



VOSS



**VOSS Insights
Arbitrator Administration Guide**

Release 24.1

May 29, 2024

Legal Information

- Copyright © 2024 VisionOSS Limited. All rights reserved.
- This information is confidential. If received in error, it must be returned to VisionOSS ("VOSS"). Copyright in all documents originated by VOSS rests in VOSS. No portion may be reproduced by any process without prior written permission. VOSS does not guarantee that this document is technically correct or complete. VOSS accepts no liability for any loss (however caused) sustained as a result of any error or omission in the document.

DOCUMENT ID: 20240529151311

Contents

- 1 What's New** **1**
 - 1.1 Arbitrator Administration Guide: Release 24.1 1

- 2 Getting Started** **2**
 - 2.1 Welcome to Insights Arbitrator 2
 - 2.2 Arbitrator Licensing 3
 - 2.3 License Auditing 4

- 3 Arbitrator Main Interface** **8**
 - 3.1 Arbitrator Main Interface 8

- 4 Configuration** **31**
 - 4.1 System Configuration 31
 - 4.2 Policy Configuration 32
 - 4.3 Asset Configuration 48
 - 4.4 Probe Configuration 59
 - 4.5 Controls 68
 - 4.6 Response Procedure Configuration 70
 - 4.7 Credential Configuration 77
 - 4.8 Customer Configuration 78
 - 4.9 Access Control 81
 - 4.10 Import & Export 96
 - 4.11 Archive Management 98
 - 4.12 Tools 128

- 5 Arbitrator Maintenance** **132**
 - 5.1 Backup and Restore the Arbitrator 132
 - 5.2 System Recovery 134
 - 5.3 Network Observability 136

1. What's New

1.1. Arbitrator Administration Guide: Release 24.1

- EKB-18816: Some configuration screens should not be accessible to non-admin users, for example, DS9 configuration. See: [Archive Management](#)
Docs updated to indicate the parts of the GUI that are only accessible to admin users.
- EKB-20028: Create API user for VOSS DEM agent. See: [Access Control](#)
Added details on the management of the API user for the VOSS DEM agent.

2. Getting Started

2.1. Welcome to Insights Arbitrator

2.1.1. Overview

Insights Arbitrator (Correlation) is 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:

- Main interface - 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.
- System Configuration - admin users only, this is the workspace used to install and set up the platform.

2.1.2. Conventions Used in this Guide

Insights topics may display a badge to indicate that functionality is only available to administrator users.

- admin-users-only

2.2. Arbitrator Licensing

2.2.1. Overview

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

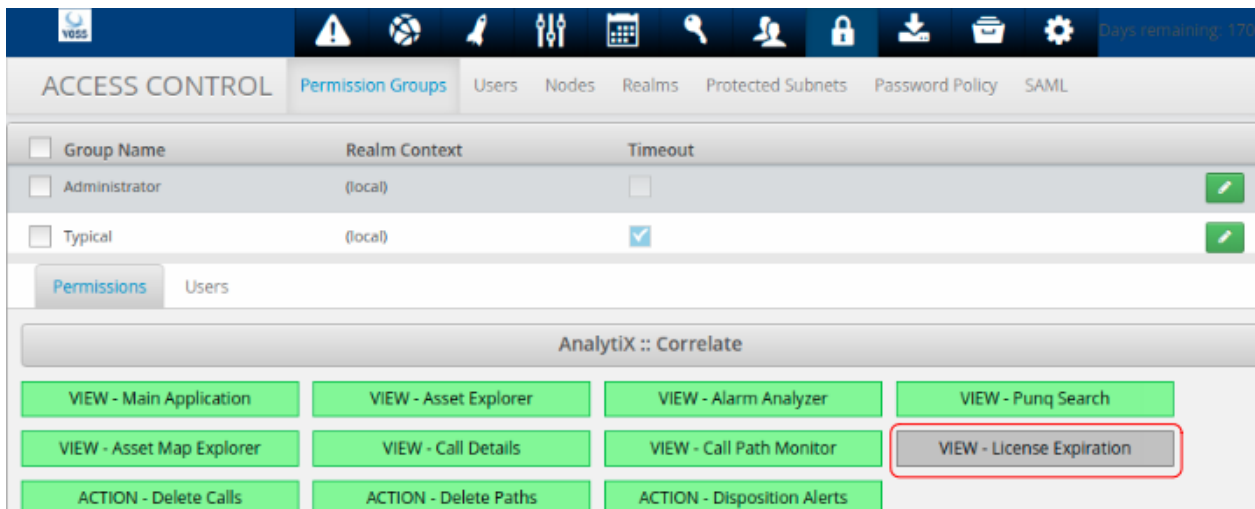
This setting can be enabled (display) or disabled (hide).



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

admin-users-only

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

admin-users-only

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.

2.3. License Auditing

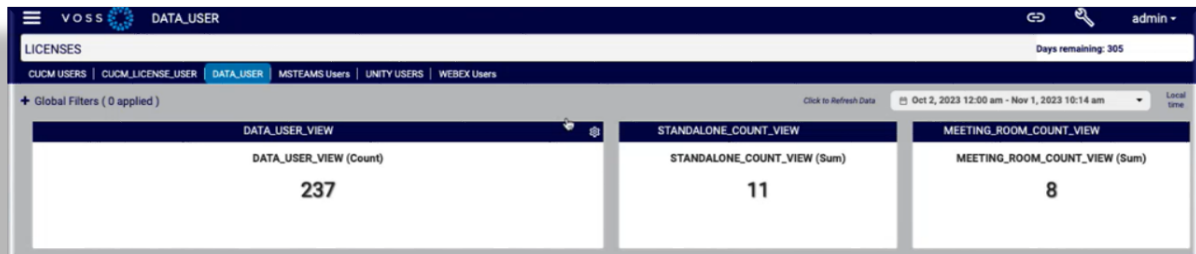
2.3.1. Overview

VOSS Insights integrates with the VOSS Cloud Licensing service to provide license auditing capabilities that allows you to view and inform VOSS of your license usage counts across various services and devices, including Cisco Unified Communications Manager (CUCM), Webex, Zoom, and Microsoft Teams.

A backend service on the Arbitrator detects probes already configured for CUCM, UCCE, UNITY, Webex, and MS Teams devices, and automatically retrieves the user accounts for the respective services.

Insights ships with resource files for the following views, which allow you to create dashboards that display user license counts for your system:

- data_user_view
- standalone_count_view
- meeting_room_count_view



The license auditing service generates a file that can be automatically sent to the VOSS Cloud Licensing service for processing.

Note: If you prefer to opt out of the automated license delivery mechanism, you will need to manually upload the license user count details to VOSS.

Related Topics

- [License Tab](#)

2.3.2. Register with the VOSS Cloud Licensing Service and Upload License File

This procedure registers your organization for syncing with the VOSS Cloud Licensing service, and optionally, allows for the license file to be automatically uploaded to the VOSS Customer Portal. Alternatively, once you've registered, you can manually upload the license file.

Registering allows licensed user counts to be added to a file that is generated on Insights Arbitrator. These files are generated daily.

Before you start

- Open the following ports to communicate with the VOSS Customer Portal at *voss.portalshape.com/*
 - Default HTTP: port 80
 - Default HTTPS: port 443
- Add the host name to an allowlist for trusted servers: *platform.voss-solutions.com*

Note: If your system is unable to reach external sites on the internet, you can use a proxy server that you set up on the Arbitrator (via **Configuration > Archive Management > Configuration Management > Proxy tab**)

Register and upload license file

1. Log in to Arbitrator as administrator, then click the toolbar **Wrench** icon (System Configuration) to open the **Configuration** GUI.
2. Click **Archive Management**, then on the **Archive Management** page, select the **License** tab.
3. Fill out your organization ID, your environment type (for example, staging, trial, or lab), and optionally, a device description.

Note: You can obtain your organization ID from the VOSS Customer Portal. Registration and file upload fails if the organization ID is incorrect.

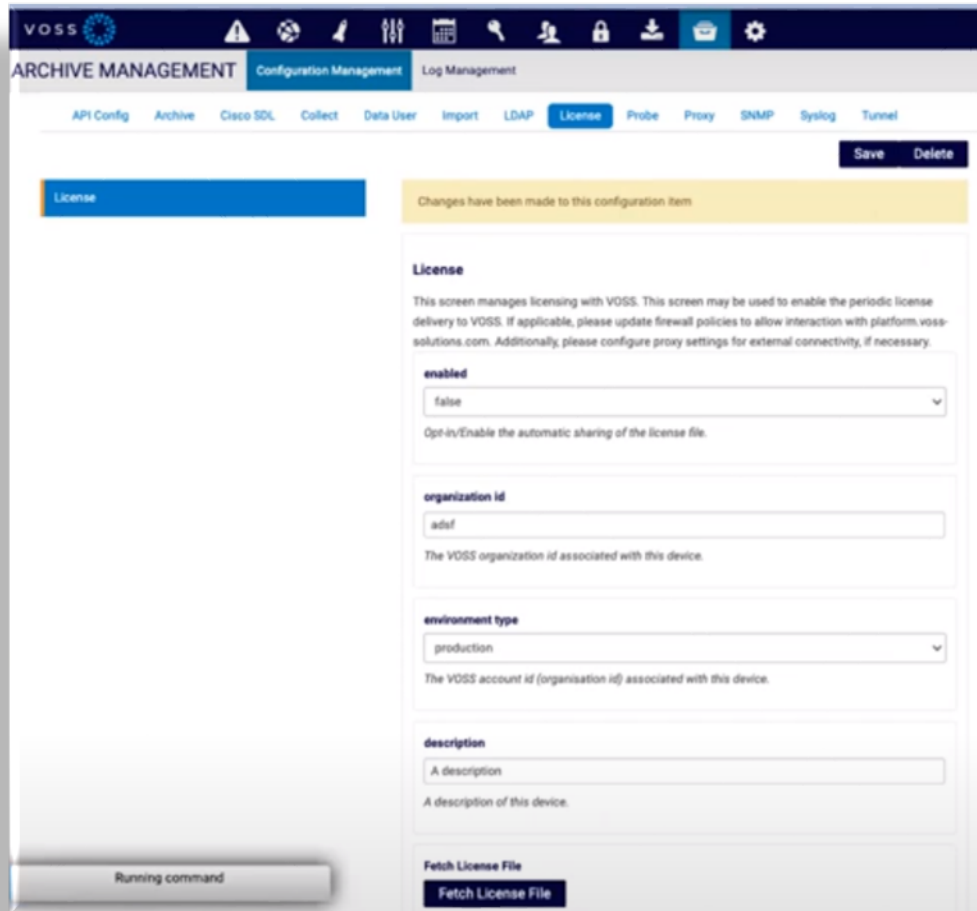
4. To allow automatic upload of generated license file to the VOSS Customer Portal, set the value of the **enabled** drop-down to `true`.

Note: If you wish to opt out of automatic file uploads, set the value to `false` (default).

5. Click **Save** to generate the license file for the organization ID you provided.
6. (Optional) On the **License** tab, click **Fetch License File**.

Note: Clicking **Fetch License File** before saving triggers an error as the license file won't have been generated yet.

To view the content of the license file you can click **View Output**.



Alternative steps:

- Option 1 - Copy license file details, and submit the details to VOSS:
 - On the **License** tab, click **Fetch License File**.
 - Click **View Output** to display the contents of the license file in a dialog on this page.
 - Copy the license file contents, and submit the details to VOSS.
- Option 2 - Download the file, and submit it to VOSS:
 - Copy the last part of the path that appears below the **Fetch License File** button (`license/latest.csv`)
 - Append the copied text to your system IP address in a URL (in a new tab).
 - The license file downloads as a `.csv` file.
 - Upload the file to the VOSS Customer Portal.

Related Topics

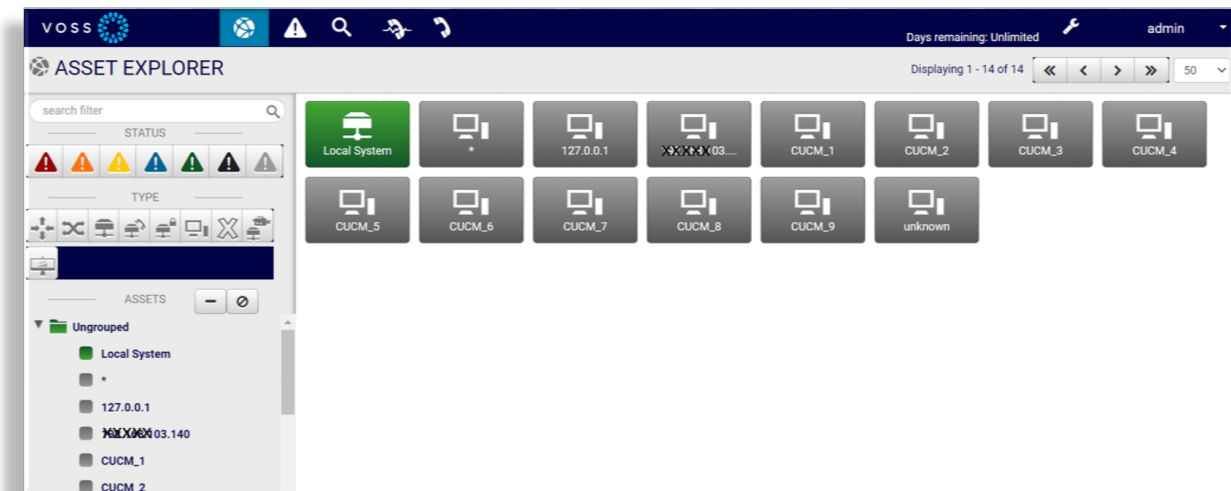
- [Archive Management \(Proxy\) in the VOSS Insights Arbitrator Administration Guide.](#)

3. Arbitrator Main Interface

3.1. Arbitrator Main Interface

3.1.1. Overview

The Arbitrator GUI has two sections. The main interface displays on first log in, while the **System Configuration** GUI, accessed via the **Wrench** icon on the main interface toolbar, is accessible only to admin users.



You can select the following functionality via the toolbar icons on Arbitrator's main interface:

- *Asset Explorer*
- *Alert Analyzer*
- *Search*
- *Call Path Monitor*
- *Call Details Explorer*

Related Topics

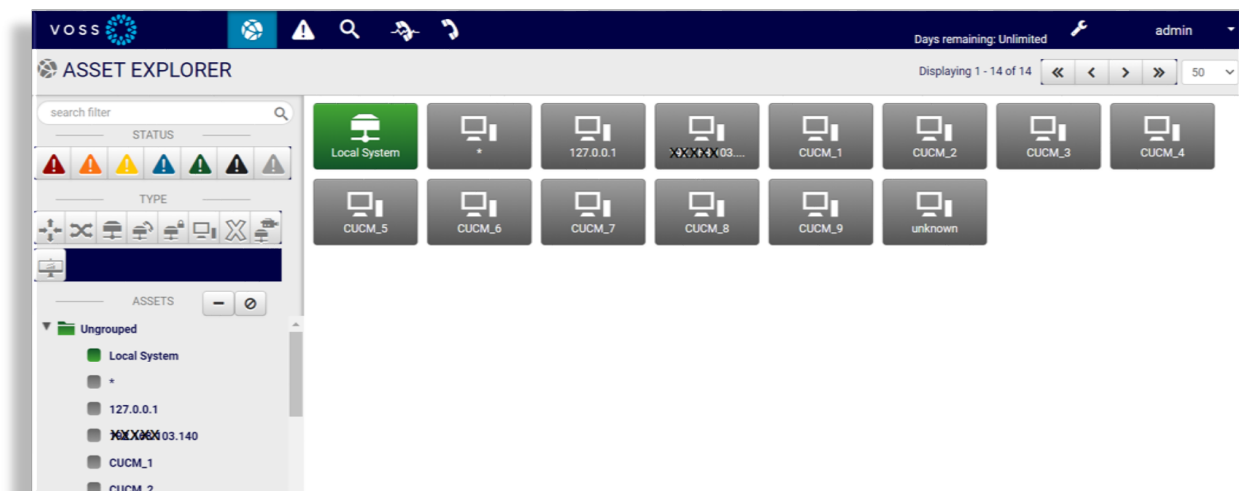
- [System Configuration](#)

3.1.2. Asset Explorer

Overview

The **Asset Explorer** tab lists devices created as assets in Arbitrator, displaying up to 100 assets per page. On this page you can also view the alert severity status of each asset, and click on an asset to view further details.

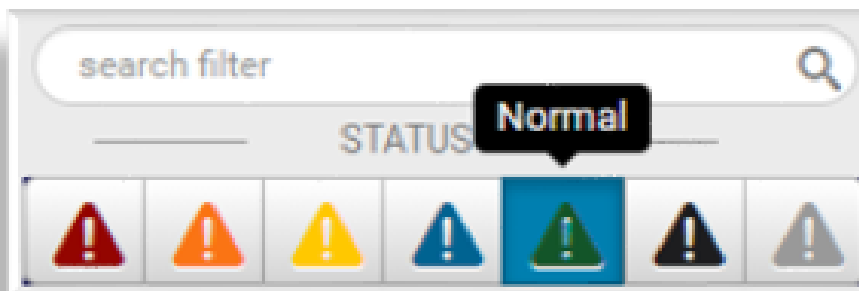
Note: If you have more than 100 assets, use the toolbar paging icons to display the next increment of assets.



Asset Alert Severity Status

Assets display the color of the current highest-level alert for that asset in the system.

Color coding is used to indicate the alert severity status of each asset:



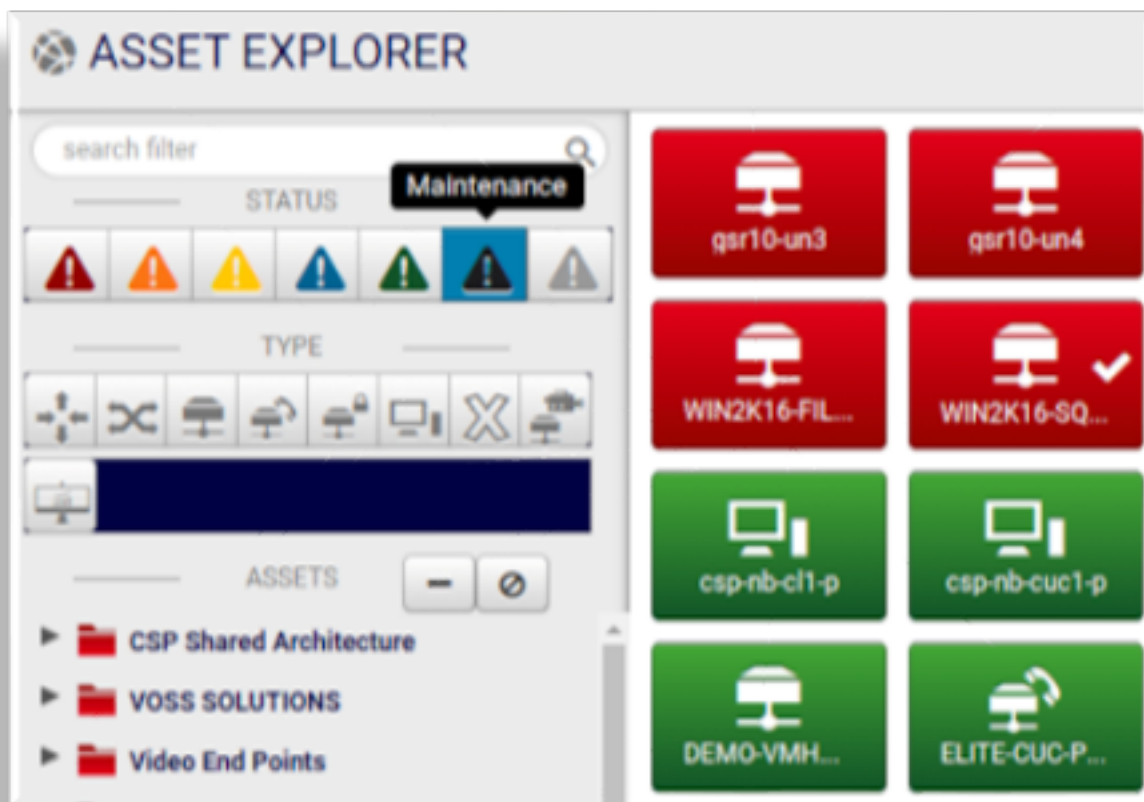
- Critical (Red)

- Major (Orange)
- Minor (Yellow)
- Informational (Blue)
- Normal (Green)
- Maintenance (Black)
- None (Gray)

Assets Search Filter

You can apply a search filter in the Asset Explorer to display only relevant assets (assets matching specified filters). You can filter assets by:

- Alert severity level, including maintenance mode
- Asset type
- Asset groups
- Keyword



Asset Details

Click on an asset in the Asset Explorer to open a summary of that asset's alarm statistics on the **Asset Details** page.

You can select the following tabs on the **Asset Details** page:

- Alerts
- Probes
- Search

Asset Details - Alerts Tab

The **Alerts** tab displays all alerts associated with the asset and allows you 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 `:ref:`arb-alert-analyzer`` section)

| DATE | NODE | POLICY | RULE | STATUS | OWNER |
|----------------------|-------|--------------------------|----------------------|--------|------------|
| 07/08/18 11:57:06 AM | depab | Class Alerts - Universal | Critical Class Error | OPEN | Unassigned |
| 07/08/18 09:25:15 AM | depab | Class Alerts - Universal | Major Class Error | OPEN | Unassigned |
| 07/08/18 09:18:21 AM | depab | Class Alerts - Universal | Critical Class Error | OPEN | Unassigned |

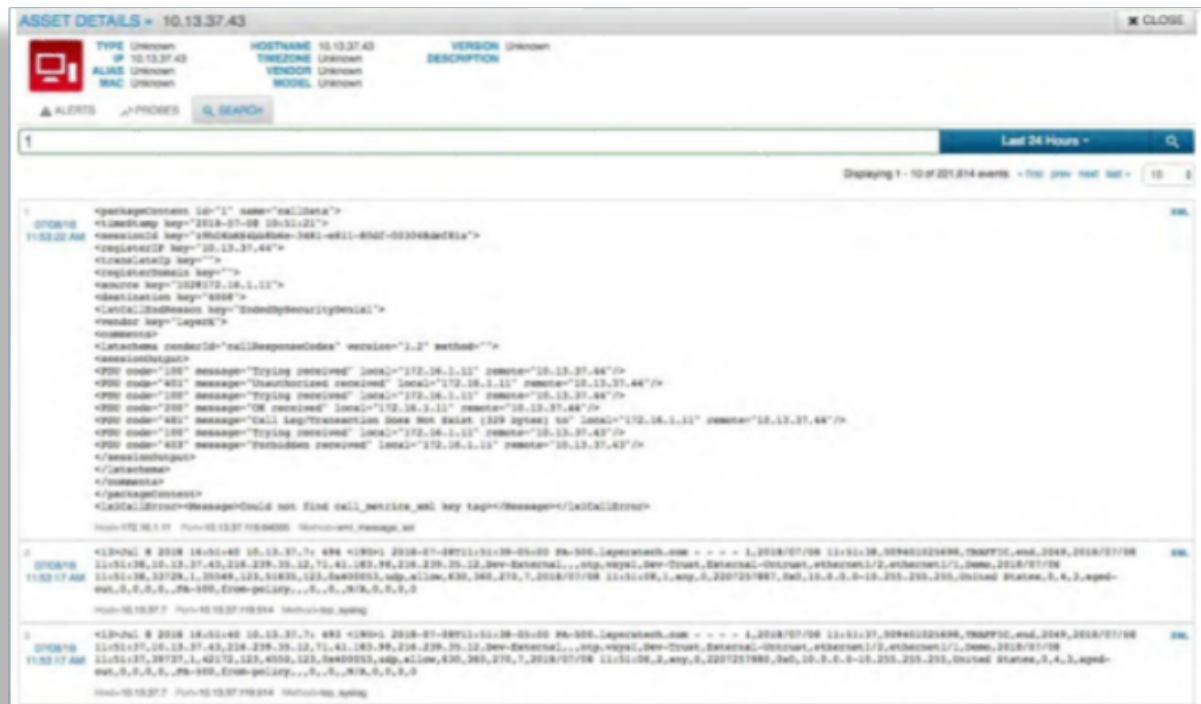
Asset Details - Probes Tab

The **Probes** tab displays all probes associated with the asset. Clicking on each probe displays 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 displays.



Asset Details - Search Tab

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



3.1.3. Alert Analyzer

Overview

On the **Alert Analyzer** page you can view all alerts coming into the system based on a first in/last out presentation. You can view older, existing alerts, as well as viewing alerts as they occur. You can disposition alerts based on activity, and view a report details associated with a specific alert. Several filter and sort options can also be applied.

The screenshot displays the Alert Analyzer interface. At the top, it shows 'ALERT ANALYZER' and 'Displaying 1 - 10 of 2,702 Alerts'. Below this is a table with columns: DATE, NODE, POLICY, RULE, STATUS, and OWNER. The first alert is expanded, showing a detailed description and a summary section.

Alert Details:

- REFERENCE ID:** 2000-01000008-00-01-28800-4430
- NODE:** depart
- POLICY:** Class Alerts - Universal
- RULE:** Critical Class Error
- OWNER:** Unassigned
- STATUS:** OPEN
- START:** 210718 01:01:37 PM
- LAST CHANGE:** -
- ELAPSED TIME:** -
- NEXT ESCALATION:** 210718 03:01:30 PM
- EXPIRES IN:** Expired
- RESPONSE PROCEDURE:** Default PP

Description: Critical Class Error (reason:'control engine' message:'Attempting Control Method (LinkToFullAlert) Parameters 1, <13>Jul 7 2018 17:58:48 10.13.37.44: <183><18306> : : 112181: suwell.laportech.com: Jul 07 2018 05:58:44 PM:312 UTC : NUC_RDMT-I-RDMT_ALERT: %AlertName-RDMTSessionsExceedsThreshold{{AlertDetail}} On Sat Jul 07 12:58:44 CDT 2018, alert RDMTSessionsExceedsThreshold has occurred. Counter SessionsActive of Class Tomcat Web Application{{set}} on node 10.13.37.44 has value of 278PE12 which is over high threshold 250:AppID=Class ANK Service:ClusterID=13nodeID=000111: RDMT_ALERT: <13>Jul 7 2018 17:58:48 10.13.37.44: <183><18306> : : 112181: suwell.laportech.com: Jul 07 2018 05:58:44 PM:312 UTC : NUC_RDMT-I-RDMT_ALERT: %AlertName-RDMTSessionsExceedsThreshold{{AlertDetail}} On Sat Jul 07 12:58:44 CDT 2018, alert RDMTSessionsExceedsThreshold has occurred. Counter SessionsActive of Class Tomcat Web Application{{set}} on node 10.13.37.44 has value of 278PE12 which is over high threshold 250:AppID=Class ANK Service:ClusterID=13nodeID=000111: RDMT_ALERT: code=99512)

Alert List:

| DATE | NODE | POLICY | RULE | STATUS | OWNER |
|--------------------|--------|--------------------------|----------------------|--------|------------|
| 210718 01:01:37 PM | depart | Class Alerts - Universal | Critical Class Error | OPEN | Unassigned |
| 210718 01:01:38 PM | depart | Class HCS PCA | RDMT_ALERT | OPEN | Unassigned |
| 210718 01:02:21 PM | depart | Class Alerts - Universal | Critical Class Error | OPEN | Unassigned |
| 210718 01:02:38 PM | depart | Class HCS PCA | RDMT_ALERT | OPEN | Unassigned |
| 210718 01:02:40 PM | depart | Class Alerts - Universal | Critical Class Error | OPEN | Unassigned |

Disposition

Disposition allows you to set the status of each alert, either one at a time, or in bulk.

The table describes the options for alert disposition:

| Option | Description |
|--------------|---|
| Open | Indicates a new alert. |
| Under Review | Indicates that the alert has moved out of the Open state and the alert journal can still be edited. |
| Acknowledge | Indicates that the alert has moved out of the Open state and the alert journal can still be edited. |
| Release | Indicates that the alert has moved out of the Open state and the alert journal can still be edited. |
| Close | Indicates that the alert has moved out of the Open state and the alert journal can still be edited. |
| Disregard | The alert is deleted from the system. |
| Close + Lock | Indicates that the alert has moved to a Closed state and the alert journal cannot be edited. |

Disposition a Single Alert

1. Expand the alert to open it (click the up/down arrows to the far right of the alert).
2. From the **Status** drop-down, select the disposition state.

The screenshot displays the 'ALERT ANALYZER' interface. At the top, it shows 'Displaying 1 - 10 of 3,800 Alerts'. Below this is a table with columns: DATE, NODE, POLICY, RULE, STATUS, and OWNER. The first alert is expanded, showing its details. A status dropdown menu is open over the first alert, listing the following options: OPEN, UNDER REVIEW, ACKNOWLEDGE, RELEASE, CLOSE, DISREGARD, and CLOSE + LOCK. The alert details include a description of a critical error, a reference ID, and various timestamps and escalation information.

Bulk Disposition Multiple Alerts

This procedure disposes a group of alerts at once.

1. Apply the required filter to the alerts - use the Filter Manager (see Alert Filters).
2. Once you have the group of alerts filtered, choose the required disposition state from the **Bulk Disposition** drop-down.

Filter by Disposition

1. Click the down-arrow at the **Status** drop-down.
2. Select a disposition status.
3. Click **Update** to apply the filter to see only those alerts with the disposition status you've selected.
4. View alerts, filtered by the selected disposition status.



Filter Manager

You can apply filters to alerts to view only a subset of alerts. You can filter by keywords, severity, and by date and time.

1. On the **Alert Analyzer** page, click the **Wrench** icon in the **Filters** pane to open the **Filter Manager**.
2. Click the Plus icon (+) to add a new filter.
3. Fill out filter criteria across the tabs: Keywords, Severity, Date & Time:
 - On the **Keywords** tab, fill out a name and description for the filter, then fill out filter criteria, which can be any or all of the following: correlation policy, correlation rule, group name, customer name, site, node, owner, or message

The screenshot shows the 'FILTER MANAGER' window with the 'KEYWORDS' tab selected. On the left, there is a list of filters with a checked entry 'Test' and a description 'This is a test filter'. Below this are 'ALLOW' and 'DISREGARD' buttons. On the right, there are input fields for: NAME (Test), DESCRIPTION (This is a test filter), POLICY, RULE (Critical Cisco Error), GROUP, CUSTOMER, SITE, NODE, MESSAGE, and OWNER.

- On the **Severity** tab, select one or more severity states:
 - 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

The screenshot shows the 'FILTER MANAGER' window with the 'SEVERITY' tab selected. On the left, there is a list of filters with an unchecked entry 'Test' and a description 'This is a test filter'. Below this are 'ALLOW' and 'DISREGARD' buttons. On the right, there is a table for selecting severity states.

| | ACTIVE | ESCALATED | ACKNOWLEDGED | EXPIRED |
|---------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| CRITICAL | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| MAJOR | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| MINOR | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| INFORMATIONAL | <input checked="" type="checkbox"/> | | | |

- On the **Date & Time** tab, set a date range for the filter, either “All Day”, a specific start and end time, a day of the week, or any combination.

The screenshot shows the 'FILTER MANAGER' window with the following elements:

- Buttons: + ADD, - REMOVE, SAVE, CANCEL.
- Tabs: KEYWORDS, SEVERITY, DATE & TIME (selected).
- Filter List: A table with one entry:

| Filter Name | Filter Text | ALLOW | DISREGARD |
|-------------|-----------------------|--------------------------|--------------------------|
| Test | This is a test filter | <input type="checkbox"/> | <input type="checkbox"/> |
- DATE: START DATE, END DATE (input fields).
- TIME:
 - ALL DAY
 - START: HOUR (0), MINUTE (0), End: HOUR (0), MINUTE (0)
- DAY OF WEEK:
 - SUNDAY
 - MONDAY
 - TUESDAY
 - WEDNESDAY
 - THURSDAY
 - FRIDAY
 - SATURDAY

Alert Journal

The Alert Journal displays the alert history as well as system and user actions. Users can add journal entries to update status or actions.

Add an Alert Journal

1. On the **Alert Analyzer** page, click the **Pause** button to stop the automatic refresh.
2. Expand the alert where you want to add an entry.
3. Click **Journals**, then fill out a journal entry in the field displaying the text, **NEW JOURNAL ENTRY**.
4. Click **Add**.
5. Click the **Play** button to resume refresh on the Alert Analyzer.

The screenshot displays the Alert Analyzer web interface. At the top, it shows 'ALERT ANALYZER' and 'Displaying 1 - 10 of 3,898 Alerts'. Below this are controls for 'FILTERS', 'SORT', 'BULK DISPOSITION', and 'STATUS'. A table lists alerts with columns for DATE, NODE, POLICY, RULE, STATUS, and OWNER. One alert is expanded to show details and a journal.

| DATE | NODE | POLICY | RULE | STATUS | OWNER |
|-------------------------|------|----------------------|----------------------|--------|------------|
| 07/08/18 12:00:40 PM | | Critical Cisco Error | Critical Cisco Error | OPEN | Unassigned |

Alert Details:
 Critical Cisco Error (13-Jul 8 2018 17:00:40 169.254.5.16: <186-206881> ; ; 203794: asldo-v-csm-pub-dimensional.com: Jul 08 2018 05:00:37 PM:410 UTC : NUC_RMTM-2-RTMT_ALERT: %AlertName=CriticalServiceDown][AlertDetail=#012 Service operational status is DOWN.#012Cisco CallManager.#012The alert is generated on Sun Jul 08 12:00:37 CDT 2018 on node asldo-v-csm-pub-dimensional.com.[AppID=Cisco AMC Service][ClusterID=][NodeID=asldo-v-csm-pub]: RTMT Alert)

Journal Entries:

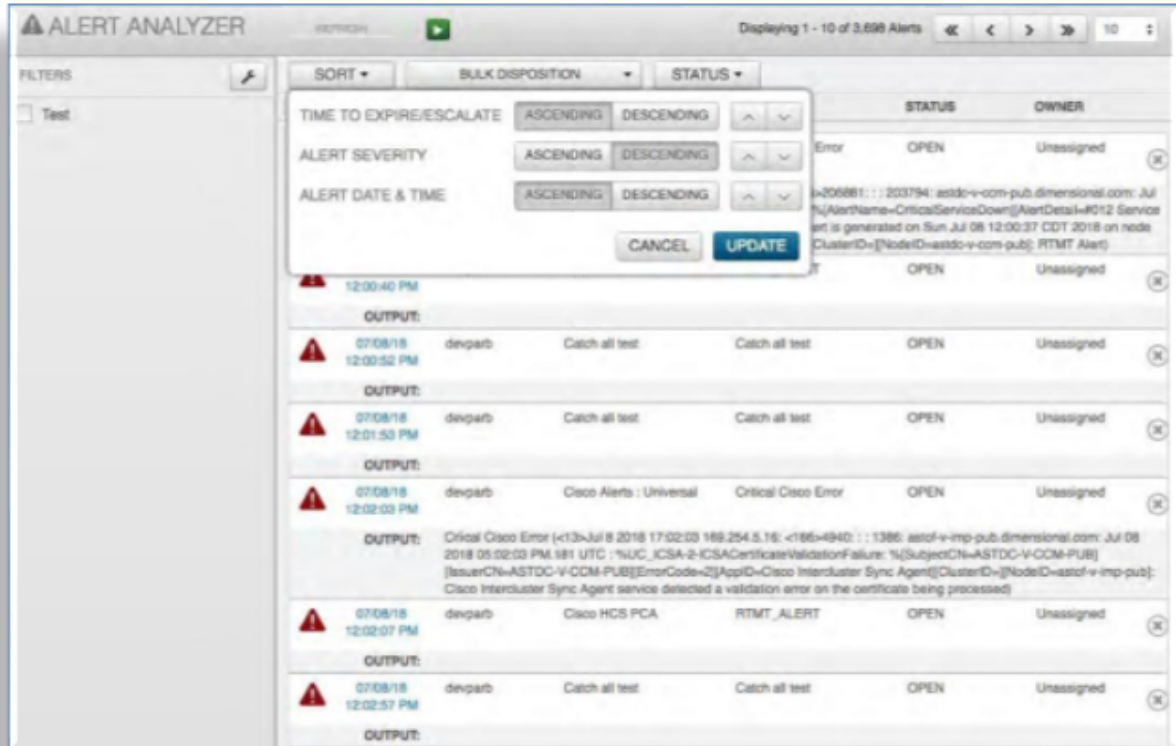
| TIMESTAMP | CREATOR | ACTION |
|----------------------|---------|---|
| 07/08/18 12:45:36 PM | system | Alert Created, Response: Default RFP Schedule: autogenerated_schedule_20x7 Node: dnpdrt(127.0.0.1) - Critical Cisco Error : Critical Cisco Error (13-Jul 8 2018 17:00:40 169.254.5.16: <186-206881> ; ; 203794: asldo-v-csm-pub-dimensional.com: Jul 08 2018 05:00:37 PM:410 UTC : %UC_RMTM-2-RTMT_ALERT: %AlertName=CriticalServiceDown][AlertDetail=#012 Service operational status is DOWN.#012Cisco CallManager.#012The alert is generated on Sun Jul 08 12:00:37 CDT 2018 on node asldo-v-csm-pub-dimensional.com.[AppID=Cisco AMC Service][ClusterID=][NodeID=asldo-v-csm-pub]: RTMT Alert) |
| 07/08/18 12:45:37 PM | system | Incident Response - Method: ALERT, Status: Success |
| 07/08/18 12:45:37 PM | system | Incident Response - Method: CONTROL, Description: New Vodafone Control, Status: Success |

Alert Sort

Alerts in the Alert Analyzer can be sorted based on the following categories:

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

The sort order for each category can be toggled between ascending and descending. Additionally, the order of each sort category will be the first to last in priority. To change this, click the down arrow or the up arrow adjacent to each category.



3.1.4. Search

Overview

Arbitrator's main interface provides the following search options:

- *Event Search*
- *Simple Search*
- *Keyword Search*
- *Use Operators with Search*
- *Date Range Search*

Event Search

The Event search view provides access to all raw data coming in to Arbitrator and provides a simple interface to search for and display results.

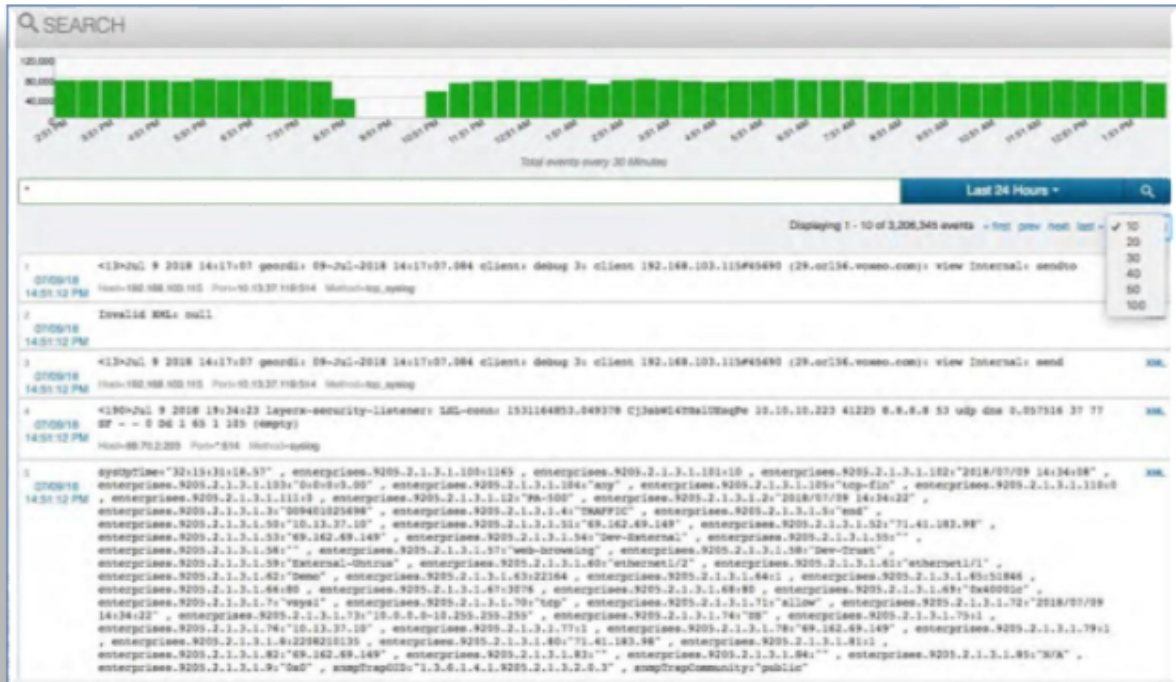
Arbitrator builds a dictionary of all words from all received logs, enabling rapid search across large volumes of data, making an otherwise complex amount of data quickly searchable and more useable.

Simple Search

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

1. In the search text input field type *
2. Press **Enter**, or click the magnifier icon.
3. View search results, which displays all log data received in the last 24 hours.

The default number of logs per page is 10, but can be increased via the drop-down below the time bar.



Keyword Search

To perform a keyword search across all logs based on the default time of “Last 24 Hours”:

1. Fill out a word or part of a word that you know is present in your data, such as “Cisco”.
The event search auto suggests a keyword as you type, based on data the Arbitrator has collected.
2. Press **Enter** to select the auto-suggested word, or click the Magnifier icon to run the search.
3. View search results, which displays all log data from the past 24 hours that contains the specified criteria.

The default number of logs per page is 10. To increase the number of logs per page, select the required number from the drop-down below the time bar.



Use Operators with Search

The Event Search allows the use of operators (AND, OR, NOT) to combine keywords that you know are present in your data for a more granular search. A search with operators searches across all logs based on the default time of “Last 24 Hours”.

1. Fill out a word or part of a word that you know is present in your data, such as “Cisco”, followed by the relevant operator (AND, OR, NOT).

Note: When using operators, the logic must match in order to retrieve data.

2. Select a keyword from the auto-suggest, or press **Enter** to run the search.
3. View search results, which displays all log data from the past 24 hours that contains the specified criteria.

The default number of logs per page is 10. To increase the number of logs per page, select the required number from the drop-down below the time bar.



Date Range Search

You can search for and apply a date to any of the possible search types discussed in this section.

The default is the last 24 hours, or choose an option from the drop-down:

- 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 a specific “From” date. Clicking in the “To” box will do the same.

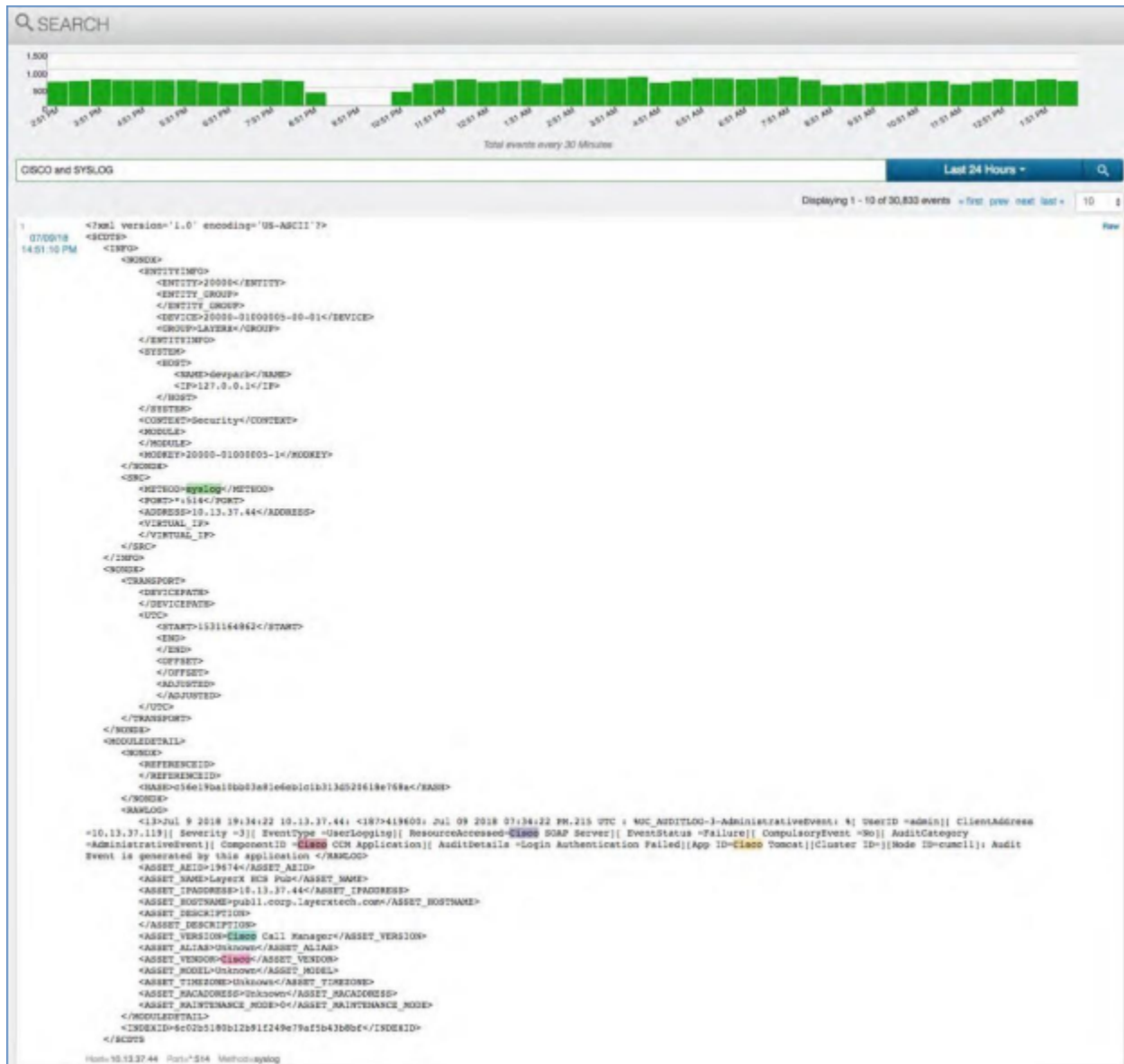


Search Result Metadata

The event search engine uses Arbitrator's core processes to store, tag, and manage data.

Click on the blue text ("XML") that displays with each log entry to open up an XML representation of the data along with additional important elements, specifically, the entity ID's, which make every event unique and formulates the "Reference ID" seen on the Alert Analyzer page. For compliance purposes, a hash of the raw log is also available, if required.

To return to the main search page, click **Raw**.



3.1.5. Call Path Monitor

Arbitrator's **Call Path Monitor** allows you to manage unified communications, and the particular call path that a Voice over IP call (VoIP) takes. It displays the paths or routes that a call takes from source to destination. Each path contains the IP Addresses, number of hops, delay, and latency during the call.



Sorting Call Paths

The Call Path Monitor provides three options for sorting data on the page and for represented call paths:

| | |
|---------------|---|
| 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. |

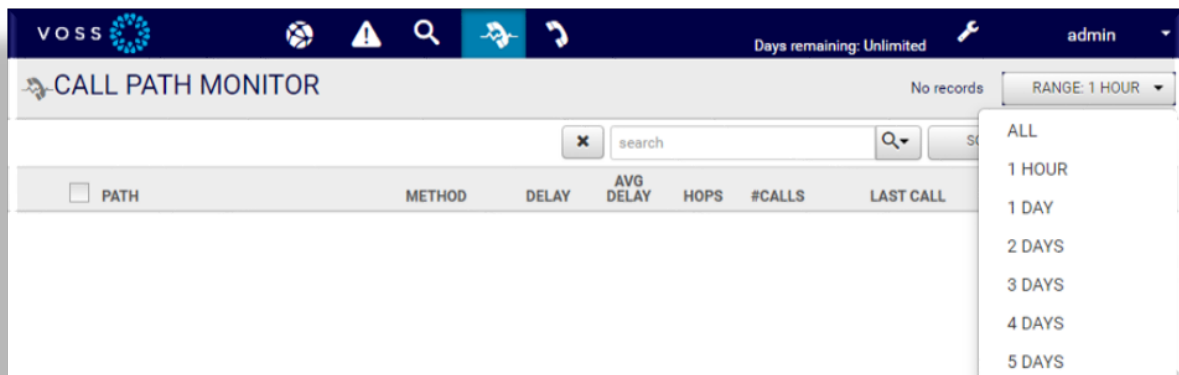
For each sort option, you can also choose to view the data in ascending or descending order.



Call Path Time Range

The Call Path Monitor time range setting allows you to define the time range for which you wish to view collected call paths. The **Range** drop-down provides the following options:

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

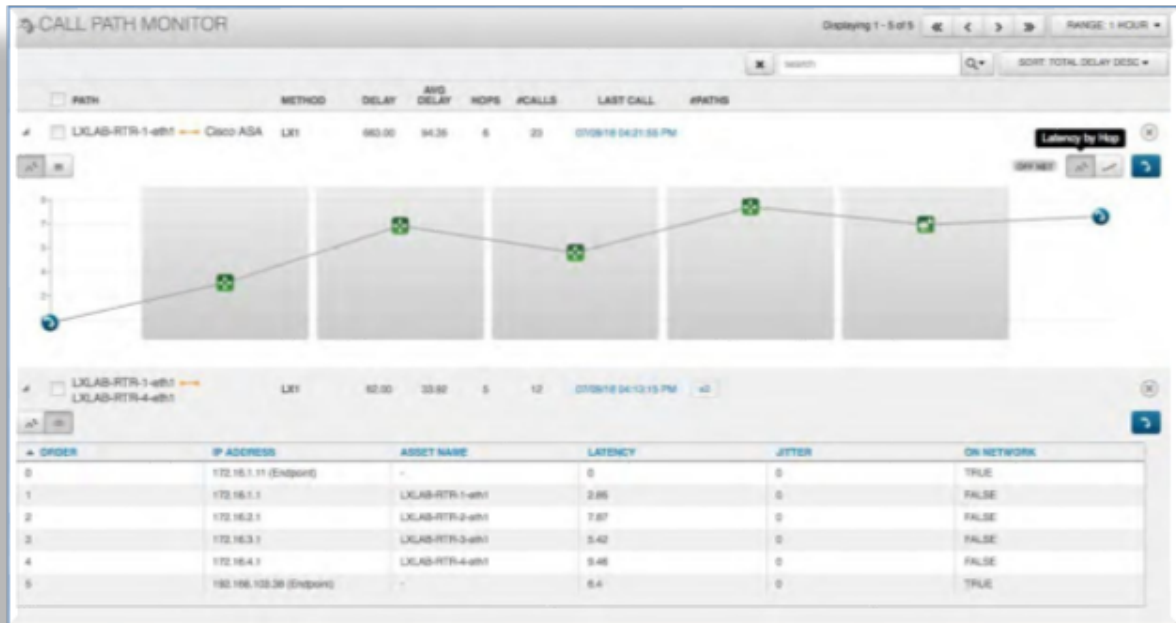


Expanded Call Path View

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 the arrow adjacent to the relevant call path.

By default, the view is in graph mode. To switch to the table view, 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 use to search and filter for a relevant call (one or more).

- Source
- Destination
- Method
- Hops

The screenshot shows a search filter dialog box. It has a search input field with a magnifying glass icon. Below the input field are four checkboxes, all of which are checked: SOURCE, DESTINATION, METHOD, and HOPS. Each checkbox is followed by an empty text input field. At the bottom of the dialog are two buttons: 'CLOSE' and 'SEARCH'.

View Call Details from the Call Path

In the Call Path Monitor you can drill into the specific call details directly from the chart.

Click the blue Phone icon in the path row to open the Call Details Explorer view for that call path.

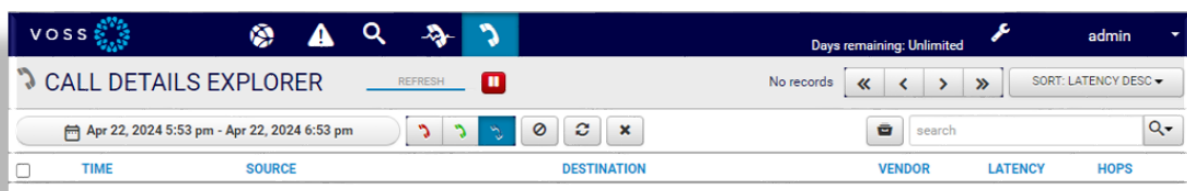
3.1.6. Call Details Explorer

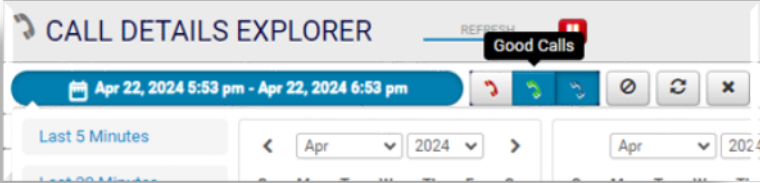
The Call Details Explorer is the main page for managing unified communications and the details of a particular call path that a Voice over IP (VoIP) call takes. This page displays the time, source destination, vendor, latency, and hops (at the top of the page). The bottom pane displays the call path with each hop, along with the call metrics, such as packets lost, jitter, R-Factor, and MOS.



Call Details Explorer Toolbar

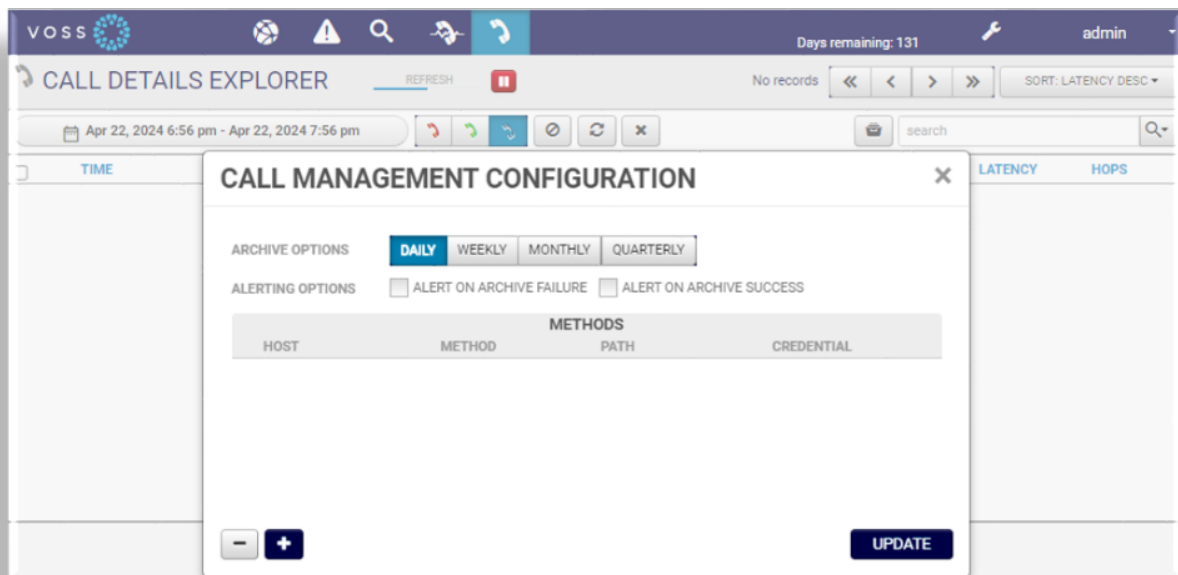
The table describes the functional elements on the Call Details Explorer toolbar:



| Element | Description |
|------------------------------|--|
| Filter by date and time | The date and time calendar allows you to search call details for a specified date and time range. You can select a date and time from the calendar, or select from a range of predefined options, from Last 5 Minutes, to Last 12 Months, or for the previous hour, day, or week. |
| Filter by call quality | <p>The Phone icons allow you to filter your data to view only good calls, only bad calls, or view both good and bad calls.</p> <ul style="list-style-type: none"> • Bad Calls (Red) • Good Calls (Green) • Bad and Good Calls (Blue)  |
| Clear Filters | Removes all applied filters and displays call details in the default display mode. |
| Update | Applies a predefined refresh timer to the page. Click Update to request new data, on demand. |
| Delete Selected Calls | Deletes any call selected on the page. |
| Refresh, Play, or Pause Data | Click the Pause/Play icon to pause or restart the data refresh cycle. This is useful when reviewing a specific call. |
| Sort | <p>Provides the following sort options for call details. You can sort by:</p> <ul style="list-style-type: none"> • The time the call was placed • The source that placed the call • The call destination • The vendor, which 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 • The total number of hops the call took <p>You can sort each option in ascending or descending order.</p> |
| Search | <p>A free text search field that also has options to use predefined criteria, either of the following:</p> <ul style="list-style-type: none"> • Search by the source IP that made the call • Search by the destination IP that received the call • Search by vendor, which identifies the method that created the call. Options are LX1 (the VOSS Raptor Call Path generator) and RTCP (Avaya-specific RTCP and call path data) |

| Element | Description |
|-------------------------------|---|
| Call Management Configuration | <p>Click the File icon adjacent to the Search bar to open the Call Management Configuration dialog, where you can configure settings to manage the call table on the Call Details Explorer page.</p> <p>In very busy or large environments it is imperative that you manage the data being collected in the Call Detail Explorer. Having potentially thousands of calls can lead to the data becoming difficult to manage. These settings provide optional time and methods for which call data can be archived. Options are daily, weekly, monthly, or quarterly. Ensure that you toggle on Alert on Archive Failure, and Alert on Archive Success. Available archival methods are SCP, SFTP, or SMB. Each requires a host, path, and credential. Multiple methods may be added.</p> |

The image shows the Call Management Configuration dialog:



4. Configuration

4.1. System Configuration

4.1.1. Overview

Insights Arbitrator's **System Configuration** GUI is accessible via the toolbar **Wrench** icon (System Configuration), on the main user interface.



The **Configuration** GUI toolbar icons provide access to configuration options for the following:

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

The screenshot displays the Voss Policy Configuration interface. The top navigation bar includes the Voss logo, a search icon, a calendar icon, a user icon, a lock icon, a download icon, and a settings icon. The user is logged in as 'admin' and has 313 days remaining. The main content area is divided into two sections: 'Policies' and 'Rules'.

Policies:

| Name | Failover | Count |
|-----------------|--------------------------|-------|
| Cuom_CmCat_Cm | <input type="checkbox"/> | 146 |
| Touy | <input type="checkbox"/> | 5 |
| Ack Alert | <input type="checkbox"/> | 2 |
| Demo2 | <input type="checkbox"/> | 1 |
| Infinity | <input type="checkbox"/> | 1 |
| Ping | <input type="checkbox"/> | 1 |
| Second Dchannel | <input type="checkbox"/> | 1 |

Rules:

| Name | Threshold | Window | Severity | Response Procedure | Actions |
|-------------------------------|-----------|----------|---------------|--------------------|---------|
| Alarm ID: 50506 (DChannelO... | 1 time | 1 minute | Critical | Default IRP | ↔ 2 ☰ ✓ |
| Alarm ID: 50500 (CallManag... | 1 time | 1 minute | Critical | Default IRP | ↔ 2 ☰ ✓ |
| Alarm ID: 50501 (SDLLinkiSV) | 1 time | 1 minute | Minor | Default IRP | ↔ 2 ☰ ✓ |
| Alarm ID: 50502 (SDLLinkOO... | 1 time | 1 minute | Critical | Default IRP | ↔ 2 ☰ ✓ |
| Alarm ID: 50503 (CMVersion... | 1 time | 1 minute | Informational | Default IRP | ↔ 2 ☰ ✓ |

Related Topics

- [Arbitrator Main Interface](#)

4.2. Policy Configuration

4.2.1. Overview

Policies are 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

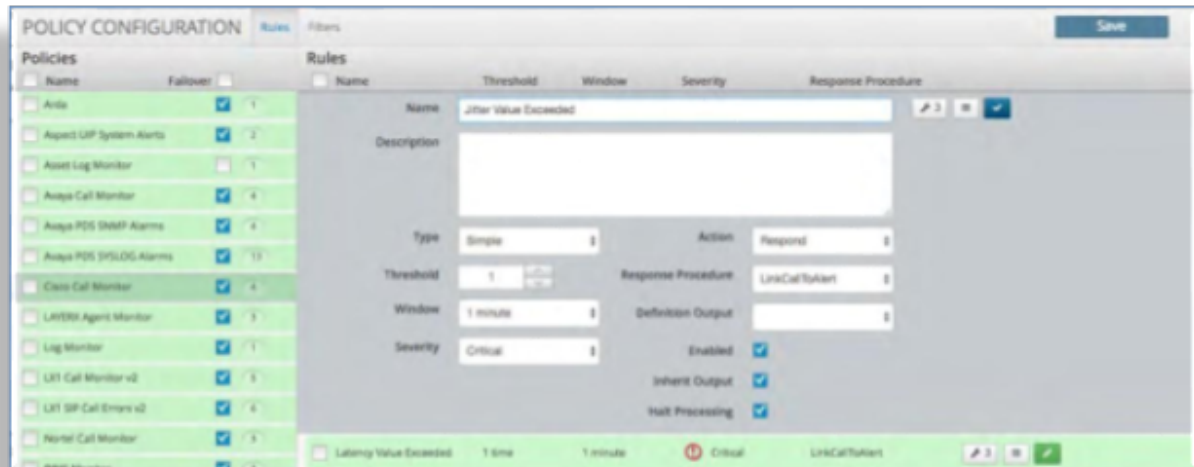
This screenshot is identical to the one above, showing the Voss Policy Configuration interface with the same 'Policies' and 'Rules' sections.

4.2.2. Correlation Rules

A correlation rule extracts data from the various sources and then defines the parameters for creating an alert within a policy. It may contain one 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 | 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. 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. Unique: Same as Simple but as a definition will be the only one. |
| Threshold | Defines how many times this rule is to match before an action occurs. |
| Window | The time window for the rule to match before an action occurs. |

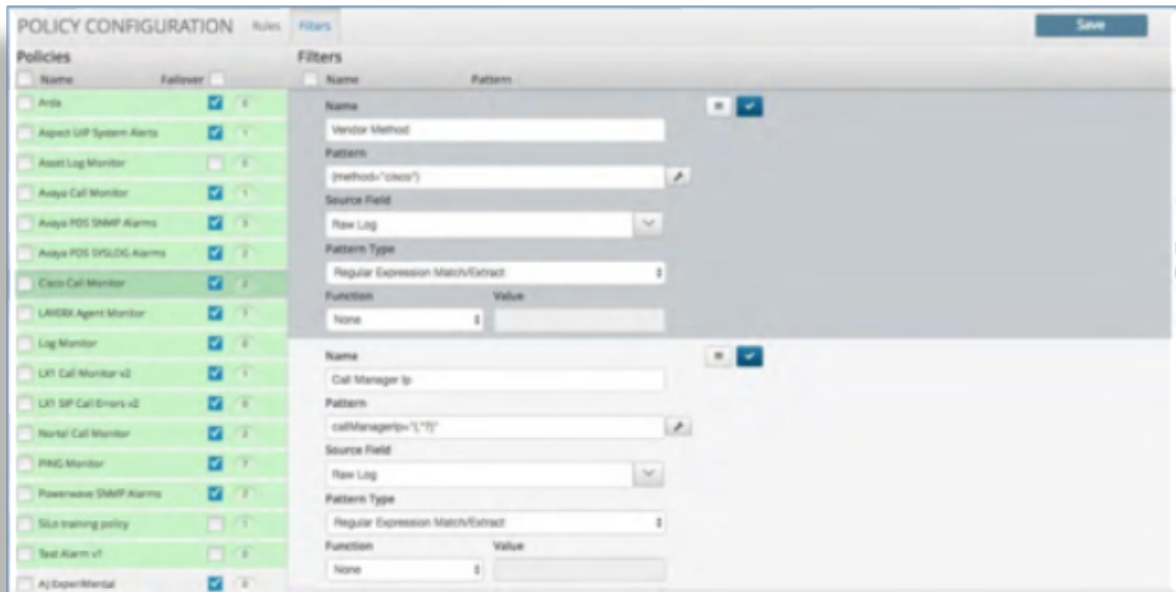
| Parameter | Description |
|-------------------------|--|
| Severity | Indicates what is to appear in the Status field on the Alert Viewer monitor. Select the severity for this rule: <ul style="list-style-type: none"> • Informational • Minor • Major • Critical |
| Action | Choose the action that is to occur for this rule, based on the selection in the Severity field <ul style="list-style-type: none"> • Respond - If the condition is met, set a marker and send an alert. • Track - If the condition is met, track the event, but do not post it to the Alert Analyzer. • Track/Respond - If the condition is met, send an alert and continue to monitor. • 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. • Submit - Submit the results of a correlation event back into the Correlation Engine so that the behavior can be analyzed and re- correlated. • 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 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 | <p>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.</p> <p>The Regex Wizard has two sections:</p> <ol style="list-style-type: none"> 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. 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 | <p>From the drop-down, choose the type of expression you want to use:</p> <ul style="list-style-type: none"> • String Match • Regular Expression Match • Regular Expression Match/Extract (Most Often Used) • Regular Expression Multi-Valued Extract |
| Function | <p>If the extracted data is integer-based, you can apply the following functions for comparing data:</p> <ul style="list-style-type: none"> • None • Greater Than • Less Than • Same |
| Value | This field is available only if the data extracted is an integer. |



4.2.3. 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:

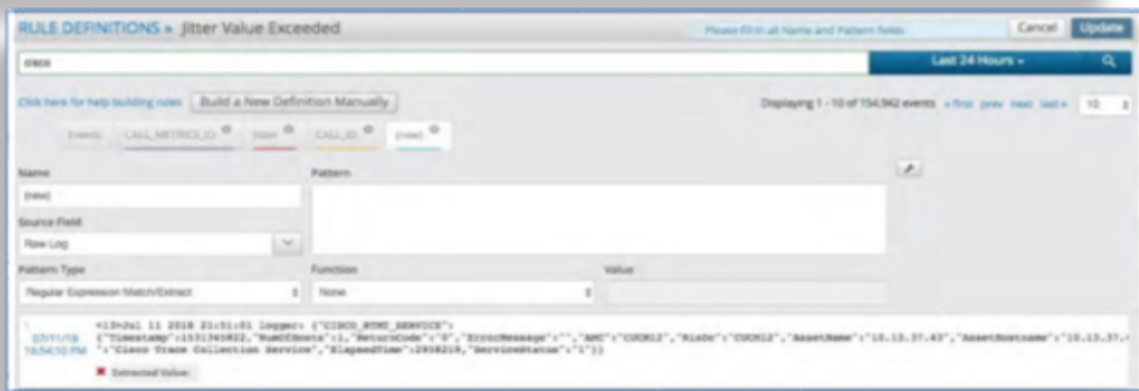
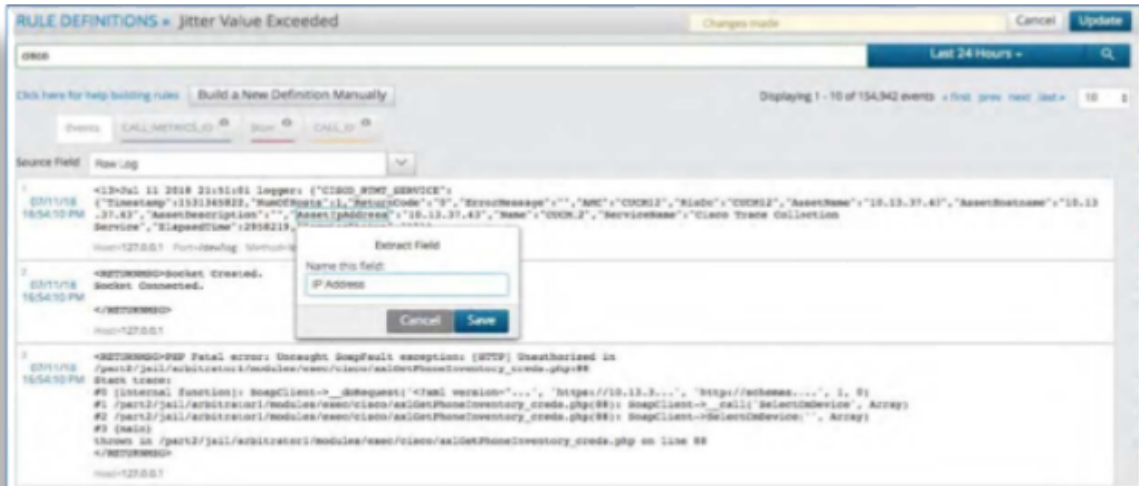
- As a filter on the policy
- As a specific rule definition.

4.2.4. Correlation Definitions

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

| Parameter | Description |
|-----------|---|
| Name | <p>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.</p> <p>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.</p> <p>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.</p> |
| Pattern | <p>Within the Regex Wizard there are 2 sections:</p> <ul style="list-style-type: none">• 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.• 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. |

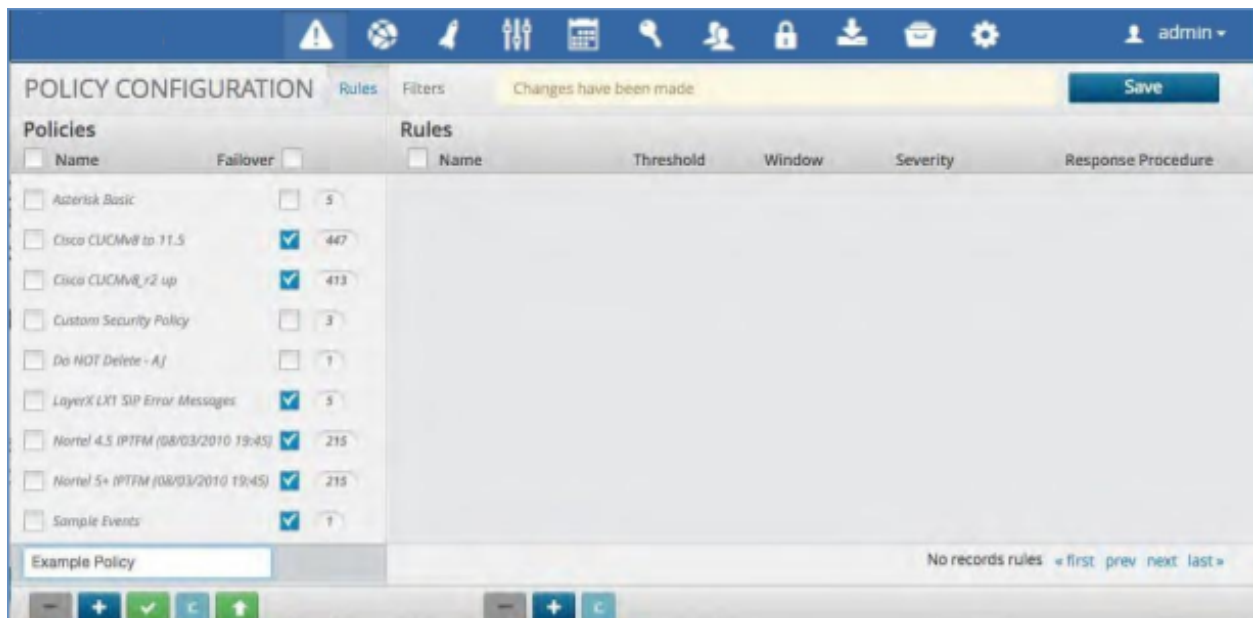
| Parameter | Description |
|--------------|--|
| Source Field | In the drop-down box select the source from which the data is being extracted. |
| Pattern Type | <p>Select from the drop-down box the type of expression you want to utilize:</p> <ul style="list-style-type: none"> • String Match • Regular Expression Match • Regular Expression Match/Extract (Most Often Used) • Regular Expression Multi-Valued Extract <hr/> <p>Note: The “Extract” pattern types above will cause the correlation engine to include the definition name and the matched value in the Alert Message.</p> <hr/> |
| Function | <p>The functions below may be used to change what the correlation engine counts as a “match” in the log. Alerts are only triggered if the specific number of matches are found.</p> <ul style="list-style-type: none"> • None - Default. Only use Pattern type matching to trigger a match. • Greater Than - Should only be applied to integer values. If the extracted value is greater than the configured value, then a “match” is made. • Less Than - should on be applied to integer values. If the extracted value is less than the configured value, then a “match” is made. • Same - Can be applied to both Text or Integer. If the extracted value is the same as previous occurrences, a match triggered. For example, if multiple devices are sending an error message, only the first error will trigger an alert. If the desired goal is to trigger an alert for unique IP address, then the IP address definition should have the Same function applied. |
| Value | This field will only be available if the function selected is either “Greater Than” or “Less Than”. |



4.2.5. Add a Policy

To add 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.



4.2.6. Add a Correlation Rule

To add 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.

The screenshot displays the 'POLICY CONFIGURATION' interface. On the left, there is a 'Policies' list with various monitoring rules like 'Avaya POS SMDP Alarms' and 'Cisco Call Monitor'. The main area shows a 'Rules' table with columns for Name, Threshold, Window, Severity, and Response Procedure. Below the table, a detailed configuration form for a rule is visible, including fields for Name, Description, Type, Threshold, Window, Severity, Action, Response Procedure, Definition Output, Enabled, Inherit Output, and Halt Processing. The 'Name' field contains '[red]'. The 'Severity' is set to 'Informational'. The 'Action' is 'Track/Respond'. The 'Response Procedure' is 'Default PIP'. The 'Enabled' checkbox is checked. At the bottom right, it says 'Displaying 1 - 4 of 4 rules'.

4.2.7. Add a Definition

To add 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.

The screenshot shows the 'POLICY CONFIGURATION' interface. At the top, there are tabs for 'Rules' and 'Filters'. Below this is a table with columns: 'Policies', 'Name', 'Follower', 'Rules', 'Threshold', 'Window', 'Severity', and 'Response Procedure'. The first row is 'Cisco Call Monitor' with a follower of '4', a rule of 'Jitter Value Exceeded', a threshold of '1 time', a window of '1 minute', a severity of 'Critical', and a response procedure of 'LinkCallToken'. A blue arrow points to a 'Save' button in the top right corner. Another blue arrow points to a small icon in the response procedure column.

This screenshot shows the 'RULE DEFINITIONS' for the 'Jitter Value Exceeded' rule. It displays a list of events with columns for 'Events', 'CALL_METRIC_ID', 'CALL_ID', and 'Time'. The first event is from '2018-11-15 16:54:10 PM'. A modal window titled 'Extract Field' is open, showing 'Name: IP Address' and a 'Save' button. A blue arrow points to the 'Save' button in the modal.

This screenshot shows the 'RULE DEFINITIONS' for the 'Jitter Value Exceeded' rule, focusing on the 'Pattern' field. The 'Pattern Type' is set to 'Regular Expression Match-Extract'. The 'Function' is 'None' and the 'Value' is empty. A blue arrow points to a 'Save' button in the top right corner.

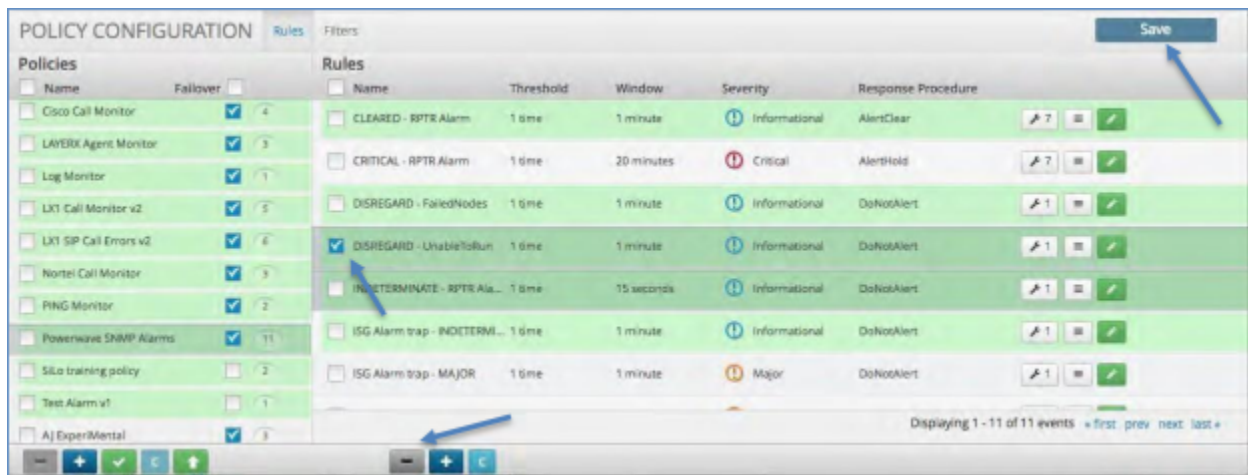
The screenshot shows the 'Regex Wizard' interface. It has two tabs: 'Select a Log' and 'Create Regex'. The 'Select a Log' tab is active, showing a search for logs with a 'Last 24 Hours' filter. Below the search results, there is a list of extracted values from a log entry, including fields like 'CALL_ID', 'CALL_METRIC_ID', and 'VARIABLE_NAME'.

This screenshot shows the 'WHERE DOES THE MATCH BEGIN?' section of the 'Regex Wizard'. It contains a text area with a complex regular expression and several checkboxes for matching options: 'Include this text in my capture', 'Match until end of line', and 'Match until end of line'. A 'REGEX GENERATED' section is visible at the bottom.

4.2.8. Delete 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.



4.2.9. Delete 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.

The screenshot shows the 'POLICY CONFIGURATION' interface. On the left, there is a 'Policies' table with columns for Name, Fallover, and a checkbox. The 'Powerwave SNMP Alarms' policy is selected, and its name is italicized. On the right, there is a 'Rules' table with columns for Name, Threshold, Window, Severity, and Response Procedure. A blue arrow points to the 'Save' button in the top right corner.

| Policies | | | Rules | | | | |
|---|-------------------------------------|----|--|-----------|------------|---------------|--------------------|
| Name | Fallover | | Name | Threshold | Window | Severity | Response Procedure |
| <input type="checkbox"/> Cisco Call Monitor | <input checked="" type="checkbox"/> | 4 | <input type="checkbox"/> CLEARED - RPTR Alarm | 1 time | 1 minute | Informational | AlertClear |
| <input type="checkbox"/> LAXDRX Agent Monitor | <input checked="" type="checkbox"/> | 3 | <input type="checkbox"/> CRITICAL - RPTR Alarm | 1 time | 20 minutes | Critical | AlertHold |
| <input type="checkbox"/> Log Monitor | <input checked="" type="checkbox"/> | 1 | <input type="checkbox"/> DISREGARD - FailedNodes | 1 time | 1 minute | Informational | DoNotAlert |
| <input type="checkbox"/> LX1 Call Monitor v2 | <input checked="" type="checkbox"/> | 5 | <input type="checkbox"/> DISREGARD - UnableToRun | 1 time | 1 minute | Informational | DoNotAlert |
| <input type="checkbox"/> LX1 SIP Call Errors v2 | <input checked="" type="checkbox"/> | 6 | <input type="checkbox"/> INDETERMINATE - RPTR Ala... | 1 time | 15 seconds | Informational | DoNotAlert |
| <input type="checkbox"/> Nortel Call Monitor | <input checked="" type="checkbox"/> | 3 | <input type="checkbox"/> ISG Alarm trap - INDETERMI... | 1 time | 1 minute | Informational | DoNotAlert |
| <input type="checkbox"/> PING Monitor | <input checked="" type="checkbox"/> | 2 | <input type="checkbox"/> ISG Alarm trap - MAJOR | 1 time | 1 minute | Major | DoNotAlert |
| <input checked="" type="checkbox"/> Powerwave SNMP Alarms | <input checked="" type="checkbox"/> | 11 | <input type="checkbox"/> ISG Alarm trap - MAJOR | 1 time | 1 minute | Major | DoNotAlert |
| <input type="checkbox"/> Site training policy | <input type="checkbox"/> | 2 | | | | | |
| <input type="checkbox"/> Test Alarm v1 | <input type="checkbox"/> | 1 | | | | | |
| <input type="checkbox"/> AJ Exper/Mental | <input checked="" type="checkbox"/> | 3 | | | | | |
| <input type="checkbox"/> ALSTOYBARN : Alert Exa... | <input checked="" type="checkbox"/> | 9 | | | | | |

4.2.10. Disable or Enable 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.

The screenshot shows the 'POLICY CONFIGURATION' interface. The 'Powerwave SNMP Alarms' policy is selected, and its name is italicized. A blue arrow points to the green checkmark at the bottom of the policy row. A yellow banner at the top indicates 'Changes have been made'.

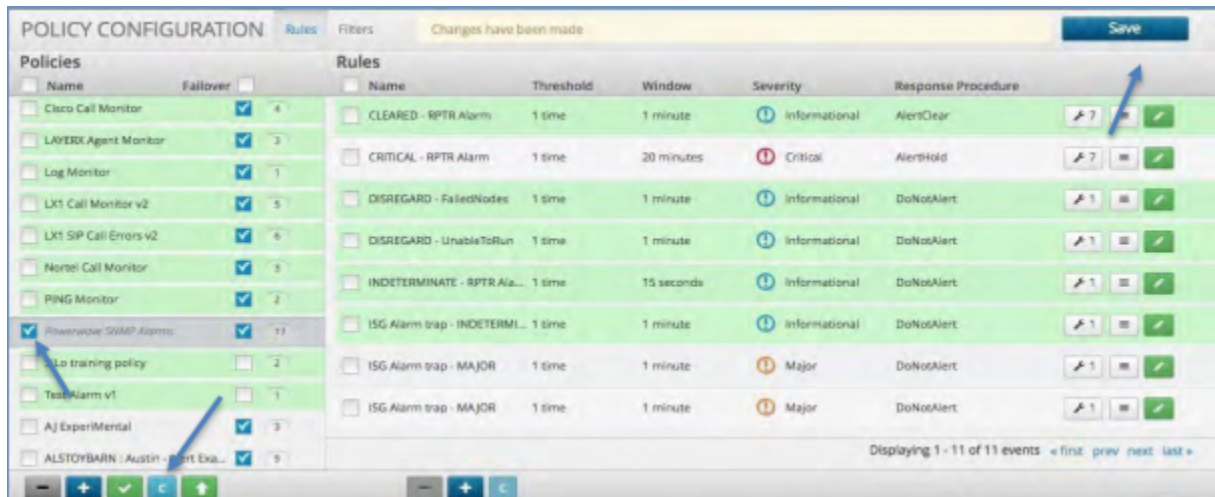
| Policies | | | Rules | | | | |
|--|-------------------------------------|----|--|-----------|------------|---------------|--------------------|
| Name | Fallover | | Name | Threshold | Window | Severity | Response Procedure |
| <input type="checkbox"/> Cisco Call Monitor | <input checked="" type="checkbox"/> | 4 | <input type="checkbox"/> CLEARED - RPTR Alarm | 1 time | 1 minute | Informational | AlertClear |
| <input type="checkbox"/> LAXDRX Agent Monitor | <input checked="" type="checkbox"/> | 3 | <input type="checkbox"/> CRITICAL - RPTR Alarm | 1 time | 20 minutes | Critical | AlertHold |
| <input type="checkbox"/> Log Monitor | <input checked="" type="checkbox"/> | 1 | <input type="checkbox"/> DISREGARD - FailedNodes | 1 time | 1 minute | Informational | DoNotAlert |
| <input type="checkbox"/> LX1 Call Monitor v2 | <input checked="" type="checkbox"/> | 5 | <input type="checkbox"/> DISREGARD - UnableToRun | 1 time | 1 minute | Informational | DoNotAlert |
| <input type="checkbox"/> LX1 SIP Call Errors v2 | <input checked="" type="checkbox"/> | 6 | <input type="checkbox"/> INDETERMINATE - RPTR Ala... | 1 time | 15 seconds | Informational | DoNotAlert |
| <input type="checkbox"/> Nortel Call Monitor | <input checked="" type="checkbox"/> | 3 | <input type="checkbox"/> ISG Alarm trap - INDETERMI... | 1 time | 1 minute | Informational | DoNotAlert |
| <input type="checkbox"/> PING Monitor | <input checked="" type="checkbox"/> | 2 | <input type="checkbox"/> ISG Alarm trap - MAJOR | 1 time | 1 minute | Major | DoNotAlert |
| <i><input checked="" type="checkbox"/> Powerwave SNMP Alarms</i> | <input checked="" type="checkbox"/> | 11 | <input type="checkbox"/> ISG Alarm trap - MAJOR | 1 time | 1 minute | Major | DoNotAlert |
| <input type="checkbox"/> Site training policy | <input type="checkbox"/> | 2 | | | | | |
| <input type="checkbox"/> Test Alarm v1 | <input type="checkbox"/> | 1 | | | | | |
| <input type="checkbox"/> AJ Exper/Mental | <input checked="" type="checkbox"/> | 3 | | | | | |
| <input type="checkbox"/> ALSTOYBARN : Alert Exa... | <input checked="" type="checkbox"/> | 9 | | | | | |

4.2.11. Clone 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.



4.2.12. Export or 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.

+ Global Filters (0 applied)

[Click to Refresh Data](#)

Mar 9, 2022 9:09 am - Mar 9, 2022 10:09 am

| System log | | | | | | | |
|------------|---------------------------------------|----------|--------|--------|---------|----------|--|
| Search | | | | | | | |
| | txt 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} |

Export a Policy

1. Select the check boxes of the policies to export, or select the **Name** check box at the top of the **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.

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)"
```

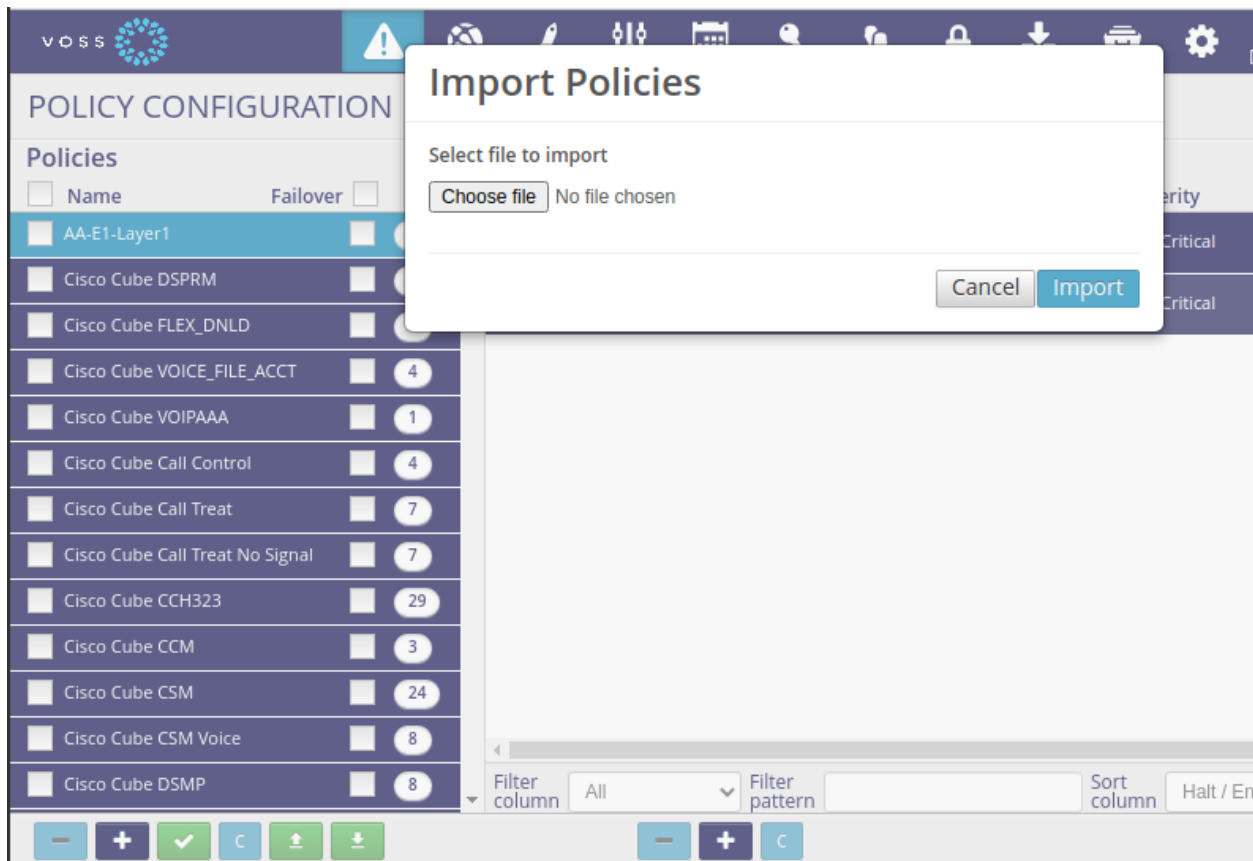
Note:

- 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](#).



4.3. Asset Configuration

4.3.1. Overview

On the **Asset Configuration** tab you can add, edit, and remove assets and asset groups, import or export assets, and configure monitor profiles.

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.

| IP Address | Asset Name | Description | Type | Monitor Profile |
|---------------|--------------|---------------------------|---------|-----------------|
| * | * | | Unknown | No profiles set |
| XXXXXXXX.173 | Local System | Local Arbitrator Platform | Server | 1 profile set |
| 127.0.0.1 | 127.0.0.1 | | Unknown | No profiles set |
| XXXXXXXX3.140 | XXXXXXXX140 | | Unknown | No profiles set |
| CUCM_1 | CUCM_1 | | Unknown | No profiles set |
| CUCM_2 | CUCM_2 | | Unknown | No profiles set |
| CUCM_3 | CUCM_3 | | Unknown | No profiles set |
| CUCM_4 | CUCM_4 | | Unknown | No profiles set |
| CUCM_5 | CUCM_5 | | Unknown | No profiles set |
| CUCM_6 | CUCM_6 | | Unknown | No profiles set |

Note: A system log table (`insights_system_log`) logs user actions, and a user can create a dashboard to view these actions.

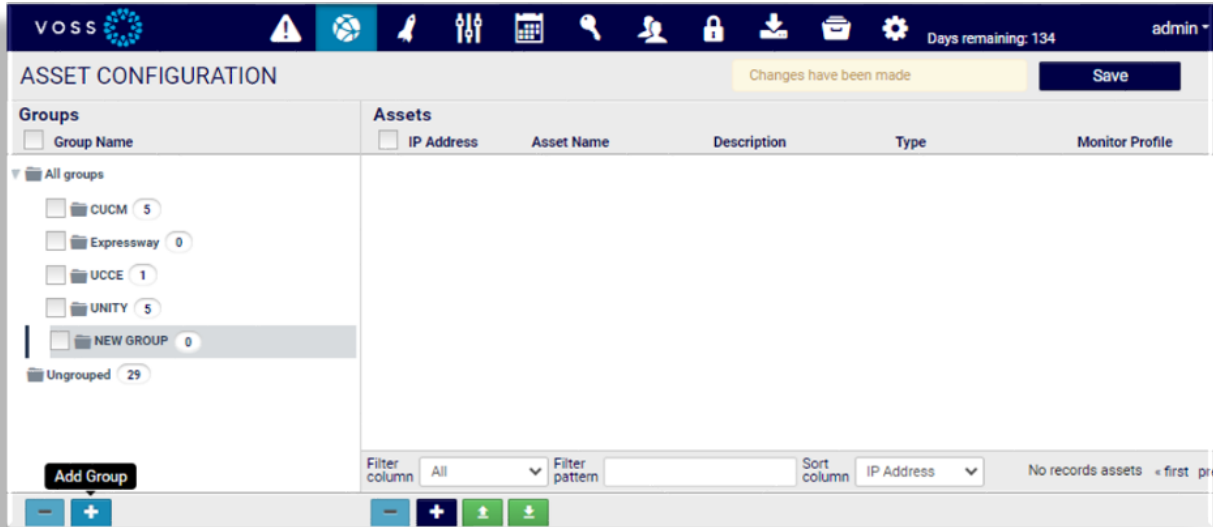
Related Topics

Log Search in the Dashboard Administration Guide

4.3.2. Add an Asset Group

To add a new asset group:

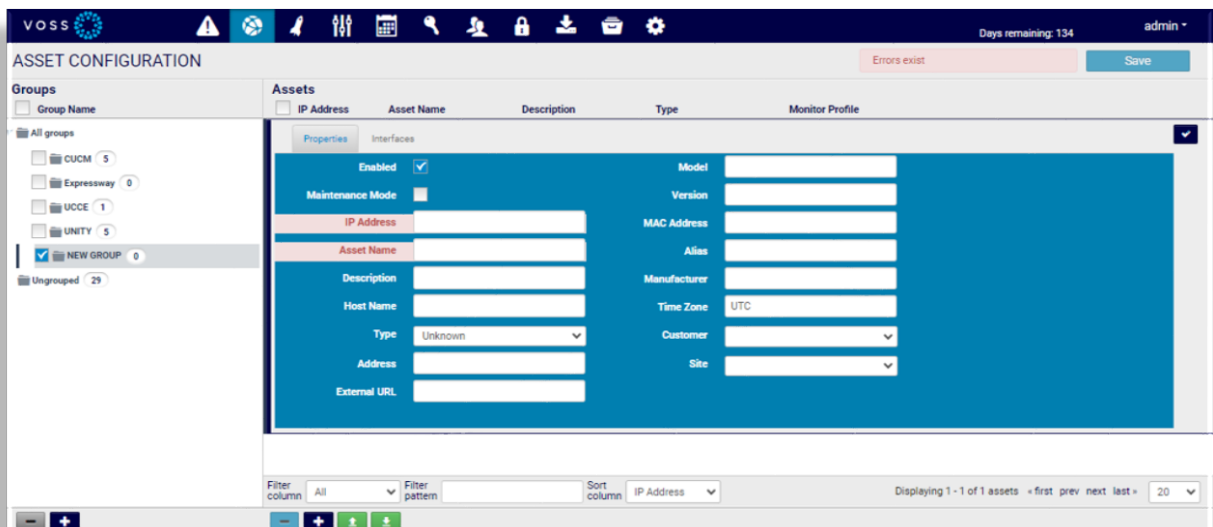
1. On the **Asset Configuration** tab, click the Plus icon (+) at the bottom left corner of the **Groups** panel.
2. Click in the new folder created in the panel, fill out a group name, and press **Enter**.
3. Save your changes.



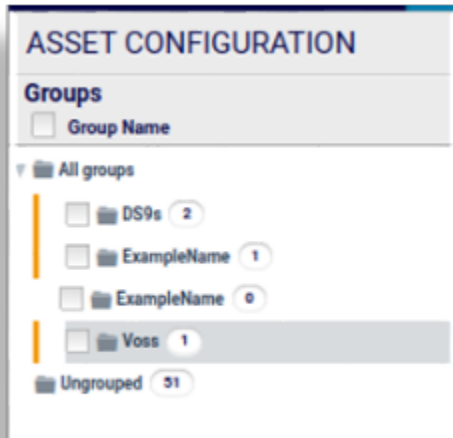
4.3.3. Add an Asset to a Group

To add a new asset to a group:

1. On the **Asset Configuration** tab, select the asset group where you want to add an asset.
2. Click the Plus icon (+) at the bottom of the **Assets** panel.
3. On the **Properties** tab for the new asset, fill out at least the mandatory fields, **IP Address** and **Asset Name**, then select an asset type, if know, for example, group, router, firewall switch, or one of the other asset types listed in the drop-down.
4. On the **Interfaces** tab for the new asset, add new interfaces, one or more.
5. Click the **Check** icon to the right of the asset details panel to add the new asset.
6. Save your changes.



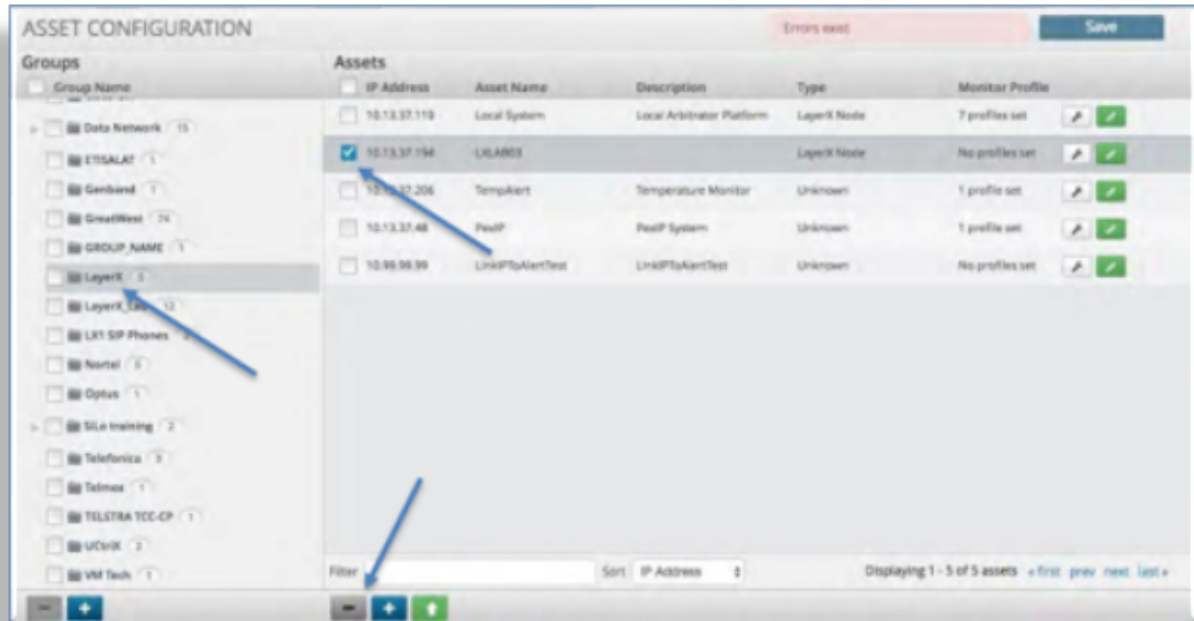
Note: Modification: If present, then more than one asset in more than one group can be modified when *modifying* assets. Change bars are displayed next to each asset and group when the assets or groups modified, for example:



4.3.4. Delete Assets

To delete assets in an asset group:

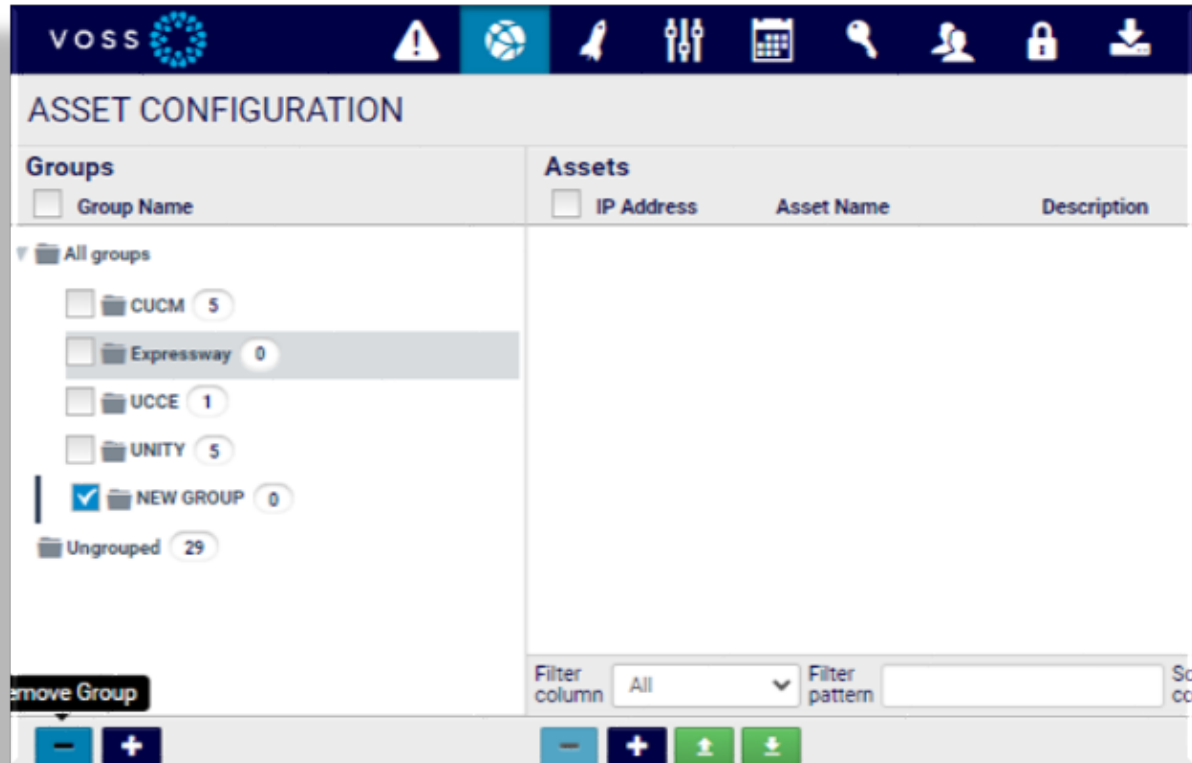
1. On the **Asset Configuration** tab, select the relevant group to display its assets.
2. From the **Assets** panel, select the checkbox for each asset in the group that you wish to remove (one or more).
3. Click the **Minus** icon (-) at the bottom of the **Assets** panel.
4. Click **Save**.



4.3.5. Delete an Asset Group

To delete an asset group:

1. On the **Asset Configuration** tab, select the asset group you wish to delete (one or more).
2. Click the **Minus** icon (-) at the bottom of the **Groups** panel.
3. Click **Save**.



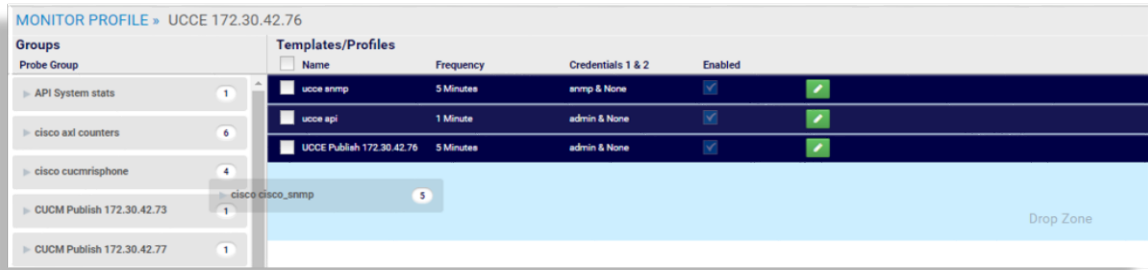
4.3.6. Assign a Probe to an Asset

A probe is a script or set of commands that are saved in the system and can be used to gather data, to issue commands to systems, and to 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 used to retrieve data from a particular asset.

To assign a probe to an asset:

1. On the **Asset Configuration** tab, select the relevant asset group to display its assets.
2. In the **Assets** panel, select the relevant asset in the group that the probe will run against, then click the **Wrench** icon for the asset to open the **Monitor Profile** screen, where you can add a monitor profile to the asset.
3. On the **Monitor Profile** screen, view available saved probes.
4. From the **Probe Group** pane, select and then drag the probe you want to assign to the asset to the **Template/Profiles** panel.



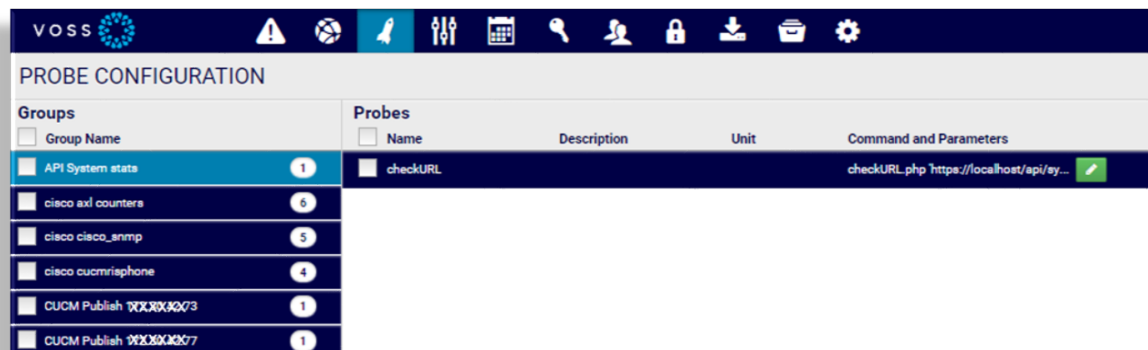
5. Click the **Edit** icon (Green Pencil) at the relevant profile entry in the **Template/Profiles** panel (the probe group you dragged to the panel).
6. Edit the profile to define the frequency the probe runs, the credentials needed for the probe to run, the schedule for the probe to run. You can also choose to start it immediately.

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

7. Click **Update** to save your changes and to return to the **Asset Configuration** tab.

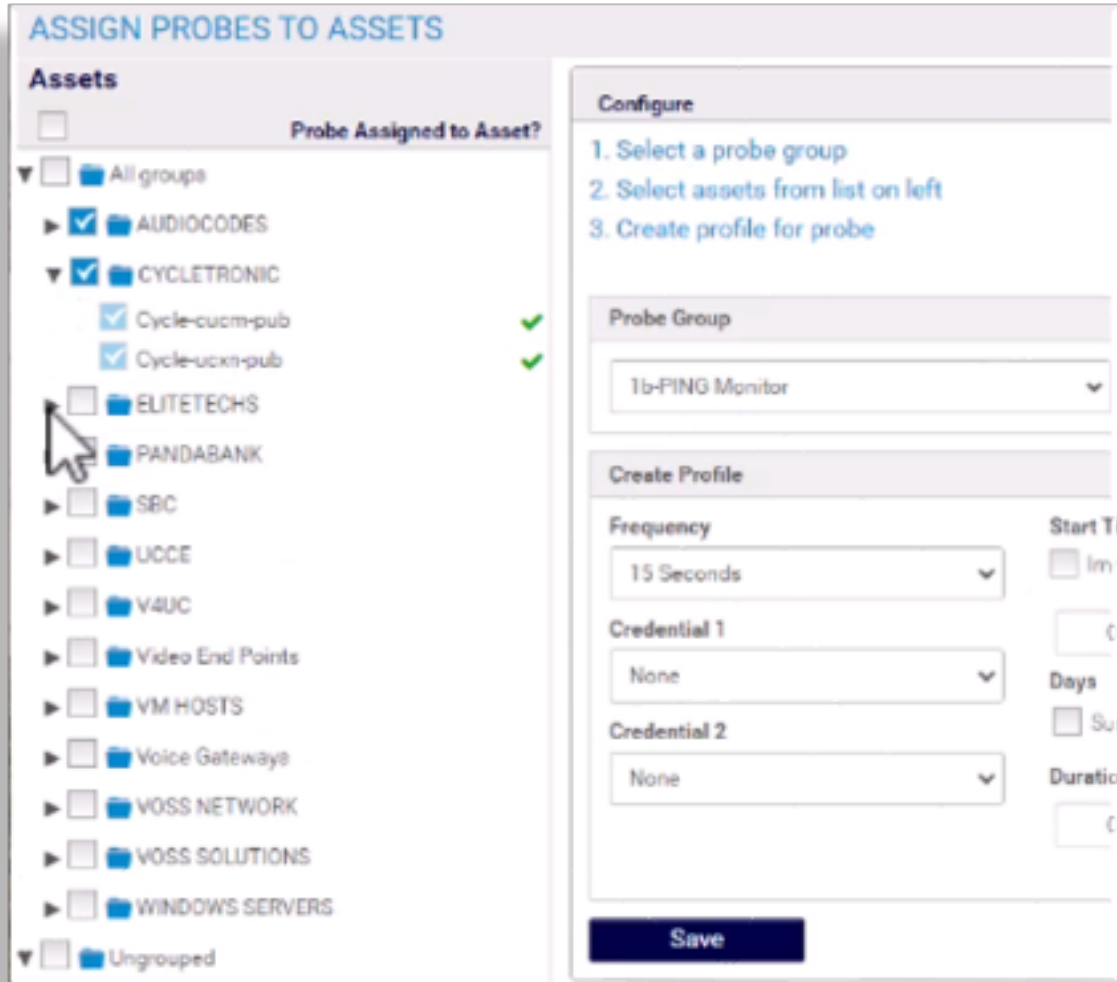
4.3.7. Bulk Assign Probes to an Asset

1. In the Arbitrator **System Configuration** Gui, select the **Probes** icon to open the **PROBE CONFIGURATION** tab.



2. Click the Globe icon at the bottom of the **Groups** panel to open the **ASSIGN PROBES TO ASSETS** page.
3. From the **Probe Group** drop-down in the **Configure** panel, select a probe group.
4. From the **Assets** panel, expand the tree and select the checkbox for each asset where you want to assign the selected probe group.

Note: A green check mark adjacent to any asset indicates an existing assignment.



5. In the **Configure** panel, at **Create Profile**, configure frequency and credentials.
6. Click **Save** to assign the probe to all the assets you selected.

4.3.8. Assign a Customer to an Asset

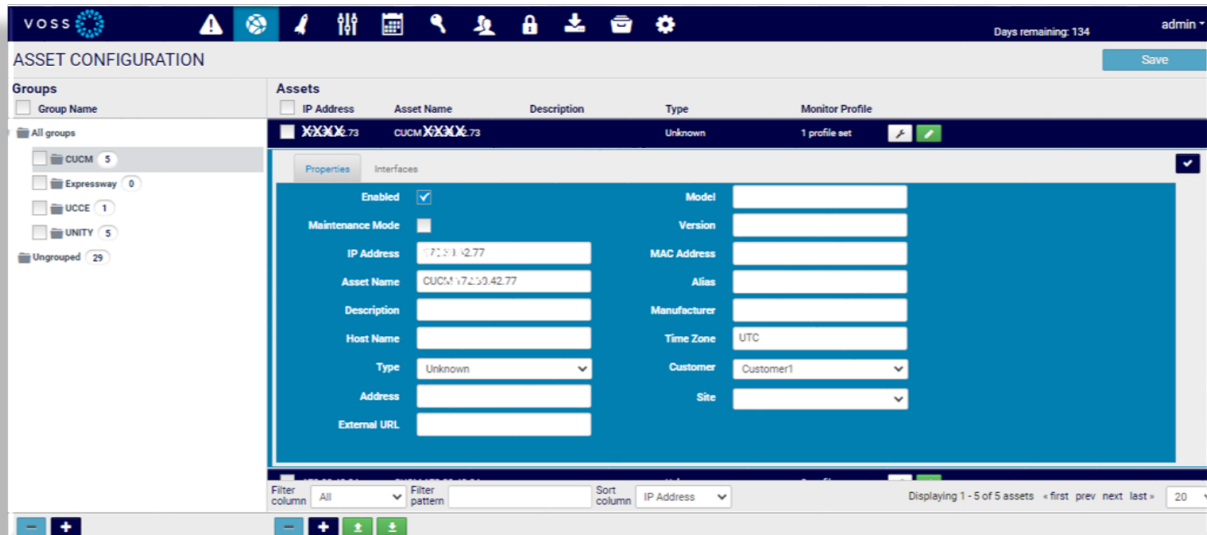
Arbitrator ships with multi-tenancy, which allows different customers to see correlated or collected results of only their data.

Within the configuration of assets, you can assign each asset to a specific customer.

To assign a customer to an asset:

1. On the **Asset Configuration** tab, click the relevant asset group to display its assets.
2. In the **Assets** panel, click the Edit icon (pencil) for the relevant asset to open its configuration screen.
3. On the **Properties** tab, click the down-pointing arrow at the **Customer** drop-down to view available customers.
4. Select the customer that the asset belongs to, then click the Blue Check Mark icon at the top right of the panel to update the configuration.

5. Click **Save**.

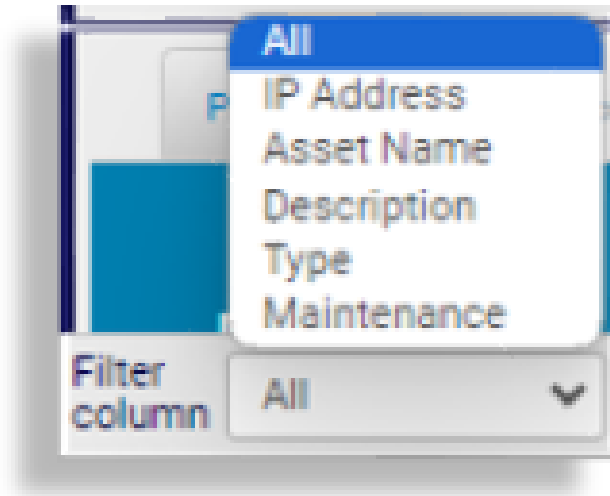


4.3.9. Place an Asset in Maintenance Mode

Arbitrator allows any asset to be placed into maintenance mode. Placing an asset in maintenance mode stops Arbitrator from responding with alerts until the asset is removed from maintenance mode. Data is still collected, but no alerts are sent when an asset is in maintenance mode.

1. On the **Asset Configuration** tab, select the asset group to display its assets.
2. Select the asset you wish to place into maintenance mode.
3. Click the Pencil icon for the selected asset to open its configuration screen.
4. On the **Properties** tab, select the **Maintenance Mode** checkbox, then select the Blue Check Mark at the top right of the panel to update the configuration.
5. Click **Save** to save the maintenance mode settings.

Note: You can filter the **Assets** panel to display any assets in maintenance mode by selecting **Maintenance** from the **Filter column** drop-down at the bottom of the **Assets** panel.



4.3.10. Export and Import Assets

On the **ASSET CONFIGURATION** tab you can export and import an asset that you exported from another system.

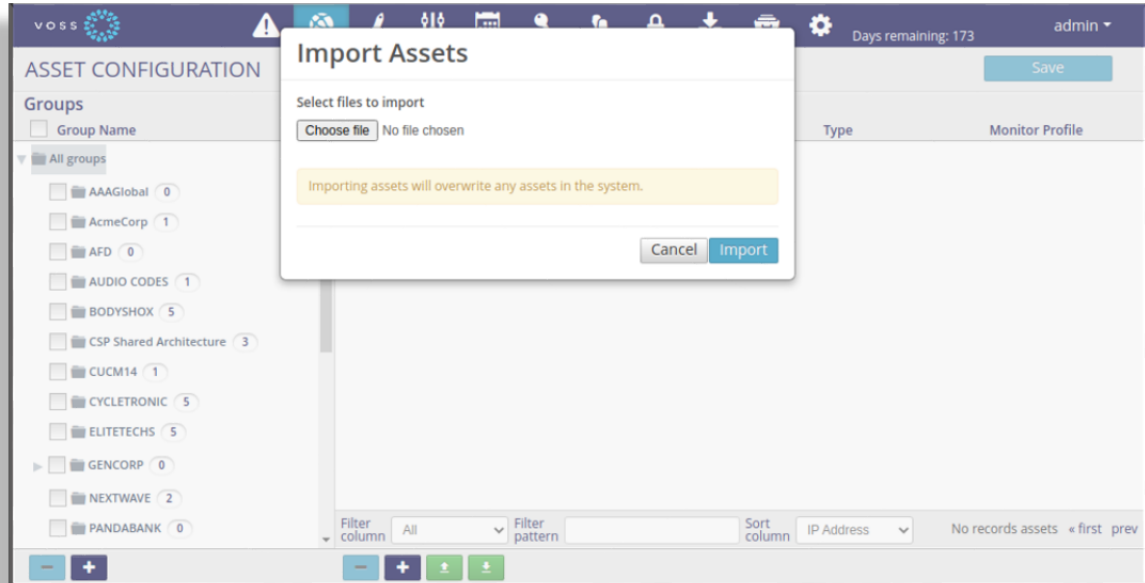
- When selecting asset groups, all assets belonging to those groups are selected (selecting individual assets will not take effect).
- If the **Group Name** checkbox is selected, all assets are included - both **All groups** and **Ungrouped**.

Export Assets

1. On the **Asset Configuration** tab, select a group to display its assets, and select relevant assets for the group. Alternatively, select **Group Name** at the top of the **Groups** pane to select all assets in all groups.
2. Click the **Export Assets** button (green down arrow at the bottom of the **Assets** panel) to launch the **Export CSV** dialog.
3. Fill out a CSV filename. You won't need to fill out the file extension, `.csv`.
4. Click **Export** to create the export file, then view progress until the **Export finished** dialog displays.
5. Click **Download**. The CSV file is saved to a download location you choose.

Import Assets

1. On the **Asset Configuration** tab, click the **Import Assets** button (green up arrow at the bottom of the **Assets** panel) to launch the **Import Assets** dialog.
2. Click **Choose File**, then browse to an exported (and optionally modified) CSV file on your local computer.



3. Click **Import**.

Next steps

- Assign probes to the imported assets - see *Assign a Probe to an Asset* in this guide.

Asset CSV Format

The following columns are in an exported CSV file:

```
"Asset Name",Description,"IP Address","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:

- Mandatory fields are: Asset Name, IP Address.
- 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).
-

4.4. Probe Configuration

4.4.1. Overview

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.

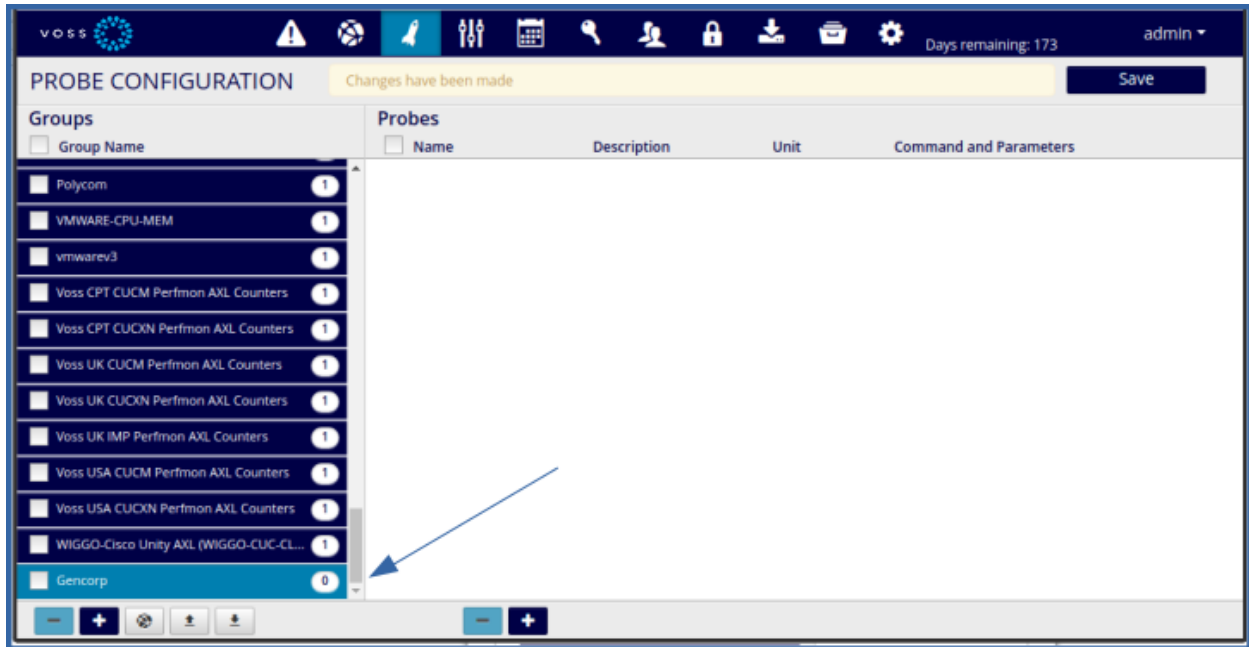
For PRI and SIP Trunk probes for Cisco Voice Gateways, reference:

Arbitrator Cisco PRI and SIP Probe Configuration

4.4.2. Add 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.



4.4.3. Clone a Probe Group

To clone an existing Probe Group:

1. Click the Probe icon from the Menu bar.
2. Select a Probe group to clone from.
3. Click the “C” icon within the Groups pane in the bottom left corner.
4. The cloned “Group” name shows: *<source group name> clone*. Modify this name to the required name.
5. Click the “Save” icon to save the added Probe.
6. The probes contained in this new group can also be modified. Refer to the steps to add, clone and modify probes.

The screenshot displays the Voss Probe Configuration interface. At the top, there is a navigation bar with the Voss logo, a warning icon, a globe, a person icon, a calendar, a key, a person icon, a lock, a download icon, a folder icon, and a gear icon. The user is logged in as 'admin' and has 1684 days remaining. The main title is 'PROBE CONFIGURATION' with a 'Save' button on the right.

The interface is divided into two main sections: 'Groups' and 'Probes'.

Groups: A list of groups with checkboxes and counts:

| Group Name | Count |
|-------------------------------------|-------|
| 1-Cisco CUCM RIS CmDevice_creds | 3 |
| 1b-PING Monitor | 1 |
| 4-Cisco CUCM Version | 1 |
| 5-Cisco RTMT | 1 |
| 6.Cisco Expressway-API | 2 |
| 6a.Cisco Expressway Call Detail-API | 1 |
| 6b.Cisco Expressway - SNMP | 2 |
| 7.CUCM Perfmom AXL Counters | 1 |
| 8.Cisco Unity Perfmom AXL Counters | 1 |
| 9.Cisco IIMP Perfmom AXL Counters | 1 |
| 9a.CUCM-END USER | 1 |
| 9b.VOSS4UC | 1 |

Probes: A table of existing probes:

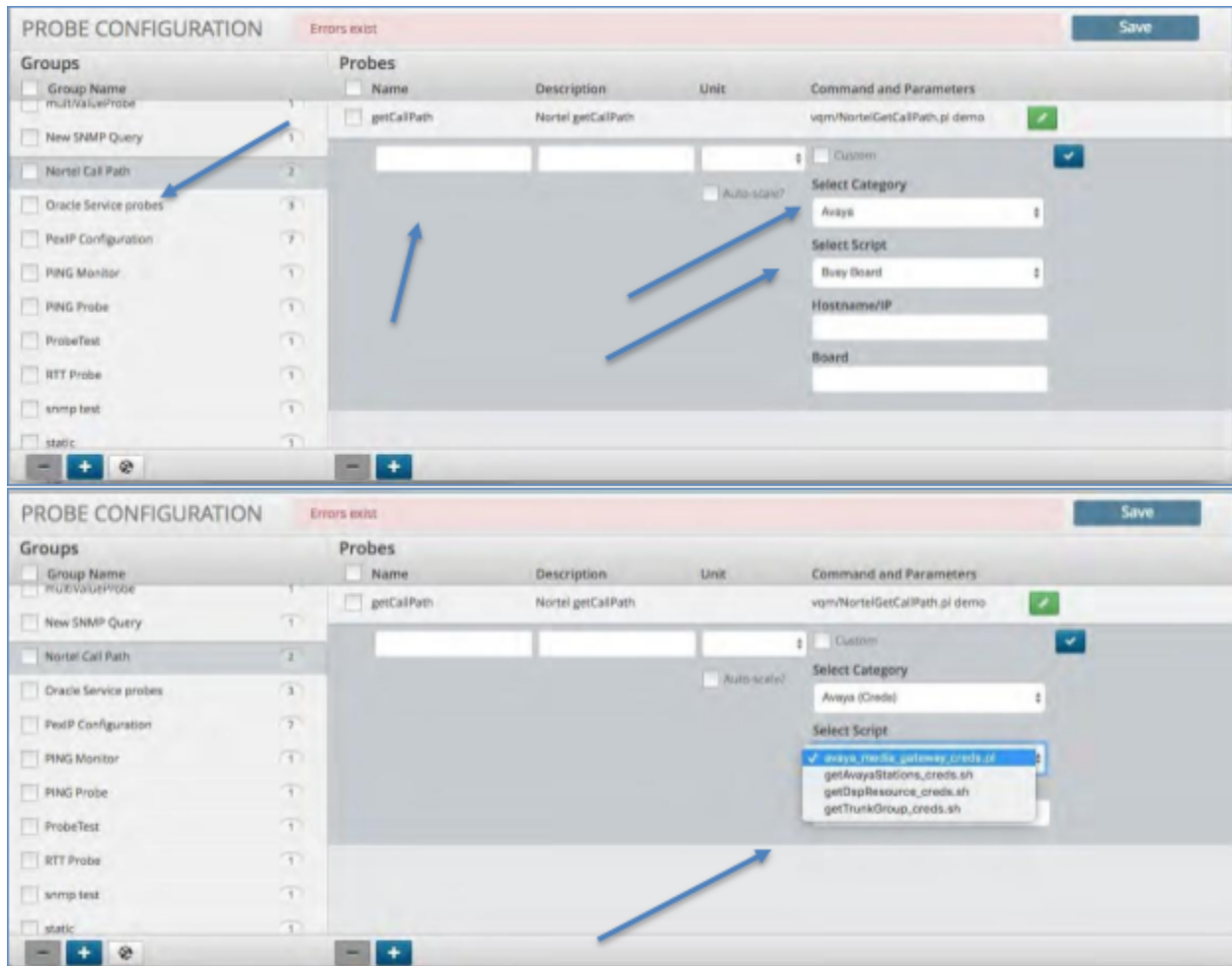
| Name | Description | Unit | Command and Parameters |
|-----------------|---------------------------------|------|---|
| RIS API data | phone, media resources, SIP ... | | cisco/cucmrissipphone/collectrissipho... |
| SIP Trunk | | | cisco/cucmrissiptrunk/collectrissiptru... |
| Media Resources | | | cisco/cucmrissimediaresources/collectr... |

At the bottom of the interface, there are two panels. The left panel has a 'clone' button (a blue square with a white 'C'). The right panel also has a 'clone' button. A red arrow labeled 'clone' points from the 'clone' button in the right panel to the 'clone' button in the left panel.

4.4.4. Create 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.



4.4.5. Clone a Probe

Since devices such as CUCM and Unity Connection require dedicated probes, it is useful to clone (create a copy) and modify an existing probe for this purpose.

To clone a probe:

1. Click the probe from which you wish to clone.

Note: Insights also provides a list of templates that can be cloned for the specific purpose.

2. Click the **Clone probe** icon (C) at the bottom of the **Probes** panel.
3. The clone is created, displaying with naming format, *<source probe name> clone*. Modify this name to the required name, and update any other required properties.

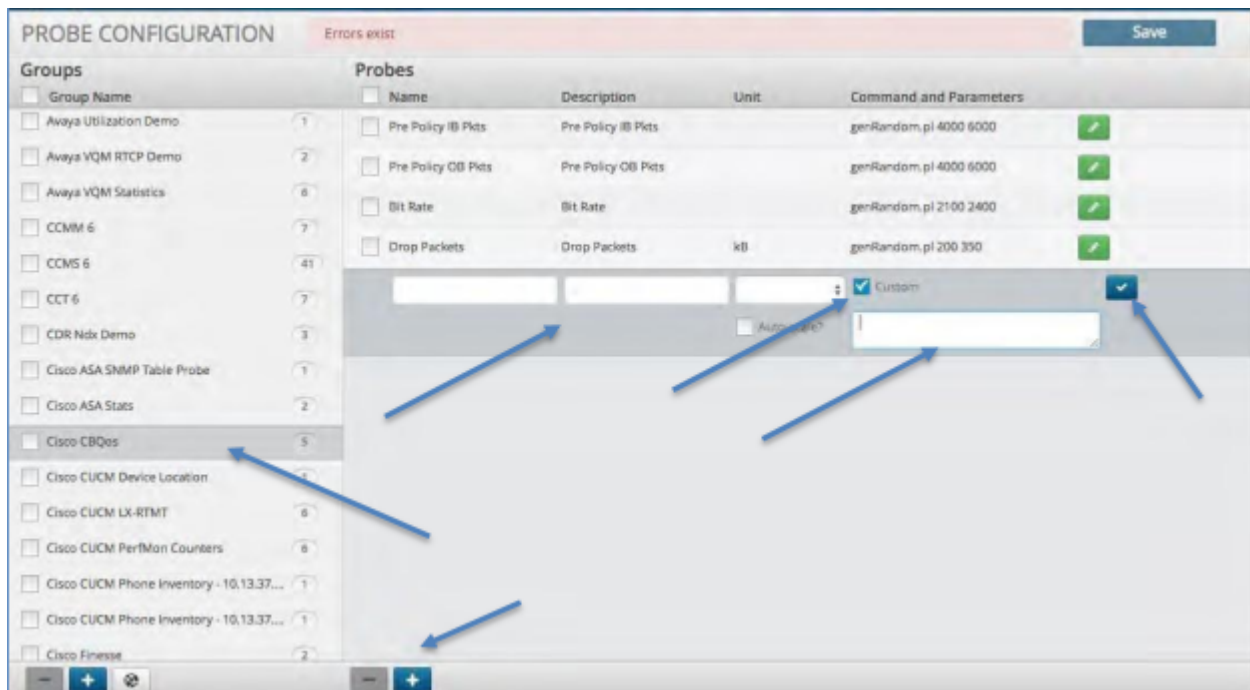
Note: For a CUCM probe, this typically includes **Cucm Ip Address**.

4. Click the **Done** icon (blue check mark to the right of the clone's properties panel).
5. Click **Save** to add the new probe created from the clone.

4.4.6. Create a Custom Probe

To create a new Probe:

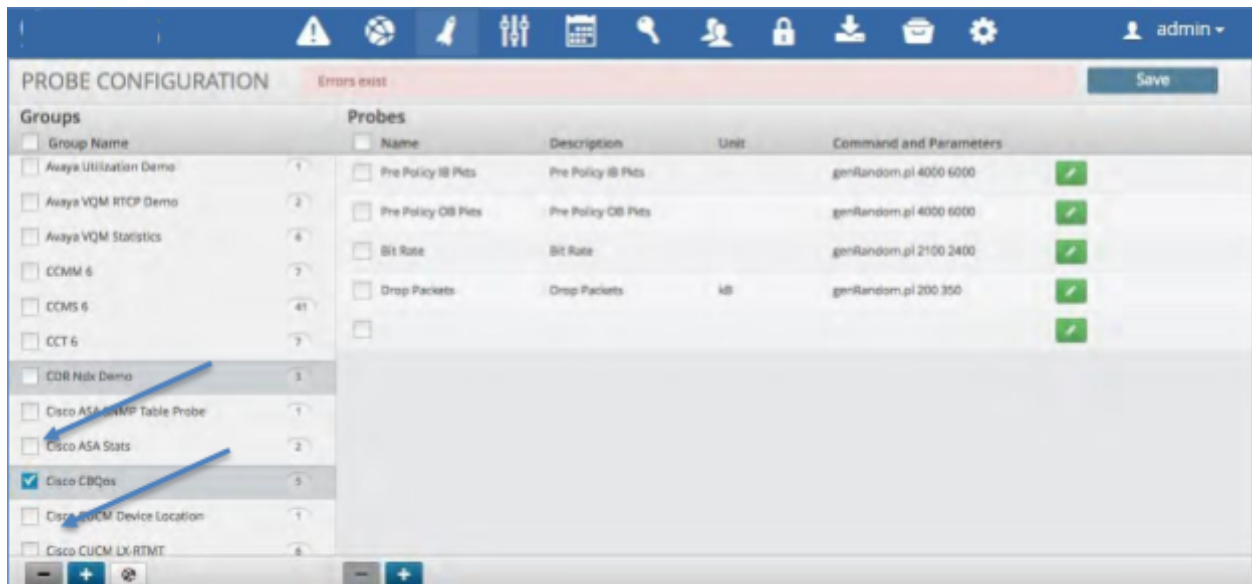
1. Click the group in which you wish to create a new Probe.
2. Click the Plus icon within the Probes panel.
3. Enter the name and description of the Probe.
4. Select and click the check icon from the field titled "Custom". This field is utilized when putting a custom probe in place versus utilizing the 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.



4.4.7. Delete a Probe Group

To delete a Probe Group:

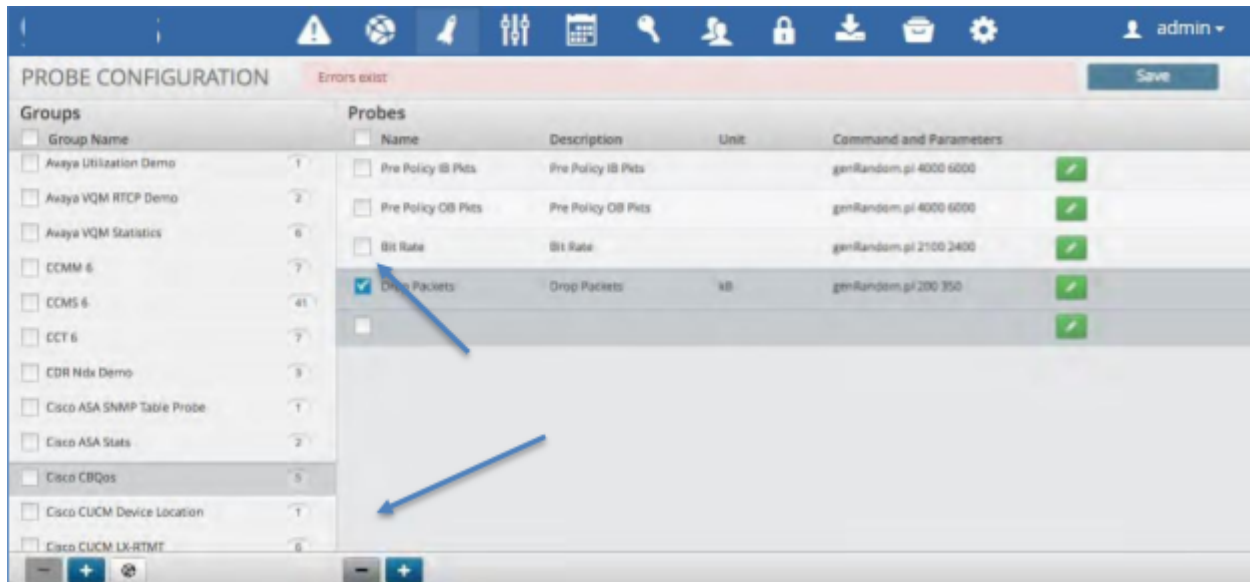
1. Click the check box next to the group name you wish to delete.
2. Click the Minus icon within the Probe Group panel in the bottom left.
3. Click the “Save” icon to save the changes.



4.4.8. Delete 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.



4.4.9. Export and Import a Profile

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.

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.

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.

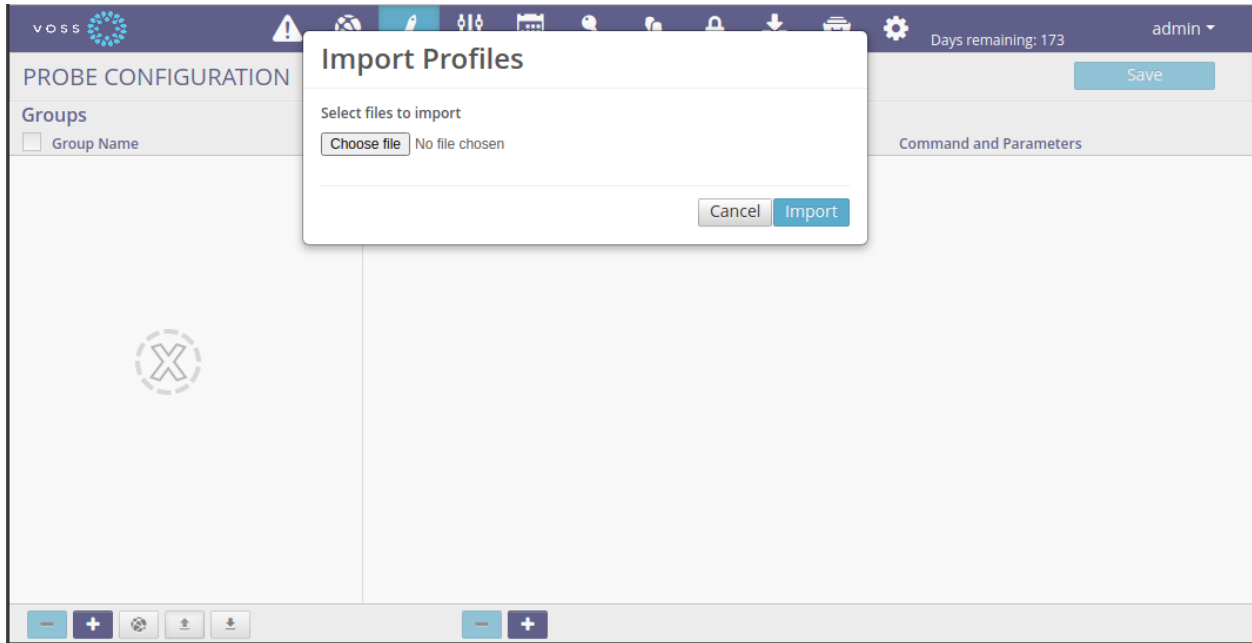
Profile CSV Format

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.
-



Assign 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:

MONITOR PROFILE > Local System

| Groups | | Templates/Profiles | | | |
|---|---|---|-----------|-------------------|-------------------------------------|
| Probe Group | | <input type="checkbox"/> Name | Frequency | Credentials 1 & 2 | Enabled |
| » Cisco CUCM Version | 1 | <input type="checkbox"/> Local System Stats | 1 Minute | None & touy | <input checked="" type="checkbox"/> |
| » Cisco Expressway | 3 | <input type="checkbox"/> Test Probe | 1 Minute | None & loc | <input checked="" type="checkbox"/> |
| » Cisco Telepresence API - Call Details | 1 | <input type="checkbox"/> PING Monitor | 1 Minute | ray & loc | <input checked="" type="checkbox"/> |

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.

MONITOR PROFILE » Local System

| Groups | | Templates/Profiles | | | |
|---|---|---|-----------|-------------------|-------------------------------------|
| Probe Group | | <input type="checkbox"/> Name | Frequency | Credentials 1 & 2 | Enabled |
| ▶ Cisco CUCM Version | 1 | <input type="checkbox"/> Local System Stats | 1 Minute | None & touy | <input checked="" type="checkbox"/> |
| ▶ Cisco Expressway | 3 | <input type="checkbox"/> Test Probe | 1 Minute | None & loc | <input checked="" type="checkbox"/> |
| ▶ Cisco Telepresence API - Call Details | 1 | <input type="checkbox"/> PING Monitor | 1 Minute | ray & loc | <input checked="" type="checkbox"/> |
| | | <input type="checkbox"/> Cisco CUCM Version | 1 Minute | ray & loc | <input checked="" type="checkbox"/> |

4.5. Controls

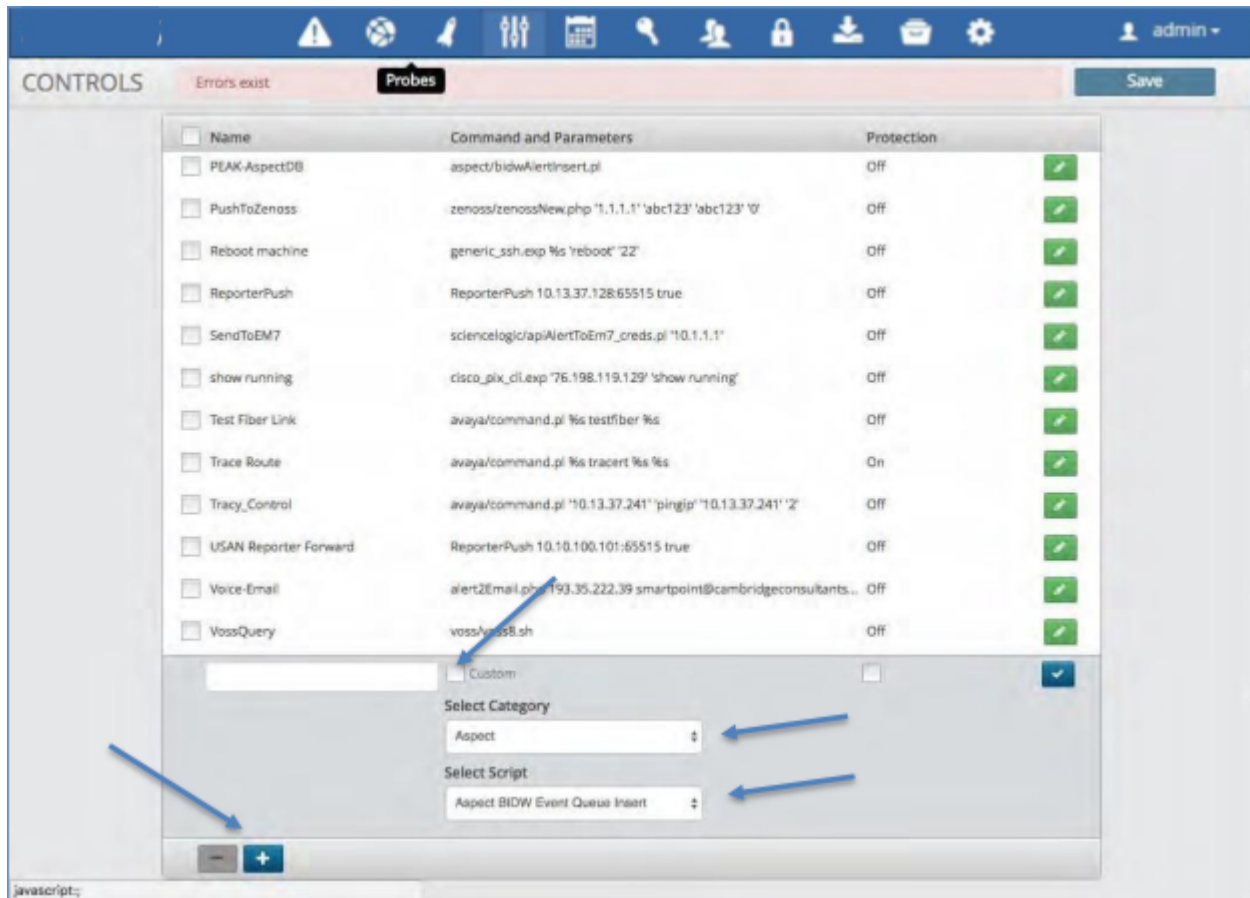
4.5.1. Overview

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.

4.5.2. Create a Control

To create a new Control:

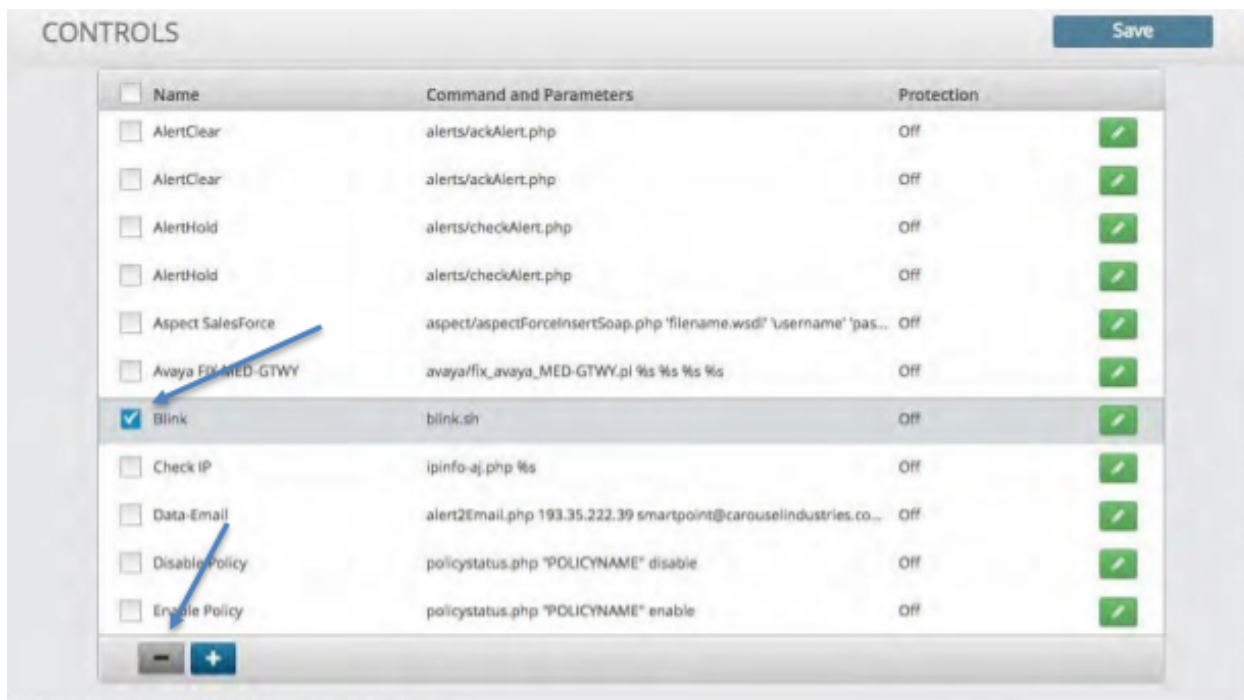
1. Click the Plus icon within the control panel.
2. Enter the name of the Control.
3. De-select the check icon from the field titled "Custom". This field is utilized when putting a custom Control in place versus utilizing the ones within the system.
4. Click and Select from the categories dropdown list 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.



4.5.3. Delete 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.



4.6. Response Procedure Configuration

4.6.1. Overview

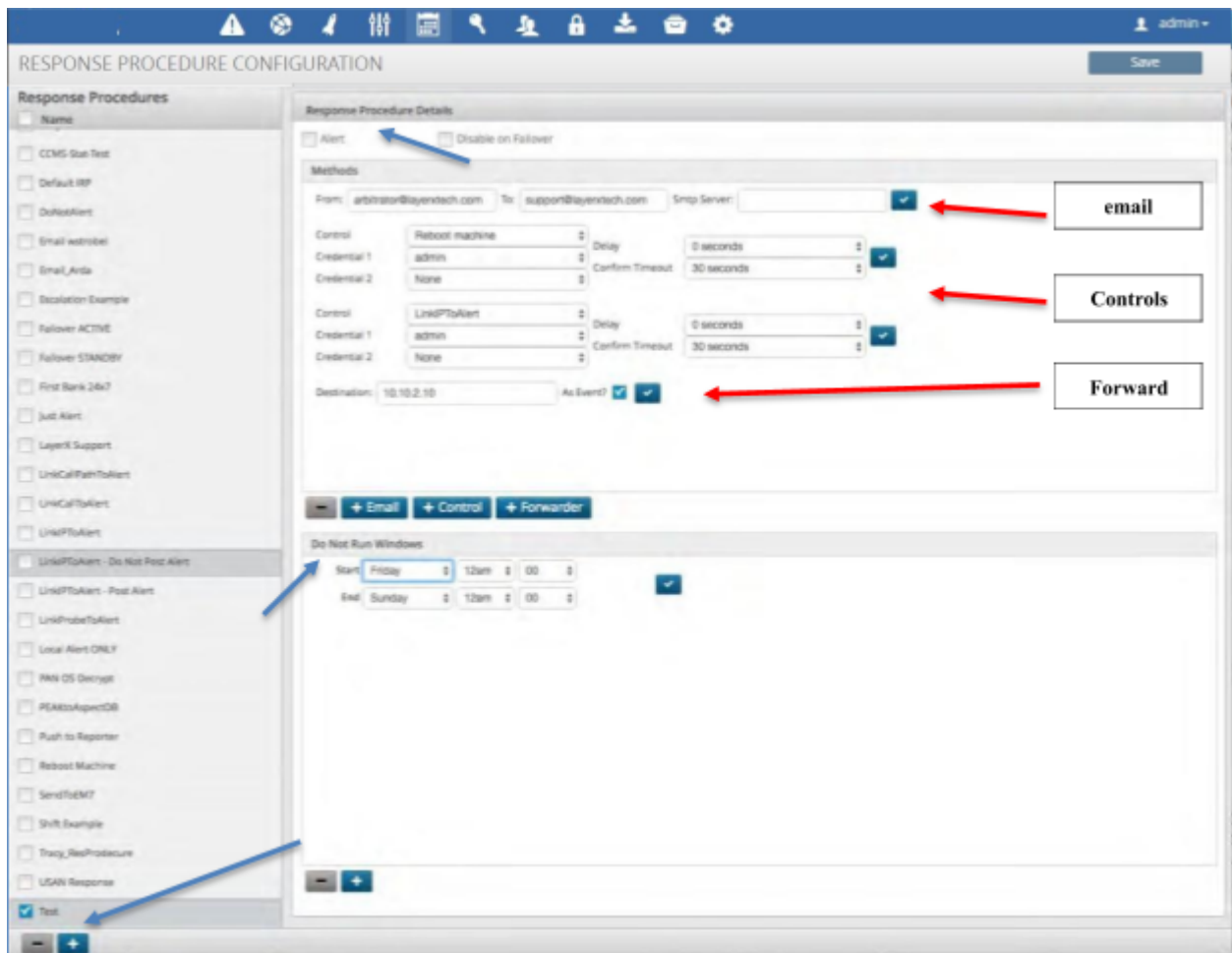
The Response Procedure configuration panel allows you to define an automated response to a correlated event. Each Response Procedure can be assigned to one or more Correlation Rules while also containing and/or executing one or more of the following responses:

| 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. |

4.6.2. Create a Response Procedure

To create a response procedure:

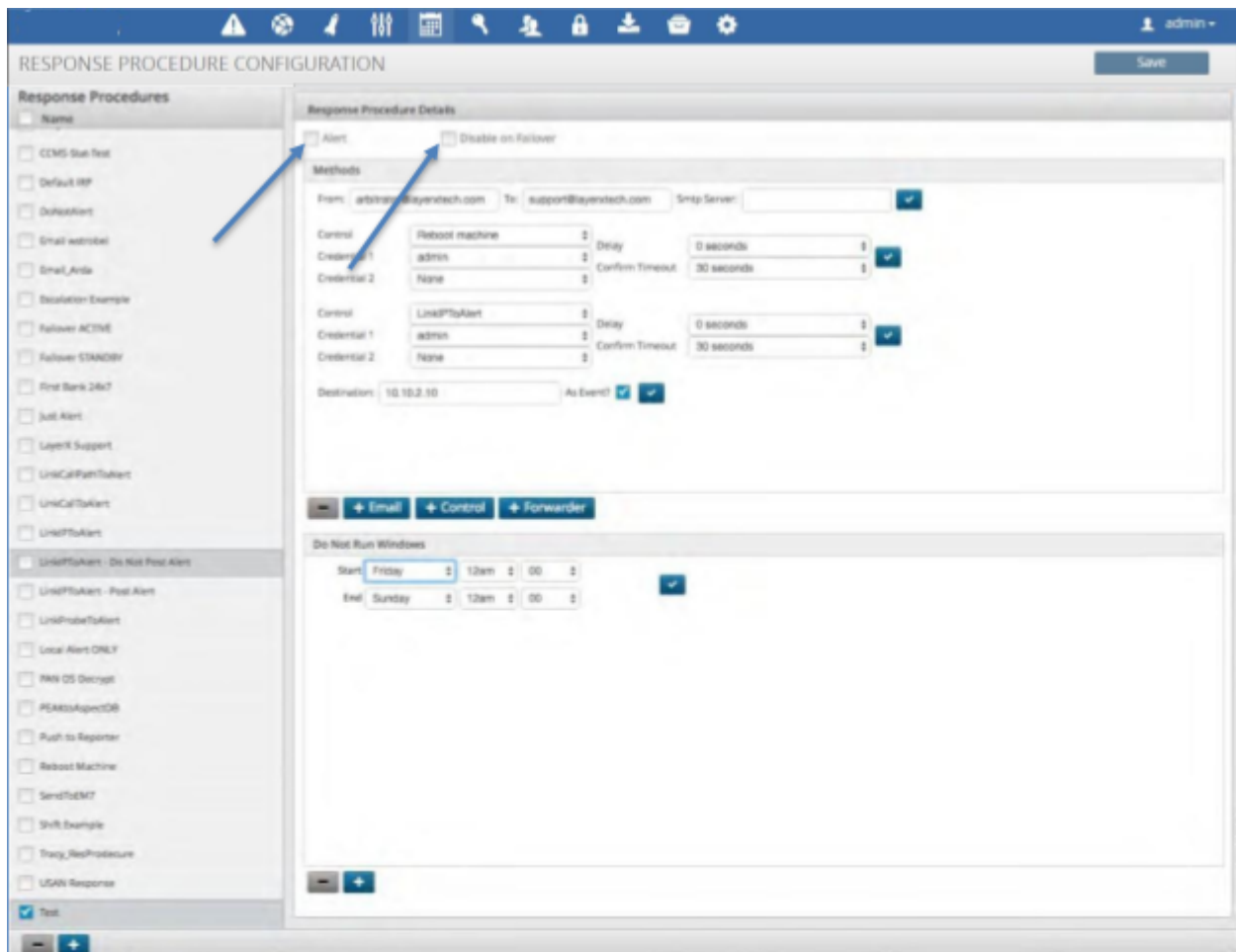
1. Click the “Calendar” icon at the top of the Configuration panel.
2. Click the plus icon in the bottom left of the Response Procedure name panel. A box will open up where you can fill in the name of your response procedure.
3. The panel to the right is broken into two sections:
 - a. Response Procedure 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.



4.6.3. Assign an Alert to a Response Procedure

To assign the Alert function to a response procedure:

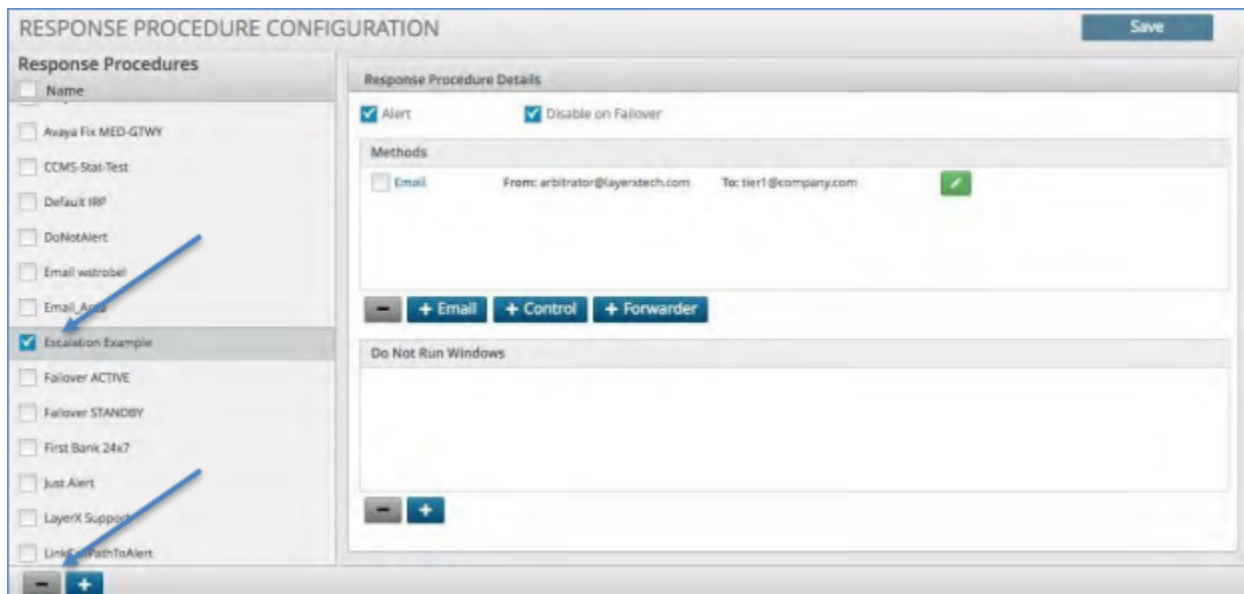
1. Click the Alert check box in the top left of the Response Procedure Details panel.
2. If this system you are configuring is intended to be the redundant platform then click the Disable on Failover box to allow all data to flow but no actions to take place.








4.6.4. Delete 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.



4.6.5. Enable ServiceNow Integration

| <input type="checkbox"/> Name | Command and Parameters | Protection | |
|--|---------------------------------------|--------------------------|---|
| <input type="checkbox"/> LinkIPToAlert | LinkIPToAlert | Off |  |
| <input type="checkbox"/> ReporterPush Reading | ReporterPush 172.30.15.121:65515 true | Off |  |
| <input type="checkbox"/> ReporterPush-GC | ReporterPush 172.25.87.6:65515 true | Off |  |
| <input type="checkbox"/> VpnSyslog | vpnSyslogAlert.sh | Off |  |
| <input type="checkbox"/> <input type="text" value=""/> | <input type="checkbox"/> Custom | <input type="checkbox"/> |  |
| Select Category <input type="text" value="ServiceNow"/> | | | |
| Select Script <input type="text" value="PushToServiceNow"/> | | | |
| Service Now IP Address / Hostname <input type="text" value=""/> | | | |
| Service Now Username <input type="text" value=""/> | | | |
| Service Now Password <input type="text" value=""/> | | | |

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. Uncheck **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.

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

ServiceNow images:

4.6. Response Procedure Configuration

Incident Details: INC0010023

Configuration item:

Assignment group:

Assigned to:

* Short description: LXTALERT: ARB_REFERENCEID=20000-01009001-00-01-7134-14 ARB_POLICY_MODULE=MultiTest ARB_CORRELATION_RULE=Some Rule

Related Search Results:

- Automatic Replies (Out Of Office)** on. Click the File tab. Click Automatic Replies. Click Rules, and then click Add Rule. Under... for the rule to be applied. If you want to specif... Preview Attach
- Firewall Rule Change** Cisco Firewall Appliance Preview Order
- About Windows 10** the microphone to talk with her instead. Rule the web with Microsoft Edge Microsoft Edge is the first browser Preview Attach

Notes | Related Records | Closure Information

Watch list:

Work notes list:

Additional comments (Customer visible):

Activity:

- System Administrator** 2016-12-13 12:52:14
LXTALERT: ARB_REFERENCEID=20000-01009001-00-01-7134-14 ARB_POLICY_MODULE=MultiTest ARB_CORRELATION_RULE=Some Rule ARB_MESSAGE=Some Rule : Multitest (2)
- System Administrator** 2016-12-13 12:52:14
Impact: 1 - High
Incident state: New
Opened by: System Administrator
Priority: 1 - Critical

| Number | Opened | Short description | Caller | Priority | State | Category | Assignment group | Assigned to |
|------------|---------------------|---|----------------------|--------------|-------|----------------|------------------|-------------|
| INC0020001 | 2016-08-10 09:14:29 | test | System Administrator | 3 - Moderate | New | Inquiry / Help | | 2006 |
| INC0010023 | 2016-12-13 12:52:14 | LXTALERT: ARB_REFERENCEID=20000-01009001-00-01-7134-14 ARB_POLICY_MODULE=MultiTest ARB_CORRELATION_RULE=Some Rule | | 1 - Critical | New | Software | | 2012 |
| INC0010022 | 2016-12-13 12:52:11 | LXTALERT: ARB_REFERENCEID=20000-01009001-00-01-7134-16 ARB_POLICY_MODULE=MultiTest ARB_CORRELATION_RULE=Some Rule Major | | 2 - High | New | Software | | 2012 |
| INC0010021 | 2016-12-13 12:52:08 | LXTALERT: ARB_REFERENCEID=20000-01009001-00-01-7134-19 ARB_POLICY_MODULE=MultiTest ARB_CORRELATION_RULE=Some Rule Info | | 5 - Planning | New | Software | | 2012 |
| INC0010020 | 2016-12-13 12:52:04 | LXTALERT: ARB_REFERENCEID=20000-01009001-00-01-7134-18 ARB_POLICY_MODULE=MultiTest ARB_CORRELATION_RULE=Some Rule Minor | | 4 - Low | New | Software | | 2012 |

4.7. Credential Configuration

4.7.1. Overview

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)

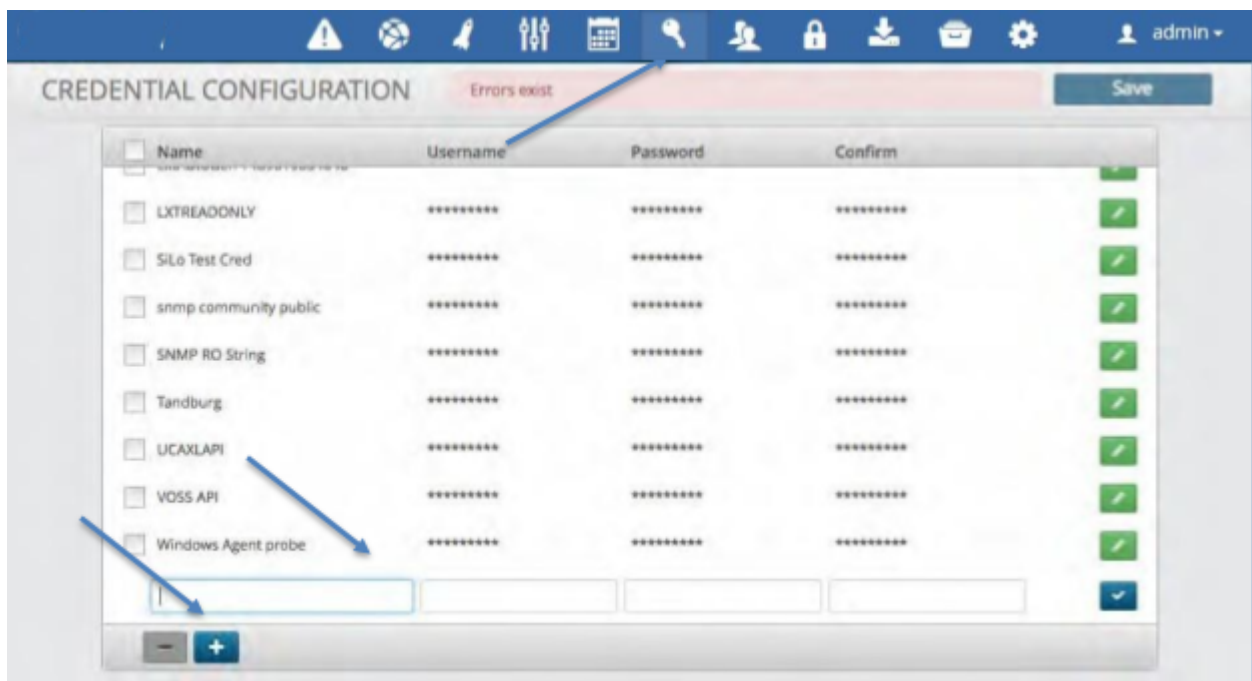
4.7.2. Create a Credential

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, Password and Confirm fields.

Note: The text displays as clear text only until the entry saved, whereupon it displays as asterisks (*).

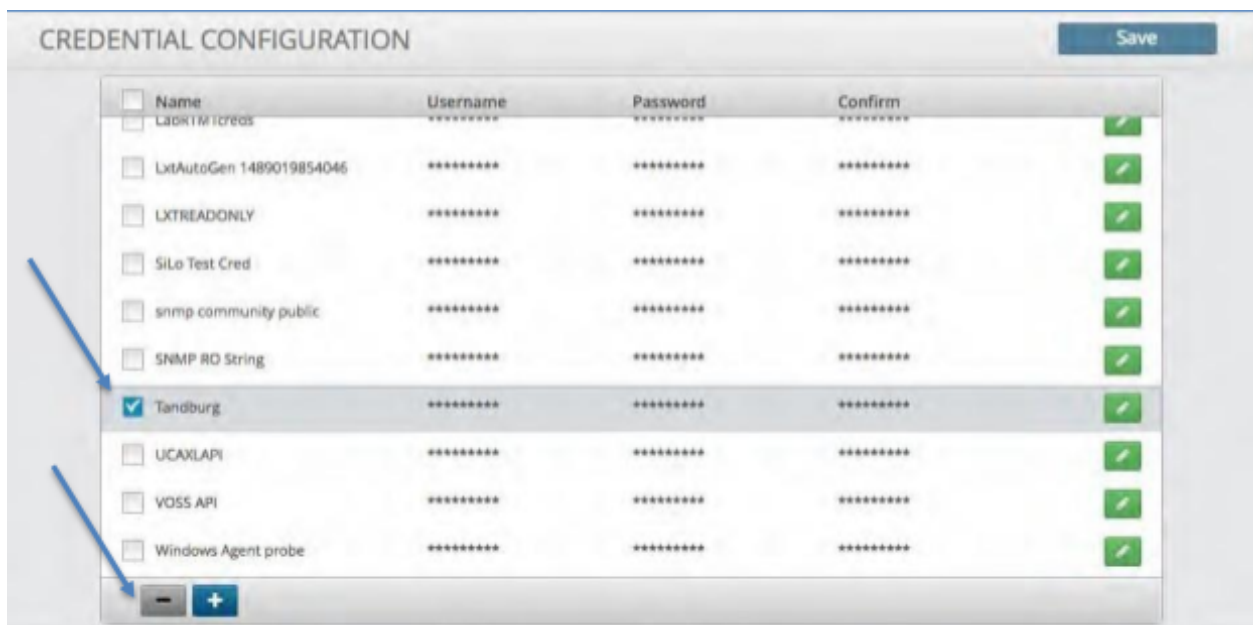
5. Click the blue check box.
6. Click the Save icon to save the credential.



4.7.3. Delete 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.



4.8. Customer Configuration

4.8.1. Overview

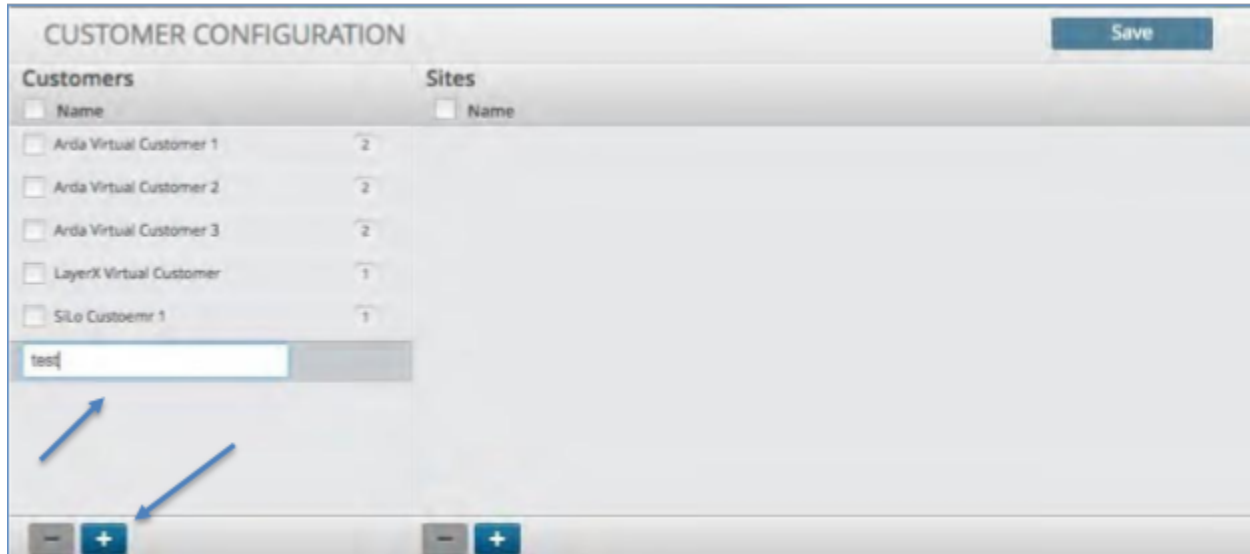
To enable multi-tenancy (assets, alerts and data) utilize the customer configuration panel to define a customer and their related locations (sites). Once defined, the Customer field can be applied to an asset and or a user to restrict access to other customers assets, alerts and data.

(See: Asset Configuration, Access Control Configuration).

4.8.2. Create a Customer

To create a Customer:

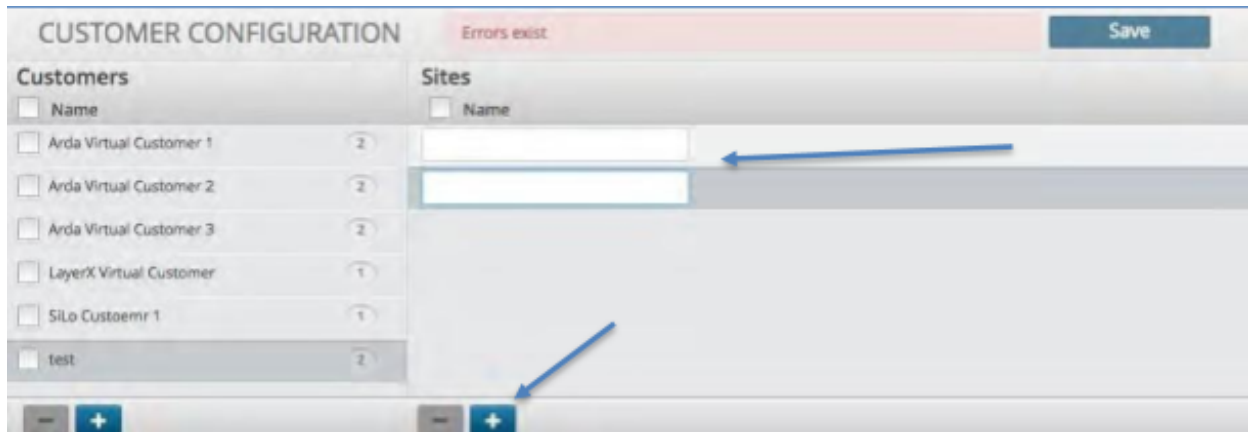
1. Click the “customer” icon in the menu bar at the top.
2. Click the plus icon in the bottom left corner of the customer panel.
3. Enter the name of the Customer to be added and press Enter.
4. Enter the Username and Password fields.
5. Click the Save icon to in the upper right corner.
6. Proceed to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



4.8.3. Create a Customer Site

To create a site for a Customer:

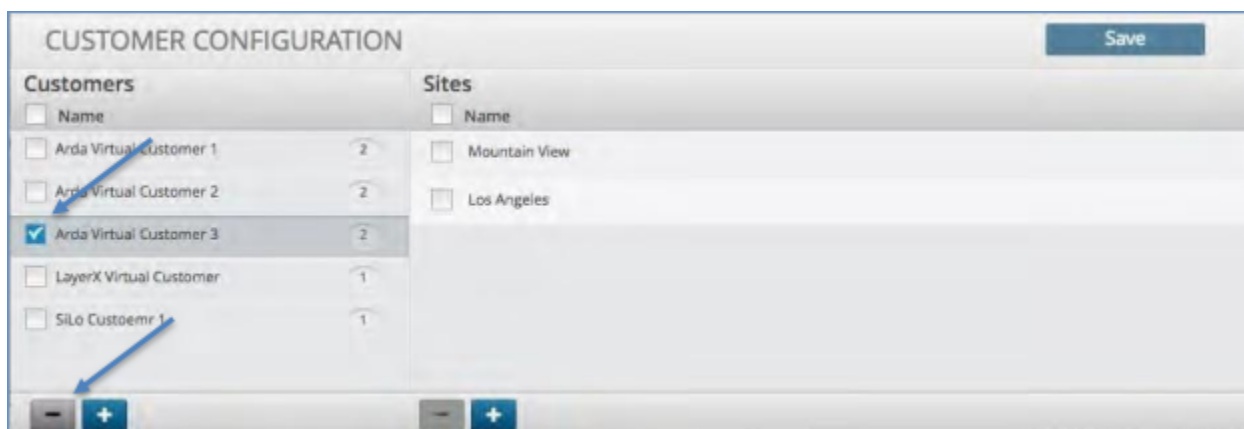
1. Click the customer to which you wish to add the site.
2. Click the plus icon in the bottom of the site panel.
3. Enter the site name and press Enter.
4. Add additional sites if applicable.
5. Click the Save icon to in the upper right corner.



4.8.4. Delete a Customer

To delete a Customer:

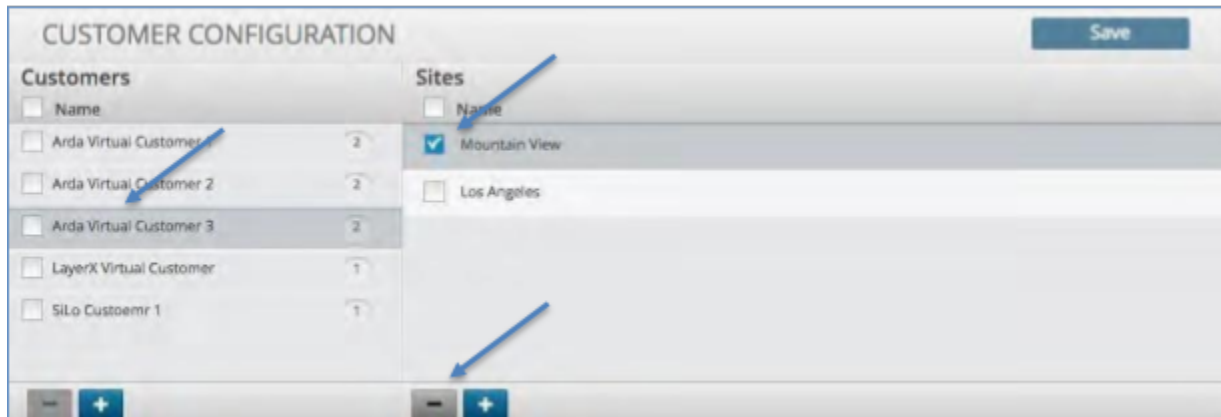
1. Click the check box of the customer you wish to delete.
2. Click the minus icon in the bottom of the site panel.
3. Click the Save icon to in the upper right corner.



4.8.5. Delete 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.



4.9. Access Control

4.9.1. Overview

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.

You can select the following tabs on this page:

- *Permission Groups Tab*
- *Users Tab*
- *Nodes Tab*
- *Realms Tab*
- *Protected Subnets Tab*
- *Password Policy Tab*
- *SAML Tab*

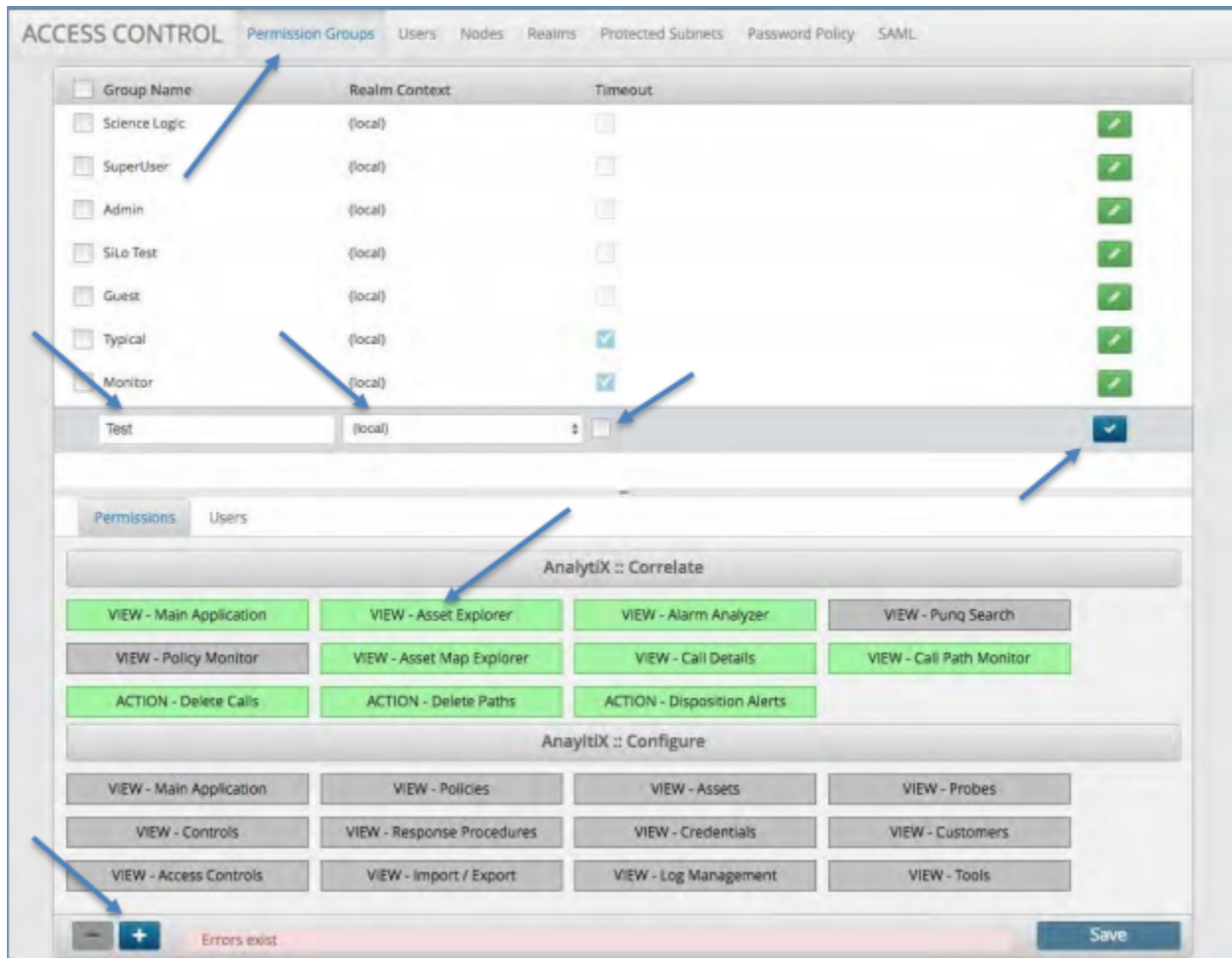
4.9.2. Permission Groups Tab

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.

Create 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.

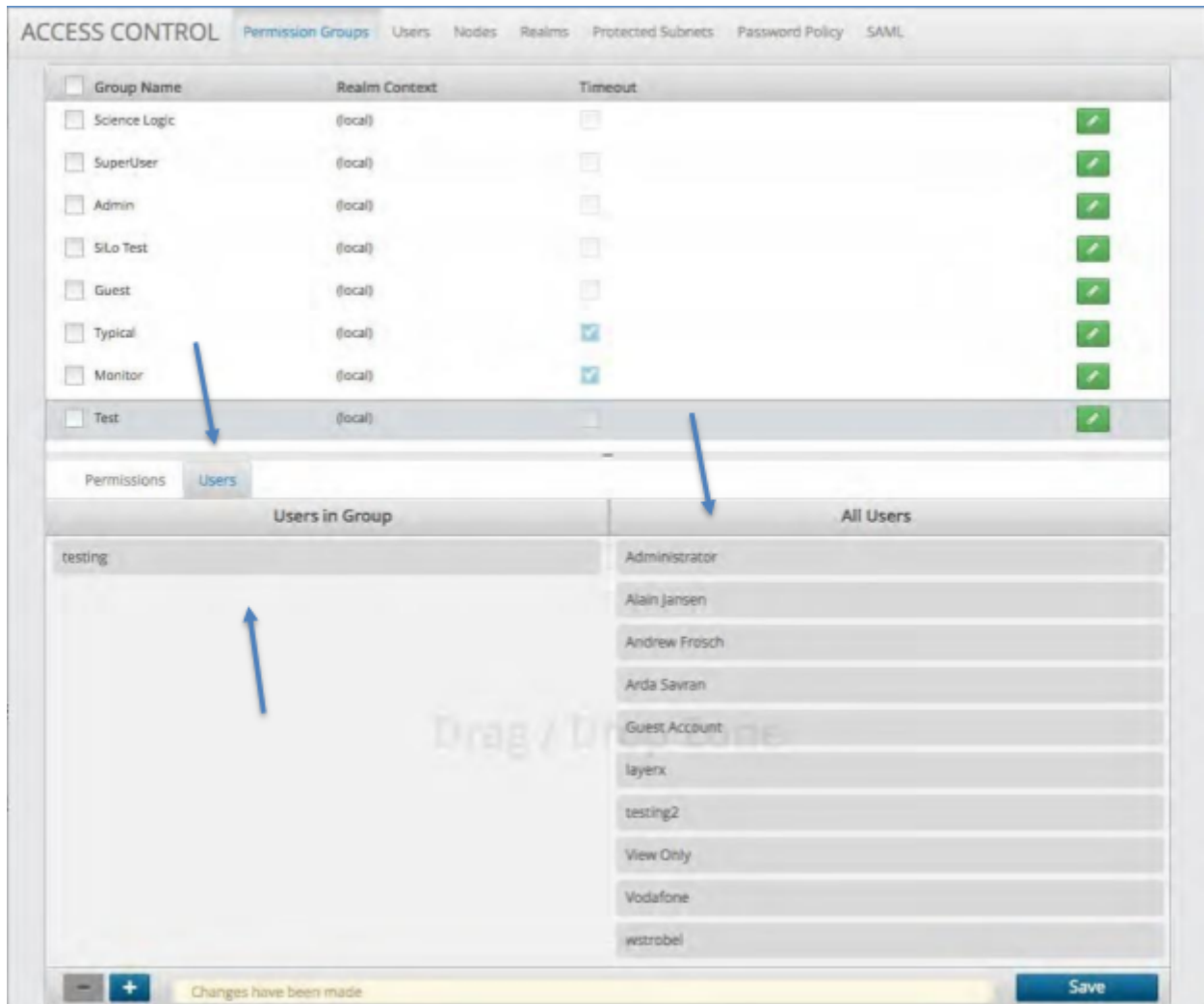


Assign and remove users to/from a permission group

Assign a User to a Permission Group

Note: From release 24.1, a permission group API has been added for the new `voss_agent_api_user`. This group has no permissions. Refer to the [Users Tab](#) for details on the new user in this 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.



4.9.3. Users Tab

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.

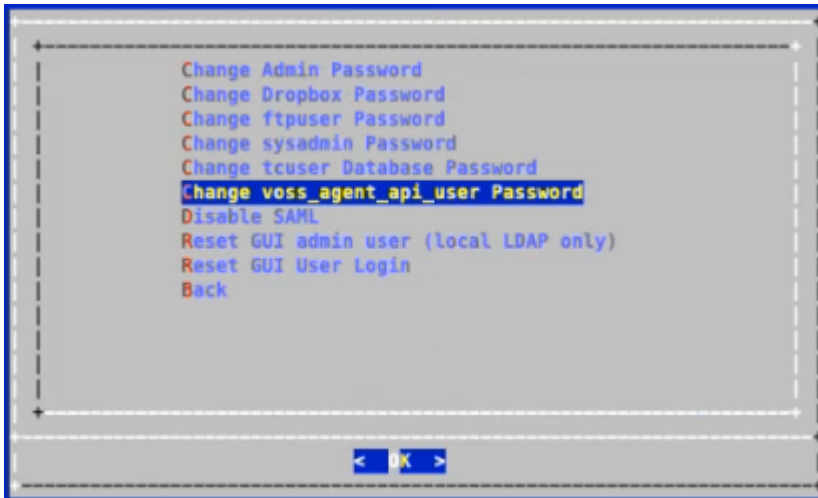
Note: From release 24.1, a new user `voss_agent_api_user` has been added that is specifically used by the VOSS Insights Forwarder - an agent that collects statistics such as latency and response times on various cloud endpoints, along with system CPU statistics, which is sent by means of the API back to the Arbitrator (this user is restricted to these agent routes). The user has no permissions and is the single member of the new API permission group that similarly has no permissions.

In order for this user is to be used, the user password needs to be updated after upgrade, either by:

- Editing the user on the **Users** form.

or

- Using the administrator console menu: **Administration > Change Passwords.**



Add 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.

The screenshot displays the 'ACCESS CONTROL' interface, specifically the 'Users' tab. The interface includes a navigation bar with tabs for 'Permission Groups', 'Users', 'Nodes', 'Realms', 'Protected Subnets', 'Password Policy', and 'SAML'. Below the navigation bar, there is a 'Filter' and 'Sort' section. The main area contains a table of users with the following columns: Full Name, Username, Password, Confirm, Email, Super-User, Force Password Change, and Locked Out. The table lists several users, including Administrator, Alain Jansen, Andrew Frosch, Arda Savran, Guest Account, layerx, testing, testing2, View Only, Vodafone, and wstrobei. At the bottom of the table, there are input fields for 'Customer' and a checkbox for 'Disable multi tenancy'. A minus icon is located at the bottom left, and a 'Save' button is at the bottom right. A red error bar at the bottom indicates 'Errors exist'.

| <input type="checkbox"/> | Full Name | Username | Password | Confirm | Email | Super-User | Force Password Change | Locked Out |
|--------------------------|---------------|----------|----------|---------|-------------------------|-------------------------------------|--------------------------|--------------------------|
| <input type="checkbox"/> | Administrator | admin | ***** | ***** | afrosch@layerxtech.com | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> | Alain Jansen | ajansen | ***** | ***** | ajansen@layerxtech.com | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> | Andrew Frosch | afrosch | ***** | ***** | afrosch@layerxtech.com | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> | Arda Savran | asavran | ***** | ***** | asavran@layerxtech.com | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> | Guest Account | guest | ***** | ***** | support@layerxtech.com | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> | layerx | layerx | ***** | ***** | support@layerxtech.com | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> | testing | testing | ***** | ***** | support@layerxtech.com | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> | testing2 | testing2 | ***** | ***** | support@layerxtech.com | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> | View Only | viewonly | ***** | ***** | view@layerxtech.com | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> | Vodafone | voda | ***** | ***** | support@layerxtech.com | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> | wstrobei | wstrobei | ***** | ***** | wstrobei@layerxtech.com | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

Delete 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.

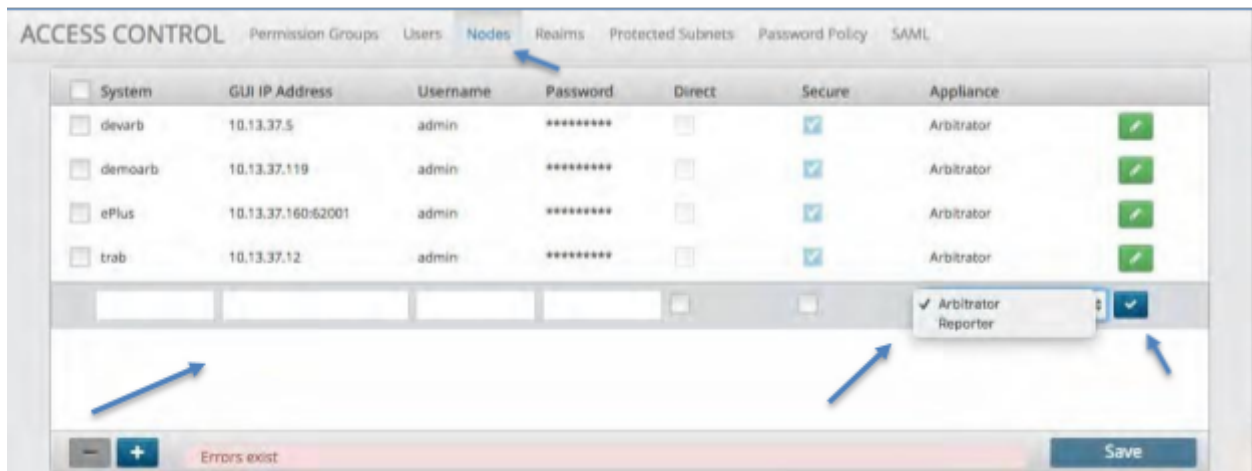
4.9.4. Nodes Tab

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.

Create 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.



Delete 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.

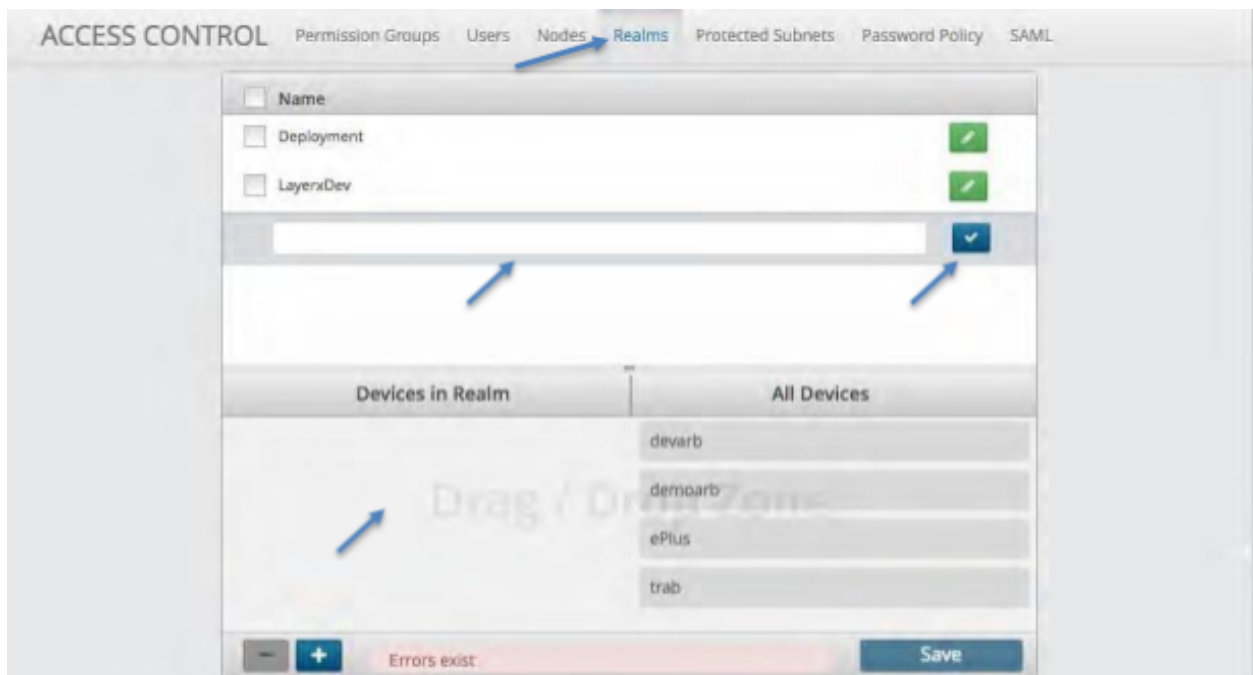
4.9.5. Realms Tab

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.

Create 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.



Delete 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.

4.9.6. Protected Subnets Tab

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.

Create a protected subnet

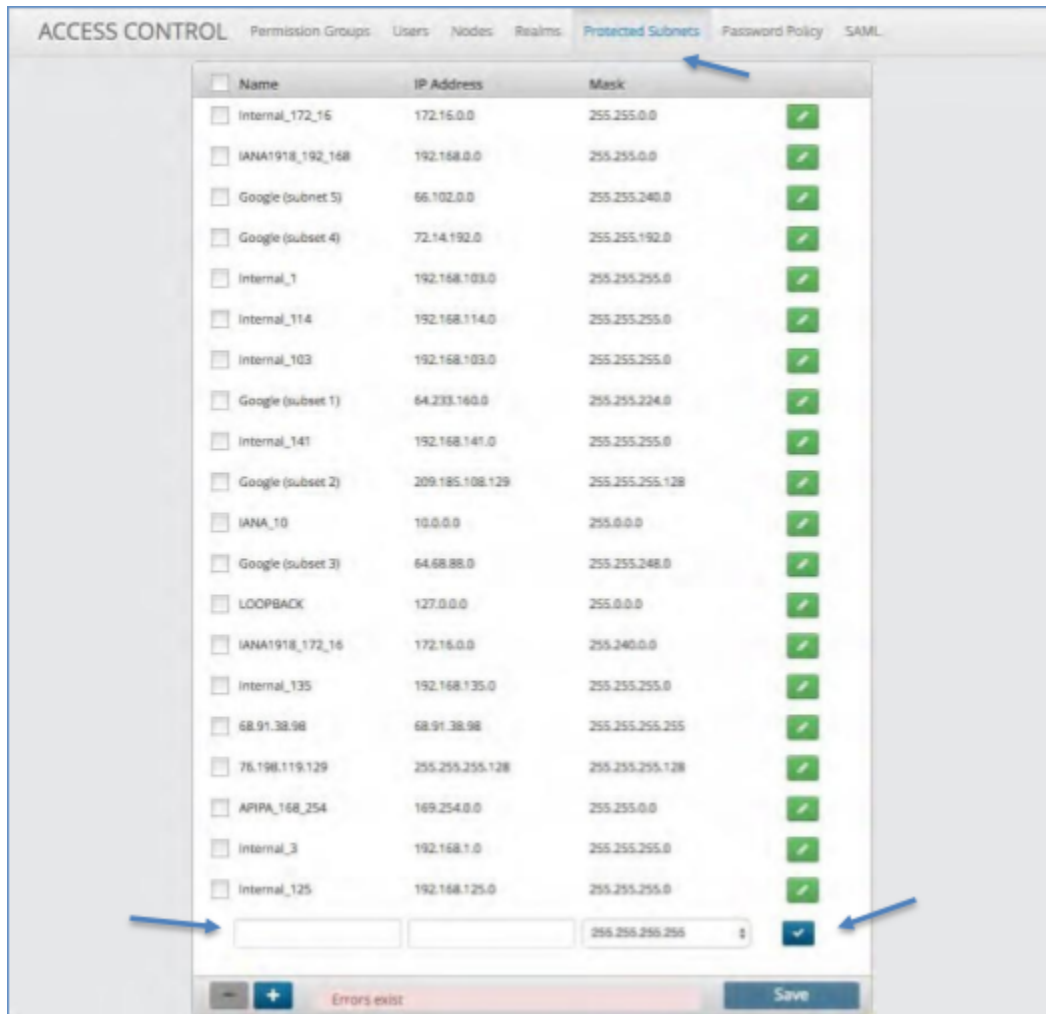
To create a Protected Subnet:

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.

Delete 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.



4.9.7. Password Policy Tab

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.

Create 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.

The screenshot shows the 'ACCESS CONTROL' configuration page with the 'Password Policy' tab selected. The settings are as follows:

| Setting | Value | Character Set |
|------------------------|-------|---------------|
| Minimum Length | 7 | |
| Minimum Uppercase | 1 | A-Z |
| Minimum Lowercase | 1 | a-z |
| Minimum Numeric | 1 | 0-9 |
| Minimum Special | 1 | !@#%&*()[] |
| Password Lifespan | 0 | days |
| Maximum Login Attempts | 20 | |

A 'Save' button is located at the bottom of the configuration panel.

4.9.8. SAML Tab

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

Note: SAML is an open standard for exchanging authentication and authorization data between parties, in particular, between an identity provider and a service provider. SAML is an XML-based markup language for security assertions (statements that service providers use to make access-control decisions).

VOSS Insights supports SSO for authentication via the SAML v2.0 standard for SSO. When SAML is enabled for your system, the **Sign Out** menu option (accessible via the **admin** menu) is not required or available as the Insights system does not initiate the termination in this case.

SAML is enabled/disabled on the SAML tab of the Configuration screen in Arbitrator. To bypass SAML authentication, you can set `nosaml=true` in the URL.

Set up SSO via SAML

To create single sign-on via SAML:

1. Click the SAML tab at the top of the screen (adjacent 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.

Note: The **Sign Out** option is removed from the Profile menu when SAML is enabled.

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.)

ACCESS CONTROL [Permission Groups](#) [Users](#) [Nodes](#) [Realms](#) [Protected Subnets](#) [Password Policy](#) **SAML**

Enable SAML

Disable Multi Tenancy

SAML Signature Algorithm

Attribute Mappings

Email (Optional):

Username (Optional):

First or Display Name (Optional):

Last Name (Optional):

Identity Provider Metadata XML

** Required*

Paste your metadata XML here

Service Provider Information

Provide this information to your Identity Provider

Audience URI (SP Entity ID):

Single Login URL:

Single Logout URL:

Metadata: [View Details](#) | [Download](#)

X.509 Certificate (2048 Bit): [View Details](#) | [Download](#)

Save

ACCESS CONTROL Permission Groups Users Nodes Realms Protected Subnets Password Policy SAML

Enable SAML

Disable Multi Tenancy

SAML Signature Algorithm

Attribute Mappings

Email (Optional):

Username (Optional):

First or Display Name (Optional):

Last Name (Optional):

Identity Provider Metadata XML

** Required*

Paste your metadata XML here

SAML Metadata ✕

```
<?xml version="1.0"?>
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
entityID="http://demoarb.layerxtech.com/saml2/module.php/saml/sp/metadata.php/default-sp">
<md:SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:1.1:protocol
urn:oasis:names:tc:SAML:2.0:protocol">
<md:KeyDescriptor use="signing">
<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:X509Data>

<ds:X509Certificate>MIID5zCCAs+gAwIBAgLJAly0+0SPiFX0MA0GCSqGSIb3DQEBCwUAMIGJM0swC
QYDVQQGEwJVUzEOMAwGA1UECAwVGV4YXN0dDZANBgNVBAMcMBklydmliuZzEPMA0GA1UECgwG
GF5ZkxJ4M08wDQYDVQQLEDAZsYXlcnngxEDA0BgNVBAMMB2RlbnBhcnRlJTAjBgkqhkiG9w0B
CQEFWnN1cHRvbnRAbGF5ZkxJ4dGVjaCSjbn20wHhcNMTg0MTE3MjMjMzQ3WjBjBIT
ELMAkGA1UEBhMCVWVmbDQAMBgNVBAQMBVJleGFzZGFzMQ8wDQYDVQQHDAZJbnZpbmexDzAN
BgNVBAMcMBklydmliuZzEPMA0GA1UECAwVGV4YXN0dDZANBgNVBAMcMBklydmliuZzEP
MA0GA1UECgwGGF5ZkxJ4MRAwDgYDVQQDDAdkZXZwYXJIMSUwIwYJKoZIh
vcNAQkBFhZzdXBw3J0QXheWVyeHRiY2guY291MlIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA4ZgbuCEgq3E/RrHvoMyyjhYtcsGITvqvUkmbkmD9eP75vBS4QyIT55HY7DW72z
GrjGqsjrpk5DPBIMf6kBljIMjUbK4V3L0TCoaCq5u0rD9YLSeVAmSm0aNF/X1diTAb3Lc8Vq
Mceh7PsvMn9CqCImJ++x3U2BvAGS78OC6BUUhD4d8U4E5/WsJ+x1wEceYsRGN16c7A156O6Yr9
BelU000pq6m6k6YXjC6XWNvLTK18G5ZcG5NAUJKKdnTep4yhgtokRJuXh2wVbD/rQJZfk+D7yQLSspfc41
DbVmfJRCla7LgkGdV+Rhb0KvtjOpVQ5Z6w2T5xlwbdwIDAQABo1AwTjAdBgNVHQ4EFgQUUv
fDaBSaubH6fUtzgbEVEm8vBtlwHwYDVROjBBgwFoAUUvIDaBSaubH6fUtzgbEV
Em8vBtlwQAYDVROjBBAUwAwEB/zANBgkqhkiG9w0BA
QsFAAOCAQEAYk084TvcTgZxuoNhcX20f9T6v7IRzO1280Uih8ydBSwbNmP9vXP69IA9dz
lmi4TUHfDwJqElz+M4HKz07DzZn60LW+ZnWZDXnodFzuYAThdsVkeZn+BXT+vD3w9fPNm
xpPPFbK8e6X/8eJum63cil8Kbd4yVS7750VDQPBT2JulV8JizjQSUr11MDir3R9Z+EtIKUjrlt4
CLVsn9h40fzDYobr315XKojEjDiSq7Vy8WEYXP00IHm6nkEvUs85jyLxsXcjw3N
TbtzQeMBppuVOByGValEWlGjFyg8++t/qGJuoCQR/LT06LzFek2rCg/t9wGzEnmjwH
YpGw==</ds:X509Certificate>
</ds:X509Data>
```

Service Provider Information

Provide this information to your Identity Provider

Audience URI (SP Ent ID):

Single Login URL:

Single Logout URL:

Metadata: [View Details](#) [Download](#)

X.509 Certificate (2048 Bit): [View Details](#) [Download](#)

Save

ACCESS CONTROL | Permission Groups | Users | Nodes | Realms | Protected Subnets | Password Policy | **SAML**

Enable SAML

Disable Multi Tenancy

SAML Signature Algorithm: sha1

Attribute Mappings

Email (Optional):

Username (Optional):

First or Display Name (Optional):

Last Name (Optional):

Identity Provider Metadata XML

* Required

Poste your metadata XML here

SAML Certificate

```

-----BEGIN CERTIFICATE-----
MIID5zCCAs+gAwIBAgIJAlY0+05PIFXDMA0GCSqGSIb3DQEBCwUAMIGJMswCQYD
VQQGEwJVUzEOMAwGA1UEGAwFVG4YXmDzANBgNVBAcMBkdydmVzZEPMA0GA1UE
CgwGbGF5ZXJ4MQ8wDQYDVQQLEDAZsYXlcnGxEADAQBgNVBAMMB2RldnBhcnkuTAJ
BgkqhkiG9w0BCQEWFnN1cHBvcnRAbGF5ZXJ4dGVjaC5jb20wHhcNMTE3MjIx
MzQ3WWhcNmJgMTE3MjIxMzQ3WjCBTELMAkGA1UEBhMCVWx0DjAMBGNVBAgMBVRl
eFZlMQ8wDQYDVQQQHDAAZJcnZpbmVzZANBgNVBAoMBmRmcmVhWVYyDEPMA0GA1UECwwG
bGF5ZXJ4MRAwDgYDVQQDDAdkZmVzYXlMSUwvhwYKozZlhcNAQKBzZzdXBwb3J0
QGxheWVyeHRIY2guY29tMlIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCGKCAQEA
4ZgbuCEgq3E/RrHvoMyyjHYtcsGtVqvUkmbkmD9eP75vBS4fQyIT55HY7DW72z
GrjGsqjpk5sDPBIM86kBUIMjUbkK4V3L0TCoaCq5u0rjD9YLSelVAMsm0aNF/X1
dITab3Lc9VqMceh7PsvMn9CqCImJ+X3J2BvAGS78OC6BUUhD4d8Uf4E5Wsj+X1w
EceYsRGN16c7Ai56O6Yr9BelU000pq6mk8xYXIC6XWVnLTKi8G5zcG5NAUHKKn
Tep4yhgtkRjUbXh2wWbD/rQJZFk+D7yDLsptc41DbVmFJRCla7LgkGdqV+Rh80
KVtjOpVQ5Z6w2T5xwWbdwIDAQAB01AwTJAdBgNVHQ4EFgQUUvDaBSaubH6fUtz
gbEVEm8v8tlwHwYDVR0jBBgwFoAUUvDaBSaubH6fUtzgbEVEm8v8tlwDAYDVR0T
BAUwAwEB/zANBgkqhkiG9w0BAQsFAAOCAQEAAyK094TvcTgZxuoNhcX20f9T6vI7I
RzOt280Uj8ydBSwbNimP9vXP69IA9dzlml4TUHDwJqEtz+M/4HKz07DzZrh60LW-Z
NWZ0NodxFzYATrdsVKEZn+BXT+vD3w8fPNmXPfFbK8e6X/8eJum63cll8Kbd4
yVS7750VDQPBT2JuuV8JzjJQSURf1MDlr3R9Z+EtIKUjlt4CLVsn8h40fzDYo
br315XkoJeDisq7Vy9WEYXp00IHm6nkEvUs95jyLxsXcjw3NTbtzQeMBppuW0By
GValEWfGfyg8++/qGJuoCQr/LT06LzFek2rCg/r9wGzEnmjwHYpGw==
-----END CERTIFICATE-----

```

Service Provider Information

Provide this information to your Identity Provider

Audience URI (SP Entity ID):

Single Login URL:

Single Logout URL:

Metadata: [View Details](#) [Download](#)

X.509 Certificate (2048 Bit): [View Details](#) [Download](#)

Save

4.10. Import & Export

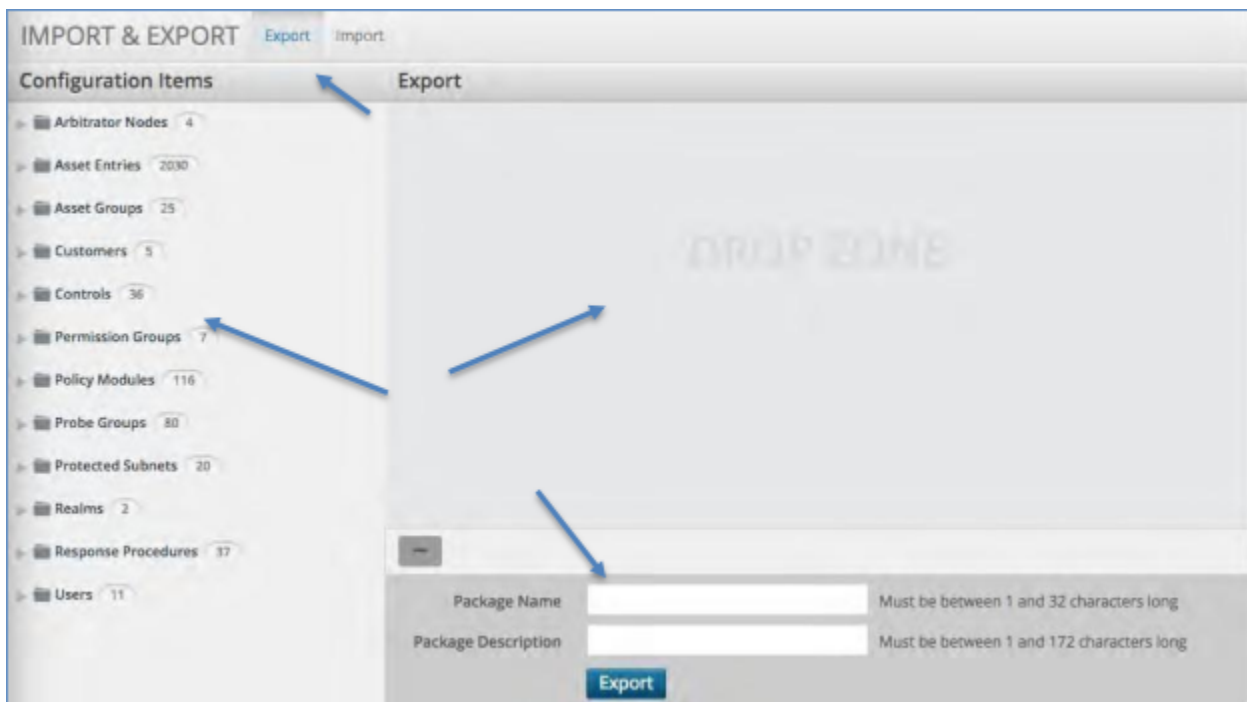
4.10.1. Overview

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.

4.10.2. Exporting

To export configuration items:

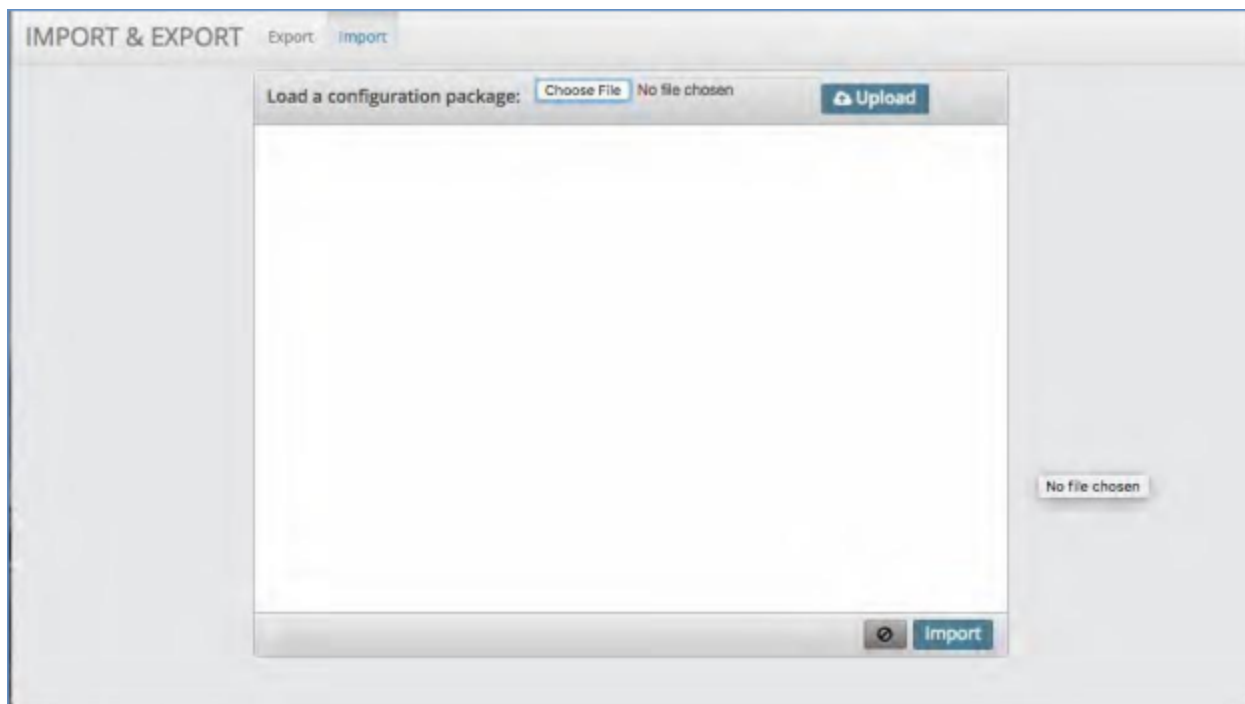
1. Click the Export tab at the top of the screen.
2. On the left-hand side will be folders containing all of the configuration items. Either drag whole folders over to the drop zone or open a folder and select a specific item to drag to the drop zone.
3. Once complete give the package a name in the box 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.



4.10.3. 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.



4.11. Archive Management

4.11.1. Overview

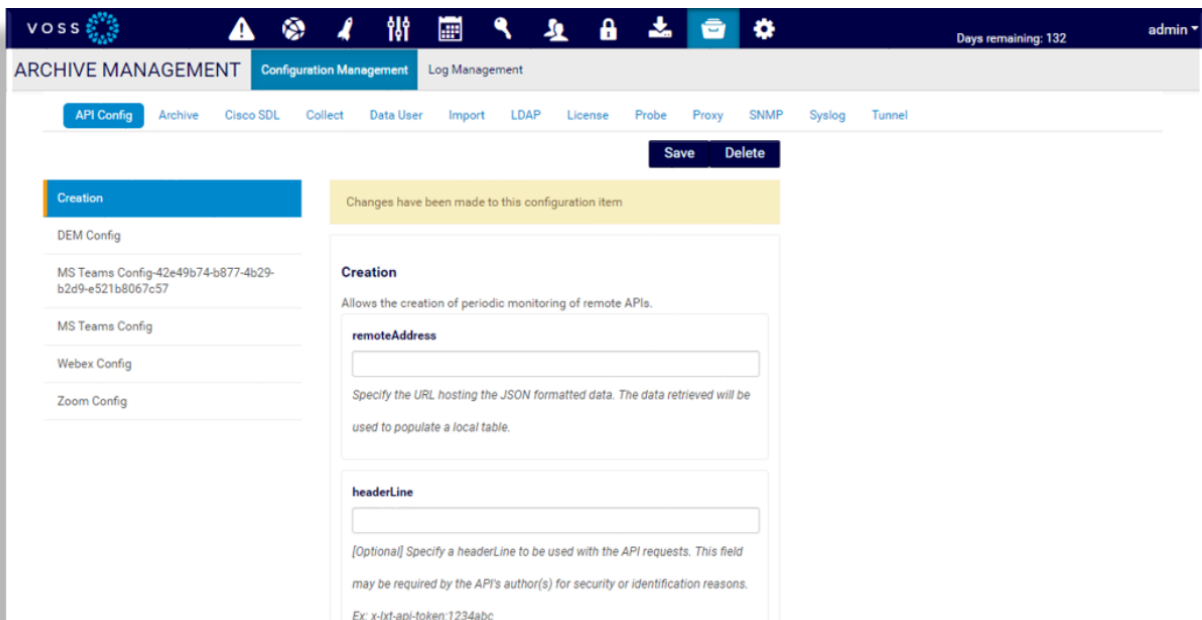
admin-users-only

The Arbitrator **Archive Management** page provides options for backing up and configuring the Arbitrator correlation platform.

You can select the following tabs on this page:

- *Configuration Management Tab*
- *Log Management Tab*

Note: Archive Management is only accessible to admin users.



4.11.2. Configuration Management Tab

You can select the following tabs on the Archive Management > Configuration Management tab:

- *API Config Tab*
- *Archive Tab*
- *Cisco SDL Tab*
- *Collect Tab*
- *Data User Tab*

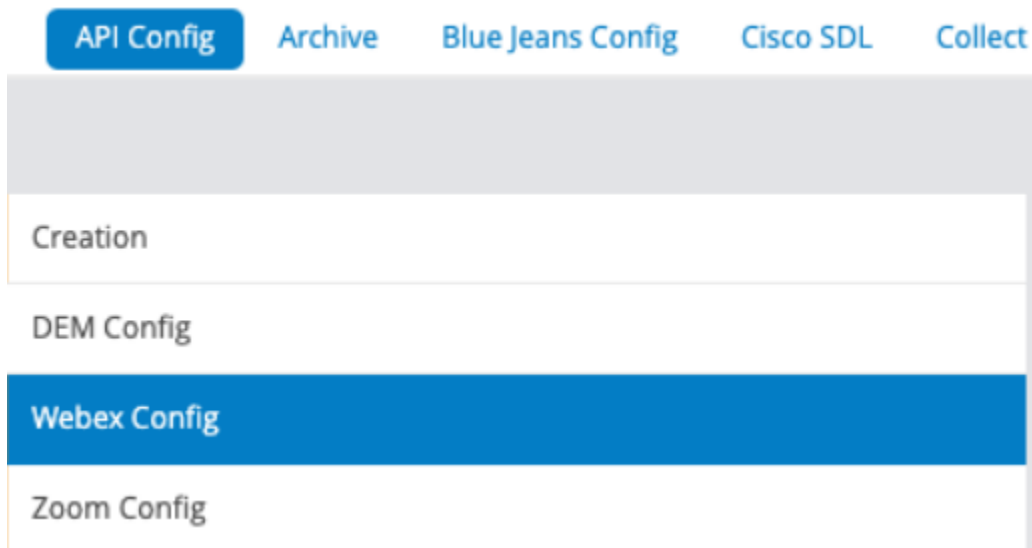
- *Import Tab*
- *LDAP Tab*
- *License Tab*
- *Probe Tab*
- *Proxy Tab*
- *SNMP Tab*
- *Syslog Tab*
- *Tunnel Tab*

API Config Tab

This tab allows you to set up a number of API configurations to enable monitoring, for example, of Webex or MS Teams.

Webex Config

The Webex Config option allows the configuration of Webex monitoring. A dashboard is available to visualize the data.



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.)

To configure Webex API:

1. From the Arbitrator main user interface, click the **System Configuration** toolbar icon (wrench) to open the Arbitrator **Configuration** GUI.
2. Click the toolbar **Cabinet** icon to open **Archive Management**.
3. On the **Configuration Management** tab, select the **API Config** tab.
4. On the **API Config** tab, select **Webex Config**, then configure settings in the right pane:
 - a. Click the **Create Access Token** button, then fill out your account credentials and copy the JSON string that performs OAuth handshake with Webex. You'll paste this into **AccessToken**.
 - b. At the **Enabled** drop-down, select `enabled`.
 - c. At **CUSTOMER**, fill out the customer name (if multi-tenancy is required).
 - d. At **AccessToken**, paste the copied JSON token from step a.

The JSON format is as follows (line breaks here not in string):

```
{ "access_token": "xxxxxxxxxxxxxxxxxxxxxxxxxxxx",  
  "expires_in": nnnnnnn,  
  "refresh_token": "xxxxxxxxxxxxxxxxxxxxxxxxxxxx",  
  "refresh_token_expires_in": nnnnnnn,  
  "token_type": "Bearer" }
```

- 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.)

VOSS

ARCHIVE MANAGEMENT Configuration Management Log Management

API Config Archive Blue Jeans Config Cisco SDL Collect Import LDAP Probe SNMP Syslog Tunnel

Creation

DEM Config

Webex Config

Zoom Config

Changes have been made to this configuration item

Webex Config

Allows the enable and configuration of Webex monitoring.

Create Access Token

Create Access Token

This step is required to allow the creation of an access token.

Enabled

enabled

Capture Webex's statistics using the Access Token provided from <https://marketplace.webex.us/> Recommendation: Manually overwrite the ExpirationTime to a much greater time.

CUSTOMER

ABC Telecom

Name of Customer.

AccessToken

{"access_token": "ZjlyZjAyYmE1YTUyNS00YWZlLWl3OGEt"}

AccessToken to be used for requests.

Command: Webex Config: Create Access Token

Status: Finished

Output: success

Close View Output

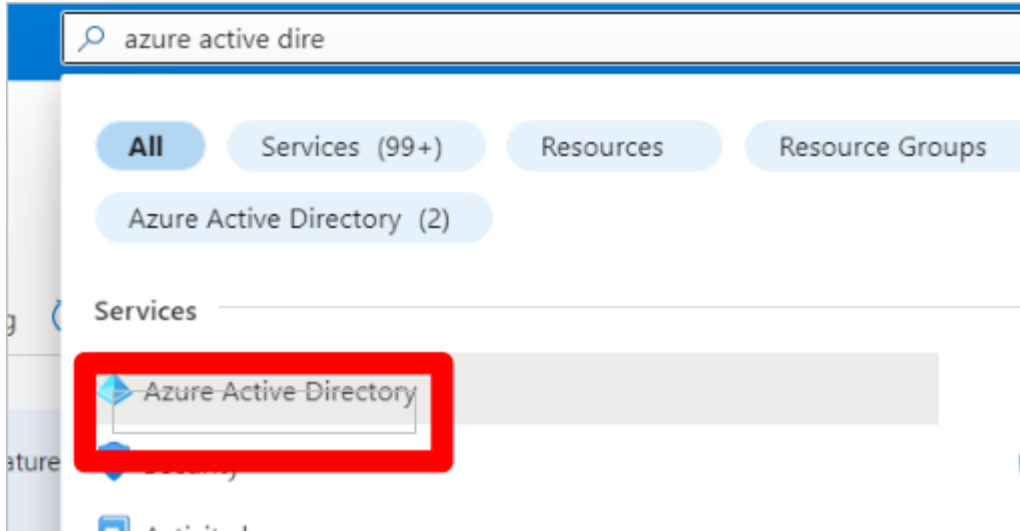
Created configurations can be deleted or modified. This will be needed for Access Tokens, as these contain an `expires_in` value.

MS Teams Config

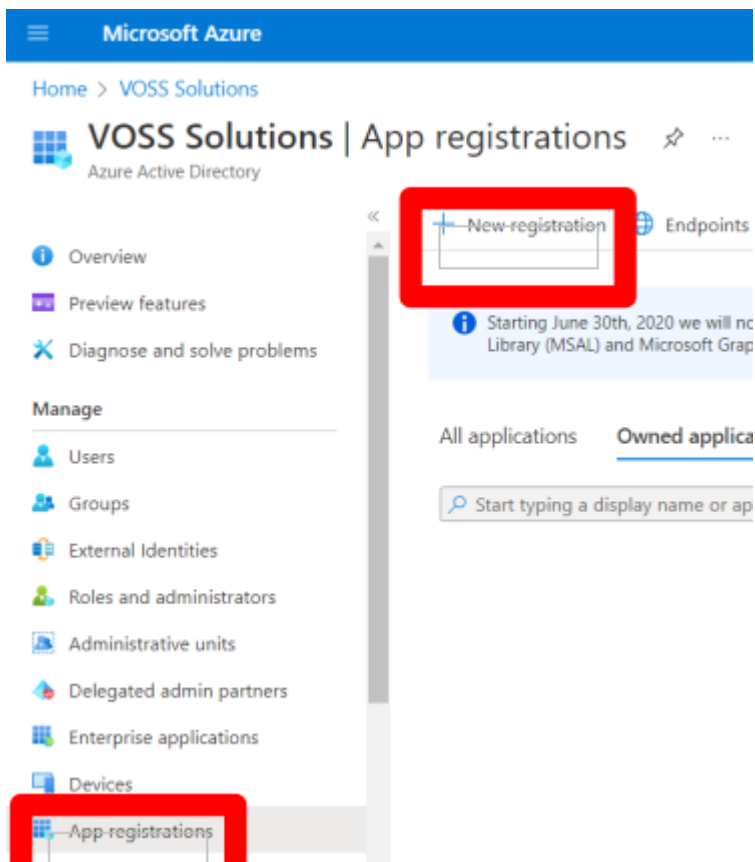
MS Teams Config settings allow you to configure MS Teams monitoring.

The MS Teams API configuration requires an initial application registration on Microsoft Azure. To set this up:

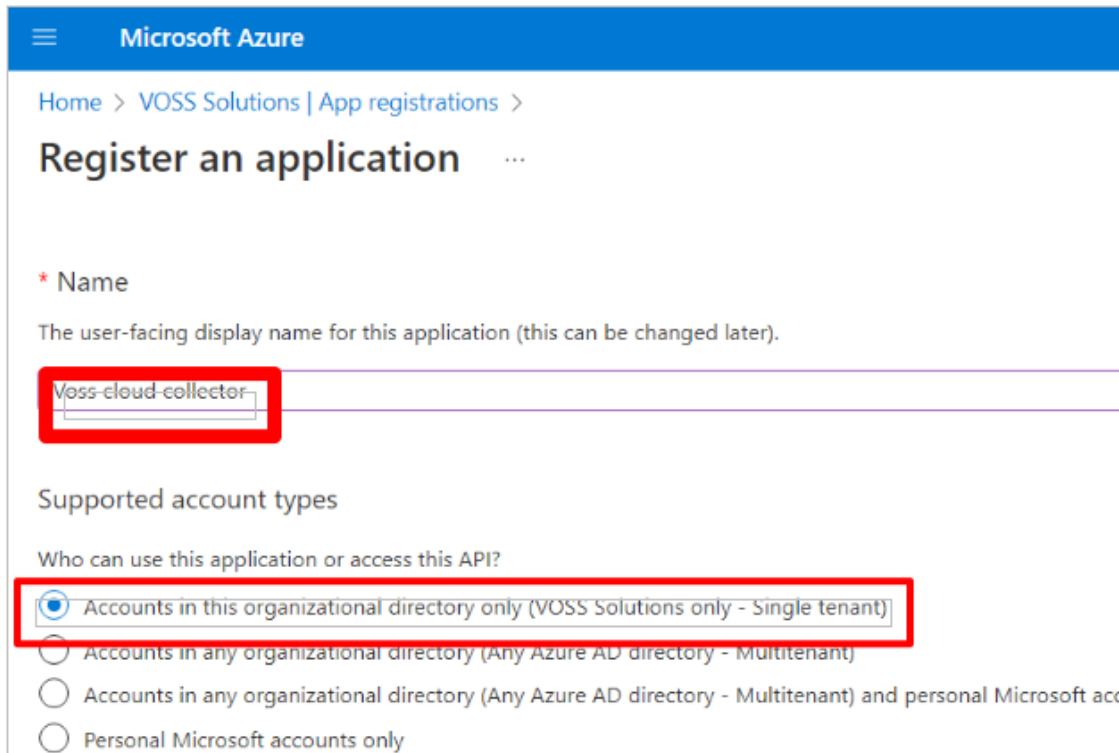
1. Search for Azure Active Directory:



2. Select **Manage > App registrations**, then select **New Registration**



3. Fill out a meaningful application **Name** to display to users and under **Supported account types**, select **Accounts in this organization directory** and click **Register**.



Microsoft Azure

Home > VOSS Solutions | App registrations >

Register an application

*** Name**

The user-facing display name for this application (this can be changed later).

Voss-cloud-collector

Supported account types

Who can use this application or access this API?

Accounts in this organizational directory only (VOSS Solutions only - Single tenant)

Accounts in any organizational directory (Any Azure AD directory - Multitenant)

Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft acc

Personal Microsoft accounts only

4. When the new application is registered, locate the **Application (client) ID** and **Directory (tenant) ID** on the next page and store these values in a secure location.

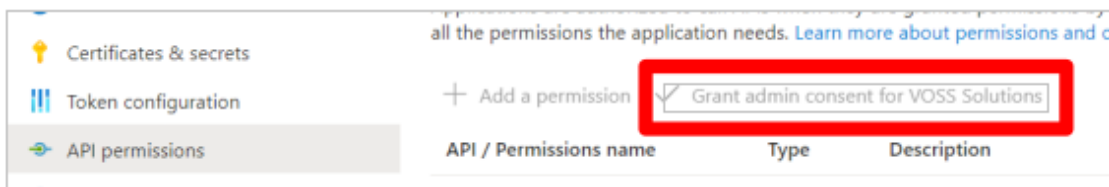
The screenshot displays the Microsoft Azure portal interface for an application named 'VOSS MS Teams Collector'. The left-hand navigation pane includes sections for 'Manage' and 'API permissions', with the latter being highlighted by a red rectangular box. The main content area, under the 'Essentials' heading, lists several application identifiers: 'Display name' (VOSS MS Teams), 'Application (client) ID' (redacted), 'Object ID' (redacted), and 'Directory (tenant) ID' (redacted). The 'Application (client) ID' and 'Directory (tenant) ID' fields are also highlighted with red boxes. Below these fields, the 'Supported account types' are listed as 'My organization'. A notification banner at the bottom of the Essentials section states: 'Starting June 30th, 2020 we will no longer support Authentication Library (MSAL) and Micro'.

5. Select the **API permissions** menu under **Manage** and then select the following **Application permissions**:

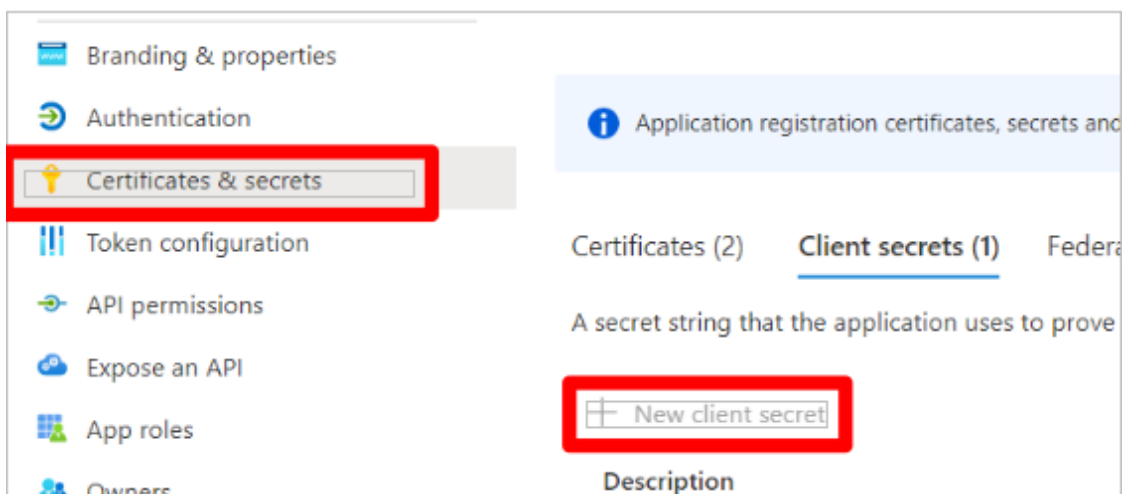
- CallRecords.Read.All
- Device.Read.All
- DeviceManagementApps.Read.All
- DeviceManagementApps.ReadWrite.All
- DeviceManagementConfiguration.Read.All
- DeviceManagementConfiguration.ReadWrite.All
- DeviceManagementServiceConfig.Read.All
- DeviceManagementServiceConfig.ReadWrite.All
- Directory.Read.All
- Directory.ReadWrite.All
- User.Read.All
- User.ReadBasic.All

- User.ReadWrite.All
- Group.Read.All
- Group.ReadWrite.All
- GroupMember.Read.All
- ServiceHealth.Read.All
- TeamworkDevice.Read.All
- TeamworkDevice.ReadWrite.All

6. Grant admin consent:



7. From **Certificates & secrets**, create authentication from **New client secret**:



8. Copy the value and store in a secure location.

| Description | Expires | Value ⓘ | Secret ID | |
|--------------------------------|-----------|------------|------------|---|
| VOSS MS Teams Collector Secret | 6/22/2023 | [REDACTED] | [REDACTED] |   |

The following stored values will be used on the Arbitrator configuration dialog screen:

- Application (client) ID
- Client secret value
- Directory (tenant) ID

Configure the tenant collection from the Arbitrator

Configuration is carried out on the Arbitrator **Settings** menu via **Archive Management > API Config > MS Teams Config**.

The screenshot displays the 'MS Teams Config' page in the Voss Archive Management system. The interface includes a top navigation bar with the Voss logo and various utility icons. Below this, a breadcrumb trail shows 'ARCHIVE MANAGEMENT' > 'Configuration Management' > 'Log Management'. A secondary navigation bar contains tabs for different configuration types: 'API Config', 'Archive', 'Blue Jeans Config', 'Cisco SDL', 'Collect', 'Import', 'LDAP', 'Probe', 'SNMP', 'Syslog', and 'Tunnel'. On the left, a sidebar menu lists configuration categories: 'Creation', 'DEM Config', 'MS Teams Config' (highlighted in blue), 'Webex Config', and 'Zoom Config'. The main content area features a yellow notification banner stating 'Changes have been made to this configuration'. The 'MS Teams Config' section includes a description: 'Allows the enable and configuration of MS Teams'. It has an 'Enabled' checkbox currently checked with the value 'enabled'. Below this, there is a text field for 'CUSTOMER' with the placeholder 'Tenant id of Customer.' To the right, a larger form contains fields for 'Name' (placeholder: 'Friendly user name of Customer.'), 'ClientID' (placeholder: 'Client ID to be used for requests.'), and 'ClientSecret' (placeholder: 'Client Secret to be used for requests.'). At the bottom of this form are two buttons: 'Save Data' (with the instruction 'Create an entry for the supplied customer.') and 'Verify Access' (with the instruction 'Tests the API access by trying to fetch the license info. Response should be JSON-formatted list of license values, or else MS Graph error codes.').

New Tenants can be created with **Enabled** either enabled or disabled. If disabled, no API requests will be made until it is enabled.

1. Enter stored values:

- Enter the tenant id (**Directory (tenant) ID**) in the **CUSTOMER** field
- Enter an easily identifiable account name in the **Name** field.
- Enter the client ID (**Application (client) ID**) in the **ClientID** field.
- Enter the client secret **Value** in the **ClientSecret** field.

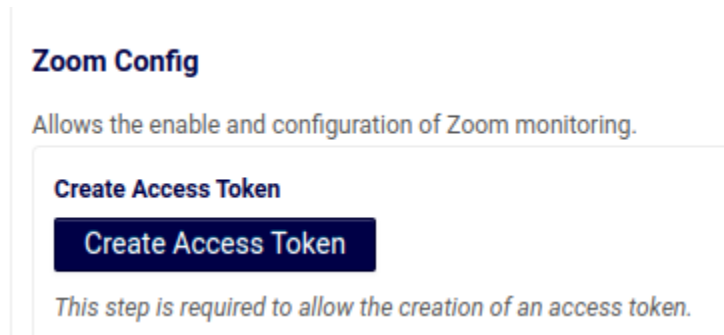
These values should be for a client that is dedicated to this use and should not be used to request a token from any other source while the API collector is enabled.

2. Click **Save Data** to save the configuration.

3. Refresh the screen (move away from the configuration screen to another and back) to see the new configuration.

Zoom Config

An access token is required for the configuration of Zoom monitoring.



Click the **Create Access Token** button to be redirected to get an access token.

1. If Zoom statistics are to be captured, select **enabled** from the **Enabled** drop-down.
2. Enter a **Customer** name for the associated customer.
3. Enter the received access token in the **AccessToken** input box.
4. Enter a refresh token in the **RefreshToken** input box.
5. Click the **Verify Access Token** button to test the entered access token.

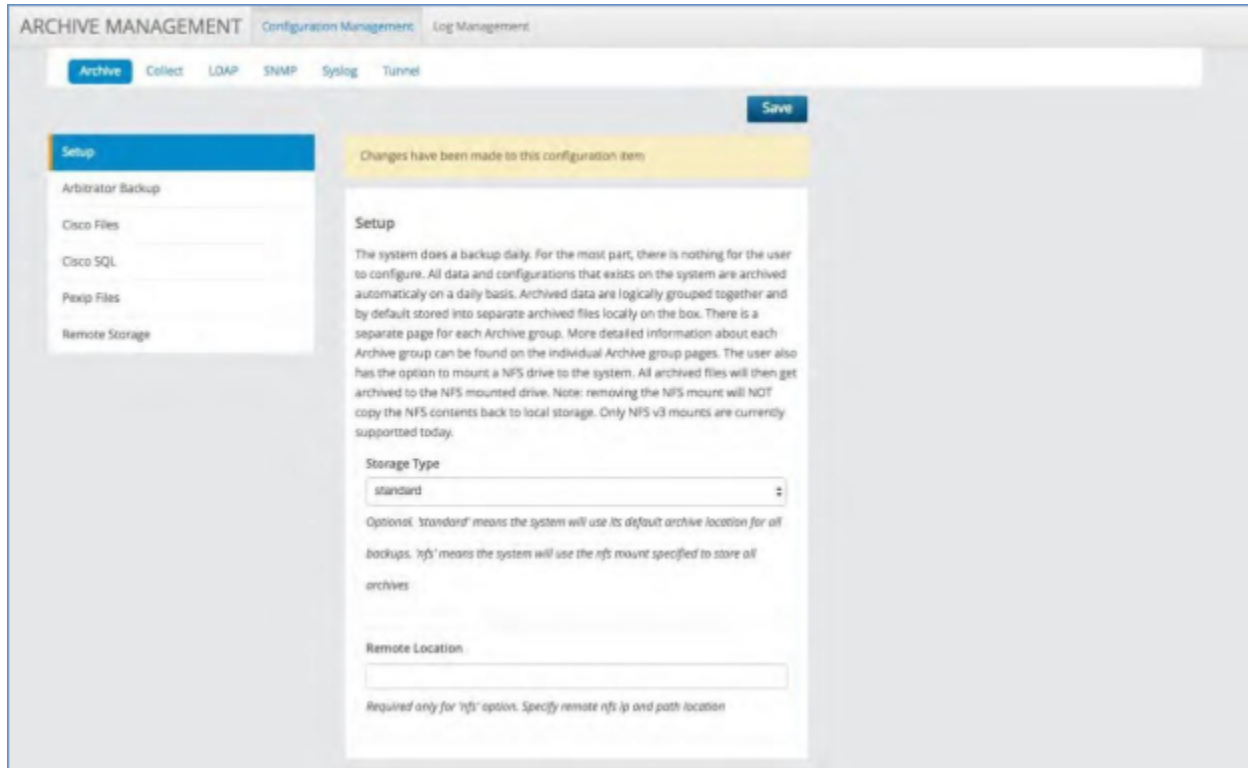
Archive Tab

The Archive tab provides a number of options based on the specific functions you wish 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

(Idap), 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.

The screenshot displays the ARCHIVE MANAGEMENT web interface. At the top, there are tabs for 'Configuration Management' and 'Log Management'. Below these, a navigation bar includes 'Archive', 'Collect', 'LDAP', 'SNMP', 'Syslog', and 'Tunnel'. A 'Save' button is visible in the top right corner. On the left side, a sidebar menu lists 'Setup', 'Arbitrator Backup' (which is highlighted), 'Cisco Files', 'Cisco SQL', 'Pexip Files', and 'Remote Storage'. The main content area features a yellow notification banner stating 'Changes have been made to this configuration item'. Below this, the 'Arbitrator Backup' section contains a descriptive paragraph and four configuration fields: 'archive_interval' (set to 'daily'), 'method' (set to 'local'), 'destination' (set to '/chroot/iscp/pub/xt_archive'), and 'monthsKept' (set to 'notSupported').

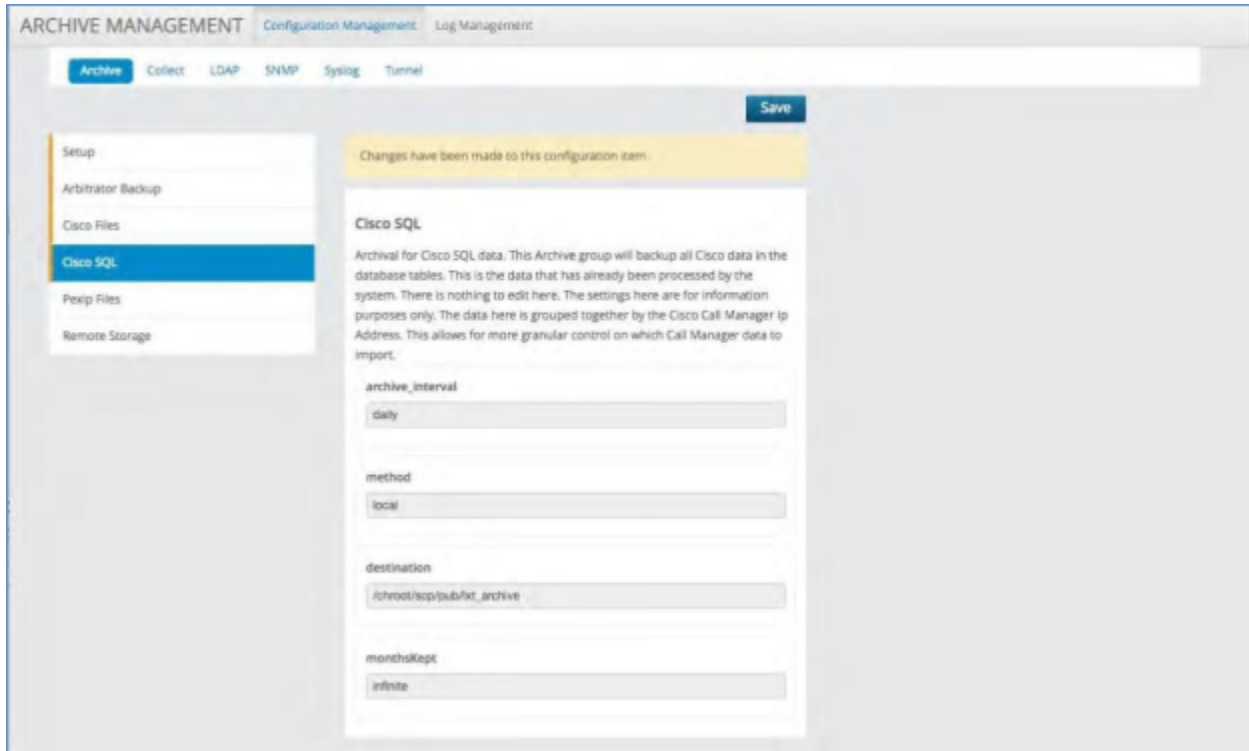
Cisco Files

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.

The screenshot displays the 'ARCHIVE MANAGEMENT' web interface. At the top, there are tabs for 'Configuration Management' and 'Log Management'. Below these, a navigation bar includes 'Archive', 'Collect', 'LDAP', 'SNMP', 'Syslog', and 'Tunnel'. A 'Save' button is located in the top right corner. On the left side, a sidebar menu lists 'Setup', 'Arbitrator Backup', 'Cisco Files' (which is highlighted in blue), 'Cisco SQL', 'Pcap Files', and 'Remote Storage'. The main content area features a yellow notification banner stating 'Changes have been made to this configuration item.' Below this, the 'Cisco Files' configuration section is shown. It includes a descriptive paragraph: 'Archival for Cisco files. This Archive group will backup all Cisco CDR and Cisco CMR raw files. These are the files that are shipped 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.' The configuration fields are: 'status' (dropdown menu set to 'enabled'), 'archive_interval' (dropdown menu set to 'daily'), 'method' (dropdown menu set to 'local'), 'destination' (text input field containing '/chroot/scp/pub/ftd_archive'), and 'monthsKept' (dropdown menu set to 'notSupported'). A small warning icon is visible next to the 'status' dropdown.

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.

Ndx

This screen can be used to manage Ndx files on the system.

max_ndx_file_size

1

The maximum size the ndx searchable file should be. Once the max size is hit, the ndx server will create a new ndx file.

max_searchable_days

1

The maximum number of days that should be searchable. Ndx files greater than this time will still live on the system but will not be searchable from the UI.

monthsKept

6

The maximum number of months to keep ndx archives around. Each archived ndx will take up disk space. Warning, increasing this number too large may require customer to also increase the hard disk size.

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.

The screenshot displays the 'ARCHIVE MANAGEMENT' web interface. At the top, there are tabs for 'Configuration Management' and 'Log Management'. Below these, a navigation bar includes 'Archive', 'Collect', 'LDAP', 'SNMP', 'Syslog', and 'Tunnel'. A 'Save' button is located in the top right corner. On the left side, a sidebar menu lists 'Setup', 'Arbitrator Backup', 'Cisco Files', 'Cisco SQL', 'Pexip Files' (which is highlighted in blue), and 'Remote Storage'. The main content area features a yellow notification banner stating 'Changes have been made to this configuration item'. Below this is the 'Pexip Files' configuration section, which includes a descriptive paragraph about archiving Pexip files and a warning about the 'disabled' status. The configuration fields are as follows:

- status:** A dropdown menu currently set to 'enabled'. Below it, text explains that 'enabled' keeps original files while 'disabled' removes them to conserve space.
- archive_interval:** A dropdown menu set to 'daily'.
- method:** A dropdown menu set to 'local'.
- destination:** A text input field containing '/chroot/scp/pub/txt_archive'.
- monthsKept:** A text input field containing 'notSupported'.

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 MANAGEMENT Configuration Management Log Management

Archive SQL
Cisco Files
Cisco SQL
Cisco Expressway SQL
Cisco RIS SQL
Cisco RTMT SQL
MSTeams SQL (legacy data)
Ndx
Oracle Files
Oracle SQL
Pexip Files
Pexip SQL
Polycom SQL
UHE SQL
Vdf Cisco
Vdf Ovip
Webex SQL

Remote Storage

Remote Storage

This page does not describe an Archive Group. If standard / local storage is chosen in the Archive Setup page, then this screen allows the user to configure remote archival of the systems 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 system.

archive_interval
daily

Select an option

- disabled
- nfs
- rsync
- rsyncToAtrb
- scp
- sftp

disabled - keep archives locally. nfs - Will mount a network file system as a local drive, which preserves local device disk space. scp - System will copy archives to a remote location. Scp is not a sync. In order 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. In order to reduce load on system and network, system only copies new / changing archives over to the sftp location. rsync - System will sync archive directory to remote system. The remote system must have rsync installed for this to work. rsyncToAtrb - System will sync archives directory to a remote system. This utilizes the rsync protocol so both systems will always be in sync.

IP location
172.30.42.175

username
sftpuser

password
.....

options

destination
/backups

monthsKept
infinite

- **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/1xt_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

Check NFS Host

Check NFS Mount

Check NFS Mount

- * **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 Tab

The Collect tab defines configuration options for the collection of CDRs.

Control

This panel enables and disables the processing of various file types. When a file type is disabled, files of this type are added to a backlog, and are processed when processing is re-enabled.

The table lists the control options you can enable and disable:

| | |
|-----------------|---|
| DEM | Enables/disables Digital Experience Monitoring (DEM) collection on the Arbitrator. DEM provides the ability to test connectivity to web-based systems, such as Microsoft Teams, and to deliver metrics for the following: <ul style="list-style-type: none">• Overall round-trip times to the application• The number of hops taken• Best and worst latency• The connection path, displayed hop-by-hop DEM agents on the Arbitrator provide connectivity and performance statistics to various MS Teams internet endpoints, including Microsoft Graph. When enabled, the job runs every 5 minutes, and policies (rules) imported to Arbitrator fire incident alerts when any of the DEM-collected metrics are out of the permitted thresholds. To verify that the Arbitrator policies are firing alerts and to view the logs, you can search in Arbitrator for either “dem_connectivity” or “dem_web_performance”. |
| Cisco UCM | |
| Oracle SBC | |
| Pexip | |
| NGIN | Enables/disables NGIN-XML processing |
| Palladion | |
| NMR | |
| Infovista GSIP | |
| Infovista IPSLA | |

The screenshot displays the Voss Archive Management Configuration Management interface. The top navigation bar includes 'ARCHIVE MANAGEMENT', 'Configuration Management', and 'Log Management'. Below this, a secondary navigation bar lists various configuration categories: API Config, Archive, Cisco SDL, **Collect**, Data User, Import, LDAP, License, Probe, Proxy, SNMP, Syslog, and Tunnel. A 'Save' and 'Delete' button is visible in the top right corner of the configuration area.

The main configuration area is titled 'Control' and contains a message: 'Changes have been made to this configuration item'. Below this message, the 'Control' section is detailed:

- Control**: This screen allows the file processing mechanism to be suspended. The system will still receive files, but the file contents will not be processed until re-enabled.
- DEM**: A dropdown menu is set to 'disabled'. Below it, the text reads: 'Enable/Disable Digital Experience Monitoring processing.'
- Cisco UCM**: A dropdown menu is set to 'enabled'. Below it, the text reads: 'Enable/Disable Cisco Unified Call Manager processing.'
- Cisco ME**: A dropdown menu is set to 'enabled'. Below it, the text reads: 'Enable/Disable Cisco ME processing.'
- Oracle SBC**: A dropdown menu is set to 'enabled'. Below it, the text reads: 'Enable/Disable Oracle Session Border Controller processing.'
- Pexip**: A dropdown menu is set to 'enabled'. Below it, the text reads: 'Enable/Disable Pexip processing.'

Cisco Remote Copy

This panel defines the storage location of collected Cisco CDR/CMR files.

The default location is "local", which is 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.

The screenshot displays the Voss Archive Management web interface. The top navigation bar includes the Voss logo and several icons. Below it, the main menu shows 'ARCHIVE MANAGEMENT' with sub-sections for 'Configuration Management' and 'Log Management'. A secondary menu lists various configuration options: 'API Config', 'Archive', 'Blue Jeans Config', 'Cisco SDL', 'Collect', 'Import', 'LDAP', 'Probe', and 'SNMP'. The 'Collect' option is currently selected. On the right side of the main menu, there are 'Save' and 'Delete' buttons.

The left sidebar contains a list of configuration categories: 'Avaya Datastore', 'Cisco', 'Cisco Remote Copy' (highlighted in blue), 'Oracle Microsoft Operator Connect', 'Vdf', and 'Voss Analytics'.

The main content area features a yellow notification banner at the top stating 'Changes have been made to this configuration item'. Below this, the 'Cisco Remote Copy' configuration form is displayed. The form includes a title 'Cisco Remote Copy' and a description: 'Use this to configure CDR/CMR forwarding to a remote system.' The form contains four input fields, each with a label and a description:

- IP location:** The input field contains '10.13.37.8'. The description below it reads: 'Specify the IP address of the remote location.'
- username:** The input field contains 'drop'. The description below it reads: 'Specify the username to be used to access the remote location.'
- password:** The input field contains a series of asterisks. The description below it reads: 'Specify the password to be used to access the remote location.'
- destination:** The input field contains '/chroot/scp/pub/cucm'. The description below it reads: 'Specify the path on the remote system.'

At the bottom of the form, there is a 'Verify Config' button.

Oracle Microsoft Operator Connect

If customer CDR folders for Oracle Call Manager were set up during Arbitrator setup, then parsing CDRs and using API calls to create the call record in the MS Tenant via the Operator Connect API is configured from the setup up on the **Oracle Microsoft Operator Connect** screen.

The screenshot displays the Voss Archive Management web interface. At the top, there is a dark blue navigation bar with the Voss logo and several icons. Below this is a light blue header with the text "ARCHIVE MANAGEMENT" and "Configuration Management" (which is highlighted). A secondary navigation bar contains various configuration options: API Config, Archive, Blue Jeans Config, Cisco SDL, Collect (highlighted), Import, LDAP, Probe, SNMP, Syslog, and Tun.

On the left side, there is a sidebar menu with the following items: Avaya Datastore, Cisco, Cisco Remote Copy, Oracle Microsoft Operator Connect (highlighted in blue), Vdf, and Voss Analytics.

The main content area on the right features a yellow notification banner at the top stating "Changes have been made to this configuration item". Below this is the configuration page for "Oracle Microsoft Operator Connect". The page includes the following sections:

- Oracle Microsoft Operator Connect**: Use this to configure SBC forwarding to Microsoft Operator Connect.
- Client ID**: A text input field with the instruction "Specify the client_id to be used to access the remote location."
- Client Secret**: A text input field with the instruction "Specify the client_secret to be used to access the remote location."
- Tenant**: A text input field with the instruction "Specify the tenant to be used to access the remote location."
- Resource**: A text input field.

For CDR folder setup, see the "Add Customer CDR Folders" topic in the Arbitrator Install Guide.

Import Tab

This tab allows you to import configuration data to a server from a csv file.

Note: Only csv file imports are supported.

LDAP Tab

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. Note that Microsoft AD passwords are never stored locally. Authentication always occurs with external Microsoft AD. Once authenticated, the system allows a user access based on their local system privileges. In order to properly configure these settings, the customer administrator requires an in-depth knowledge of the customer's Microsoft AD architecture. Improper configuration may cause too little or too many users in the system.

The screenshot displays the Voss Archive Management web interface. The top navigation bar includes the Voss logo and various system icons. Below the navigation bar, the main menu shows 'ARCHIVE MANAGEMENT' with sub-menus for 'Configuration Management' and 'Log Management'. The 'Configuration Management' sub-menu is active, and the 'LDAP' tab is selected. The page title is 'External Config'. A yellow notification banner at the top right states 'Changes have been made to this configuration item'. The main content area is titled 'External Config' and contains a detailed description of the system's LDAP configuration options. Below the description, there is a 'Test LDAP configuration' section with a 'Test LDAP configuration' button and a note: 'Use this button to test the configuration that is filled in the form below.' The form includes three fields: 'external_type' (a dropdown menu set to 'local'), 'is_ssl' (a dropdown menu set to 'true'), and 'ip' (a text input field). Below the 'ip' field, a note states: 'Required only for 'windows' setting. Ip Address of Microsoft Active Directory.'

License Tab

This tab registers your system for integration with the VOSS Cloud License service for user license count auditing, and allows the licensed user counts files to be sent to VOSS automatically.

You can also view and download license files on this tab, and upload license files to VOSS.

The screenshot shows the VOSS ARCHIVE MANAGEMENT interface. The top navigation bar includes 'ARCHIVE MANAGEMENT', 'Configuration Management', and 'Log Management'. Below this, a secondary navigation bar lists various configuration options: 'API Config', 'Archive', 'Cisco SDL', 'Collect', 'Data User', 'Import', 'LDAP', 'License', 'Probe', 'Proxy', 'SNMP', 'Syslog', and 'Tunnel'. The 'License' option is currently selected. On the right side of the navigation bar, there are 'Save' and 'Delete' buttons. A yellow notification banner at the top of the main content area reads 'Changes have been made to this configuration item'. The main content area is titled 'License' and contains the following information:

- License**: This screen manages licensing with VOSS. This screen may be used to enable the periodic license delivery to VOSS. If applicable, please update firewall policies to allow interaction with platform.voss-solutions.com. Additionally, please configure proxy settings for external connectivity, if necessary.
- enabled**: A dropdown menu currently set to 'false'. Below it is the text 'Opt-in/Enable the automatic sharing of the license file.'
- organization id**: A text input field containing 'adsf'. Below it is the text 'The VOSS organization id associated with this device.'
- environment type**: A dropdown menu currently set to 'production'. Below it is the text 'The VOSS account id (organisation id) associated with this device.'
- description**: A text input field containing 'A description'. Below it is the text 'A description of this device.'
- Fetch License File**: A button labeled 'Fetch License File'.

At the bottom left of the interface, there is a 'Running command' button.

Related Topics

- [License Auditing](#)

Proxy Tab

To allow for cloud services access, proxy configuration (both authenticated and unauthenticated) is supported.

You can configure the Proxy on the Arbitrator **Settings** menu from **ARCHIVE MANAGEMENT > Configuration Management > Proxy**.

The screenshot shows the Voss Archive Management web interface. At the top, there is a dark blue navigation bar with the Voss logo and various icons. Below this is a light grey breadcrumb trail: ARCHIVE MANAGEMENT > Configuration Management > Log Management. A secondary navigation bar contains links for API Config, Archive, Blue Jeans Config, Cisco SDL, Collect, Import, LDAP, Probe, Proxy (highlighted with a red box), SNMP, Syslog, and Tunnel. On the right side of this bar are Save and Delete buttons. A yellow notification banner at the top of the main content area states: "Changes have been made to this configuration item". The main content area has a blue header for "Proxy Config". Below this, a description reads: "Adds configuration for Proxy use in external data creation." The configuration form includes four input fields: "ipAddress" (containing "10.0.0.1"), "proxyPort" (containing "19001"), "userName" (containing "UserX"), and "password" (containing "*****"). Each field has a descriptive label below it. At the bottom of the form, there are two sections: "Set Proxy" with a "Set Proxy" button and "Remove Proxy" with a "Remove Proxy" button. Both sections include instructions on how to use the buttons.

1. Fill out the required **Proxy Config** values: **ipAddress**, **proxyPort**, **userName** **password**.
2. Click **Save**.
3. To enable the saved values, click **Set Proxy**.

Important: The proxy is used only by services that use APIs for their data, and are set up in **Archive Management > Configuration Management > API Config**: Webex, Teams and Zoom.

If it is necessary to remove the proxy configuration, click **Remove Proxy**. This will reset the configuration to empty settings from the system. In order to clear the configuration screen, you will then need to click **Delete** at the top of the form. This will remove any confusion as to the proxy settings in the future.

SNMP Tab

This tab configures SNMP v3 user config, which allows the system to be configured to work with SNMP v3. It allows you to select the specific authentication and encryption methods to be used.

The screenshot shows the 'SNMPv3 User Config' configuration page within the 'ARCHIVE MANAGEMENT' interface. The page is part of the 'Configuration Management' section, with sub-sections for 'Archive', 'Collect', 'LDAP', 'SNMP', 'Syslog', and 'Tunnel'. A 'Save' button is visible in the top right corner. The main configuration area is titled 'SNMPv3 User Config' and includes a message: 'Changes have been made to this configuration item'. Below this, there is a 'Commit SNMPv3 User Configuration' button. The configuration fields are as follows:

- Engine ID:** OCTECT STRING
- User Name:** OCTECT STRING
- Authentication Protocol:** MD5
- Authentication Pass Phrase:** (empty text field)
- Encryption Protocol:** AES
- Encryption Pass Phrase:** (empty text field)

Syslog Tab

This tab configures the IP address of your central syslog server.

Note: This is a system-wide setting.

The system can send out syslog messages about several of the internal functions, including backup and archival success. If an IP address is specified, the system will send any internal VOSS Insights messages onto the specified syslog server.

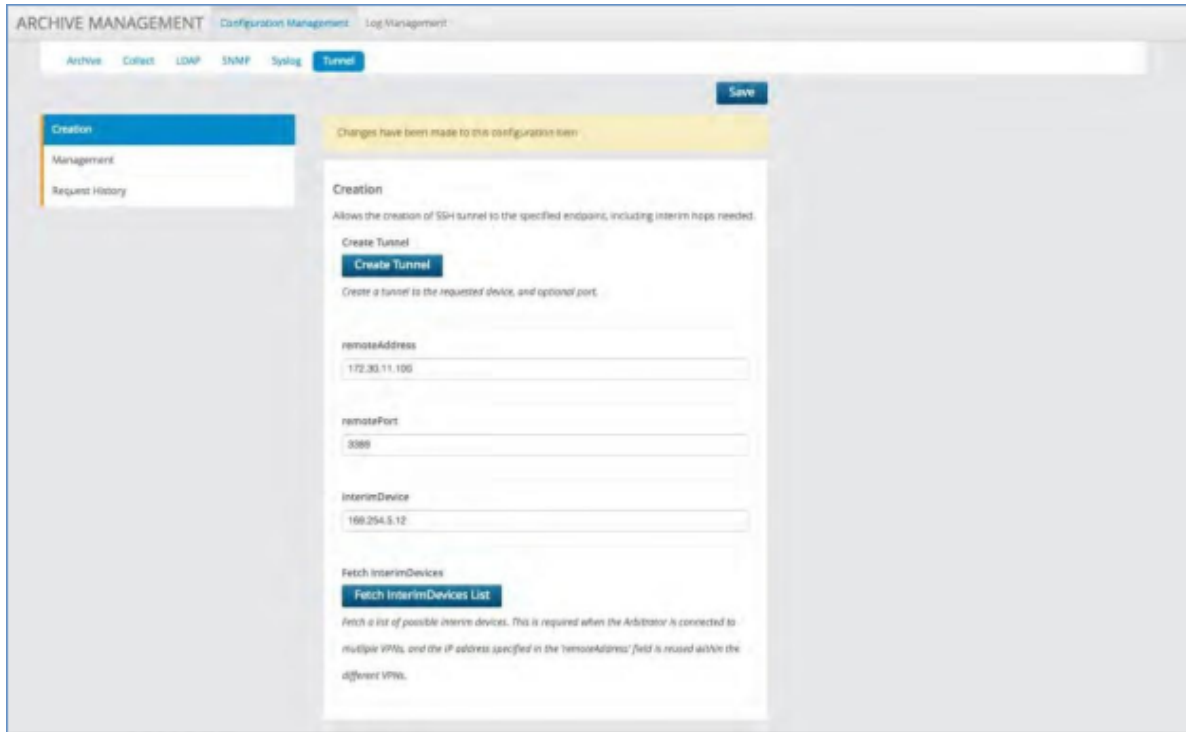
Only one central syslog server can be specified at this time. Please validate firewall settings are open to allow incoming messages on the specified IP address and port.

The screenshot shows the 'Syslog Server' configuration page within the 'ARCHIVE MANAGEMENT' interface. The page title is 'Syslog Server' and it includes a 'Save' button. A yellow notification banner at the top states 'Changes have been made to this configuration item'. The main content area is titled 'Syslog Server' and contains the following text: '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 Layer X 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.' Below this text are three input fields: 'external_syslog_ip' (with a text input field), 'protocol' (with a dropdown menu showing 'tcp'), and 'external_syslog_port' (with a text input field showing '514'). Each input field has a small 'Optional' label and a note: 'Optional. Enter in the ip address of your organization's central syslog server. A single Ip Address or a single Domain name. Note. Domain name entries must resolve through the system configured DNS (asn specified in system DNS settings)' for the IP field, and 'Optional. Enter in the port. Default syslog port is 514' for the port field.

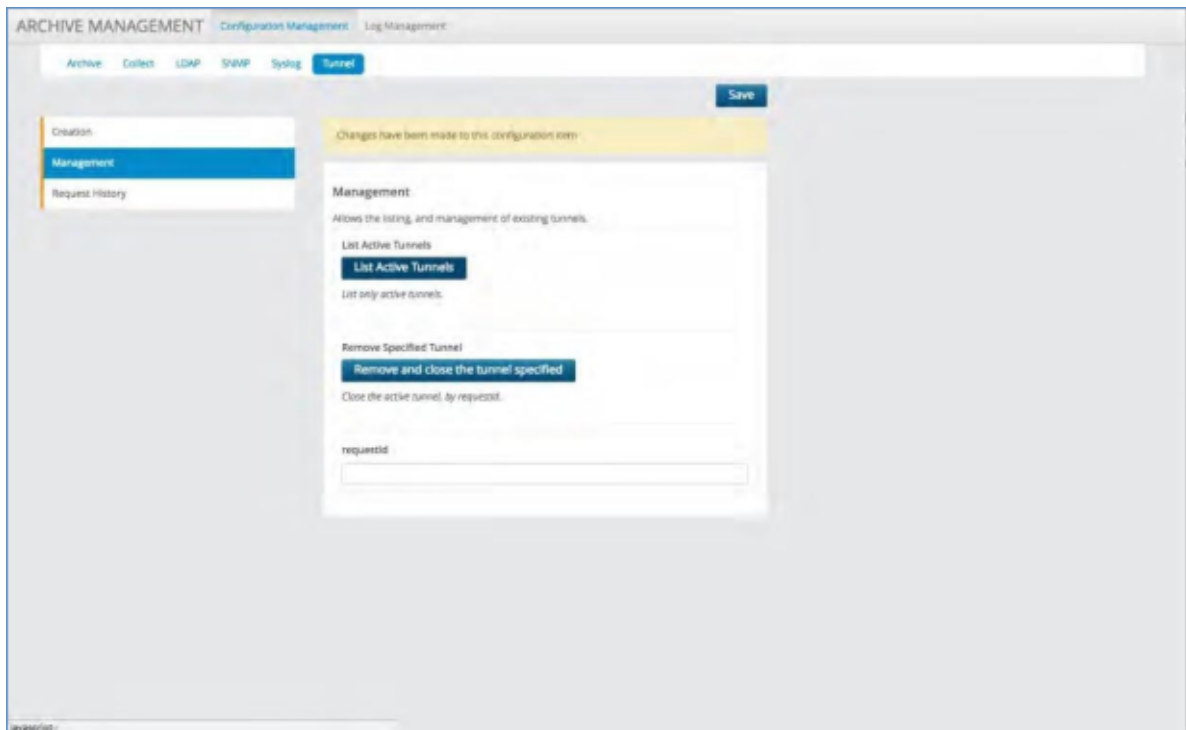
Tunnel Tab

This tab allows you to create VPN tunnels between Arbitrator platforms. Three options are available:

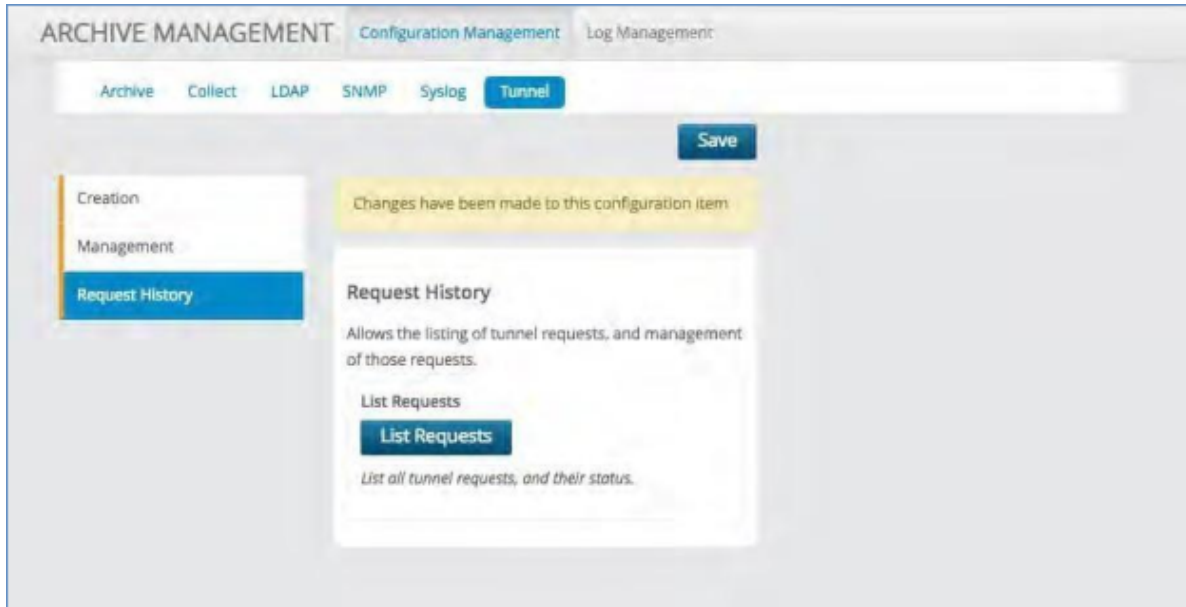
- Creation - allows creation of SSH tunnel to the specified endpoint, including the interim hops needed.



- Management - used for listing and managing all of the existing tunnels.



- Request History - allows listing of tunnel requests and management of those requests.



4.11.3. Log Management Tab

The **Log Management** tab (in **Archive Management**) allows you to customize the archival of the index data store. It can be performed based on Size, Time or a combination of both.

Set the archival process

This procedure sets up the archival process.

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


Archive Methods

| <input type="checkbox"/> IP Address | Method |
|-------------------------------------|--------|
| 0.0.0.0 | SCP |
| | SCP |
| | SFTP |
| | SMP |

ARCHIVE MANAGEMENT Configuration Management: Log Management

Errors exist Save

Archive Settings



● Used Space (570 GB) ● Free Space (375 GB)

Current Intervals

4 GB

10 Days

Last Archive Time

Aug 19, 2018 13:50

Archive Index Every

4 GB

10 Days

Alerting Options

Alert on archive success

Alert on archive failure

Archive Methods

| <input type="checkbox"/> IP Address | Method | Path | Credentials |
|-------------------------------------|--------|------|-------------|
| 0.0.0.0 | SCP | | None |

+

4.12. Tools

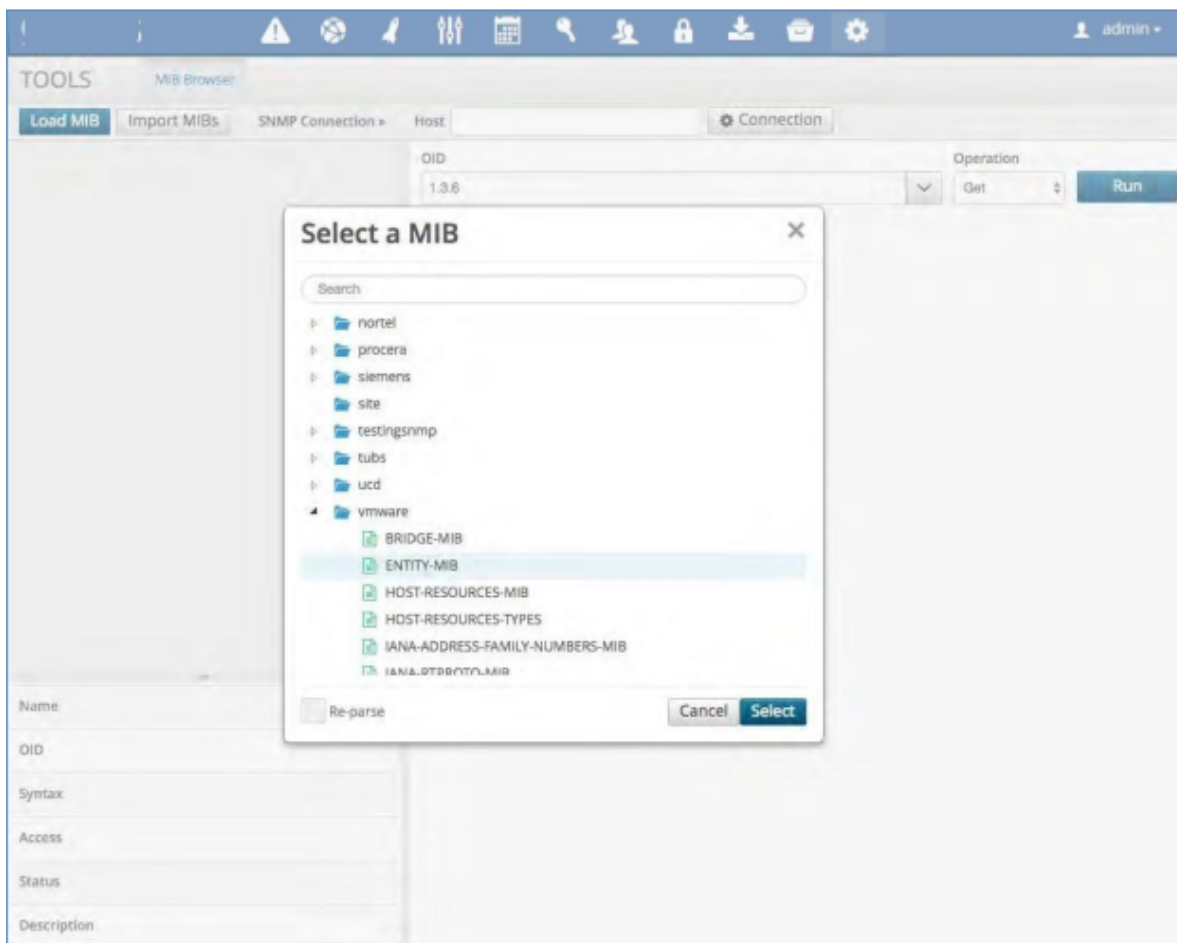
4.12.1. Overview

The **SNMP Tools** page allows you to load or import MIBs and then build SNMP actions/ scripts to be saved as probes within the platform.

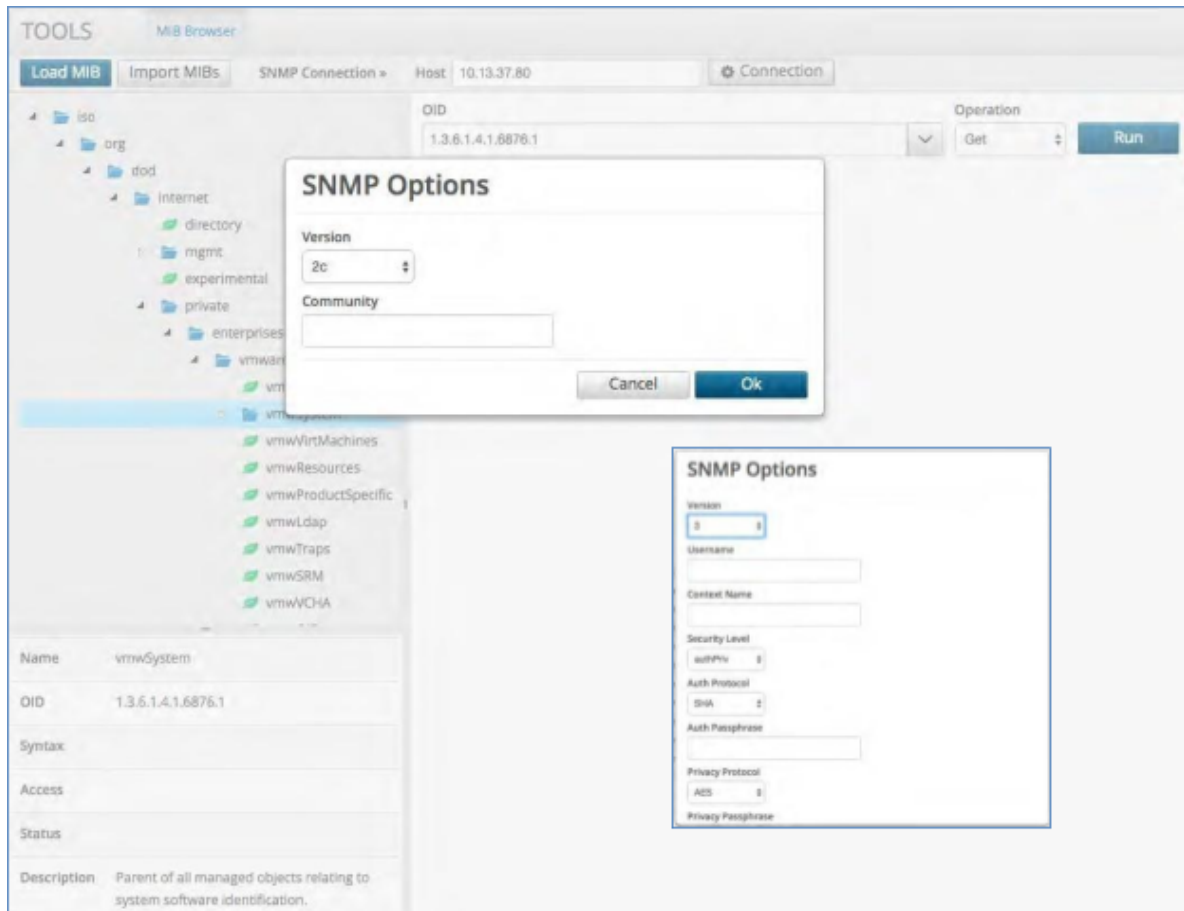
Insights ships with a library of MIBs that can be opened by choosing the **Load MIB** button. If a new one is needed it can be imported by selecting the **Import MIBs** button.

4.12.2. Load a MIB

1. On the **Tools** page, click **Load MIB**.
2. In the **Select a MIB** dialog, view the choice of all the manufacturer MIBs available in the system, then select the relevant MIB.
3. Scroll through and select the desired MIB.



3. Once selected you can open up all of the branches and leaves and view each associated OID.
4. Choose the folder you wish to use, and fill out the connection settings for that system.
5. 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.



6. Choose the operation to perform: GET, GET NEXT or WALK
7. 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.
8. Do this for each Probe you want to create.

The screenshot shows the 'OID' management interface. At the top, the 'OID' field contains '1.3.6.1.4.1.6876.1'. An 'Operation' dropdown menu is open, showing options: 'Get' (checked), 'Get Next', and 'Walk'. A 'Run' button is visible to the right. Below this is the 'Results' section, which includes a search bar for 'Text OID', a 'Toggle Numeric/Text OID' button, and a 'Create Probe' button. The main table displays the following data:

| Text OID | Value | Type |
|--|-------------|--------|
| <input checked="" type="checkbox"/> VMWARE-SYSTEM-MIB::vmwProdName.0 | VMware ESXi | STRING |
| <input type="checkbox"/> VMWARE-SYSTEM-MIB::vmwProdVersion.0 | 6.0.0 | STRING |
| <input type="checkbox"/> VMWARE-SYSTEM-MIB::vmwProdBuild.0 | 2494585 | STRING |
| <input type="checkbox"/> VMWARE-SYSTEM-MIB::vmwProdUpdate.0 | 0 | STRING |
| <input type="checkbox"/> VMWARE-SYSTEM-MIB::vmwProdPatch.0 | 0 | STRING |

The 'Create Probe' dialog box is shown. It contains the following fields and options:

- OID:** .1.3.6.1.4.1.6876.1.1.0
- Probe Name:** (empty text field)
- Add to existing probe group**
 - Application:** ssh probe
- Create a new probe group**
 - Probe Group Name:** (empty text field)

Buttons for 'Cancel' and 'Create' are located at the bottom right.

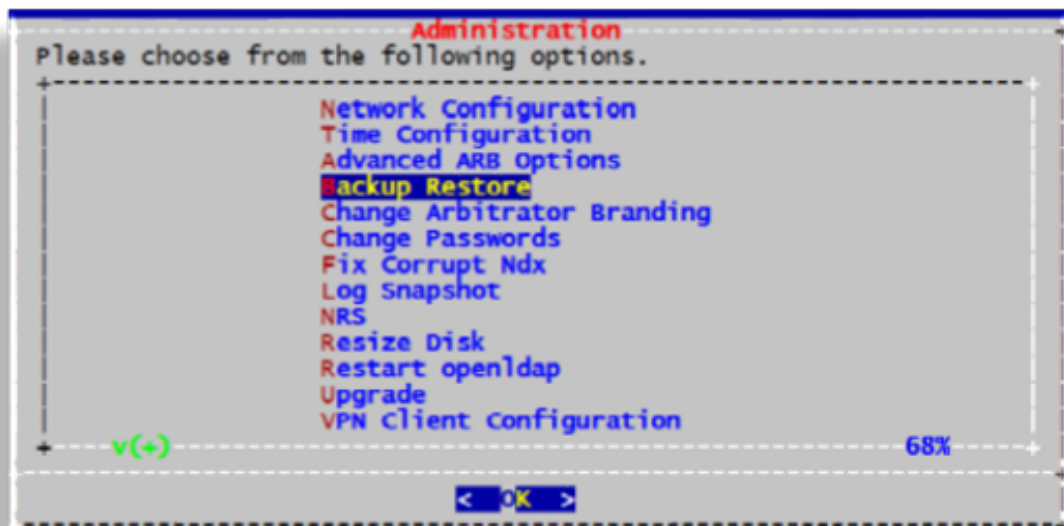
9. When you select "Create Probe" a new box will open that will allow you to give the Probe a name and either save it to an existing Probe Group or create a new one.
10. Now you have a new Probe that will run the particular SNMP command you requested.

5. Arbitrator Maintenance

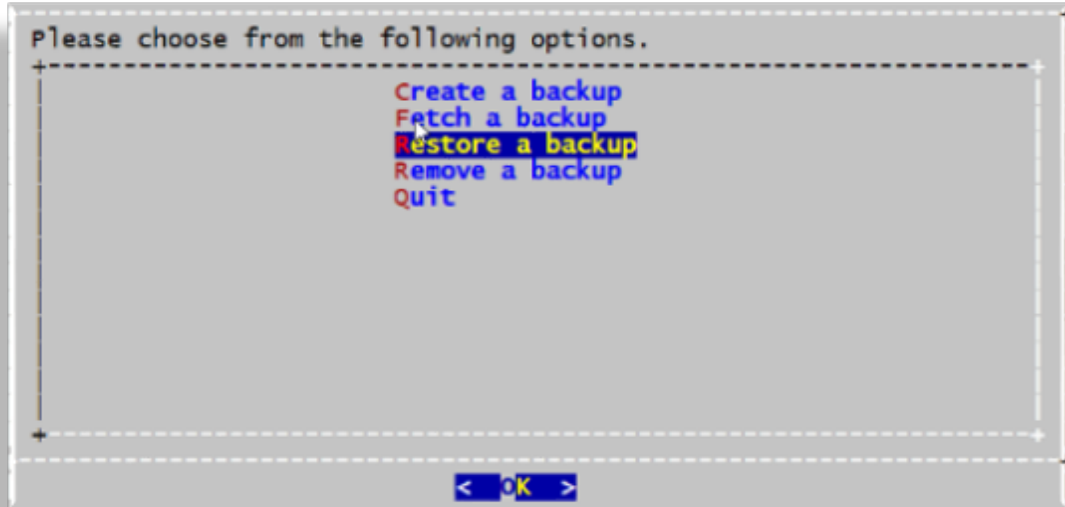
5.1. Backup and Restore the Arbitrator

This procedure backs up Insights Arbitrator, retrieves the backup files, and restores the system.

1. Configure the Arbitrator backup. See *Archive Tab*.
2. Restore the Arbitrator application from a backup:
 1. Log in to CLI as an admin.
 2. In the **Administration** menu, select **Backup Restore**, then click **OK**.



3. Select **Restore a backup**.



4. Optionally, run the `Fetch` command to retrieve backup files.
5. Select the local backup you wish to restore. Choose an option:
 - To restore data from the nightly backups, select `self`.
 - To restore from another source, including a remote backup of this device, select the relevant source.

Note: Additional restore locations can (optionally) be retrieved using the `Fetch` command, or the **Restore** screen selects this device as the target of the `rsyncToArb` method.

6. Select the data types to restore. The image provides an example. Later releases may include additional data types:



7. 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)
█
```

8. 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)?
```

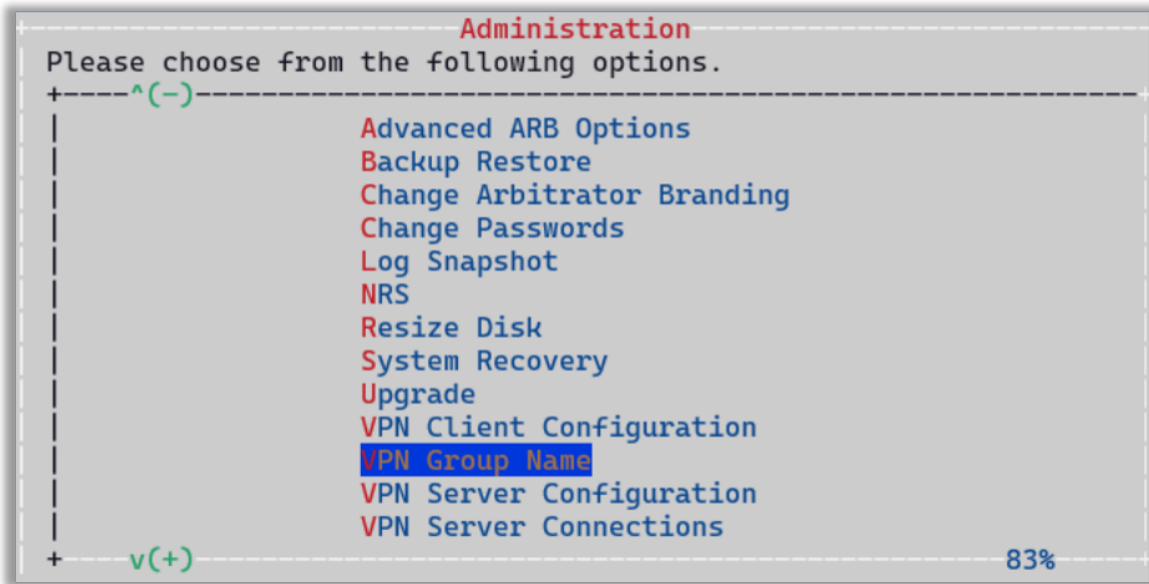
9. Monitor restore progress. A system message confirms when the restore is complete.

Important: Restoring Insights Arbitrator may take several hours, especially on larger systems and/or when restoring more data.

5.2. System Recovery

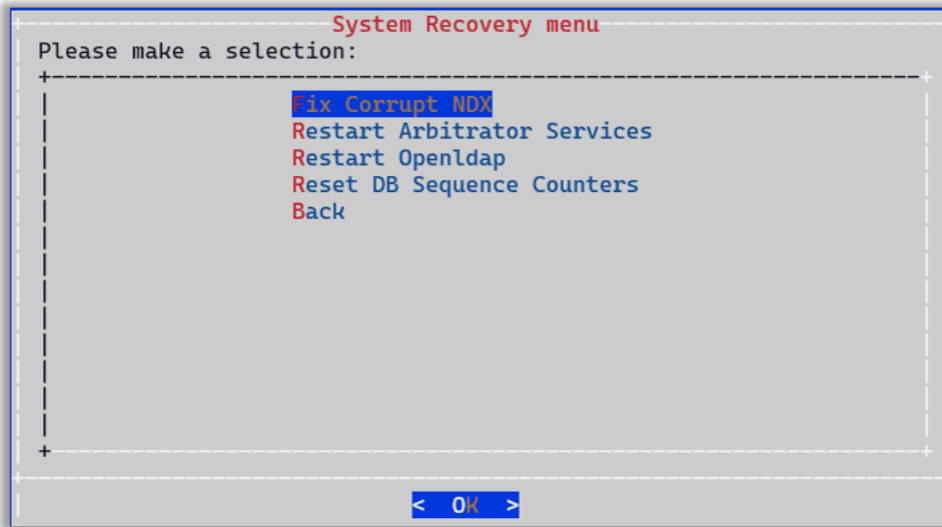
This procedure provides access to options that allow you to troubleshoot and recover Arbitrator services in the event of system errors.

1. Log in to CLI as an admin.
2. On the **Administration** menu, select **System Recovery**.



3. On the **System Recovery** menu, choose an option for the issue you're trying to resolve. Options are:

| | |
|-----------------------------|--|
| Fix corrupt NDX | May be used to repair the NDX. The NDX is the backbone of the "Search" screen in the user interface. If the "Search" screen displays zero results, the NDX may be corrupt. This option terminates the current NDX files and start a new NDX set of files. |
| Restart Arbitrator services | Allows you to restart the Arbitrator's core services involved in collection, correlation, and alerting. This option is useful when attempting to debug a scenario where alerts are not firing. |
| Restart OpenLDAP | Used specifically for restarting the OpenLDAP service. This option is useful when attempting to debug authentication issues in the user interface. |
| Reset DB sequence counters | This option provides an optional (last resort) method for resolving a rare scenario when alerts stop firing. If you've exhausted the normal troubleshooting checks for alerting, this option may be used as a final resort. This method has been shown to fix rare issues in the past, and is provided as an option until the issue may be auto-detected and automatically repaired. |



5.3. Network Observability

5.3.1. Overview

Network observability is configured on the Arbitrator as a set of probe scripts that collect and analyze data from the customer's network devices.

Note: The probe scripts comprise a set of SNMP v2 scripts and a set of SNMP v3 scripts. Both v2 and v3 of the SNMP scripts perform the same function. The version you'll use depends on whether your device supports SNMP v2 or SNMP v3.

Data is presented for analysis via read-only network observability reference dashboards in the Insights Dashboard system. The dashboards have read access to the database tables on Arbitrator, and allow you to determine in greater detail why alerts have occurred.

Related Topics

- [Probe Configuration](#)
- [Asset Configuration](#)
- [Insights Reference Dashboards in the Dashboard Administration Guide](#)

5.3.2. Configure Network Observability Probe Groups

This procedure configures network observability probe groups in Arbitrator.

1. Log in to the Arbitrator.
2. Click the toolbar Wrench icon to open the **System Configuration** interface.
3. Click the **Probes** icon to open the **Probe Configuration** page.
4. Click the Plus icon (+) at the bottom of the **Groups** panel to add the first probe group, then fill out a probe group name, and tab out of the field to add the probe group.

Important: We have provided a recommended configuration of the following four probe groups, including a recommended naming convention and probe configuration parameters, in [Network Observability](#):

- Network Observability 5 min
- Network Observability 10 min
- Network Observability SNMP 10 min
- Network Observability SNMP 5 min,

For example, for the first probe group you add, you can use *Network Observability 5 min* as the probe group name.

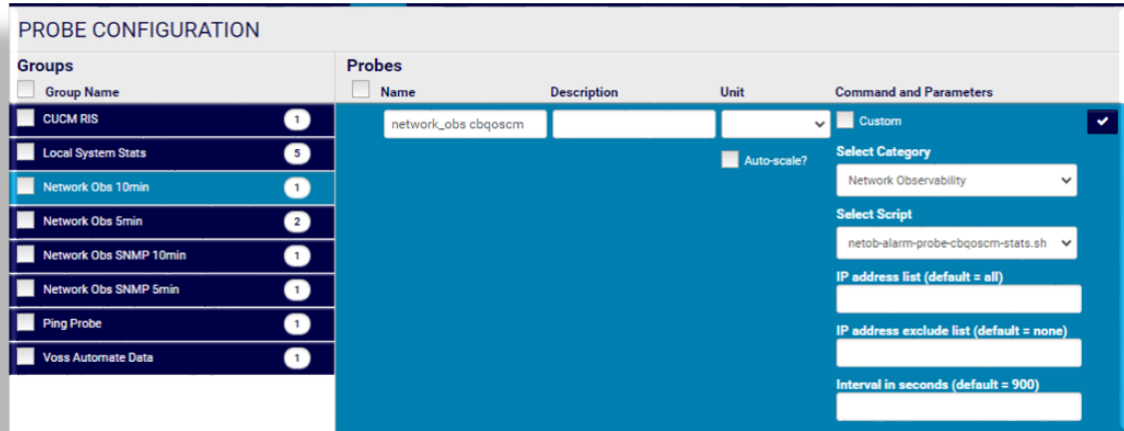
5. Add the probes for the probe group you added.

Note: It is recommended that you use the probe configuration parameters provided in the table, in [Network Observability](#).

- On the **Probes** panel, at **Select Category**, click the down-arrow, then select **Network Observability**.

Note: Clear the **Custom** checkbox to display the **Select Category** drop-down.

- Fill out the probe name.
- Select the relevant script, based on the recommended configuration in [Network Observability](#).
- If relevant for the probe you're configuring, you will need to provide SNMP credentials.
- Click the check icon to save the probe.



6. Repeat these steps to add the rest of the probe groups and probes required for network observability, based on the settings provided in *Network Observability*.
7. Click **Save**.

Next steps:

- Once you've set up the probe groups, the SNMP probe groups are applied to the device you're collecting data from.
- Assign customers to assets. For details, see *Asset Configuration*

In order for the network observability probe groups to return useful data, the corresponding assets should have “customer” and “site” assignment. This is done via the **Asset Configuration** menu in Arbitrator.

- In **Asset Configuration**, locate the Arbitrator (in the **Assets** panel).
 - Click on the wrench icon to configure the monitor profile.
 - Drag the relevant probe group into the **Templates/Profiles** panel, then click the wrench icon to set the frequency, as per the settings for the probe group in *Network Observability*.
- Repeat this step to add other probe groups, and to configure their frequency.
- Click **Update**.

5.3.3. Recommended Network Observability Probe Group Configuration

This topic describes a recommended setup for the four probe groups required for optimal network observability.

The table describes the recommended network observability probe group configuration:

| Probe Group | Configuration |
|--------------------------------------|---|
| 1. Network Observability 5 min | <p>There are two probes to set up for this probe group:</p> <ol style="list-style-type: none"> 1. Network Observability Asset Impact This probe detects the impact of network observability alarms on locations. <ul style="list-style-type: none"> • Scripts to use with this probe: <ul style="list-style-type: none"> – <code>netob-asset-impact-assessment.sh</code> • Category: Network Observability • Parameters: N/A • Applied to: Arbitrator • Frequency: 5 minutes • Credentials: N/A 2. Network Observability Interface Event Detections This probe detects the interface counter changes for discards and errors. <ul style="list-style-type: none"> • Script to use with this probe: <ul style="list-style-type: none"> – <code>netob-alarm-probe-interface-stats.sh</code> • Category: Network Observability • Parameters: Use defaults, unless customization is required. • Applied to: Arbitrator • Frequency: 5 minutes • Credentials: N/A |
| 2. Network Observability 10 min | <p>This probe group contains one probe. The probe detects the cbqoscm counter changes.</p> <ul style="list-style-type: none"> • Probe name: Network Observability CB QoS Event Detections • Script to use with this probe: <ul style="list-style-type: none"> – <code>netob-alarm-probe-cbqoscm-stats.sh</code> • Category: Network Observability • Parameters: Use defaults, unless customization is required. • Applied to: Arbitrator • Frequency: 10 minutes • Credentials: N/A |
| 3. Network Observability SNMP 10 min | <p>This probe group contains one probe. The probe is used for netob-cisco-cbq-mib-stats-snmpv3 collection for group01.</p> <ul style="list-style-type: none"> • Probe name: Network Observability CBQ • Script to use with this probe - either of the following: <ul style="list-style-type: none"> – <code>netob-cisco-cbq-mib-stats-snmpv3.sh</code> – <code>netob-cisco-cbq-mib-stats-snmpv2c.sh</code> • Category: Network Observability • Parameters: Supply appropriate credentials, where applicable. • Applied to: Asset • Frequency: 10 minutes • Credentials: SNMP |

| Probe Group | Configuration |
|-------------------------------------|--|
| 4. Network Observability SNMP 5 min | <p>This probe group contains one probe. The probe is used for netob-ifmib-interface-stats-snmpv3 collection for group01.</p> <ul style="list-style-type: none">• Probe name: Network Observability Interface• Script to use with this probe - either of the following:<ul style="list-style-type: none">– netob-ifmib-interface-stats-snmpv3.sh– netob-ifmib-interface-stats-snmpv2c.sh• Category: Network Observability• Parameters: Supply appropriate credentials, where applicable.• Applied to: Asset• Frequency: 5 minutes• Credentials: SNMP |