• None<br>• Greater Than<br>• Less Than<br>• Same |
| Value | This field is available only if the data extracted is an integer. |




### Example: Policies and Alerts

Let's say you have a Ping policy that you've set to alert after 10 failures in 20 minutes.

Depending on how you've set up your rules, the following may occur:

- The policy may run against all your assets and trigger an alarm if the cumulative Ping failure (across all assets) hits 10
- The policy may trigger an alarm for each asset that fails a ping 10 times in 20 minutes

Thus if it sees 10 failures (across all assets) in 20 minutes, an alert is triggered. However, if you want 10 failures per asset, you need a definition for the IP address, and set the filter function to **Same**, which defines that when you see 10 failures for the same IP address, trigger an alert.

You can configure this definition in two ways:

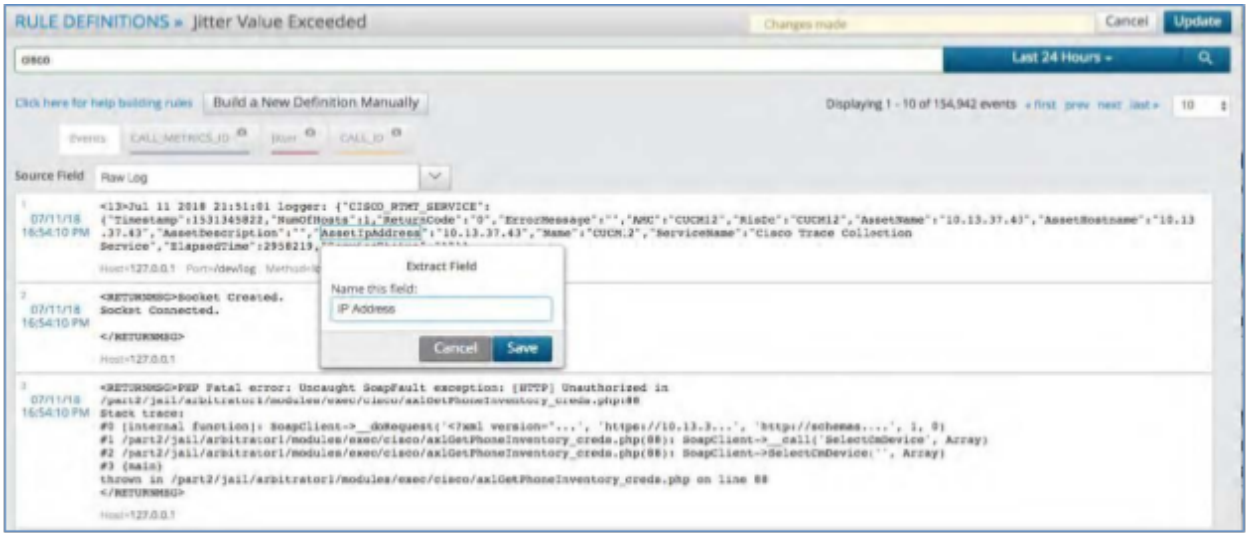
- As a filter on the policy
- As a specific rule definition.

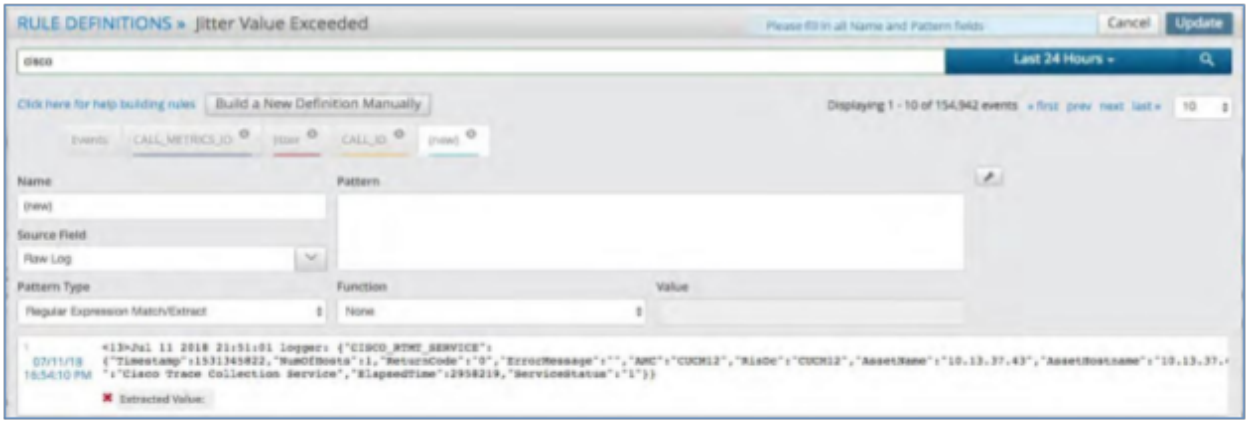
### Correlation Definitions

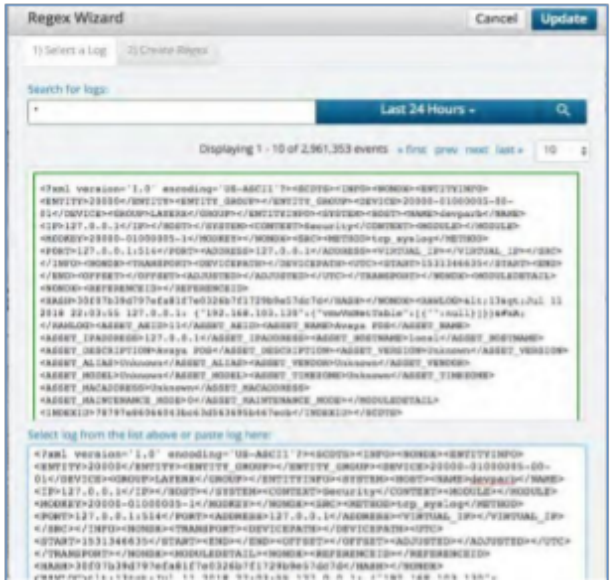
A Correlation Definition defines what criteria to match within the data. Each definition will consist of the following parameters:

| Parameter | Description |
|---|---|
| Name | Name this as close as possible to the data elements being extracted. That way the output matches the name once viewed in the alert text. It is also utilized in the key value pair within the alert text.<br>This is the extraction methodology utilized to pull the particular data point(s) out. Simply find the log containing the data by utilizing the search bar above. Within that log you can highlight the text you want to extract. Once highlighted a box will pop up allowing you to name the field and extract it. This will automatically create the Regex to extract the data. The highlight method is about 95% accurate.<br>If you have trouble with this method due to special characters in the data set, then you can utilize the “wrench” icon beside the Pattern box and it will bring up the “Regex Wizard” to assist in finding and extracting the data. |
| Pattern | Within the Regex Wizard there are 2 sections:<br>• Select a Log: In the top section you can search and select the log or data set you will be utilizing. That will then show up in the bottom portion under the phrase “Select log from the list above or paste log here:”. As the phrase indicates you can copy and paste a log into this section as well.<br>• Create Regex: Once you have your log then go to this section. Here you can utilize the wizard to create the Regular Expression required. Close the wizard and copy this pattern the Regex into the box under Pattern. |

| Parameter | Description |
|---|---|
| Source Field | In the drop-down box select the source from which the data is being extracted. |
| Pattern Type | Select from the drop-down box the type of expression you want to utilize:<br>• String Match<br>• Regular Expression Match<br>• Regular Expression Match/Extract (Most Often Used)<br>• Regular Expression Multi-Valued Extract |
| Function | If the extracted data is integer based, then you can apply the following functions that will allow you to compare the data:<br>• None<br>• Greater Than<br>• Less Than<br>• Same |
| Value | This field will only be available if the data extracted is an integer. |



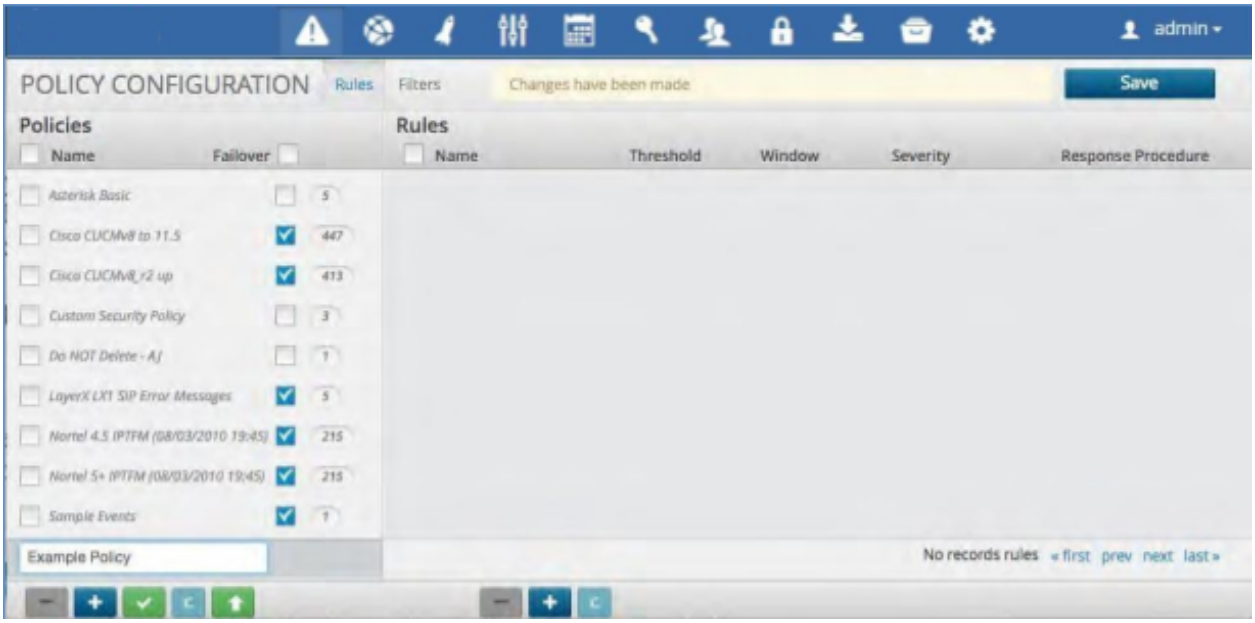




### Creating a Policy

To Create a Policy:

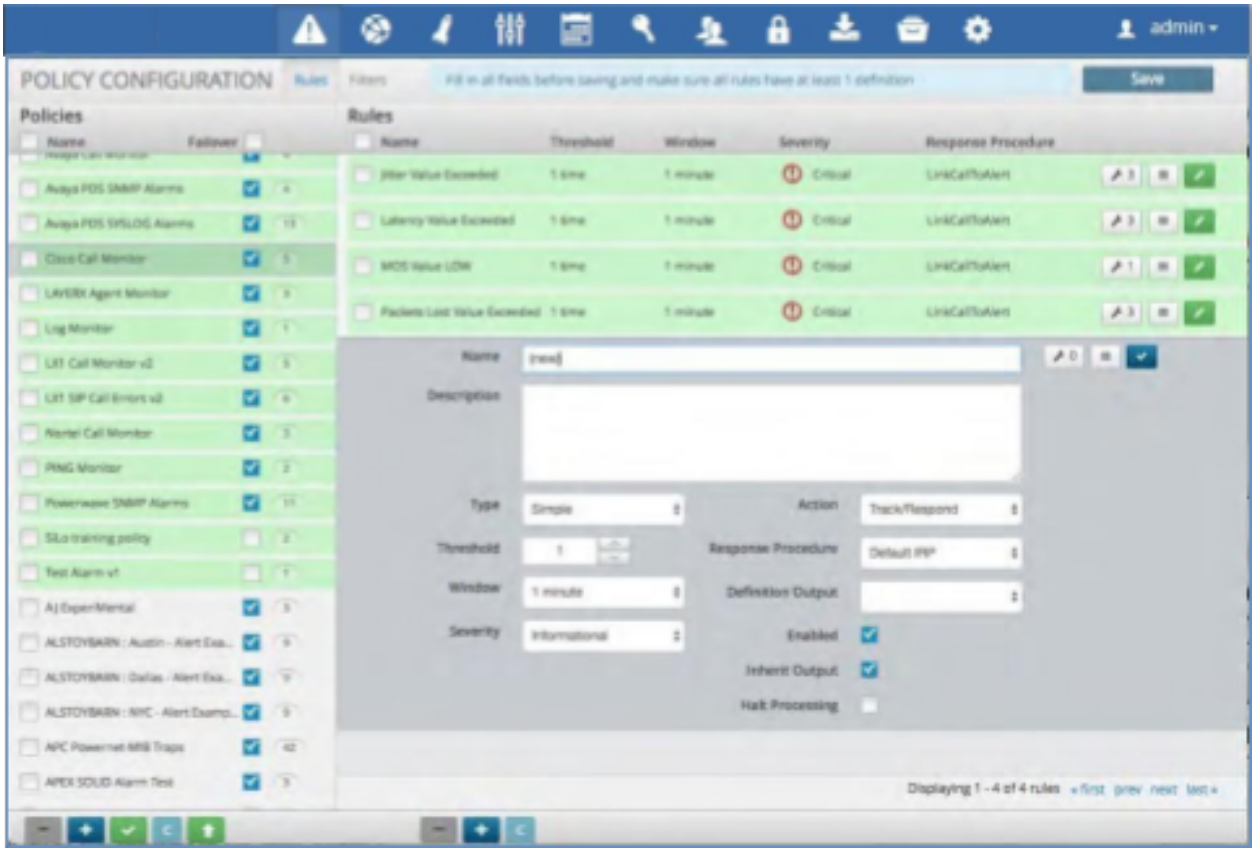
1. Click the Policy View from the Configuration Menu Bar at the top of the page.
2. Click the Plus Icon at the bottom left of the Policies panel
3. Fill in the Policy name and press enter.




### Creating a Correlation Rule

To Create a new Correlation Rule:

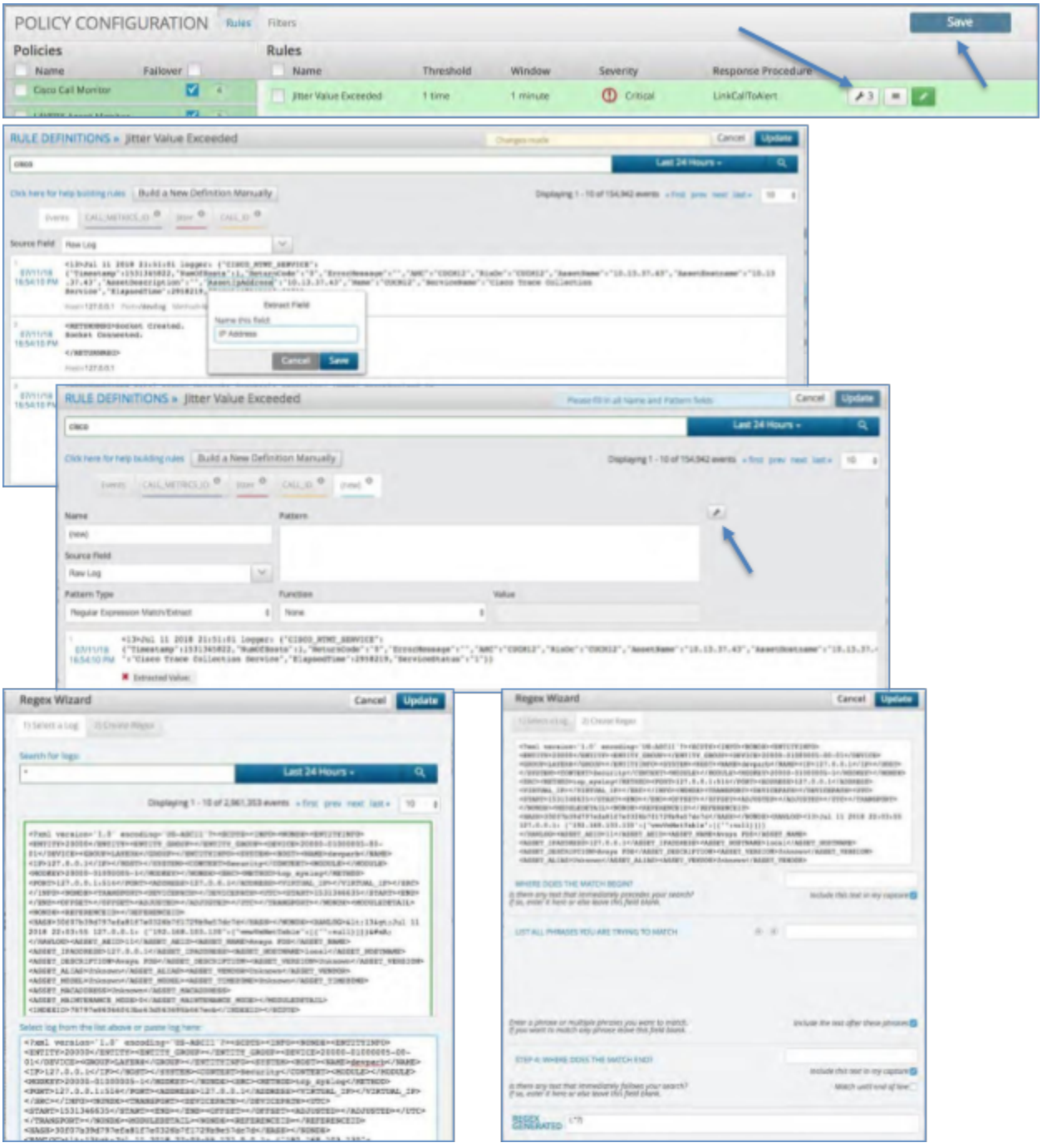
1. Click the Policy to which you wish to add the rule.
2. Click the Plus icon at the bottom of the Rules panel.
3. Fill in the rule name and the parameters.




### Creating a Definition

To create a new definition:

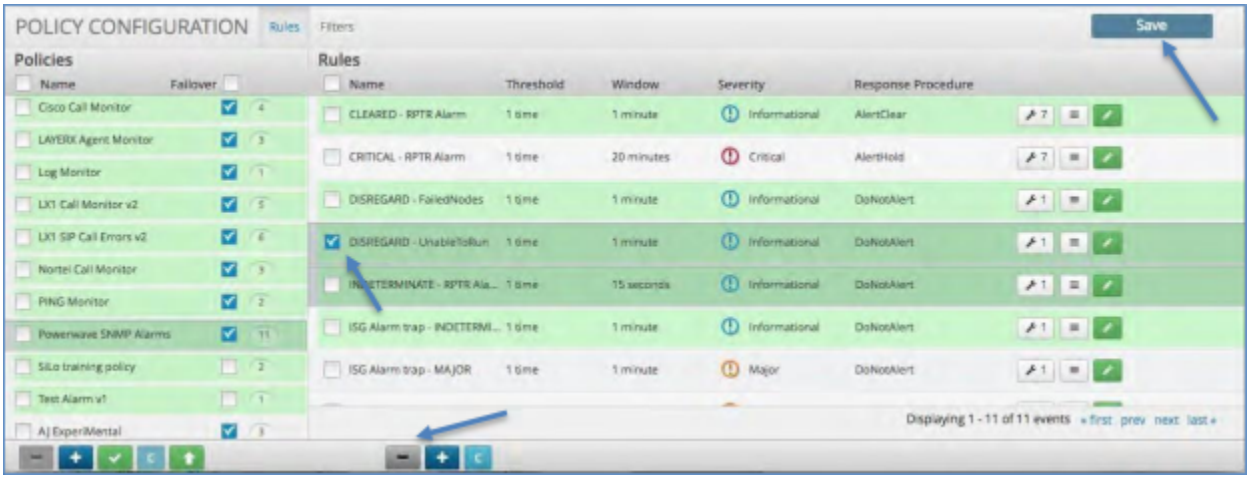
1. Click the wrench icon within any rule to bring up the search engine.
2. Enter a search term that is relevant or is in the log that you would like to match and press Enter. This will return the last 10 logs with this term in them.
3. Utilize the highlight and extract procedure or the Regex Wizard as described in the in “Correlation Definitions” section above.
4. Once finished click Update in the top right of the screen and be sure to save your Definition on the next page.



### Deleting a Correlation Rule

To delete a Correlation Rule:

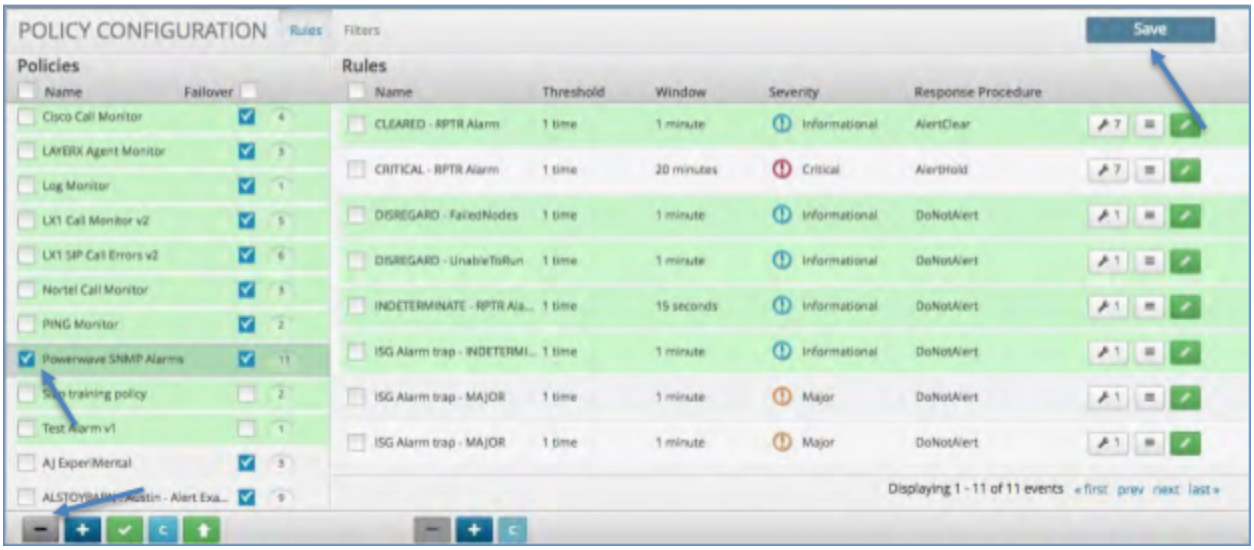
1. Click the policy name on the left side of the screen.
2. Click the check box on the Correlation rule you wish to delete.
3. Click the minus icon at the bottom of the correlation panel.
4. Click the Save icon in the upper right to save your change.




### Deleting a Policy

To delete a Policy:

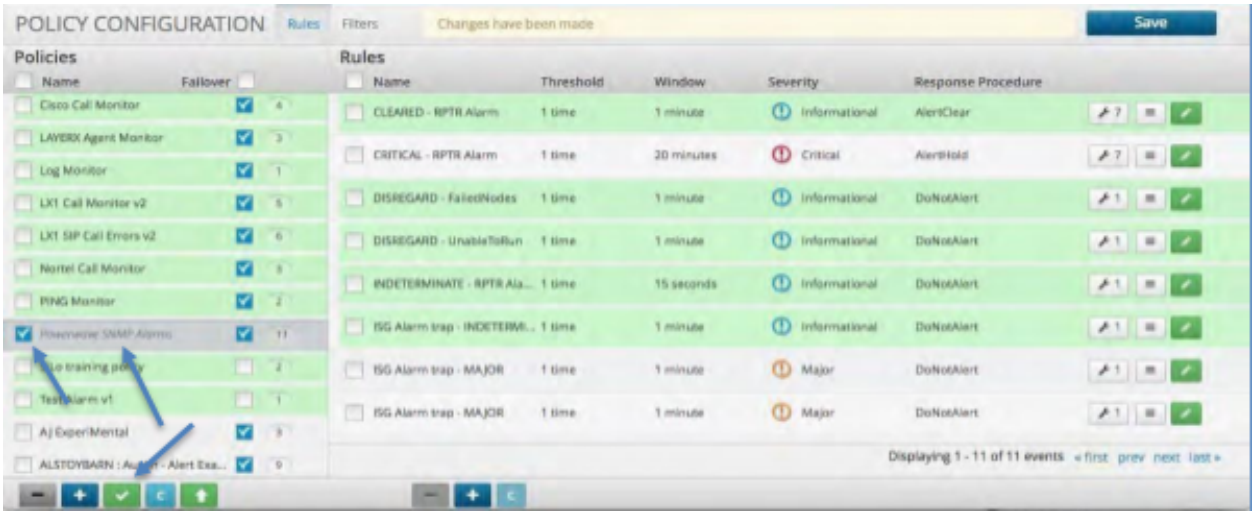
1. Click the check box next to the name of the Policy you wish to delete.
2. Click the minus icon in the bottom left of the policy panel.
3. Click the Save icon in the upper right to save your change.



### Disabling and Enabling a Policy

To Disable and Enable a Policy:

1. Select the Policy by clicking the check box next to the name of the policy.
2. Click the Green Check Box at the bottom of the Policies listing column.
3. The Name of the Policy will become italicized indicating that the Policy is Disabled
4. To Enable the Policy: Click the Green Check Box again. The name will turn back to a normal font indicating it is enabled.

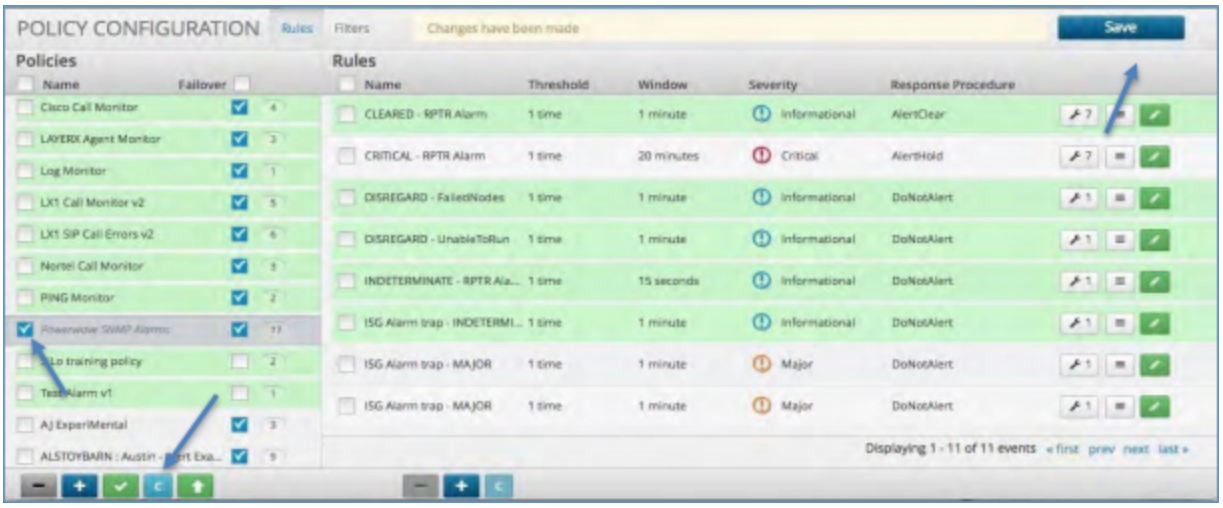



### Cloning a Policy

Cloning a Policy allows the quick replication of all of the Correlation Policy rules and definitions. The user then can simply change only the required elements for the new policy.

To Clone a Policy:

1. Select the Policy by clicking the check box next to the name of the policy.
2. Click the Blue “C” Box at the bottom of the Policies listing column.
3. Rename the Policy and make your modifications.
4. Be sure to click Save to save the new policy.



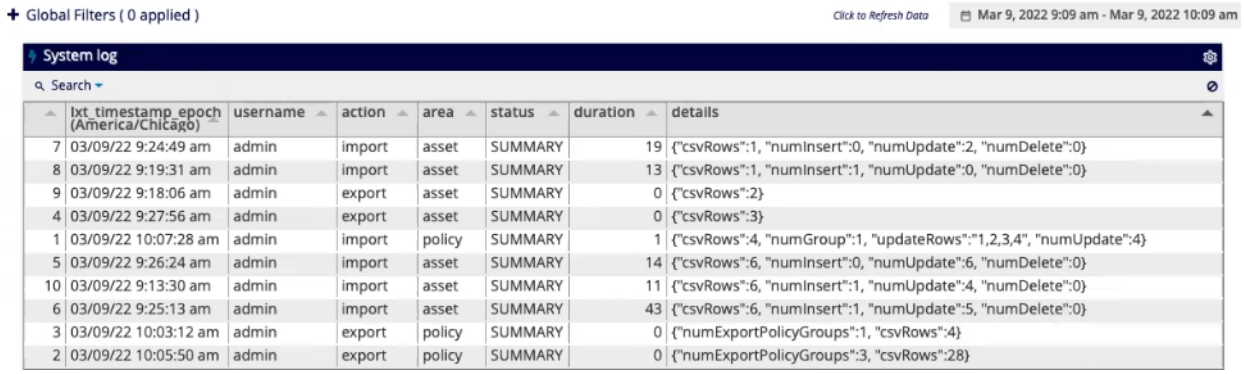

## Export and Import a Policy

The Arbitrator platform allows for full export / import of all of its configuration. Within the Policy Configuration section, you can export and import the policy that you exported from another system.

A new system log table `insights_system_log` has also been added to log user actions and a user can create a dashboard to view these actions.

See the:

Log Search Section in the Dashboard and Reporting Administration Guide.




| | lxt_timestamp_epoch (America/Chicago) | username | action | area | status | duration | details |
|---|---|---|---|---|---|---|---|
| 7 | 03/09/22 9:24:49 am | admin | import | asset | SUMMARY | 19 | {"csvRows":1, "numInsert":0, "numUpdate":2, "numDelete":0} |
| 8 | 03/09/22 9:19:31 am | admin | import | asset | SUMMARY | 13 | {"csvRows":1, "numInsert":1, "numUpdate":0, "numDelete":0} |
| 9 | 03/09/22 9:18:06 am | admin | export | asset | SUMMARY | 0 | {"csvRows":2} |
| 4 | 03/09/22 9:27:56 am | admin | export | asset | SUMMARY | 0 | {"csvRows":3} |
| 1 | 03/09/22 10:07:28 am | admin | import | policy | SUMMARY | 1 | {"csvRows":4, "numGroup":1, "updateRows":"1,2,3,4", "numUpdate":4} |
| 5 | 03/09/22 9:26:24 am | admin | import | asset | SUMMARY | 14 | {"csvRows":6, "numInsert":0, "numUpdate":6, "numDelete":0} |
| 10 | 03/09/22 9:13:30 am | admin | import | asset | SUMMARY | 11 | {"csvRows":6, "numInsert":1, "numUpdate":4, "numDelete":0} |
| 6 | 03/09/22 9:25:13 am | admin | import | asset | SUMMARY | 43 | {"csvRows":6, "numInsert":1, "numUpdate":5, "numDelete":0} |
| 3 | 03/09/22 10:03:12 am | admin | export | policy | SUMMARY | 0 | {"numExportPolicyGroups":1, "csvRows":4} |
| 2 | 03/09/22 10:05:50 am | admin | export | policy | SUMMARY | 0 | {"numExportPolicyGroups":3, "csvRows":28} |

To Export a Policy:

1. Select the check boxes of the policies to export, or select the **Name** check box at the top of he **Policies** list to select *all* policies.
2. Click the green Down arrow button at the bottom of the **POLICY CONFIGURATION** panel.
3. The **Export CSV** dialog opens. Enter a **CSV file name** (You do not have to add the `.csv` file extension) and click **Export**.
4. The **Export finished** dialog shows when the export file has been created. Click **Download** to save the CSV file to your selected download location.

To Import a Policy:

1. Click the green Up arrow button at the bottom of the **POLICY CONFIGURATION** panel.
2. A pop-up box will appear asking you choose your file.

3. Click the **Choose file** button and select the exported CSV file that you have saved to your computer.
4. Click the **Import** button.

### Policy CSV Format

The following columns are in an exported CSV file:

```
"row action","policy group name",name,description,type,action,severity,
"respond procedure","SubCategory (definition: regular expression match)",
"Message (definition: regular expression match/extract)"
```

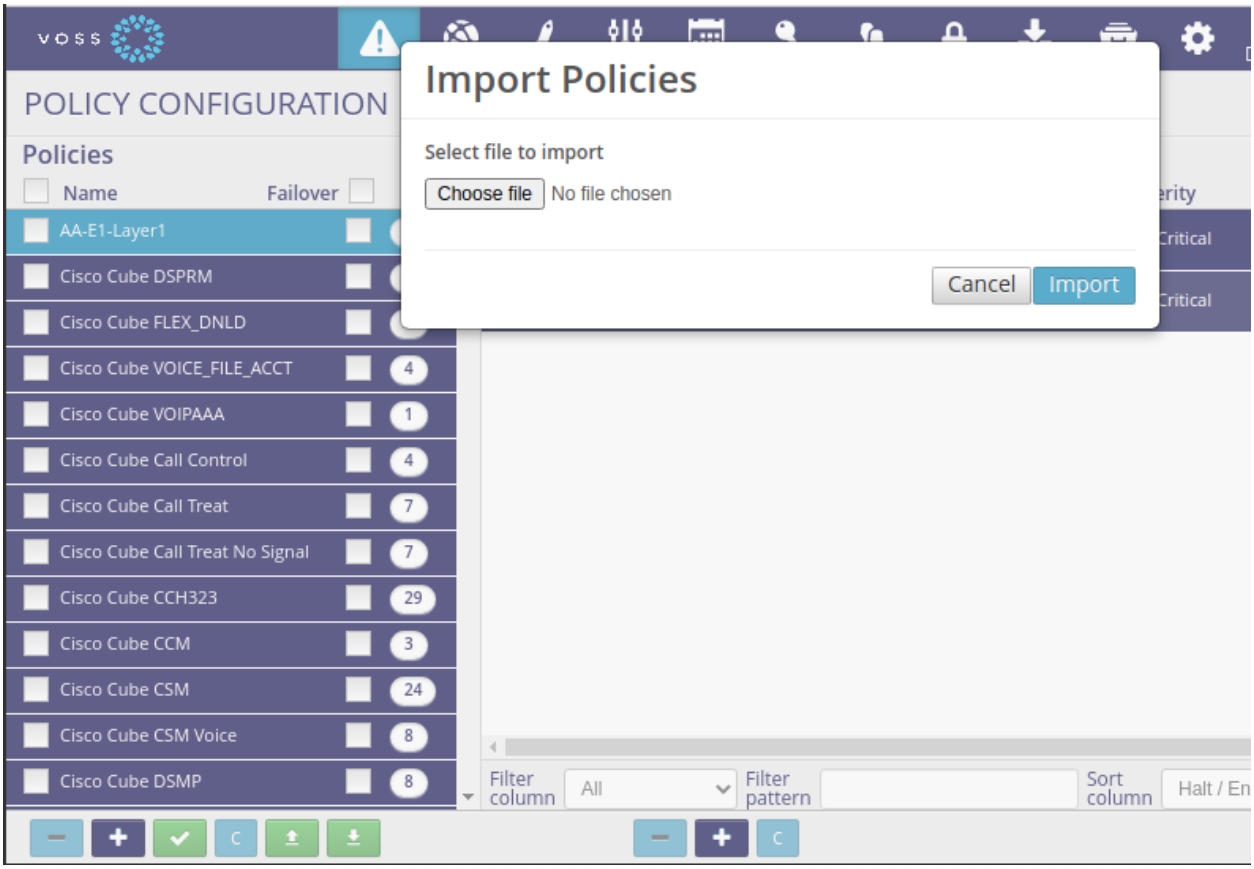
---

**Note:**

- The "`row action`" column is used when importing and if it contains “delete”, then the row will be deleted upon import.
- The "`respond procedure`" column can be used when importing and should then contain the Response Procedure name *exactly* as it exists on the system. If a procedure is found, then it will be assigned to the associated rule. If a new value is entered, a new Response Procedure is created. The default Response Procedure is used if no value is entered.
- The combination: “policy group name”, “name”, “respond procedure” should be unique in CSV row. If a policy found, its data will be updated. If not found, new policy will be inserted. The “name” has to be unique. If a rule is found, its data will be updated. If not found, new rule will be inserted to the policy indicated in “policy group name”.

  See: *Response Procedure Configuration*.

---




## 4.1.2. Asset Configuration

The Asset Configuration panel allows you to create Assets and Asset Groupings. Assets can be any devices that are either sending data or from which data is being retrieved. Each Asset can be assigned to a specific customer to create a multi-tenant environment.

A new system log table `insights_system_log` has also been added to log user actions and a user can create a dashboard to view these actions.

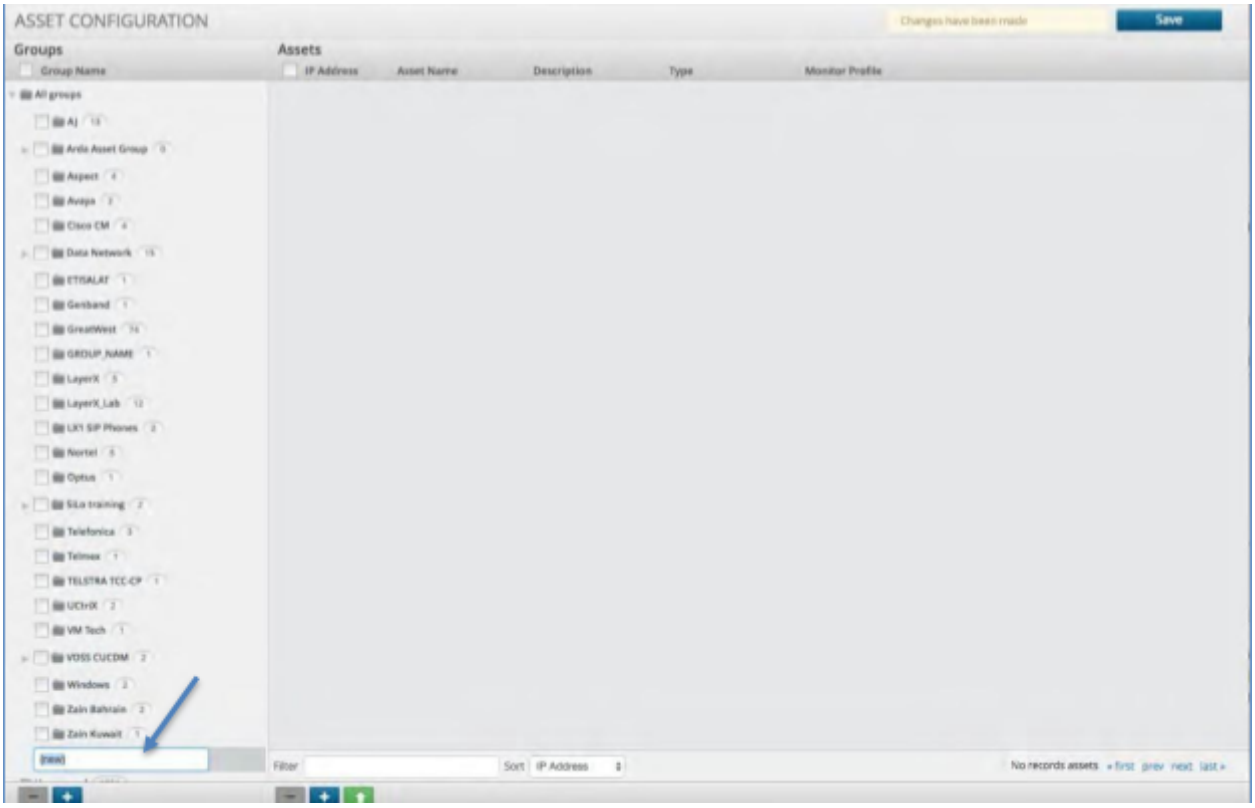
See the:

Log Search Section in the Dashboard and Reporting Administration Guide.

### Creating an Asset Group

To create a new Asset Group:

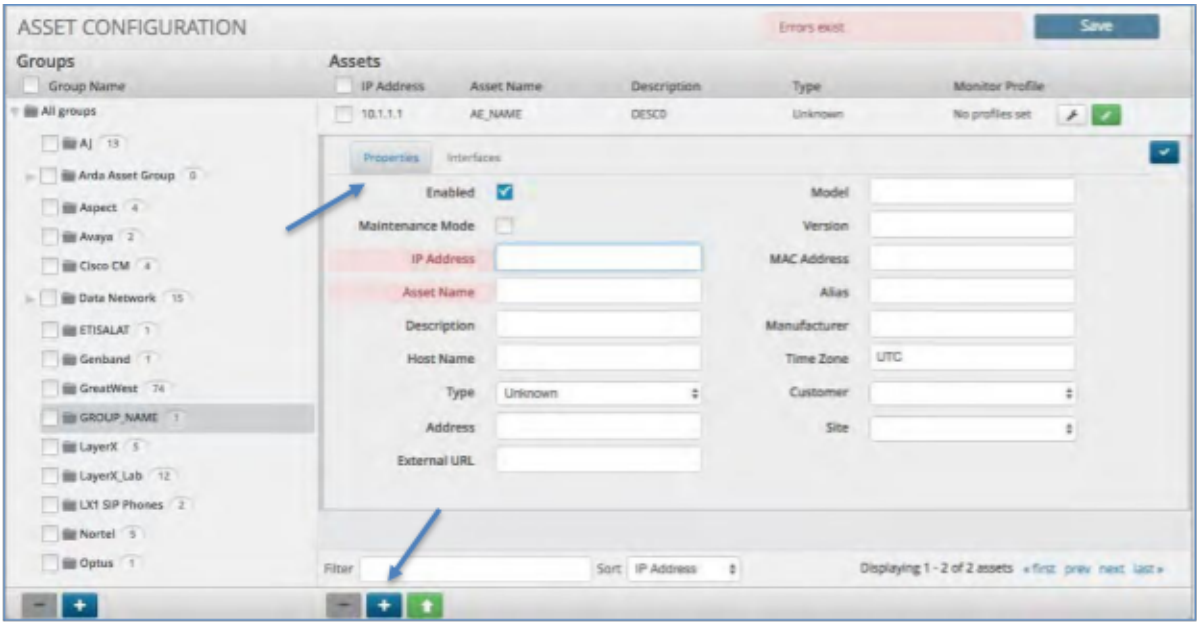
1. Click the Asset icon from the Menu bar.
2. Click the Plus icon in the bottom left corner of the Asset Groups panel.
3. Enter the Group name and press Enter.
4. Click the Save icon in the upper right.

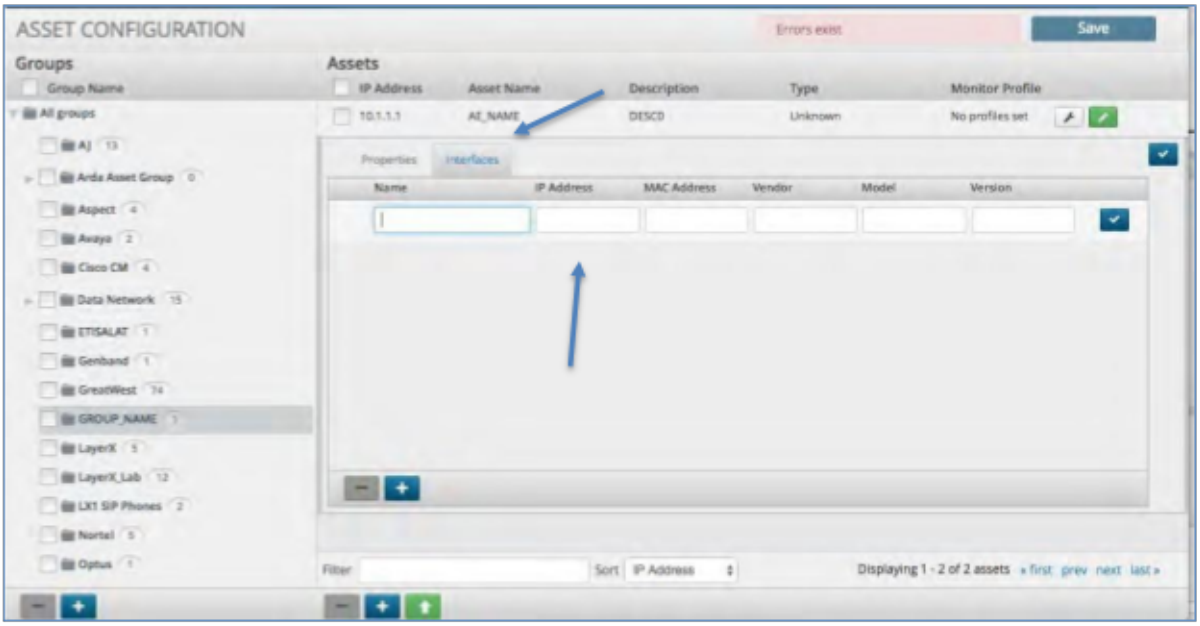



### Adding an Asset to an Existing Group

To add a new Asset to a Group:

1. Click Asset Group to which you wish to add an asset.
2. Click the Plus icon at the bottom of the Asset panel.
3. An asset entry box will open up. Fill out all of the details for the asset under “Properties”.
4. Click the “Interface” tab and fill out the details, if applicable.
5. Click the check button to the right of the screen to add the asset.

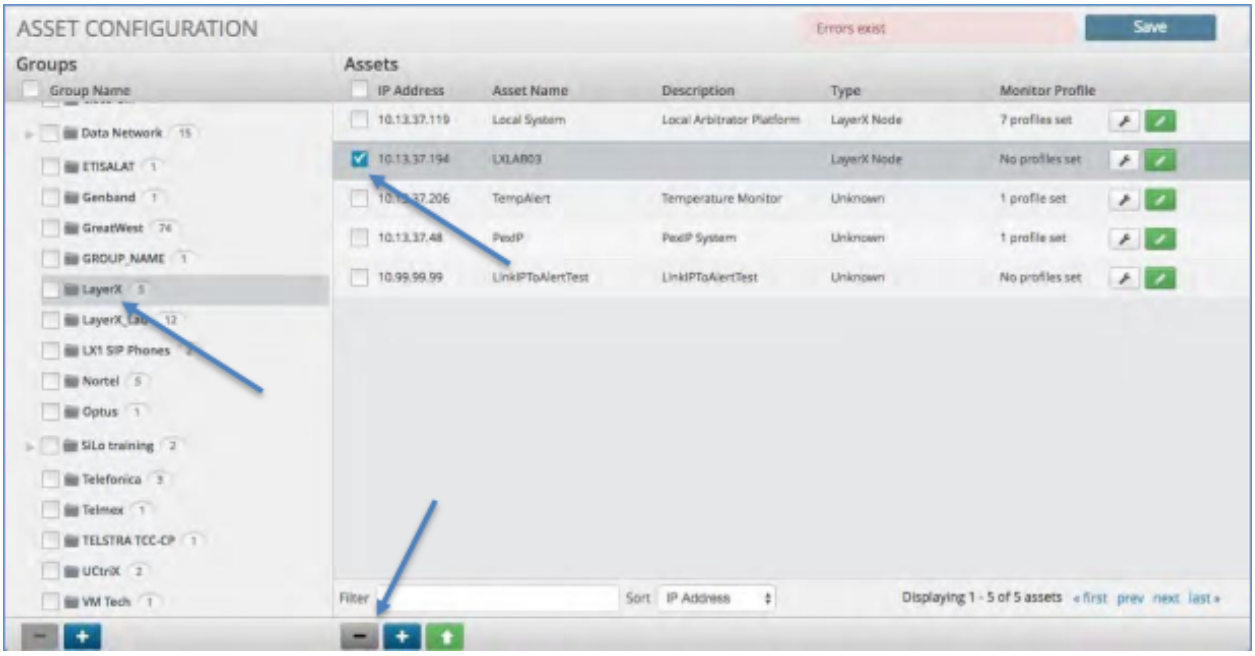



### Deleting an Asset

To delete an Asset:

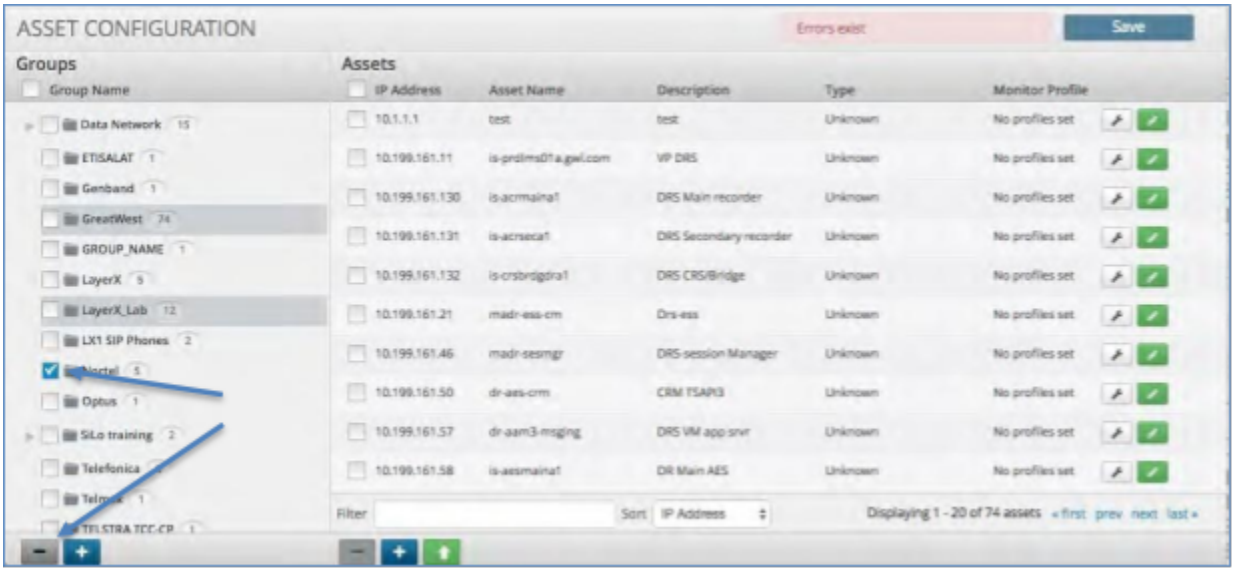
1. Click the Asset Group in which your Asset is located.
2. Click the “check” box next to the asset you wish to delete.
3. Click the “minus” icon within the Asset panel.
4. Click the “Save” icon in the upper right corner.




### Deleting an Asset Group

To delete an Asset Group:

1. Click the “check” box next to the Asset Group you wish to delete.
2. Click the “minus” icon in the bottom left of the Asset Group panel.
3. Click the “Save” icon in the upper right corner.



### Assigning a Probe to an Asset

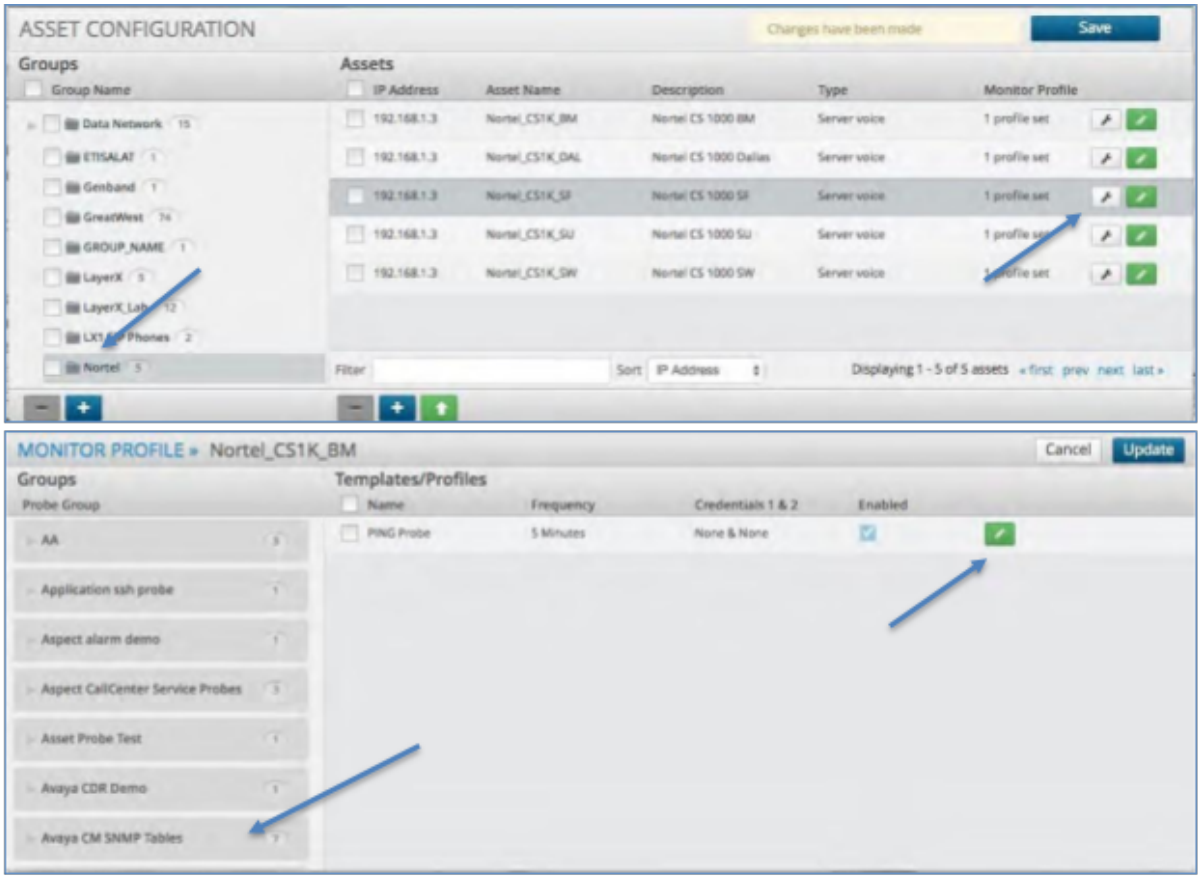
A Probe is a script or set of commands that are saved in the system and can be utilized to gather data, issue commands to systems, auto repair or send data. Assigning a probe to an asset is typically done to retrieve data from that asset. Commands such as an SNMP GET or an API call are utilized to retrieve data from a particular asset.

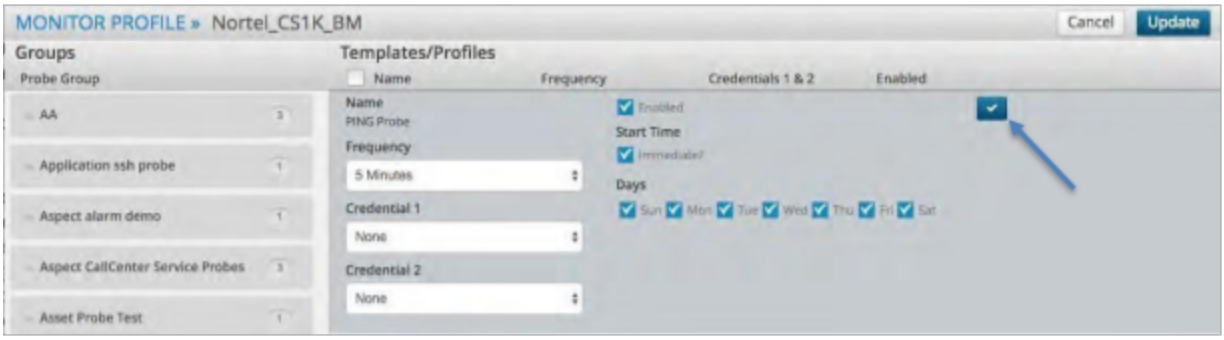
To assign a Probe to an Asset:

1. Click the asset group and then click on the actual asset within that group that the Probe will run against.
2. Click the wrench icon, which will add a monitor profile to the asset.
3. The Probe Group (covered in the next section) screen is opened where you can select from all of the saved Probes in the system.
4. Select the desired Probe
5. Next click the green pencil icon, which will open up a profile to define the frequency the probe runs, the credentials needed for the probe to run, the schedule for the Probe to run and the choice to start it immediately.

   **Note:** For SP25, the frequency for Polycom devices is set at 5 minutes.

6. Once complete click the check button to finalize the probe. This will take you back to the Asset screen and to the asset you had selected.

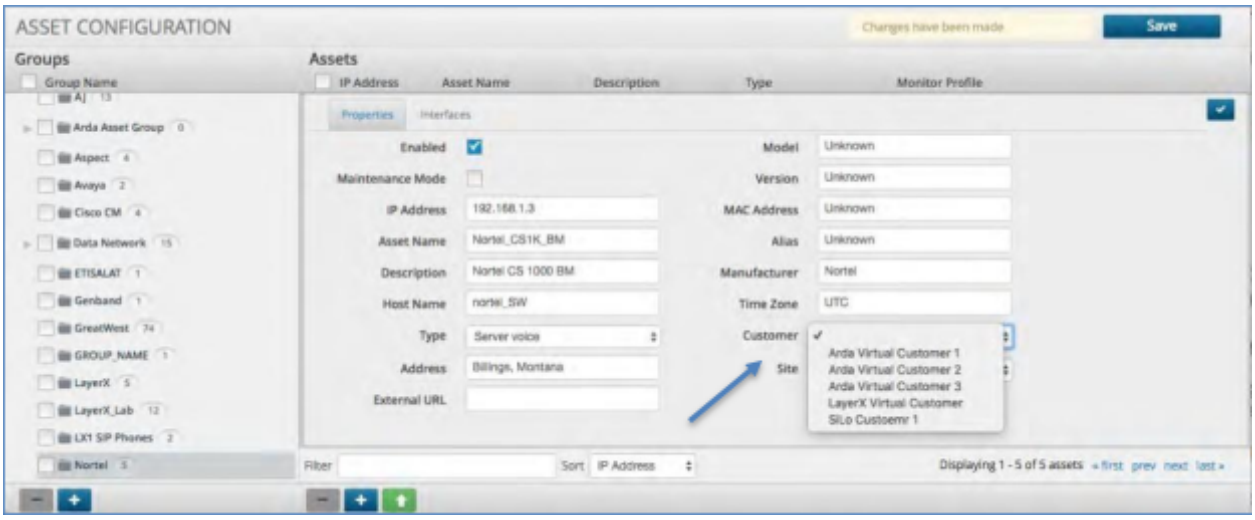





### Assigning a Customer to an Asset

The Correlation Platform has multi-tenancy built in that provides the ability for different customers to see correlated or collected results of only their data. Within the configuration of assets, you can assign each asset to a specific customer. To assign a Customer to an Asset:

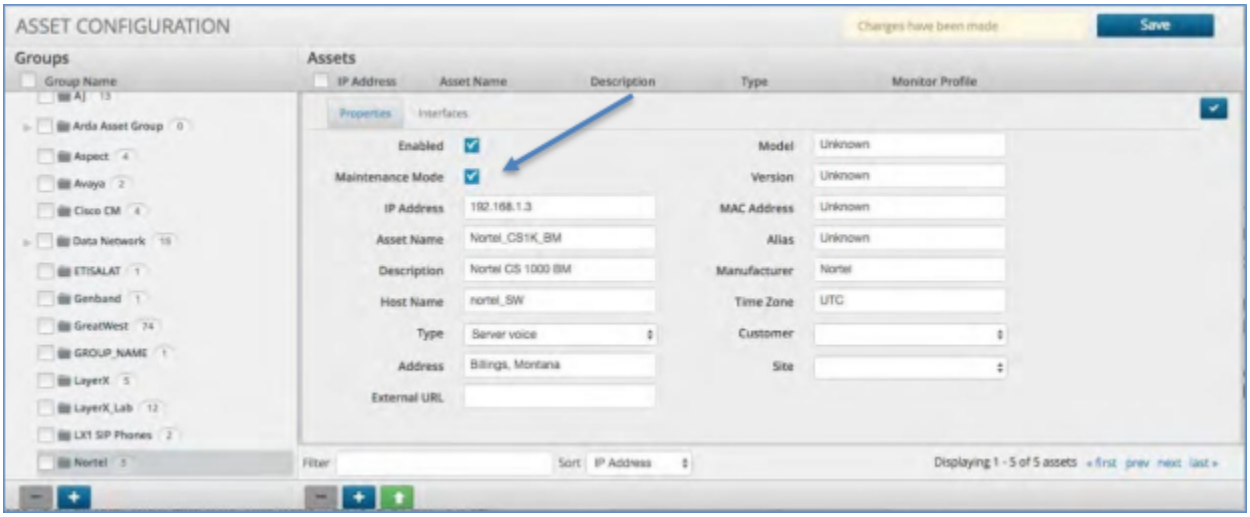
1. Click the asset group and then click on the actual asset within that group that is to be assigned to a Customer.
2. Click the pencil icon that will open up the details of that asset.
3. Click the field labeled Customer and a drop-down list of available Customers will appear.
4. Select the Customer that the asset belongs to and then click the blue check box in the top right.
5. Click the Save icon to save the changes.



### Placing an Asset in Maintenance Mode

The Correlation Platform allows any asset to be placed into Maintenance mode. Doing so will stop the platform from responding with alerts until it is removed from the mode. Data will still be collected but alerts will not be sent.

1. Click the asset group and then click on the actual asset within that group that is to be put into Maintenance mode.
2. Click the pencil icon that will open up the details of that asset.
3. Check the box next to the label Maintenance Mode and then click the blue check box in the top right.
4. Click the “plus” icon to return to the Asset Group and then click the “Save” icon to save the Maintenance Mode settings.




### Export and Import an Asset

Within the **ASSET CONFIGURATION** section, you can export and import the asset that you exported from another system.

- When selecting asset groups, all assets belong to those groups will be selected (selecting individual assets will not take effect).
- If the **Group Name** checkbox is selected, all assets will be included - both **All groups** and **Ungrouped**.

To Export an Asset:

1. Select the check boxes of the assets to export, or select the **Group name** check box at the top of he **Groups** list to select *all* assets.
2. Click the green Down arrow button at the bottom of the **ASSET CONFIGURATION** panel.
3. The **Export CSV** dialog opens. Enter a **CSV file name** (You do not have to add the `.csv` file extension) and click **Export**.
4. The **Export finished** dialog shows when the export file has been created. Click **Download** to save the CSV file to your selected download location.

To Import an Asset:

1. Click the green Up arrow button at the bottom of the **ASSET CONFIGURATION** panel.

2. A pop-up box will appear asking you choose your file.
3. Click the **Choose file** button and select the exported CSV file that you have saved to your computer.
4. Click the **Import** button.

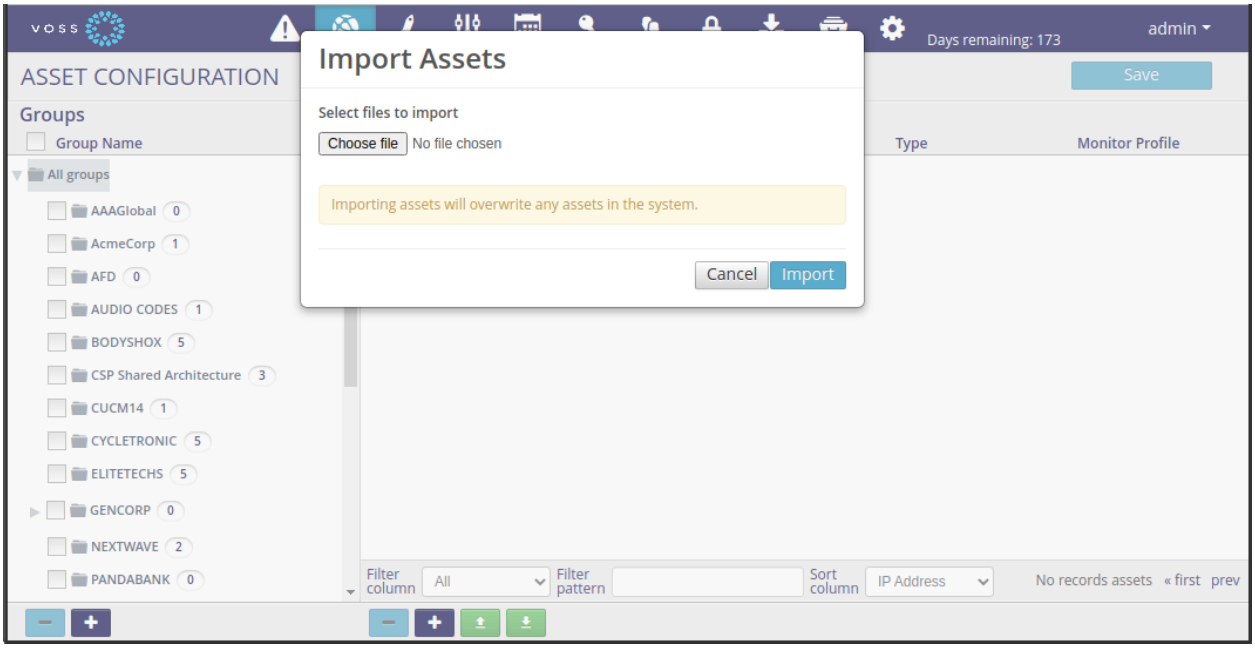
### Asset CSV Format

The following columns are in an exported CSV file:

```
"Asset Name",Description,"IP Addres","MAC Address",Vendor,
Model,Version,"Host Name",Alias,"Asset Group Name",
"Type of Device(see below)","Device's Timezone",Comments,
"Physical Address","Customer Name","Site Name","Row Action"
```

**Note:**

- The `"Row Action"` column is used when importing and if it contains “delete”, then the row will be deleted upon import.
- Row uniqueness is the combination of: “IP Address”, “Customer Name”, “Site Name”. If an asset found, its data will be updated. if not, new asset will be inserted under the asset group indicated in column “Asset Group Name”.
- The column “Asset Group Name” has to be unique. if an asset group is found, its data will be updated. If not, a new asset group will be inserted.
- There are 2 entries in the import CSV:
  - An asset with data in all columns. Most important is the very first column “Asset Name”.
  - An interface is a property of an asset. An interface only has data in from column “Description” to “Host Name”. Most important is that it does not have data on the very first column “Asset Name”. All CSV interface row(s) will be under an asset just right above it(them).



### 4.1.3. Probe Configuration

The Probes Configuration panel allows you to assign a group of scripts to an asset that can run on a set interval. These scripts will allow for data collection from many types of devices. The protocols can be API, SNMP or custom CLI scripts. SNMP v3 is also supported.

The return data from the Probes can then be injected into the system for correlation or can be stored in the database to allow for analysis on the Dashboard/Reporting server.

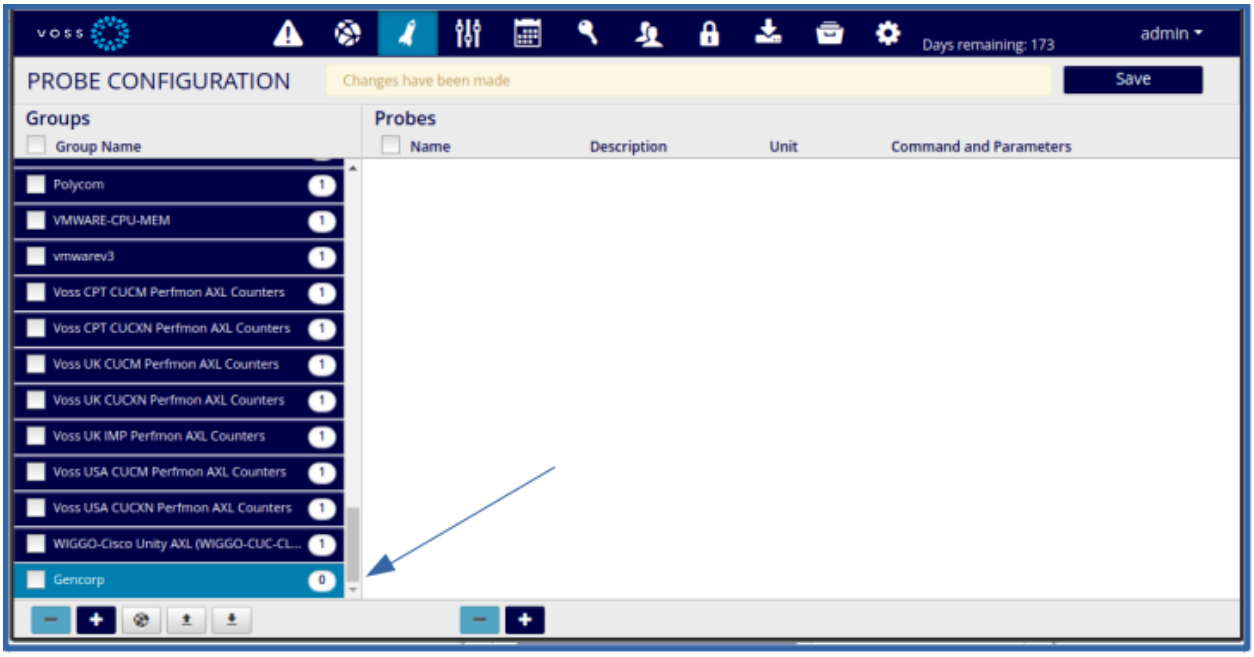
For PRI and SIP Trunk probes for Cisco Voice Gateways, reference:

Arbitrator Cisco PRI and SIP Probe Configuration

#### Creating a Probe Group

To create a new Probe Group:

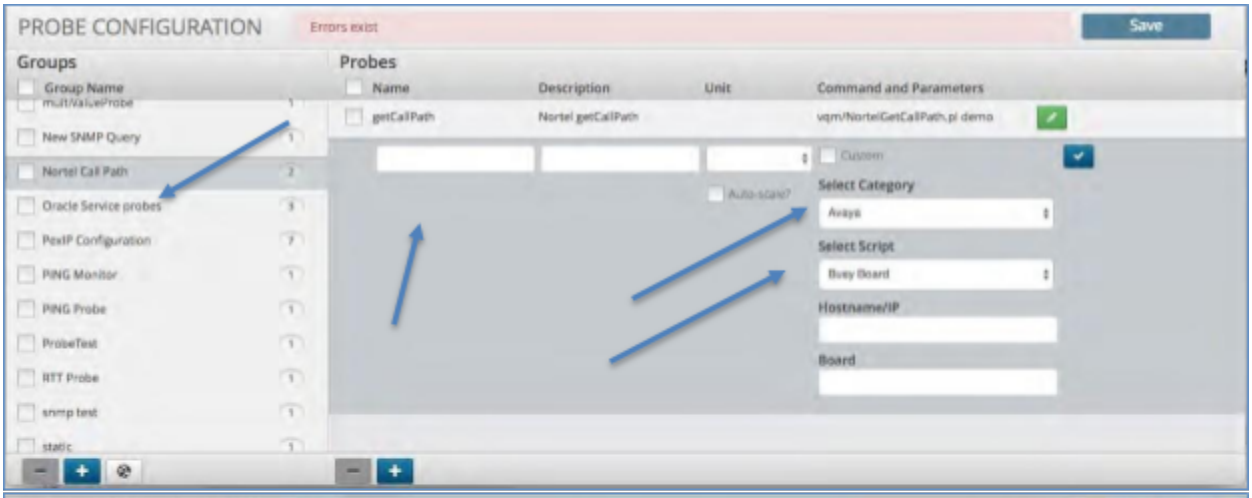
1. Click the Probe icon from the Menu bar.
2. Click the “Plus” icon within the Groups pane in the bottom left corner.
3. Enter the “Group” name and press Enter.
4. Click the “Save” icon in the upper right corner.

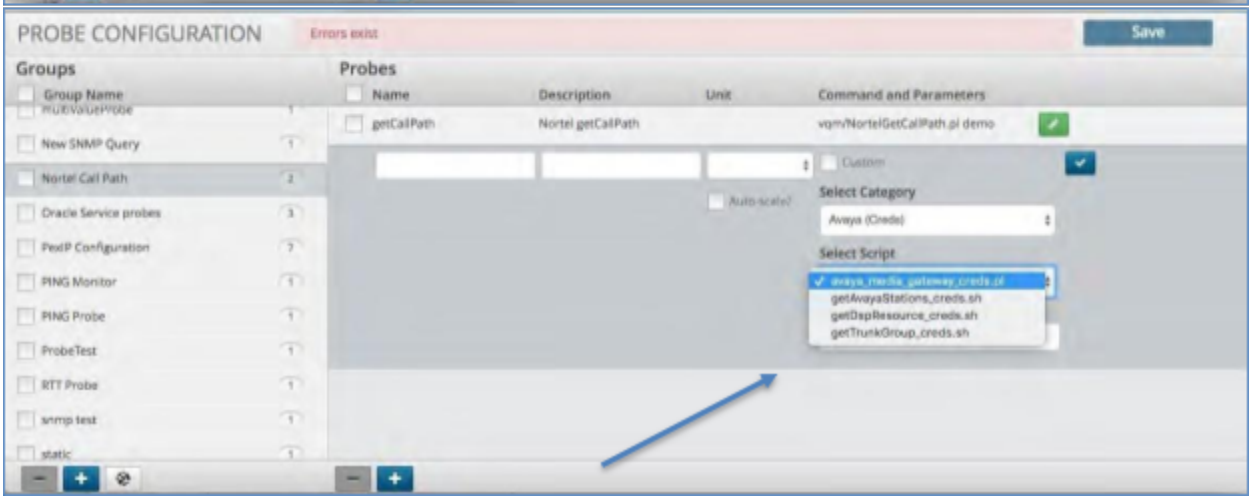


### Creating a Probe

To create a new Probe:

1. Click the group in which you wish to create a new Probe.
2. Click the Plus icon within the Probes panel.
3. Enter the name and description of the Probe.
4. De-select the check icon from the field titled “Custom”. This field is utilized when putting a custom probe in place versus utilizing the ones within the system.
5. Select the Probe Category from the drop-down list. This will populate the scripts available in that category within the drop-down menu titled “Select Script”.
6. Select a script from the script drop-down list.
7. Enter any additional information required by the selected script, such as the hostname, IP, etc.
8. Click the “Check” icon to close the probe in the far right of the Probe panel.
9. Click the “Save” icon to save the added Probe.

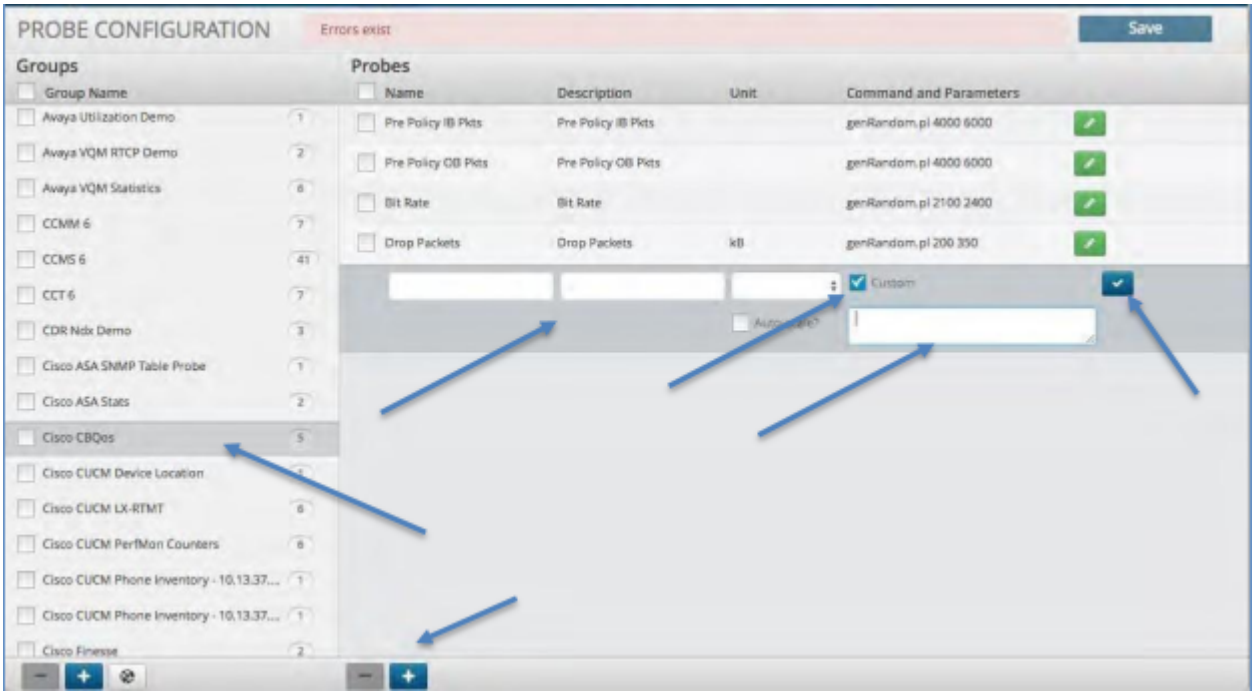


### Creating a Custom Probe

To create a new Probe:

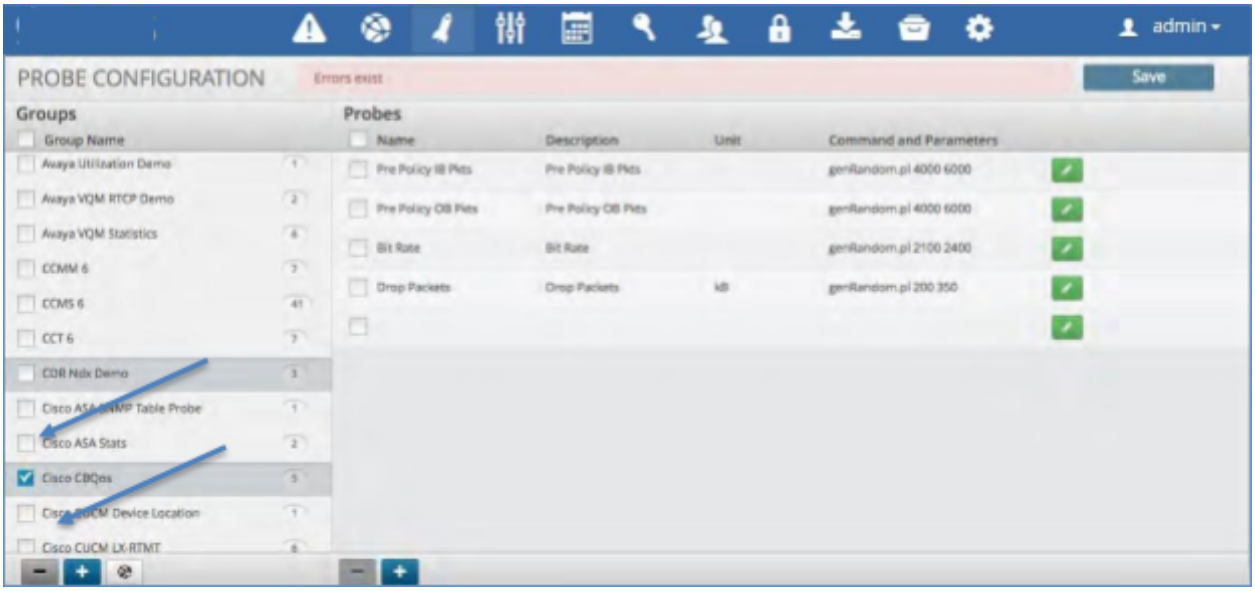
1. Click the group in which you wish to create a new Probe.
2. Click the Plus icon within the Probes panel.
3. Enter the name and description of the Probe.
4. Select and click the check icon from the field titled “Custom”. This field is utilized when putting a custom probe in place versus utilizing the ones within the system.
5. Enter the path and script that you wish to run.
6. Click the “Check” icon to close the probe in the far right of the Probe panel.
7. Click the “Save” icon to save the added Probe.




### Deleting a Probe Group

To delete a Probe Group:

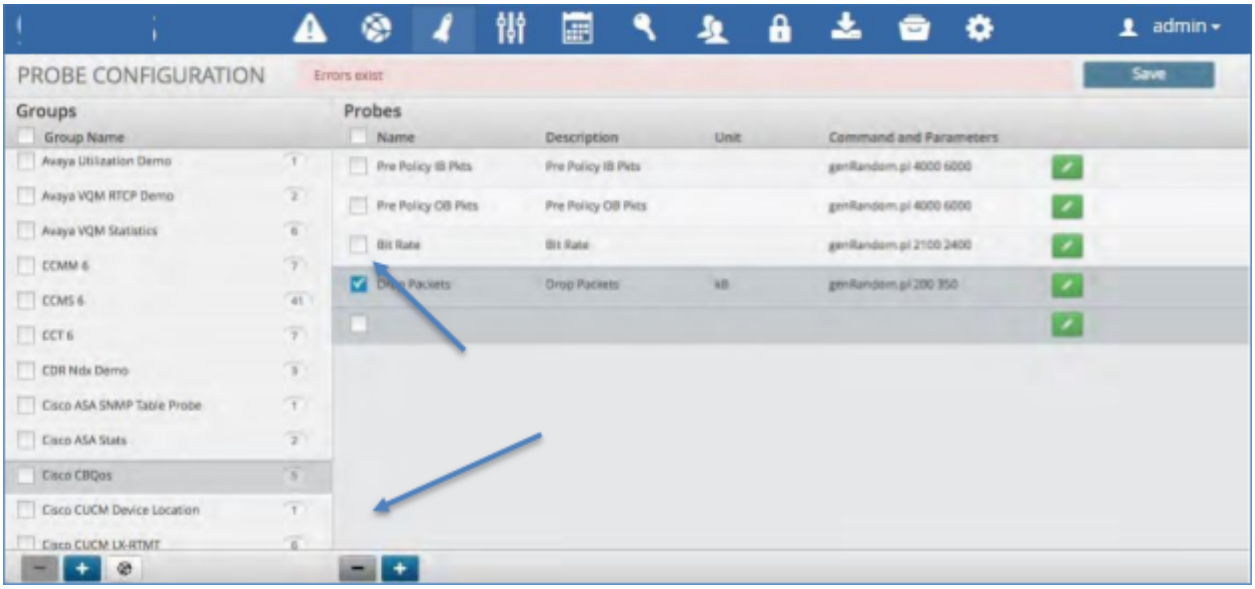
1. Click the check box next to the group name you wish to delete.
2. Click the Minus icon within the Probe Group panel in the bottom left.
3. Click the “Save” icon to save the changes.




### Deleting a Probe

To delete a Probe:

1. Click the check box next to the Probe name you wish to delete.
2. Click the Minus icon within the Probe panel in the bottom right.
3. Click the “Save” icon to save the changes.



### Export and Import a Profile (assignment of a probe to an asset)

**Important:** This import/export is special. Since we do not have a Profile main screen, the import/export profiles are in Probe Configuration; the same as the legacy push button (right next import/export buttons).

Within the **PROBE CONFIGURATION** section, you can export and import the profiles that you exported from another system.

A new system log table `insights_system_log` has also been added to log user actions and a user can create a dashboard to view these actions.

See the:

Log Search Section in the Dashboard and Reporting Administration Guide.

To Export a Profile:

1. Click the Down arrow button at the bottom of the **PROBE CONFIGURATION** panel.

   Since this is a probe configuration, we cannot select individual profiles, so it will export all profiles in the system.
2. The **Export CSV** dialog opens. Enter a **CSV file name** (You do not have to add the `.csv` file extension) and click **Export**.
3. The **Export finished** dialog shows when the export file has been created. Click **Download** to save the CSV file to your selected download location.

To Import a Profile:

1. Click the Up arrow button at the bottom of the **PROBE CONFIGURATION** panel.
2. A pop-up box will appear asking you choose your file.
3. Click the **Choose file** button and select the exported CSV file that you have saved to your computer.
4. Click the **Import** button.

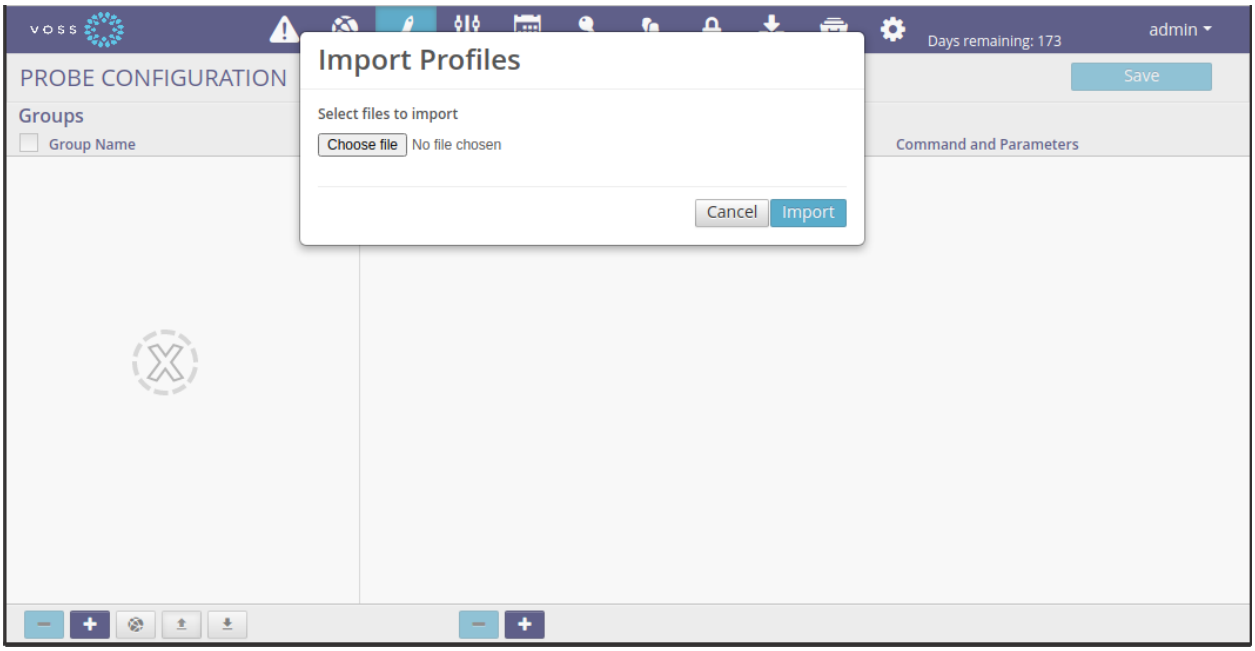
### Profile CSV Format

The following columns are in an exported CSV file:

```
"Row Action","Asset Name","IP Address","Customer Name",
"Site Name","Probe Group Name","Credential 1 Name",
"Credential 2 Name","Frequency (s)",Enable
```

**Note:**

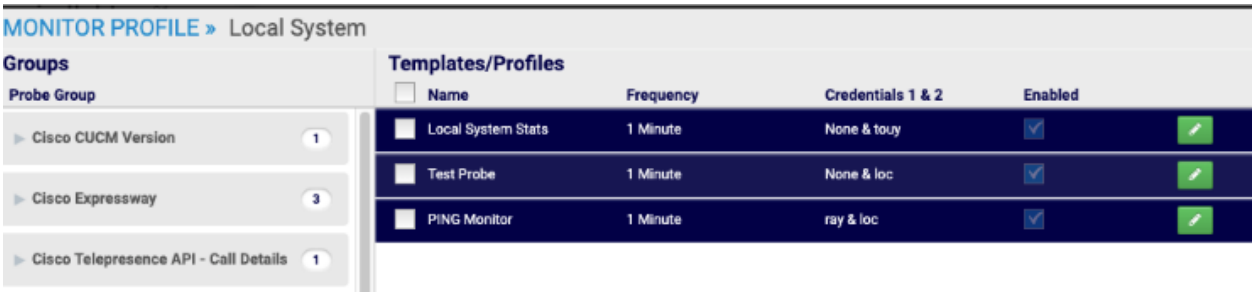
- The `"Row Action"` column is used when importing and if it contains “delete”, then the row will be deleted upon import.
- “Probe Group Name” must be unique.
- Combination: “IP Address”,”Customer Name”,”Site Name” must to be unique.
- “Asset Name” is used as a reference of the asset.
- When importing and if an asset and a probe group are found, then a profile will be updated/inserted. If not, nothing to import.




### Assignment of a probe to an asset

A probe group assigned to an asset can be modified using a profile CSV file import by specifying the related “Asset Name” and “Probe Group Name” in the CSV file.

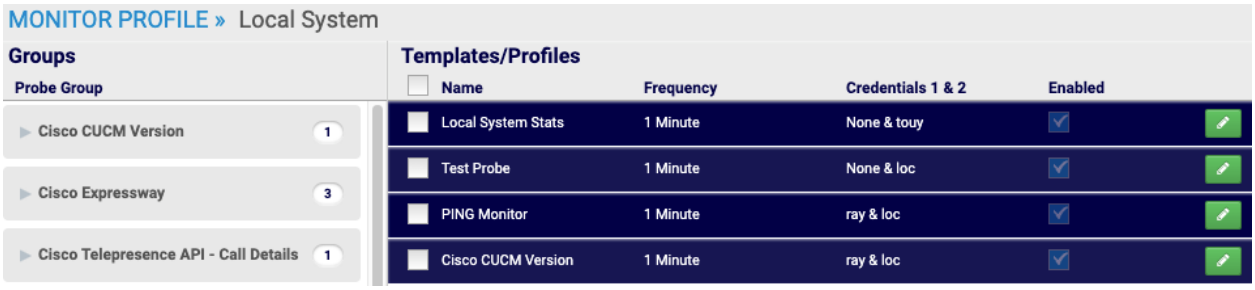
For example, consider an asset “Local System” that has 3 profiles:




We can assign probe “Cisco CUCM Version” to asset “Local System” as a CSV file import:

| Row Action | Asset Name | IP Address | Customer Name | Site Name | Probe Group Name | Credential 1 Name | Credential 2 Name | Frequency (s) | Enable |
|---|---|---|---|---|---|---|---|---|---|
| | Local System | 10.13.37.149 | | | Cisco CUCM Version | ray | loc | 60 | TRUE |

After importing, the profile is added to the probe group.



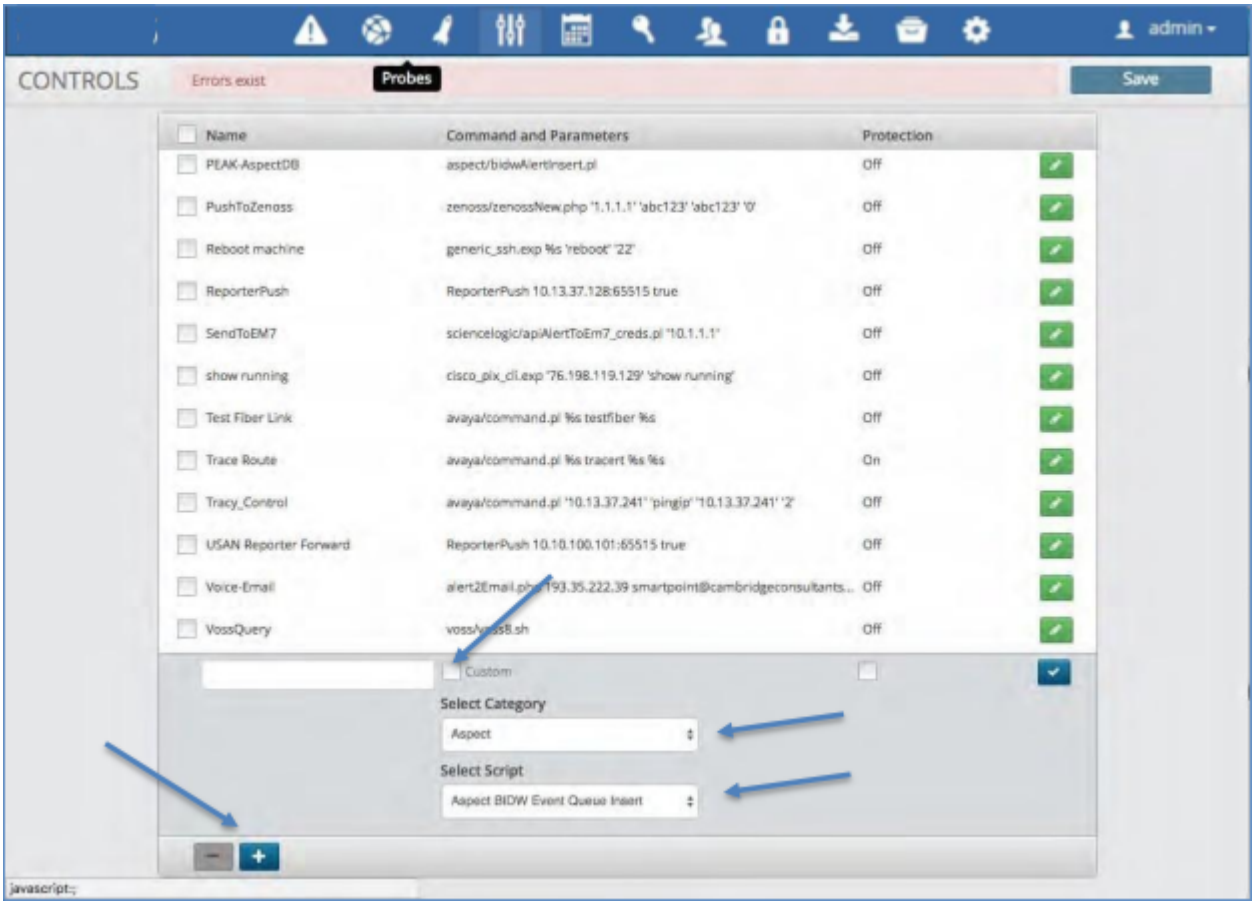

## 4.1.4. Controls

The Controls Configuration panel allows you to define a script or routine that can be executed by a response procedure or attached as a probe. These controls can be passed variables extracted from a correlation rule. The resulting return of the scripts execution can be mapped to the database, used as an action or can be injected back into the system to be correlated against another element.

### Creating a Control

To create a new Control:

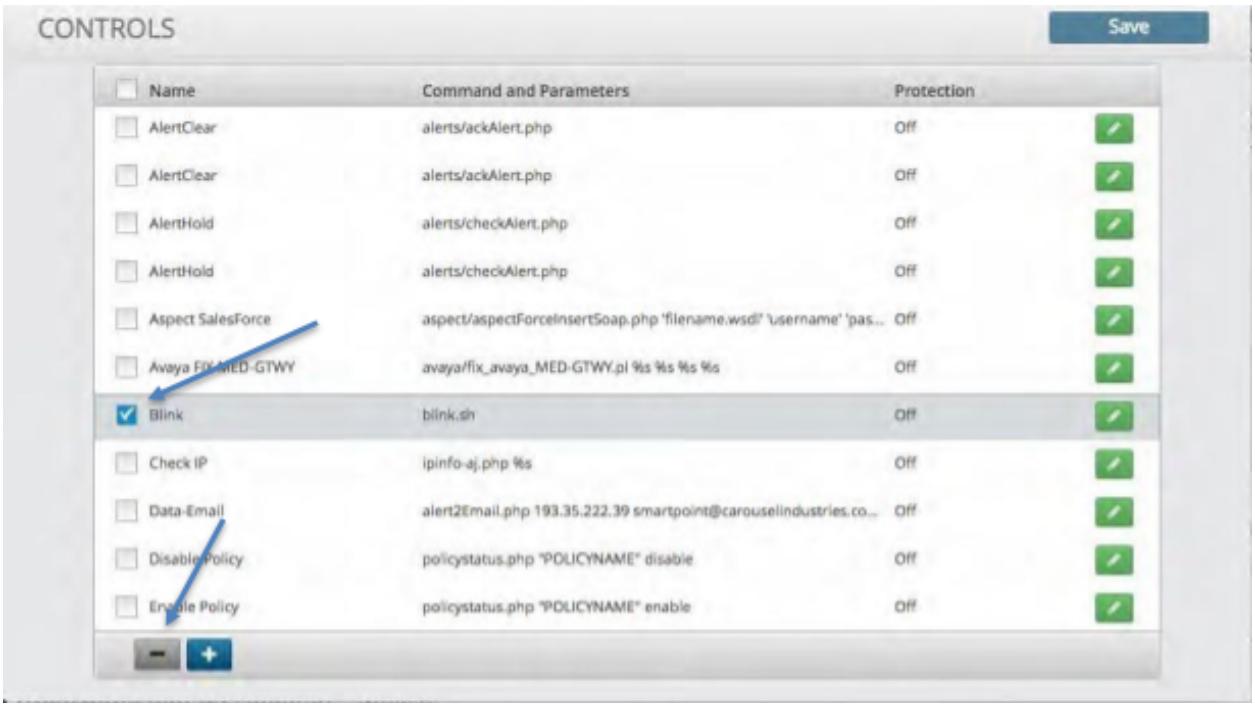
1. Click the Plus icon within the control panel.
2. Enter the name of the Control.
3. De-select the check icon from the field titled “Custom”. This field is utilized when putting a custom Control in place versus utilizing the ones within the system.
4. Click and Select from the categories dropdown list to populate the scripts dropdown.
5. Select a script from the script dropdown list.
6. Enter any additional information required by the selected script.
7. Click the Check icon to close the control in the far right of the control panel
8. Click Save icon.




### Deleting a Control

To delete a Control:

1. Click the check box next to the Control name you wish to delete.
2. Click the Minus icon within the Control panel at the bottom.
3. Click the “Save” icon to save the changes.




### 4.1.5. Response Procedure Configuration

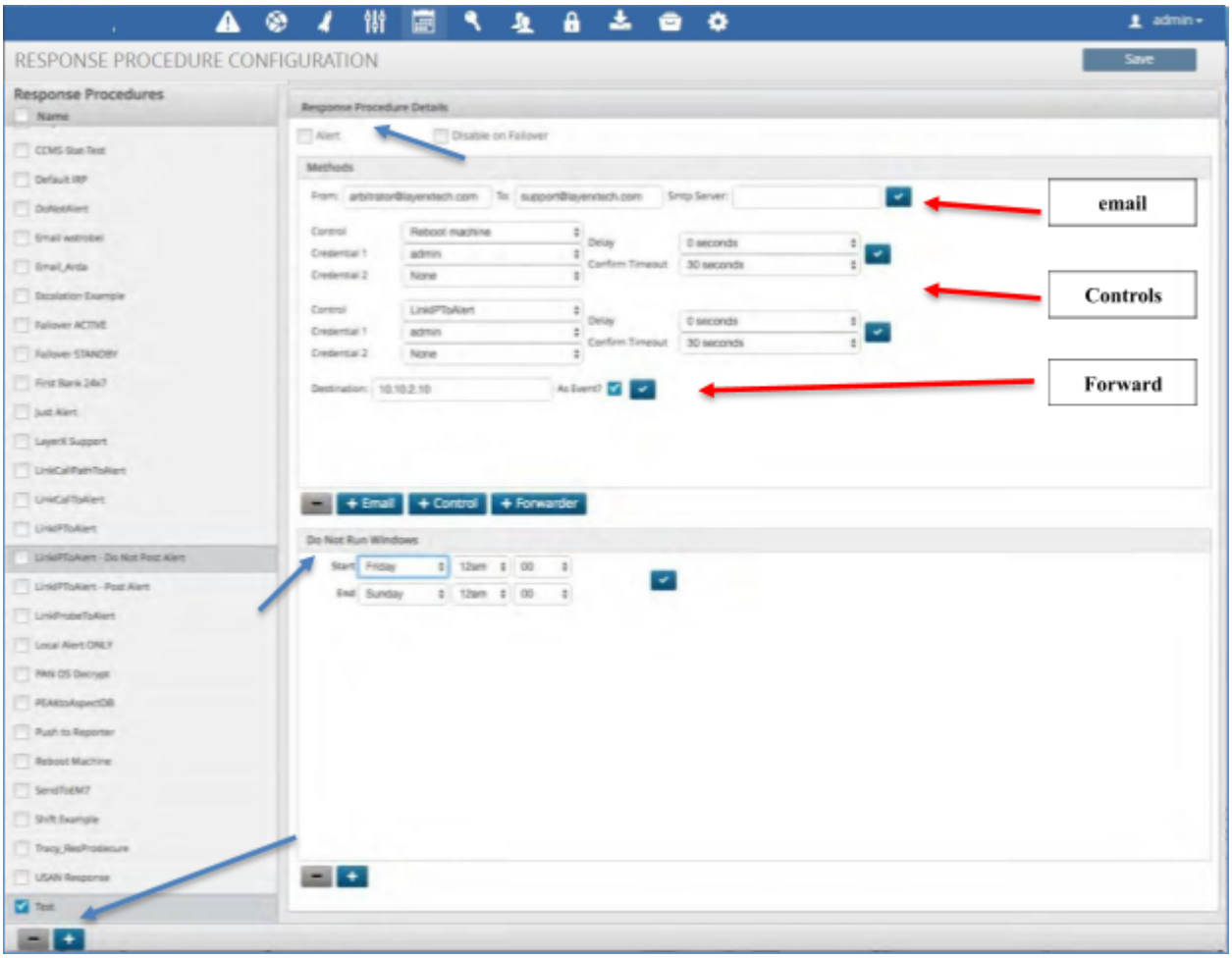
The Response Procedure configuration panel allows you to define an automated response to a correlated event. Each Response Procedure can be assigned to one or more Correlation Rules while also containing and/or executing one or more of the following responses:

| Action | Description |
|---|---|
| Alert | Visually show the alert in the alert views within the User Interface. |
| Email | An email will be sent to the recipients address and contain the Policy and Correlation Rule details that are triggered. Additionally, any data that is extracted from the correlated event will be included. |
| Control | Executes the selected Control Script as a result of the correlated event. Data from the correlated event will be passed to the script as well. These scripts can be utilized as run-book and/or automated remediation. |
| Forward | The forward allows the correlated event to be forwarded to another Arbitrator Correlation platform. |

### Creating a Response Procedure

To create a response procedure:

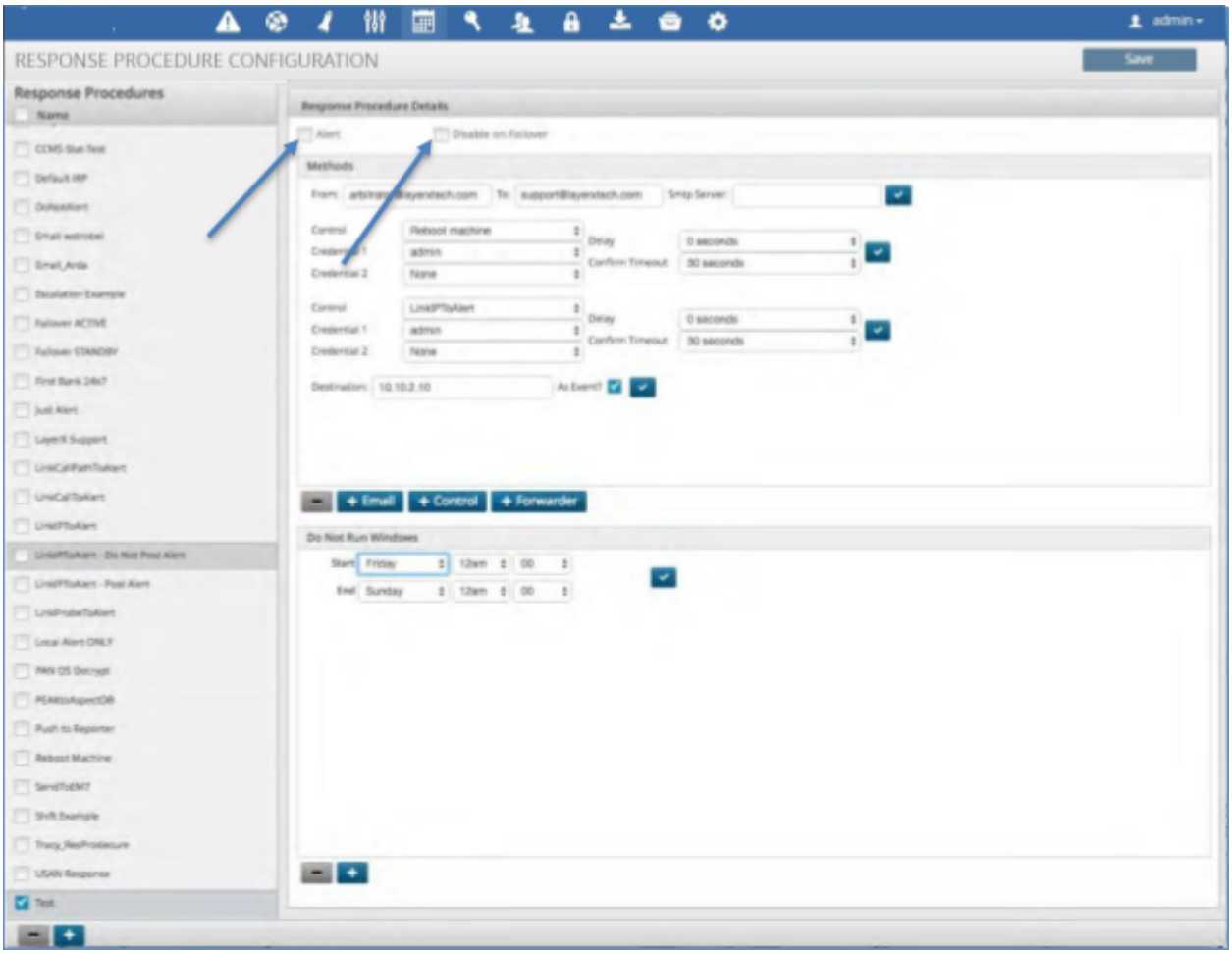
1. Click the “Calendar” icon at the top of the Configuration panel.
2. Click the plus icon in the bottom left of the Response Procedure name panel. A box will open up where you can fill in the name of your response procedure.
3. The panel to the right is broken into two sections:
    a. Response Procedure Details – This is the section that you select to add the elements defined in the table above.
    b. Do Not Run Windows – Allows you to define certain date and times that you don’t want the system to take the actions within the Response Procedure.



### Assigning an Alert to a Response Procedure

To assign the Alert function to a response procedure:

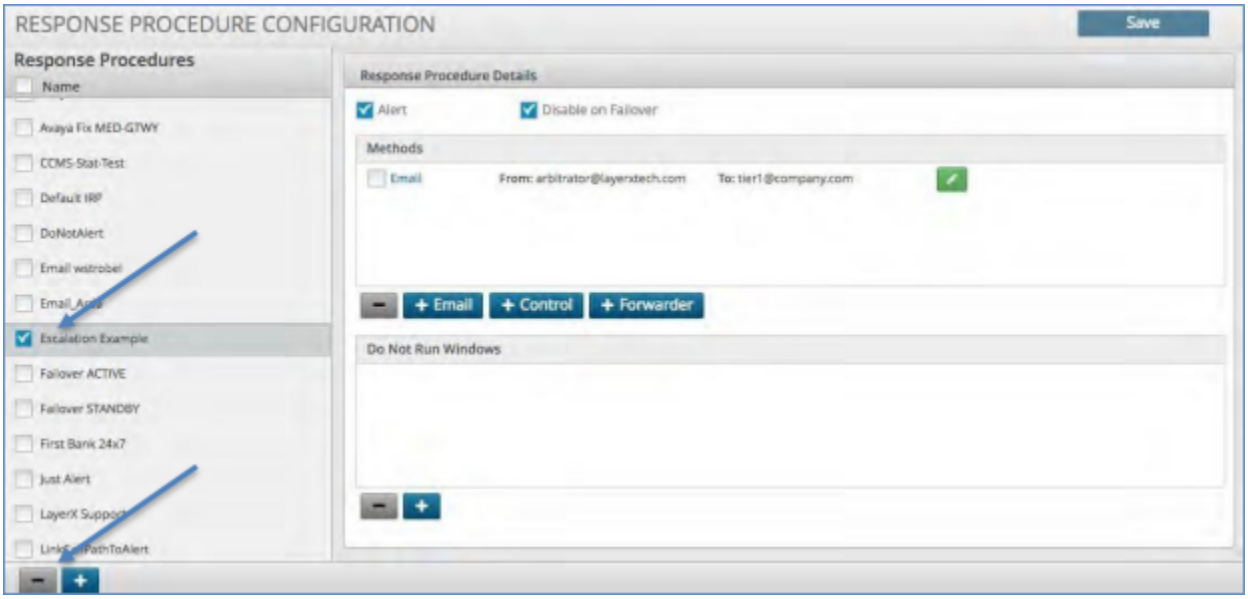
1. Click the Alert check box in the top left of the Response Procedure Details panel.
2. If this system you are configuring is intended to be the redundant platform then click the Disable on Failover box to allow all data to flow but no actions to take place.



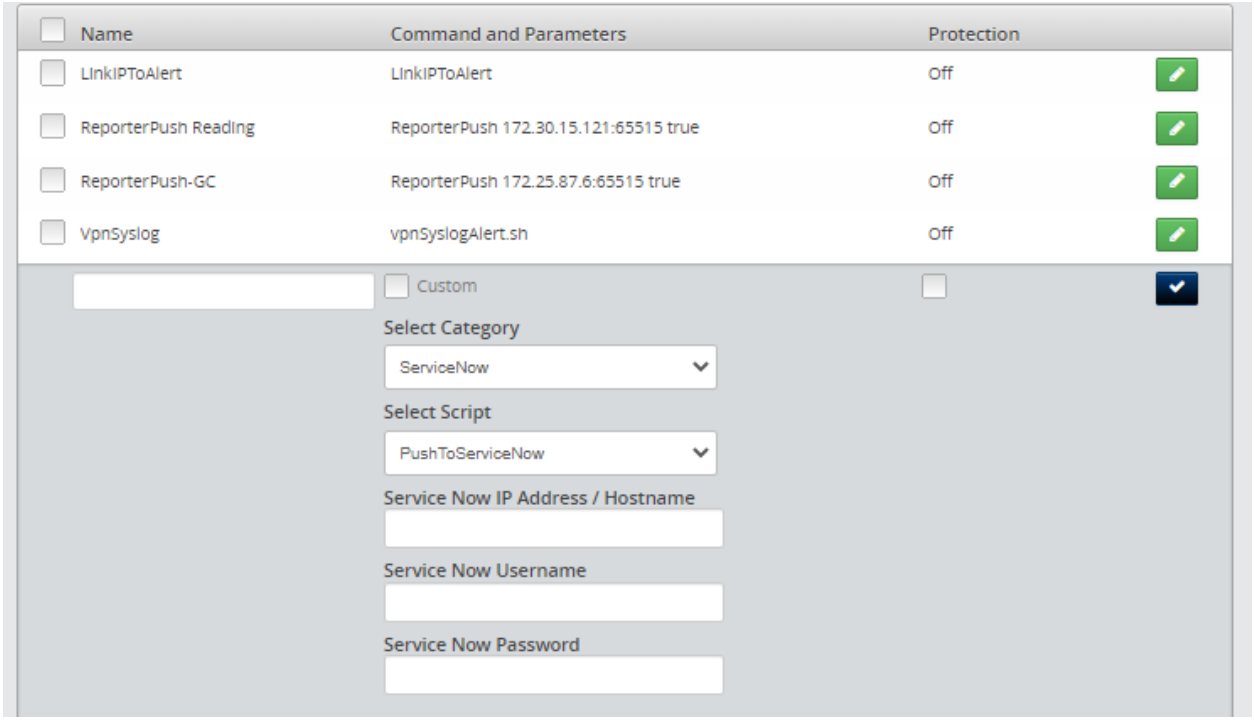

### Deleting a Response Procedure

To delete a Response Procedure:

1. Click the box next to the Response Procedure name.
2. Click the minus icon at the bottom of the Response Procedure name panel.
3. Click the Save icon to save your changes.




### 4.1.6. How to Enable ServiceNow Intergration




1. Navigate to Configuration (cog icon) on the arbitrator.
2. Navigate to Control and click + to enter a new control.
3. In the **Name** text box enter ServiceNow.
4. Untick **Custom**.
5. Fill in the following details:

- **Select Category**: ServiceNow
- **Select Script**: PushToServiceNow
- **Service Now IP Address** / **Hostname:**
- **Service Now Username:**
- **Service Now Password:**

6. Tick the blue tick box.
7. Click the **Save**.
8. Navigate to the Response Procedure Configuration menu.
9. Apply the control to the required IRP, such as the default IRP.

### 4.1.7. ServiceNow One Way Incident Integration

As the Correlation Platform detects new incidents a response procedure is defined to send the event into ServiceNow utilizing their API. Incident Response Procedures (IRP) are defined on an incident basis. Thus you can choose which events need to be sent to ServiceNow based on severity, type, threshold, or others. When the IRP kicks off it will create an event, insert the following fields and send it to ServiceNow:

- short description: Arbitrator Policy, Rule and Reference_Id
- description: full message from arbitrator
- severity: severity
- urgency: based on severity
- impact: based on severity
- category: software
- comments: full message from Arbitrator

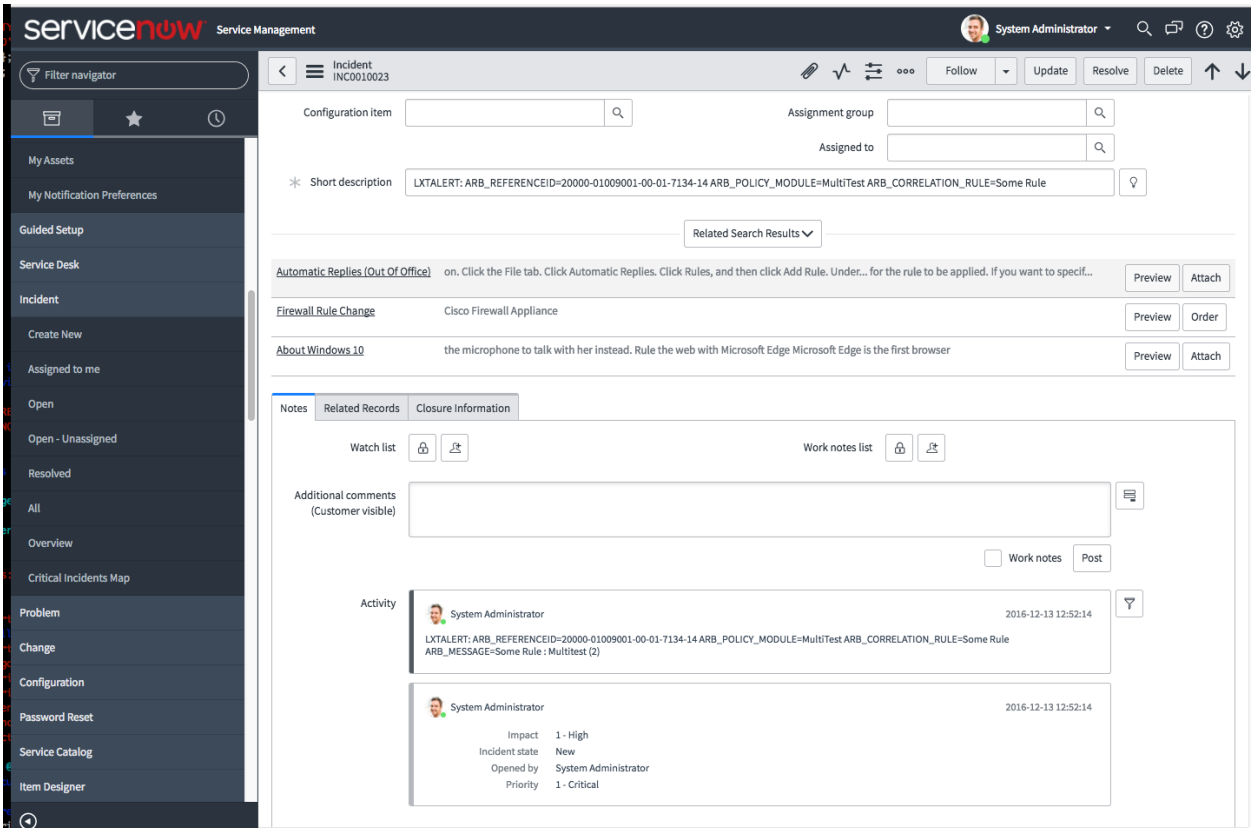
#### ServiceNow Requirements

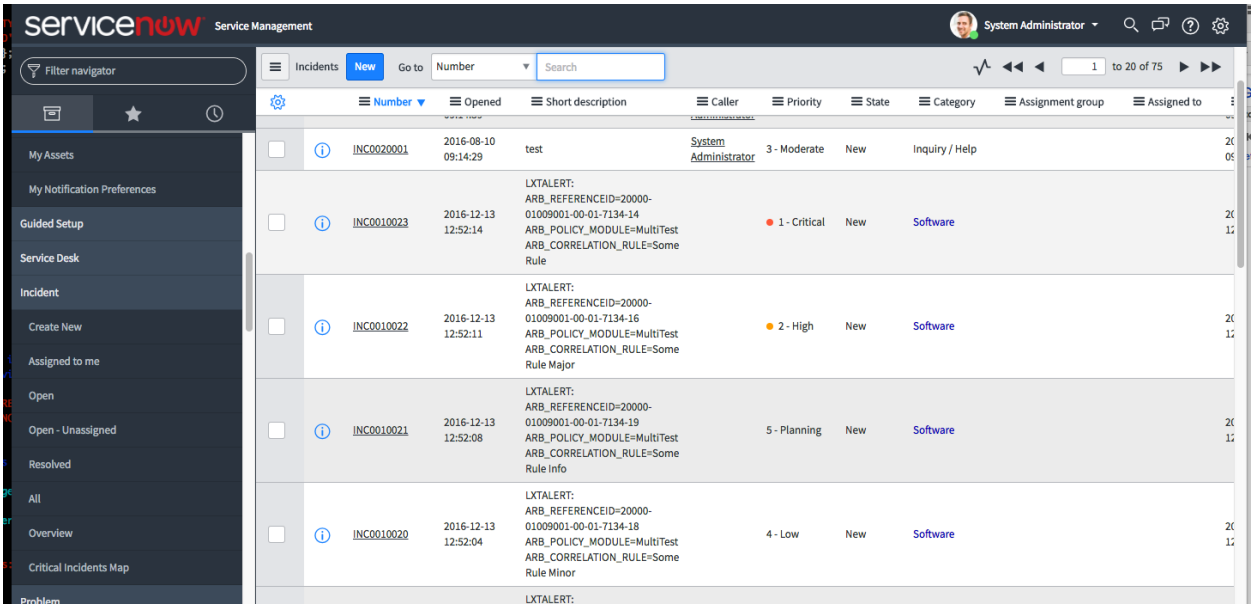
- ServiceNow URL
- ServiceNow User with SOAP API rights to insert Incidents
- ServiceNow Password

#### Arbitrator Correlation Configuration

- Version Required: 4.0001-15b
- Script: `servicenow/PushToServiceNow.pl`
- parameters:
  - `URL_TO_SERVICENOW_INSTANCE`
  - `USERNAME`
  - `PASSWORD`

## Screenshots From ServiceNow



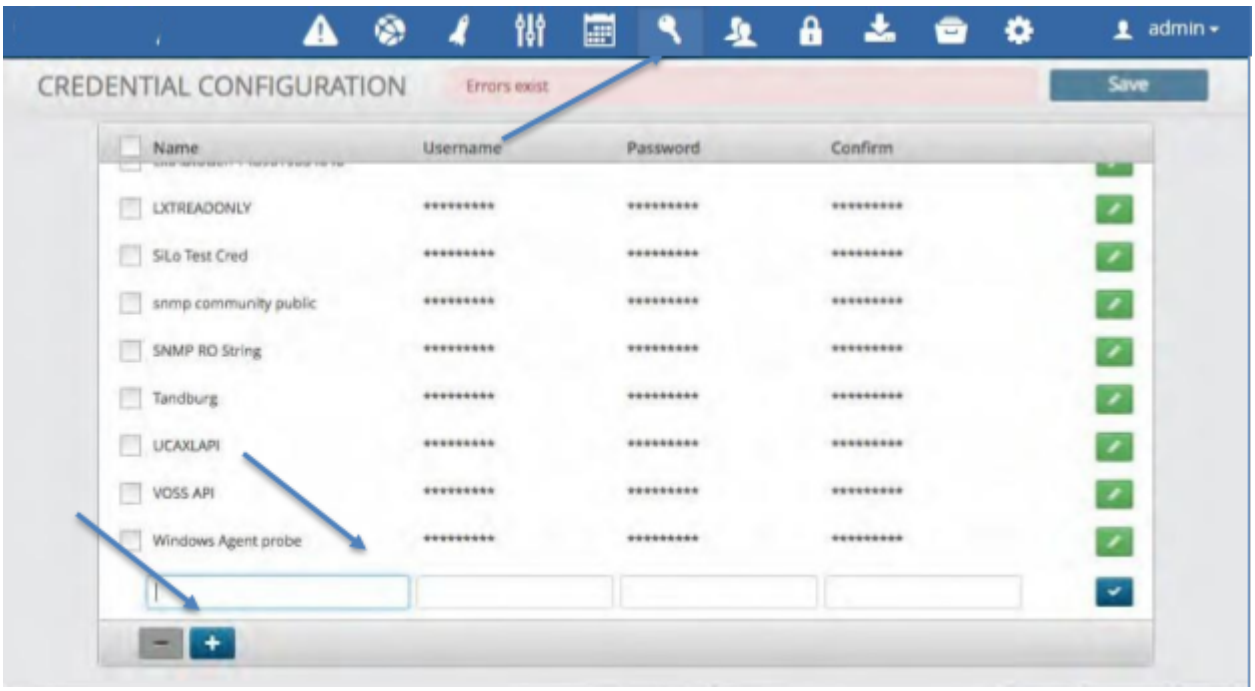
### 4.1.8. Credential Configuration

The Credentials configuration panel allows you to define and store credentials securely. These credentials can be assigned to a Probe or Control to allow for secure access to an asset, ticketing system or script. (See: Asset Configuration, Response Procedure Configuration)

#### Creating a Credential

To create a Credential:

1. Click the “key” icon in the menu bar at the top.
2. Click the plus icon in the bottom left corner.
3. Enter the name to be assigned to the Credential.
4. Enter the Username and Password fields.
5. Click the blue check box.
6. Click the Save icon to save the credential.




#### Deleting a Credential

To delete a Credential:

1. Click the check box to the left of the credential name you wish to delete.
2. Click the minus icon in the bottom left of the screen.
3. Click the Save icon to save your changes.


### 4.1.9. Customer Configuration

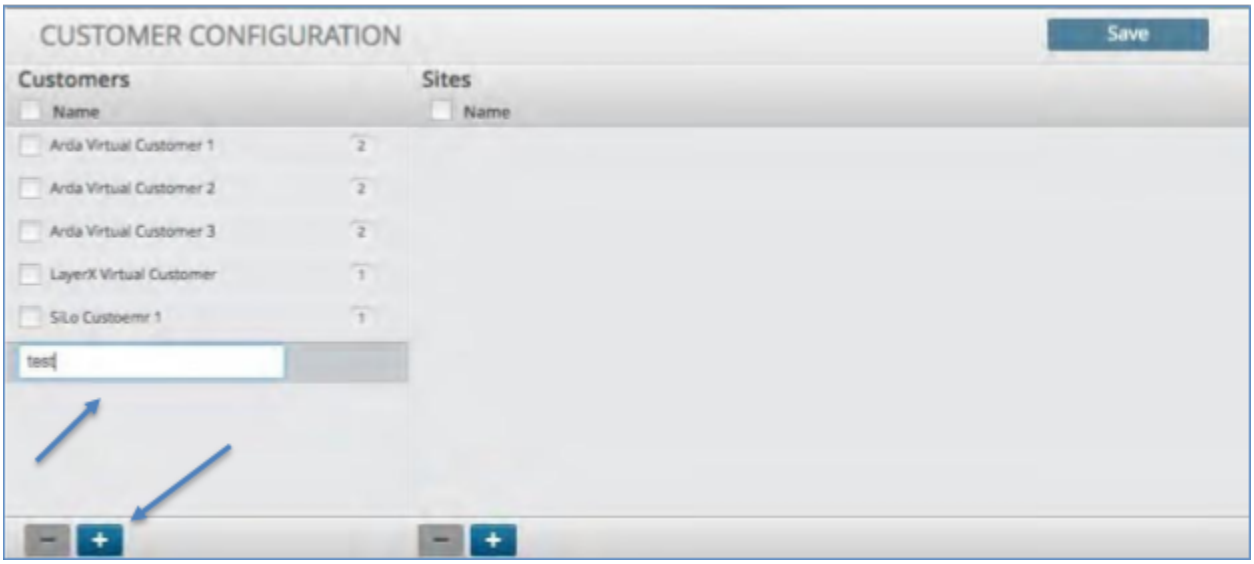
To enable multi-tenancy (assets, alerts and data) utilize the customer configuration panel to define a customer and their related locations (sites). Once defined, the Customer field can be applied to an asset and or a user to restrict access to other customers assets, alerts and data.

(See: Asset Configuration, Access Control Configuration).

#### Creating a Customer

To create a Customer:

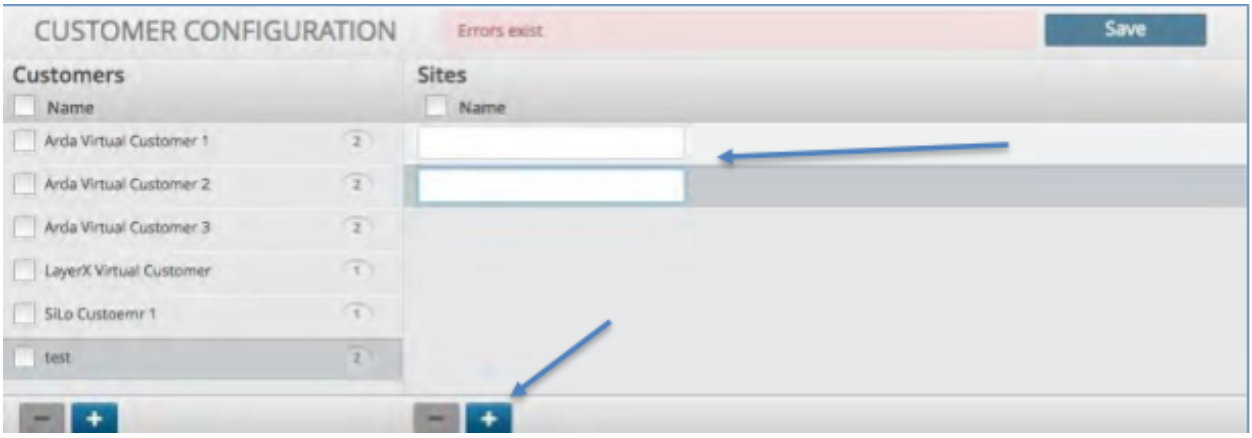
1. Click the “customer” icon in the menu bar at the top.
2. Click the plus icon in the bottom left corner of the customer panel.
3. Enter the name of the Customer to be added and press Enter.
4. Enter the Username and Password fields.
5. Click the Save icon to in the upper right corner.
6. Proceed to creating a Customer Site.




### Creating a Customer Site

To create a site for a Customer:

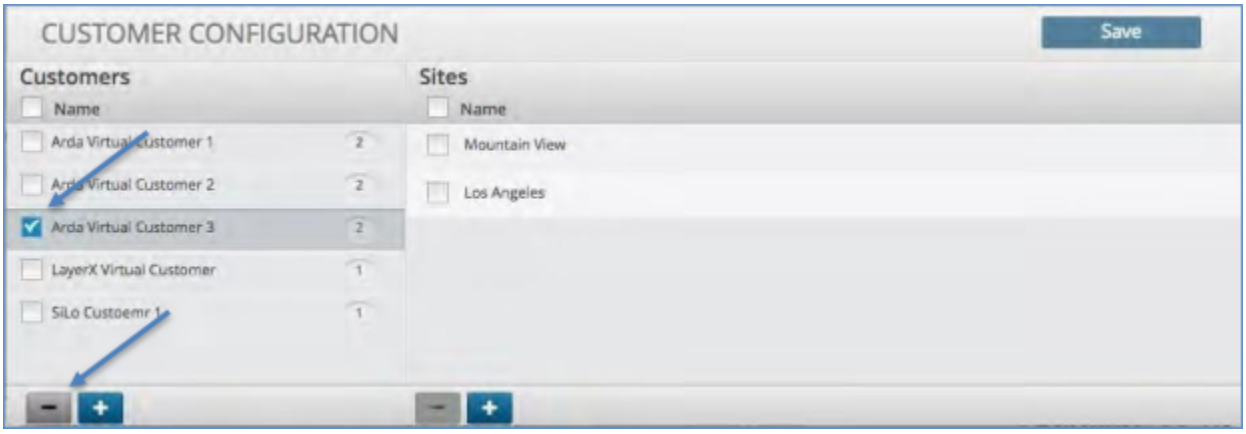
1. Click the customer to which you wish to add the site.
2. Click the plus icon in the bottom of the site panel.
3. Enter the site name and press Enter.
4. Add additional sites if applicable.
5. Click the Save icon to in the upper right corner.



### Deleting a Customer

To delete a Customer:

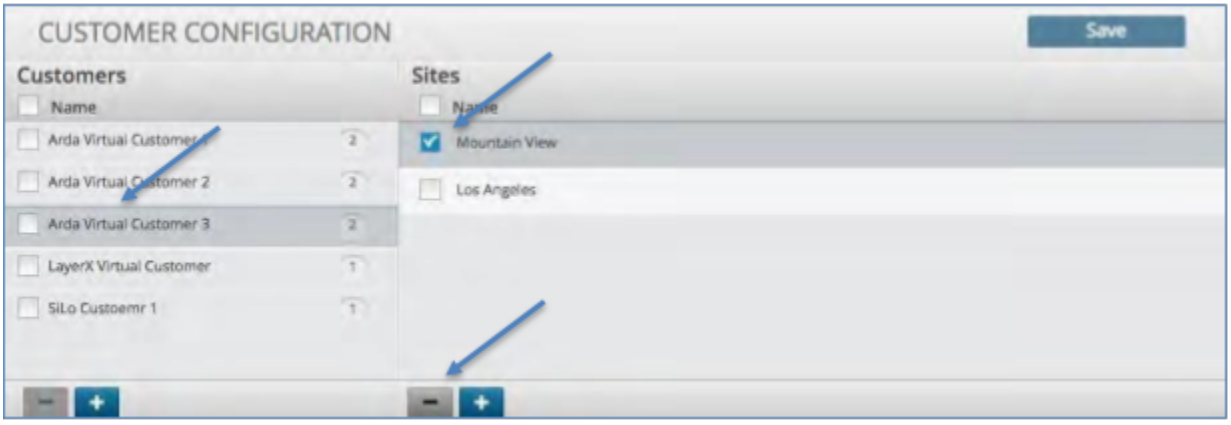
1. Click the check box of the customer you wish to delete.
2. Click the minus icon in the bottom of the site panel.
3. Click the Save icon to in the upper right corner.




### Deleting a Customer Site

To delete a site for a Customer:

1. Click the customer in which you wish to delete the site.
2. Click the minus icon in the bottom of the site panel.
3. Click the Save icon to in the upper right corner.



### 4.1.10. Access Control

The Access Controls Configuration panel allows for specific Role Based Access Controls to be enabled. These controls are based on the role of the user and the customer to which they belong.

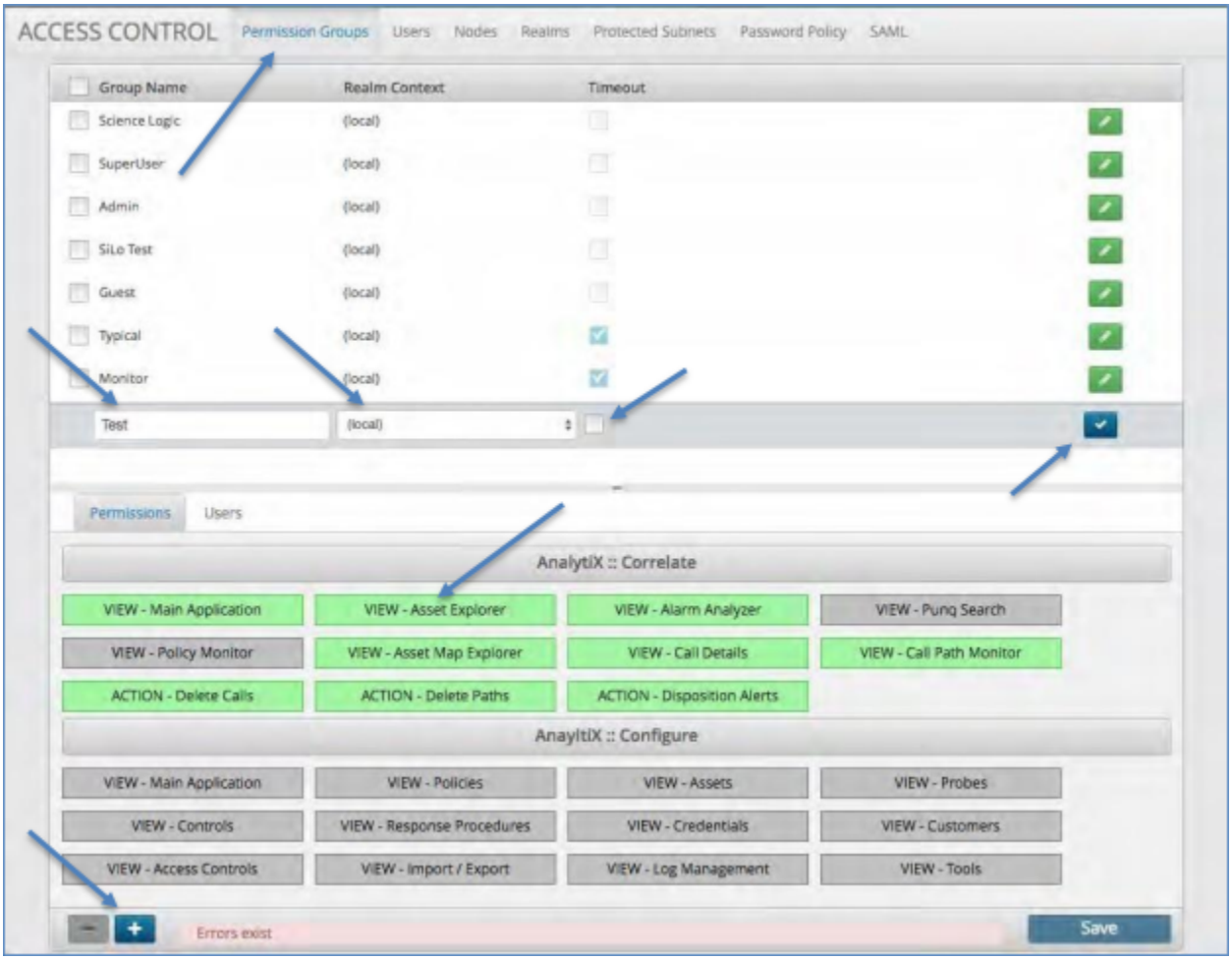
#### Permission Groups

The first tab under the Access Controls is the Permission Groups. This allows the admin to define a group that has specific capabilities/rights and subsequently add users to these groups.

#### Creating a Permission Group

To create a Permission Group:

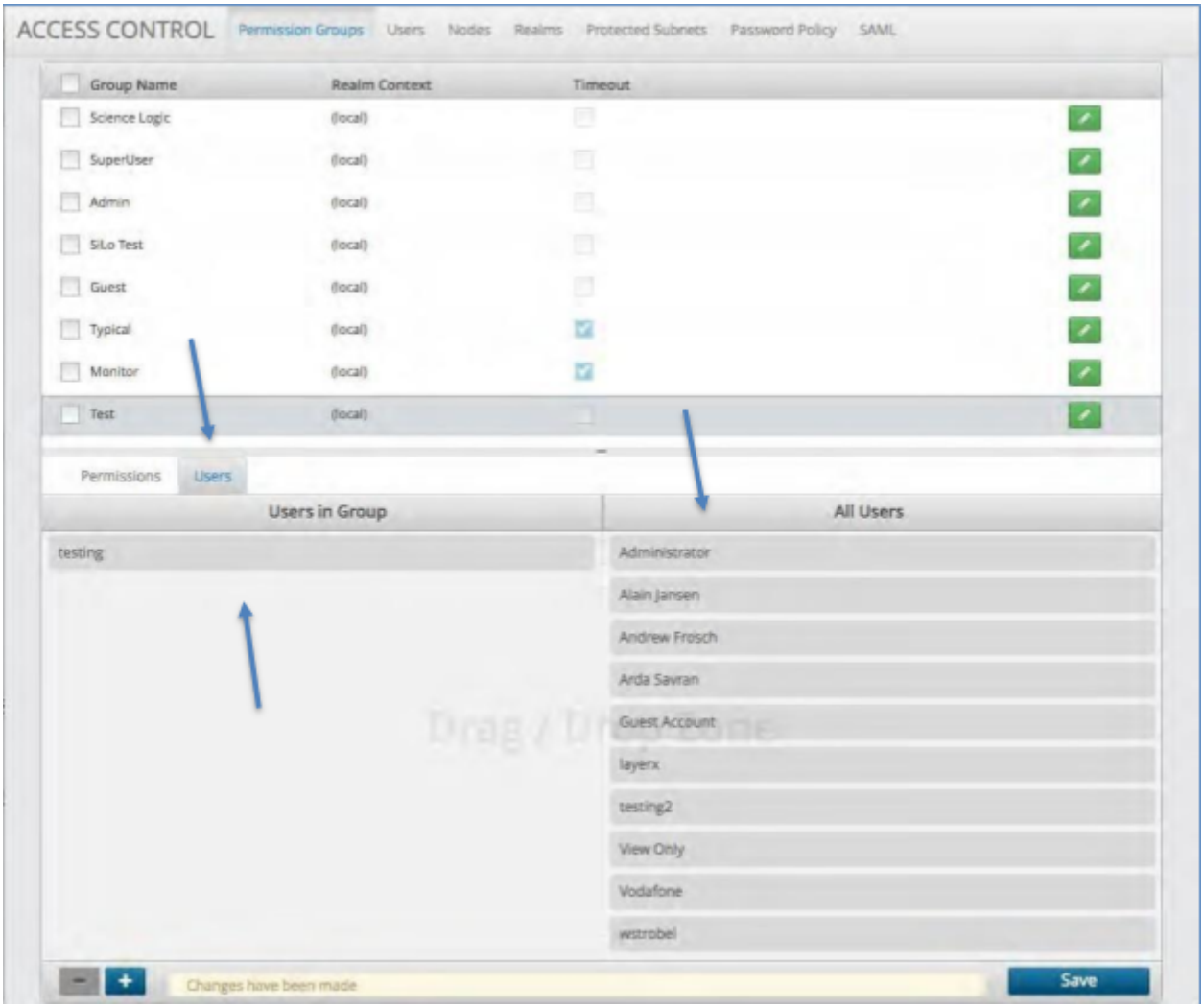
1. Click the Permission Group tab under the Access Control panel. A list of defined groups will be displayed.
2. Click the blue plus icon at the bottom of the panel.
3. Fill in the name of the group and select Realm Context drop-down button. This will always be local for a single Arbitrator deployment.
4. Click the Timeout box if you wish this user group to have their session timeout for non- use and require them to log back into the UI.
5. Select each system screen name tab that you wish to grant access to this group. As you select each tab it will turn green indicating that this system screen will be available to this group.
6. Click the blue check icon when complete.
7. Click Save to complete the addition of the group.




### Assigning and Removing Users to and from a Permission Group

To Assign a User to a Permission Group:

1. Click User next to the Permission tab. A list of All Users and Users in Groups will be displayed.
2. Click the Group to which you wish to add a User.
3. Drag the desired user(s) from the “All Users” section to the drop zone under “Users in Group”.
4. To remove a User from a Permission Group simply drag the user from the “Users in Group” section over to the “All Users” section
5. Click Save to complete the action.




### Users

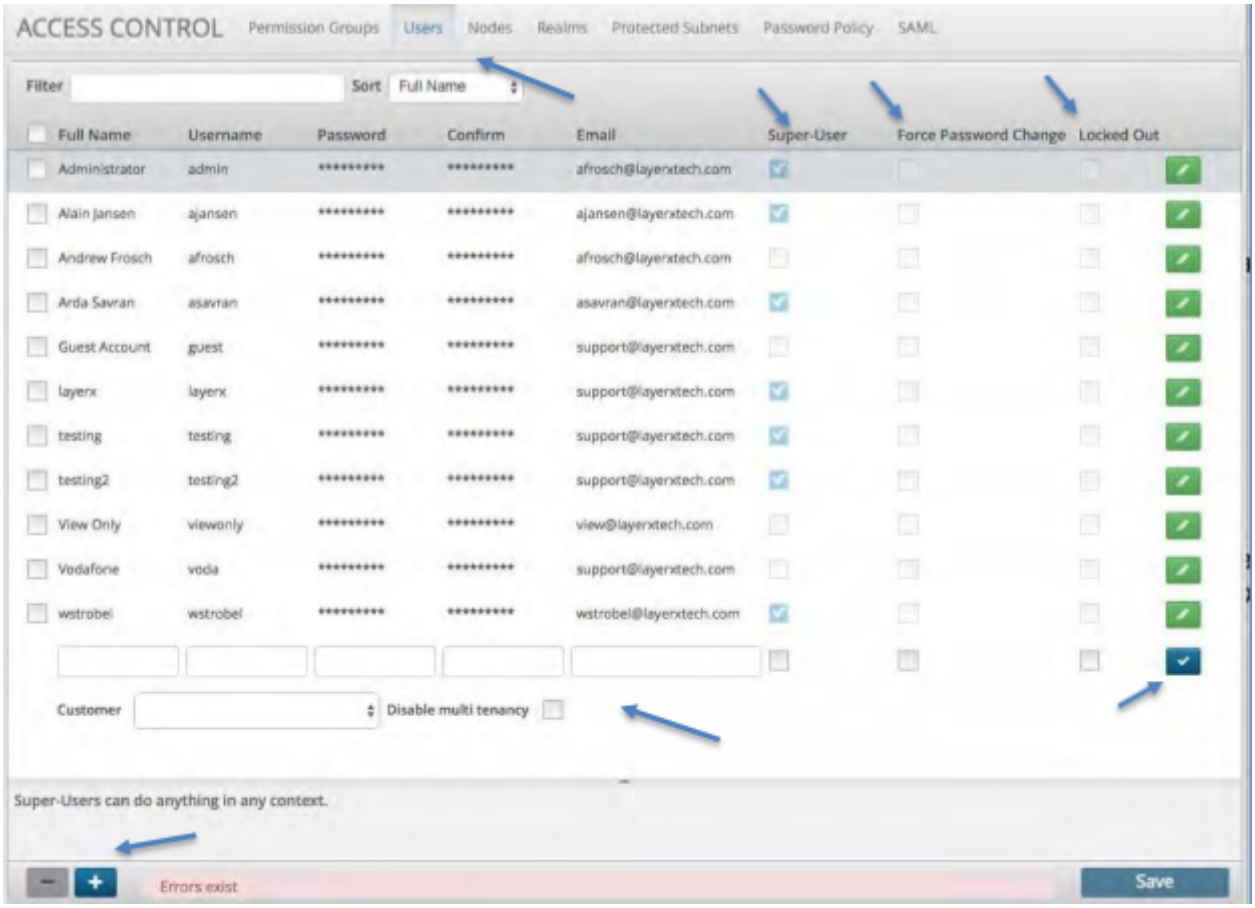
The Users tab allows you to create a new user or modify an existing one. The users can be set up as “Super Users” or assigned roles in the permission groups. Once the user is added and saved then they will be available to add to the Permission Groups per the last section.

### Creating a New User

To create a new User:

1. Click the User tab at the top of the screen next to Permission Groups.
2. Click the blue plus icon at the bottom of the screen.
3. Fill in the required fields. (Full Name, Username, Password, Confirm and Email).
4. Check the Super-User box if applicable.
5. Check the Force Password Change if you want this user to follow the Password Policy.
6. Click the Locked Out box if you want this user to time on inactivity on the UI.

7. Select the Customer drop-down box and assign the user to a customer.
8. Check the Disable multi-tenancy if this is a single customer and multi-tenancy does not apply.
9. Click the Blue check icon to set the user.
10. Click the Save button to save the user.




### Deleting a User

To delete a User:

1. Click the check box next to the User name that you wish to delete.
2. Click the minus icon at the bottom of the screen.
3. Click the Save button to save your changes.

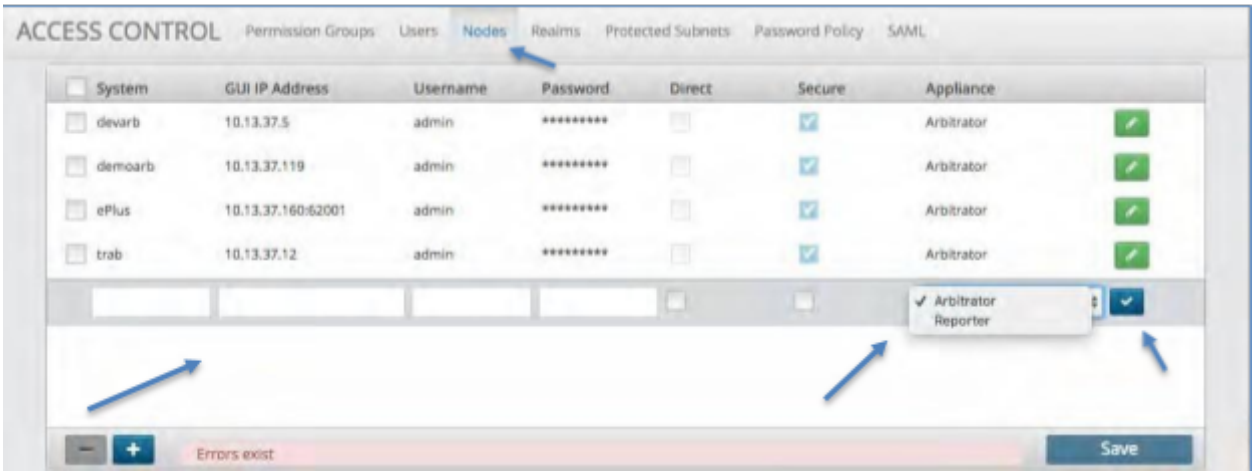
### Nodes

The Nodes tab allows you to create a new Arbitrator Correlation or Dashboard/Reporting node. Once it is added and saved then the node can be added to a Realm with other nodes.

### Creating a Node

To create a Node:

1. Click the Node tab at the top of the screen next to Users.
2. Click the blue plus icon at the bottom of the screen.
3. Fill in the required fields. (System, GUI IP Address, Username and Password).
4. Check the either the Direct box (http) or the Secure box (https) to select the communication method.
5. Select the Appliance drop-down box and choose the type of system you are adding.
6. Click the Blue check icon to set the Node.
7. Click the Save button to save the Node.




### Deleting a Node

To delete a Node:

1. Click the check box next to the Node name that you wish to delete.
2. Click the minus icon at the bottom of the screen.
3. Click the Save button to save your changes.

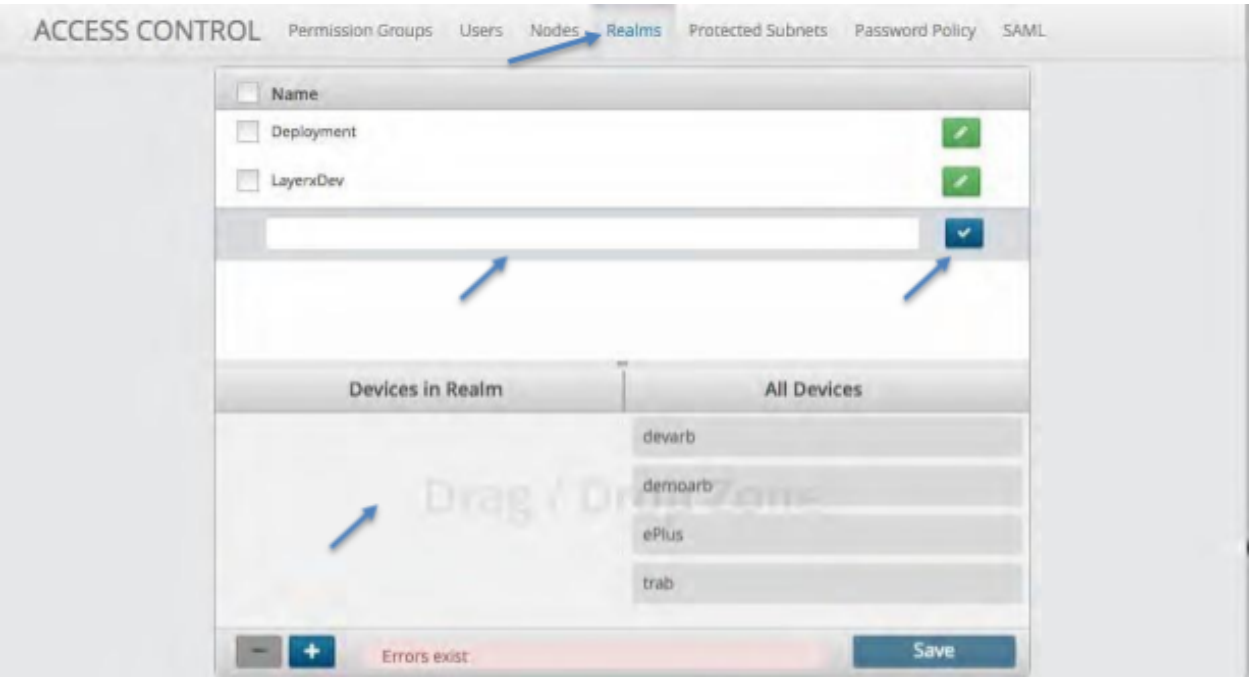
### Realms

The Realm tab allows you to create a new Realm where VOSS Insights systems can be grouped to communicate with each other. Once it is added and saved then Nodes can be added to the Realm.

### Creating a Realm

To create a Realm:

1. Click the Realm tab at the top of the screen next to Nodes.
2. Click the blue plus icon at the bottom of the screen.
3. Fill in the Realm name that you desire.
4. Click the Blue check icon to set the Realm.
5. Drag the systems that you want in the Realm into the drop zone.
6. Click the Save button to save the Realm.




### Deleting a Realm

To delete a Realm:

1. Click the check box next to the Realm name that you wish to delete.
2. Click the minus icon at the bottom of the screen.
3. Click the Save button to save your changes.

### Protected Subnets

The Protected Subnets tab allows you to input the IP addresses of subnets that will be protected from a control running against them. The Control will check this list prior to running and will not run a script against a device that is within a protected subnet.

### Creating a Protected Subnet

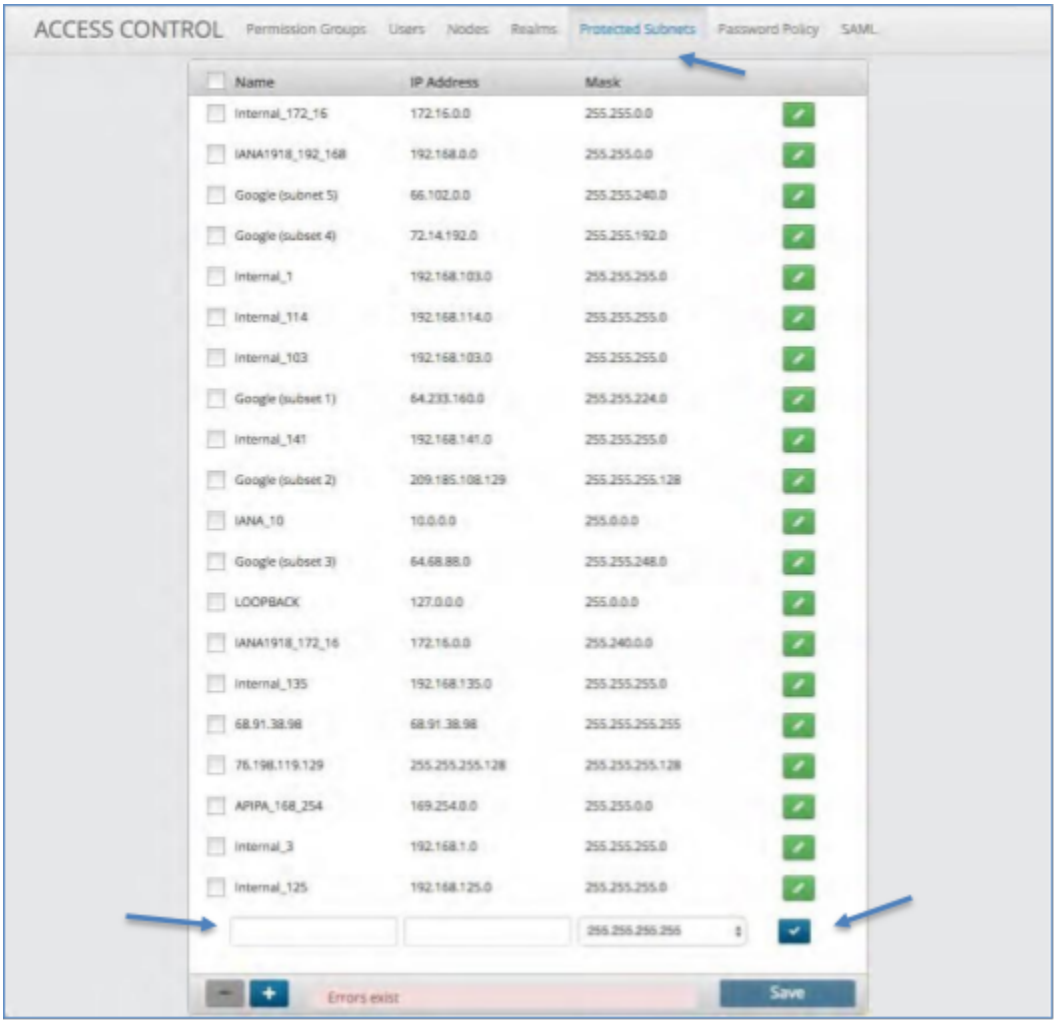
To create a Protected Subnet:

1. Click the Protected Subnet tab at the top of the screen next to Realms.
2. Click the blue plus icon at the bottom of the screen.
3. Fill in the Name, IP Address and Mask of the Protected Subnet.
4. Click the Blue check icon to set the Protected Subnet.
5. Click the Save button to save your changes.

### Deleting a Protected Subnet

To delete a Protected Subnet:

1. Click the check box next to the Protected Subnet name that you wish to delete.
2. Click the minus icon at the bottom of the screen.
3. Click the Save button to save your changes.



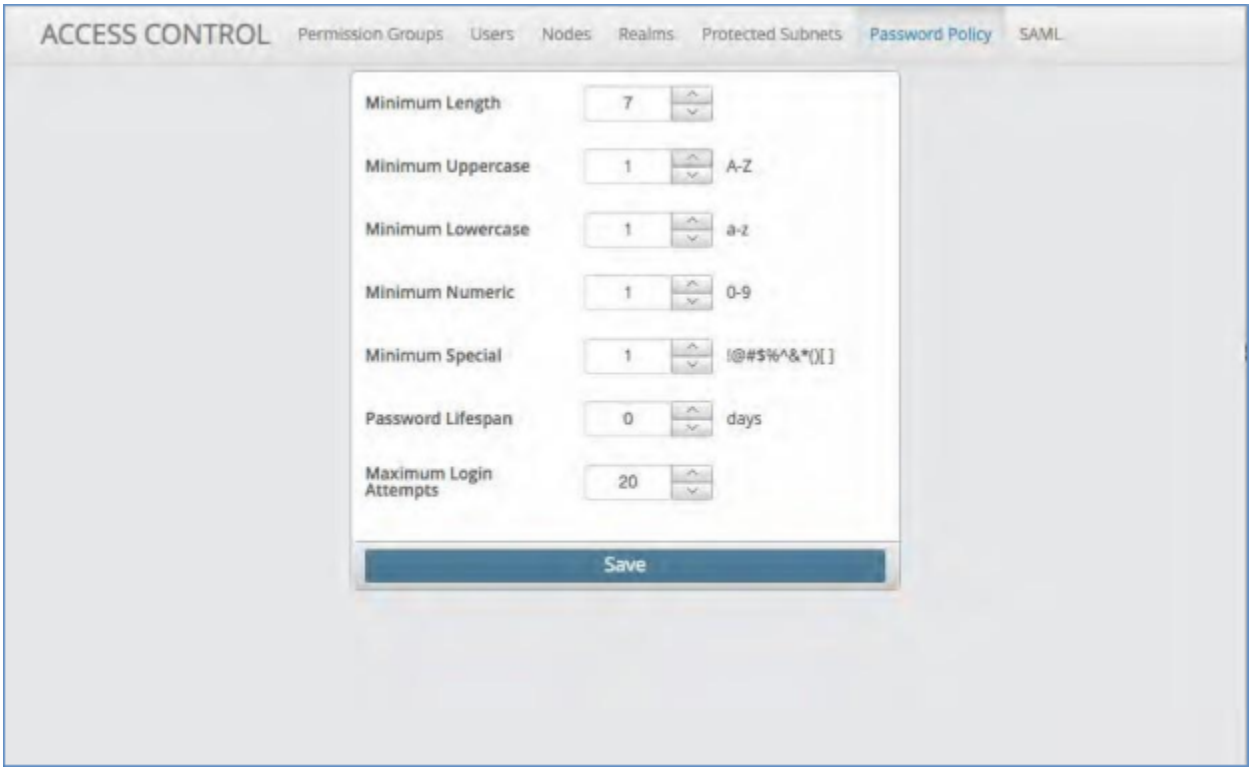

### Password Policy

The Password Policy tab allows you to set and enforce password rules to access the system. Each field is optional thus the user can choose the best policy to enforce.

### Creating a Password Policy

To create a Password Policy:

1. Click the Password Policy tab at the top of the screen next to Protected Subnets.
2. Within the box you have an option of Minimum Length, Minimum Uppercase, Minimum Lowercase, Minimum Numeric, Minimum Special, Password Lifespan and Maximum Login Attempts.
3. Fill in the desired inputs into each of these fields.
4. Click the Save button to save your changes.




### SAML

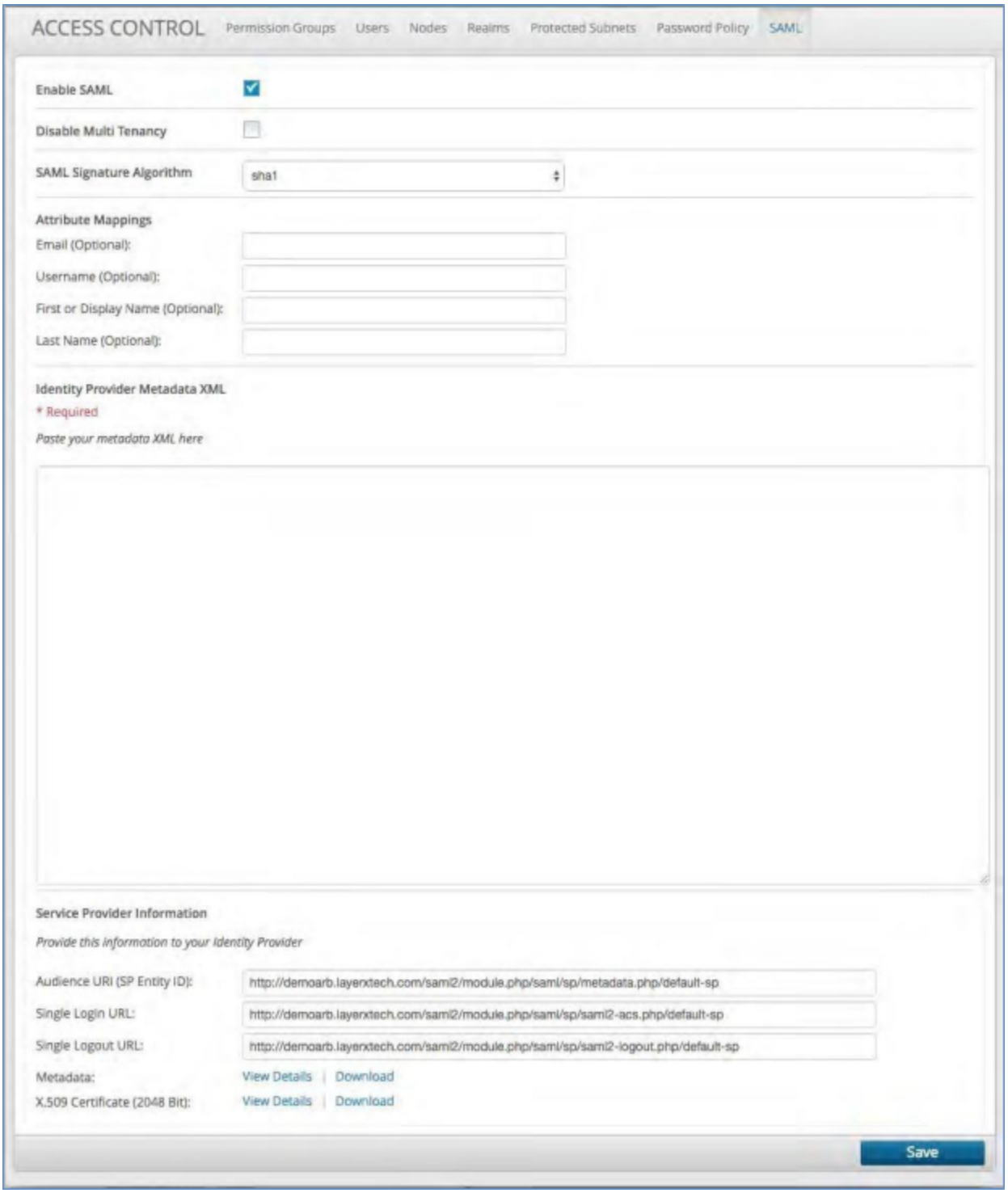
The SAML tab allows you to configure single sign-on to other user management platforms by utilizing the Security Assertion Markup Language (SAML). This is an open standard for exchanging authentication and authorization data between systems.

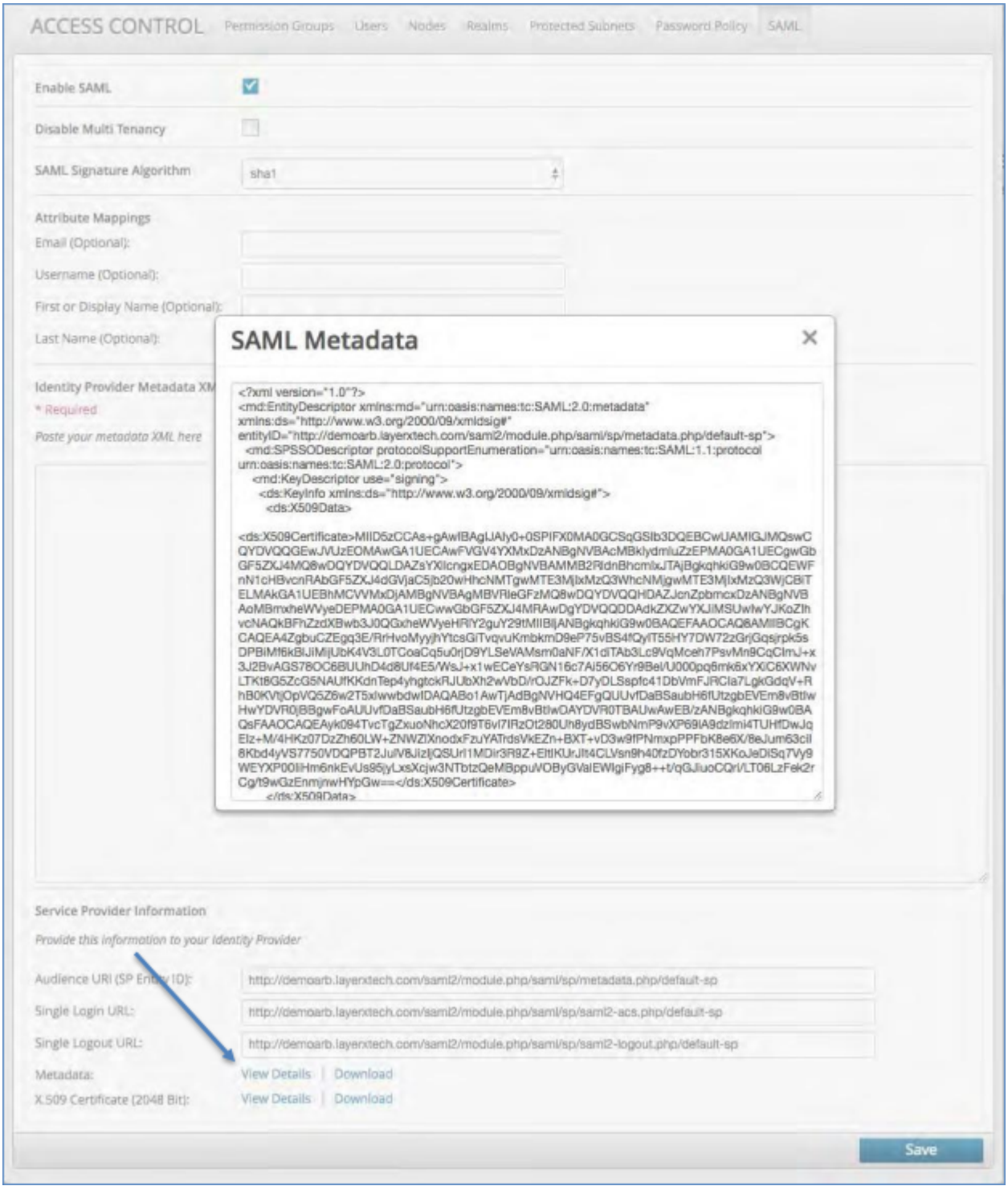
### Creating single sign-on via SAML

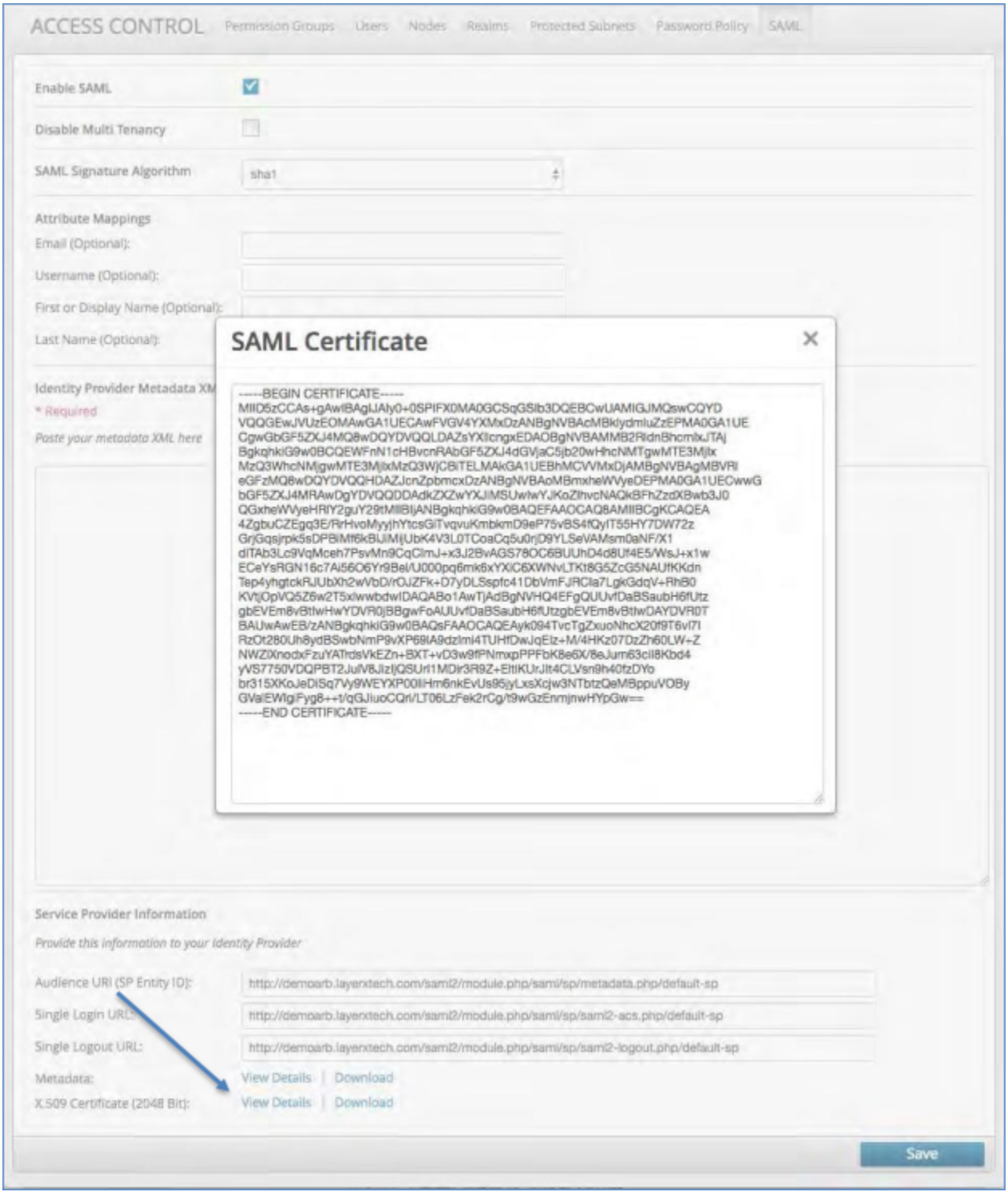
To create single sign-on via SAML:

1. Click the SAML tab at the top of the screen next to Password Policy. The attributes on this page require you to interact with your administrator of allowed users.
2. Click the box next to Enable SAML.
3. If the system is supporting a single customer, then click the Disable Multi-Tenancy.
4. Fill in the optional principal attributes.
5. From your administrator obtain the Identity Provider Metadata XML and paste it into the box provided.
6. From the following boxes provide each of the following to your Identity Provider:
    a. Audience URL (SP Entity ID)
    b. Single Login URL
    c. Single Logout URL
    d. Click to view or download the platform SAML Metadata
    e. Click to view or download the platform X.509 Certificate (2048 Bit)

7. Click the Save button to commit the SAML configuration.
8. (See Figures on the next few pages.)







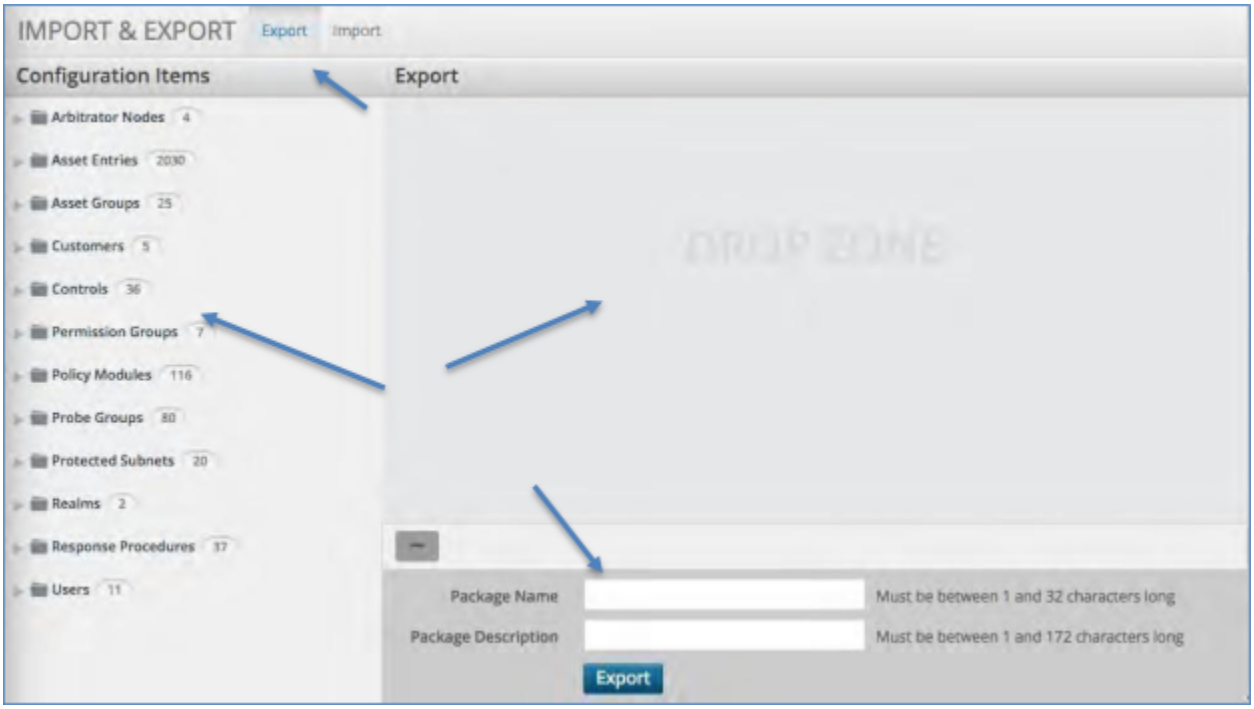
### 4.1.11. Import & Export

The Import & Export Configuration panel allows you to select all or parts of the system configuration to be exported to file or to import already exported files into the system.

#### Exporting

To export configuration items:

1. Click the Export tab at the top of the screen.
2. On the left-hand side will be folders containing all of the configuration items. Either drag whole folders over to the drop zone or open a folder and select a specific item to drag to the drop zone.
3. Once complete give the package a name in the box next to Package Name.
4. Then give the package a description in the box next to Package Description.
5. When complete click the Export button.
6. The package file will download to your local computer.

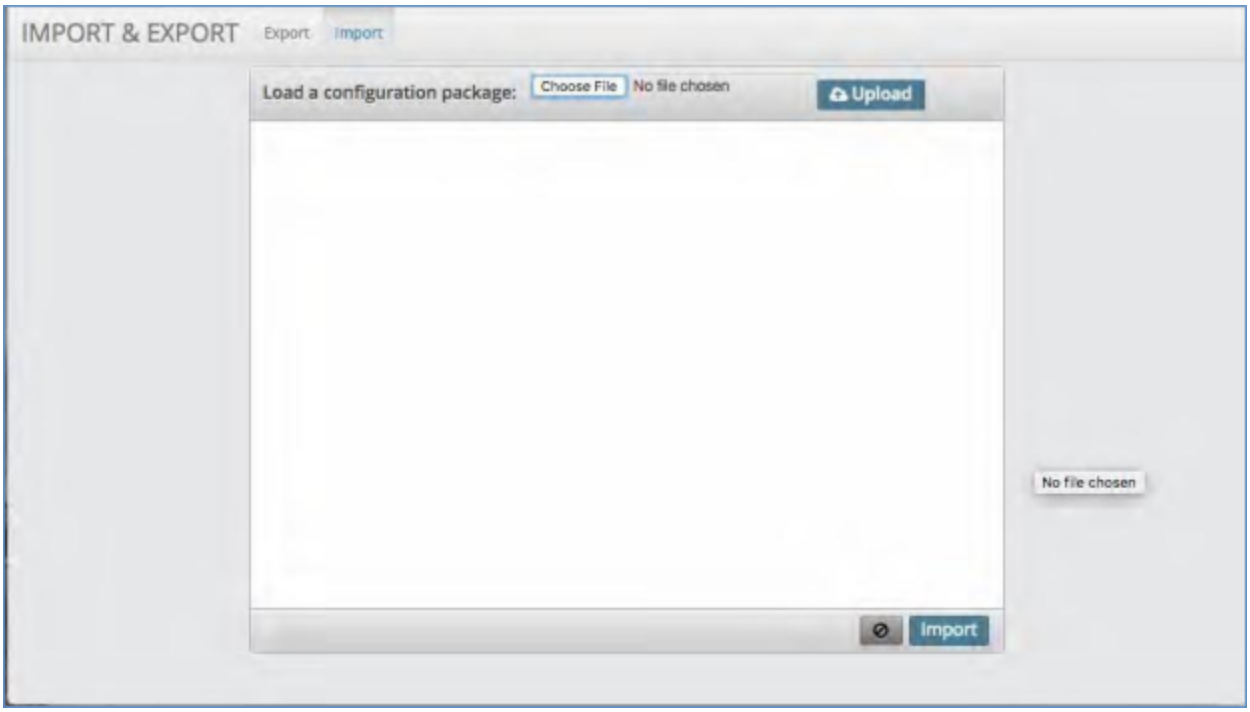



#### Importing

To import configuration items:

1. Click the Import tab at the top of the screen.
2. Select the file you wish to import by clicking the “choose file” button. This will open up your local file system to select the file from where you have it stored on your computer.
3. Double click the file or highlight it and click “Open”.
4. Click the Upload button. This will open up all of the configuration items you are importing.

5. Make any changes to the settings as required.
6. Click Import.
7. A progress screen will pop up. Once complete click OK.

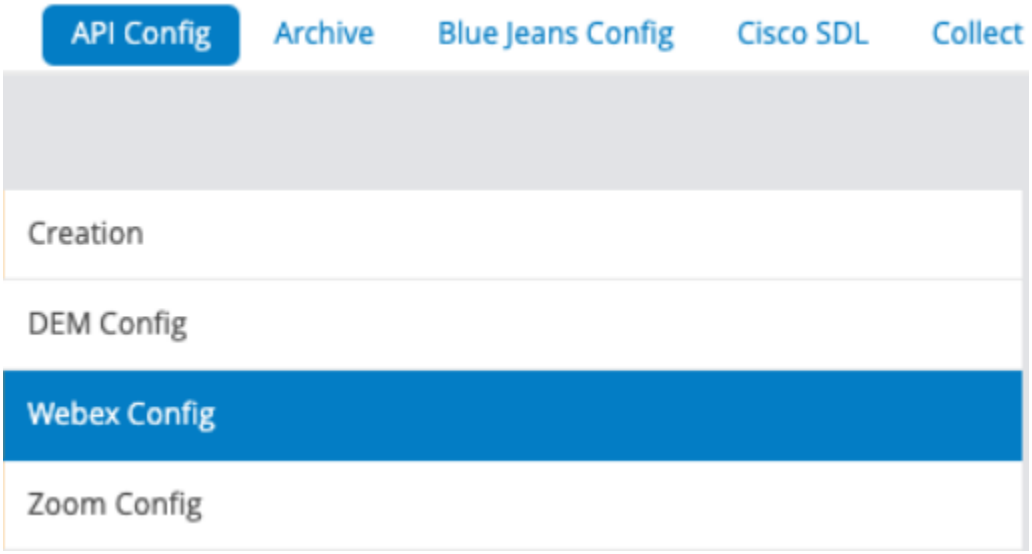



### 4.1.12. Archive Management

The Archive Management panel provides options on backing up the Arbitrator Correlation platform.

A number of API configurations to enable monitoring can be configured.

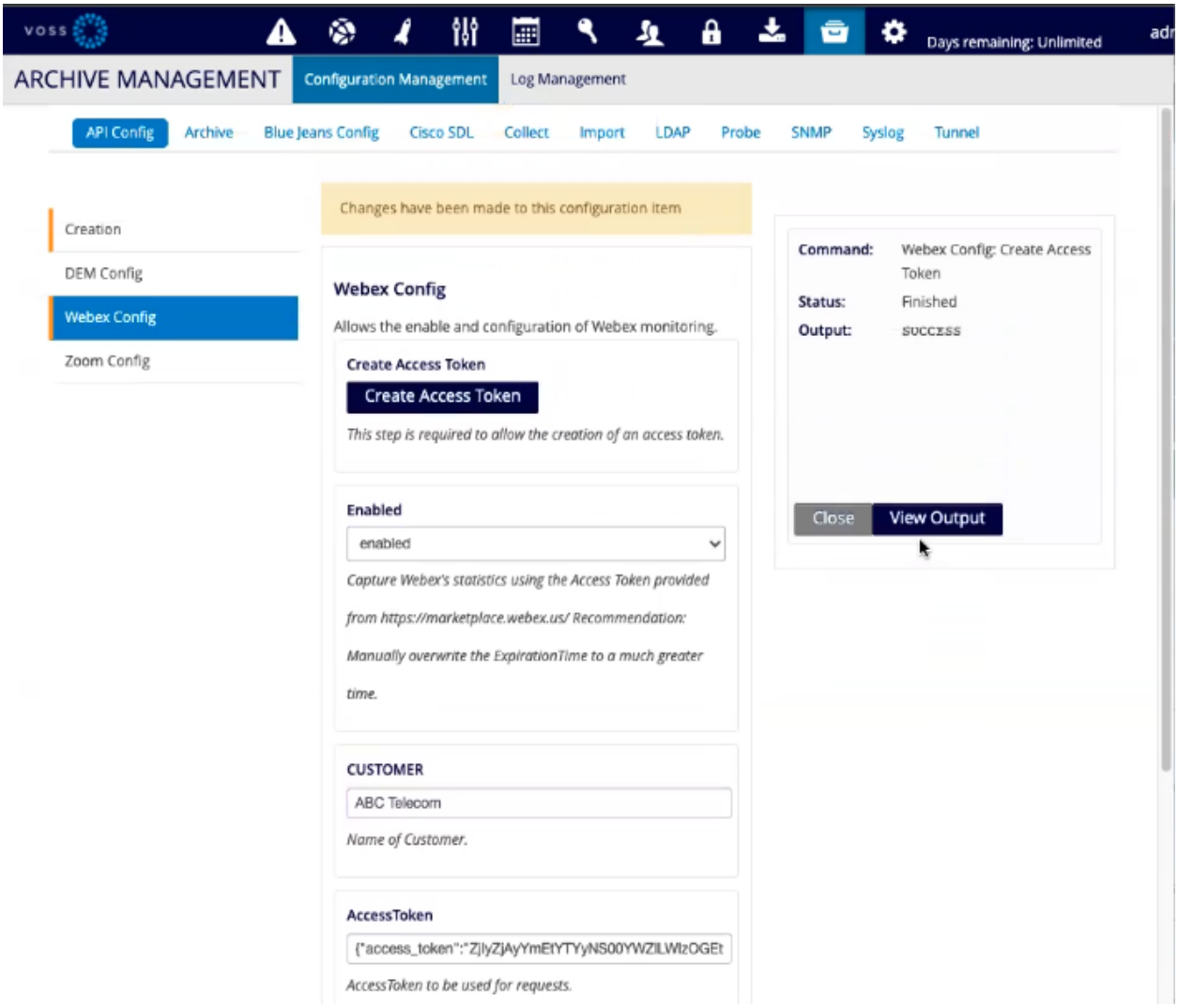
From SP25, **Webex Config** is available to enable the configuration of Webex monitoring. (Requires Dashboard SP66 Release for visualization)




**Note:** For Webex API support, your network should be configured to access: `https://webexapis.com/v1`, port 443. (Admin menu > LayerX Network Configuration, **DNS Settings** may need to be configured to reach the external site.)

### Webex API Configuration Steps

1. From the main landing page, select the **System Configuration** (wrench/spanner), which opens a new tab.
2. On the new tab, select **Archive Management** (file cabinet).
3. Go to **Configuration Management > API Config > Webex Config** to fill in the settings:
    a. Click the **Create Access Token** button, enter your account credentials and copy the JSON string which performs OAuth handshake with Webex.
    b. Set **Enabled** to `enabled`.
    c. At **CUSTOMER** enter the Customer Name (if multi-tenancy is required)
    d. At **AccessToken** paste the copied JSON token from step a.
    e. Click **Verify Access Token** and to verify, inspect the output in **View Output**.
    f. Click **Save Access Token**, which will create a new Customer-specific “Webex Config - <XYZ>” entry. under the **API Config** list. (You need to click away and return to **Configuration Management** to reload with the new entry.)




Created configurations can be deleted or modified. This will be needed for Access Tokens, as these contain an `expires_in` value.

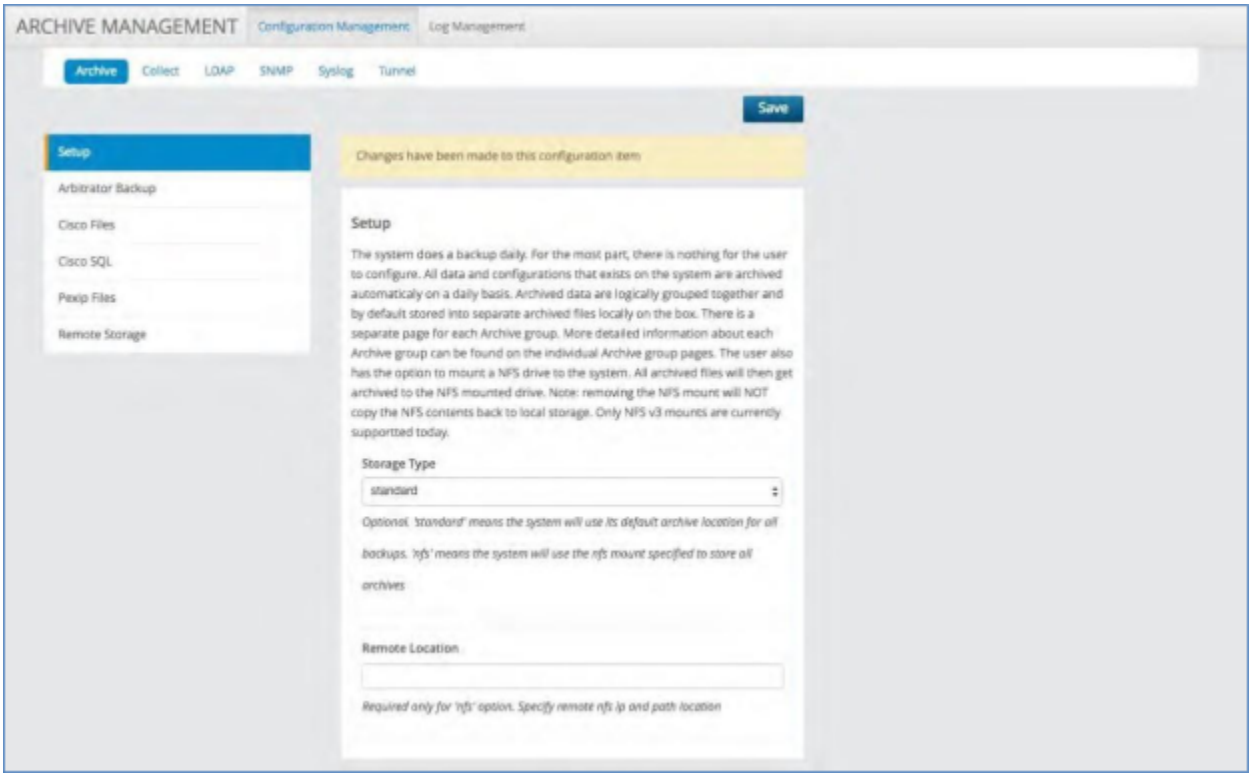
### Archive

Under the Archive tab there are a few options based on the specific functions the user wants to backup.

### Setup

The system does a backup daily. For the most part, there is nothing for the user to configure. All data and configurations that exists on the system are archived automatically on a daily basis.

Archived data are logically grouped together and by default stored into separate archived files locally on the box. There is a separate page for each Archive group. More detailed information about each Archive group can be found on the individual Archive group pages. The user also has the option to mount an NFS drive to the system. All archived files will then get archived to the NFS mounted drive. Note: removing the NFS mount will NOT copy the NFS contents back to local storage. Only NFS v3 mounts are currently supported today.

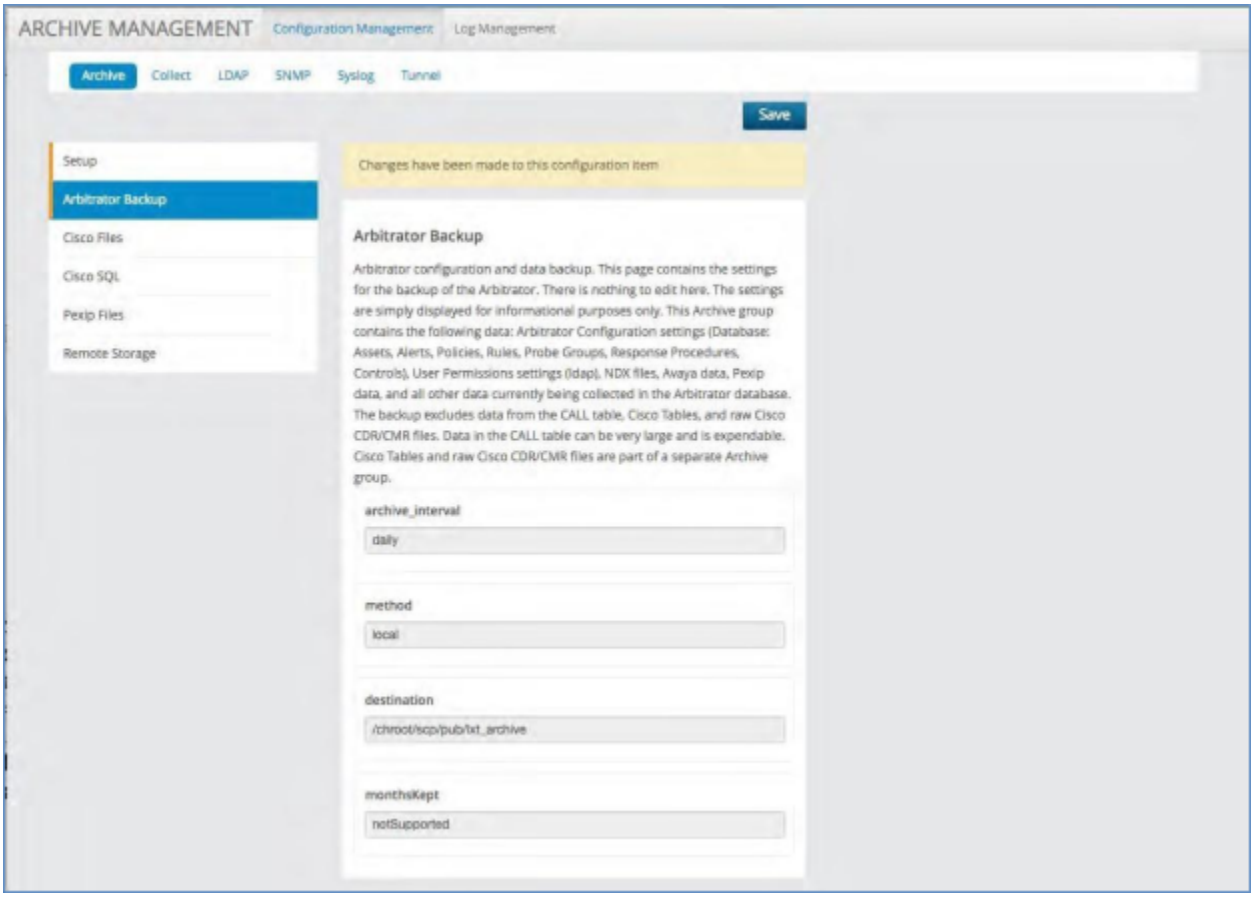



### Arbitrator Backup

This page contains the settings for the backup of the Arbitrator. There is nothing to edit here. The settings are simply displayed for informational purposes only. This Archive group contains the following data: Arbitrator Configuration settings (Database: Assets, Alerts, Policies, Rules, Probe Groups, Response Procedures, Controls), User Permissions settings

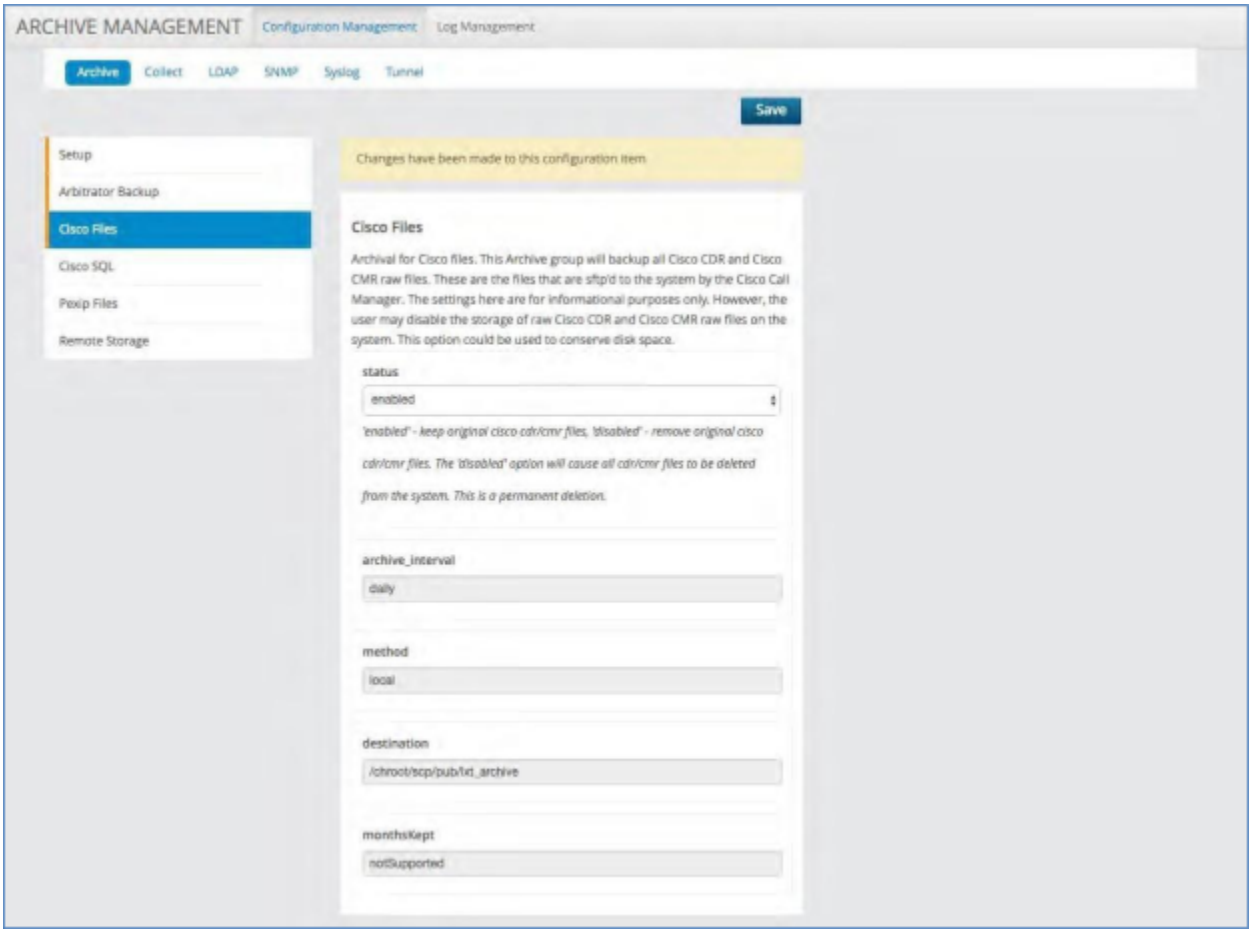
(ldap), NDX files, Avaya data, Pexip data, and all other data currently being collected in the Arbitrator database.

The backup excludes data from the CALL table, Cisco Tables, and raw Cisco CDR/CMR files. Data in the CALL table can be very large and is expendable. Cisco Tables and raw Cisco CDR/CMR files are part of a separate Archive group.



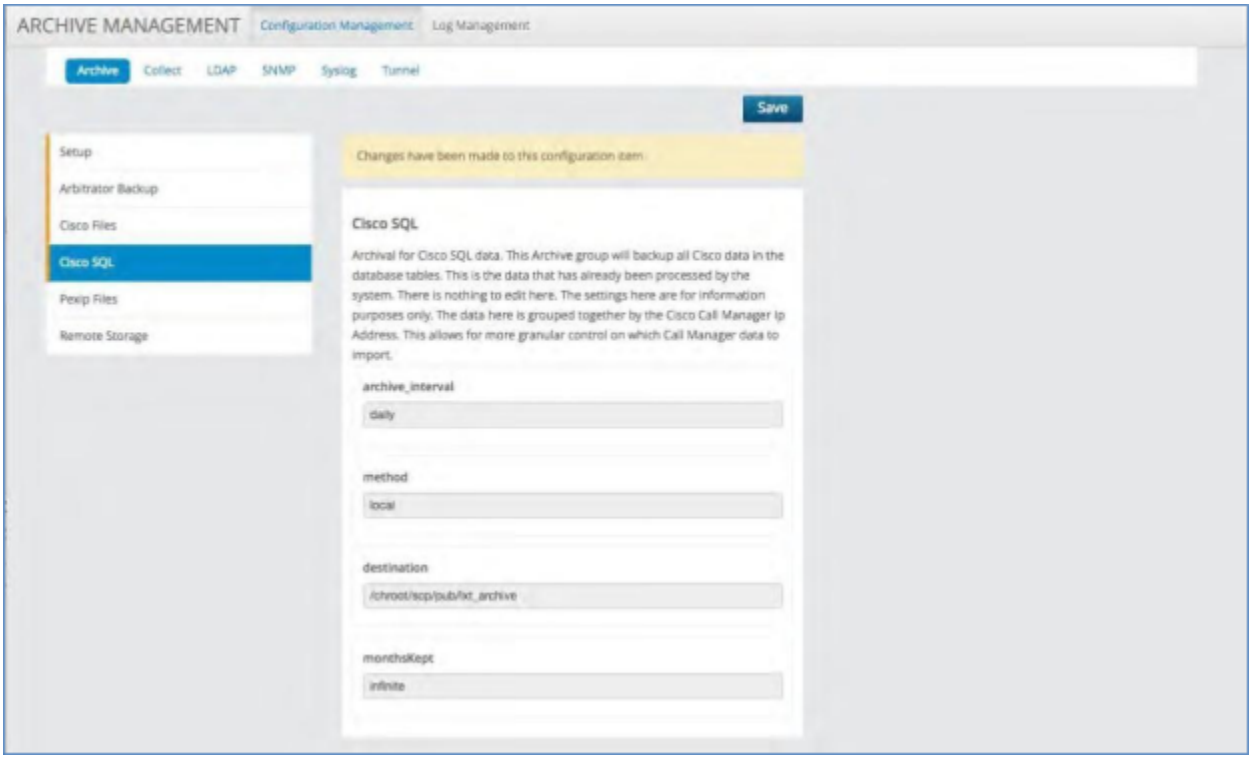

### Cisco Files

Archival for Cisco files. This Archive group will back up all Cisco CDR and Cisco CMR raw files. These are the files that are SFTP'd to the system by the Cisco Call Manager. The settings here are for informational purposes only. However, the user may disable the storage of raw Cisco CDR and Cisco CMR raw files on the system. This option could be used to conserve disk space.



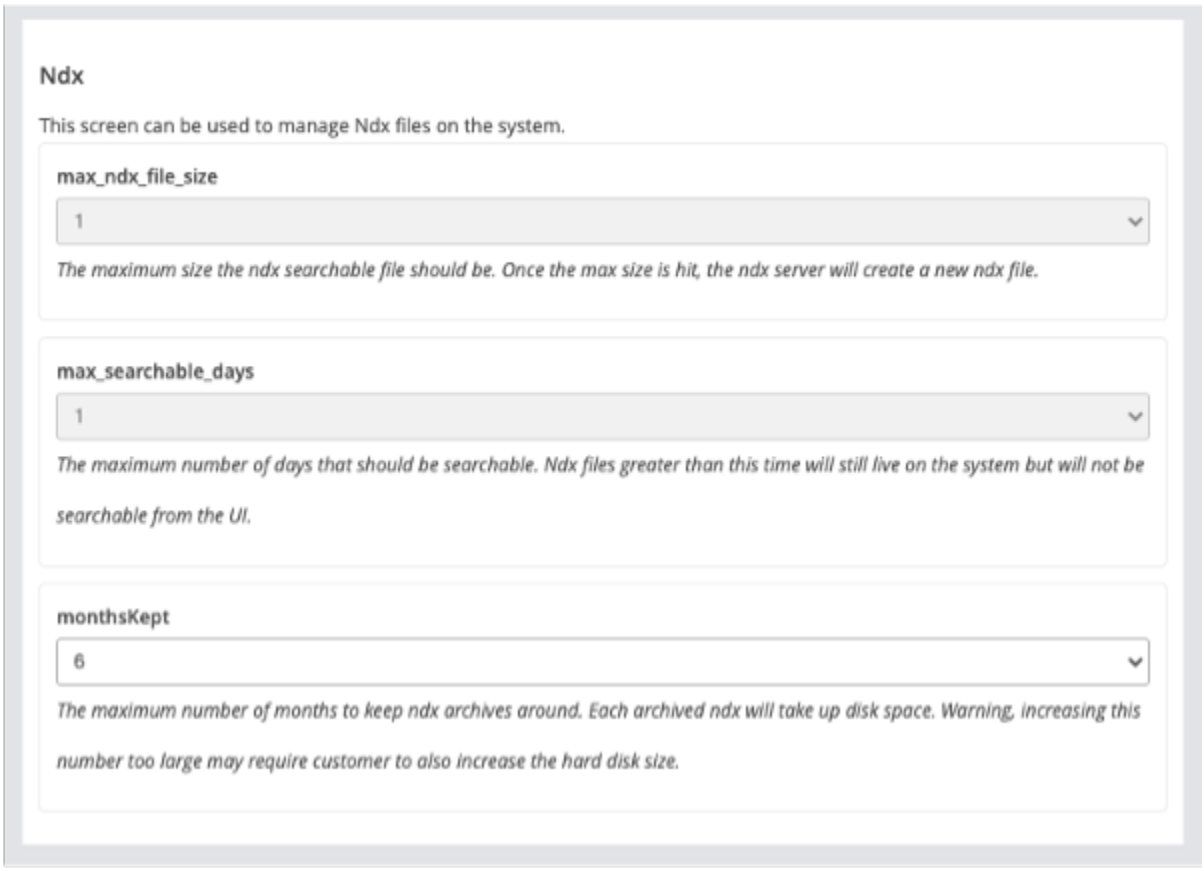

### Cisco SQL

Archival for Cisco SQL data. This Archive group will back up all Cisco data in the database tables. This is the data that has already been processed by the system. There is nothing to edit here. The settings here are for information purposes only. The data here is grouped together by the Cisco Call Manager IP Address. This allows for more granular control on which Call Manager data to import.



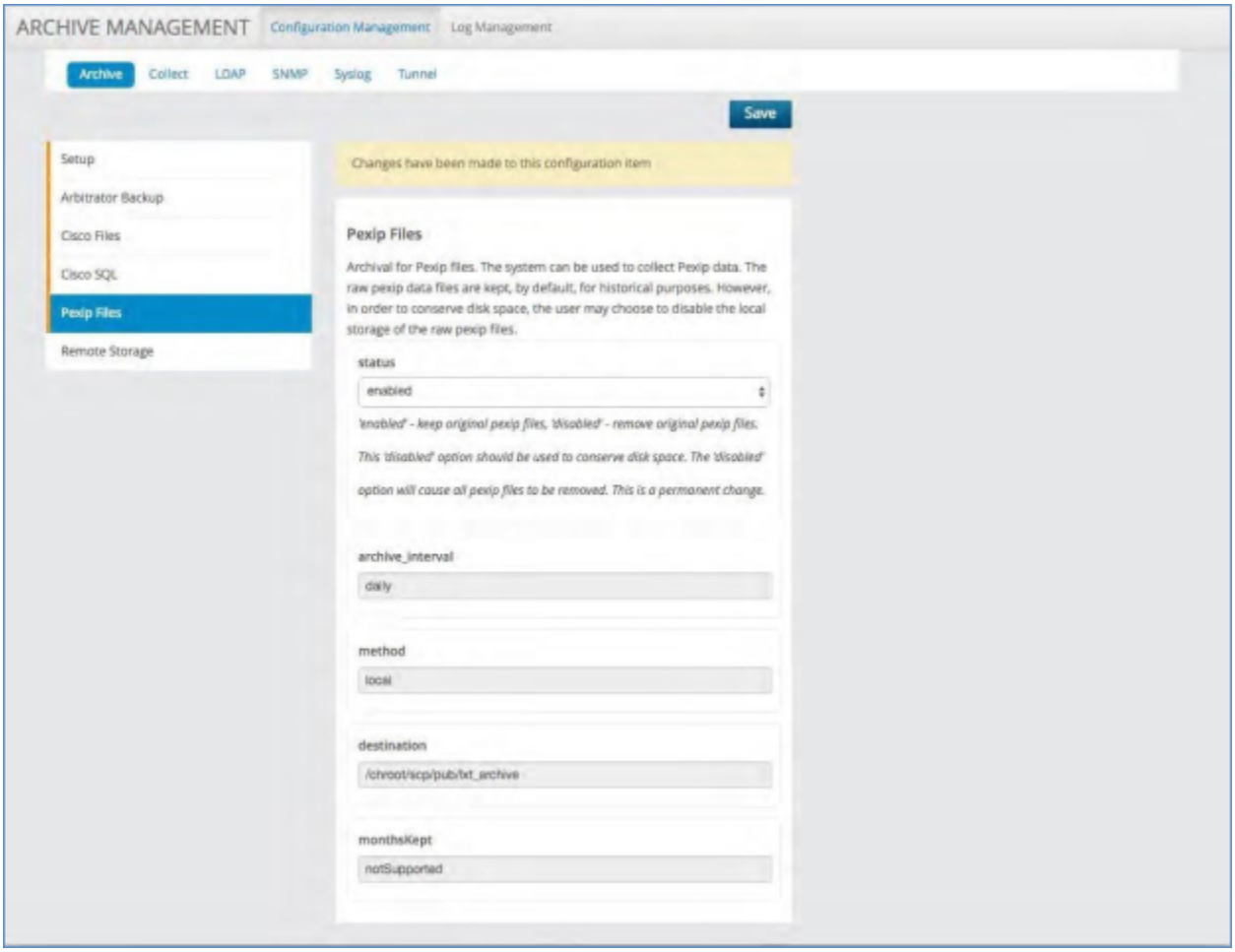

### Ndx

This Archive group will manage Ndx files on the system. Default **monthsKept** is 6 months.




### Pexip Files

Archival for Pexip files. The system can be used to collect PEXIP data. The raw PEXIP data files are kept, by default, for historical purposes. However, in order to conserve disk space, the user may choose to disable the local storage of the raw PEXIP files.




### Remote Storage

If standard / local storage is chosen in the Archive Setup page, then this screen allows the user to configure remote archival of the Arbitrator backup files. Each Archive group produces one or many archive files. The system can be configured to SCP these archive files to a backup location or to another Arbitrator.

The archives can be sent to a separate backup location (NFS, SFTP-server, SCP or remote synced to another Arbitrator).

- **archive_interval**

  This can be set on a schedule of:

  i. Daily

  ii. Weekly

  iii. Monthly

- Method: **Select an option**
  - **disable** - System will reset storage options, e.g. archives locations are reset to the local system if these were previously on a remote host.
  - **nfs** - System will mount the filesystem as a local drive. The system `drop/lxt_archive` directory is linked with a symbolic link to `/mnt/nfsshare` on a host, thereby saving space on the system.

Selecting this option enables additional controls:


  * **Check NFS Host**: Click and use the **View Output** button to see verification output.
  * **Check NFS Mount**: Check the **destination** location (entered below) *after* saving the configuration. **View Output** shows disk usage on the destination of the NFS host.

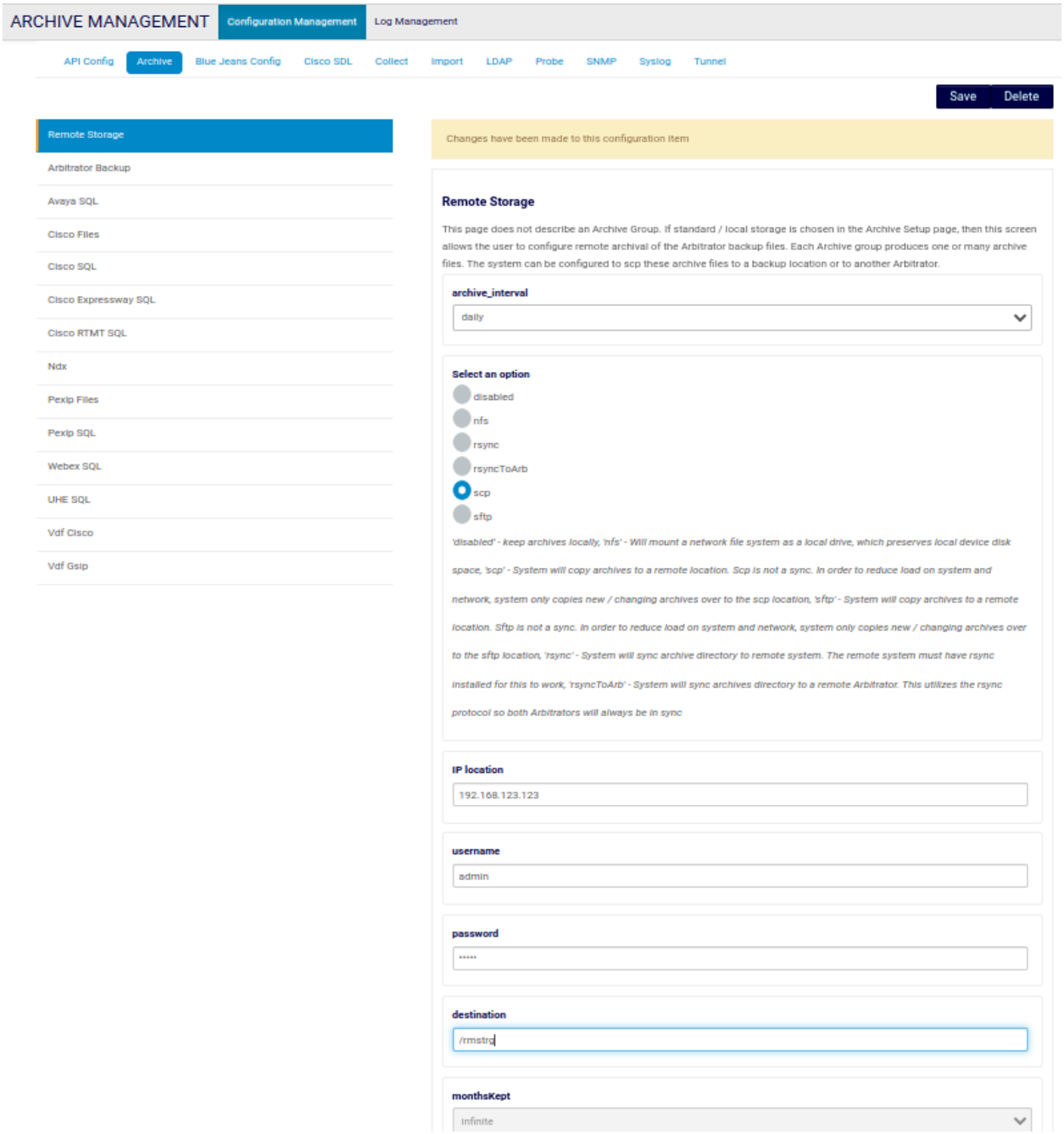
- **rsync** - System will sync the archive directory to remote system. The remote system must have rsync installed for this to work.
- **rsyncToArb** - System will sync the archives directory to a remote Arbitrator. This utilizes the rsync protocol so both Arbitrators will always be in sync.
- **scp** - System will copy archives to a remote location. Scp is not a sync. To reduce load on system and network, system only copies new / changing archives over to the scp location.
- **sftp** - System will copy archives to a remote location. Sftp is not a sync. To reduce load on system and network, system only copies new / changing archives over to the sftp location.

- **IP location**

  IP address. Also add **username** and **password**.

- **destination**

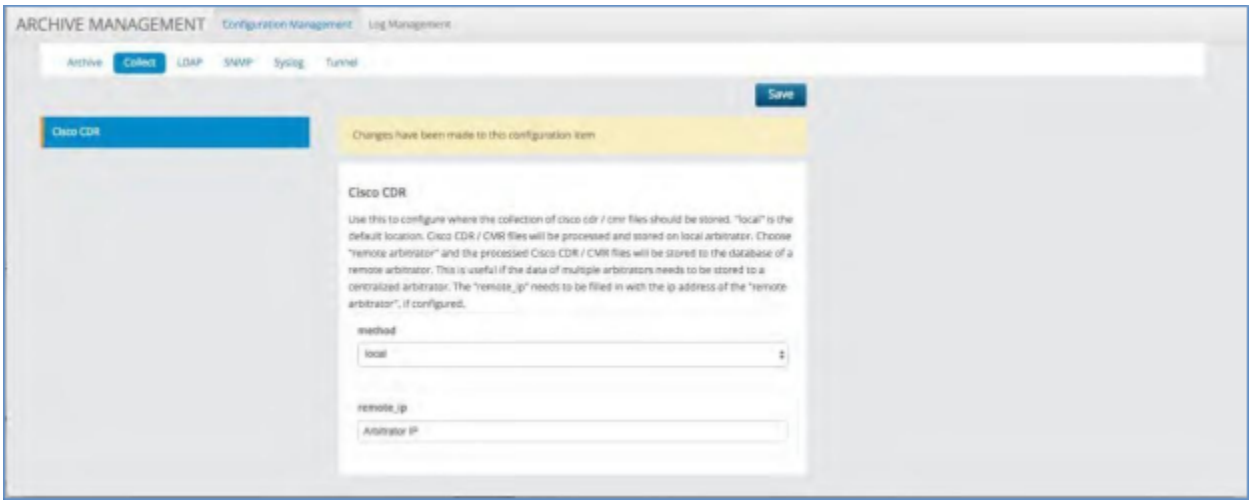
  The path on the remote server to the folder where backups are to be stored.




See also: *Backup and Restore the Arbitrator*.

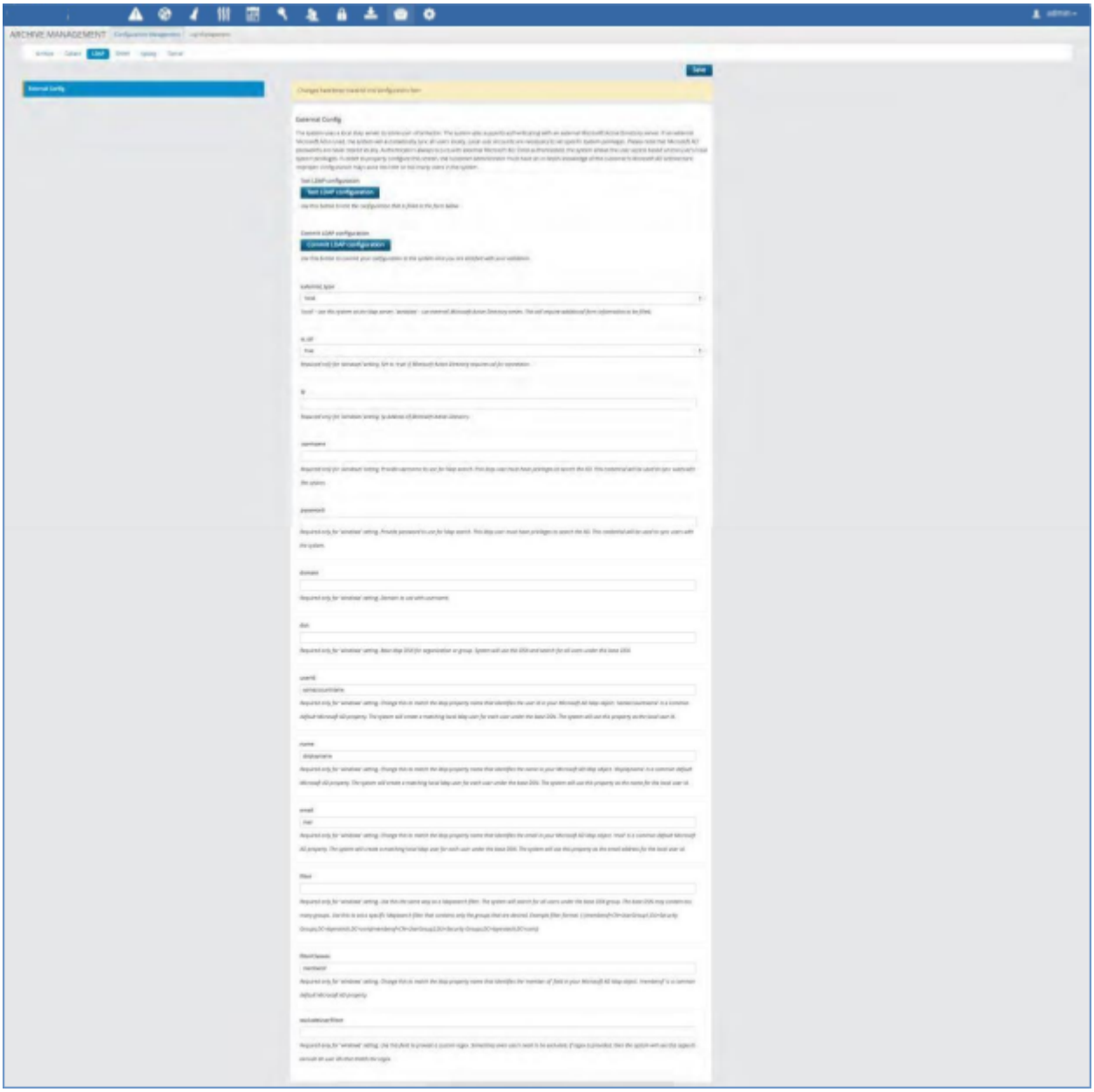
### Collect

The Collect tab allows you to choose where to store Cisco CDR/CMR files. Use this section to configure where the collection of Cisco CDR/CMR files should be stored. “local” is the default location and will be the local Arbitrator Correlation platform. Choose “remote arbitrator” and the processed Cisco CDR/CMR files will be stored to the database of a remote arbitrator. This is useful if the data of multiple arbitrators needs to be stored to a centralized arbitrator. The “remote_ip” needs to be filled in with the ip address of the “remote arbitrator”, if configured.



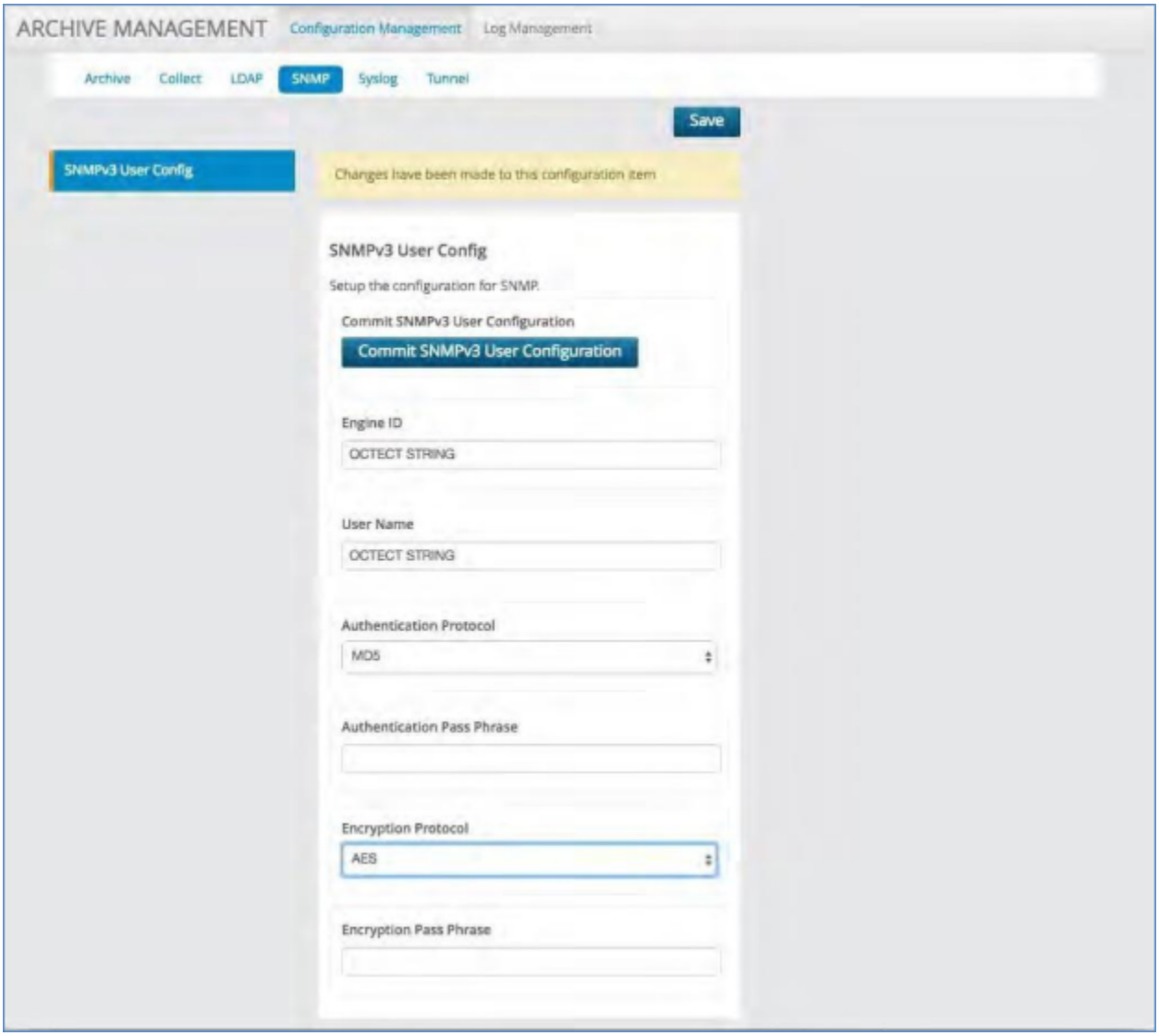

### LDAP External Config

The system uses a local LDAP server to store user information. The system also supports authenticating with an external Microsoft Active Directory server. If an external Microsoft AD is used, the system will automatically sync all users locally. Local user accounts are necessary to set specific system privileges. Please note that Microsoft AD passwords are never stored locally. Authentication always occurs with external Microsoft AD. Once authenticated, the system allows the user access based on the user’s local system privileges. In order to properly configure this screen, the customer administrator must have an in-depth knowledge of the customer’s Microsoft AD architecture. Improper configuration may cause too little or too many users in the system.



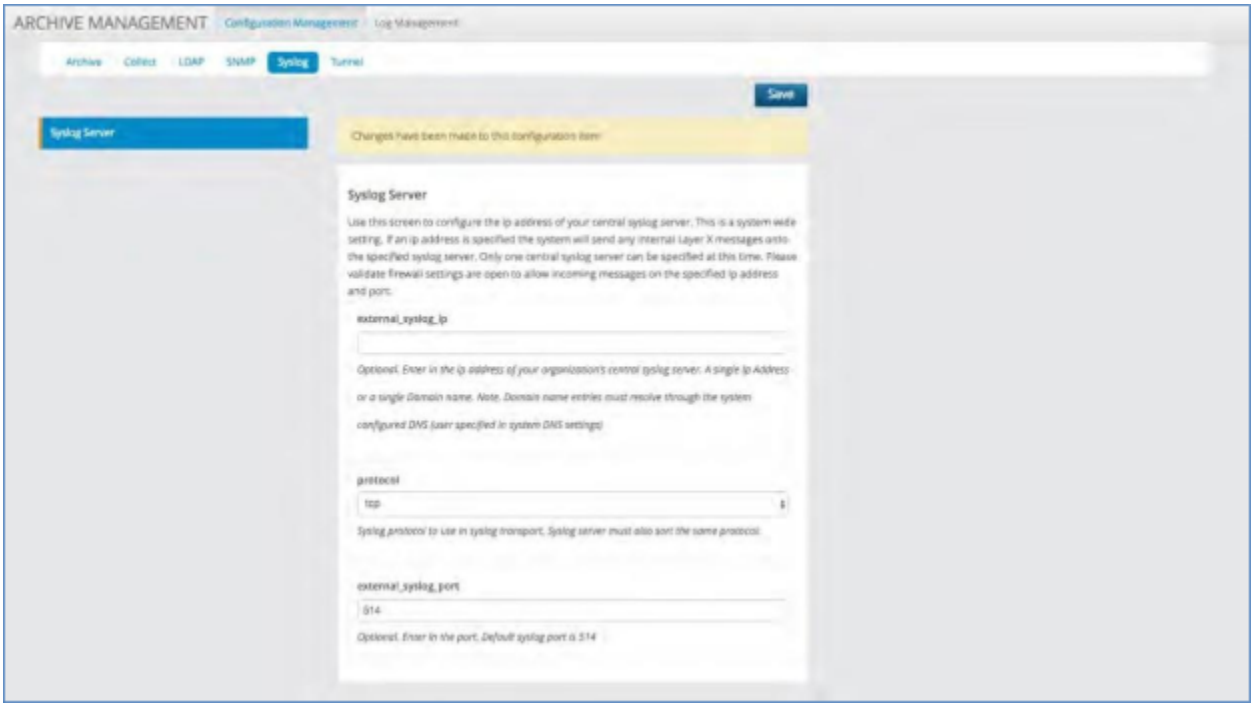
### SNMP V3 User Config

This allows the system to be configured to work with SNMP v3. It allows you to select the specific authentication and encryption methods to be utilized.




### Syslog Server

The system has the ability to send out syslog messages about several of the internal functions including backup and archival success. Use this screen to configure the IP address of your central syslog server. This is a system wide setting. If an IP address is specified, the system will send any internal VOSS Insights messages onto the specified syslog server. Only one central syslog server can be specified at this time. Please validate firewall settings are open to allow incoming messages on the specified IP address and port.

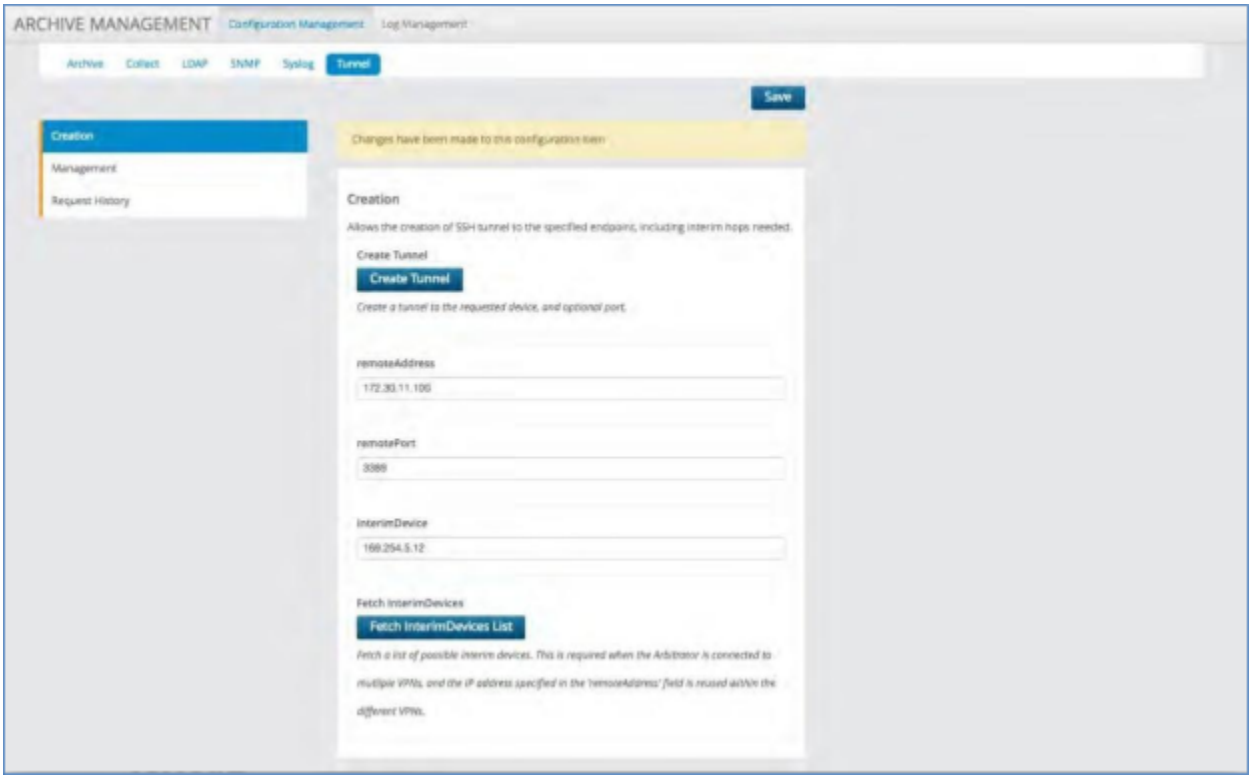



### Tunnel

This tab allows you to go in and create VPN tunnels between Arbitrator Correlation platforms.

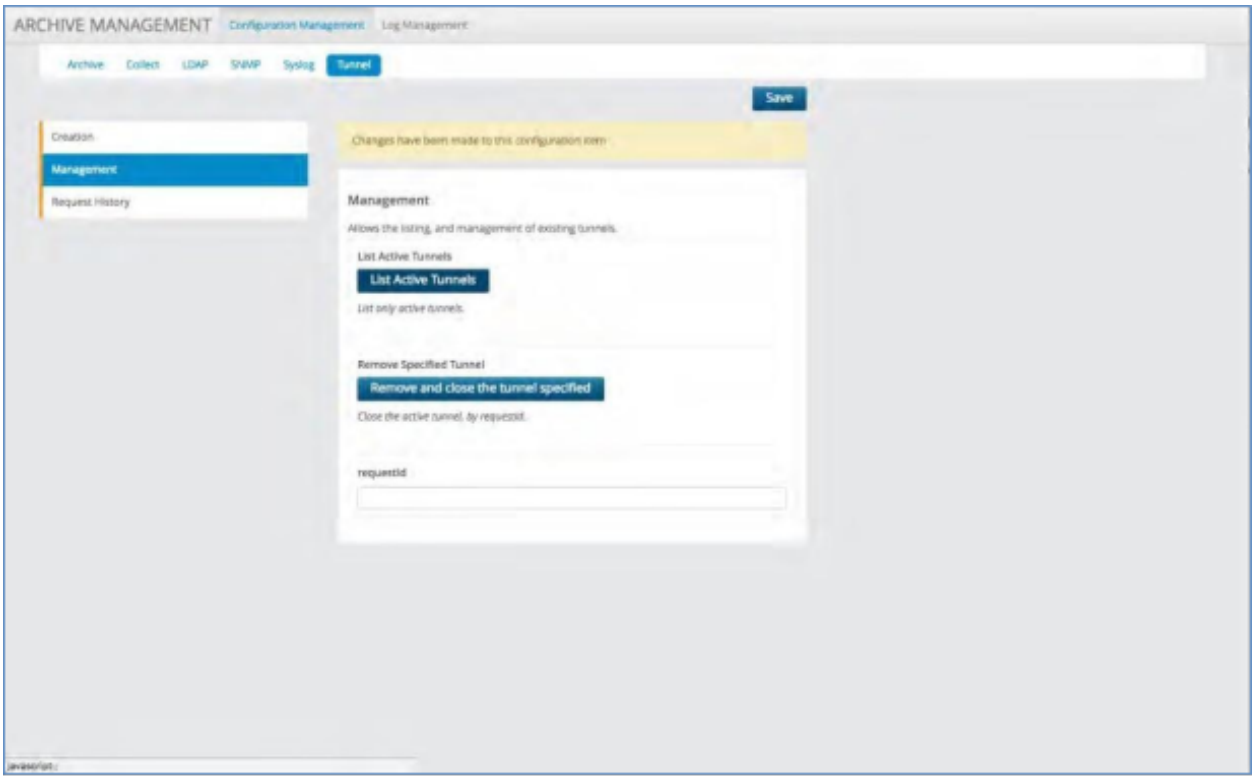
### Creation

Allows the creation of SSH tunnel to the specified endpoint, including the interim hops needed.



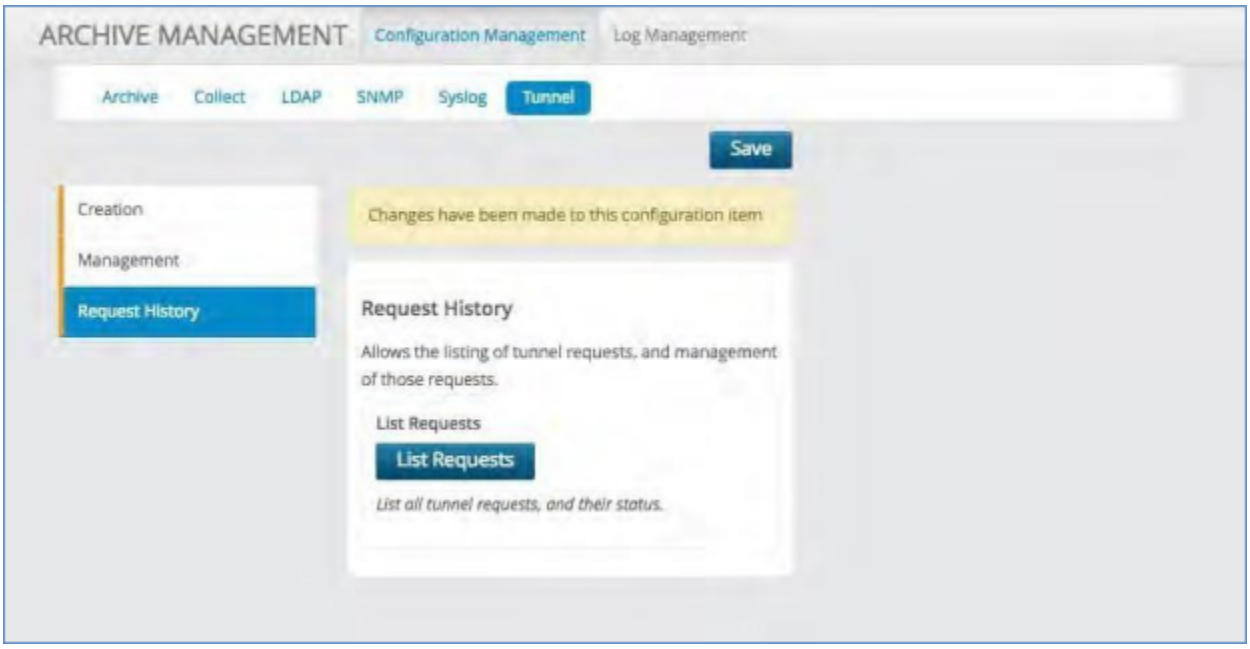

### Management

Use this tab to list and manage all of the existing tunnels.



### Request History

Allows the listing of tunnel requests and management of those requests.

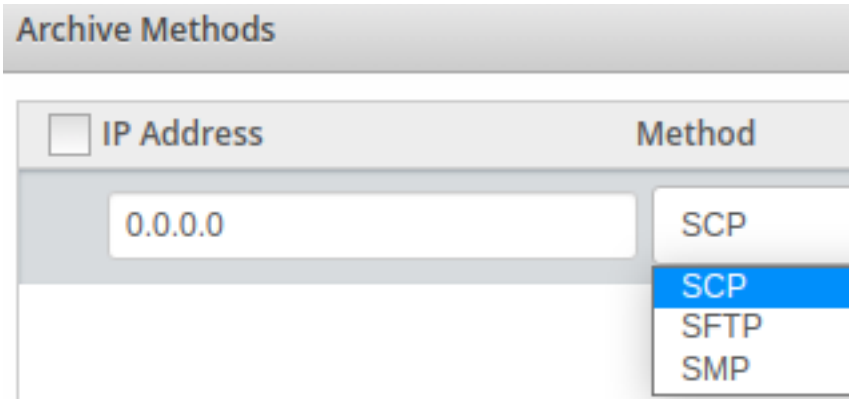


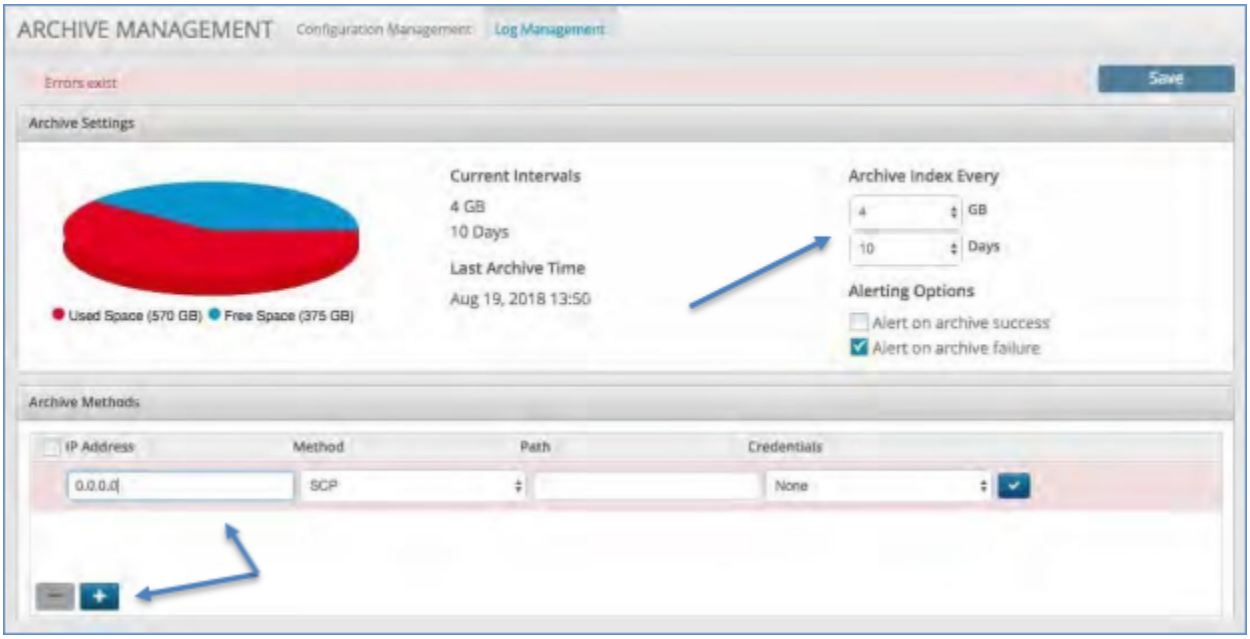

## 4.1.13. Log Management

The Log Management panel allows you to customize the archival of the index data store. It can be performed based on Size, Time or a combination of both.

To set the archival process click on the Log Management tab:

1. Select the file size at which to start the archive.
2. Select the time interval at which to start the archive.
3. Add the location to where the archive file will be sent.
4. Set the **IP Address**, Choose the **Method** of transport (e.g. SFTP), give it a **Path** and input any **Credentials** required.






## 4.1.14. Tools

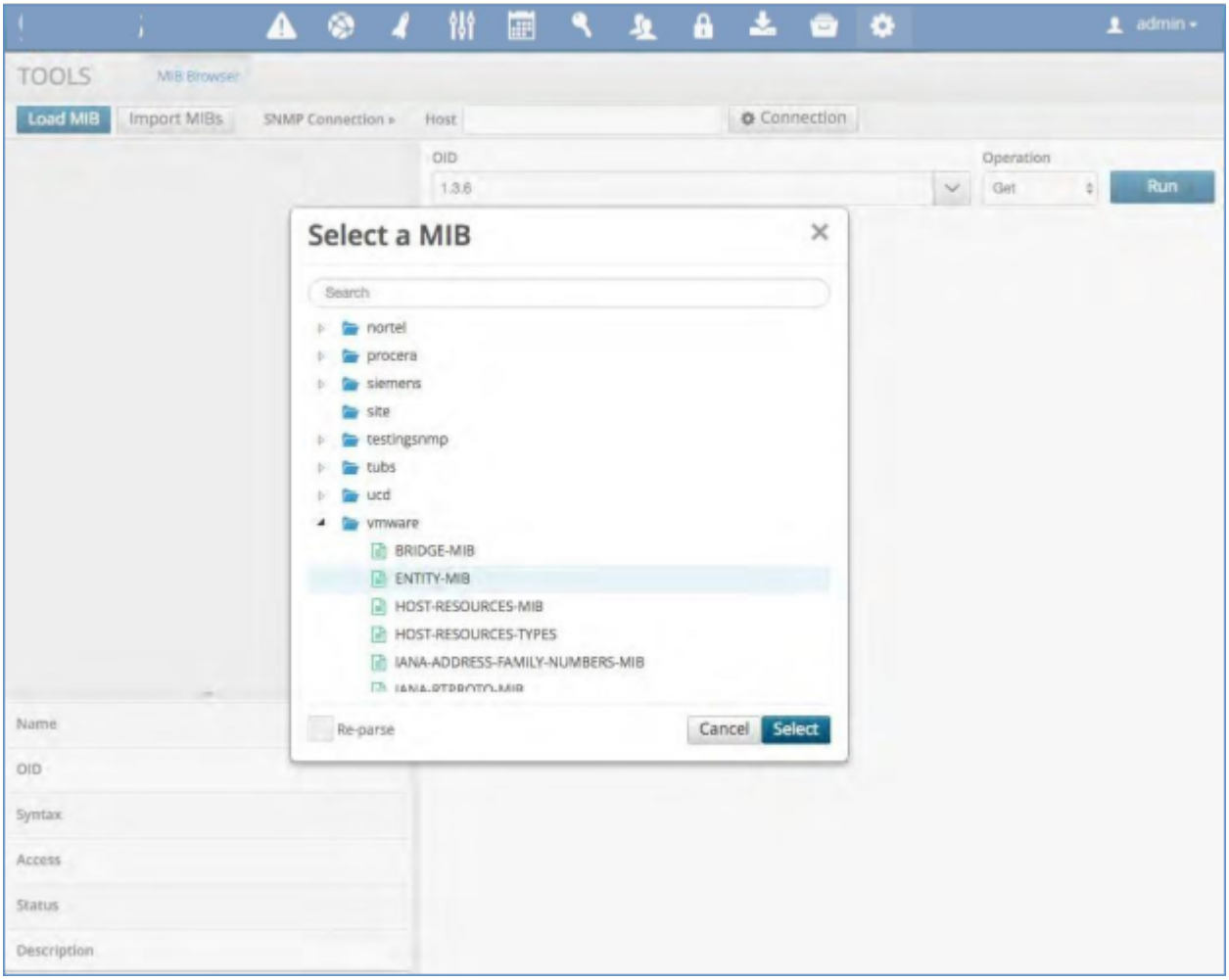
### SNMP Tools

The SNMP Tools panel allows you to very easily load or import MIBs and then build SNMP actions/ scripts to be saved as Probes within the platform. The system comes with a library of MIBs that can be opened by selecting the Load button. If a new one is needed it can be imported by selecting the Import button.

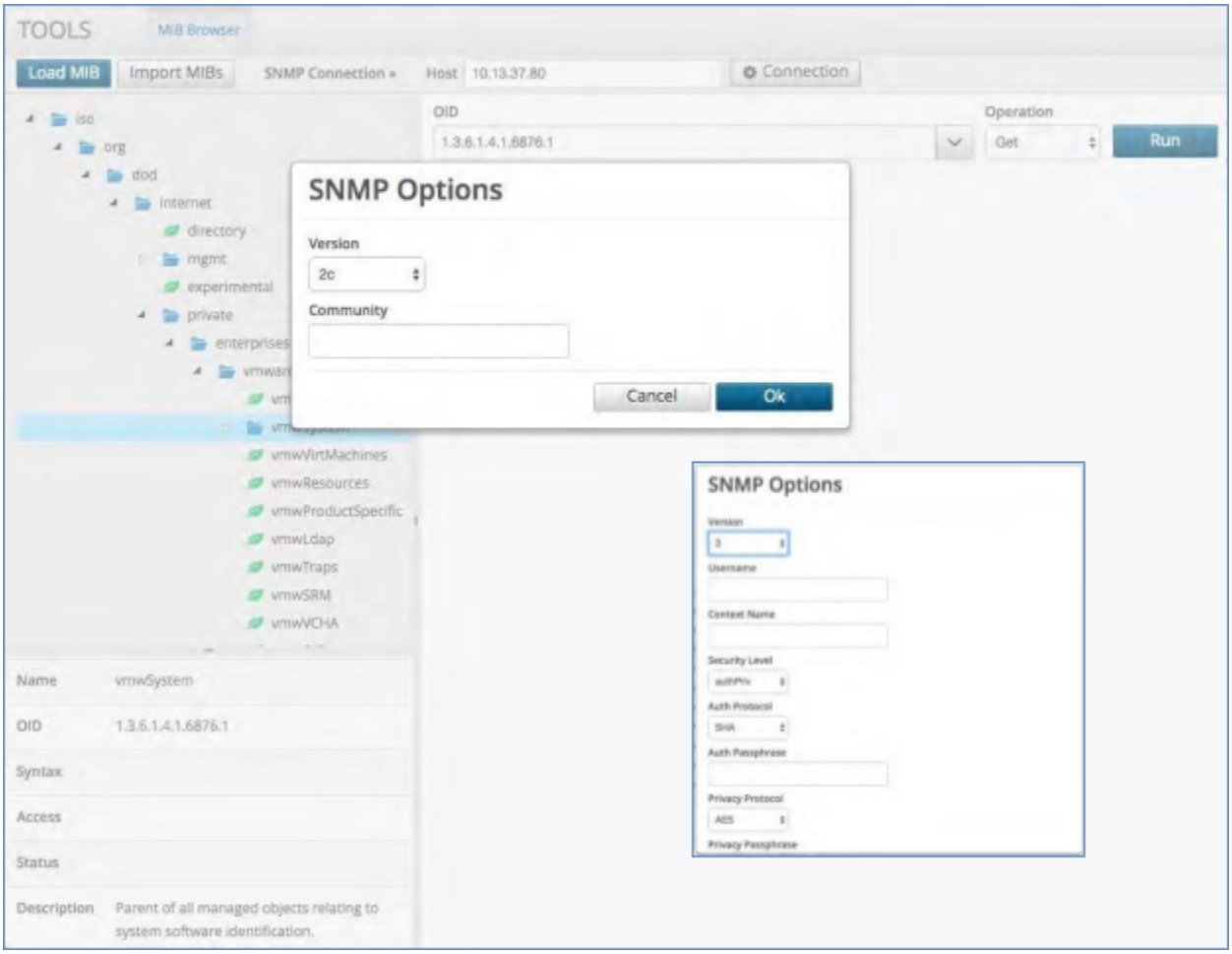
The system comes with a library of MIBs that can be opened by selecting the Load button. Click the Tools Tab:

1. To load an existing MIB simply select the Load button
2. A window will open up with a choice of all the manufacturer MIBs available in the system.
3. Scroll through and select the desired MIB.

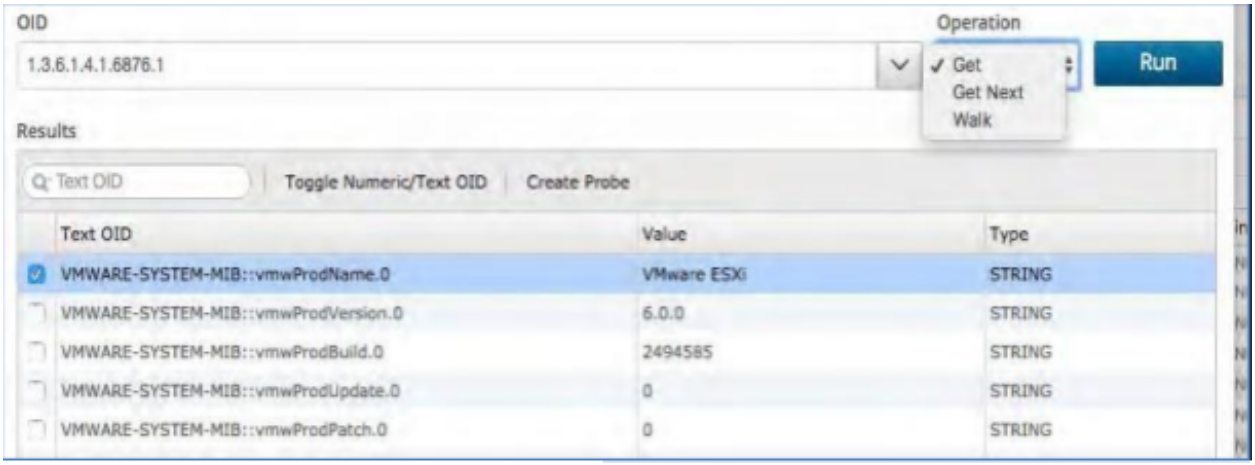
3. Scroll through and select the desired MIB.




4. Once selected you can open up all of the branches and leaves and view each associated OID.
5. Choose the folder you wish to utilize and input the connection settings for that system.
6. Select the Connection button, input the host name or IP and choose the SNMP version. If selecting V3 then a set of different parameters will pop up and you will need to fill these in.




7. Choose the operation to perform: GET, GET NEXT or WALK
8. The operation will return the values of the OID you query in the field below it. Checking any of the boxes beside the field will un-gray the “Create Probe” box.
9. Do this for each Probe you want to create.





10. When you select “Create Probe” a new box will open that will allow you to give the Probe a name and either save it to an existing Probe Group or create a new one.
11. Now you have a new Probe that will run the particular SNMP command you requested.

# 5. Backup and Restore

## 5.1. Backup and Restore the Arbitrator

### 5.1.1. Step 1: Backup

To configure the Arbitrator backup, see *Archive*.

#### Next steps

- Restore

### 5.1.2. Step 2: Restore

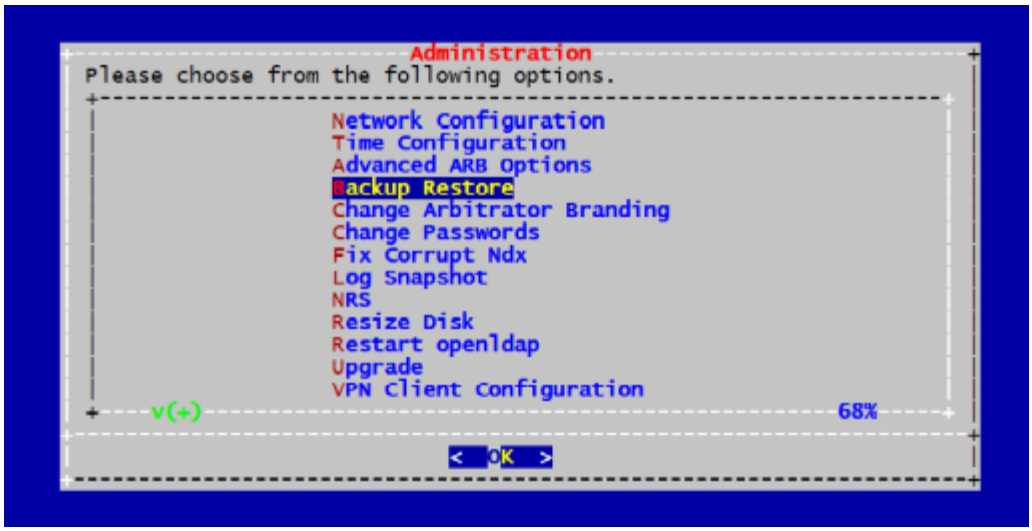
This procedure restores a backup of the Insights Arbitrator.

**Pre-requisites**:

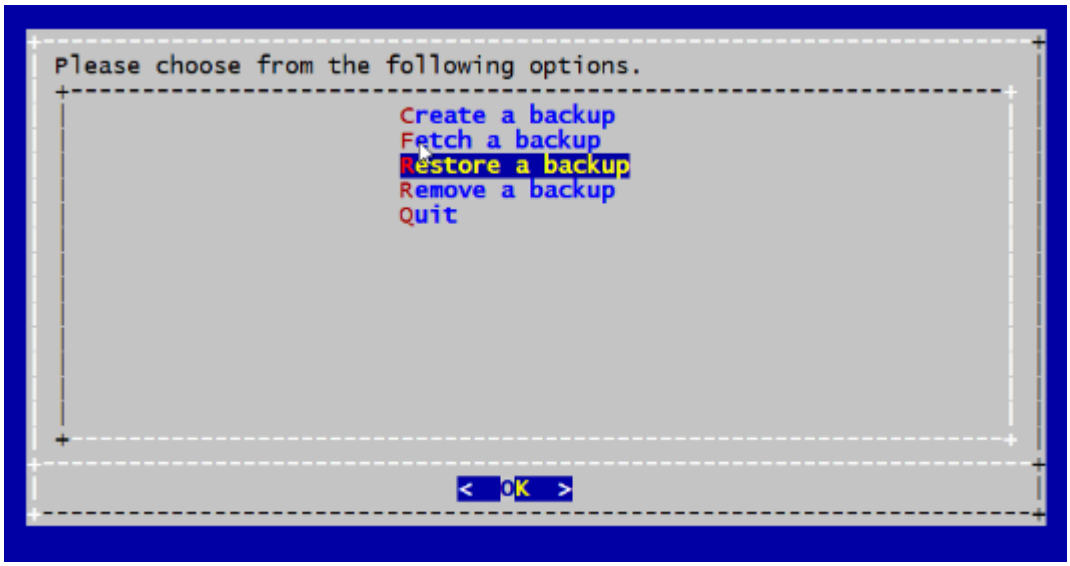
- Backup (see see: *Archive*)

**To restore the Arbitrator application from a backup**:

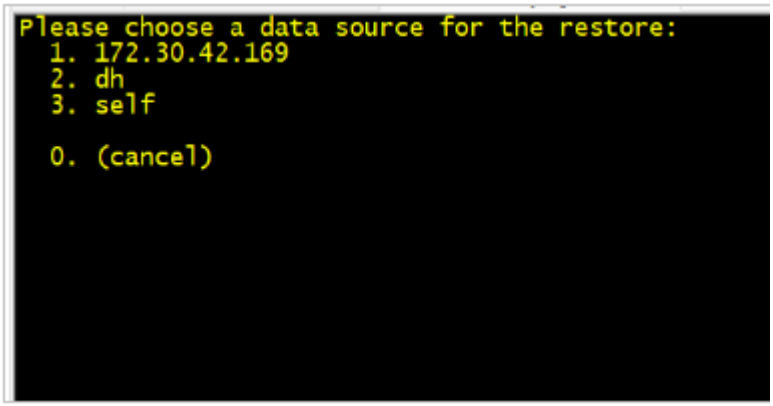
1. Log in to CLI as an admin
2. Go to **Backup Restore** and click **OK**.




3. Navigate to **Restore a backup**.




4. Select the data source of the backup. This will be either `self` - which is stored locally, or a remote location. The example below has `dh` as an sftp server.




5. Select the data types to restore.

```
self
Please choose a data type to restore:
  1. All
  2. Avaya
  3. CISCO
  4. Config
  5. DEM
  6. Identity
  7. NDX
  8. Pexip
  9. Polycom
  10. Themes
  11. UHE
  12. VDF
  13. Webex
  14. Zoom
  15. DBDATA_ONLY

  0. (cancel)
```

6. Select the number of months to restore (0 to 60 or all).

```
self All
self All
How many months of data to restore?  (0..60, all)

  (no number means cancel)
```

7. Confirm the restore.

```
self All 0
Requested data and configurations will be restored.
Existing data and configurations may be replaced/overwritten.
Are you sure you wish to restore the data (y/n)?
```

8. View the system message that confirms the restore is complete.