Arbitrator Data Correlation Administration and User Guide

Jul 01, 2021

Legal Information

Please take careful note of the following legal notices:

-
- VOSS, VisionOSS and VOSS-4-UC are trademarks of VisionOSS Limited.
- No part of this document may be reproduced or transmitted in any form without the prior written permission of VOSS.
- VOSS does not guarantee that this document is technically correct, complete, or that the product is free from minor flaws. VOSS endeavors to ensure that the information contained in this document is correct, whilst every effort is made to ensure the accuracy of such information, VOSS accepts no liability for any loss (however caused) sustained as a result of any error or omission in the same.
- This document is used entirely at the users own risk. VOSS cannot be held responsible or liable for any damage to property, loss of income, and or business disruption arising from the use of this document.
- The product capabilities described in this document and the actual capabilities of the product provided by VOSS are subject to change without notice.
- VOSS reserves the right to publish corrections to this document whenever VOSS deems it necessary.
- All vendor/product names mentioned in this document are registered trademarks and belong to their respective owners. VOSS does not own, nor is related to, these products and vendors. These terms have been included to showcase the potential of the VOSS solution and to simplify the deployment of these products with VOSS should you select to utilize them.

Security Information

This product may contain cryptographic features that may be subject to state and local country laws that govern the import, export, transfer and use of such features. The provision of this software does not imply that third-party authorization to import, export, distribute or use encryption in your particular region has been obtained. By using this product, you agree to comply with all applicable laws and regulations within your region of operation. If you require further assistance, please contact your dedicated VOSS support person.

Contents

1. What’s New

1.1. Arbitrator Data Correlation Administration and User Guide: Release SP23

- Arbitrator License remaining days will now be displayed in UI upon login.See: *Arbitrator Licensing*
- New PRI and SIP Trunk probes for Cisco Voice Gateways. Please reference Arbitrator Cisco PRI and SIP Probe Configuration for instructions.See: *Configuration*
- New config screen added to allow customer ndx file retention times. Default is 6 months.See: *Configuration*

2. Introduction

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

2.1. Purpose

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

2.2. Intended Audience

The audience intended for this User's Guide includes 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.

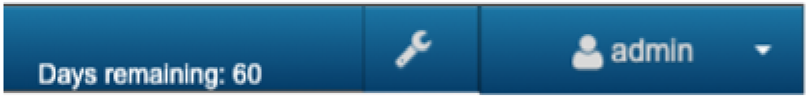
2.3. Organization

The Arbitrator platform design allows it to be used in multiple workflows. There isn't any linear flow that has to be followed. However, there are some elements that need to be configured in a specific order. Those will be pointed out in each section. This document is categorized as follows:

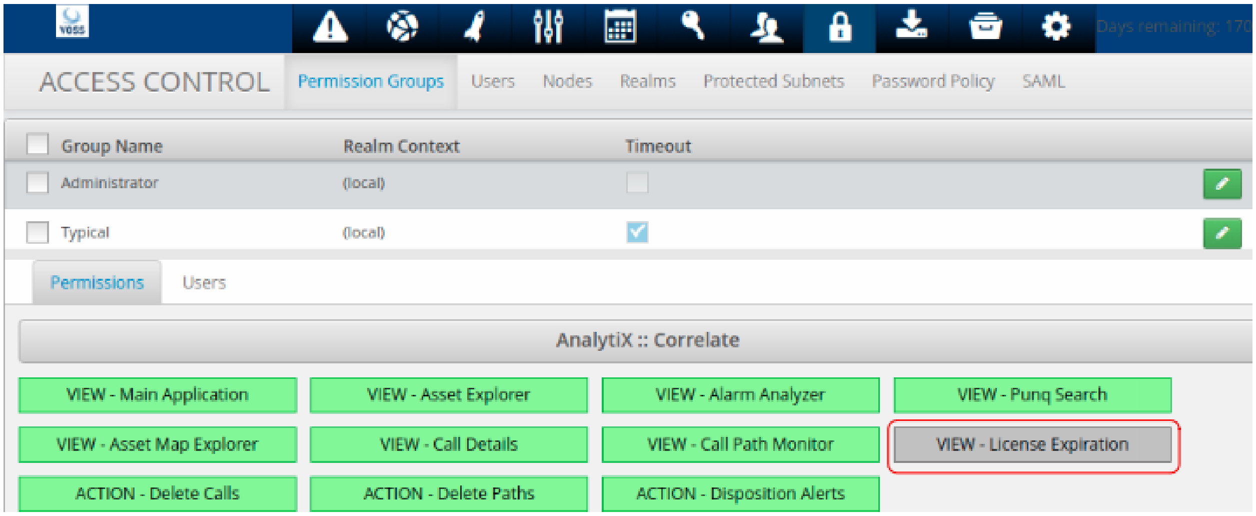
1. Correlate: This is the main UI screen to visualize the monitored systems and manage alerts for those systems. This is the primary view where the user spends the most time. The views within this workspace are constantly updating with the newly gathered data.
2. Configuration: This is the workspace utilized to perform configuration, setup and installation of the platform.

3. Arbitrator Licensing

The Arbitrator License remaining days is displayed in the UI upon login.



This **VIEW - License Expiration** setting can be enabled or hidden from the **Permission Groups** on the **ACCESS CONTROL**:



□ Group Name	Realm Context	Timeout
□ Administrator	(local)	□
□ Typical	(local)	☑

Alternatively, to see how many days left from the main menu for the logged in user:

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

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 licence file.

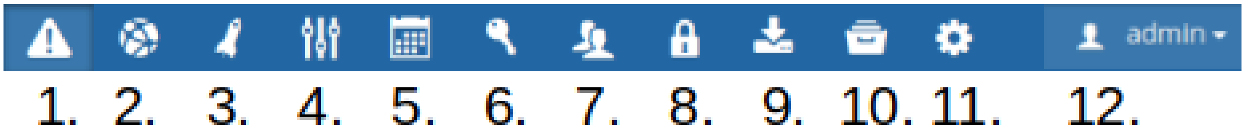
4. Correlate

4.1. Menu Bar

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

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

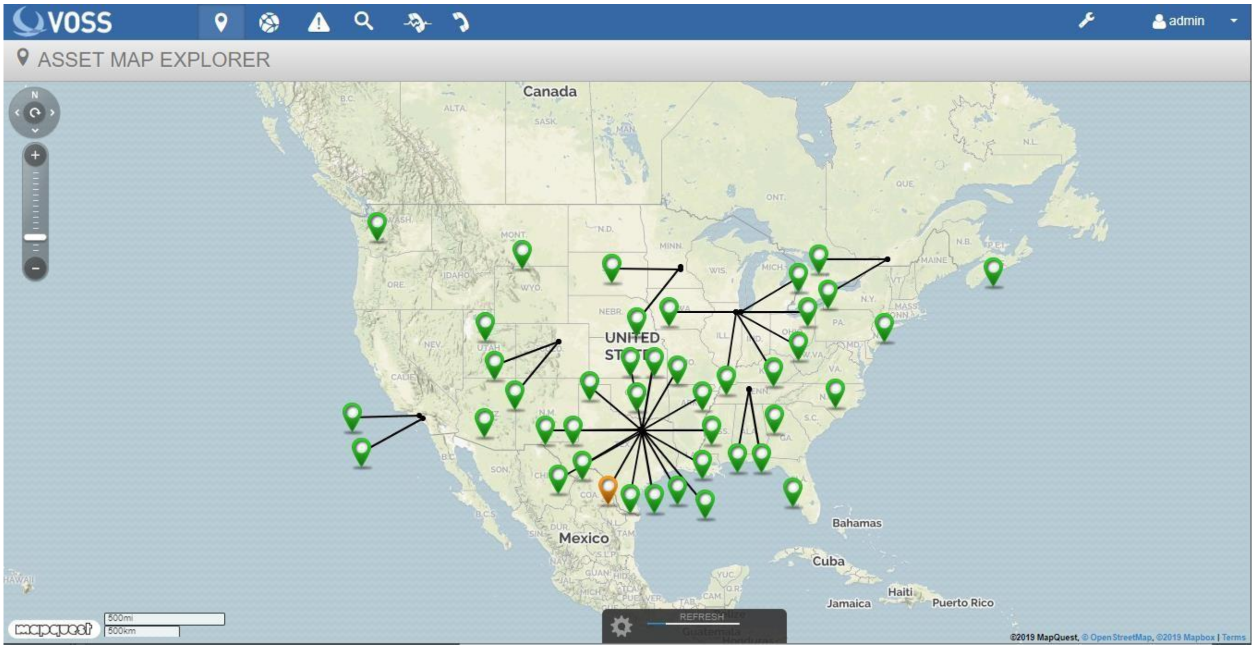
This menu is located at the top of the browser page and allows you to navigate to each of the Arbitrator views. Each are shown below:



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

4.2. Assets

4.2.1. Asset Map Explorer



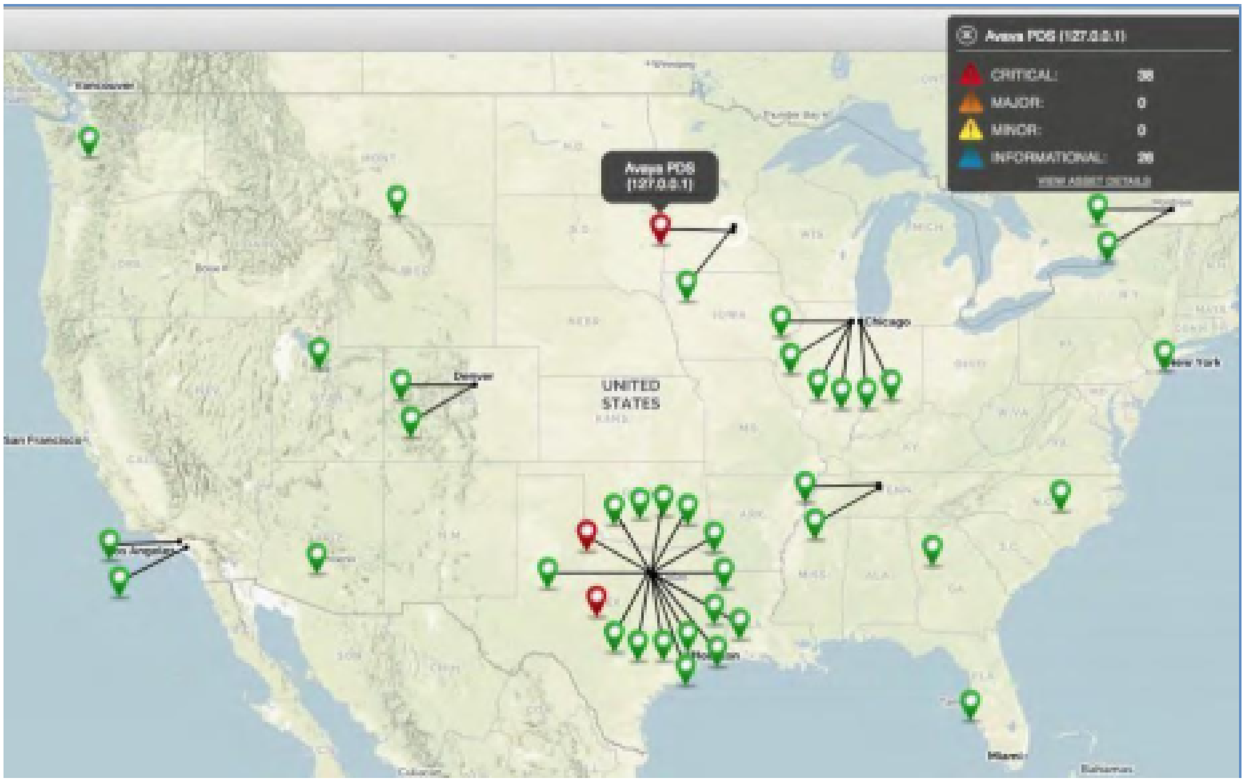
This view displays all of the defined assets in the system on a map for visual grouping according to their physical location. The location or address of the assets are input in the asset configuration section within the Configuration interface. This view is integrated with the MapQuest API (Internet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

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

4.2.2. Asset Overview

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

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



Avaya PDS (127.0.0.1)

CRITICAL: 38

MAJOR: 0

MINOR: 0

INFORMATIONAL: 28

VIEW ASSET DETAILS

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

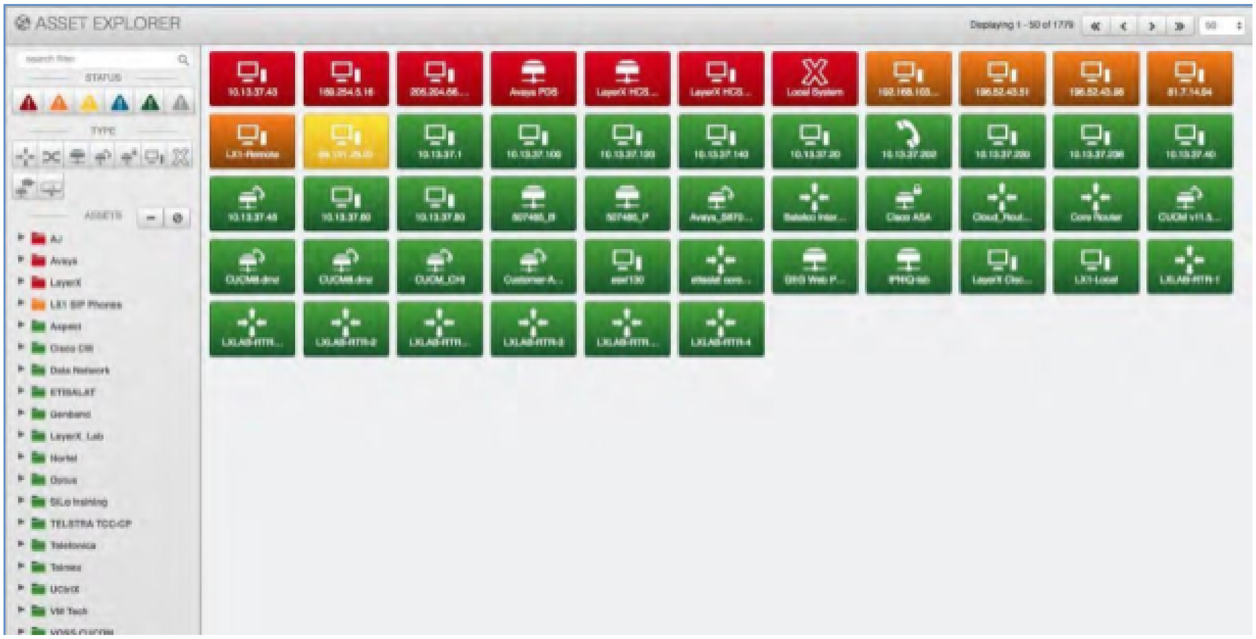
4.2.3. Asset Explorer

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

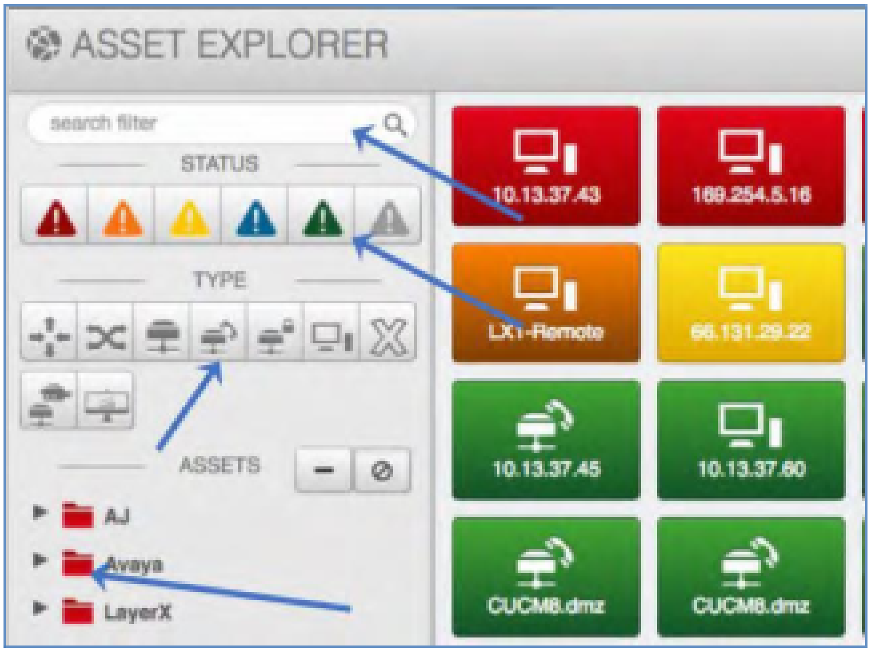
Only devices created as Assets in the Arbitrator system will be rendered in the view. Since Correlated events create alarms in the system, asset icon colors will change to reflect the severity level of the alert. Assets display the color of the current highest-level alert for that asset in the system.

Alert Severity Levels:

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



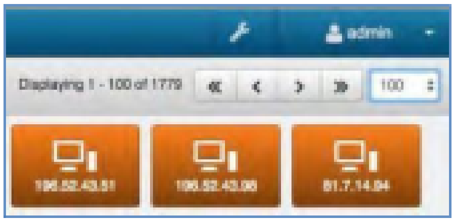
4.2.4. Asset Filtering



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

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

4.2.5. Asset Explorer Navigation



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

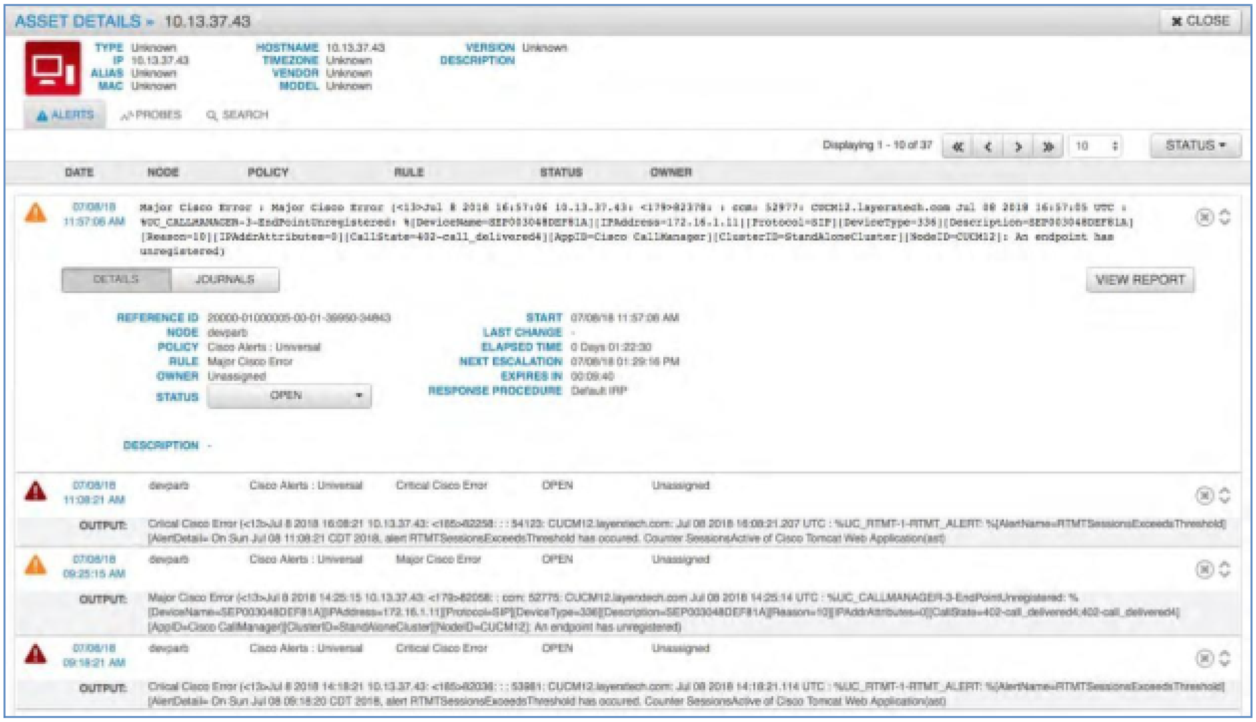
4.2.6. Asset Details View

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

- Alerts
- Probes
- Search

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

4.2.7. Asset Details: Alerts Tab



TYPE Unknown
IP 10.13.37.43
ALIAS Unknown
MAC Unknown
HOSTNAME 10.13.37.43
TIMEZONE Unknown
VENDOR Unknown
MODEL Unknown
VERSION Unknown
DESCRIPTION

DATE	NODE	POLICY	RULE	STATUS	OWNER
07/08/18 11:57:06 AM	Major Cisco Error : Major Cisco Error (<13>Jul 8 2018 16:57:06 10.13.37.43: <179>82378: : com: 52977: CUCM12.layerstech.com Jul 08 2018 16:57:05 UTC : %UC_CALLMANAGER-3-EndPointUnregistered: %[DeviceName=SEP003048DEF81A][IPAddress=172.16.1.11][Protocol=SIP][DeviceType=336][Description=SEP003048DEF81A][Reason=10][IPAddrAttributes=0][CallState=402-call_delivered4][AppID=Cisco CallManager][ClusterID=StandAloneCluster][NodeID=CUCM12]: An endpoint has unregistered)				

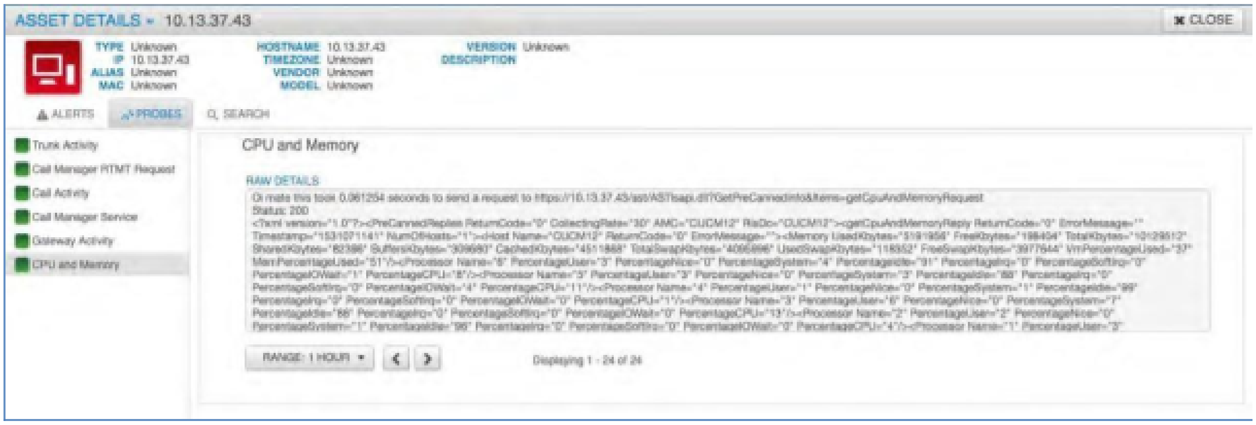
REFERENCE ID 20000-01000005-00-01-39950-34843
NODE devparb
POLICY Cisco Alerts : Universal
RULE Major Cisco Error
OWNER Unassigned
STATUS OPEN
START 07/08/18 11:57:06 AM
LAST CHANGE -
ELAPSED TIME 0 Days 01:22:30
NEXT ESCALATION 07/08/18 01:29:16 PM
EXPIRES IN 00:09:40
RESPONSE PROCEDURE Default IRP
DESCRIPTION -

DATE	NODE	POLICY	RULE	STATUS	OWNER
07/08/18 11:08:21 AM	devparb	Cisco Alerts : Universal	Critical Cisco Error	OPEN	Unassigned
OUTPUT:	Critical Cisco Error (<13>Jul 8 2018 16:08:21 10.13.37.43: <185>82258: : : 54123: CUCM12.layerstech.com: Jul 08 2018 16:08:21.207 UTC : %UC_RTMT-1-RTMT_ALERT: %[AlertName=RTMTSessionsExceedsThreshold][AlertDetail= On Sun Jul 08 11:08:21 CDT 2018, alert RTMTSessionsExceedsThreshold has occured. Counter SessionsActive of Cisco Tomcat Web Application(ast)				
07/08/18 09:25:15 AM	devparb	Cisco Alerts : Universal	Major Cisco Error	OPEN	Unassigned
OUTPUT:	Major Cisco Error (<13>Jul 8 2018 14:25:15 10.13.37.43: <179>82058: : com: 52775: CUCM12.layerstech.com Jul 08 2018 14:25:14 UTC : %UC_CALLMANAGER-3-EndPointUnregistered: %[DeviceName=SEP003048DEF81A][IPAddress=172.16.1.11][Protocol=SIP][DeviceType=336][Description=SEP003048DEF81A][Reason=10][IPAddrAttributes=0][CallState=402-call_delivered4;402-call_delivered4][AppID=Cisco CallManager][ClusterID=StandAloneCluster][NodeID=CUCM12]: An endpoint has unregistered)				
07/08/18 09:18:21 AM	devparb	Cisco Alerts : Universal	Critical Cisco Error	OPEN	Unassigned
OUTPUT:	Critical Cisco Error (<13>Jul 8 2018 14:18:21 10.13.37.43: <185>82036: : : 53981: CUCM12.layerstech.com: Jul 08 2018 14:18:21.114 UTC : %UC_RTMT-1-RTMT_ALERT: %[AlertName=RTMTSessionsExceedsThreshold][AlertDetail= On Sun Jul 08 09:18:20 CDT 2018, alert RTMTSessionsExceedsThreshold has occured. Counter SessionsActive of Cisco Tomcat Web Application(ast)				

We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

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

4.2.8. Asset Details: Probes



TYPE Unknown
IP 10.13.37.43
ALIAS Unknown
MAC Unknown
HOSTNAME 10.13.37.43
TIMEZONE Unknown
VENDOR Unknown
MODEL Unknown
VERSION Unknown
DESCRIPTION

- 🟩 Trunk Activity
- 🟩 Call Manager RTMT Request
- 🟩 Call Activity
- 🟩 Call Manager Service
- 🟩 Gateway Activity
- 🟩 CPU and Memory

CPU and Memory

RAW DETAILS

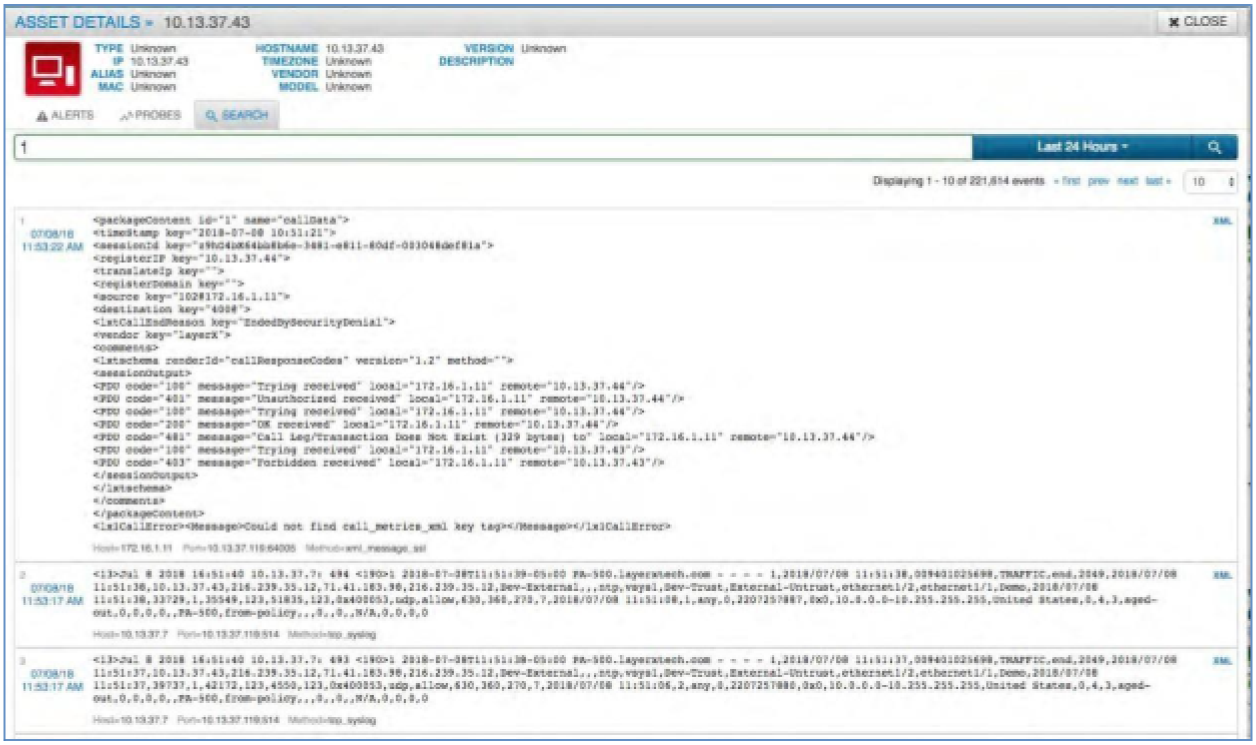
```
Oi mate this took 0.061254 seconds to send a request to https://10.13.37.43/ast/ASTIsapi.dll?GetPreCannedInfo&Items=getCpuAndMemoryRequest
Status: 200
<?xml version="1.0"?><PreCannedReplies ReturnCode="0" CollectingRate="30" AMC="CUCM12" RisDc="CUCM12"><getCpuAndMemoryReply ReturnCode="0" ErrorMessage=""
Timestamp="1531071141" NumOfHosts="1"><Host Name="CUCM12" ReturnCode="0" ErrorMessage=""><Memory UsedKbytes="3191956" FreeKbytes="198404" TotalKbytes="10129512"
SharedKbytes="82386" BuffersKbytes="309680" CachedKbytes="4511868" TotalSwapKbytes="4095996" UsedSwapKbytes="118552" FreeSwapKbytes="3977644" VmPercentageUsed="37"
MemPercentageUsed="51"/><Processor Name="6" PercentageUser="3" PercentageNice="0" PercentageSystem="4" PercentageIdle="91" PercentageIrq="0" PercentageSoftIrq="0"
PercentageIOWait="1" PercentageCPU="8"/><Processor Name="3" PercentageUser="3" PercentageNice="0" PercentageSystem="3" PercentageIdle="88" PercentageIrq="0"
PercentageSoftIrq="0" PercentageIOWait="4" PercentageCPU="11"/><Processor Name="4" PercentageUser="1" PercentageNice="0" PercentageSystem="1" PercentageIdle="99"
PercentageIrq="0" PercentageSoftIrq="0" PercentageIOWait="0" PercentageCPU="1"/><Processor Name="3" PercentageUser="6" PercentageNice="0" PercentageSystem="7"
PercentageIdle="86" PercentageIrq="0" PercentageSoftIrq="0" PercentageIOWait="0" PercentageCPU="13"/><Processor Name="2" PercentageUser="2" PercentageNice="0"
PercentageSystem="1" PercentageIdle="96" PercentageIrq="0" PercentageSoftIrq="0" PercentageIOWait="0" PercentageCPU="4"/><Processor Name="1" PercentageUser="3"
```

Displaying 1 - 24 of 24

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

4.2.9. Asset Details: Search

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



TYPE Unknown
IP 10.13.37.43
ALIAS Unknown
MAC Unknown
HOSTNAME 10.13.37.43
TIMEZONE Unknown
VENDOR Unknown
MODEL Unknown
VERSION Unknown
DESCRIPTION

1

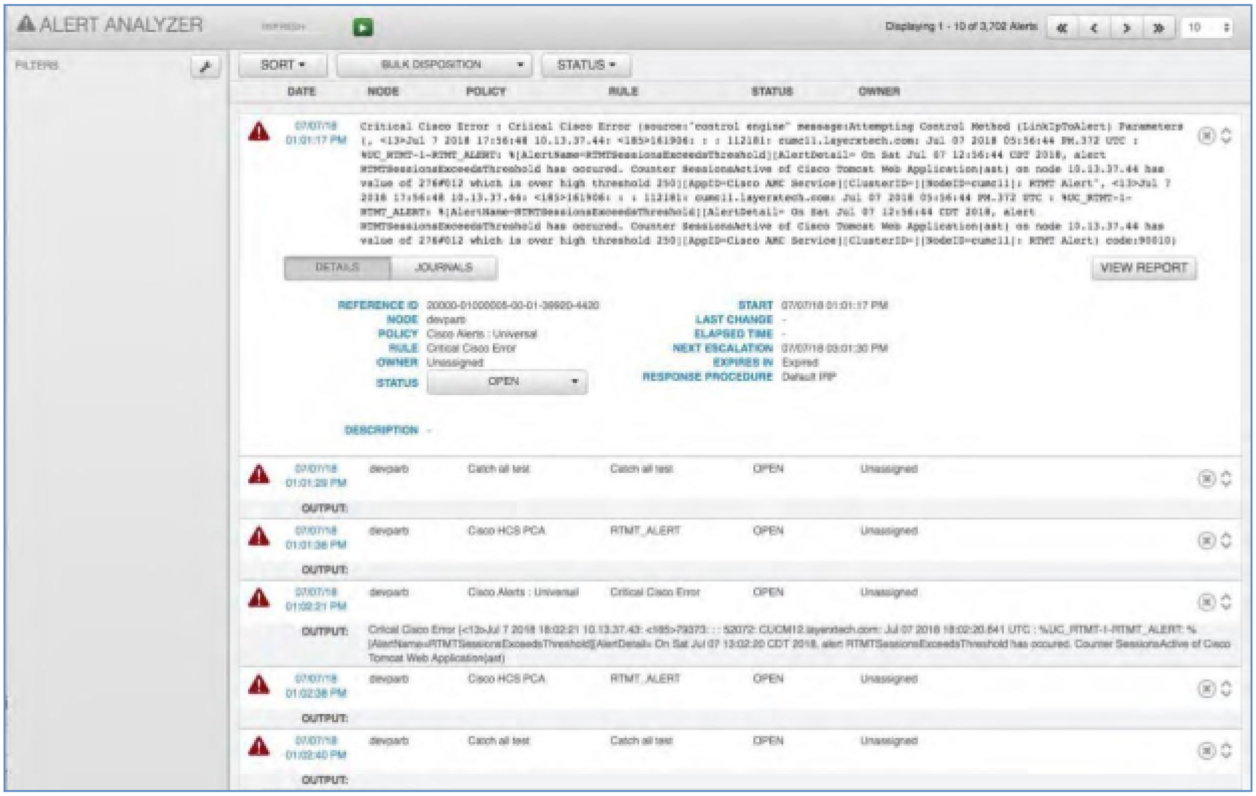
Displaying 1 - 10 of 221,614 events « first prev next last » 10

```
1
07/08/18
11:53:22 AM
<packageContent id="1" name="callData">
<timeStamp key="2018-07-08 10:51:21">
<sessionId key="a9bd4b064bb8b6e-3481-e811-80df-003048def81a">
<registerIP key="10.13.37.44">
<translateIp key="">
<registerDomain key="">
<source key="102#172.16.1.11">
<destination key="4008">
<lxtCallEndReason key="EndedBySecurityDenial">
<vendor key="layerX">
<comments>
<lxtschema renderId="callResponseCodes" version="1.2" method="">
<sessionOutput>
<PDU code="100" message="Trying received" local="172.16.1.11" remote="10.13.37.44"/>
<PDU code="401" message="Unauthorized received" local="172.16.1.11" remote="10.13.37.44"/>
<PDU code="100" message="Trying received" local="172.16.1.11" remote="10.13.37.44"/>
<PDU code="200" message="OK received" local="172.16.1.11" remote="10.13.37.44"/>
<PDU code="481" message="Call Leg/Transaction Does Not Exist (329 bytes) to" local="172.16.1.11" remote="10.13.37.44"/>
<PDU code="100" message="Trying received" local="172.16.1.11" remote="10.13.37.43"/>
<PDU code="403" message="Forbidden received" local="172.16.1.11" remote="10.13.37.43"/>
</sessionOutput>
</lxtschema>
</comments>
</packageContent>
<lxlCallError><Message>Could not find call_metrics_xml key tag></Message></lxlCallError>
Host=172.16.1.11 Port=10.13.37.119:64005 Method=xml_message_ssl

2
07/08/18
11:53:17 AM
<13>Jul 8 2018 16:51:40 10.13.37.7: 494 <190>1 2018-07-08T11:51:39-05:00 PA-500.layerxtech.com - - - - 1,2018/07/08 11:51:38,009401025698,TRAFFIC,end,2049,2018/07/08
11:51:38,10.13.37.43,216.239.35.12,71.41.183.98,216.239.35.12,Dev-External,,,ntp,vsys1,Dev-Trust,External-Untrust,ethernet1/2,ethernet1/1,Demo,2018/07/08
11:51:38,33729,1,35549,123,51835,123,0x400053,udp,allow,630,360,270,7,2018/07/08 11:51:08,1,any,0,2207257887,0x0,10.0.0.0-10.255.255.255,United States,0,4,3,aged-
out,0,0,0,0,,PA-500,from-policy,,,0,,0,,N/A,0,0,0,0
Host=10.13.37.7 Port=10.13.37.119:514 Method=tcp_syslog

3
07/08/18
11:53:17 AM
<13>Jul 8 2018 16:51:40 10.13.37.7: 493 <190>1 2018-07-08T11:51:38-05:00 PA-500.layerxtech.com - - - - 1,2018/07/08 11:51:37,009401025698,TRAFFIC,end,2049,2018/07/08
11:51:37,10.13.37.43,216.239.35.12,71.41.183.98,216.239.35.12,Dev-External,,,ntp,vsys1,Dev-Trust,External-Untrust,ethernet1/2,ethernet1/1,Demo,2018/07/08
11:51:37,39737,1,42172,123,4550,123,0x400053,udp,allow,630,360,270,7,2018/07/08 11:51:06,2,any,0,2207257880,0x0,10.0.0.0-10.255.255.255,United States,0,4,3,aged-
out,0,0,0,0,,PA-500,from-policy,,,0,,0,,N/A,0,0,0,0
Host=10.13.37.7 Port=10.13.37.119:514 Method=tcp_syslog
```

4.3. Alerts

4.3.1. Alert Analyzer

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



DATE	NODE	POLICY	RULE	STATUS	OWNER
07/07/18 01:01:17 PM					

```
Critical Cisco Error : Critical Cisco Error (source:"control engine" message:Attempting Control Method (LinkIpToAlert) Parameters
(, <13>Jul 7 2018 17:56:48 10.13.37.44: <185>161906: : : 112181: cumc11.layerxtech.com: Jul 07 2018 05:56:44 PM.372 UTC :
%UC_RTMT-1-RTMT_ALERT: %[AlertName=RTMTSessionsExceedsThreshold][AlertDetail= On Sat Jul 07 12:56:44 CDT 2018, alert
RTMTSessionsExceedsThreshold has occured. Counter SessionsActive of Cisco Tomcat Web Application(ast) on node 10.13.37.44 has
value of 276#012 which is over high threshold 250][AppID=Cisco AMC Service][ClusterID=][NodeID=cumc11]: RTMT Alert", <13>Jul 7
2018 17:56:48 10.13.37.44: <185>161906: : : 112181: cumc11.layerxtech.com: Jul 07 2018 05:56:44 PM.372 UTC : %UC_RTMT-1-
RTMT_ALERT: %[AlertName=RTMTSessionsExceedsThreshold][AlertDetail= On Sat Jul 07 12:56:44 CDT 2018, alert
RTMTSessionsExceedsThreshold has occured. Counter SessionsActive of Cisco Tomcat Web Application(ast) on node 10.13.37.44 has
value of 276#012 which is over high threshold 250][AppID=Cisco AMC Service][ClusterID=][NodeID=cumc11]: RTMT Alert) code:90010)
```

REFERENCE ID 20000-01000005-00-01-39920-4420
NODE devparb
POLICY Cisco Alerts : Universal
RULE Critical Cisco Error
OWNER Unassigned
STATUS OPEN ▾

START 07/07/18 01:01:17 PM
LAST CHANGE -
ELAPSED TIME -
NEXT ESCALATION 07/07/18 03:01:30 PM
EXPIRES IN Expired
RESPONSE PROCEDURE Default IRP

DESCRIPTION -

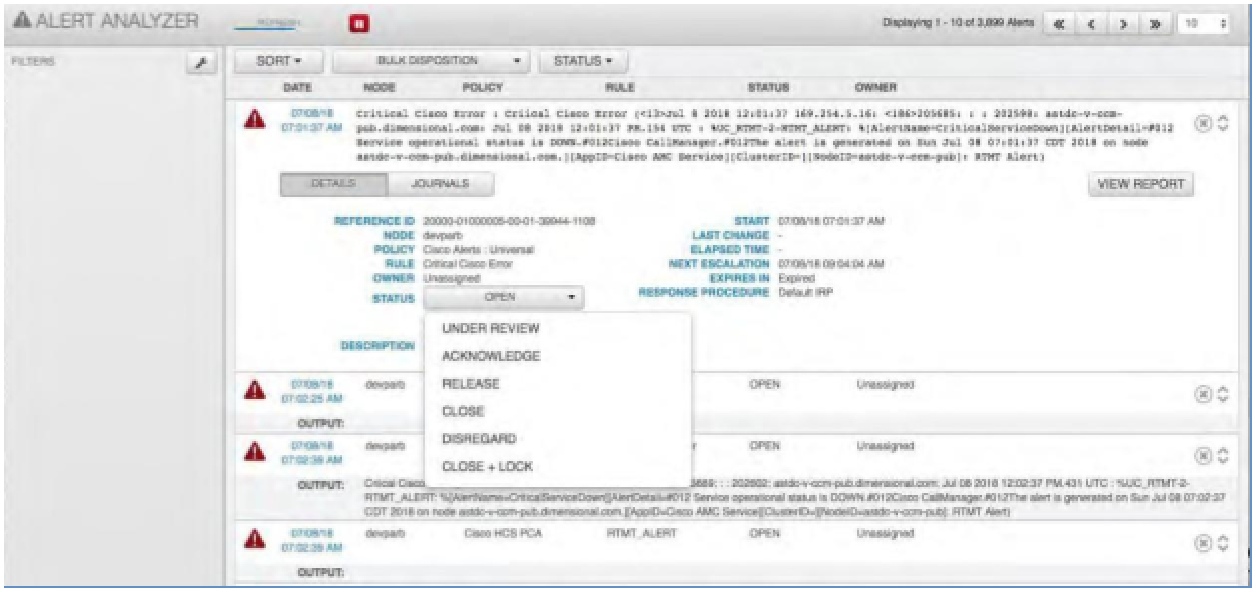
DATE	NODE	POLICY	RULE	STATUS	OWNER
07/07/18 01:01:29 PM	devparb	Catch all test	Catch all test	OPEN	Unassigned
OUTPUT:					
07/07/18 01:01:38 PM	devparb	Cisco HCS PCA	RTMT_ALERT	OPEN	Unassigned
OUTPUT:					
07/07/18 01:02:21 PM	devparb	Cisco Alerts : Universal	Critical Cisco Error	OPEN	Unassigned
OUTPUT:	Critical Cisco Error [<13>Jul 7 2018 18:02:21 10.13.37.43: <185>79373: : : 52072: CUCM12.layerxtech.com: Jul 07 2018 18:02:20.841 UTC : %UC_RTMT-1-RTMT_ALERT: %[AlertName=RTMTSessionsExceedsThreshold][AlertDetail= On Sat Jul 07 13:02:20 CDT 2018, alert RTMTSessionsExceedsThreshold has occured. Counter SessionsActive of Cisco Tomcat Web Application(ast)				
07/07/18 01:02:38 PM	devparb	Cisco HCS PCA	RTMT_ALERT	OPEN	Unassigned
OUTPUT:					
07/07/18 01:02:40 PM	devparb	Catch all test	Catch all test	OPEN	Unassigned
OUTPUT:					

4.3.2. Alert Disposition

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

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

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



07/08/18 07:01:37 AM

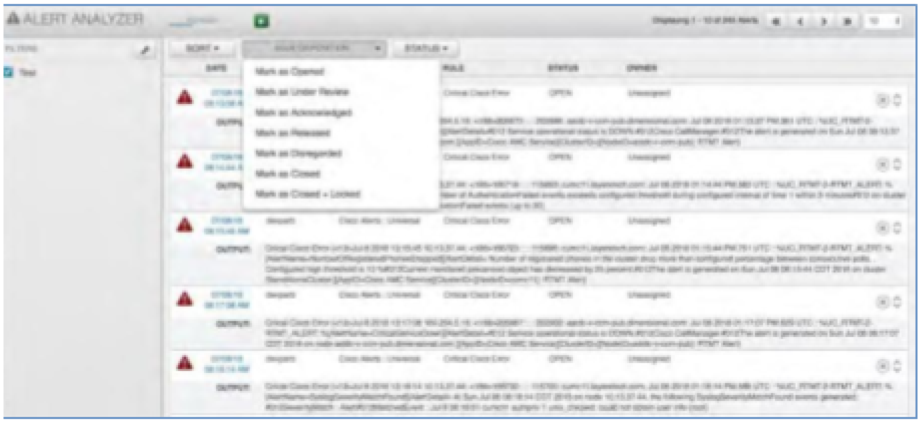
```
critical Cisco Error : Critical Cisco Error (<13>Jul 8 2018 12:01:37 169.254.5.16: <186>205685: : : 202598: astdc-v-ccm-
pub.dimensional.com: Jul 08 2018 12:01:37 PM.156 UTC : %UC_RTMT-2-RTMT_ALERT: %[AlertName=CriticalServiceDown][AlertDetail=#012
Service operational status is DOWN.#012Cisco CallManager.#012The alert is generated on Sun Jul 08 07:01:37 CDT 2018 on node
astdc-v-ccm-pub.dimensional.com.][AppID=Cisco AMC Service][ClusterID=][NodeID=astdc-v-ccm-pub]: RTMT Alert)
```

REFERENCE ID 20000-01000005-00-01-39944-1108
NODE devparb
POLICY Cisco Alerts : Universal
RULE Critical Cisco Error
OWNER Unassigned
STATUS OPEN
DESCRIPTION

START 07/08/18 07:01:37 AM
LAST CHANGE -
ELAPSED TIME -
NEXT ESCALATION 07/08/18 09:04:04 AM
EXPIRES IN Expired
RESPONSE PROCEDURE Default IRP

DATE	NODE	POLICY	RULE	STATUS	OWNER
07/08/18 07:02:25 AM	devparb			OPEN	Unassigned
07/08/18 07:02:39 AM	devparb			OPEN	Unassigned
07/08/18 07:02:39 AM	devparb	Cisco HCS PCA	RTMT_ALERT	OPEN	Unassigned

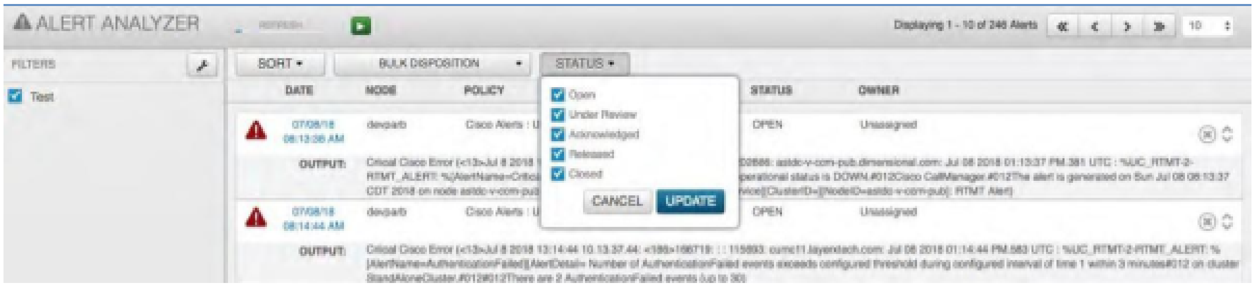
OUTPUT: Critical Cisco [illegible] 3689: : : 202602: astdc-v-ccm-pub.dimensional.com: Jul 08 2018 12:02:37 PM.431 UTC : %UC_RTMT-2-RTMT_ALERT: %[AlertName=CriticalServiceDown][AlertDetail=#012 Service operational status is DOWN.#012Cisco CallManager.#012The alert is generated on Sun Jul 08 07:02:37 CDT 2018 on node astdc-v-ccm-pub.dimensional.com.][AppID=Cisco AMC Service][ClusterID=][NodeID=astdc-v-ccm-pub]: RTMT Alert)



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

4.3.3. Filtering by Disposition

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



DATE	NODE	POLICY	STATUS	OWNER
07/08/18 08:13:38 AM	devparb	Cisco Alerts : U	OPEN	Unassigned
07/08/18 08:14:44 AM	devparb	Cisco Alerts : U	OPEN	Unassigned

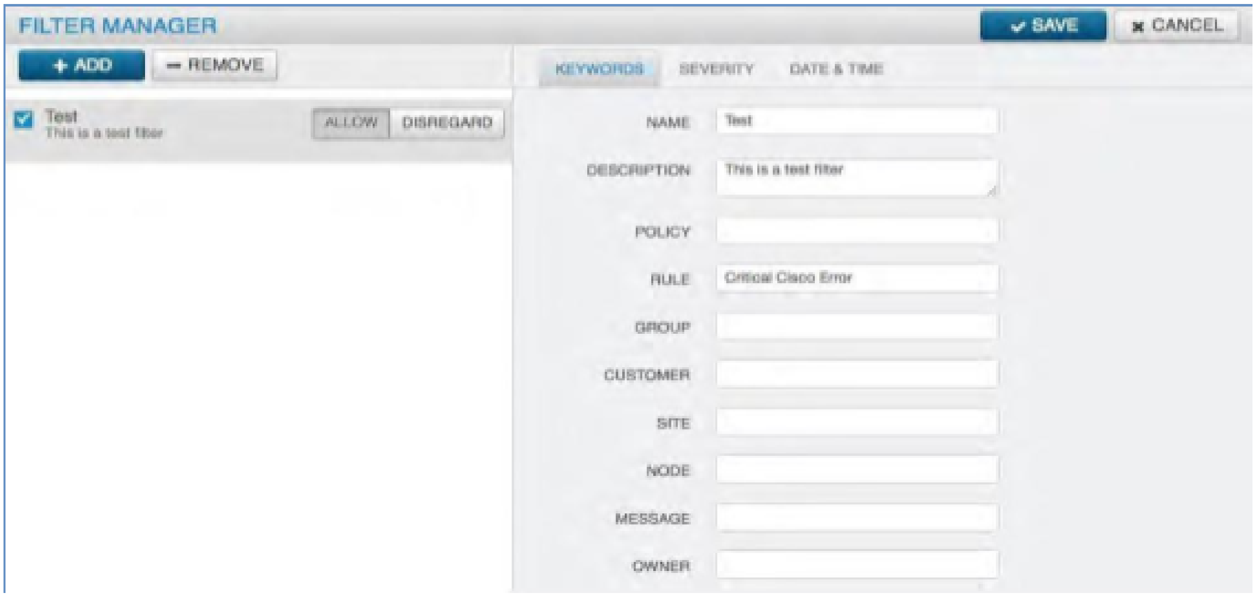
OUTPUT: Critical Cisco Error (<13>Jul 8 2018 [illegible] 02686: astdc-v-ccm-pub.dimensional.com: Jul 08 2018 01:13:37 PM.381 UTC : %UC_RTMT-2-RTMT_ALERT: %[AlertName=Critica[illegible]perational status is DOWN.#012Cisco CallManager.#012The alert is generated on Sun Jul 08 08:13:37 CDT 2018 on node astdc-v-ccm-pub[illegible]vice][ClusterID=][NodeID=astdc-v-ccm-pub]: RTMT Alert)

OUTPUT: Critical Cisco Error (<13>Jul 8 2018 13:14:44 10.13.37.44: <186>166719: : : 115693: cumc11.layentech.com: Jul 08 2018 01:14:44 PM.583 UTC : %UC_RTMT-2-RTMT_ALERT: %[AlertName=AuthenticationFailed][AlertDetail= Number of AuthenticationFailed events exceeds configured threshold during configured interval of time 1 within 3 minutes#012 on cluster StandAloneCluster.#012#012There are 2 AuthenticationFailed events (up to 30)

4.3.4. Alert Filters

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

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



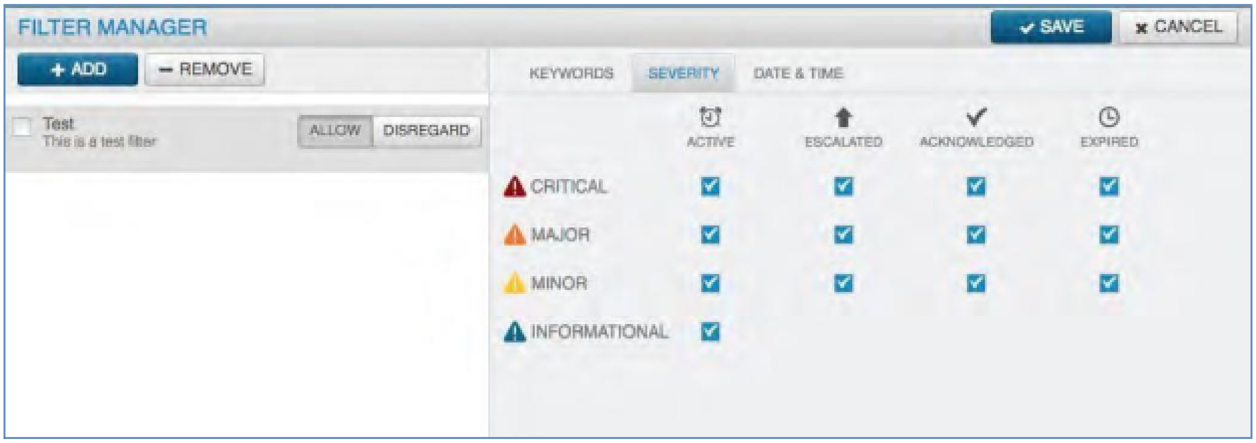
☑ Test
This is a test filter

NAME: Test

DESCRIPTION: This is a test filter

RULE: Critical Cisco Error

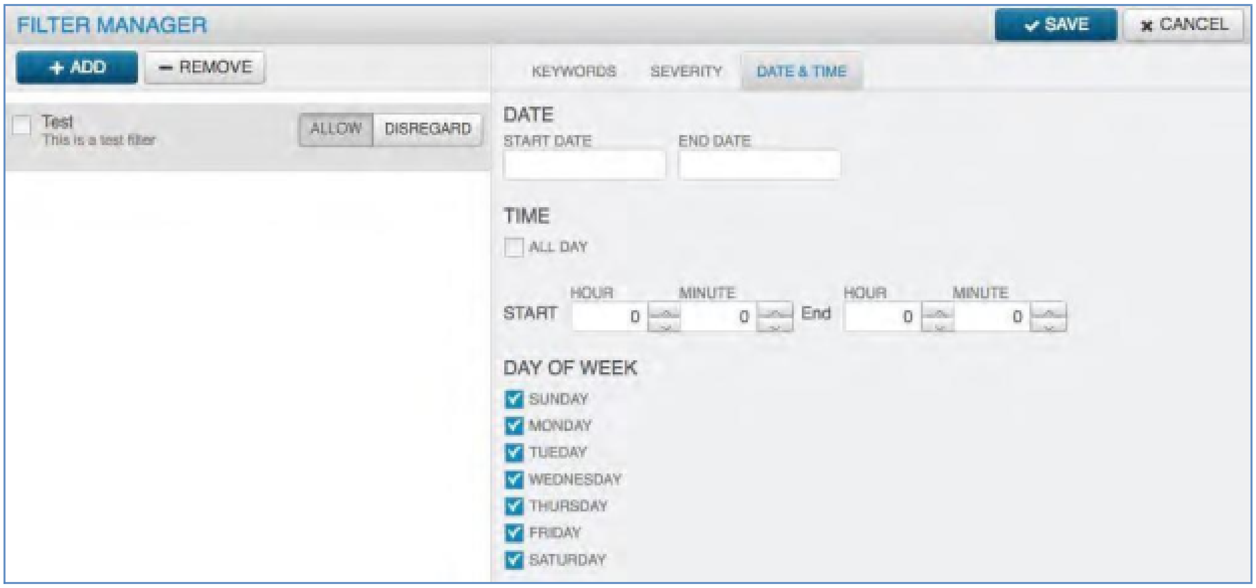
- Severity: The filter can be set based on the chosen severity or severities. Additionally, the state or states can be chosen with each severity. Click the levels desired.
  - Active: Alert is currently in one of the active states
  - Escalated: Alert has been escalated based on the timer in the correlation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



□ Test
This is a test filter

	ACTIVE	ESCALATED	ACKNOWLEDGED	EXPIRED
CRITICAL	☑	☑	☑	☑
MAJOR	☑	☑	☑	☑
MINOR	☑	☑	☑	☑
INFORMATIONAL	☑			

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



□ Test
This is a test filter

DATE
START DATE
END DATE

TIME
□ ALL DAY

	HOUR	MINUTE		HOUR	MINUTE
START	0	0	End	0	0

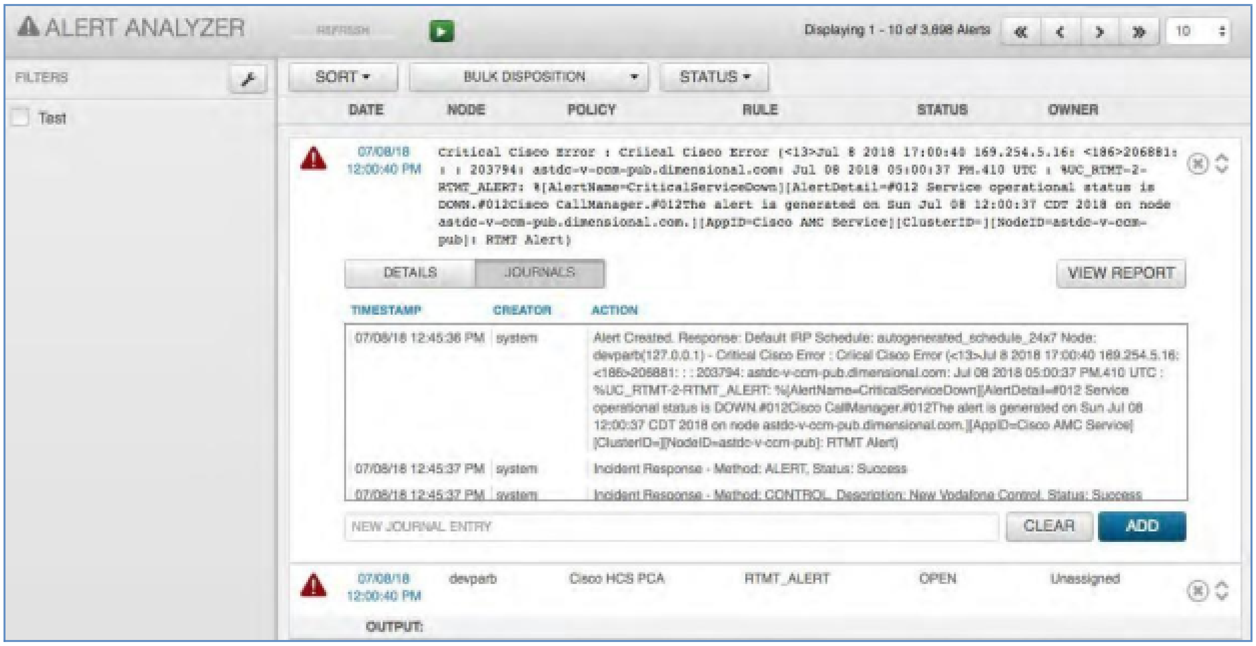
DAY OF WEEK
☑ SUNDAY
☑ MONDAY
☑ TUEDAY
☑ WEDNESDAY
☑ THURSDAY
☑ FRIDAY
☑ SATURDAY

4.3.5. Alert Journal

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

To add an Alert Journal:

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



07/08/18 12:00:40 PM

```
Critical Cisco Error : Crilical Cisco Error (<13>Jul 8 2018 17:00:40 169.254.5.16: <186>206881:
: : 203794: astdc-v-ccm-pub.dimensional.com: Jul 08 2018 05:00:37 PM.410 UTC : %UC_RTMT-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
astdc-v-ccm-pub.dimensional.com.][AppID=Cisco AMC Service][ClusterID=][NodeID=astdc-v-ccm-
pub]: RTMT Alert)
```

TIMESTAMP	CREATOR	ACTION
07/08/18 12:45:36 PM	system	Alert Created. Response: Default IRP Schedule: autogenerated_schedule_24x7 Node: devparb(127.0.0.1) - Critical Cisco Error : Crilical Cisco Error (<13>Jul 8 2018 17:00:40 169.254.5.16: <186>206881: : : 203794: astdc-v-ccm-pub.dimensional.com: Jul 08 2018 05:00:37 PM.410 UTC : %UC_RTMT-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 astdc-v-ccm-pub.dimensional.com.][AppID=Cisco AMC Service][ClusterID=][NodeID=astdc-v-ccm-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

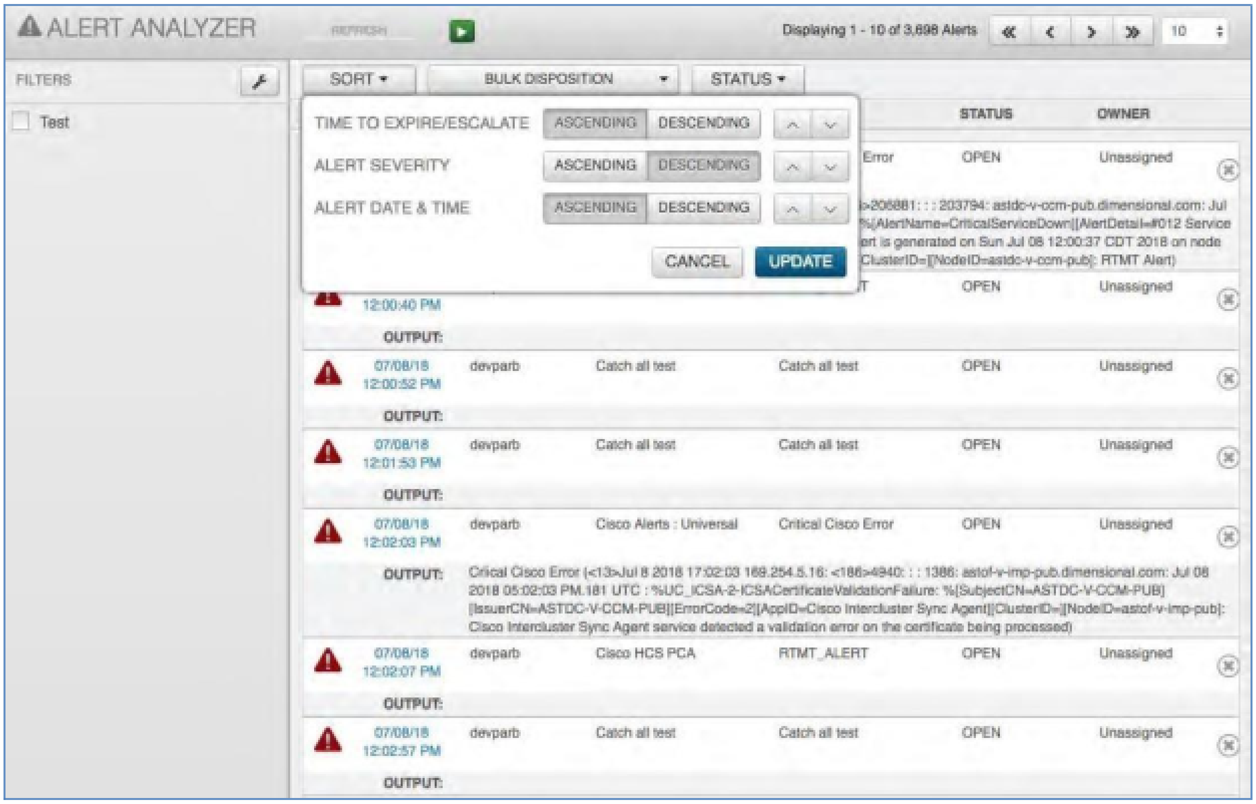
DATE	NODE	POLICY	RULE	STATUS	OWNER
07/08/18 12:00:40 PM	devparb	Cisco HCS PCA	RTMT_ALERT	OPEN	Unassigned

4.3.6. Alert Sorting

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

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

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



```
                                                          STATUS     OWNER
                                           Error          OPEN       Unassigned
                                           >206881: : : 203794: astdc-v-ccm-pub.dimensional.com: Jul
                                           %[AlertName=CriticalServiceDown][AlertDetail=#012 Service
                                           ert is generated on Sun Jul 08 12:00:37 CDT 2018 on node
                                           ClusterID=][NodeID=astdc-v-ccm-pub]: RTMT Alert)
           12:00:40 PM                     T              OPEN       Unassigned
   OUTPUT:
07/08/18   devparb   Catch all test        Catch all test OPEN       Unassigned
12:00:52 PM
   OUTPUT:
07/08/18   devparb   Catch all test        Catch all test OPEN       Unassigned
12:01:53 PM
   OUTPUT:
07/08/18   devparb   Cisco Alerts : Universal   Critical Cisco Error   OPEN   Unassigned
12:02:03 PM
   OUTPUT:   Crical Cisco Error (<13>Jul 8 2018 17:02:03 169.254.5.16: <186>4940: : : 1386: astof-v-imp-pub.dimensional.com: Jul 08
             2018 05:02:03 PM.181 UTC : %UC_ICSA-2-ICSACertificateValidationFailure: %[SubjectCN=ASTDC-V-CCM-PUB]
             [IssuerCN=ASTDC-V-CCM-PUB][ErrorCode=2][AppID=Cisco Intercluster Sync Agent][ClusterID=][NodeID=astof-v-imp-pub]:
             Cisco Intercluster Sync Agent service detected a validation error on the certificate being processed)
07/08/18   devparb   Cisco HCS PCA         RTMT_ALERT     OPEN       Unassigned
12:02:07 PM
   OUTPUT:
07/08/18   devparb   Catch all test        Catch all test OPEN       Unassigned
12:02:57 PM
   OUTPUT:
```

4.4. Search

4.4.1. Event Search

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

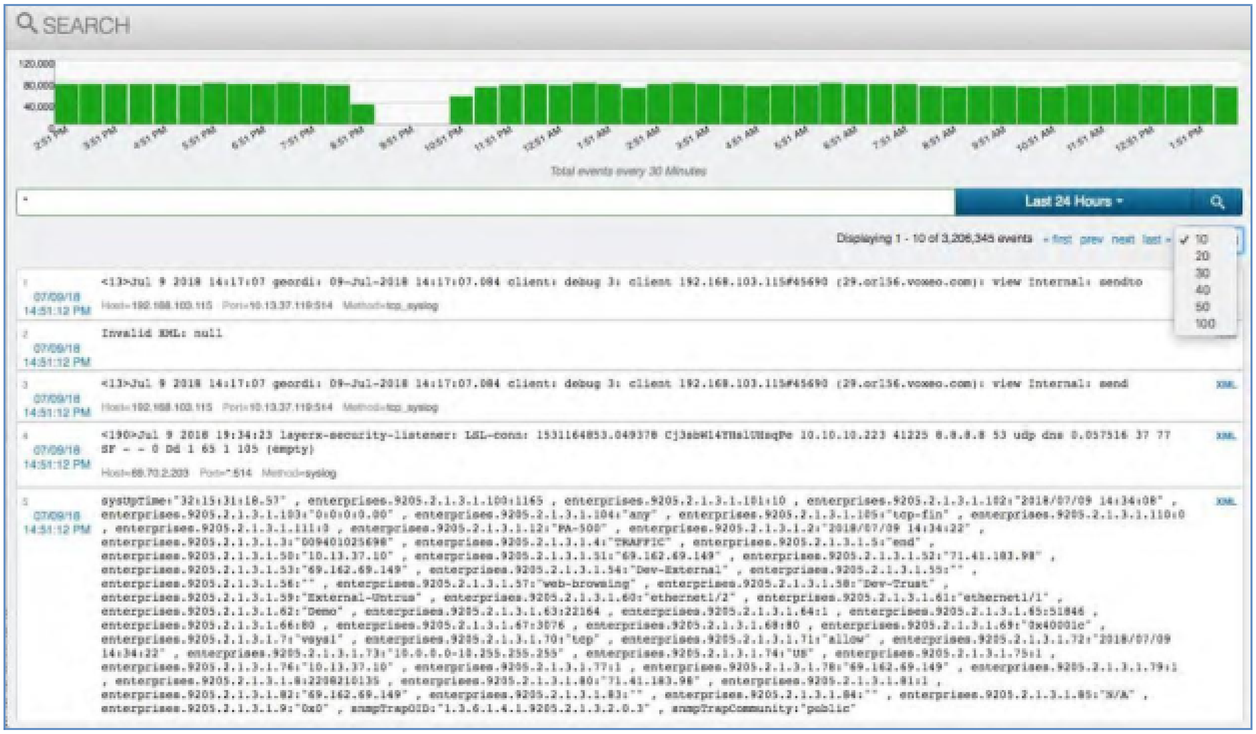
4.4.2. Simple Searching

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

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

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

We appreciate and value your comments. Email: doc-feedback@voss-solutions.com



```
*
```

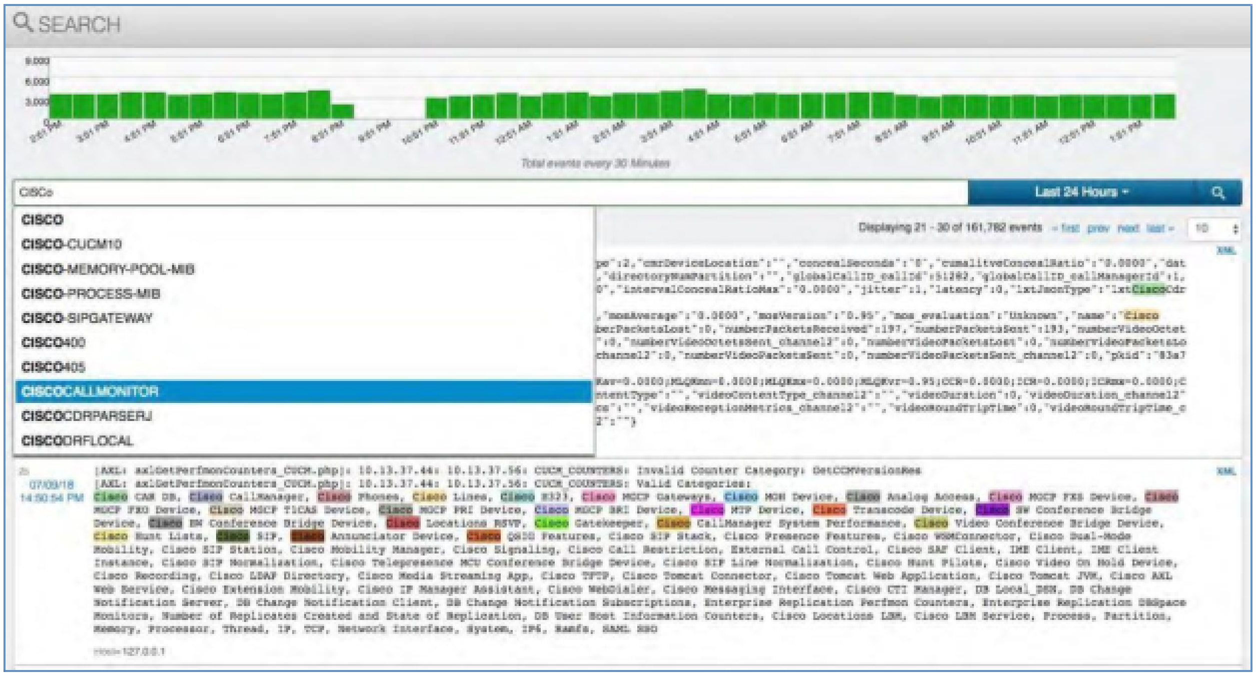
Displaying 1 - 10 of 3,206,345 events

```
1 07/09/18 14:51:12 PM
<13>Jul 9 2018 14:17:07 geordi: 09-Jul-2018 14:17:07.084 client: debug 3: client 192.168.103.115#45690 (29.or156.voxeo.com): view Internal: sendto
Host=192.168.103.115   Port=10.13.37.119:514   Method=tcp_syslog

2 07/09/18 14:51:12 PM
Invalid XML: null

3 07/09/18 14:51:12 PM
<13>Jul 9 2018 14:17:07 geordi: 09-Jul-2018 14:17:07.084 client: debug 3: client 192.168.103.115#45690 (29.or156.voxeo.com): view Internal: send
Host=192.168.103.115   Port=10.13.37.119:514   Method=tcp_syslog

4 07/09/18 14:51:12 PM
<190>Jul 9 2018 19:34:23 layerx-security-listener: LSL-conn: 1531164853.049378 Cj3sbW14THslUHsqPe 10.10.10.223 41225 8.8.8.8 53 udp dns 0.057516 37 77
SF - - 0 Dd 1 65 1 105 (empty)
Host=68.70.2.203   Port=*:514   Method=syslog

5 07/09/18 14:51:12 PM
sysUpTime:"32:15:31:18.57" , enterprises.9205.2.1.3.1.100:1165 , enterprises.9205.2.1.3.1.101:10 , enterprises.9205.2.1.3.1.102:"2018/07/09 14:34:08" ,
enterprises.9205.2.1.3.1.103:"0:0:0:0.00" , enterprises.9205.2.1.3.1.104:"any" , enterprises.9205.2.1.3.1.105:"tcp-fin" , enterprises.9205.2.1.3.1.110:0
, enterprises.9205.2.1.3.1.111:0 , enterprises.9205.2.1.3.1.12:"PA-500" , enterprises.9205.2.1.3.1.2:"2018/07/09 14:34:22" ,
enterprises.9205.2.1.3.1.3:"009401025698" , enterprises.9205.2.1.3.1.4:"TRAFFIC" , enterprises.9205.2.1.3.1.5:"end" ,
enterprises.9205.2.1.3.1.50:"10.13.37.10" , enterprises.9205.2.1.3.1.51:"69.162.69.149" , enterprises.9205.2.1.3.1.52:"71.41.183.98" ,
enterprises.9205.2.1.3.1.53:"69.162.69.149" , enterprises.9205.2.1.3.1.54:"Dev-External" , enterprises.9205.2.1.3.1.55:"" ,
enterprises.9205.2.1.3.1.56:"" , enterprises.9205.2.1.3.1.57:"web-browsing" , enterprises.9205.2.1.3.1.58:"Dev-Trust" ,
enterprises.9205.2.1.3.1.59:"External-Untrus" , enterprises.9205.2.1.3.1.60:"ethernet1/2" , enterprises.9205.2.1.3.1.61:"ethernet1/1" ,
enterprises.9205.2.1.3.1.62:"Demo" , enterprises.9205.2.1.3.1.63:22164 , enterprises.9205.2.1.3.1.64:1 , enterprises.9205.2.1.3.1.65:51846 ,
enterprises.9205.2.1.3.1.66:80 , enterprises.9205.2.1.3.1.67:3076 , enterprises.9205.2.1.3.1.68:80 , enterprises.9205.2.1.3.1.69:"0x40001c" ,
enterprises.9205.2.1.3.1.7:"vsys1" , enterprises.9205.2.1.3.1.70:"tcp" , enterprises.9205.2.1.3.1.71:"allow" , enterprises.9205.2.1.3.1.72:"2018/07/09
14:34:22" , enterprises.9205.2.1.3.1.73:"10.0.0.0-10.255.255.255" , enterprises.9205.2.1.3.1.74:"US" , enterprises.9205.2.1.3.1.75:1 ,
enterprises.9205.2.1.3.1.76:"10.13.37.10" , enterprises.9205.2.1.3.1.77:1 , enterprises.9205.2.1.3.1.78:"69.162.69.149" , enterprises.9205.2.1.3.1.79:1
, enterprises.9205.2.1.3.1.8:2208210135 , enterprises.9205.2.1.3.1.80:"71.41.183.98" , enterprises.9205.2.1.3.1.81:1 ,
enterprises.9205.2.1.3.1.82:"69.162.69.149" , enterprises.9205.2.1.3.1.83:"" , enterprises.9205.2.1.3.1.84:"" , enterprises.9205.2.1.3.1.85:"N/A" ,
enterprises.9205.2.1.3.1.9:"0x0" , snmpTrapOID:"1.3.6.1.4.1.9205.2.1.3.2.0.3" , snmpTrapCommunity:"public"
```

4.4.3. Keyword Searching

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

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



```
pe":2,"cmrDeviceLocation":"","concealSeconds":"0","cumalitveConcealRatio":"0.0000","dat
,"directoryNumPartition":"","globalCallID_callId":51282,"globalCallID_callManagerId":1,
0","intervalConcealRatioMax":"0.0000","jitter":1,"latency":0,"lxtJsonType":"lxtCiscoCdr

,"mosAverage":"0.0000","mosVersion":"0.95","mos_evaluation":"Unknown","name":"Cisco
berPacketsLost":0,"numberPacketsReceived":197,"numberPacketsSent":193,"numberVideoOctet
":0,"numberVideoOctetsSent_channel2":0,"numberVideoPacketsLost":0,"numberVideoPacketsLo
channel2":0,"numberVideoPacketsSent":0,"numberVideoPacketsSent_channel2":0,"pkid":"83a7

Kav=0.0000;MLQKmn=0.0000;MLQKmx=0.0000;MLQKvr=0.95;CCR=0.0000;ICR=0.0000;ICRmx=0.0000;C
ontentType":"","videoContentType_channel2":"","videoDuration":0,"videoDuration_channel2"
cs":"","videoReceptionMetrics_channel2":"","videoRoundTripTime":0,"videoRoundTripTime_c
2":""}
```

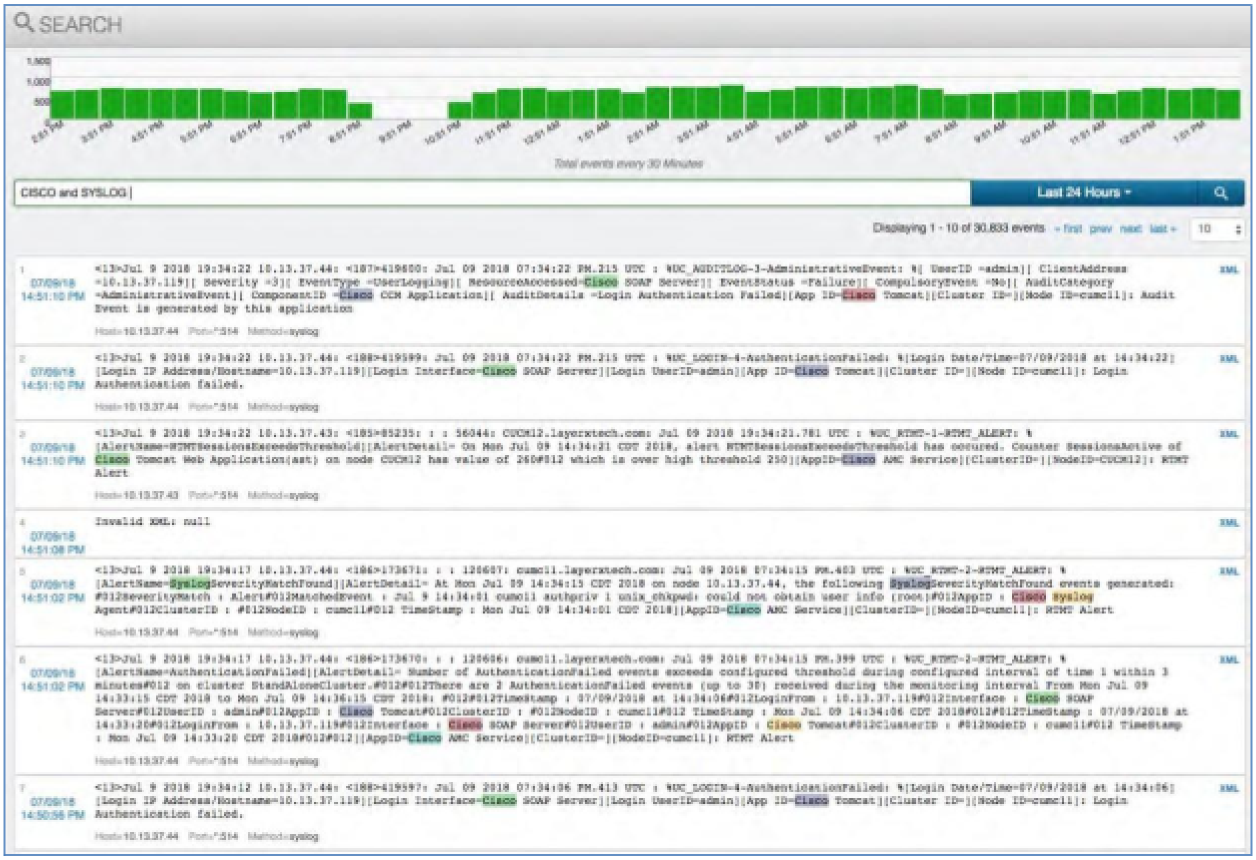
```
[AXL: axlGetPerfmonCounters_CUCM.php]: 10.13.37.44: 10.13.37.56: CUCM_COUNTERS: Invalid Counter Category: GetCCMVersionRes
[AXL: axlGetPerfmonCounters_CUCM.php]: 10.13.37.44: 10.13.37.56: CUCM_COUNTERS: Valid Categories:
Cisco CAR DB, Cisco CallManager, Cisco Phones, Cisco Lines, Cisco H323, Cisco MGCP Gateways, Cisco MOH Device, Cisco Analog Access, Cisco MGCP FXS Device, Cisco
MGCP FXO Device, Cisco MGCP T1CAS Device, Cisco MGCP PRI Device, Cisco MGCP BRI Device, Cisco MTP Device, Cisco Transcode Device, Cisco SW Conference Bridge
Device, Cisco HW Conference Bridge Device, Cisco Locations RSVP, Cisco Gatekeeper, Cisco CallManager System Performance, Cisco Video Conference Bridge Device,
Cisco Hunt Lists, Cisco SIP, Cisco Annunciator Device, Cisco QSIG Features, Cisco SIP Stack, Cisco Presence Features, Cisco WSMConnector, Cisco Dual-Mode
Mobility, Cisco SIP Station, Cisco Mobility Manager, Cisco Signaling, Cisco Call Restriction, External Call Control, Cisco SAF Client, IME Client, IME Client
Instance, Cisco SIP Normalization, Cisco Telepresence MCU Conference Bridge Device, Cisco SIP Line Normalization, Cisco Hunt Pilots, Cisco Video On Hold Device,
Cisco Recording, Cisco LDAP Directory, Cisco Media Streaming App, Cisco TFTP, Cisco Tomcat Connector, Cisco Tomcat Web Application, Cisco Tomcat JVM, Cisco AXL
Web Service, Cisco Extension Mobility, Cisco IP Manager Assistant, Cisco WebDialer, Cisco Messaging Interface, Cisco CTI Manager, DB Local_DSN, DB Change
Notification Server, DB Change Notification Client, DB Change Notification Subscriptions, Enterprise Replication Perfmon Counters, Enterprise Replication DBSpace
Monitors, Number of Replicates Created and State of Replication, DB User Host Information Counters, Cisco Locations LBM, Cisco LBM Service, Process, Partition,
Memory, Processor, Thread, IP, TCP, Network Interface, System, IP6, Ramfs, SAML SSO
```

host=127.0.0.1

4.4.4. Utilizing Conjunctions with Searching

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

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



CISCO and SYSLOG |

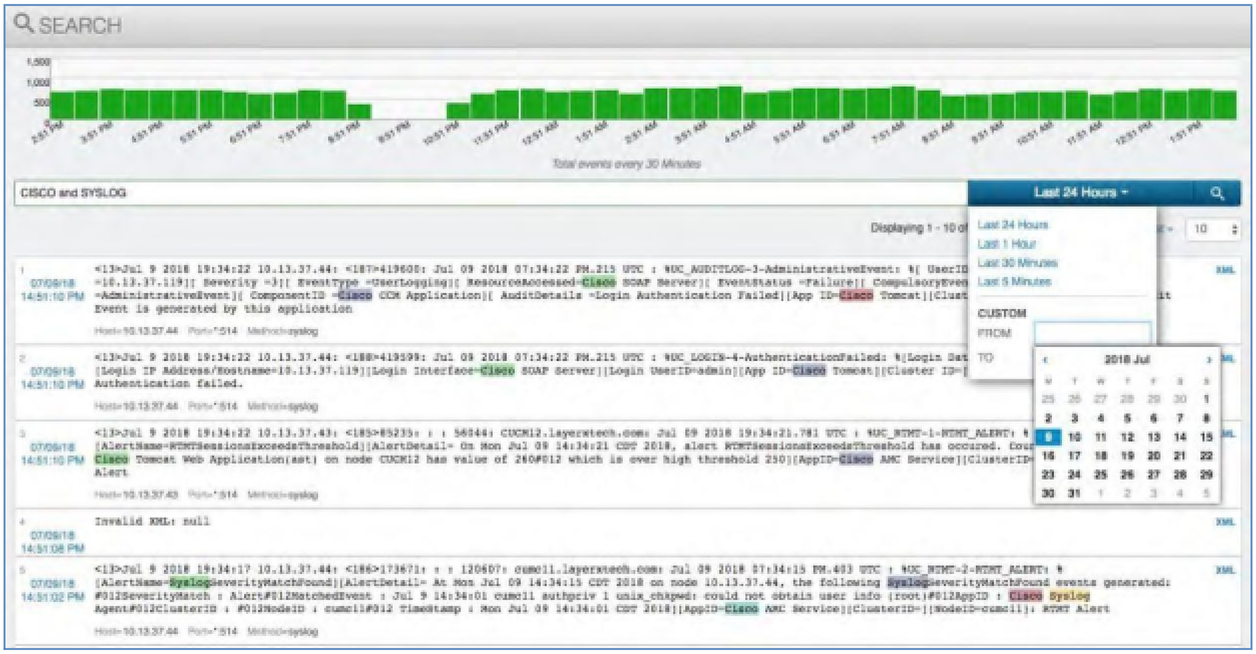
Displaying 1 - 10 of 30,833 events

```
1  07/09/18 14:51:10 PM
<13>Jul 9 2018 19:34:22 10.13.37.44: <187>419600: Jul 09 2018 07:34:22 PM.215 UTC : %UC_AUDITLOG-3-AdministrativeEvent: %[ UserID =admin][ ClientAddress
=10.13.37.119][ Severity =3][ EventType =UserLogging][ ResourceAccessed=Cisco SOAP Server][ EventStatus =Failure][ CompulsoryEvent =No][ AuditCategory
=AdministrativeEvent][ ComponentID =Cisco CCM Application][ AuditDetails =Login Authentication Failed][App ID=Cisco Tomcat][Cluster ID=][Node ID=cucm11]: Audit
Event is generated by this application
Host=10.13.37.44  Port=*514  Method=syslog

2  07/09/18 14:51:10 PM
<13>Jul 9 2018 19:34:22 10.13.37.44: <188>419599: Jul 09 2018 07:34:22 PM.215 UTC : %UC_LOGIN-4-AuthenticationFailed: %[Login Date/Time=07/09/2018 at 14:34:22]
[Login IP Address/Hostname=10.13.37.119][Login Interface=Cisco SOAP Server][Login UserID=admin][App ID=Cisco Tomcat][Cluster ID=][Node ID=cucm11]: Login
Authentication failed.
Host=10.13.37.44  Port=*514  Method=syslog

3  07/09/18 14:51:10 PM
<13>Jul 9 2018 19:34:22 10.13.37.43: <185>85235: : : 56044: CUCM12.layerxtech.com: Jul 09 2018 19:34:21.781 UTC : %UC_RTMT-1-RTMT_ALERT: %
[AlertName=RTMTSessionsExceedsThreshold][AlertDetail= On Mon Jul 09 14:34:21 CDT 2018, alert RTMTSessionsExceedsThreshold has occured. Counter SessionsActive of
Cisco Tomcat Web Application(ast) on node CUCM12 has value of 260#012 which is over high threshold 250][AppID=Cisco AMC Service][ClusterID=][NodeID=CUCM12]: RTMT
Alert
Host=10.13.37.43  Port=*514  Method=syslog

4  07/09/18 14:51:08 PM
Invalid XML: null

5  07/09/18 14:51:02 PM
<13>Jul 9 2018 19:34:17 10.13.37.44: <186>173671: : : 120607: cucm11.layerxtech.com: Jul 09 2018 07:34:15 PM.403 UTC : %UC_RTMT-2-RTMT_ALERT: %
[AlertName=SyslogSeverityMatchFound][AlertDetail= At Mon Jul 09 14:34:15 CDT 2018 on node 10.13.37.44, the following SyslogSeverityMatchFound events generated:
#012SeverityMatch : Alert#012MatchedEvent : Jul 9 14:34:01 cucm11 authpriv 1 unix_chkpwd: could not obtain user info (root)#012AppID : Cisco Syslog
Agent#012ClusterID : #012NodeID : cucm11#012 TimeStamp : Mon Jul 09 14:34:01 CDT 2018][AppID=Cisco AMC Service][ClusterID=][NodeID=cucm11]: RTMT Alert
Host=10.13.37.44  Port=*514  Method=syslog

6  07/09/18 14:51:02 PM
<13>Jul 9 2018 19:34:17 10.13.37.44: <186>173670: : : 120606: cucm11.layerxtech.com: Jul 09 2018 07:34:15 PM.399 UTC : %UC_RTMT-2-RTMT_ALERT: %
[AlertName=AuthenticationFailed][AlertDetail= Number of AuthenticationFailed events exceeds configured threshold during configured interval of time 1 within 3
minutes#012 on cluster StandAloneCluster.#012#012There are 2 AuthenticationFailed events (up to 30) received during the monitoring interval From Mon Jul 09
14:33:15 CDT 2018 to Mon Jul 09 14:36:15 CDT 2018: #012#012TimeStamp : 07/09/2018 at 14:34:06#012LoginFrom : 10.13.37.119#012Interface : Cisco SOAP
Server#012UserID : admin#012AppID : Cisco Tomcat#012ClusterID : #012NodeID : cucm11#012 TimeStamp : Mon Jul 09 14:34:06 CDT 2018#012#012TimeStamp : 07/09/2018 at
14:33:20#012LoginFrom : 10.13.37.119#012Interface : Cisco SOAP Server#012UserID : admin#012AppID : Cisco Tomcat#012ClusterID : #012NodeID : cucm11#012 TimeStamp
: Mon Jul 09 14:33:20 CDT 2018#012#012][AppID=Cisco AMC Service][ClusterID=][NodeID=cucm11]: RTMT Alert
Host=10.13.37.44  Port=*514  Method=syslog

7  07/09/18 14:50:56 PM
<13>Jul 9 2018 19:34:12 10.13.37.44: <188>419597: Jul 09 2018 07:34:06 PM.413 UTC : %UC_LOGIN-4-AuthenticationFailed: %[Login Date/Time=07/09/2018 at 14:34:06]
[Login IP Address/Hostname=10.13.37.119][Login Interface=Cisco SOAP Server][Login UserID=admin][App ID=Cisco Tomcat][Cluster ID=][Node ID=cucm11]: Login
Authentication failed.
Host=10.13.37.44  Port=*514  Method=syslog
```

4.4.5. Date Range Searching

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

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



CISCO and SYSLOG

Displaying 1 - 10 of

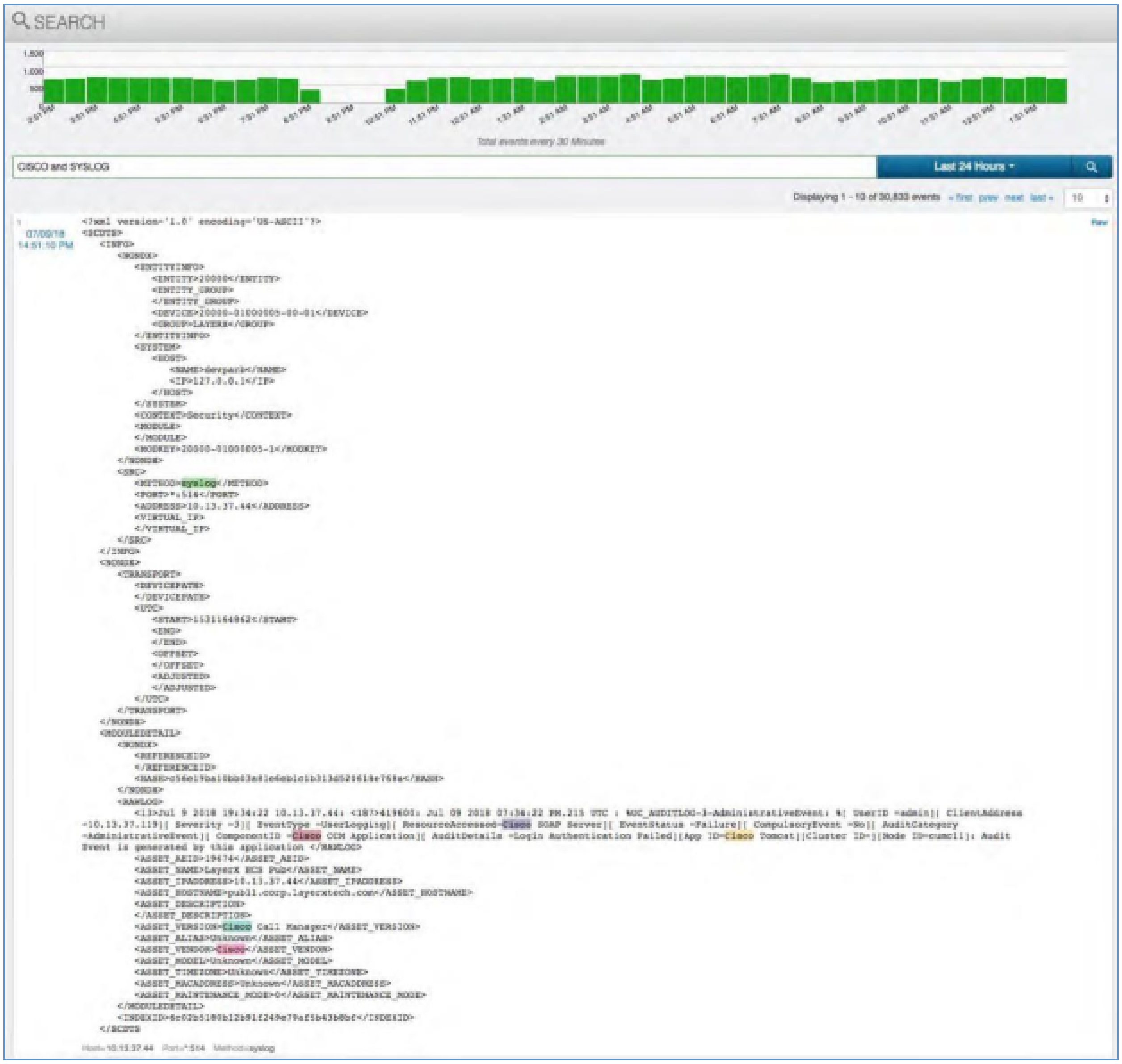
10

```
1   <13>Jul 9 2018 19:34:22 10.13.37.44: <187>419600: Jul 09 2018 07:34:22 PM.215 UTC : %UC_AUDITLOG-3-AdministrativeEvent: %[ UserID
07/09/18  =10.13.37.119][ Severity =3][ EventType =UserLogging][ ResourceAccessed=Cisco SOAP Server][ EventStatus =Failure][ CompulsoryEvent
14:51:10 PM  =AdministrativeEvent][ ComponentID =Cisco CCM Application][ AuditDetails =Login Authentication Failed][App ID=Cisco Tomcat][Clust   it
    Event is generated by this application
    Host=10.13.37.44  Port=*514  Method=syslog

2   <13>Jul 9 2018 19:34:22 10.13.37.44: <188>419599: Jul 09 2018 07:34:22 PM.215 UTC : %UC_LOGIN-4-AuthenticationFailed: %[Login Dat
07/09/18  [Login IP Address/Hostname=10.13.37.119][Login Interface=Cisco SOAP Server][Login UserID=admin][App ID=Cisco Tomcat][Cluster ID=[
14:51:10 PM  Authentication failed.
    Host=10.13.37.44  Port=*514  Method=syslog

3   <13>Jul 9 2018 19:34:22 10.13.37.43: <185>85235: : : 56044: CUCM12.layerstech.com: Jul 09 2018 19:34:21.781 UTC : %UC_RTMT-1-RTMT_ALERT: %
07/09/18  [AlertName=RTMTSessionsExceedsThreshold][AlertDetail= On Mon Jul 09 14:34:21 CDT 2018, alert RTMTSessionsExceedsThreshold has occured. Cou
14:51:10 PM  Cisco Tomcat Web Application(ast) on node CUCM12 has value of 260#012 which is over high threshold 250][AppID=Cisco AMC Service][ClusterID=
    Alert
    Host=10.13.37.43  Port=*514  Method=syslog

4   Invalid XML: null
07/09/18
14:51:08 PM

5   <13>Jul 9 2018 19:34:17 10.13.37.44: <186>173671: : : 120607: cumc11.layerstech.com: Jul 09 2018 07:34:15 PM.403 UTC : %UC_RTMT-2-RTMT_ALERT: %
07/09/18  [AlertName=SyslogSeverityMatchFound][AlertDetail= At Mon Jul 09 14:34:15 CDT 2018 on node 10.13.37.44, the following SyslogSeverityMatchFound events generated:
14:51:02 PM  #012SeverityMatch : Alert#012MatchedEvent : Jul 9 14:34:01 cumc11 authpriv 1 unix_chkpwd: could not obtain user info (root)#012AppID : Cisco Syslog
    Agent#012ClusterID : #012NodeID : cumc11#012 TimeStamp : Mon Jul 09 14:34:01 CDT 2018][AppID=Cisco AMC Service][ClusterID=][NodeID=cumc11]: RTMT Alert
    Host=10.13.37.44  Port=*514  Method=syslog
```

M	T	W	T	F	S	S
25	26	27	28	29	30	1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31	1	2	3	4	5

4.4.6. Search Result Meta-Data

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



CISCO and SYSLOG

Displaying 1 - 10 of 30,833 events

1
07/09/18
14:51:10 PM

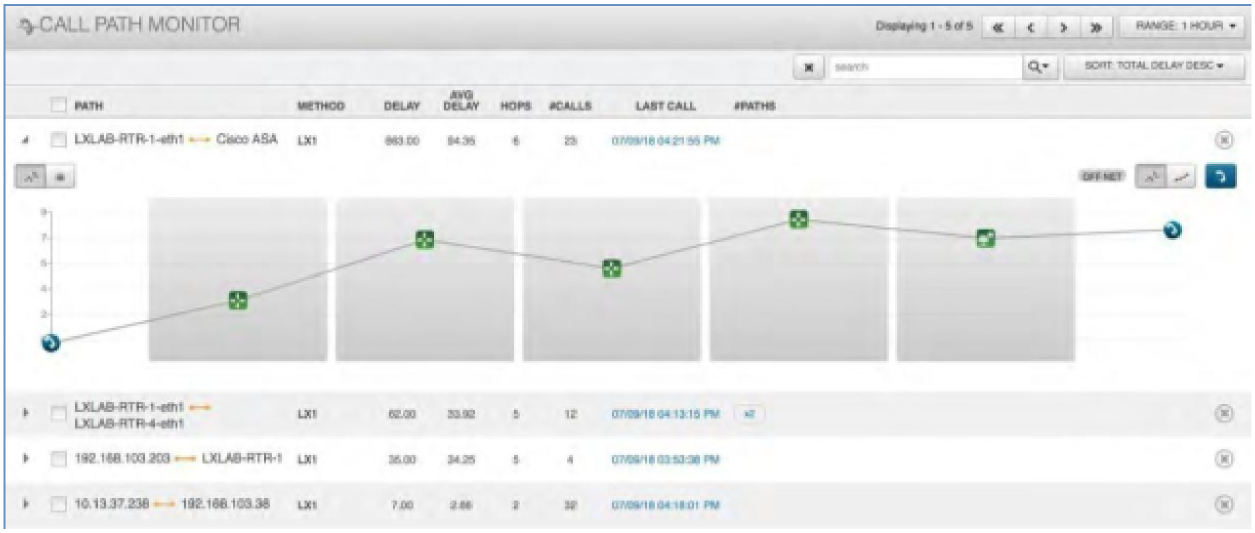
```
<?xml version='1.0' encoding='US-ASCII'?>
<SCDTS>
  <INFO>
    <NONDX>
      <ENTITYINFO>
        <ENTITY>20000</ENTITY>
        <ENTITY_GROUP>
        </ENTITY_GROUP>
        <DEVICE>20000-01000005-00-01</DEVICE>
        <GROUP>LAYERX</GROUP>
      </ENTITYINFO>
      <SYSTEM>
        <HOST>
          <NAME>devpark</NAME>
          <IP>127.0.0.1</IP>
        </HOST>
      </SYSTEM>
      <CONTEXT>Security</CONTEXT>
      <MODULE>
      </MODULE>
      <MODKEY>20000-01000005-1</MODKEY>
    </NONDX>
    <SRC>
      <METHOD>syslog</METHOD>
      <PORT>*:514</PORT>
      <ADDRESS>10.13.37.44</ADDRESS>
      <VIRTUAL_IP>
      </VIRTUAL_IP>
    </SRC>
  </INFO>
  <NONDX>
    <TRANSPORT>
      <DEVICEPATH>
      </DEVICEPATH>
      <UTC>
        <START>1531164862</START>
        <END>
        </END>
        <OFFSET>
        </OFFSET>
        <ADJUSTED>
        </ADJUSTED>
      </UTC>
    </TRANSPORT>
  </NONDX>
  <MODULEDETAIL>
    <NONDX>
      <REFERENCEID>
      </REFERENCEID>
      <HASH>c56e19ba10bb03a81e6eb1c1b313d520618e768a</HASH>
    </NONDX>
    <RAWLOG>
      <13>Jul 9 2018 19:34:22 10.13.37.44: <187>419603: Jul 09 2018 07:34:22 PM.215 UTC : %UC_AUDITLOG-3-AdministrativeEvent: %[ UserID =admin][ ClientAddress
=10.13.37.119][ Severity =3][ EventType =UserLogging][ ResourceAccessed=Cisco SOAP Server][ EventStatus =Failure][ CompulsoryEvent =No][ AuditCategory
=AdministrativeEvent][ ComponentID =Cisco CCM Application][ AuditDetails =Login Authentication Failed][App ID=Cisco Tomcat][Cluster ID=][Node ID=cucm11]: Audit
Event is generated by this application </RAWLOG>
      <ASSET_AEID>19674</ASSET_AEID>
      <ASSET_NAME>LayerX HCS Pub</ASSET_NAME>
      <ASSET_IPADDRESS>10.13.37.44</ASSET_IPADDRESS>
      <ASSET_HOSTNAME>pub11.corp.layerxtech.com</ASSET_HOSTNAME>
      <ASSET_DESCRIPTION>
      </ASSET_DESCRIPTION>
      <ASSET_VERSION>Cisco Call Manager</ASSET_VERSION>
      <ASSET_ALIAS>Unknown</ASSET_ALIAS>
      <ASSET_VENDOR>Cisco</ASSET_VENDOR>
      <ASSET_MODEL>Unknown</ASSET_MODEL>
      <ASSET_TIMEZONE>Unknown</ASSET_TIMEZONE>
      <ASSET_MACADDRESS>Unknown</ASSET_MACADDRESS>
      <ASSET_MAINTENANCE_MODE>0</ASSET_MAINTENANCE_MODE>
    </MODULEDETAIL>
    <INDEXID>6c02b5180b12b91f249e79af5b43b8bf</INDEXID>
  </SCDTS
```

Host=10.13.37.44 Port=*:514 Method=syslog

4.5. Call Path

4.5.1. Call Path Monitor

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



CALL PATH MONITOR

Displaying 1 - 5 of 5

RANGE: 1 HOUR

SORT: TOTAL DELAY DESC

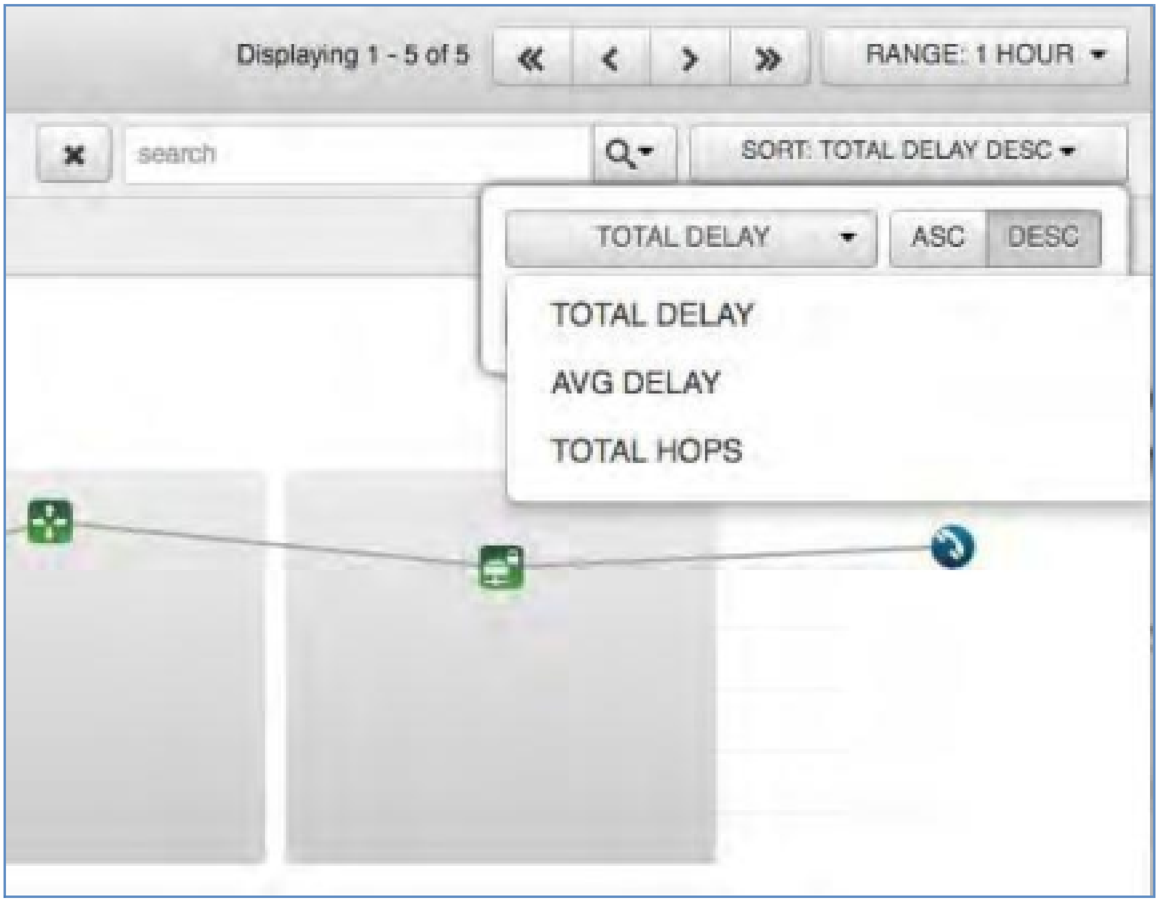
	PATH	METHOD	DELAY	AVG DELAY	HOPS	#CALLS	LAST CALL	#PATHS
□	LXLAB-RTR-1-eth1 ⟷ Cisco ASA	LX1	863.00	84.35	6	23	07/09/18 04:21:55 PM	
□	LXLAB-RTR-1-eth1 ⟷ LXLAB-RTR-4-eth1	LX1	62.00	33.92	5	12	07/09/18 04:13:15 PM	x2
□	192.168.103.203 ⟷ LXLAB-RTR-1	LX1	35.00	34.25	5	4	07/09/18 03:53:38 PM	
□	10.13.37.238 ⟷ 192.168.103.38	LX1	7.00	2.66	2	32	07/09/18 04:18:01 PM	

4.5.2. Sorting Call Paths

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

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

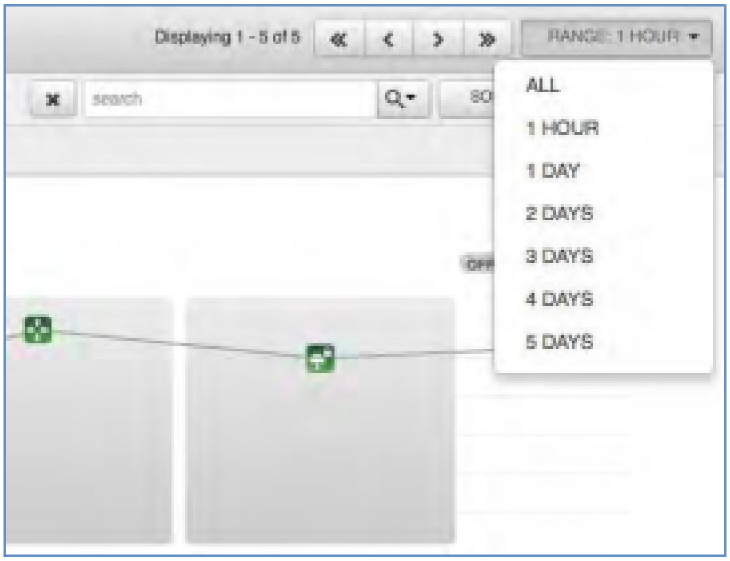
Each selection also has the choice of selecting ascending or descending order.



4.5.3. Time Range for Call Paths

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

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



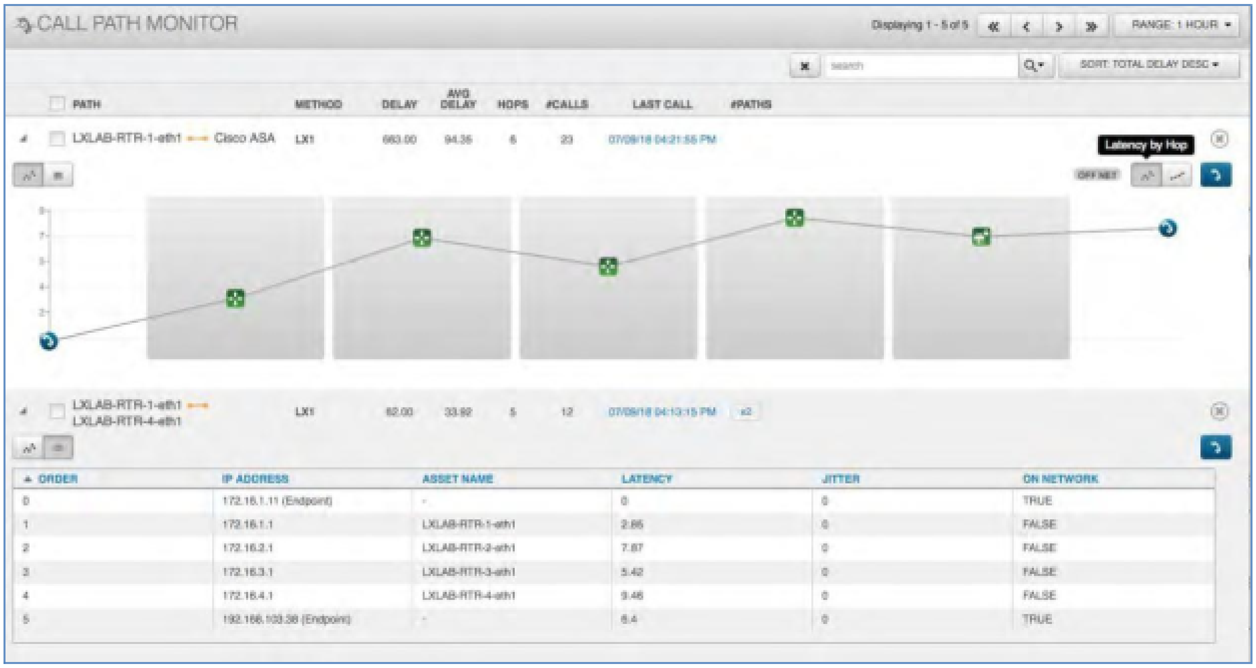
4.5.4. Expanding Call Paths

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

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

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

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



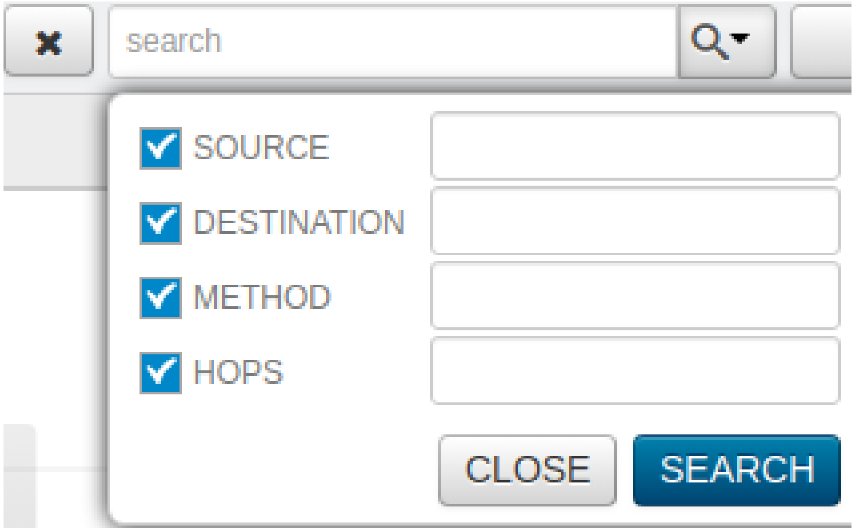
PATH	METHOD	DELAY	AVG DELAY	HOPS	#CALLS	LAST CALL	#PATHS
LXLAB-RTR-1-eth1 ⟷ Cisco ASA	LX1	663.00	94.36	6	23	07/09/18 04:21:56 PM	
LXLAB-RTR-1-eth1 ⟷ LXLAB-RTR-4-eth1	LX1	62.00	33.92	5	12	07/09/18 04:13:15 PM	x2

ORDER	IP ADDRESS	ASSET NAME	LATENCY	JITTER	ON NETWORK
0	172.16.1.11 (Endpoint)	-	0	0	TRUE
1	172.16.1.1	LXLAB-RTR-1-eth1	2.86	0	FALSE
2	172.16.2.1	LXLAB-RTR-2-eth1	7.87	0	FALSE
3	172.16.3.1	LXLAB-RTR-3-eth1	5.42	0	FALSE
4	172.16.4.1	LXLAB-RTR-4-eth1	9.46	0	FALSE
5	192.166.103.38 (Endpoint)	-	6.4	0	TRUE

4.5.5. Searching Call Paths

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

- Source
- Destination
- Method
- Hops



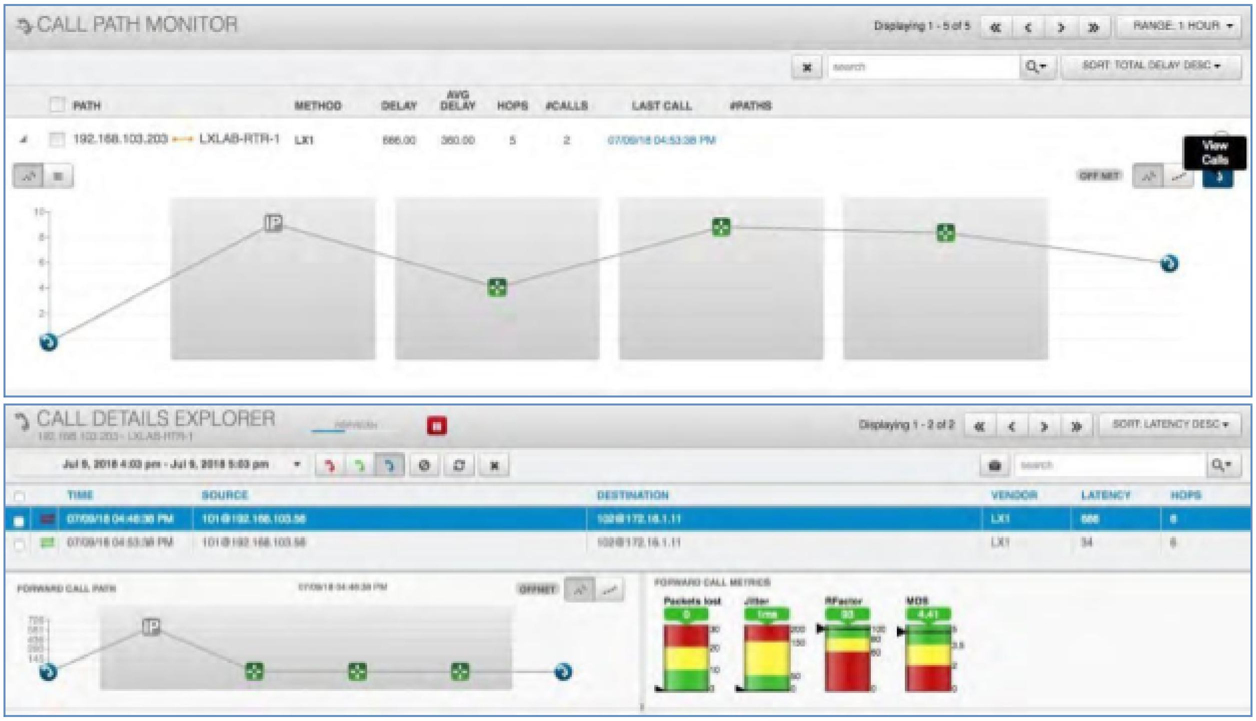
4.5.6. View Call Details from the Call Path

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

4.6. Call Details

4.6.1. Call Details Explorer

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



PATH	METHOD	DELAY	AVG DELAY	HOPS	#CALLS	LAST CALL	#PATHS
192.168.103.203 → LXLAB-RTR-1	LX1	666.00	360.00	5	2	07/09/18 04:53:38 PM	

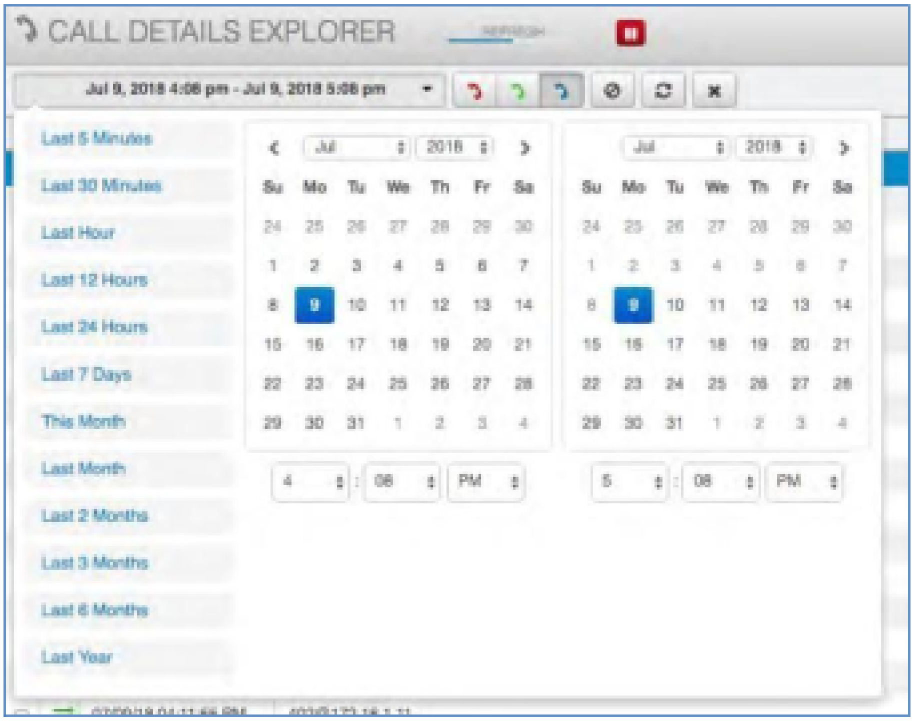
TIME	SOURCE	DESTINATION	VENDOR	LATENCY	HOPS
07/09/18 04:46:38 PM	101@192.168.103.56	102@172.16.1.11	LX1	666	6
07/09/18 04:53:38 PM	101@192.168.103.56	102@172.16.1.11	LX1	34	6

4.6.2. Filter by Date and Time

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

- Last 5 Minutes
- Last 30 Minutes
- Last Hour
- Last 12 Hours
- Last 24 Hours
- Last 7 Days * This Month
- Last Month
- Last 2 Months
- Last 3 Months
- Last 6 Months
- Last Year
- Specific Date and Time

We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

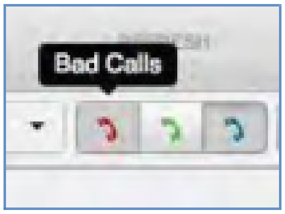


Jul 9, 2018 4:08 pm - Jul 9, 2018 5:08 pm

4 : 08 PM

5 : 08 PM

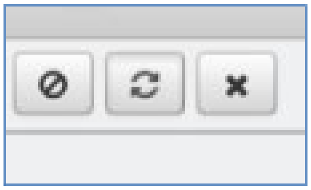
4.6.3. Filter by Call Quality



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

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

4.6.4. Clear Filter, Update and Delete Call

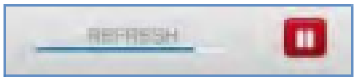


The three icons next to the call quality filters provide the functions below:

- Clear Filter: This will remove all filters set and the call details will show the default display.
- Update: The screen is pre-set with a refresh timer. Clicking this icon allows you to request new data on demand.
- Delete Call: If the check box is selected next to any call then by clicking this icon the system will delete that call.

4.6.5. Refresh Pause

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

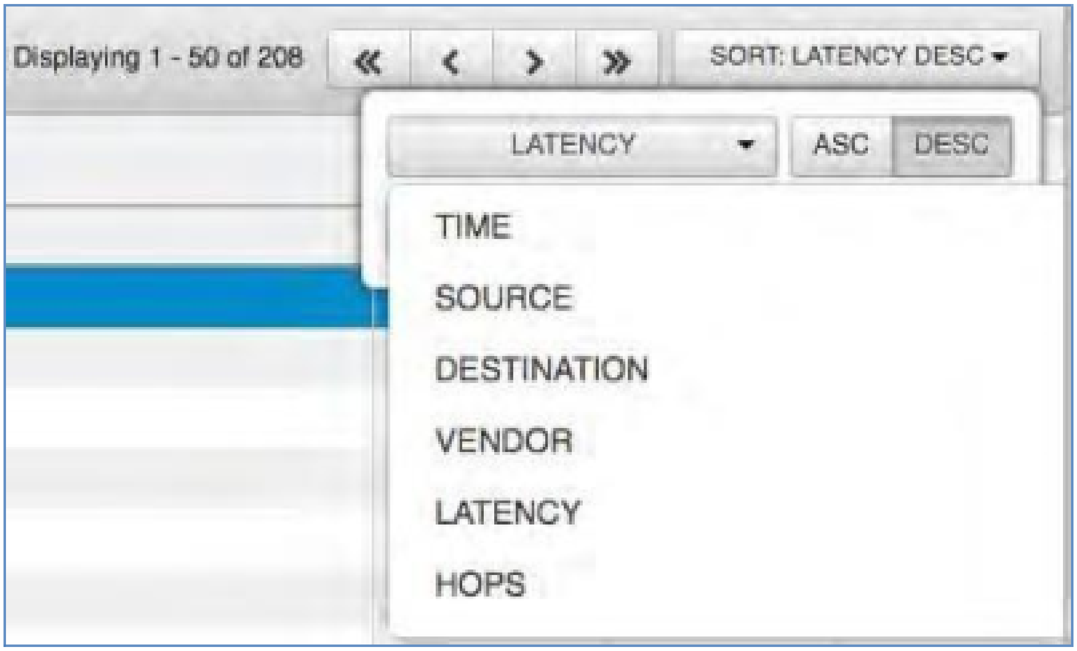


4.6.6. Sorting

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

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

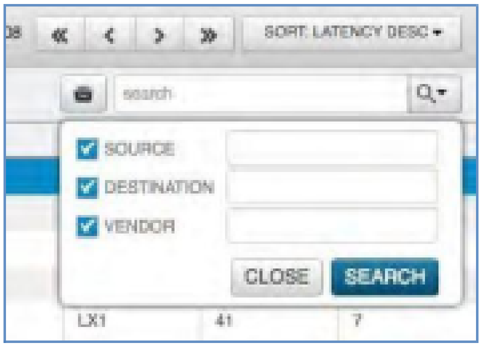
Each option allows for the choice of ascending or descending order.



4.6.7. Search Call Details

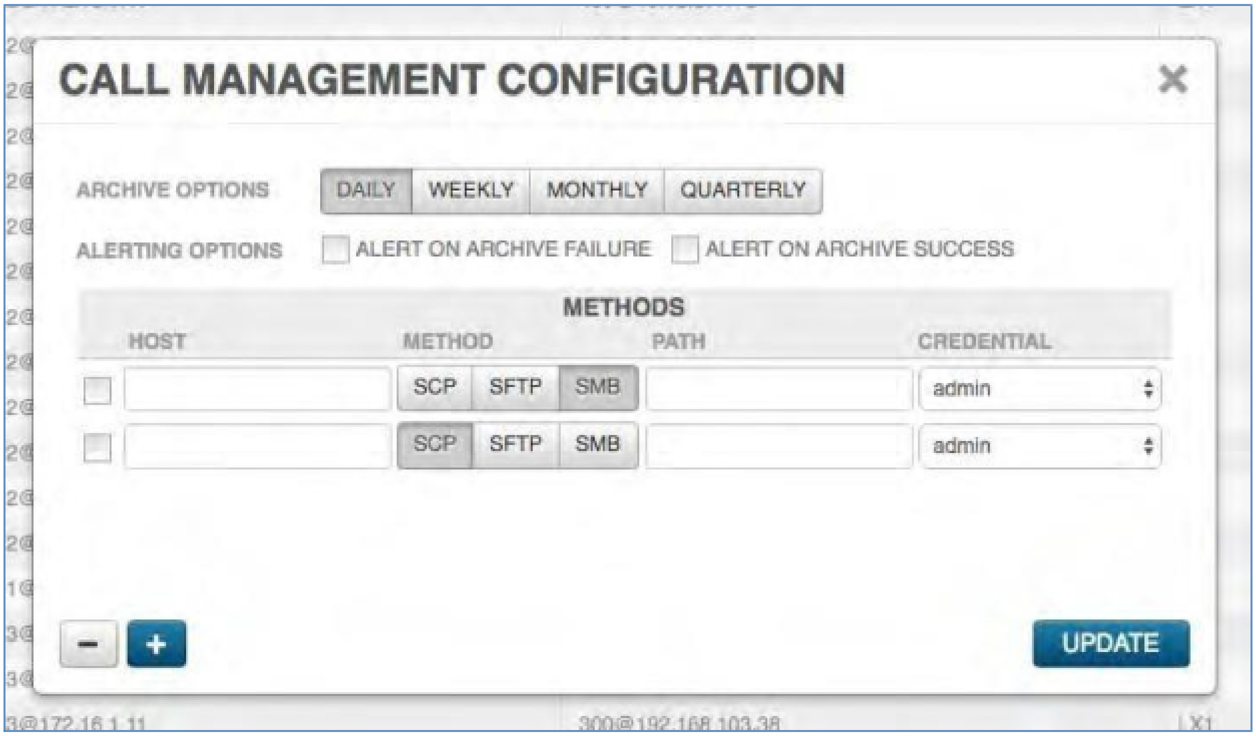
The search bar in the top right of the screen allows the user to search for specific call details. There are three options that can be utilized to search:

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



4.7. Call Management Configuration

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



CALL MANAGEMENT CONFIGURATION

ARCHIVE OPTIONS: [✓ DAILY] WEEKLY MONTHLY QUARTERLY

ALERTING OPTIONS: □ ALERT ON ARCHIVE FAILURE □ ALERT ON ARCHIVE SUCCESS

METHODS

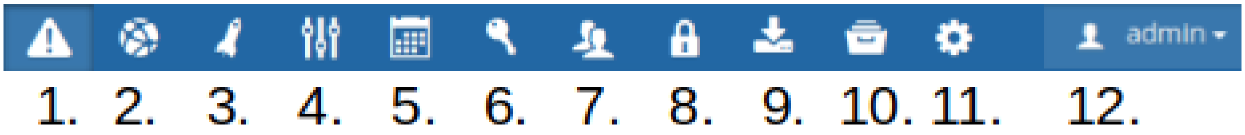
	HOST	METHOD	PATH	CREDENTIAL
□		SCP SFTP [✓ SMB]		admin
□		[✓ SCP] SFTP SMB		admin

We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

5. Configuration

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

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

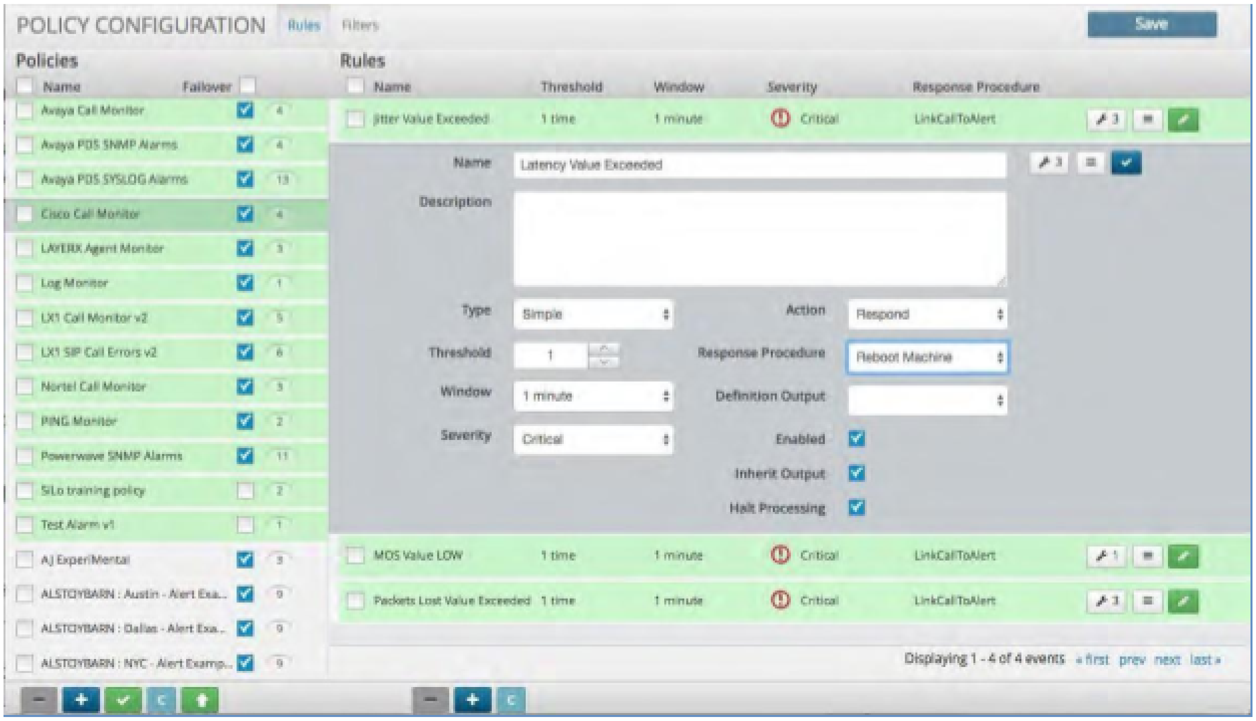


5.1. Policy Configuration

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

- Business Processes
- Infrastructure
- Security
- Applications
- Unified Communications

- Network behavior
- Metrics and Threshold Violations



POLICY CONFIGURATION Rules Filters Save

Policies

□	Name	Failover □	
□	Avaya Call Monitor	☑	4
□	Avaya PDS SNMP Alarms	☑	4
□	Avaya PDS SYSLOG Alarms	☑	13
□	Cisco Call Monitor	☑	4
□	LAYERX Agent Monitor	☑	3
□	Log Monitor	☑	1
□	LX1 Call Monitor v2	☑	5
□	LX1 SIP Call Errors v2	☑	6
□	Nortel Call Monitor	☑	3
□	PING Monitor	☑	2
□	Powerwave SNMP Alarms	☑	11
□	SiLo training policy	□	2
□	Test Alarm v1	□	1
□	AJ ExperiMental	☑	3
□	ALSTOYBARN : Austin - Alert Exa...	☑	9
□	ALSTOYBARN : Dallas - Alert Exa...	☑	9
□	ALSTOYBARN : NYC - Alert Examp...	☑	9

Rules

□	Name	Threshold	Window	Severity	Response Procedure
□	Jitter Value Exceeded	1 time	1 minute	Critical	LinkCallToAlert

Name: Latency Value Exceeded

Description:

Type: Simple

Threshold: 1

Window: 1 minute

Severity: Critical

Action: Respond

Response Procedure: Reboot Machine

Definition Output:

Enabled ☑

Inherit Output ☑

Halt Processing ☑

□	Name	Threshold	Window	Severity	Response Procedure
□	MOS Value LOW	1 time	1 minute	Critical	LinkCallToAlert
□	Packets Lost Value Exceeded	1 time	1 minute	Critical	LinkCallToAlert

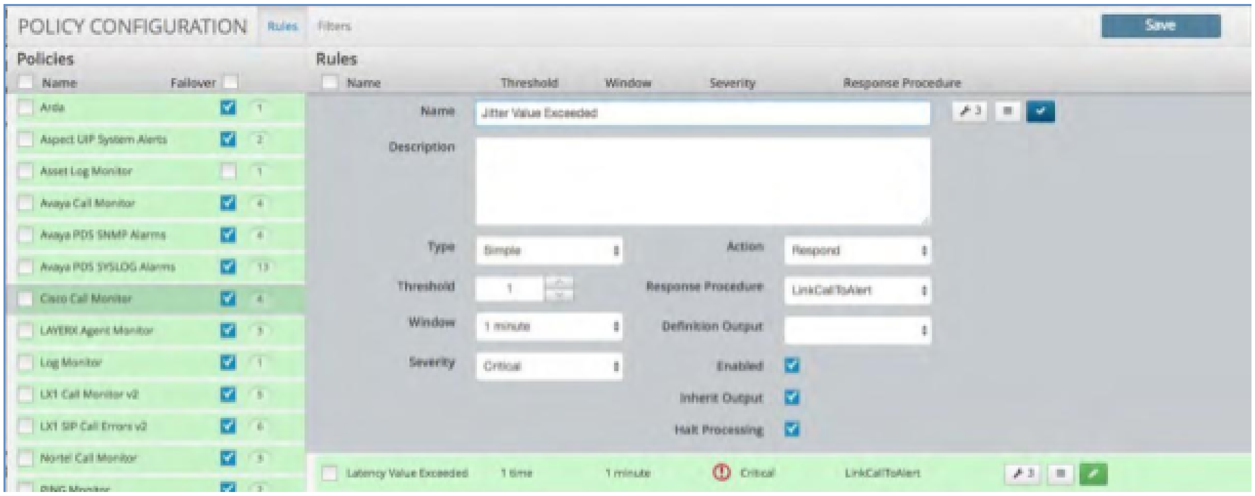
Displaying 1 - 4 of 4 events « first prev next last »

5.1.1. Correlation Rules

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

Parameter	Description
Name	Descriptive name for the correlation rule which will be displayed within an Alert and viewed in Alert Analyzer.
Description	Enter a complete description of the problem that created the alert along with any specific remediation steps that should be taken to resolve the problem.
Type	Simple: Select if the rule is to analyze a single log and as a result of the rule, you want to execute an action. 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	Selects how many times this rule is to match before an action occurs.
Window	Select the time window for the rule to match before an action occurs.

Parameter	Description
Severity	Indicates what is to appear in the Status field on the Alert Viewer monitor. Select the severity for this rule: • Informational • Minor • Major • Critical
Action	Choose the action that is to occur for this rule, based on the selection in the Severity field • 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. • 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 menu to execute when conditions have been met.
Definition Output	Selects a single Correlation Definition's extracted value to be displayed with the Alert.
Enabled	Toggle to enable/disable the rule
Inherit Output	Toggle to enable/disable whether the rule will include the results of the filter attached to the policy module.
Halt Processing	Toggle to halt processing of logs to any other rules within the policy if the rule matches. This will highlight the Policy in Green to indicate that this function is in use.
Correlation Definitions	Click the wrench icon where you can define one or more definitions match and or extract the required data from a log or event. See Correlation Definitions.
Output Order	Sets the preferred order to output the extracted data from the Correlation Definitions.
Done	Click the Done box when the rule is complete
Save	Be sure to click the Save button so your rule (or changes) are saved and committed.



□	Name	Failover □	
□	Arda	☑	1
□	Aspect UIP System Alerts	☑	2
□	Asset Log Monitor	□	1
□	Avaya Call Monitor	☑	4
□	Avaya PDS SNMP Alarms	☑	4
□	Avaya PDS SYSLOG Alarms	☑	13
□	Cisco Call Monitor	☑	4
□	LAYERX Agent Monitor	☑	3
□	Log Monitor	☑	1
□	LX1 Call Monitor v2	☑	5
□	LX1 SIP Call Errors v2	☑	6
□	Nortel Call Monitor	☑	3
□	PING Monitor	☑	2

Name: Jitter Value Exceeded

Description:

Type: Simple

Action: Respond

Threshold: 1

Response Procedure: LinkCallToAlert

Window: 1 minute

Definition Output:

Severity: Critical

Enabled: ☑

Inherit Output: ☑

Halt Processing: ☑

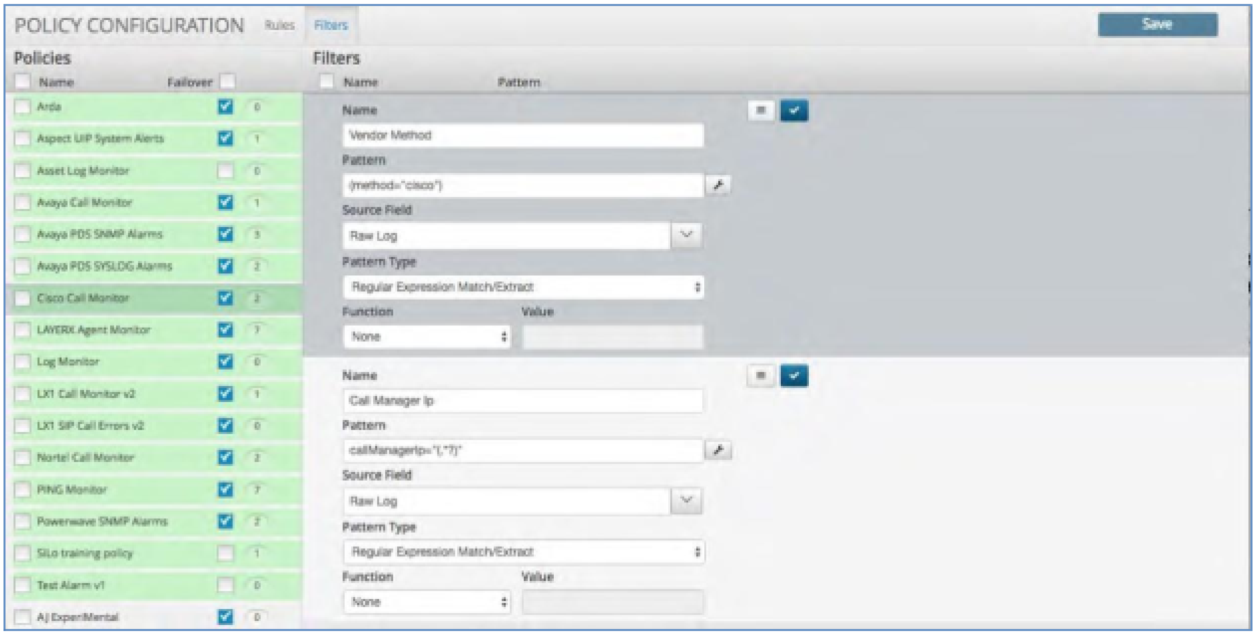
□	Name	Threshold	Window	Severity	Response Procedure
□	Latency Value Exceeded	1 time	1 minute	Critical	LinkCallToAlert

Correlation Filters are a very quick and easy way to ensure that all of the correlation rules within the policy are firing on the correct set of data. The engine will look at the filter criteria first, select only the data that matches the criteria and then look to apply the correlation rule. The user can add as many of these that are required or desired. The options in each filter are:

- Name: Name this as close as possible to the data elements being filtered. That way the output matches the name once viewed in the alert text.
- Pattern: This is the extraction methodology utilized to pull the particular data point out. Click the “wrench” icon beside this box and it will bring up the “Regex Wizard” to assist in finding and extracting the data.

  Within the Regex Wizard there are 2 sections:

  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:”. As the phrase indicates 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 utilize the wizard to create the Regular Expression required. Close the wizard and copy this pattern the Regex into the box under Pattern.
- Source Field: In the drop-down box select the source from which the data is being extracted.
- Pattern Type: Select from the drop-down box the type of expression you want to utilize:
  - String Match
  - Regular Expression Match
  - Regular Expression Match/Extract (Most Often Used)
  - Regular Expression Multi-Valued Extract
- Function: If the extracted data is integer based then you can apply the following functions that will allow you to compare the data:
  - None
  - Greater Than
  - Less Than
  - Same
- Value: This field will only be available if the data extracted is an integer.



Policies

□ Name	Failover □	
□ Arda	☑	0
□ Aspect UIP System Alerts	☑	1
□ Asset Log Monitor	□	0
□ Avaya Call Monitor	☑	1
□ Avaya PDS SNMP Alarms	☑	3
□ Avaya PDS SYSLOG Alarms	☑	2
□ Cisco Call Monitor	☑	2
□ LAYERX Agent Monitor	☑	7
□ Log Monitor	☑	0
□ LX1 Call Monitor v2	☑	1
□ LX1 SIP Call Errors v2	☑	0
□ Nortel Call Monitor	☑	2
□ PING Monitor	☑	7
□ Powerwave SNMP Alarms	☑	2
□ SiLo training policy	□	1
□ Test Alarm v1	□	0
□ AJ ExperiMental	☑	0

Filters

□ Name Pattern

Name: Vendor Method
Pattern: (method="cisco")
Source Field: Raw Log
Pattern Type: Regular Expression Match/Extract
Function: None
Value:

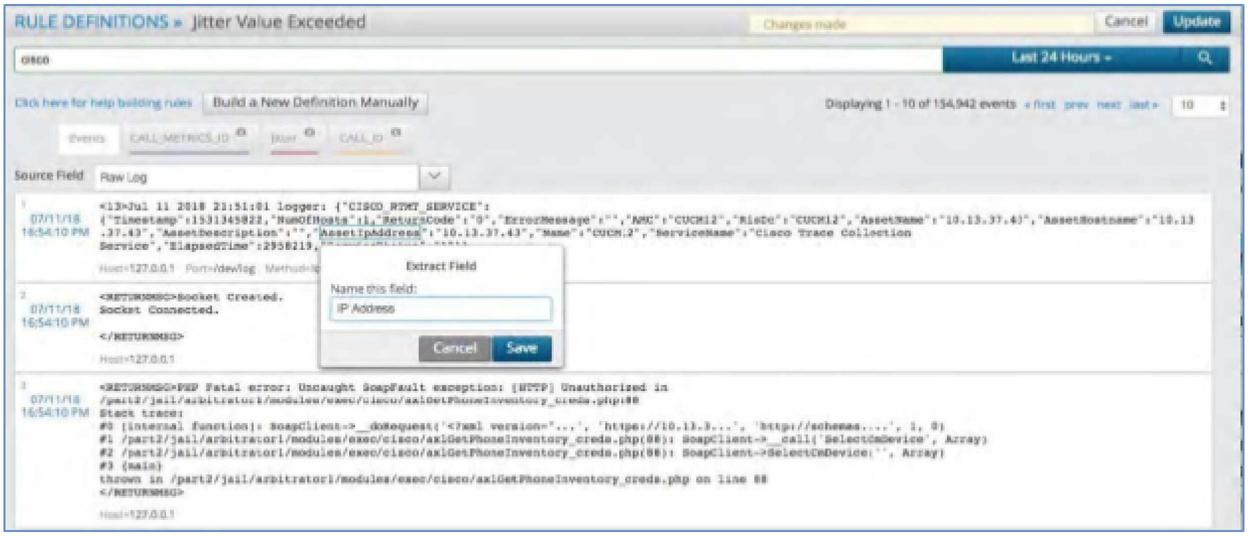
Name: Call Manager Ip
Pattern: callManagerIp="(.*?)"
Source Field: Raw Log
Pattern Type: Regular Expression Match/Extract
Function: None
Value:

5.1.2. Correlation Definitions

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

Parameter	Description
Name	Name this as close as possible to the data elements being extracted. That way the output matches the name once viewed in the alert text. It is also utilized in the key value pair within the alert text. 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. If you have trouble with this method due to special characters in the data set, then you can utilize the "wrench" icon beside the Pattern box and it will bring up the "Regex Wizard" to assist in finding and extracting the data.
Pattern	Within the Regex Wizard there are 2 sections: • 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	Select from the drop-down box the type of expression you want to utilize: • String Match • Regular Expression Match • Regular Expression Match/Extract (Most Often Used) • Regular Expression Multi-Valued Extract
Function	If the extracted data is integer based, then you can apply the following functions that will allow you to compare the data: • None • Greater Than • Less Than • Same
Value	This field will only be available if the data extracted is an integer.



1 07/11/18 16:54:10 PM

```
<13>Jul 11 2018 21:51:01 logger: {"CISCO_RTMT_SERVICE":
{"Timestamp":1531345822,"NumOfHosts":1,"ReturnCode":"0","ErrorMessage":"","ANC":"CUCM12","RisDc":"CUCM12","AssetName":"10.13.37.43","AssetHostname":"10.13
.37.43","AssetDescription":"","AssetIpAddress":"10.13.37.43","Name":"CUCM.2","ServiceName":"Cisco Trace Collection
Service","ElapsedTime":2958219,
```

Host=127.0.0.1 Port=/dev/log Method=

Name this field: IP Address

2 07/11/18 16:54:10 PM

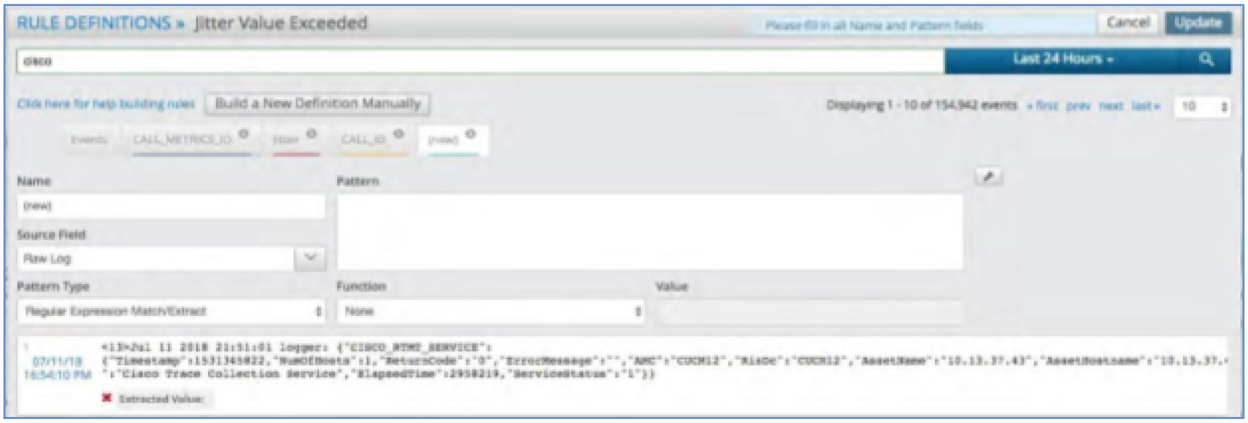
```
<RETURNMSG>Socket Created.
Socket Connected.

</RETURNMSG>
```

Host=127.0.0.1

3 07/11/18 16:54:10 PM

```
<RETURNMSG>PHP Fatal error: Uncaught SoapFault exception: [HTTP] Unauthorized in
/part2/jail/arbitrator1/modules/exec/cisco/axlGetPhoneInventory_creds.php:88
Stack trace:
#0 [internal function]: SoapClient->__doRequest('<?xml version="...', 'https://10.13.3...', 'http://schemas....', 1, 0)
#1 /part2/jail/arbitrator1/modules/exec/cisco/axlGetPhoneInventory_creds.php(88): SoapClient->__call('SelectCmDevice', Array)
#2 /part2/jail/arbitrator1/modules/exec/cisco/axlGetPhoneInventory_creds.php(88): SoapClient->SelectCmDevice('', Array)
#3 {main}
thrown in /part2/jail/arbitrator1/modules/exec/cisco/axlGetPhoneInventory_creds.php on line 88
</RETURNMSG>
```

Host=127.0.0.1


RULE DEFINITIONS » Jitter Value Exceeded
Please fill in all Name and Pattern fields
Cancel
Update
cisco
Last 24 Hours ▾
Click here for help building rules
Build a New Definition Manually
Displaying 1 - 10 of 154,942 events
« first
prev
next
last »
10
Events
CALL_METRICS_ID
Jitter
CALL_ID
(new)

Name: (new)

Pattern:

Source Field: Raw Log

Pattern Type: Regular Expression Match/Extract

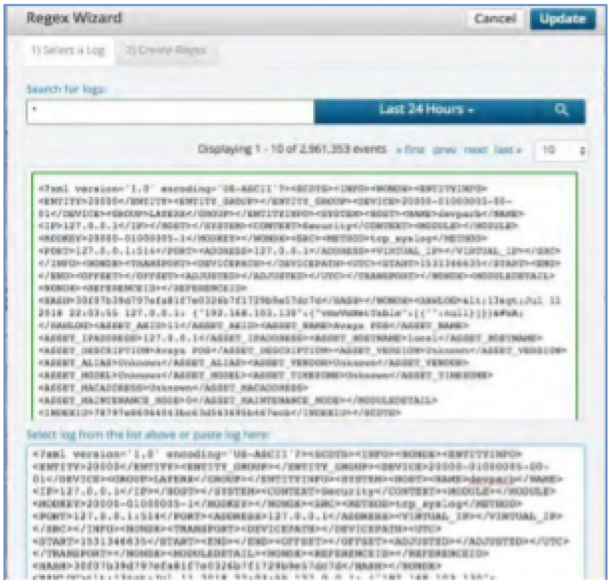
Function: None

Value:

1 07/11/18 16:54:10 PM

```
<13>Jul 11 2018 21:51:01 logger: {"CISCO_RTMT_SERVICE":
{"Timestamp":1531345822,"NumOfHosts":1,"ReturnCode":"0","ErrorMessage":"","ANC":"CUCM12","RisDc":"CUCM12","AssetName":"10.13.37.43","AssetHostname":"10.13.37.
":"Cisco Trace Collection Service","ElapsedTime":2958219,"ServiceStatus":"1"}}
```

✖ Extracted Value:

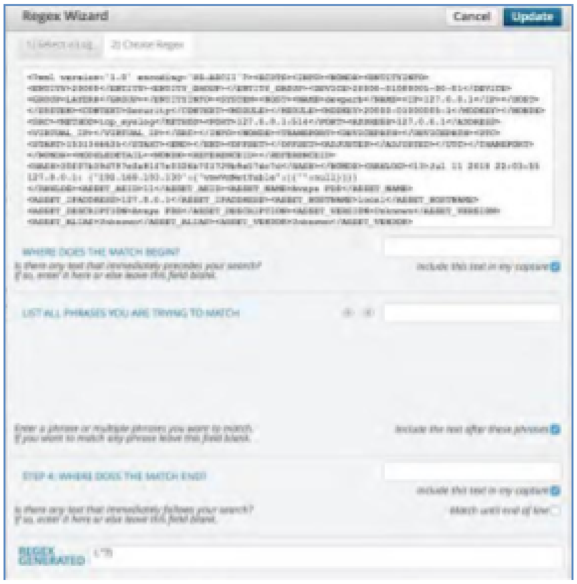


*

```
<?xml version='1.0' encoding='US-ASCII'?><SCOTS><INFO><NONDE><ENTITYINFO>
<ENTITY>20000</ENTITY><ENTITY_GROUP></ENTITY_GROUP><DEVICE>20000-01000005-00-
01</DEVICE><GROUP>LAYER8</GROUP></ENTITYINFO><SYSTEM><HOST><NAME>devpark</NAME>
<IP>127.0.0.1</IP></HOST></SYSTEM><CONTENT>Security</CONTENT><MODULE></MODULE>
<MODKEY>20000-01000005-1</MODKEY></NONDE><SRC><METHOD>tcp_syslog</METHOD>
<PORT>127.0.0.1:514</PORT><ADDRESS>127.0.0.1</ADDRESS><VIRTUAL_IP></VIRTUAL_IP></SRC>
</INFO><NONDE><TRANSPORT><DEVICEPATH></DEVICEPATH><UTC><START>1531344635</START><END>
</END><OFFSET></OFFSET><ADJUSTED></ADJUSTED></UTC></TRANSPORT></NONDE><MODULEDETAIL>
<NONDE><REFERENCEID></REFERENCEID>
<HASH>30f07b39d797efa81f7e0326b7f1729b9e57dc7d</HASH></NONDE><RAWLOG>&lt;13&gt;Jul 11
2018 22:03:55 127.0.0.1: {"192.168.103.130":{"vmwVmNetTable":[{"":null}]}}&#xA;
</RAWLOG><ASSET_AEID>11</ASSET_AEID><ASSET_NAME>Avaya PDS</ASSET_NAME>
<ASSET_IPADDRESS>127.0.0.1</ASSET_IPADDRESS><ASSET_HOSTNAME>Local</ASSET_HOSTNAME>
<ASSET_DESCRIPTION>Avaya PDS</ASSET_DESCRIPTION><ASSET_VERSION>Unknown</ASSET_VERSION>
<ASSET_ALIAS>Unknown</ASSET_ALIAS><ASSET_VENDOR>Unknown</ASSET_VENDOR>
<ASSET_MODEL>Unknown</ASSET_MODEL><ASSET_TIMEZONE>Unknown</ASSET_TIMEZONE>
<ASSET_MACADDRESS>Unknown</ASSET_MACADDRESS>
<ASSET_MAINTENANCE_MODE>0</ASSET_MAINTENANCE_MODE></MODULEDETAIL>
<INDEXID>[illegible]</INDEXID></SCOTS>
```

Select log from the list above or paste log here:

```
<?xml version='1.0' encoding='US-ASCII'?><SCOTS><INFO><NONDE><ENTITYINFO>
<ENTITY>20000</ENTITY><ENTITY_GROUP></ENTITY_GROUP><DEVICE>20000-01000005-00-
01</DEVICE><GROUP>LAYER8</GROUP></ENTITYINFO><SYSTEM><HOST><NAME>devpark</NAME>
<IP>127.0.0.1</IP></HOST></SYSTEM><CONTENT>Security</CONTENT><MODULE></MODULE>
<MODKEY>20000-01000005-1</MODKEY></NONDE><SRC><METHOD>tcp_syslog</METHOD>
<PORT>127.0.0.1:514</PORT><ADDRESS>127.0.0.1</ADDRESS><VIRTUAL_IP></VIRTUAL_IP>
</SRC></INFO><NONDE><TRANSPORT><DEVICEPATH></DEVICEPATH><UTC>
<START>1531344635</START><END></END><OFFSET></OFFSET><ADJUSTED></ADJUSTED></UTC>
</TRANSPORT></NONDE><MODULEDETAIL><NONDE><REFERENCEID></REFERENCEID>
<HASH>30f07b39d797efa81f7e0326b7f1729b9e57dc7d</HASH></NONDE>
<RAWLOG>&lt;13&gt;Jul 11 2018 22:03:55 127.0.0.1: {"192.168.103.130":
```



```
<?xml version='1.0' encoding='US-ASCII'?><SCOTS><INFO><NONDE><ENTITYINFO>
<ENTITY>20000</ENTITY><ENTITY_GROUP></ENTITY_GROUP><DEVICE>20000-01000005-00-01</DEVICE>
<GROUP>LAYER8</GROUP></ENTITYINFO><SYSTEM><HOST><NAME>devpark</NAME><IP>127.0.0.1</IP></HOST>
</SYSTEM><CONTENT>Security</CONTENT><MODULE></MODULE><MODKEY>20000-01000005-1</MODKEY></NONDE>
<SRC><METHOD>tcp_syslog</METHOD><PORT>127.0.0.1:514</PORT><ADDRESS>127.0.0.1</ADDRESS>
<VIRTUAL_IP></VIRTUAL_IP></SRC></INFO><NONDE><TRANSPORT><DEVICEPATH></DEVICEPATH><UTC>
<START>1531344635</START><END></END><OFFSET></OFFSET><ADJUSTED></ADJUSTED></UTC></TRANSPORT>
</NONDE><MODULEDETAIL><NONDE><REFERENCEID></REFERENCEID>
<HASH>30f07b39d797efa81f7e0326b7f1729b9e57dc7d</HASH></NONDE><RAWLOG><13>Jul 11 2018 22:03:55
127.0.0.1: {"192.168.103.130":{"vmwVmNetTable":[{"":null}]}}
</RAWLOG><ASSET_AEID>11</ASSET_AEID><ASSET_NAME>Avaya PDS</ASSET_NAME>
<ASSET_IPADDRESS>127.0.0.1</ASSET_IPADDRESS><ASSET_HOSTNAME>Local</ASSET_HOSTNAME>
<ASSET_DESCRIPTION>Avaya PDS</ASSET_DESCRIPTION><ASSET_VERSION>Unknown</ASSET_VERSION>
<ASSET_ALIAS>Unknown</ASSET_ALIAS><ASSET_VENDOR>Unknown</ASSET_VENDOR>
```

WHERE DOES THE MATCH BEGIN?

Is there any text that immediately precedes your search? If so, enter it here or else leave this field blank.

include this text in my capture ☑

LIST ALL PHRASES YOU ARE TRYING TO MATCH

Enter a phrase or multiple phrases you want to match. If you want to match any phrase leave this field blank.

include the text after these phrases ☑

STEP 4: WHERE DOES THE MATCH END?

include this text in my capture ☑

Is there any text that immediately follows your search? If so, enter it here or else leave this field blank.

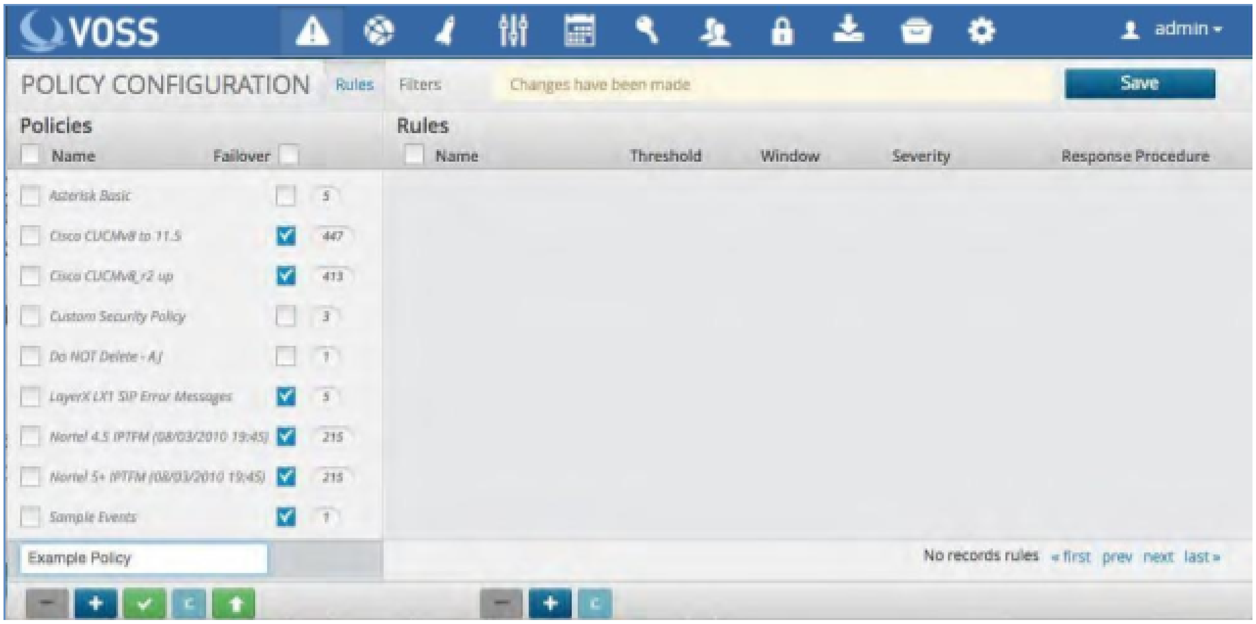
Match until end of line ☐

REGEX GENERATED: (.*?)

5.1.3. Creating a Policy

To Create a Policy:

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



Policies

□ Name	Failover □	
□ Asterisk Basic	□	5
□ Cisco CUCMv8 to 11.5	☑	447
□ Cisco CUCMv8_r2 up	☑	413
□ Custom Security Policy	□	3
□ Do NOT Delete - AJ	□	1
□ LayerX LX1 SIP Error Messages	☑	5
□ Nortel 4.5 IPTFM (08/03/2010 19:45)	☑	215
□ Nortel 5+ IPTFM (08/03/2010 19:45)	☑	215
□ Sample Events	☑	1

Example Policy

Rules

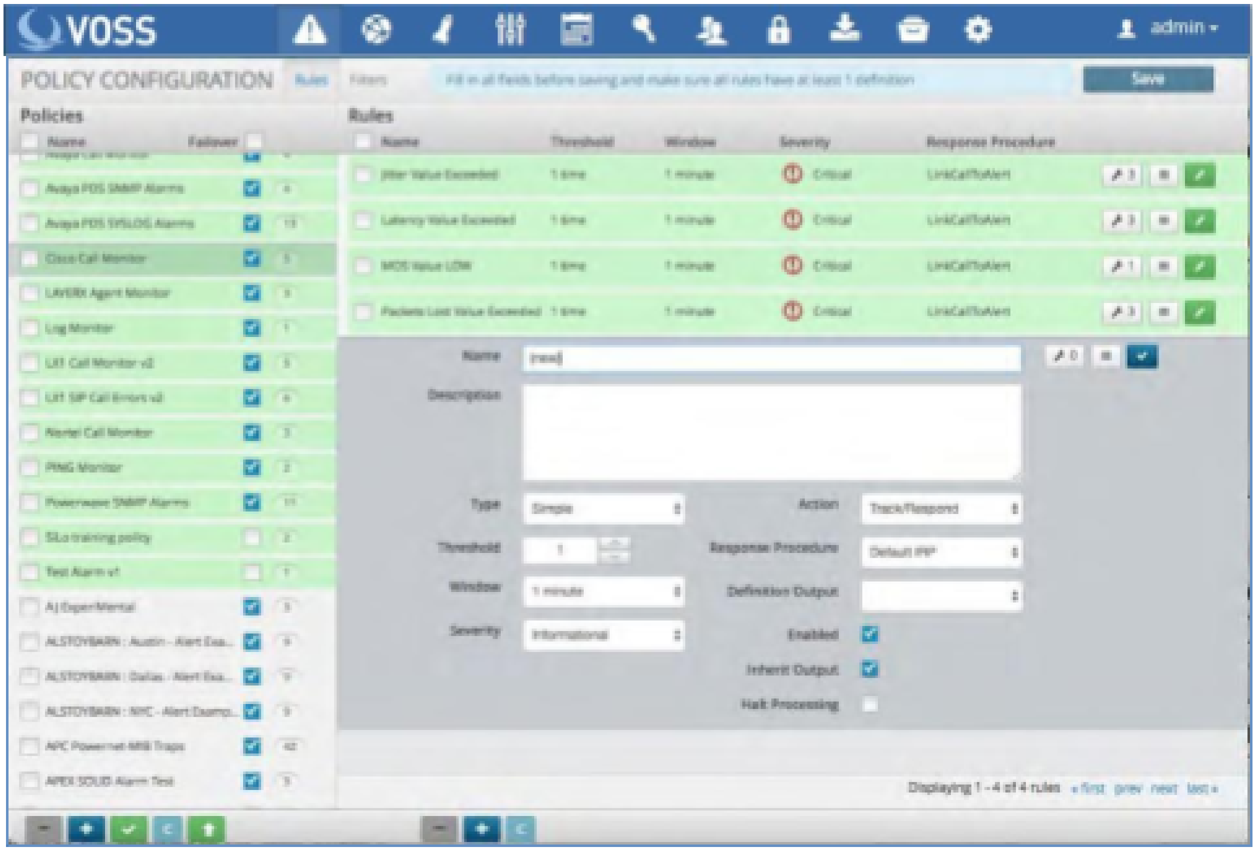
□ Name	Threshold	Window	Severity	Response Procedure

No records rules « first prev next last »

5.1.4. Creating a Correlation Rule

To Create a new Correlation Rule:

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



Fill in all fields before saving and make sure all rules have at least 1 definition

Policies

☐ Name	Failover ☐	
☐ Avaya PDS SNMP Alarms	☑	4
☐ Avaya PDS SYSLOG Alarms	☑	13
☐ Cisco Call Monitor	☑	5
☐ LAVERX Agent Monitor	☑	3
☐ Log Monitor	☑	1
☐ LXT Call Monitor v2	☑	5
☐ LXT SIP Call Errors v2	☑	6
☐ Nortel Call Monitor	☑	3
☐ PING Monitor	☑	2
☐ Powerwave SNMP Alarms	☑	11
☐ SLo training policy	☐	2
☐ Test Alarm v1	☐	1
☐ AJ ExperMental	☑	3
☐ ALSTOYBARN : Austin - Alert Exa...	☑	9
☐ ALSTOYBARN : Dallas - Alert Exa...	☑	9
☐ ALSTOYBARN : NYC - Alert Exampl...	☑	9
☐ APC Powernet-MIB Traps	☑	42
☐ APEX SOLID Alarm Test	☑	5

Rules

☐ Name	Threshold	Window	Severity	Response Procedure	
☐ Jitter Value Exceeded	1 time	1 minute	Critical	LinkCallToAlert	3
☐ Latency Value Exceeded	1 time	1 minute	Critical	LinkCallToAlert	3
☐ MOS Value LOW	1 time	1 minute	Critical	LinkCallToAlert	1
☐ Packets Lost Value Exceeded	1 time	1 minute	Critical	LinkCallToAlert	3

Name: (new) 0

Description:

Type: Simple

Action: Track/Respond

Threshold: 1

Response Procedure: Default IRP

Window: 1 minute

Definition Output:

Severity: Informational

Enabled ☑

Inherit Output ☑

Halt Processing ☐

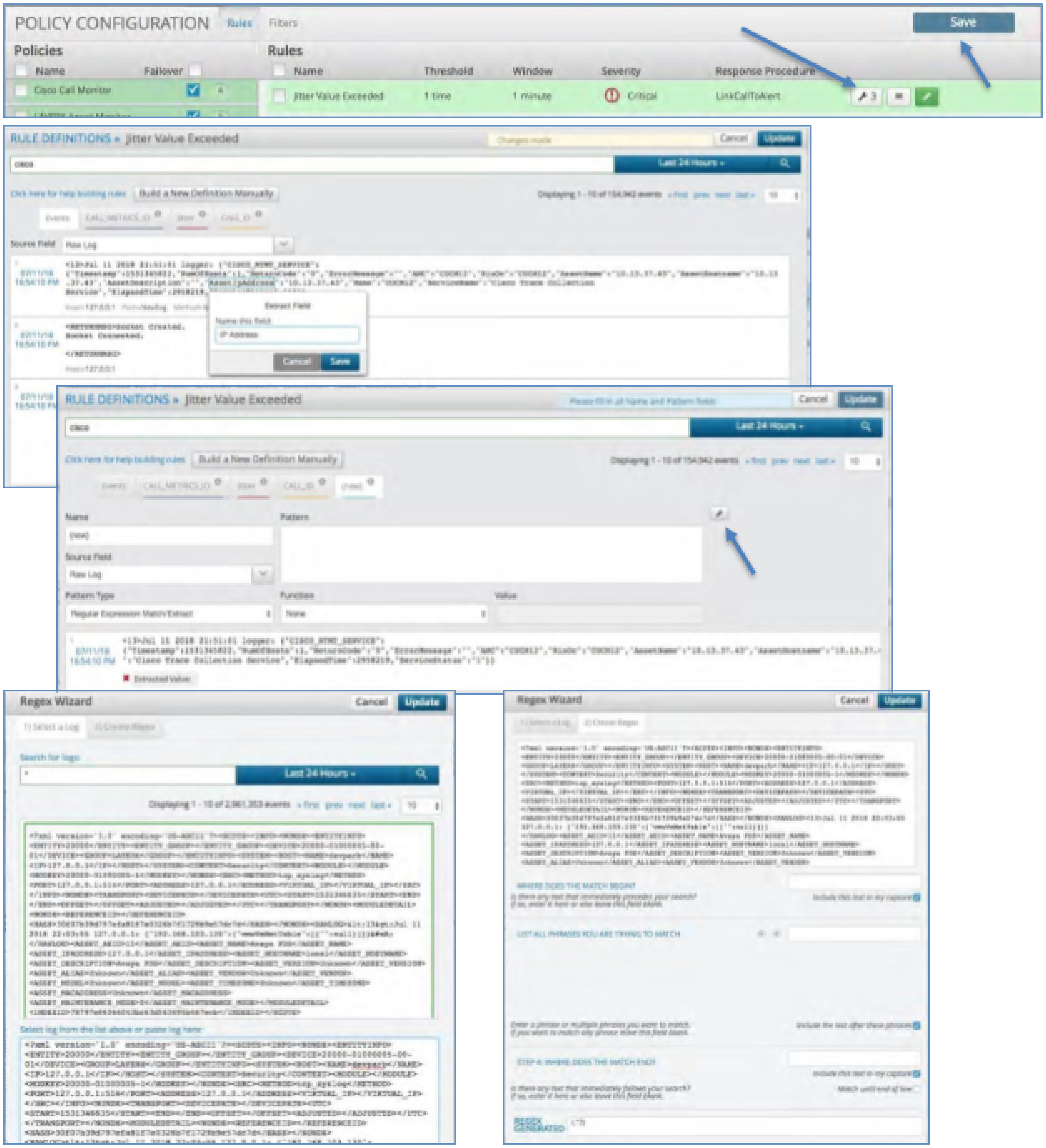
Displaying 1 - 4 of 4 rules « first prev next last »

5.1.5. Creating a Definition

To create a new definition:

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

We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

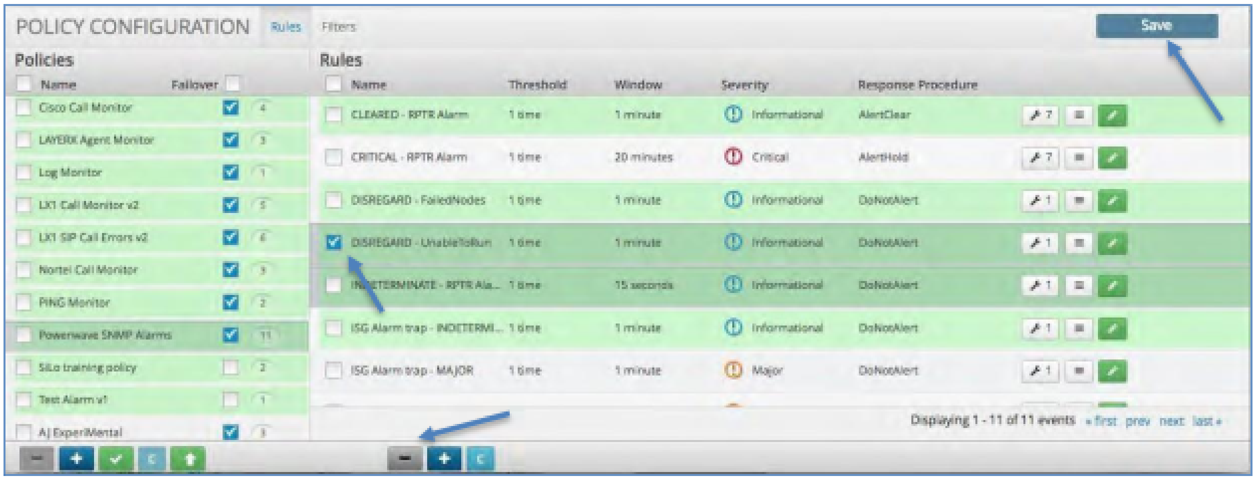


5.1.6. Deleting a Correlation Rule

To delete a Correlation Rule:

1. Click the policy name on the left side of the screen.
2. Click the check box on the Correlation rule you wish to delete.
3. Click the minus icon at the bottom of the correlation panel.

4. Click the Save icon in the upper right to save your change.



POLICY CONFIGURATION Rules Filters Save

Policies

□	Name	Failover □	
□	Cisco Call Monitor	☑	4
□	LAYERX Agent Monitor	☑	3
□	Log Monitor	☑	1
□	LX1 Call Monitor v2	☑	5
□	LX1 SIP Call Errors v2	☑	6
□	Nortel Call Monitor	☑	3
□	PING Monitor	☑	2
□	Powerwave SNMP Alarms	☑	11
□	SiLo training policy	□	2
□	Test Alarm v1	□	1
□	AJ ExperiMental	☑	3

Rules

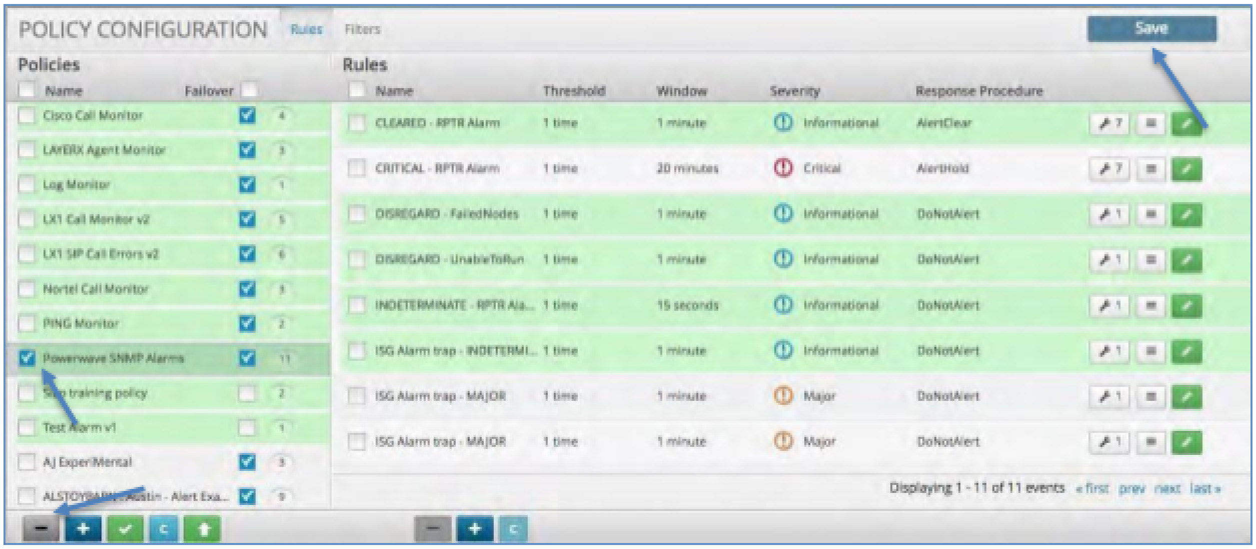
□	Name	Threshold	Window	Severity	Response Procedure	
□	CLEARED - RPTR Alarm	1 time	1 minute	Informational	AlertClear	7
□	CRITICAL - RPTR Alarm	1 time	20 minutes	Critical	AlertHold	7
□	DISREGARD - FailedNodes	1 time	1 minute	Informational	DoNotAlert	1
☑	DISREGARD - UnableToRun	1 time	1 minute	Informational	DoNotAlert	1
□	INDETERMINATE - RPTR Ala...	1 time	15 seconds	Informational	DoNotAlert	1
□	ISG Alarm trap - INDETERMI...	1 time	1 minute	Informational	DoNotAlert	1
□	ISG Alarm trap - MAJOR	1 time	1 minute	Major	DoNotAlert	1

Displaying 1 - 11 of 11 events « first prev next last »

5.1.7. Deleting a Policy

To delete a Policy:

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



POLICY CONFIGURATION Rules Filters Save

Policies

□	Name	Failover □	
□	Cisco Call Monitor	☑	4
□	LAYERX Agent Monitor	☑	3
□	Log Monitor	☑	1
□	LX1 Call Monitor v2	☑	5
□	LX1 SIP Call Errors v2	☑	6
□	Nortel Call Monitor	☑	3
□	PING Monitor	☑	2
☑	Powerwave SNMP Alarms	☑	11
□	SiLo training policy	□	2
□	Test Alarm v1	□	1
□	AJ ExperiMental	☑	3
□	ALSTOY[illegible]Austin - Alert Exa...	☑	9

Rules

□	Name	Threshold	Window	Severity	Response Procedure	
□	CLEARED - RPTR Alarm	1 time	1 minute	Informational	AlertClear	7
□	CRITICAL - RPTR Alarm	1 time	20 minutes	Critical	AlertHold	7
□	DISREGARD - FailedNodes	1 time	1 minute	Informational	DoNotAlert	1
□	DISREGARD - UnableToRun	1 time	1 minute	Informational	DoNotAlert	1
□	INDETERMINATE - RPTR Ala...	1 time	15 seconds	Informational	DoNotAlert	1
□	ISG Alarm trap - INDETERMI...	1 time	1 minute	Informational	DoNotAlert	1
□	ISG Alarm trap - MAJOR	1 time	1 minute	Major	DoNotAlert	1
□	ISG Alarm trap - MAJOR	1 time	1 minute	Major	DoNotAlert	1

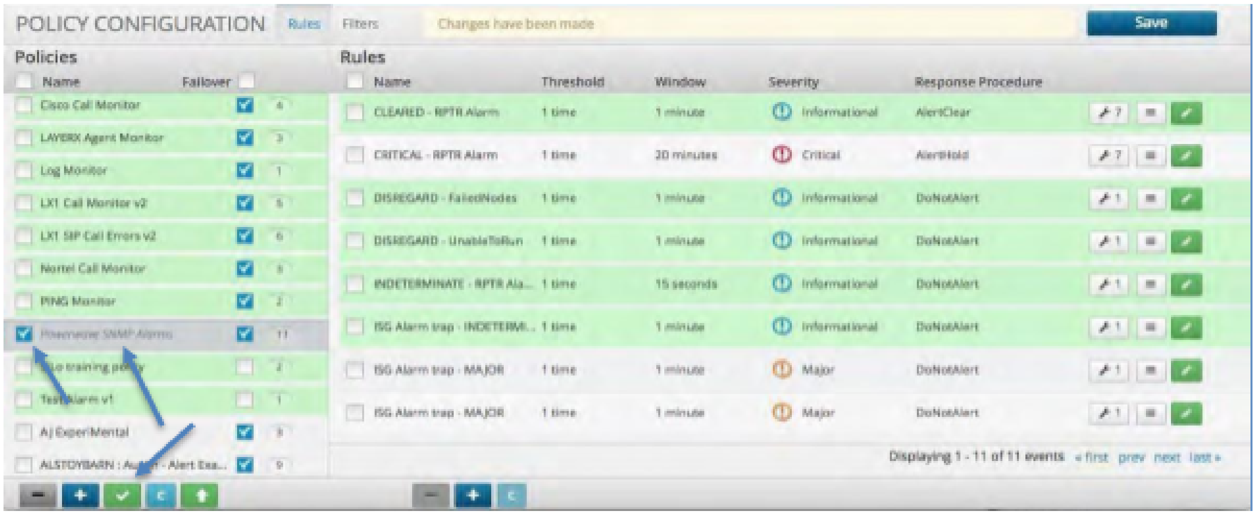
Displaying 1 - 11 of 11 events « first prev next last »

5.1.8. Disabling and Enabling a Policy

To Disable and Enable a Policy:

1. Select the Policy by clicking the check box next to the name of the policy.
2. Click the Green Check Box at the bottom of the Policies listing column.
3. The Name of the Policy will become italicized indicating that the Policy is Disabled

4. To Enable the Policy: Click the Green Check Box again. The name will turn back to a normal font indicating it is enabled.



POLICY CONFIGURATION Rules Filters Changes have been made Save

Policies

□	Name	Failover □	
□	Cisco Call Monitor	☑	4
□	LAYERX Agent Monitor	☑	3
□	Log Monitor	☑	1
□	LX1 Call Monitor v2	☑	5
□	LX1 SIP Call Errors v2	☑	6
□	Nortel Call Monitor	☑	8
□	PING Monitor	☑	2
☑	Powerwave SNMP Alarms	☑	11
□	Lo training policy	□	2
□	TestAlarm v1	□	1
□	AJ ExperiMental	☑	3
□	ALSTOYBARN : Austin - Alert Exa...	☑	9

Rules

□	Name	Threshold	Window	Severity	Response Procedure
□	CLEARED - RPTR Alarm	1 time	1 minute	Informational	AlertClear
□	CRITICAL - RPTR Alarm	1 time	20 minutes	Critical	AlertHold
□	DISREGARD - FailedNodes	1 time	1 minute	Informational	DoNotAlert
□	DISREGARD - UnableToRun	1 time	1 minute	Informational	DoNotAlert
□	INDETERMINATE - RPTR Ala...	1 time	15 seconds	Informational	DoNotAlert
□	ISG Alarm trap - INDETERMI...	1 time	1 minute	Informational	DoNotAlert
□	ISG Alarm trap - MAJOR	1 time	1 minute	Major	DoNotAlert
□	ISG Alarm trap - MAJOR	1 time	1 minute	Major	DoNotAlert

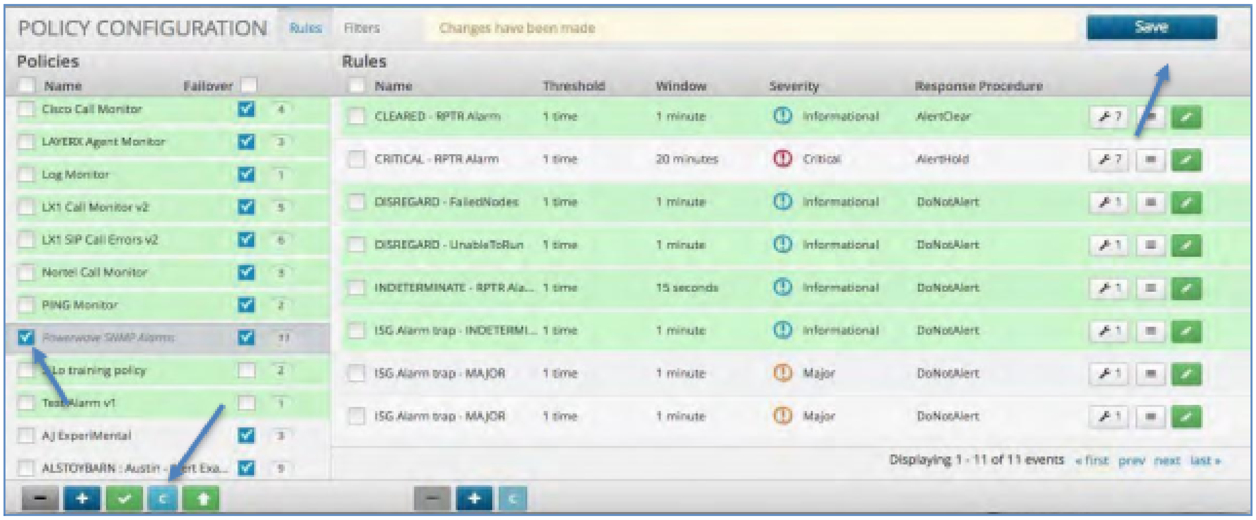
Displaying 1 - 11 of 11 events « first prev next last »

5.1.9. Cloning a Policy

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

To Clone a Policy:

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



POLICY CONFIGURATION Rules Filters Changes have been made Save

Policies

□	Name	Failover □	
□	Cisco Call Monitor	☑	4
□	LAYERX Agent Monitor	☑	3
□	Log Monitor	☑	1
□	LX1 Call Monitor v2	☑	5
□	LX1 SIP Call Errors v2	☑	6
□	Nortel Call Monitor	☑	8
□	PING Monitor	☑	2
☑	Powerwave SNMP Alarms	☑	11
□	Lo training policy	□	2
□	TestAlarm v1	□	1
□	AJ ExperiMental	☑	3
□	ALSTOYBARN : Austin - Alert Exa...	☑	9

Rules

□	Name	Threshold	Window	Severity	Response Procedure
□	CLEARED - RPTR Alarm	1 time	1 minute	Informational	AlertClear
□	CRITICAL - RPTR Alarm	1 time	20 minutes	Critical	AlertHold
□	DISREGARD - FailedNodes	1 time	1 minute	Informational	DoNotAlert
□	DISREGARD - UnableToRun	1 time	1 minute	Informational	DoNotAlert
□	INDETERMINATE - RPTR Ala...	1 time	15 seconds	Informational	DoNotAlert
□	ISG Alarm trap - INDETERMI...	1 time	1 minute	Informational	DoNotAlert
□	ISG Alarm trap - MAJOR	1 time	1 minute	Major	DoNotAlert
□	ISG Alarm trap - MAJOR	1 time	1 minute	Major	DoNotAlert

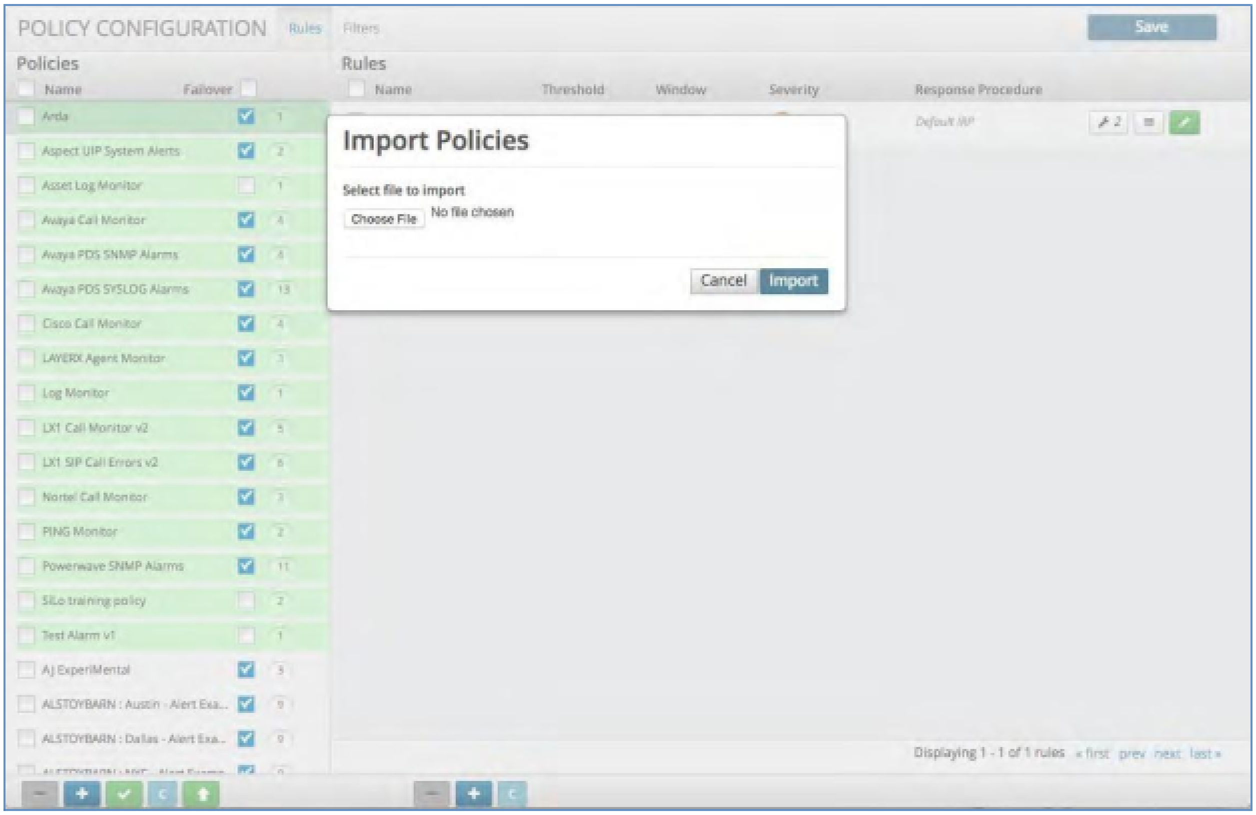
Displaying 1 - 11 of 11 events « first prev next last »

We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

5.1.10. Import a Policy

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

1. Click the green Up Arrow button at the bottom of the policy panel.
2. A pop-up box will appear asking you choose your file.
3. Click the “Choose File” button and select the exported file that you have saved to your computer.
4. Click the “Import” button.
5. Check that the policy has been imported and click Save.



□ Name	Failover □	
□ Arda	☑	1
□ Aspect UIP System Alerts	☑	2
□ Asset Log Monitor	□	1
□ Avaya Call Monitor	☑	4
□ Avaya PDS SNMP Alarms	☑	4
□ Avaya PDS SYSLOG Alarms	☑	13
□ Cisco Call Monitor	☑	4
□ LAYERX Agent Monitor	☑	3
□ Log Monitor	☑	1
□ LX1 Call Monitor v2	☑	5
□ LX1 SIP Call Errors v2	☑	6
□ Nortel Call Monitor	☑	3
□ PING Monitor	☑	2
□ Powerwave SNMP Alarms	☑	11
□ SiLo training policy	□	2
□ Test Alarm v1	□	1
□ AJ ExperiMental	☑	3
□ ALSTOYBARN : Austin - Alert Exa...	☑	9
□ ALSTOYBARN : Dallas - Alert Exa...	☑	9

Import Policies

Select file to import

Choose File No file chosen

Cancel Import

5.2. Asset Configuration

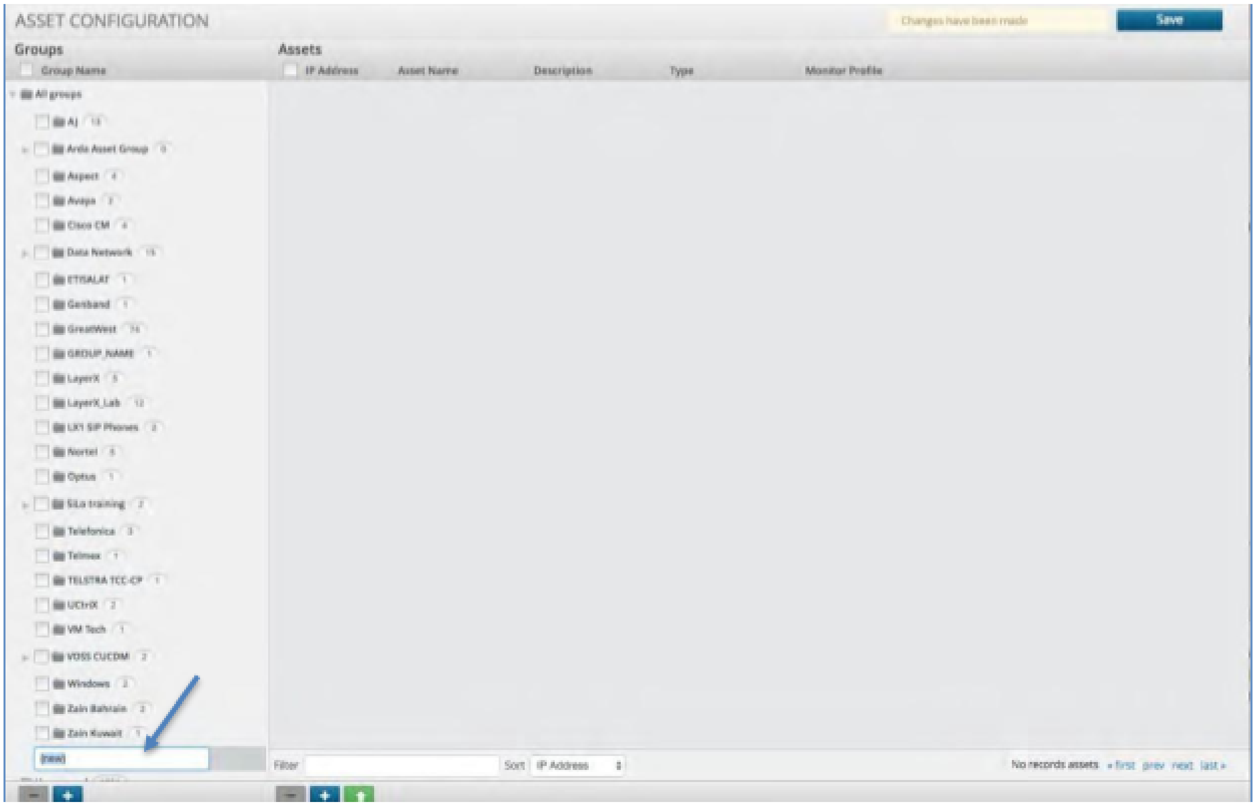
The Asset Configuration panel allows you to create Assets and Asset Groupings. Assets can be any devices that are either sending data or from which data is being retrieved. Each Asset can be assigned to a specific customer to create a multi-tenant environment.

5.2.1. Creating an Asset Group

To create a new Asset Group:

1. Click the Asset icon from the Menu bar.

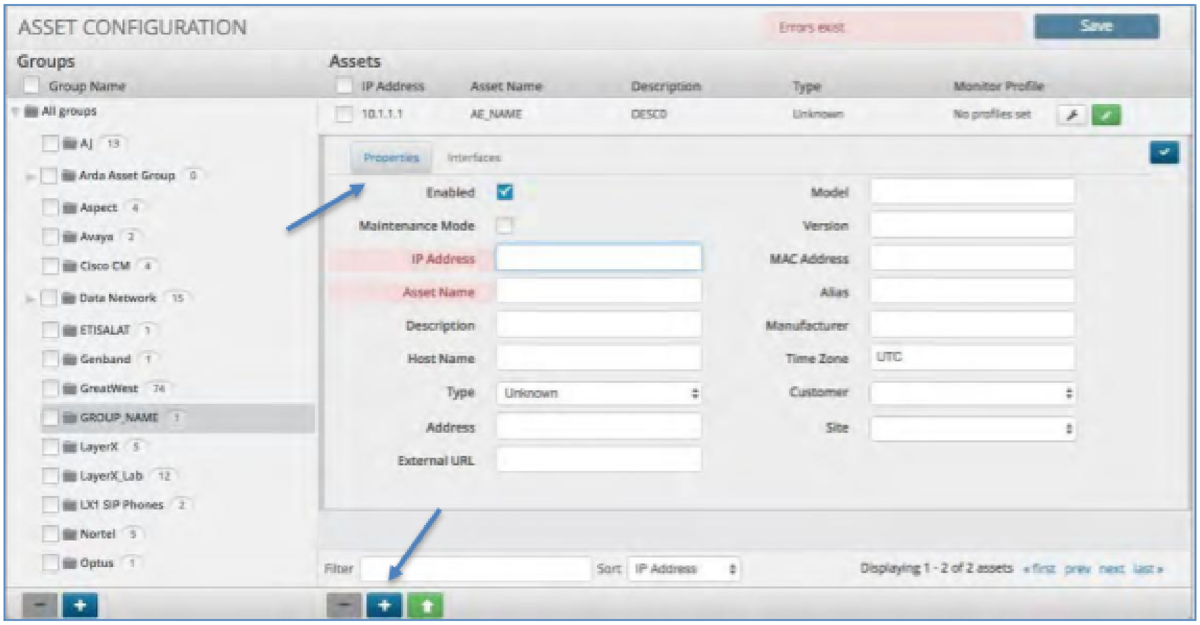
2. Click the Plus icon in the bottom left corner of the Asset Groups panel.
3. Enter the Group name and press Enter.
4. Click the Save icon in the upper right.



5.2.2. Adding an Asset to an Existing Group

To add a new Asset to a Group:

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



IP Address	Asset Name	Description	Type	Monitor Profile
10.1.1.1	AE_NAME	DESCD	Unknown	No profiles set

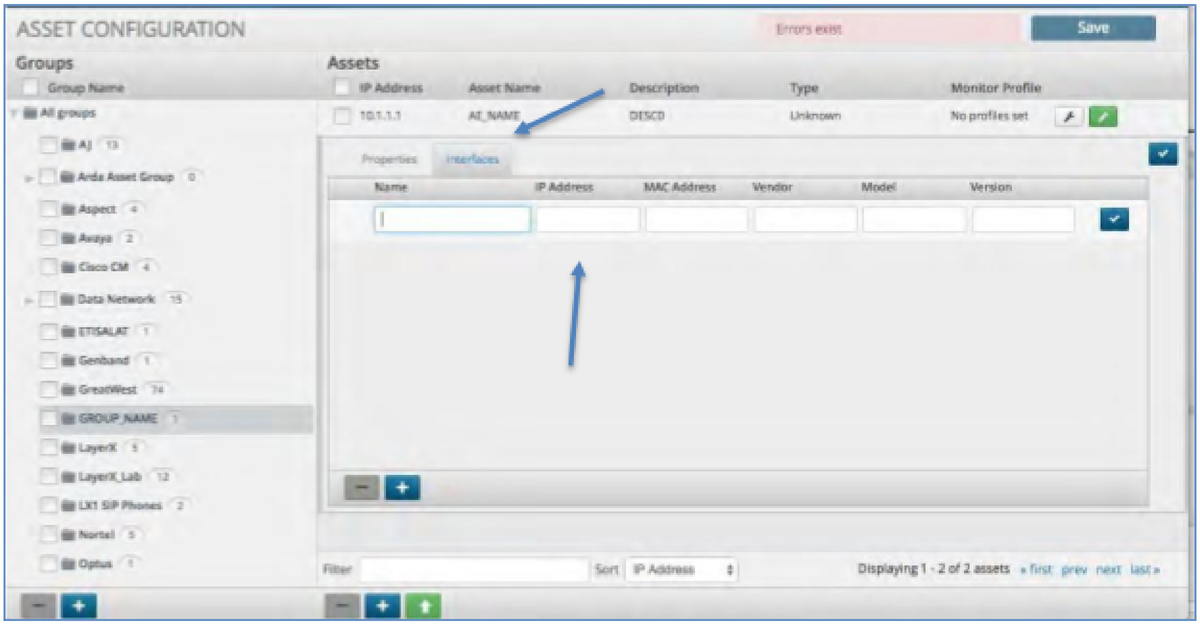
Enabled ☑

Maintenance Mode □

Type: Unknown

Time Zone: UTC

Sort: IP Address



IP Address	Asset Name	Description	Type	Monitor Profile
10.1.1.1	AE_NAME	DESCD	Unknown	No profiles set

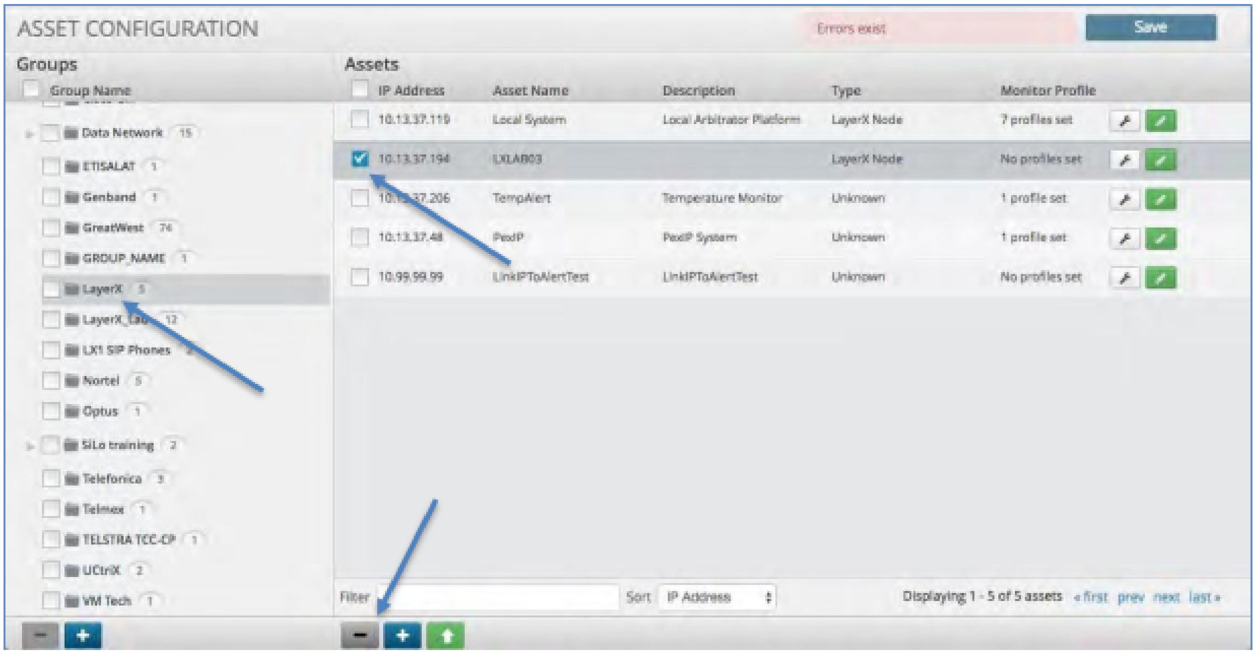
Sort: IP Address

5.2.3. Deleting an Asset

To delete an Asset:

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

We appreciate and value your comments. Email: doc-feedback@voss-solutions.com



□ Group Name	
□ Data Network	15
□ ETISALAT	1
□ Genband	1
□ GreatWest	74
□ GROUP_NAME	1
□ LayerX	5
□ LayerX_Lab	12
□ LX1 SIP Phones	2
□ Nortel	5
□ Optus	1
□ SiLo training	2
□ Telefonica	3
□ Telmex	1
□ TELSTRA TCC-CP	1
□ UCtriX	2
□ VM Tech	1

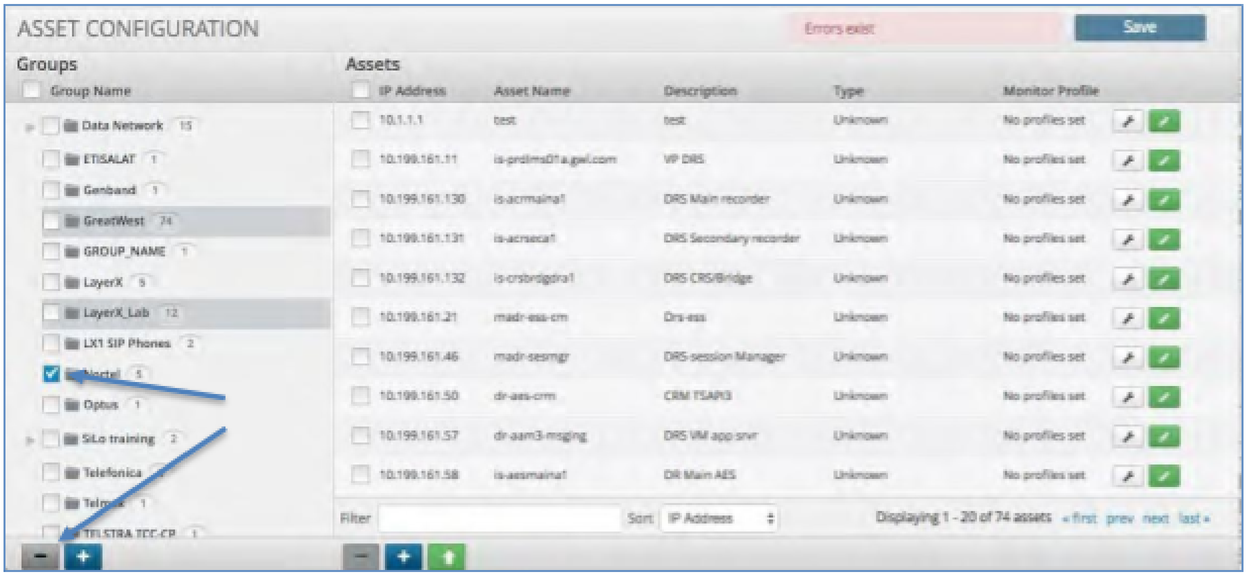
□	IP Address	Asset Name	Description	Type	Monitor Profile
□	10.13.37.119	Local System	Local Arbitrator Platform	LayerX Node	7 profiles set
☑	10.13.37.194	LXLAB03		LayerX Node	No profiles set
□	10.13.37.206	TempAlert	Temperature Monitor	Unknown	1 profile set
□	10.13.37.48	PexiP	PexiP System	Unknown	1 profile set
□	10.99.99.99	LinkIPToAlertTest	LinkIPToAlertTest	Unknown	No profiles set

Filter | Sort: IP Address | Displaying 1 - 5 of 5 assets « first prev next last »

5.2.4. Deleting an Asset Group

To delete an Asset Group:

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



□ Group Name	
□ Data Network	15
□ ETISALAT	1
□ Genband	1
□ GreatWest	74
□ GROUP_NAME	1
□ LayerX	5
□ LayerX_Lab	12
□ LX1 SIP Phones	2
☑ Nortel	5
□ Optus	1
□ SiLo training	2
□ Telefonica	
□ Telmex	1
□ TELSTRA TCC-CP	1

□	IP Address	Asset Name	Description	Type	Monitor Profile
□	10.1.1.1	test	test	Unknown	No profiles set
□	10.199.161.11	is-prdims01a.gwl.com	VP DRS	Unknown	No profiles set
□	10.199.161.130	is-acrmaina1	DRS Main recorder	Unknown	No profiles set
□	10.199.161.131	is-acrseca1	DRS Secondary recorder	Unknown	No profiles set
□	10.199.161.132	is-crsbrdgdra1	DRS CRS/Bridge	Unknown	No profiles set
□	10.199.161.21	madr-ess-cm	Drs-ess	Unknown	No profiles set
□	10.199.161.46	madr-sesmgr	DRS-session Manager	Unknown	No profiles set
□	10.199.161.50	dr-aes-crm	CRM TSAPI3	Unknown	No profiles set
□	10.199.161.57	dr-aam3-msging	DRS VM app srvr	Unknown	No profiles set
□	10.199.161.58	is-aesmaina1	DR Main AES	Unknown	No profiles set

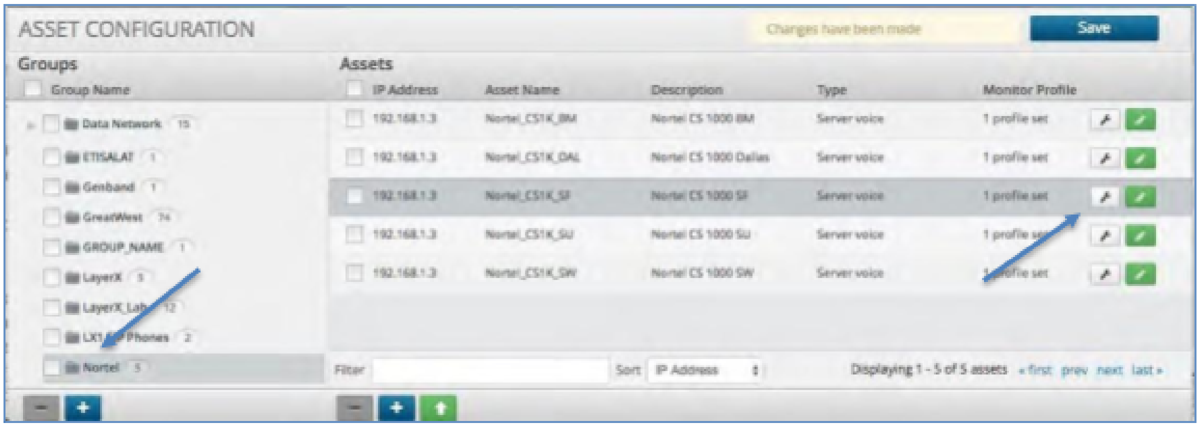
Filter | Sort: IP Address | Displaying 1 - 20 of 74 assets « first prev next last »

5.2.5. Assigning a Probe to an Asset

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

To assign a Probe to an Asset:

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



ASSET CONFIGURATION

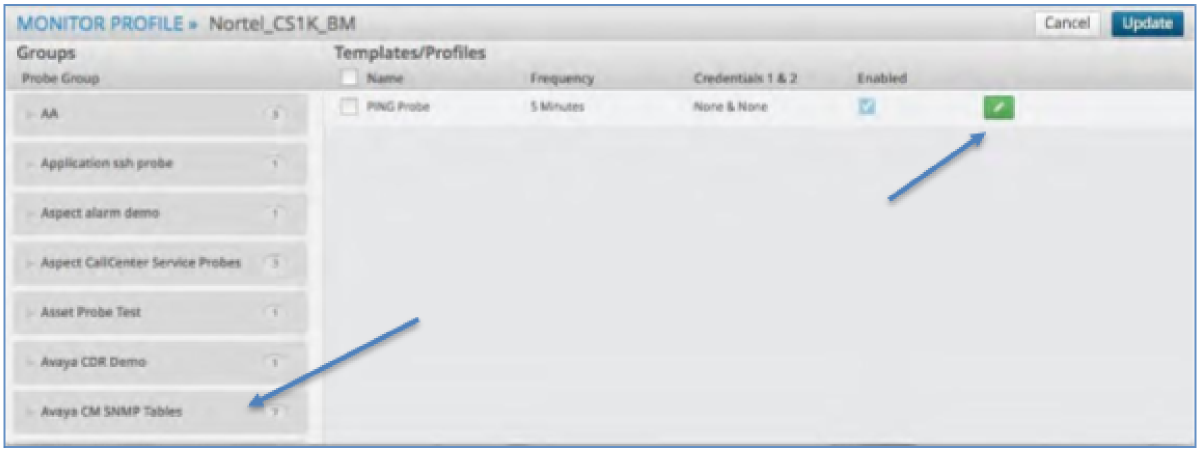
Groups

□ Group Name
□ Data Network 15
□ ETISALAT 1
□ Genband 1
□ GreatWest 74
□ GROUP_NAME 1
□ LayerX 5
□ LayerX_Lab 12
□ LX1 [illegible] Phones 2
□ Nortel 5

Assets

□	IP Address	Asset Name	Description	Type	Monitor Profile
□	192.168.1.3	Nortel_CS1K_BM	Nortel CS 1000 BM	Server voice	1 profile set
□	192.168.1.3	Nortel_CS1K_DAL	Nortel CS 1000 Dallas	Server voice	1 profile set
□	192.168.1.3	Nortel_CS1K_SF	Nortel CS 1000 SF	Server voice	1 profile set
□	192.168.1.3	Nortel_CS1K_SU	Nortel CS 1000 SU	Server voice	1 profile set
□	192.168.1.3	Nortel_CS1K_SW	Nortel CS 1000 SW	Server voice	1 profile set

Filter Sort IP Address Displaying 1 - 5 of 5 assets



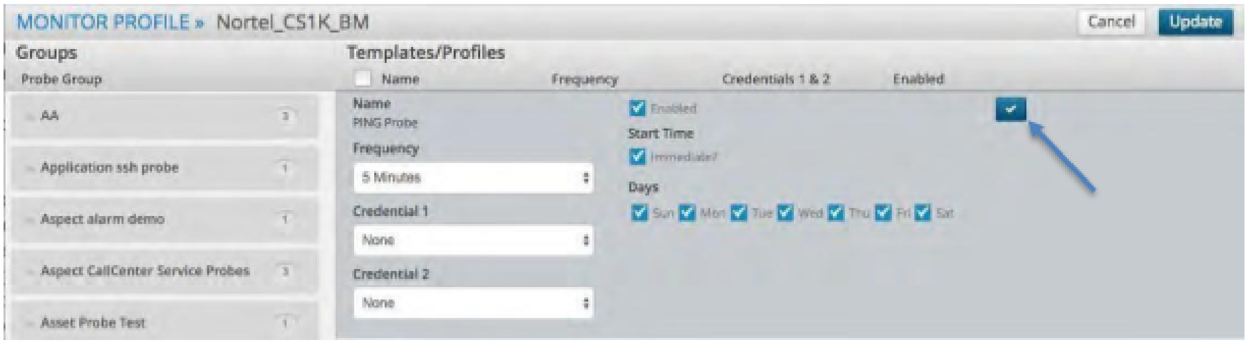
MONITOR PROFILE » Nortel_CS1K_BM

Groups

Probe Group	
AA	3
Application ssh probe	1
Aspect alarm demo	1
Aspect CallCenter Service Probes	3
Asset Probe Test	1
Avaya CDR Demo	1
Avaya CM SNMP Tables	7

Templates/Profiles

□ Name	Frequency	Credentials 1 & 2	Enabled
□ PING Probe	5 Minutes	None & None	☑



MONITOR PROFILE » Nortel_CS1K_BM

Groups

Probe Group	
AA	3
Application ssh probe	1
Aspect alarm demo	1
Aspect CallCenter Service Probes	3
Asset Probe Test	1

Templates/Profiles

□ Name | Frequency | Credentials 1 & 2 | Enabled

Name: PING Probe

Frequency: 5 Minutes

Credential 1: None

Credential 2: None

☑ Enabled

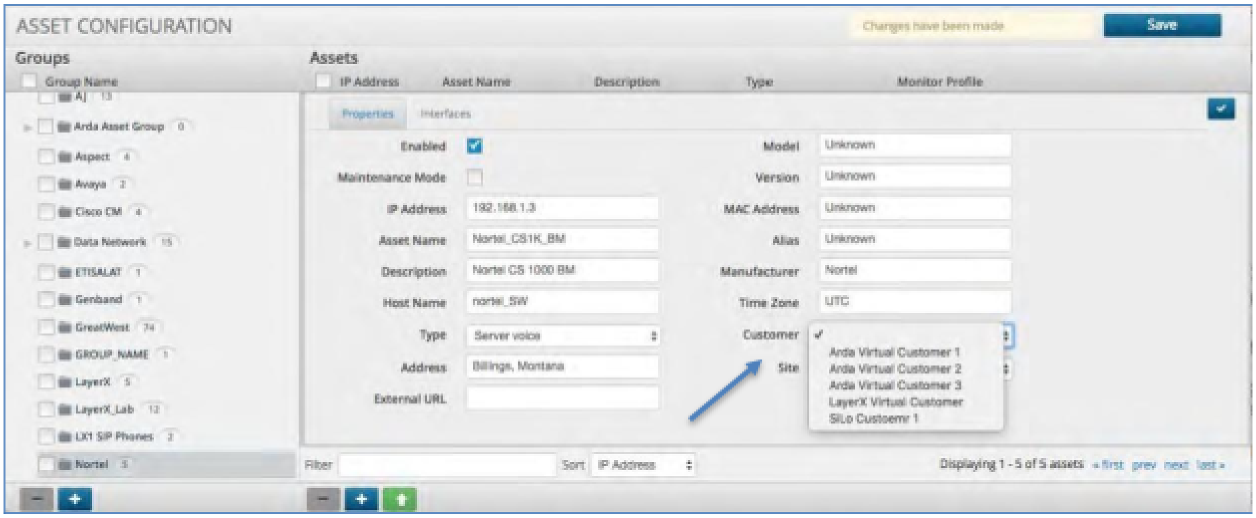
Start Time: ☑ Immediate?

Days: ☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat

5.2.6. Assigning a Customer to an Asset

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

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



ASSET CONFIGURATION

Changes have been made

Groups

Group Name	
AJ	13
Arda Asset Group	0
Aspect	4
Avaya	2
Cisco CM	4
Data Network	15
ETISALAT	1
Genband	1
GreatWest	74
GROUP_NAME	1
LayerX	5
LayerX_Lab	12
LX1 SIP Phones	2
Nortel	5

Assets

□ IP Address | Asset Name | Description | Type | Monitor Profile

Properties | Interfaces

Enabled	☑	Model	Unknown
Maintenance Mode	□	Version	Unknown
IP Address	192.168.1.3	MAC Address	Unknown
Asset Name	Nortel_CS1K_BM	Alias	Unknown
Description	Nortel CS 1000 BM	Manufacturer	Nortel
Host Name	nortel_SW	Time Zone	UTC
Type	Server voice	Customer	✓
Address	Billings, Montana	Site	
External URL			

Arda Virtual Customer 1
Arda Virtual Customer 2
Arda Virtual Customer 3
LayerX Virtual Customer
SILo Custoemr 1

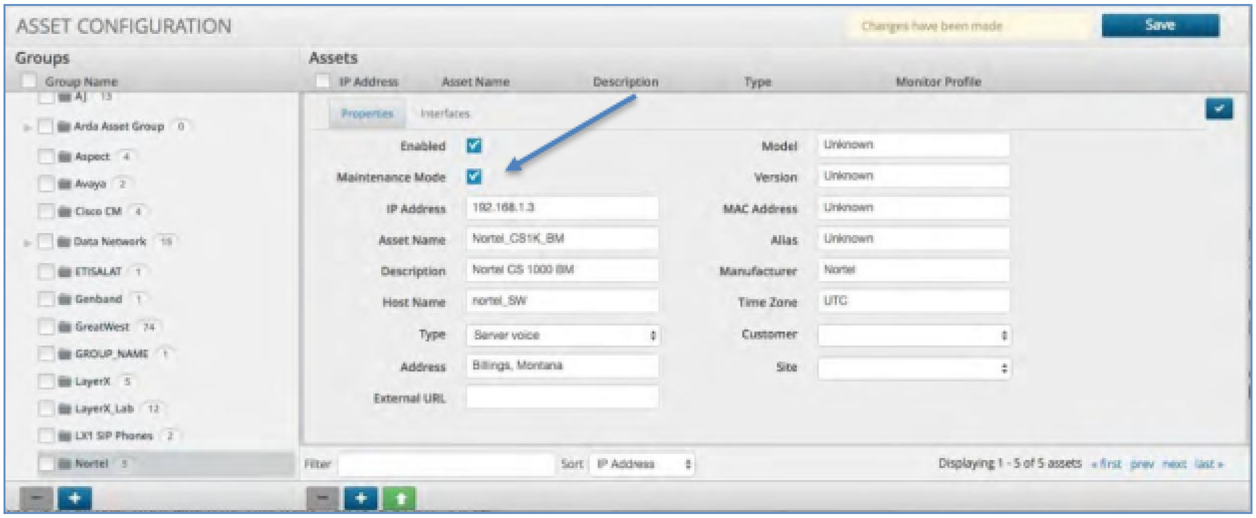
Filter | Sort: IP Address

Displaying 1 - 5 of 5 assets « first prev next last »

5.2.7. Placing an Asset in Maintenance Mode

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

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



Enabled ☑

Maintenance Mode ☑

IP Address: 192.168.1.3

Asset Name: Nortel_CS1K_BM

Description: Nortel CS 1000 BM

Host Name: nortel_SW

Type: Server voice

Address: Billings, Montana

External URL:

Model: Unknown

Version: Unknown

MAC Address: Unknown

Alias: Unknown

Manufacturer: Nortel

Time Zone: UTC

Customer:

Site:

5.3. Probe Configuration

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

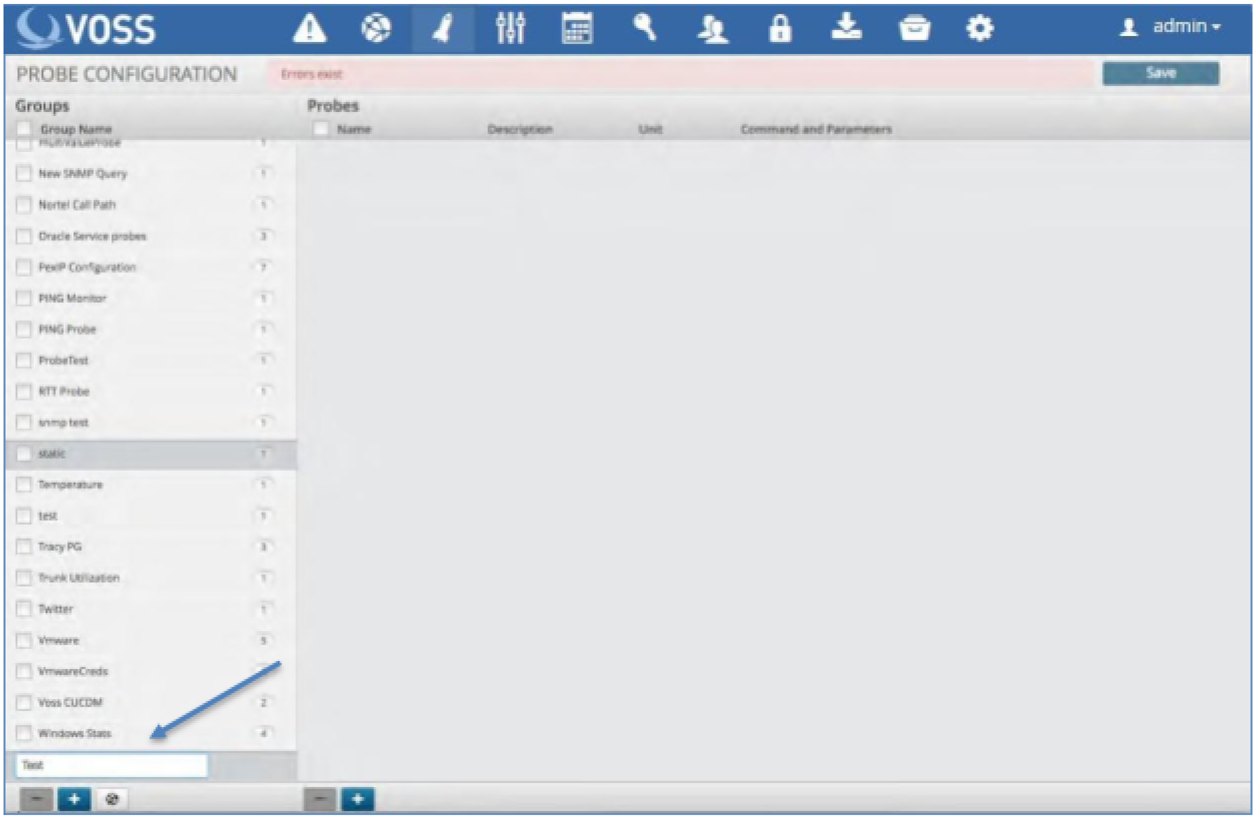
For PRI and SIP Trunk probes for Cisco Voice Gateways, reference:

Arbitrator Cisco PRI and SIP Probe Configuration

5.3.1. Creating a Probe Group

To create a new Probe Group:

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



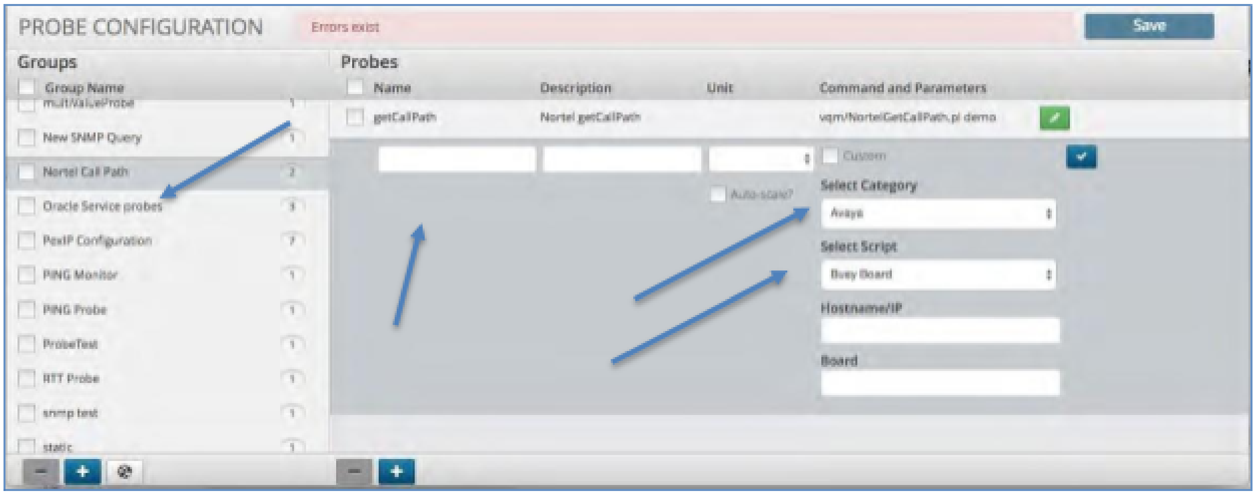
Group Name	
MultiValueProbe	1
New SNMP Query	1
Nortel Call Path	1
Oracle Service probes	3
PexIP Configuration	7
PING Monitor	1
PING Probe	1
ProbeTest	1
RTT Probe	1
snmp test	1
static	1
Temperature	1
test	1
Tracy PG	3
Trunk Utilization	1
Twitter	1
Vmware	5
VmwareCreds	
Voss CUCDM	2
Windows Stats	4
Test	

Name	Description	Unit	Command and Parameters

5.3.2. Creating a Probe

To create a new Probe:

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



Group Name	
multiValueProbe	1
New SNMP Query	1
Nortel Call Path	2
Oracle Service probes	3
PexIP Configuration	7
PING Monitor	1
PING Probe	1
ProbeTest	1
RTT Probe	1
snmp test	1
static	1

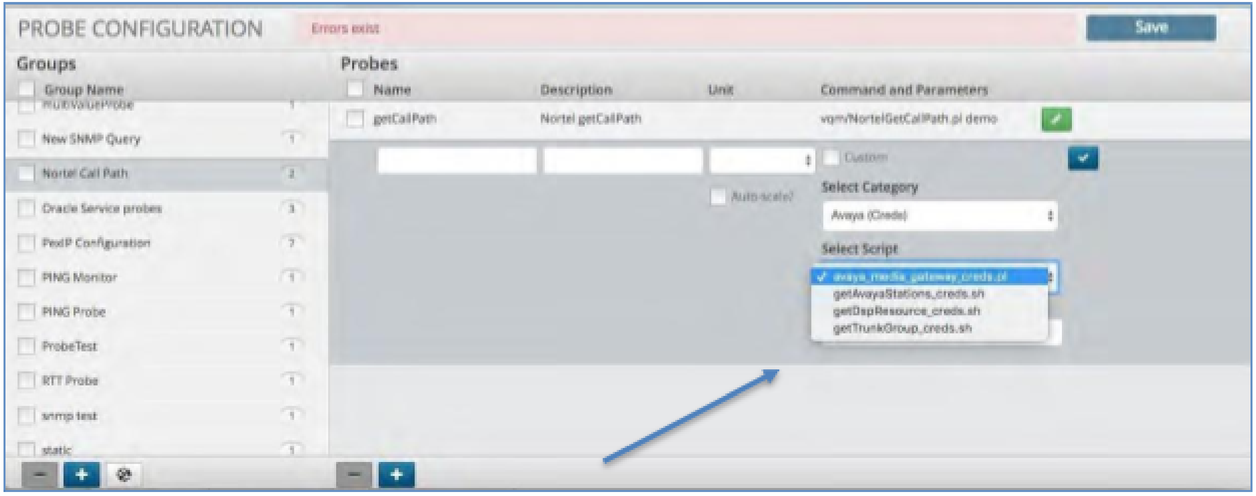
Name	Description	Unit	Command and Parameters
getCallPath	Nortel getCallPath		vqm/NortelGetCallPath.pl demo

Select Category: Avaya

Select Script: Busy Board

Hostname/IP

Board



Group Name	
multiValueProbe	1
New SNMP Query	1
Nortel Call Path	2
Oracle Service probes	3
PexIP Configuration	7
PING Monitor	1
PING Probe	1
ProbeTest	1
RTT Probe	1
snmp test	1
static	1

Name	Description	Unit	Command and Parameters
getCallPath	Nortel getCallPath		vqm/NortelGetCallPath.pl demo

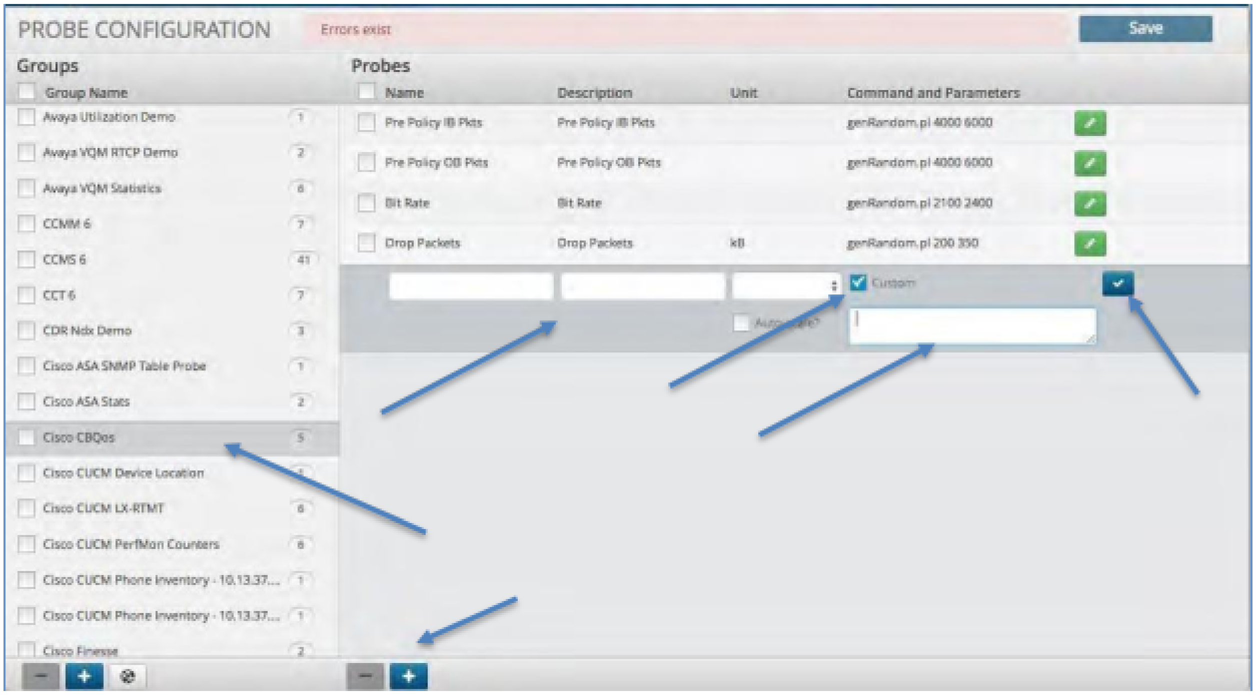
Select Category: Avaya (Creds)

Select Script:
- ✓ avaya_media_gateway_creds.pl
- getAvayaStations_creds.sh
- getDspResource_creds.sh
- getTrunkGroup_creds.sh

5.3.3. Creating a Custom Probe

To create a new Probe:

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



Groups

☐ Group Name	
☐ Avaya Utilization Demo	1
☐ Avaya VQM RTCP Demo	2
☐ Avaya VQM Statistics	6
☐ CCMM 6	7
☐ CCMS 6	41
☐ CCT 6	7
☐ CDR Ndx Demo	3
☐ Cisco ASA SNMP Table Probe	1
☐ Cisco ASA Stats	2
☐ Cisco CBQos	5
☐ Cisco CUCM Device Location	1
☐ Cisco CUCM LX-RTMT	6
☐ Cisco CUCM PerfMon Counters	8
☐ Cisco CUCM Phone Inventory - 10.13.37...	1
☐ Cisco CUCM Phone Inventory - 10.13.37...	1
☐ Cisco Finesse	2

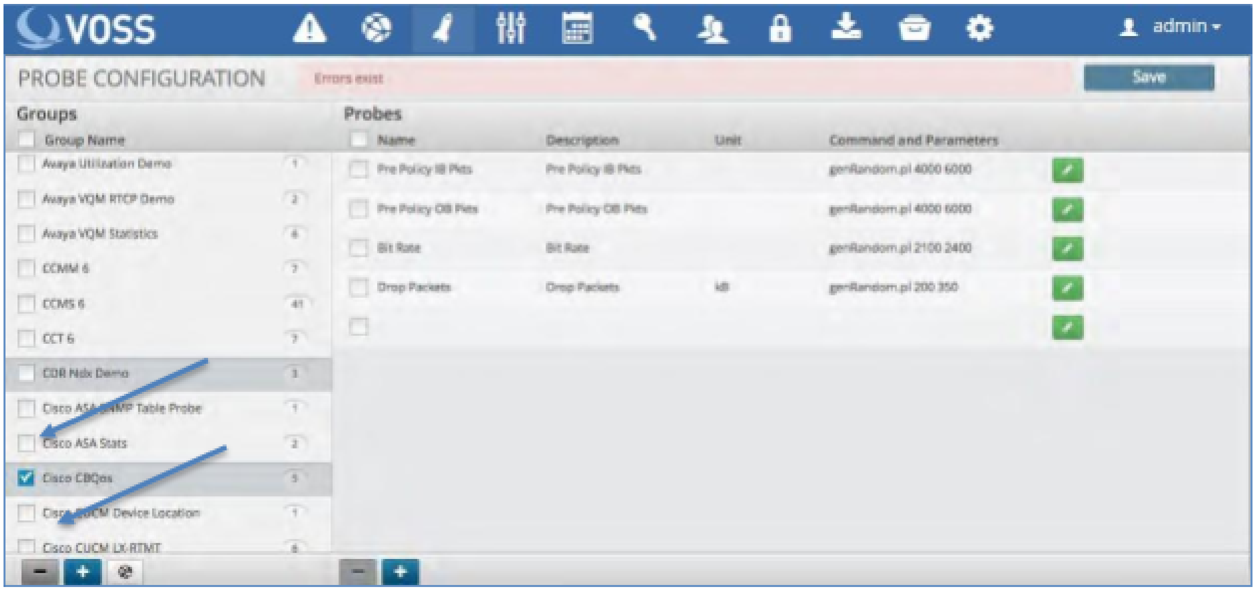
Probes

☐ Name	Description	Unit	Command and Parameters
☐ Pre Policy IB Pkts	Pre Policy IB Pkts		genRandom.pl 4000 6000
☐ Pre Policy OB Pkts	Pre Policy OB Pkts		genRandom.pl 4000 6000
☐ Bit Rate	Bit Rate		genRandom.pl 2100 2400
☐ Drop Packets	Drop Packets	kB	genRandom.pl 200 350

5.3.4. Deleting a Probe Group

To delete a Probe Group:

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



Groups

☐ Group Name	
☐ Avaya Utilization Demo	1
☐ Avaya VQM RTCP Demo	2
☐ Avaya VQM Statistics	6
☐ CCMM 6	7
☐ CCMS 6	41
☐ CCT 6	7
☐ CDR Ndx Demo	3
☐ Cisco ASA SNMP Table Probe	1
☐ Cisco ASA Stats	2
☑ Cisco CBQos	5
☐ Cisco CUCM Device Location	1
☐ Cisco CUCM LX-RTMT	6

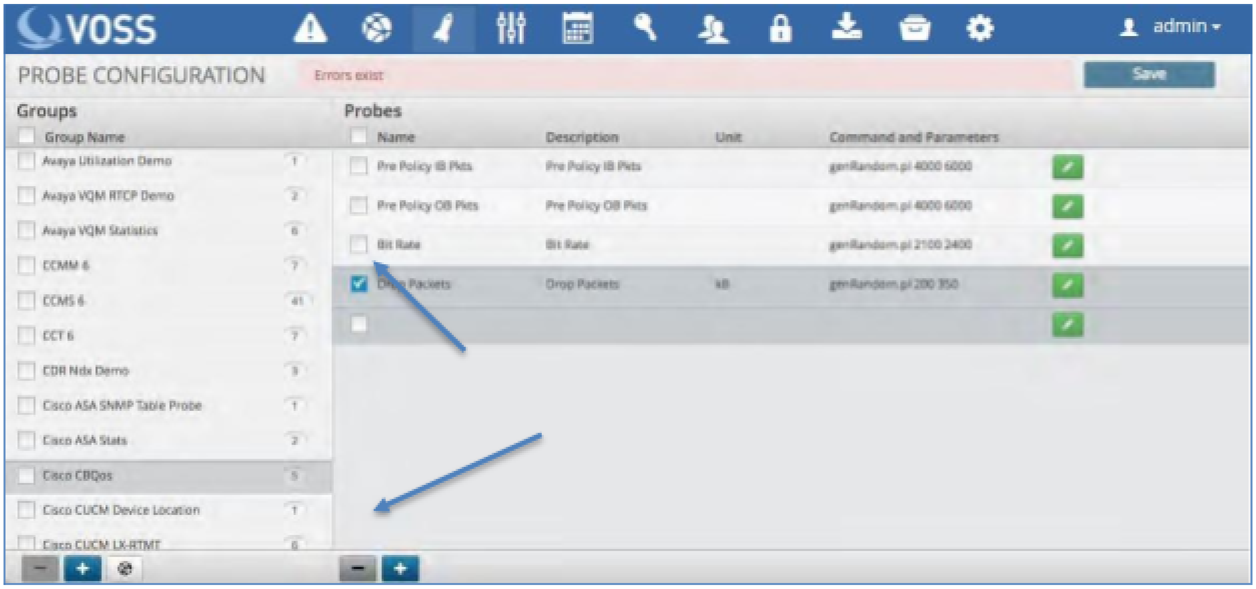
Probes

☐ Name	Description	Unit	Command and Parameters
☐ Pre Policy IB Pkts	Pre Policy IB Pkts		genRandom.pl 4000 6000
☐ Pre Policy OB Pkts	Pre Policy OB Pkts		genRandom.pl 4000 6000
☐ Bit Rate	Bit Rate		genRandom.pl 2100 2400
☐ Drop Packets	Drop Packets	kB	genRandom.pl 200 350
☐			

5.3.5. Deleting a Probe

To delete a Probe:

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



PROBE CONFIGURATION

Errors exist

Groups

□	Group Name	
□	Avaya Utilization Demo	1
□	Avaya VQM RTCP Demo	2
□	Avaya VQM Statistics	6
□	CCMM 6	7
□	CCMS 6	41
□	CCT 6	7
□	CDR Ndx Demo	9
□	Cisco ASA SNMP Table Probe	1
□	Cisco ASA Stats	2
□	Cisco CBQos	5
□	Cisco CUCM Device Location	1
□	Cisco CUCM LX-RTMT	6

Probes

□	Name	Description	Unit	Command and Parameters	
□	Pre Policy IB Pkts	Pre Policy IB Pkts		genRandom.pl 4000 6000	✎
□	Pre Policy OB Pkts	Pre Policy OB Pkts		genRandom.pl 4000 6000	✎
□	Bit Rate	Bit Rate		genRandom.pl 2100 2400	✎
☑	Drop Packets	Drop Packets	kB	genRandom.pl 200 350	✎
□					✎

5.4. Controls

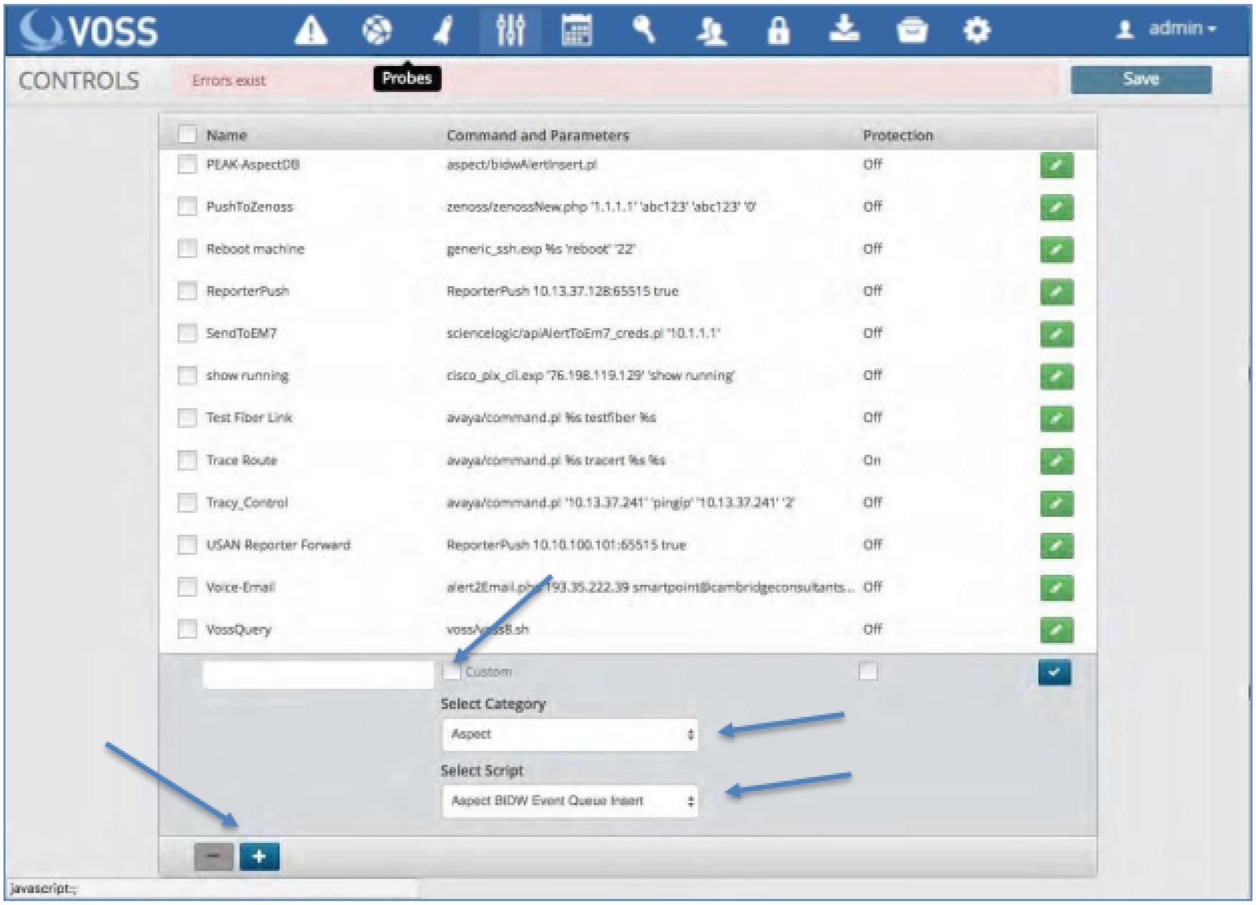
The Controls Configuration panel allows you to define a script or routine that can be executed by a response procedure or attached as a probe. These controls can be passed variables extracted from a correlation rule. The resulting return of the scripts execution can be mapped to the database, used as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

5.4.1. Creating a Control

To create a new Control:

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

8. Click Save icon.



□ Name	Command and Parameters	Protection	
□ PEAK-AspectDB	aspect/bidwAlertInsert.pl	Off	
□ PushToZenoss	zenoss/zenossNew.php '1.1.1.1' 'abc123' 'abc123' '0'	Off	
□ Reboot machine	generic_ssh.exp %s 'reboot' '22'	Off	
□ ReporterPush	ReporterPush 10.13.37.128:65515 true	Off	
□ SendToEM7	sciencelogic/apiAlertToEm7_creds.pl '10.1.1.1'	Off	
□ show running	cisco_pix_cli.exp '76.198.119.129' 'show running'	Off	
□ Test Fiber Link	avaya/command.pl %s testfiber %s	Off	
□ Trace Route	avaya/command.pl %s tracert %s %s	On	
□ Tracy_Control	avaya/command.pl '10.13.37.241' 'pingip' '10.13.37.241' '2'	Off	
□ USAN Reporter Forward	ReporterPush 10.10.100.101:65515 true	Off	
□ Voice-Email	alert2Email.php 193.35.222.39 smartpoint@cambridgeconsultants...	Off	
□ VossQuery	voss/voss8.sh	Off	
	□ Custom	□	✓

Select Category

Aspect

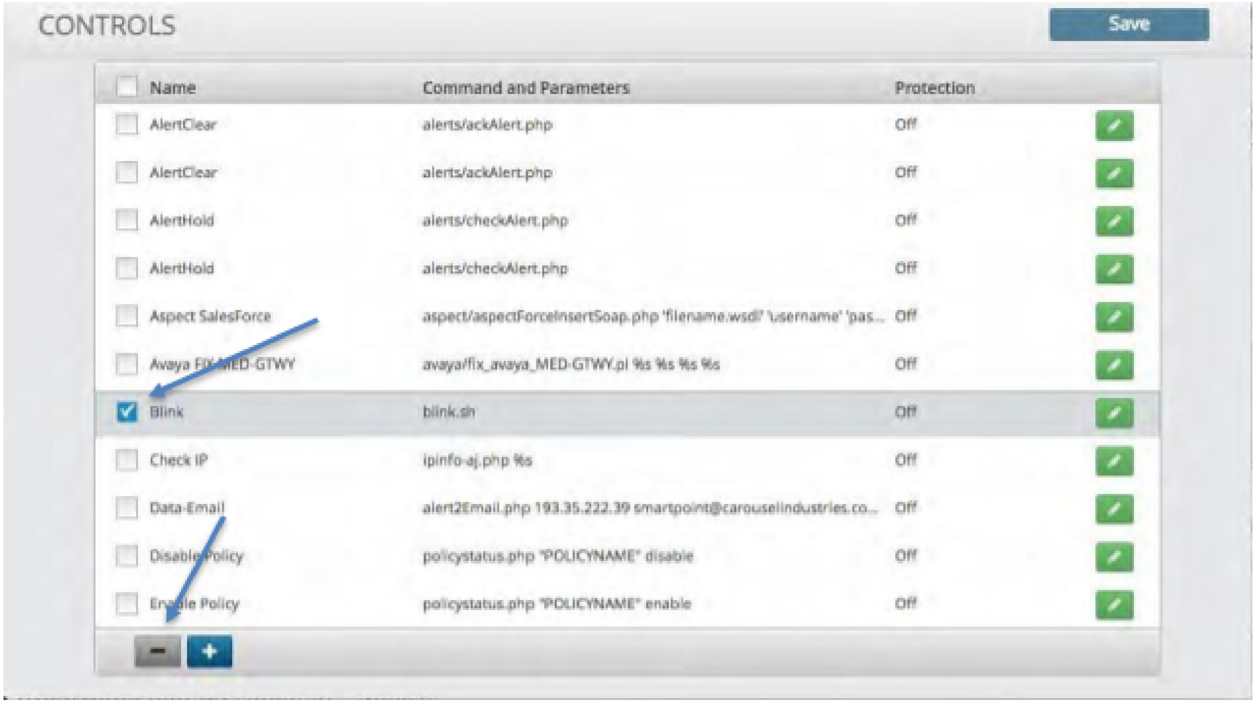
Select Script

Aspect BIDW Event Queue Insert

5.4.2. Deleting a Control

To delete a Control:

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



□	Name	Command and Parameters	Protection
□	AlertClear	alerts/ackAlert.php	Off
□	AlertClear	alerts/ackAlert.php	Off
□	AlertHold	alerts/checkAlert.php	Off
□	AlertHold	alerts/checkAlert.php	Off
□	Aspect SalesForce	aspect/aspectForceInsertSoap.php 'filename.wsdl' 'username' 'pas...	Off
□	Avaya FIX MED-GTWY	avaya/fix_avaya_MED-GTWY.pl %s %s %s %s	Off
☑	Blink	blink.sh	Off
□	Check IP	ipinfo-aj.php %s	Off
□	Data-Email	alert2Email.php 193.35.222.39 smartpoint@carouselindustries.co...	Off
□	Disable Policy	policystatus.php "POLICYNAME" disable	Off
□	Enable Policy	policystatus.php "POLICYNAME" enable	Off

5.5. Response Procedure Configuration

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

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

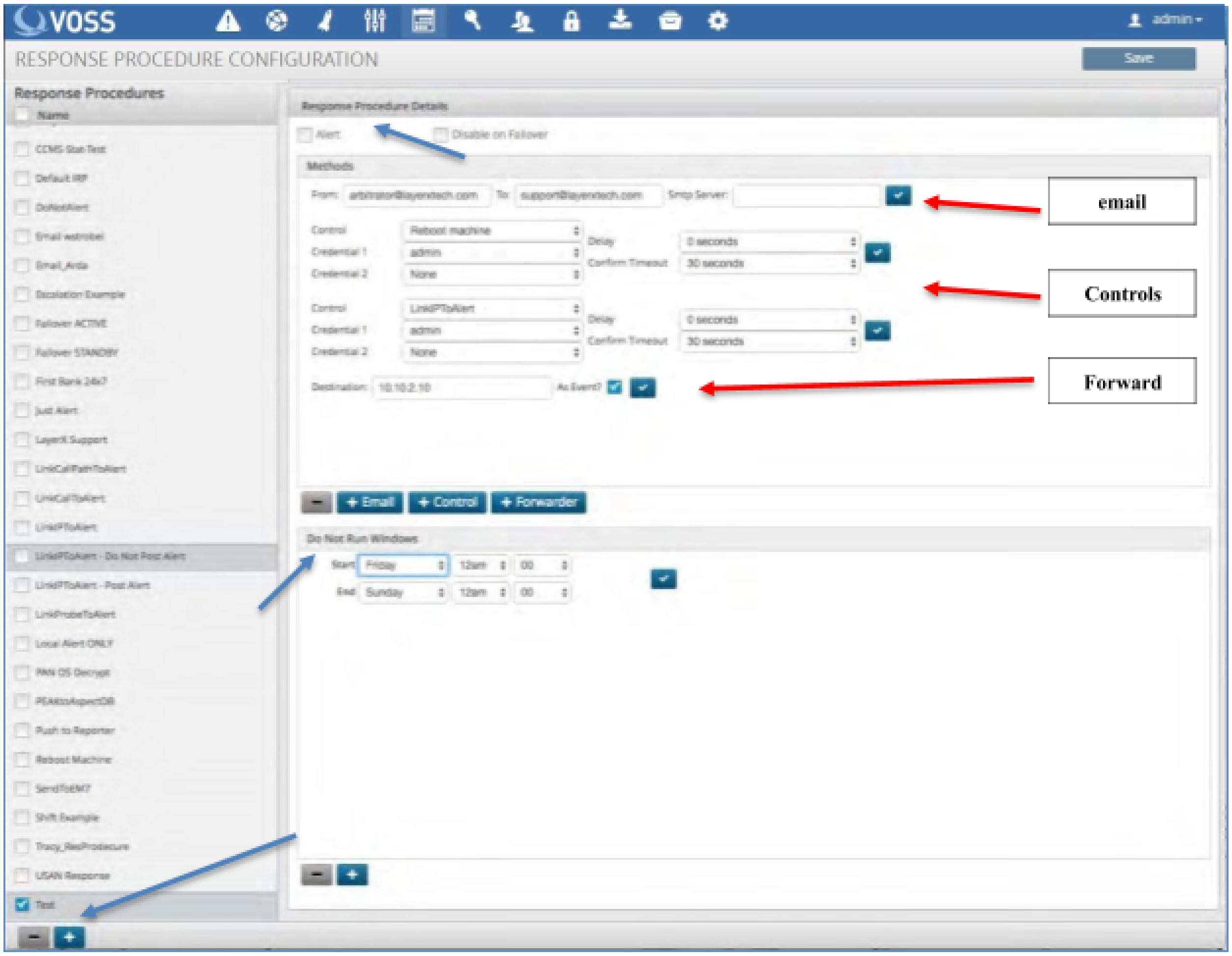
5.5.1. Creating a Response Procedure

To create a response procedure:

1. Click the “Calendar” icon at the top of the Configuration panel.
2. Click the plus icon in the bottom left of the Response Procedure name panel. A box will open up where you can fill in the name of your response procedure.

We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

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.



□ CCMS Stat Test
□ Default IRP
□ DoNotAlert
□ Email wstrobel
□ Email_Arda
□ Escalation Example
□ Failover ACTIVE
□ Failover STANDBY
□ First Bank 24x7
□ Just Alert
□ LayerX Support
□ LinkCallPathToAlert
□ LinkCallToAlert
□ LinkIPToAlert
□ LinkIPToAlert - Do Not Post Alert
□ LinkIPToAlert - Post Alert
□ LinkProbeToAlert
□ Local Alert ONLY
□ PAN OS Decrypt
□ PEAKtoAspectDB
□ Push to Reporter
□ Reboot Machine
□ SendToEM7
□ Shift Example
□ Tracy_ResProdecure
□ USAN Response
☑ Test

□ Alert □ Disable on Failover

From: arbitrator@layerxtech.com To: support@layerxtech.com Smtp Server:

Control: Reboot machine; Credential 1: admin; Credential 2: None; Delay: 0 seconds; Confirm Timeout: 30 seconds

Control: LinkIPToAlert; Credential 1: admin; Credential 2: None; Delay: 0 seconds; Confirm Timeout: 30 seconds

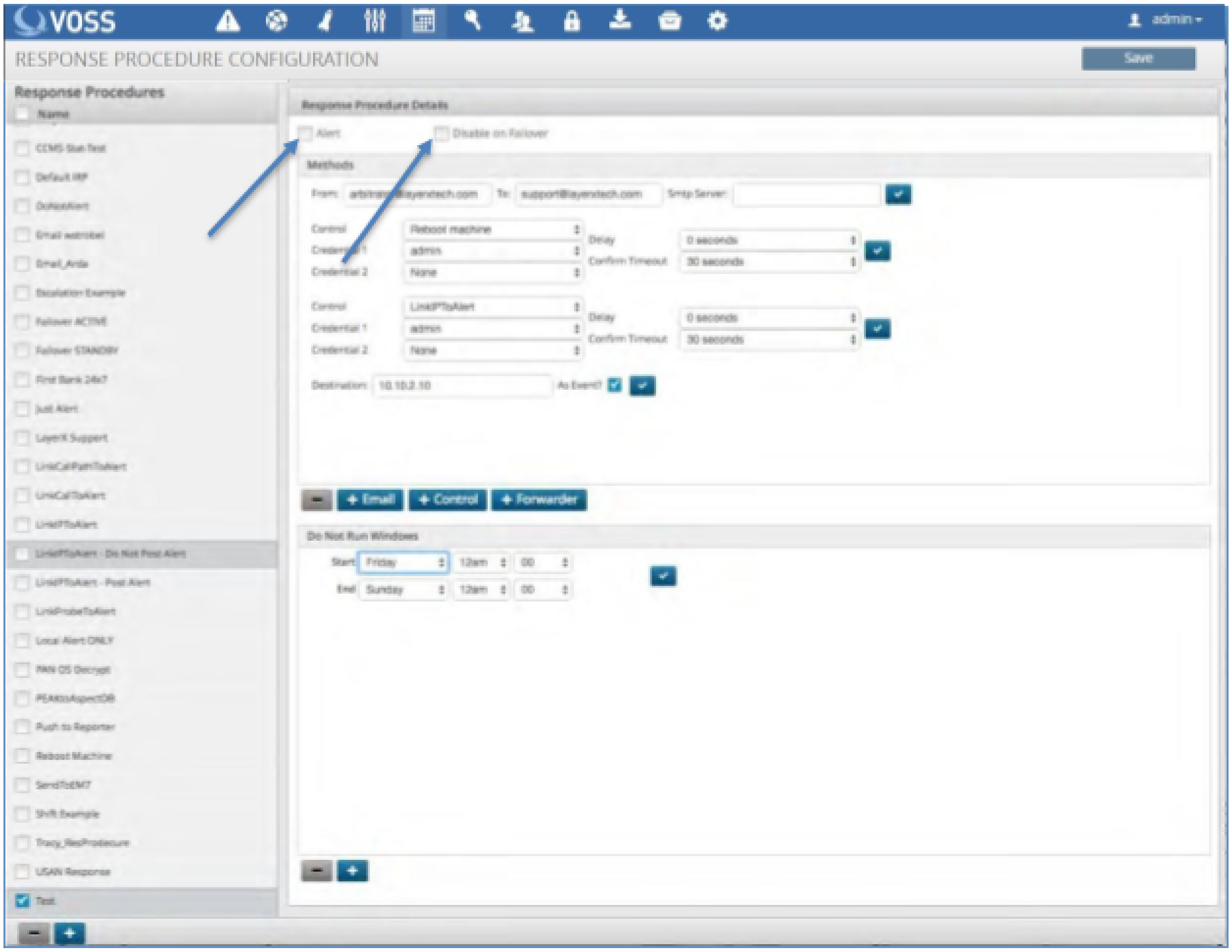
Destination: 10.10.2.10 As Event? ☑

Start: Friday 12am 00
End: Sunday 12am 00

5.5.2. Assigning an Alert to a Response Procedure

To assign the Alert function to a response procedure:

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



□ CCMS Stat Test
□ Default IRP
□ DoNotAlert
□ Email webrobel
□ Email_Arda
□ Escalation Example
□ Failover ACTIVE
□ Failover STANDBY
□ First Bank 24x7
□ Just Alert
□ LayerX Support
□ LinkCallPathToAlert
□ LinkCallToAlert
□ LinkIPToAlert
□ LinkIPToAlert - Do Not Post Alert
□ LinkIPToAlert - Post Alert
□ LinkProbeToAlert
□ Local Alert ONLY
□ PAN OS Decrypt
□ PEAKtoAspectDB
□ Push to Reporter
□ Reboot Machine
□ SendToEM7
□ Shift Example
□ Tracy_ResProcedure
□ USAN Response
☑ Test

Response Procedure Details

□ Alert □ Disable on Failover

Methods

From: arbitrator@layerxtech.com To: support@layerxtech.com Smtp Server:

Control: Reboot machine
Credential 1: admin
Credential 2: None
Delay: 0 seconds
Confirm Timeout: 30 seconds

Control: LinkIPToAlert
Credential 1: admin
Credential 2: None
Delay: 0 seconds
Confirm Timeout: 30 seconds

Destination: 10.10.2.10 As Event? ☑

Do Not Run Windows

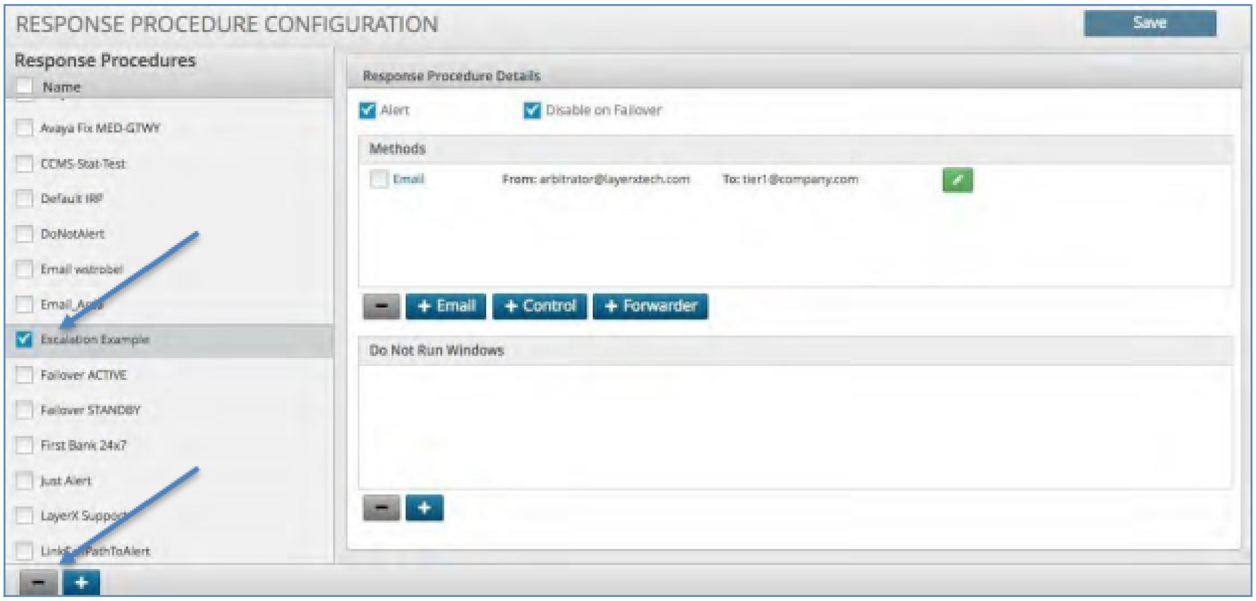
Start: Friday 12am 00
End: Sunday 12am 00

5.5.3. Deleting a Response Procedure

To delete a Response Procedure:

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

We appreciate and value your comments. Email: doc-feedback@voss-solutions.com



RESPONSE PROCEDURE CONFIGURATION

Response Procedures

□ Name

□ Avaya Fix MED-GTWY

□ CCMS-Stat-Test

□ Default IRP

□ DoNotAlert

□ Email wstrobel

□ Email_A

☑ Escalation Example

□ Failover ACTIVE

□ Failover STANDBY

□ First Bank 24x7

□ Just Alert

□ LayerX Suppo

□ Link PathToAlert

Response Procedure Details

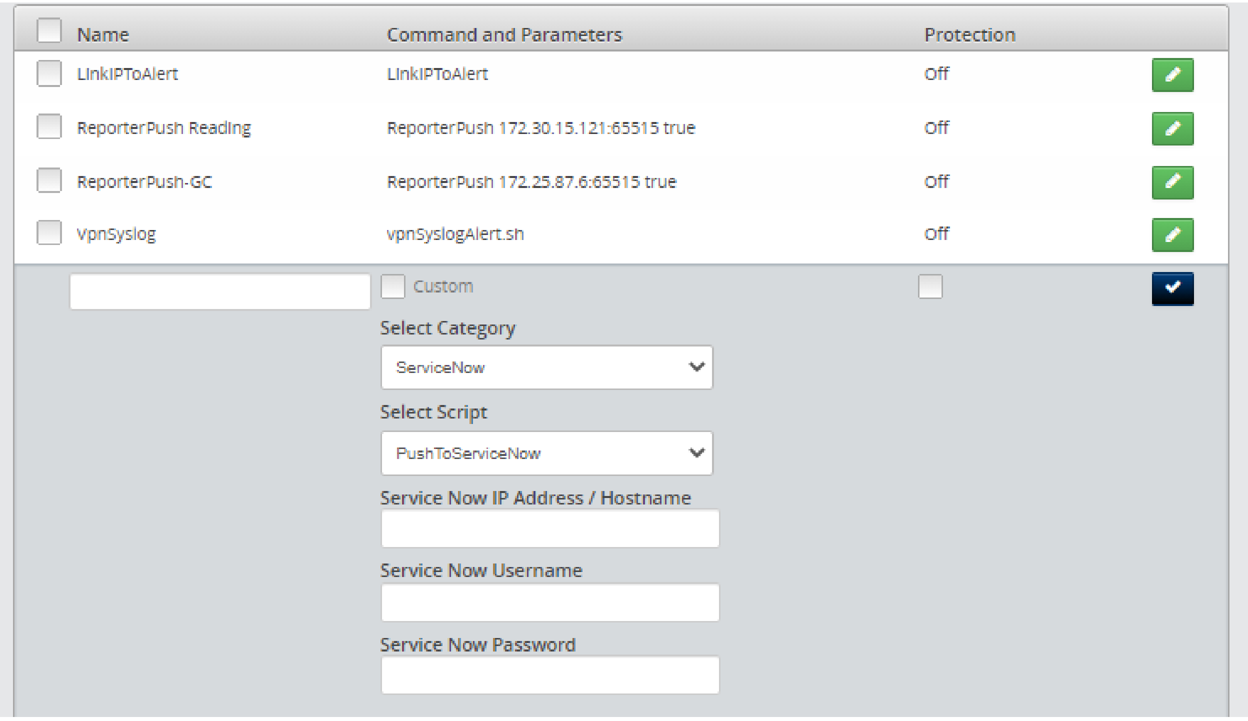
☑ Alert ☑ Disable on Failover

Methods

□ Email From: arbitrator@layerxtech.com To: tier1@company.com

Do Not Run Windows

5.6. How to Enable ServiceNow Intergration



□	Name	Command and Parameters	Protection	
□	LinkIPToAlert	LinkIPToAlert	Off	✎
□	ReporterPush Reading	ReporterPush 172.30.15.121:65515 true	Off	✎
□	ReporterPush-GC	ReporterPush 172.25.87.6:65515 true	Off	✎
□	VpnSyslog	vpnSyslogAlert.sh	Off	✎

□ Custom

Select Category: ServiceNow

Select Script: PushToServiceNow

Service Now IP Address / Hostname

Service Now Username

Service Now Password

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

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

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

5.7. ServiceNow One Way Incident Integration

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

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

5.7.1. ServiceNow Requirements

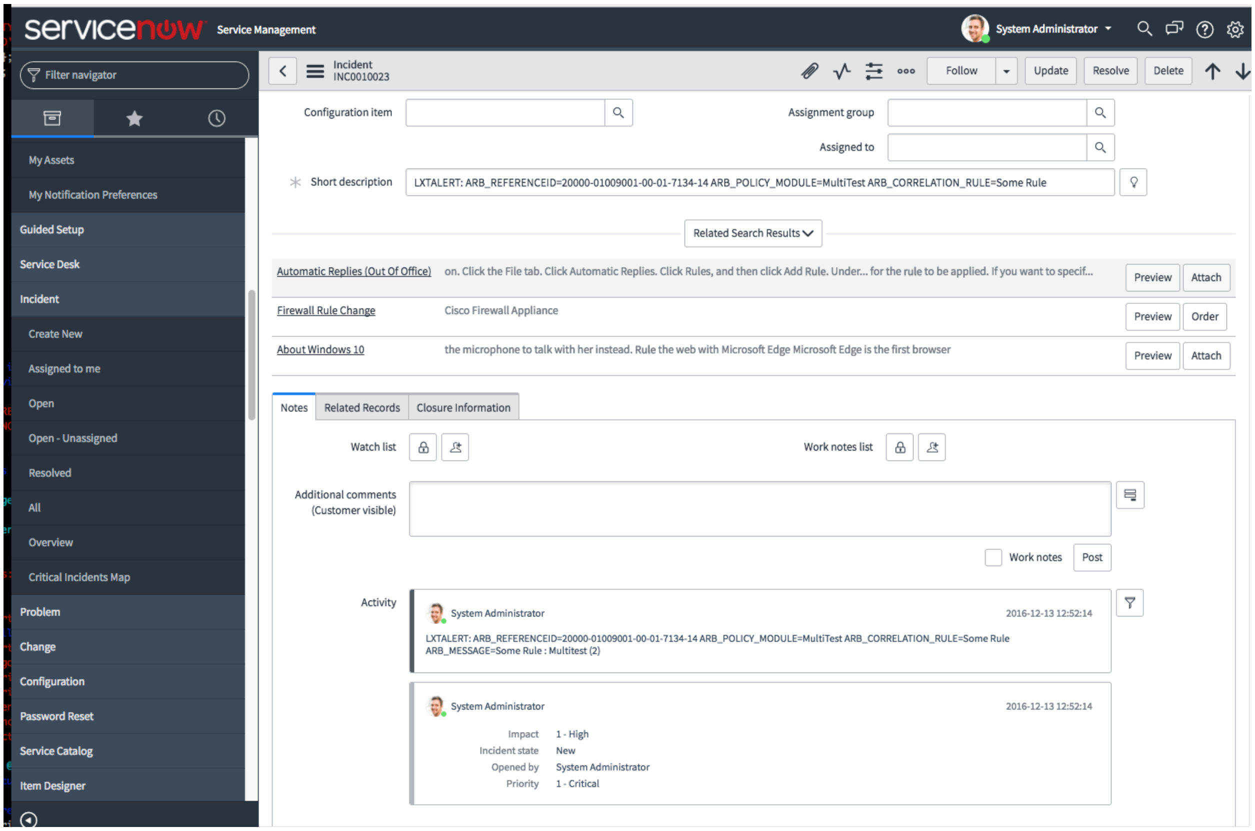
- ServiceNow URL
- ServiceNow User with SOAP API rights to insert Incidents
- ServiceNow Password

5.7.2. Arbitrator Correlation Configuration

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

- PASSWORD

5.7.3. Screenshots From ServiceNow



Incident
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

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...
Firewall Rule Change	Cisco Firewall Appliance
About Windows 10	the microphone to talk with her instead. Rule the web with Microsoft Edge Microsoft Edge is the first browser

Watch list

Work notes list

Additional comments (Customer visible)

□ Work notes

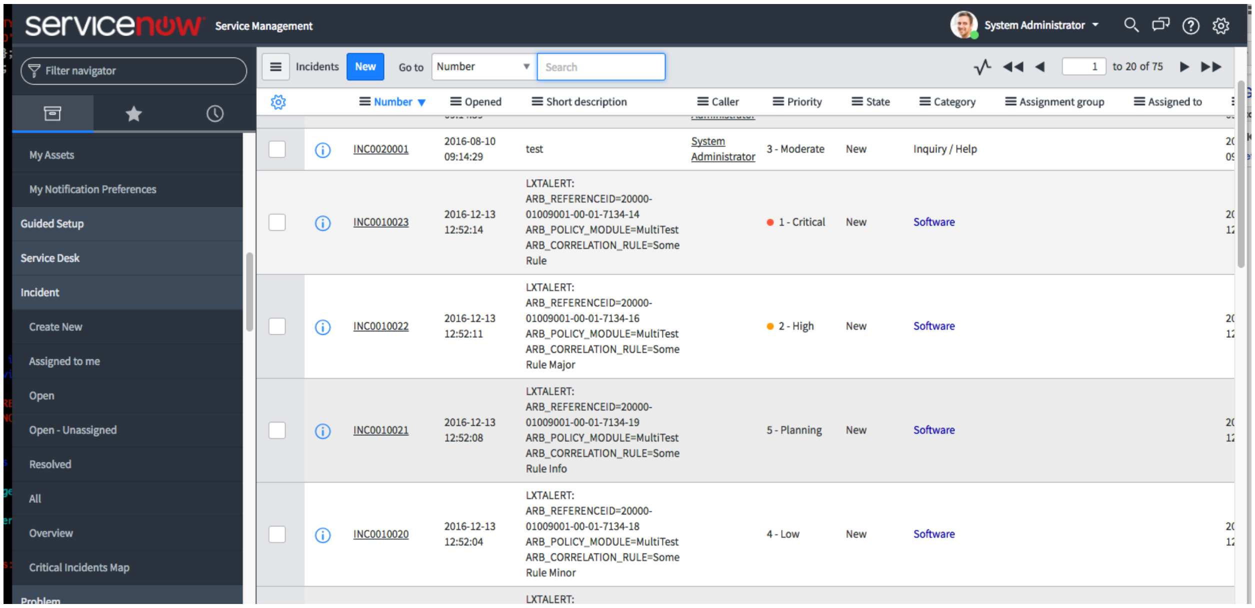
Activity

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		
□	ⓘ	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		
□	ⓘ	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		
□	ⓘ	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		
□	ⓘ	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		
				LXTALERT:						

We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

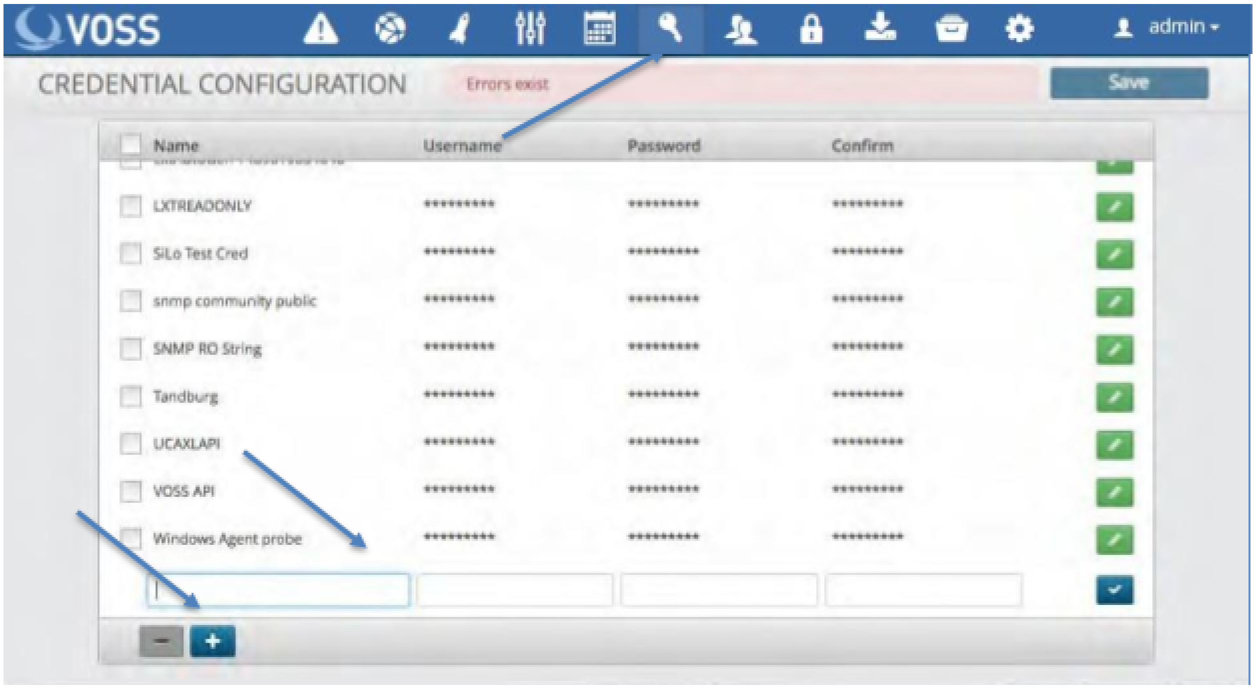
5.8. Credential Configuration

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

5.8.1. Creating a Credential

To create a Credential:

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



CREDENTIAL CONFIGURATION

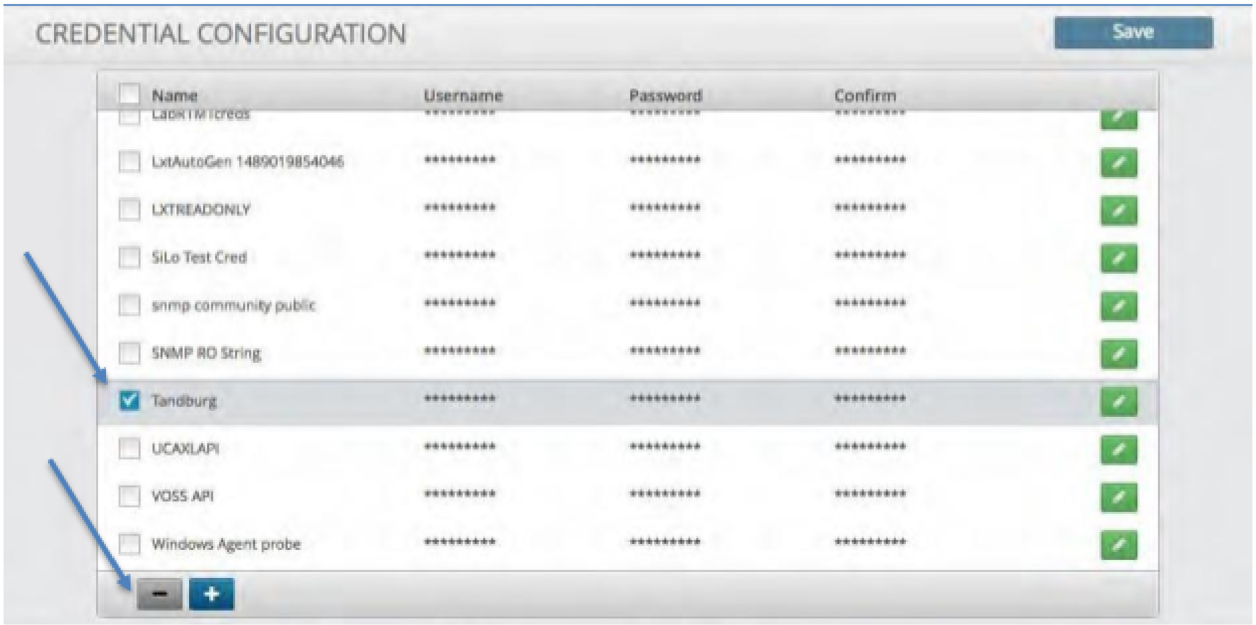
Errors exist

□	Name	Username	Password	Confirm
□	[illegible]			
□	LXTREADONLY	**********	**********	**********
□	SiLo Test Cred	**********	**********	**********
□	snmp community public	**********	**********	**********
□	SNMP RO String	**********	**********	**********
□	Tandburg	**********	**********	**********
□	UCAXLAPI	**********	**********	**********
□	VOSS API	**********	**********	**********
□	Windows Agent probe	**********	**********	**********

5.8.2. Deleting a Credential

To delete a Credential:

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



□ Name	Username	Password	Confirm
□ LabRTMcreds	**********	**********	**********
□ LxtAutoGen 1489019854046	**********	**********	**********
□ LXTREADONLY	**********	**********	**********
□ SiLo Test Cred	**********	**********	**********
□ snmp community public	**********	**********	**********
□ SNMP RO String	**********	**********	**********
☑ Tandburg	**********	**********	**********
□ UCAXLAPI	**********	**********	**********
□ VOSS API	**********	**********	**********
□ Windows Agent probe	**********	**********	**********

5.9. Customer Configuration

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

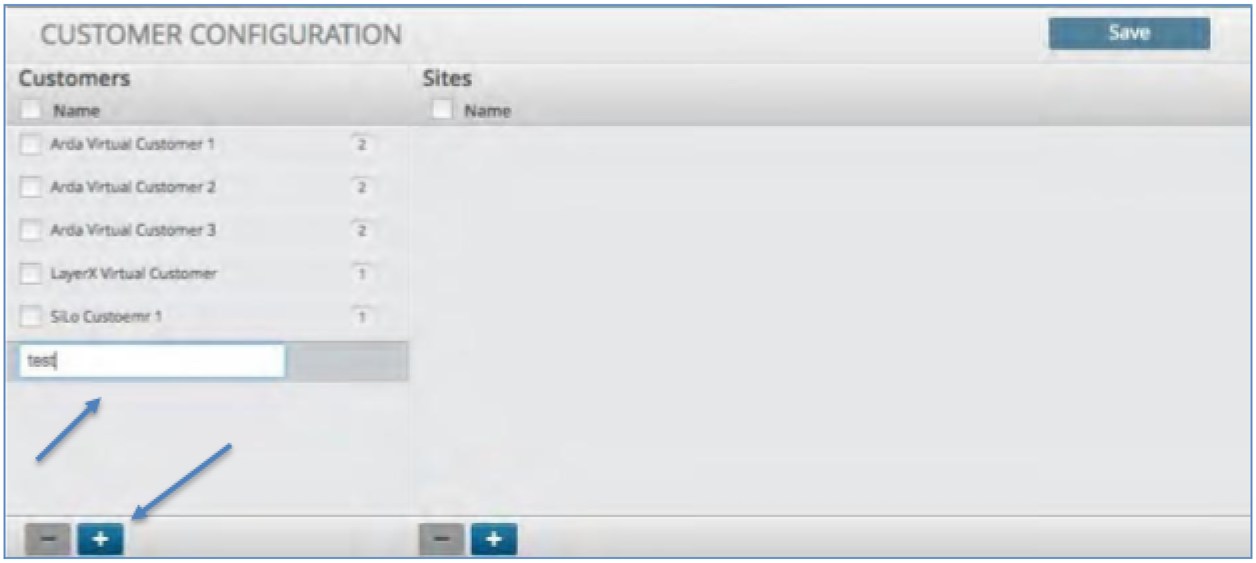
(See: Asset Configuration, Access Control Configuration).

5.9.1. Creating a Customer

To create a Customer:

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

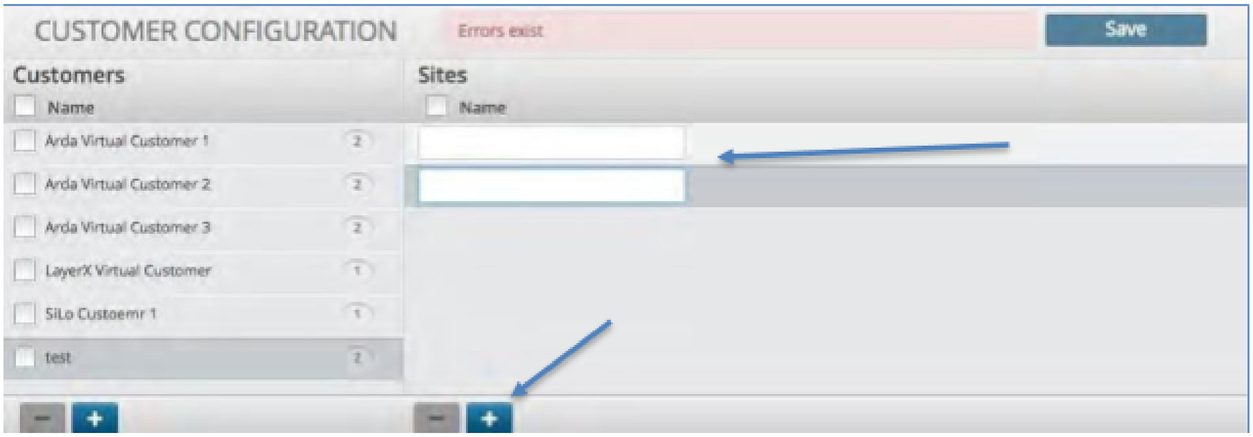
We appreciate and value your comments. Email: doc-feedback@voss-solutions.com



5.9.2. Creating a Customer Site

To create a site for a Customer:

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

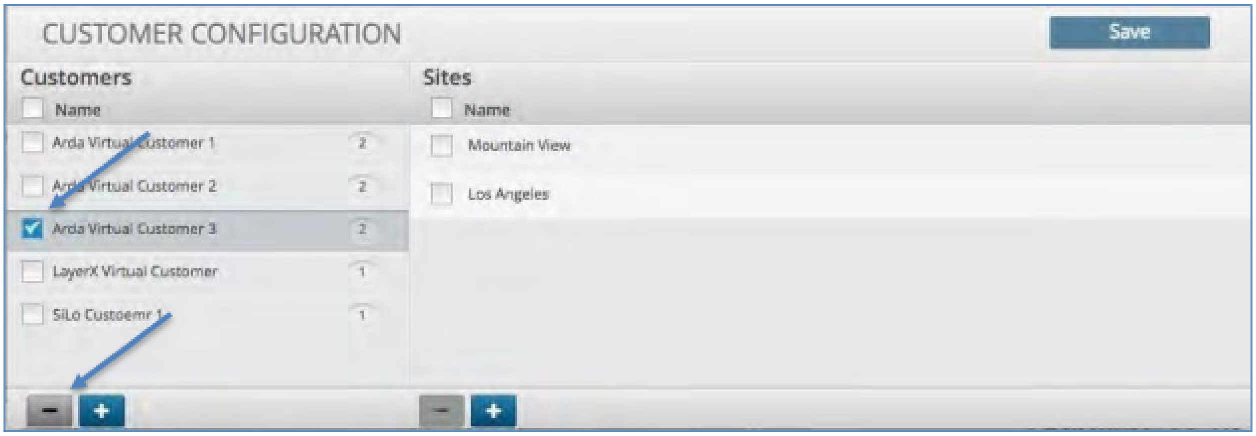


5.9.3. Deleting a Customer

To delete a Customer:

1. Click the check box of the customer you wish to delete.

2. Click the minus icon in the bottom of the site panel.
3. Click the Save icon to in the upper right corner.



Customers

	Name	
☐	Arda Virtual Customer 1	2
☐	Arda Virtual Customer 2	2
☑	Arda Virtual Customer 3	2
☐	LayerX Virtual Customer	1
☐	SiLo Custoemr 1	1

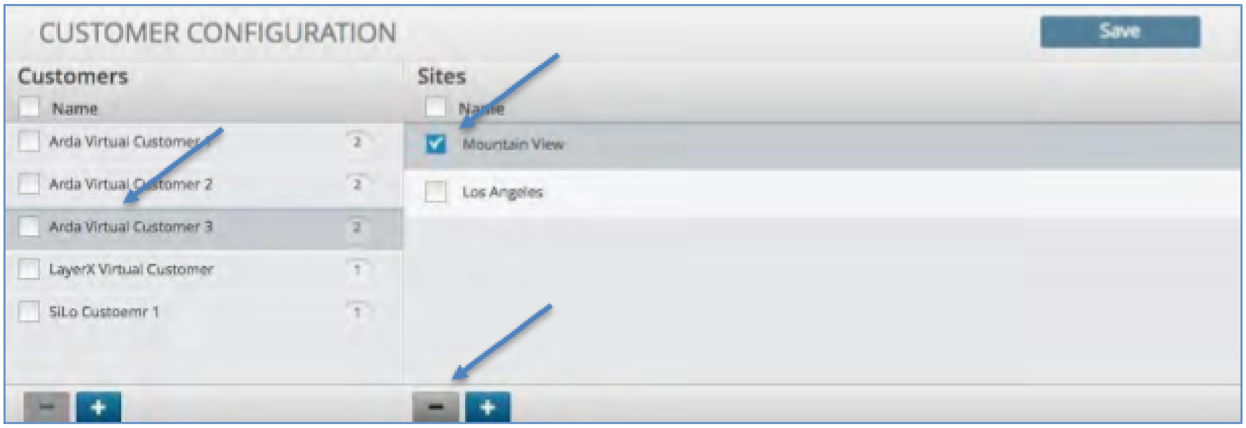
Sites

	Name
☐	Mountain View
☐	Los Angeles

5.9.4. Deleting a Customer Site

To delete a site for a Customer:

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



Customers

	Name	
☐	Arda Virtual Customer 1	2
☐	Arda Virtual Customer 2	2
☐	Arda Virtual Customer 3	2
☐	LayerX Virtual Customer	1
☐	SiLo Custoemr 1	1

Sites

	Name
☑	Mountain View
☐	Los Angeles

5.10. Access Control

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

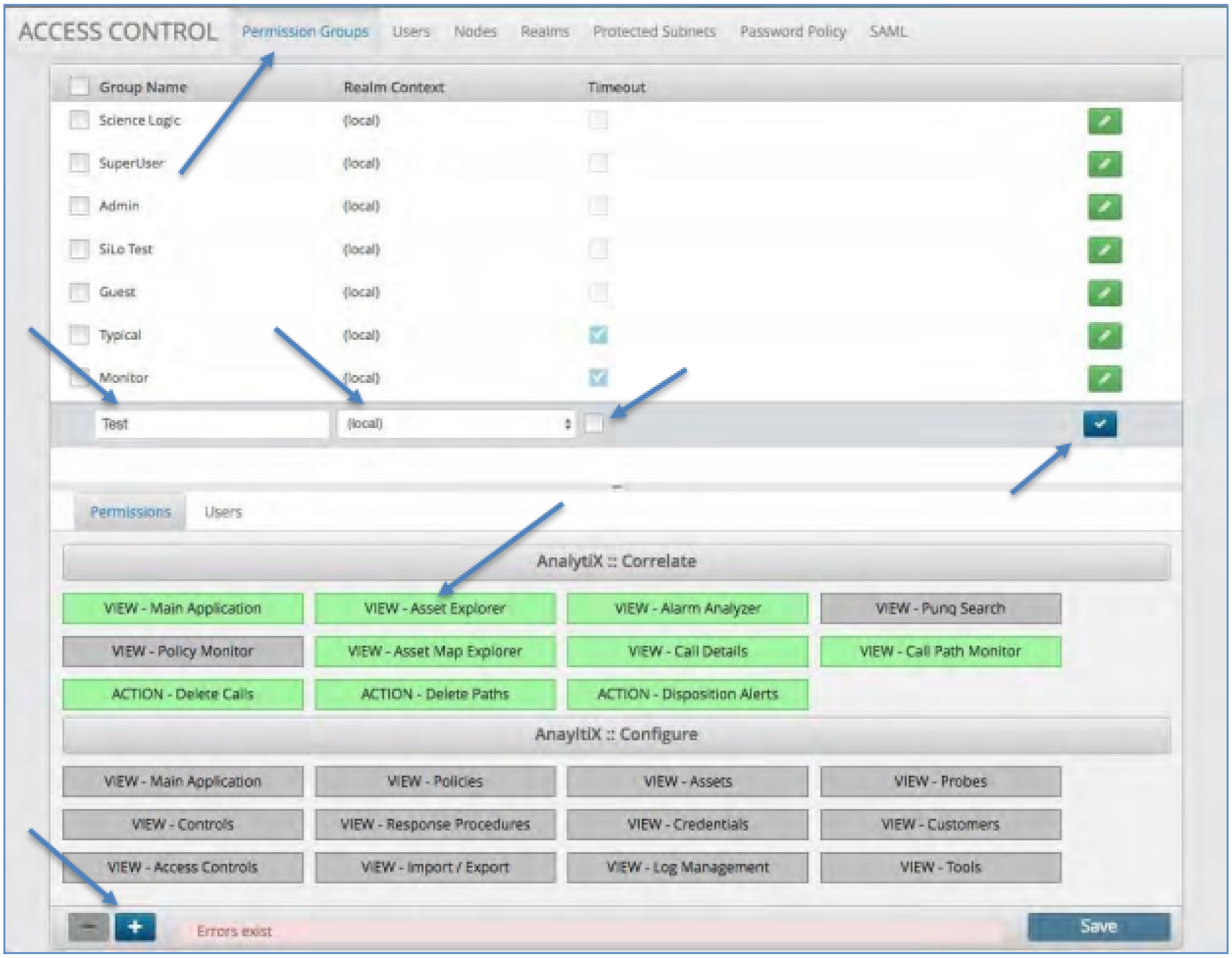
5.10.1. Permission Groups

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

Creating a Permission Group

To create a Permission Group:

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



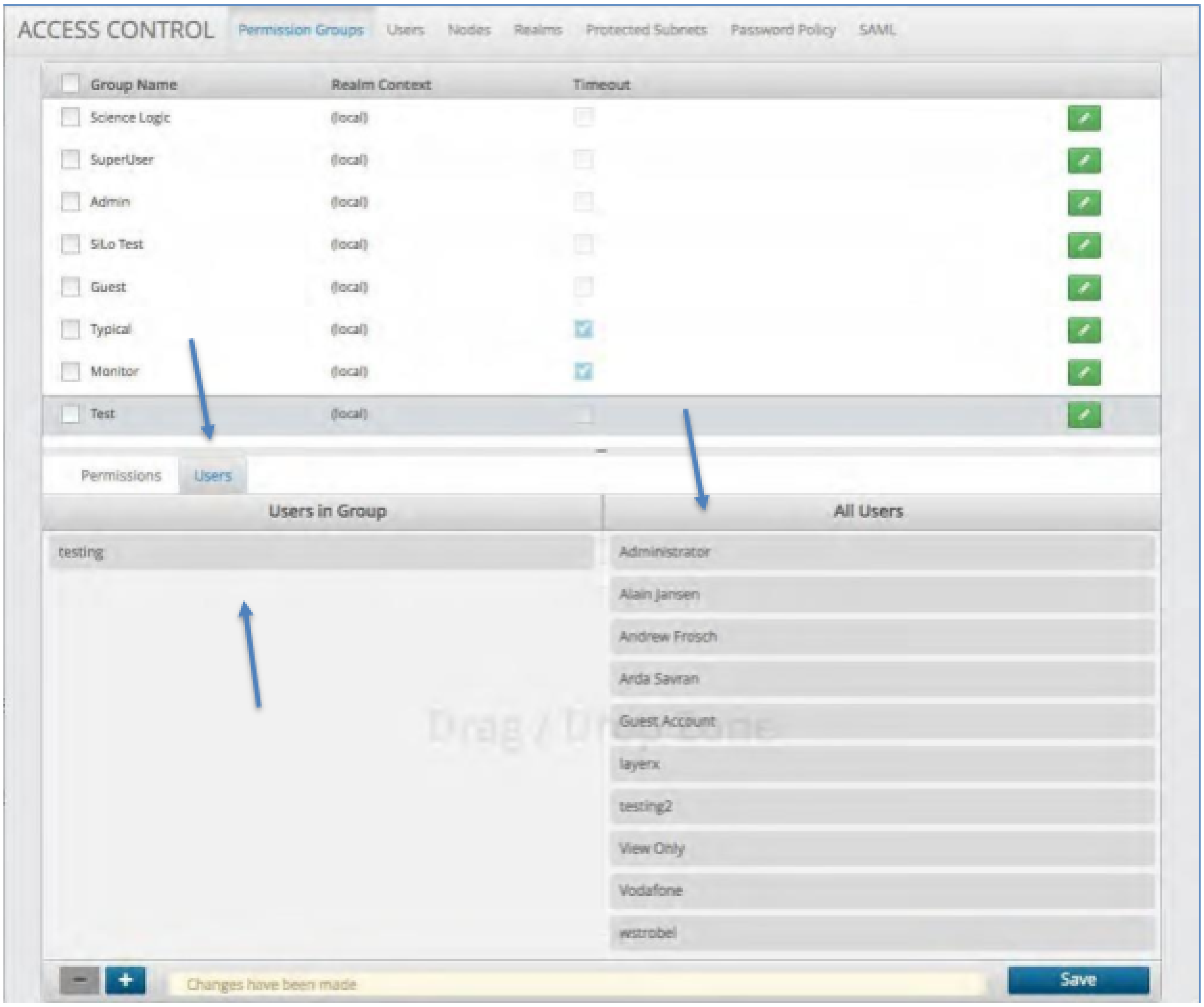
□ Group Name	Realm Context	Timeout
□ Science Logic	(local)	□
□ SuperUser	(local)	□
□ Admin	(local)	□
□ SiLo Test	(local)	□
□ Guest	(local)	□
□ Typical	(local)	☑
□ Monitor	(local)	☑
Test	(local)	□

Errors exist

Assigning and Removing Users to and from a Permission Group

To Assign a User to a Permission Group:

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



□ Group Name	Realm Context	Timeout
□ Science Logic	(local)	□
□ SuperUser	(local)	□
□ Admin	(local)	□
□ SiLo Test	(local)	□
□ Guest	(local)	□
□ Typical	(local)	☑
□ Monitor	(local)	☑
□ Test	(local)	□

Users in Group	All Users
testing	Administrator
	Alain Jansen
	Andrew Frosch
	Arda Savran
	Guest Account
	layerx
	testing2
	View Only
	Vodafone
	wstrobel

5.10.2. Users

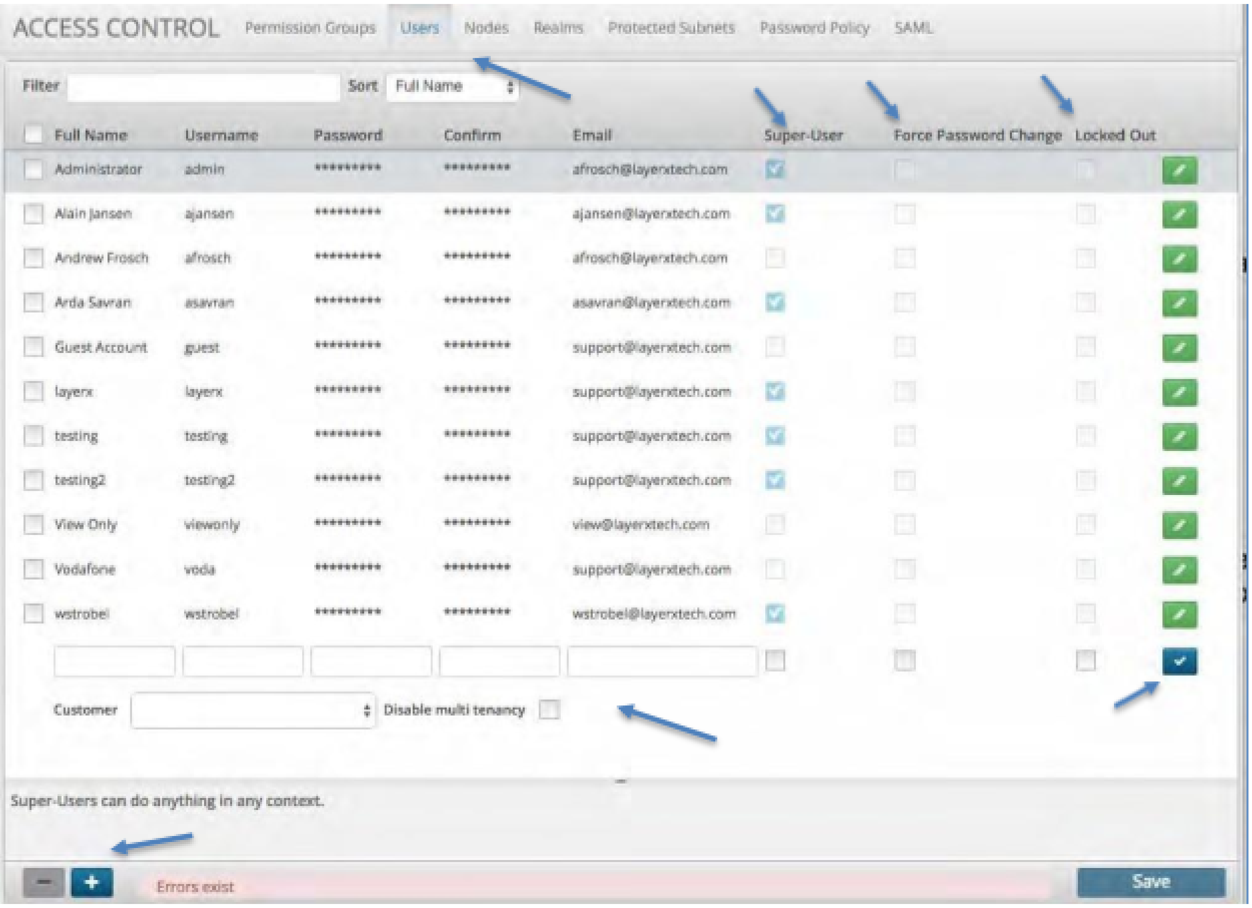
The Users tab allows you to create a new user or modify an existing one. The users can be set up as “Super Users” or assigned roles in the permission groups. Once the user is added and saved then they will be available to add to the Permission Groups per the last section.

Creating a New User

To create a new User:

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

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



Filter

Sort: Full Name

□	Full Name	Username	Password	Confirm	Email	Super-User	Force Password Change	Locked Out	
□	Administrator	admin	**********	**********	afrosch@layerxtech.com	☑	□	□	✎
□	Alain Jansen	ajansen	**********	**********	ajansen@layerxtech.com	☑	□	□	✎
□	Andrew Frosch	afrosch	**********	**********	afrosch@layerxtech.com	□	□	□	✎
□	Arda Savran	asavran	**********	**********	asavran@layerxtech.com	☑	□	□	✎
□	Guest Account	guest	**********	**********	support@layerxtech.com	□	□	□	✎
□	layerx	layerx	**********	**********	support@layerxtech.com	☑	□	□	✎
□	testing	testing	**********	**********	support@layerxtech.com	☑	□	□	✎
□	testing2	testing2	**********	**********	support@layerxtech.com	☑	□	□	✎
□	View Only	viewonly	**********	**********	view@layerxtech.com	□	□	□	✎
□	Vodafone	voda	**********	**********	support@layerxtech.com	□	□	□	✎
□	wstrobel	wstrobel	**********	**********	wstrobel@layerxtech.com	☑	□	□	✎
						□	□	□	✓

Customer | Disable multi tenancy □

Super-Users can do anything in any context.

− + Errors exist

Deleting a User

To delete a User:

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

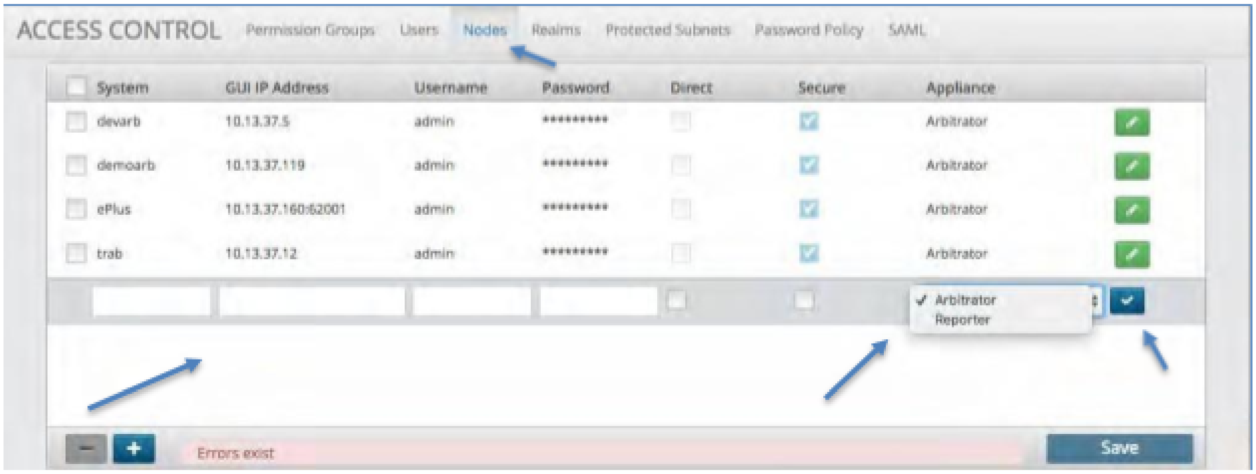
5.10.3. Nodes

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

Creating a Node

To create a Node:

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



□	System	GUI IP Address	Username	Password	Direct	Secure	Appliance	
□	devarb	10.13.37.5	admin	**********	□	☑	Arbitrator	✎
□	demoarb	10.13.37.119	admin	**********	□	☑	Arbitrator	✎
□	ePlus	10.13.37.160:62001	admin	**********	□	☑	Arbitrator	✎
□	trab	10.13.37.12	admin	**********	□	☑	Arbitrator	✎
					□	□	✓ Arbitrator Reporter	✓

Deleting a Node

To delete a Node:

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

5.10.4. Realms

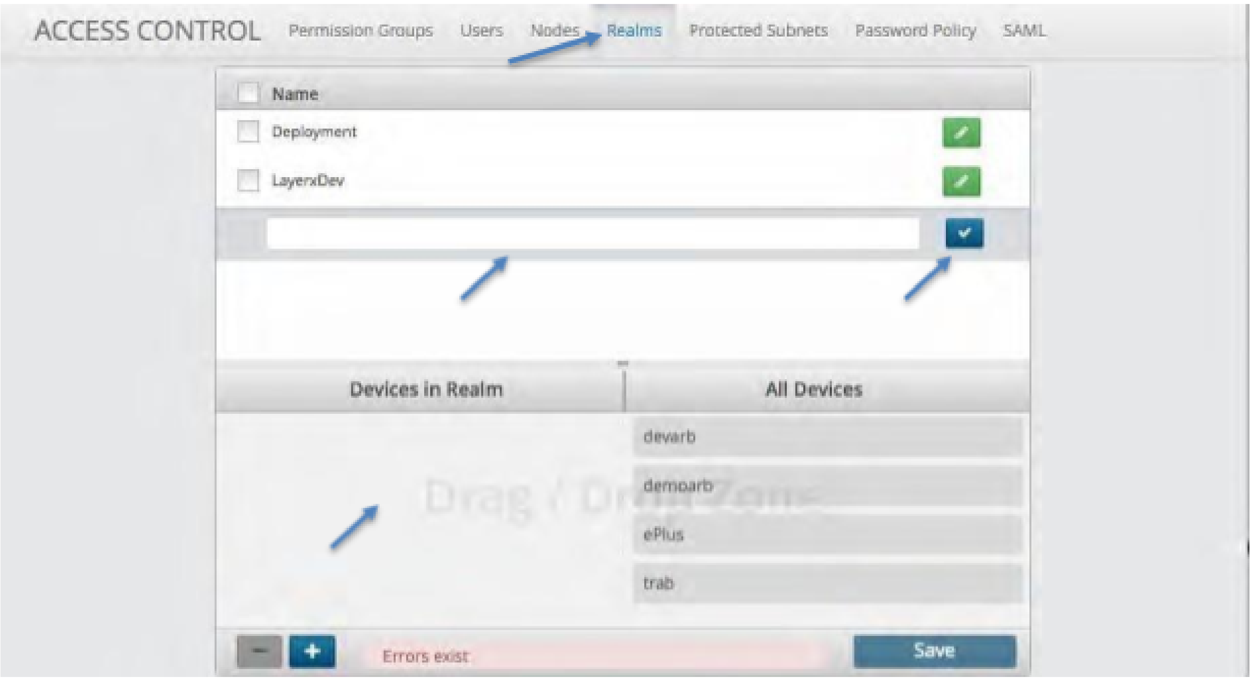
The Realm tab allows you to create a new Realm where VOSS Assurance systems can be grouped to communicate with each other. Once it is added and saved then Nodes can be added to the Realm.

Creating a Realm

To create a Realm:

1. Click the Realm tab at the top of the screen next to Nodes.
2. Click the blue plus icon at the bottom of the screen.
3. Fill in the Realm name that you desire.

4. Click the Blue check icon to set the Realm.
5. Drag the systems that you want in the Realm into the drop zone.
6. Click the Save button to save the Realm.



Deleting a Realm

To delete a Realm:

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

5.10.5. Protected Subnets

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

Creating a Protected Subnet

To create a Protected Subnet:

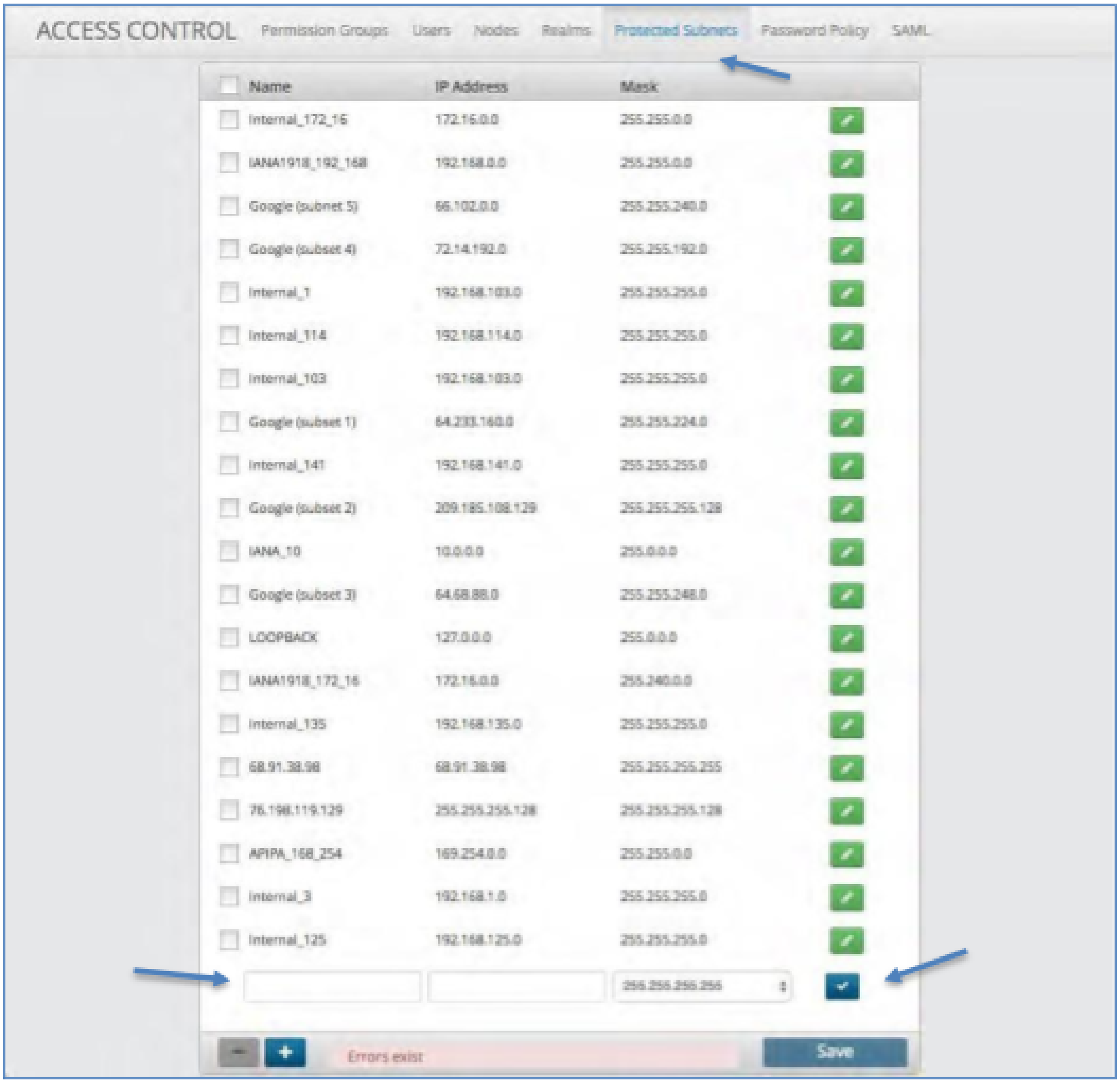
1. Click the Protected Subnet tab at the top of the screen next to Realms.
2. Click the blue plus icon at the bottom of the screen.
3. Fill in the Name, IP Address and Mask of the Protected Subnet.
4. Click the Blue check icon to set the Protected Subnet.

5. Click the Save button to save your changes.

Deleting a Protected Subnet

To delete a Protected Subnet:

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



□	Name	IP Address	Mask
□	Internal_172_16	172.16.0.0	255.255.0.0
□	IANA1918_192_168	192.168.0.0	255.255.0.0
□	Google (subnet 5)	66.102.0.0	255.255.240.0
□	Google (subset 4)	72.14.192.0	255.255.192.0
□	Internal_1	192.168.103.0	255.255.255.0
□	Internal_114	192.168.114.0	255.255.255.0
□	Internal_103	192.168.103.0	255.255.255.0
□	Google (subset 1)	64.233.160.0	255.255.224.0
□	Internal_141	192.168.141.0	255.255.255.0
□	Google (subset 2)	209.185.108.129	255.255.255.128
□	IANA_10	10.0.0.0	255.0.0.0
□	Google (subset 3)	64.68.88.0	255.255.248.0
□	LOOPBACK	127.0.0.0	255.0.0.0
□	IANA1918_172_16	172.16.0.0	255.240.0.0
□	Internal_135	192.168.135.0	255.255.255.0
□	68.91.38.98	68.91.38.98	255.255.255.255
□	76.198.119.129	255.255.255.128	255.255.255.128
□	APIPA_168_254	169.254.0.0	255.255.0.0
□	Internal_3	192.168.1.0	255.255.255.0
□	Internal_125	192.168.125.0	255.255.255.0
			255.255.255.255

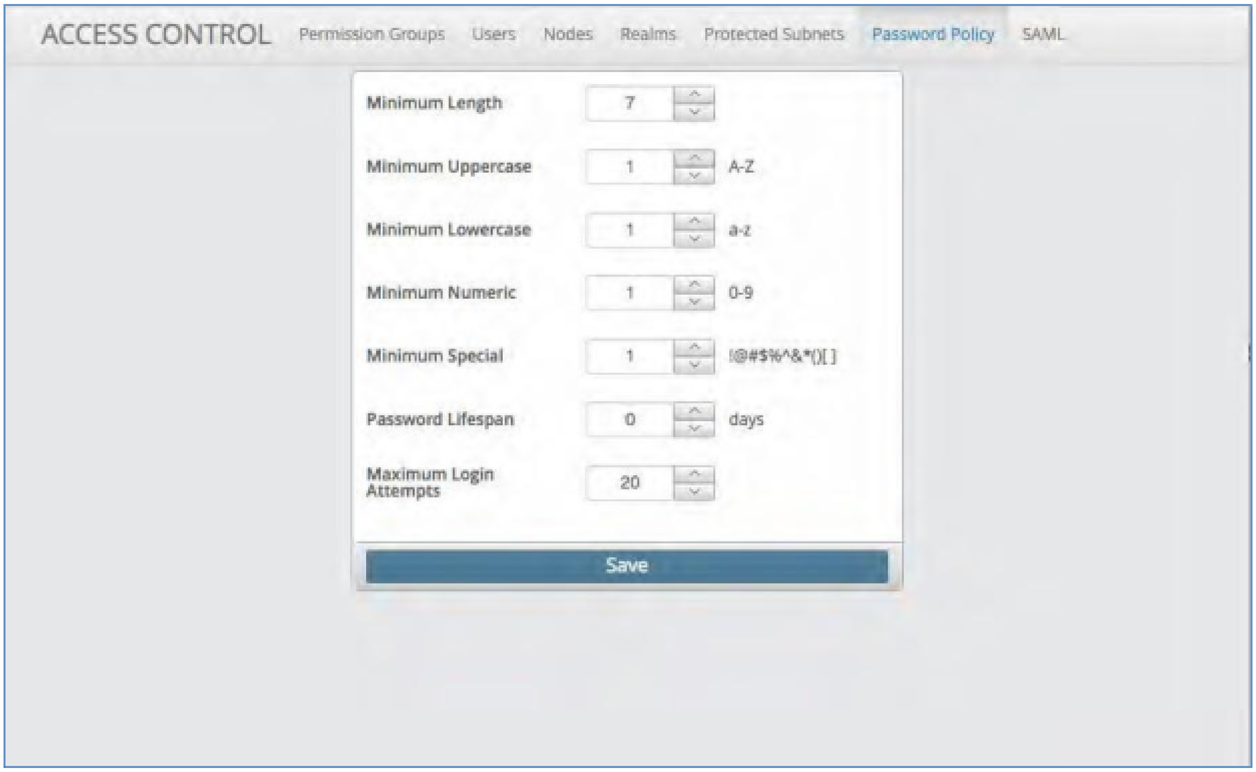
5.10.6. Password Policy

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

Creating a Password Policy

To create a Password Policy:

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



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

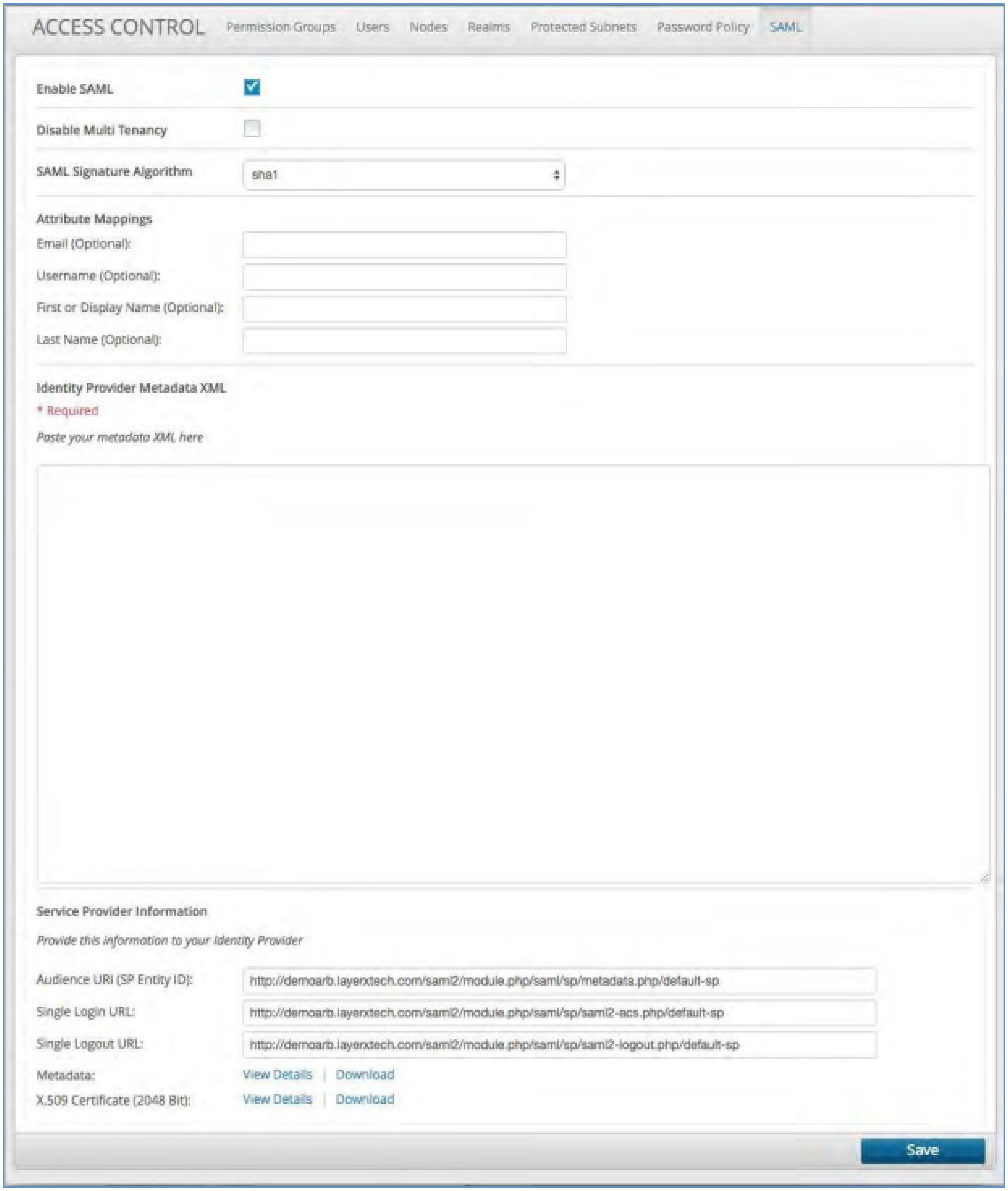
5.10.7. SAML

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

Creating single sign-on via SAML

To create single sign-on via SAML:

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



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

Paste your metadata XML here

Service Provider Information

Provide this information to your Identity Provider

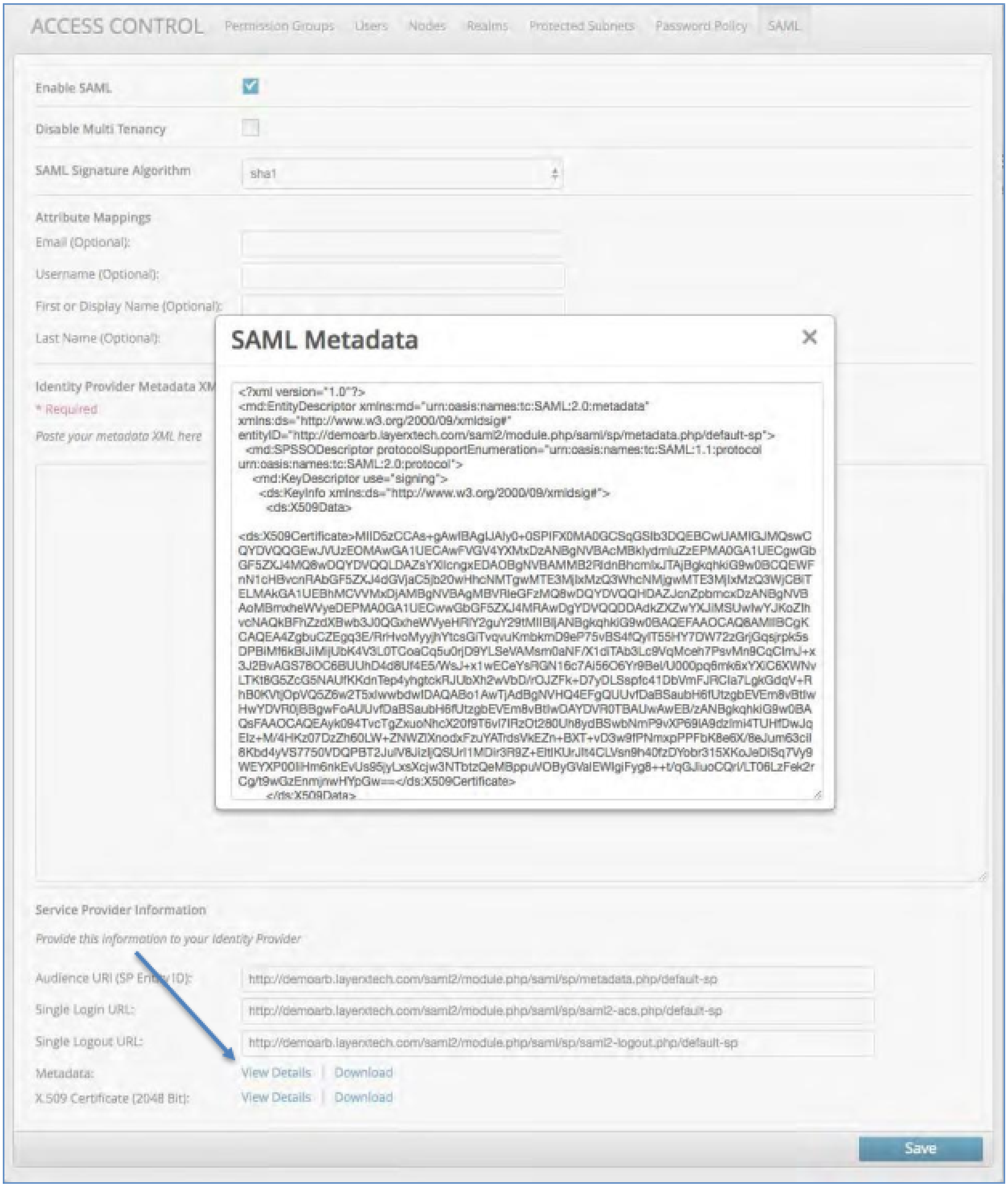
Audience URI (SP Entity ID): http://demoarb.layerxtech.com/saml2/module.php/saml/sp/metadata.php/default-sp

Single Login URL: http://demoarb.layerxtech.com/saml2/module.php/saml/sp/saml2-acs.php/default-sp

Single Logout URL: http://demoarb.layerxtech.com/saml2/module.php/saml/sp/saml2-logout.php/default-sp

Metadata: View Details | Download

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



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 XM

* 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+gAwIBAgIJAIy0+0SPIFX0MA0GCSqGSIb3DQEBCwUAMIGJMQswC
QYDVQQGEwJVUzEOMAwGA1UECAwFVGV4YXMxDzANBgNVBAcMBklydmluZzEPMA0GA1UECgwGb
GF5ZXJ4MQ8wDQYDVQQLDAZsYXIlcngxEDAOBgNVBAMMB2RldnBhcmlxJTAjBgkqhkiG9w0BCQEWF
nN1cHBvcnRAbGF5ZXJ4dGVjaC5jb20wHhcNMTgwMTE3MjIxMzQ3WhcNMjgwMTE3MjIxMzQ3WjCBIT
ELMAkGA1UEBhMCVVMxDjAMBgNVBAgMBVRleGFzMQ8wDQYDVQQHDAZJcnZpbmcxDzANBgNVB
AoMBmxheWVyeDEPMA0GA1UECwwGbGF5ZXJ4MRAwDgYDVQQDDAdkZXZwYXJIMSUwIwYJKoZIh
vcNAQkBFhZzdXBwb3J0QGxheWVyeHRlY2guY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgK
CAQEA4ZgbuCZEgq3E/RrHvoMyyjhYtcsGiTvqvuKmbkmD9eP75vBS4fQyIT55HY7DW72zGrjGqsjrpk5s
DPBiMf6kBIJiMijUbK4V3L0TCoaCq5u0rjD9YLSeVAMsm0aNF/X1dITAb3Lc9VqMceh7PsvMn9CqCImJ+x
3J2BvAGS78OC6BUUhD4d8UI4E5/WsJ+x1wECeYsRGN16c7Ai56O6Yr9BeI/U000pq6mk6xYXiC6XWNv
LTKt8G5ZcG5NAUfKKdnTep4yhgtckRJUbXh2wVbD/rOJZFk+D7yDLSspfc41DbVmFJRCIa7LgkGdqV+R
hB0KVtjOpVQ5Z6w2T5xlwwbdwIDAQABo1AwTjAdBgNVHQ4EFgQUUvfDaBSaubH6fUtzgbEVEm8vBtlw
HwYDVR0jBBgwFoAUUvfDaBSaubH6fUtzgbEVEm8vBtlwDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BA
QsFAAOCAQEAyk094TvcTgZxuoNhcX20f9T6vI7IRzOt280Uh8ydBSwbNmP9vXP69IA9dzImi4TUHfDwJq
EIz+M/4HKz07DzZh60LW+ZNWZIXnodxFzuYATrdsVkEZn+BXT+vD3w9fPNmxpPPFbK8e6X/8eJum63cII
8Kbd4yVS7750VDQPBT2JuIV8JizIjQSUrl1MDir3R9Z+EltIKUrJlt4CLVsn9h40fzDYobr315XKoJeDiSq7Vy9
WEYXP00IlHm6nkEvUs95jyLxsXcjw3NTbtzQeMBppuVOByGValEWIgiFyg8++t/qGJluoCQrl/LT06LzFek2r
Cg/t9wGzEnmjnwHYpGw==</ds:X509Certificate>
        </ds:X509Data>
```

Service Provider Information

Provide this information to your Identity Provider

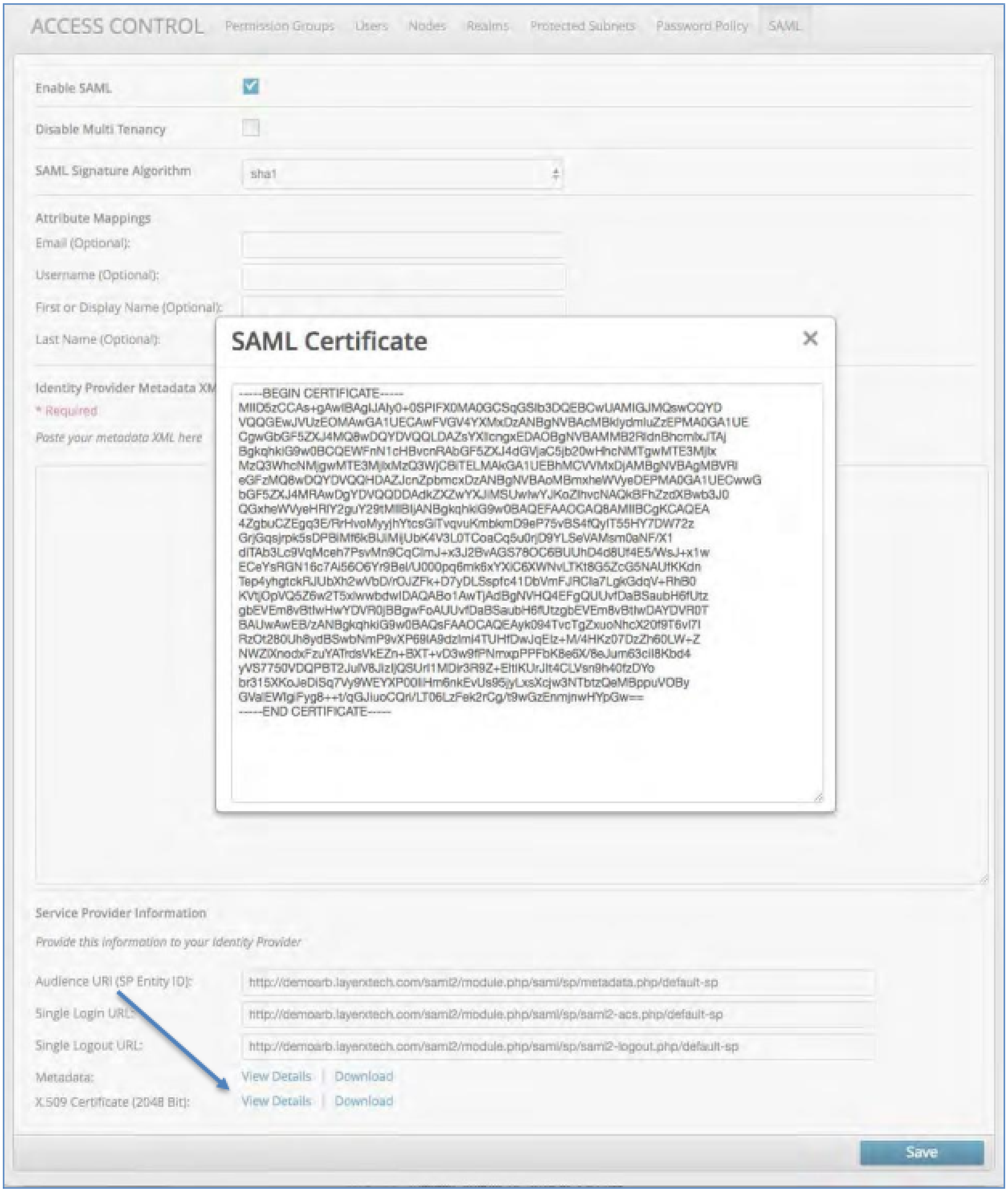
Audience URI (SP Entity ID): http://demoarb.layerxtech.com/saml2/module.php/saml/sp/metadata.php/default-sp

Single Login URL: http://demoarb.layerxtech.com/saml2/module.php/saml/sp/saml2-acs.php/default-sp

Single Logout URL: http://demoarb.layerxtech.com/saml2/module.php/saml/sp/saml2-logout.php/default-sp

Metadata: View Details | Download

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



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 XM

* Required

Paste your metadata XML here

SAML Certificate ×

```
-----BEGIN CERTIFICATE-----
MIID5zCCAs+gAwIBAgIJAIy0+0SPIFX0MA0GCSqGSIb3DQEBCwUAMIGJMQswCQYD
VQQGEwJVUzEOMAwGA1UECAwFVGV4YXMxDzANBgNVBAcMBklydmluZzEPMA0GA1UE
CgwGbGF5ZXJ4MQ8wDQYDVQQLDAZsYXIlcngxEDAOBgNVBAMMB2RldnBhcmlxJTAj
BgkqhkiG9w0BCQEWFnN1cHBvcnRAbGF5ZXJ4dGVjaC5jb20wHhcNMTgwMTE3MjIx
MzQ3WhcNMjgwMTE3MjIxMzQ3WjCBiTELMAkGA1UEBhMCVVMxDjAMBgNVBAgMBVRl
eGFzMQ8wDQYDVQQHDAZJcnZpbmcxDzANBgNVBAoMBmxheWVyeDEPMA0GA1UECwwG
bGF5ZXJ4MRAwDgYDVQQDDAdkZXZwYXJIMSUwIwYJKoZIhvcNAQkBFhZzdXBwb3J0
QGxheWVyeHRlY2guY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
4ZgbuCZEgq3E/RrHvoMyyjhYtcsGITvqvuKmbkmD9eP75vBS4fQyIT55HY7DW72z
GrjGqsjrpk5sDPBIMf6kBUIMjUbK4V3L0TCoaCq5u0rjD9YLSeVAMsm0aNF/X1
dITAb3Lc9VqMceh7PsvMn9CqCImJ+x3J2BvAGS78OC6BUUhD4d8Uf4E5/WsJ+x1w
ECeYsRGN16c7Ai56O6Yr9Bel/U000pq6mk6xYXIC6XWNvLTKt8G5ZcG5NAUfKKdn
Tep4yhgtckRJUbXh2wVbD/rOJZFk+D7yDLSspfc41DbVmFJRCla7LgkGdqV+RhB0
KVtjOpVQ5Z6w2T5xlwwbdwIDAQABo1AwTjAdBgNVHQ4EFgQUUvfDaBSaubH6fUtz
gbEVEm8vBtlwHwYDVR0jBBgwFoAUUvfDaBSaubH6fUtzgbEVEm8vBtlwDAYDVR0T
BAUwAwEB/zANBgkqhkiG9w0BAQsFAAOCAQEAyk094TvcTgZxuoNhcX20f9T6vI7I
RzOt280Uh8ydBSwbNmP9vXP69IA9dzlmi4TUHfDwJqEIz+M/4HKz07DzZh60LW+Z
NWZ0XnodxFzuYATrdsVkEZn+BXT+vD3w9fPNmxpPPFbKBe6X/8eJum63cII8Kbd4
yVS7750VDQPBT2JuIV8JizIjQSUrl1MDir3R9Z+EltIKUrJlt4CLVsn9h40fzDYo
br315XKoJeDiSq7Vy9WEYXP00lIHm6nkEvUs95jyLxsXcjw3NTbtzQeMBppuVOBy
GValEWIgiFyg8++t/qGJiuoCQri/LT06LzFek2rCg/t9wGzEnmjnwHYpGw==
-----END CERTIFICATE-----
```

Service Provider Information

Provide this information to your Identity Provider

Audience URI (SP Entity ID): http://demoarb.layerxtech.com/saml2/module.php/saml/sp/metadata.php/default-sp

Single Login URL: http://demoarb.layerxtech.com/saml2/module.php/saml/sp/saml2-acs.php/default-sp

Single Logout URL: http://demoarb.layerxtech.com/saml2/module.php/saml/sp/saml2-logout.php/default-sp

Metadata: View Details | Download

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

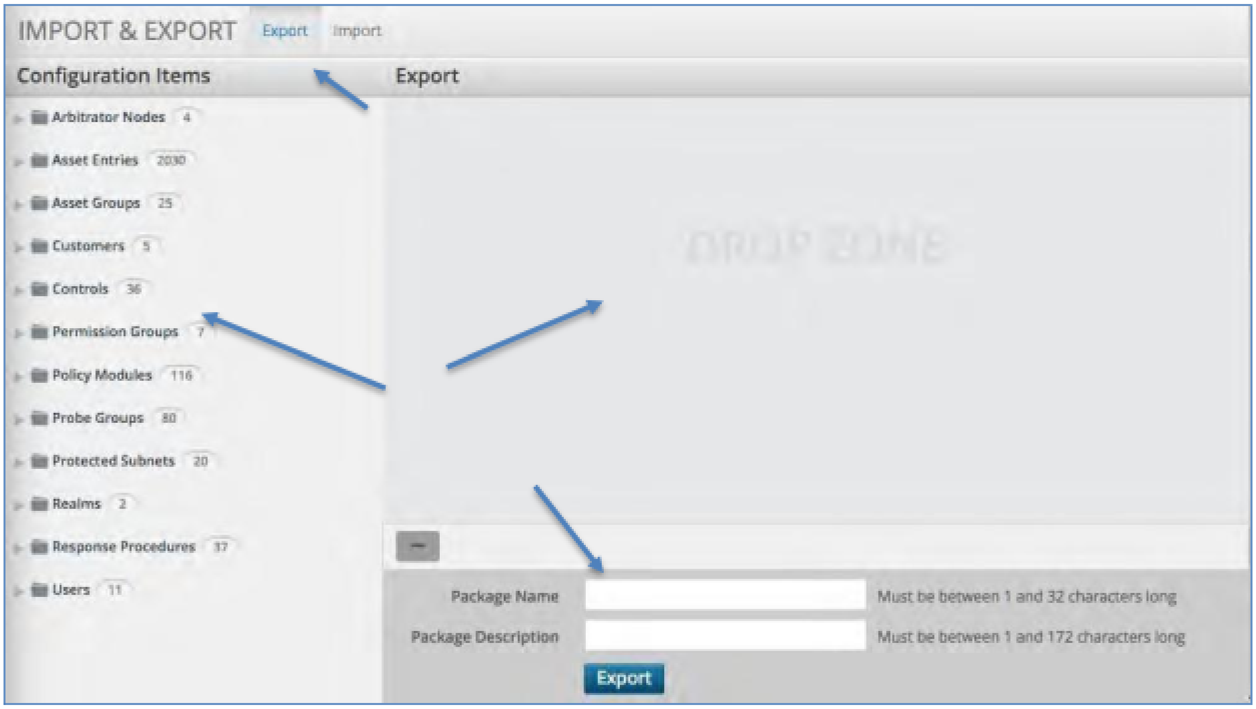
5.11. Import & Export

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

5.11.1. 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.



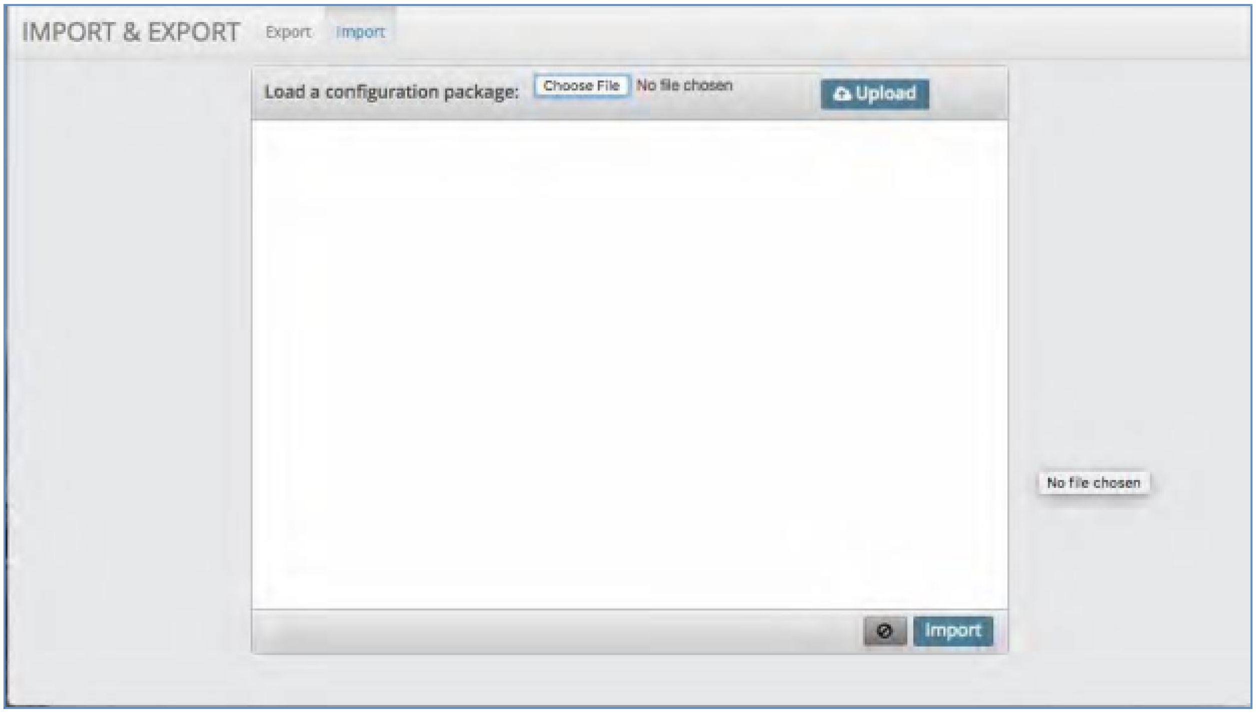
Must be between 1 and 32 characters long

Must be between 1 and 172 characters long

5.11.2. 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.



5.12. Archive Management

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

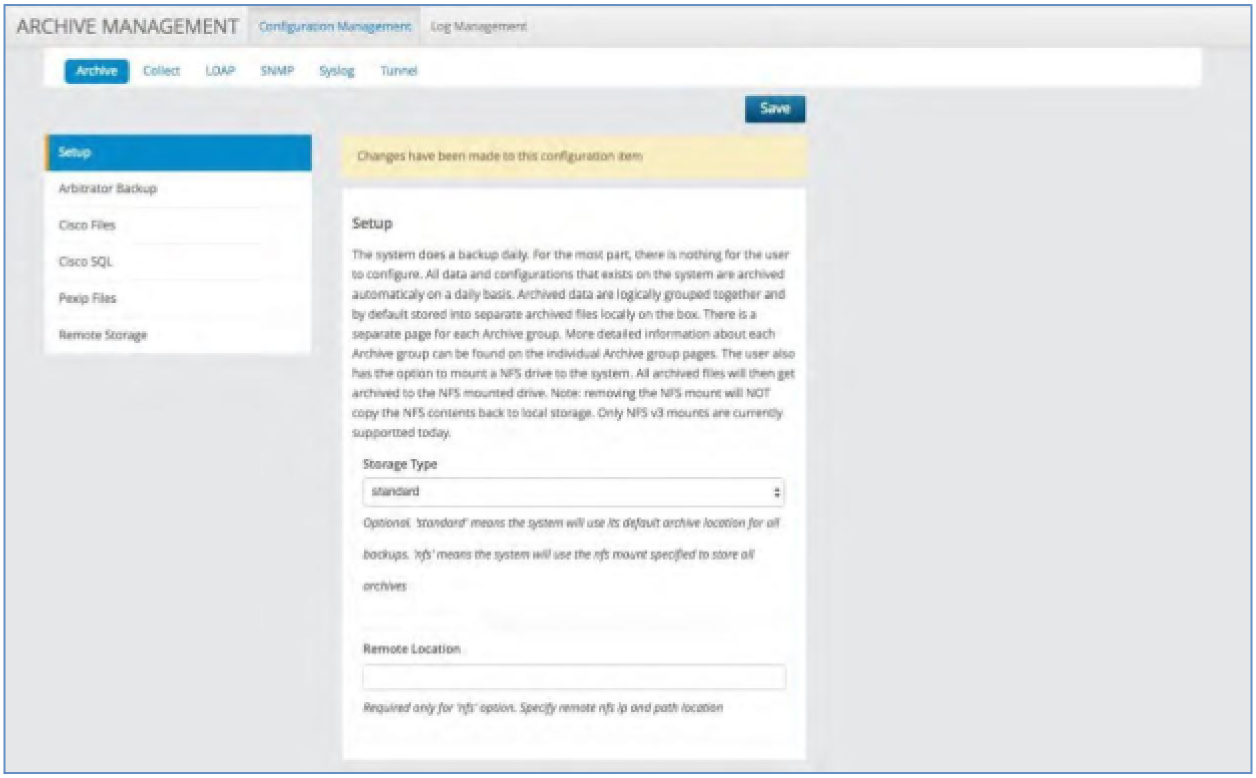
5.12.1. Archive

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

Setup

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

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



Changes have been made to this configuration item

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 automaticaly 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 a 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.

Storage Type: standard

Optional. 'standard' means the system will use its default archive location for all backups. 'nfs' means the system will use the nfs mount specified to store all archives

Remote Location:

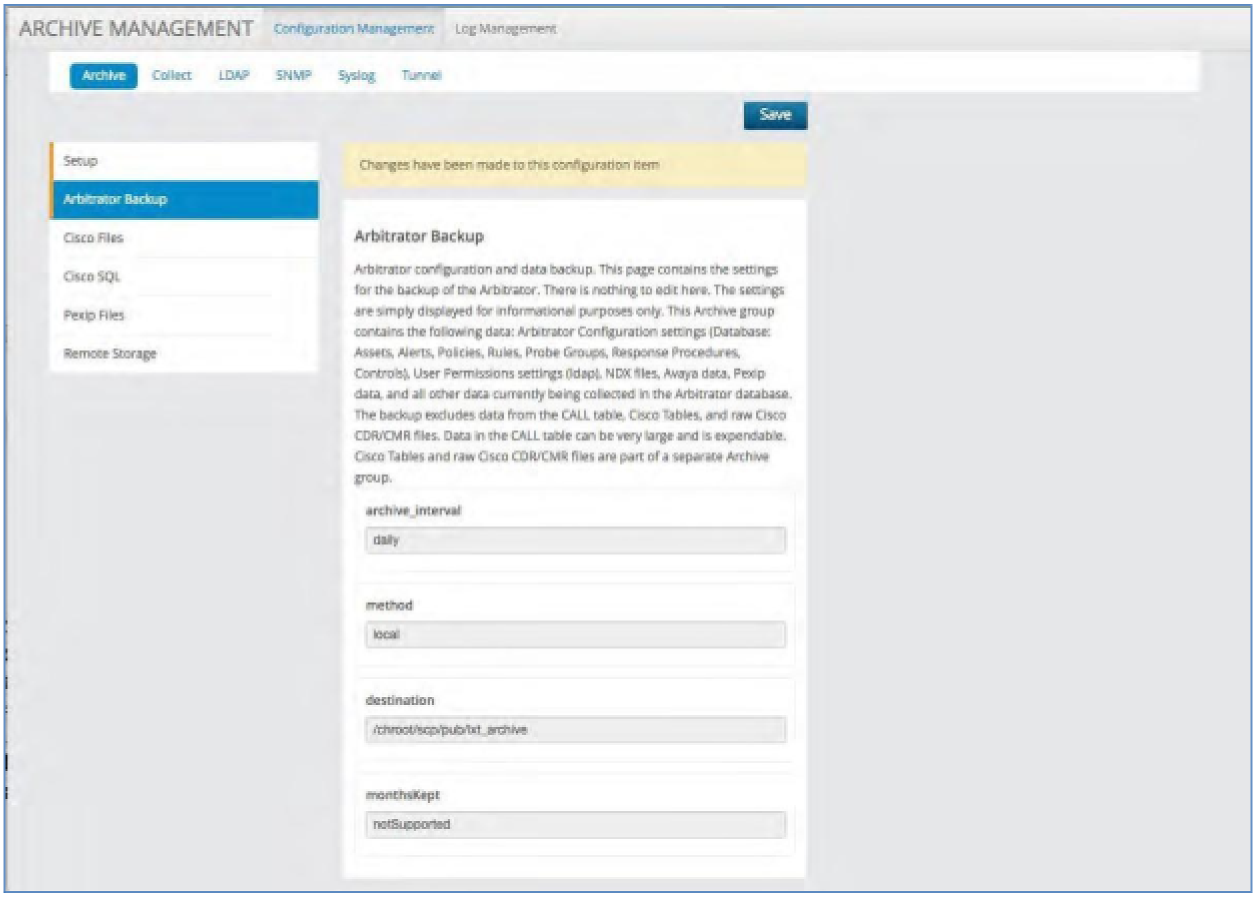
Required only for 'nfs' option. Specify remote nfs ip and path location

Arbitrator Backup

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

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

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



Changes have been made to this configuration item

Arbitrator Backup

Arbitrator configuration and data backup. This page contains the settings for the backup of the Arbitrator. There is nothing to edit here. The settings are simply displayed for informational purposes only. This Archive group contains the following data: Arbitrator Configuration settings (Database: Assets, Alerts, Policies, Rules, Probe Groups, Response Procedures, Controls), User Permissions settings (ldap), NDX files, Avaya data, Pexip data, and all other data currently being collected in the Arbitrator database. The backup excludes data from the CALL table, Cisco Tables, and raw Cisco CDR/CMR files. Data in the CALL table can be very large and is expendable. Cisco Tables and raw Cisco CDR/CMR files are part of a separate Archive group.

archive_interval: daily

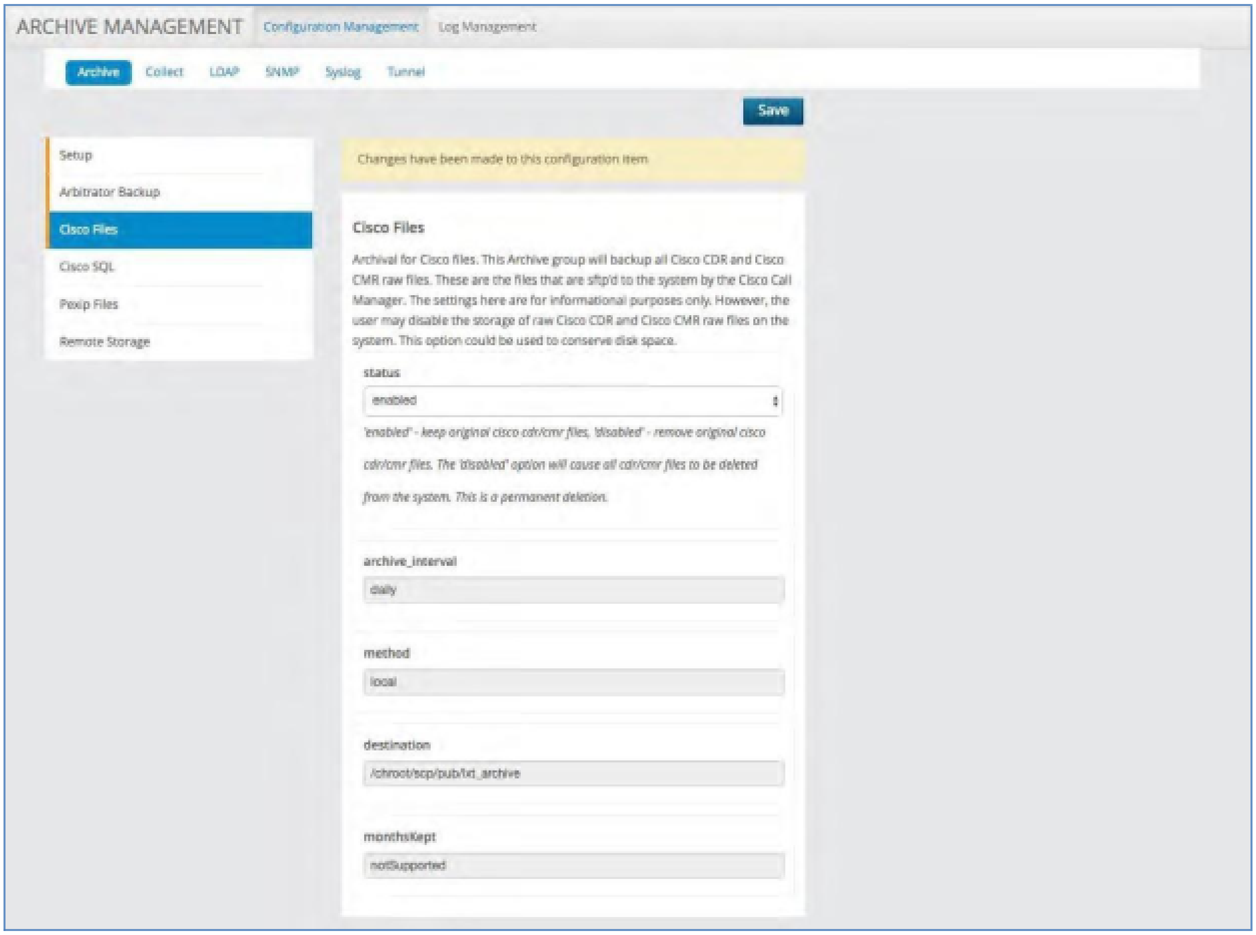
method: local

destination: /chroot/scp/pub/txt_archive

monthsKept: 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.



Changes have been made to this configuration item

Cisco Files

Archival for Cisco files. This Archive group will backup 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.

status: enabled

'enabled' - keep original cisco cdr/cmr files, 'disabled' - remove original cisco cdr/cmr files. The 'disabled' option will cause all cdr/cmr files to be deleted from the system. This is a permanent deletion.

archive_interval: daily

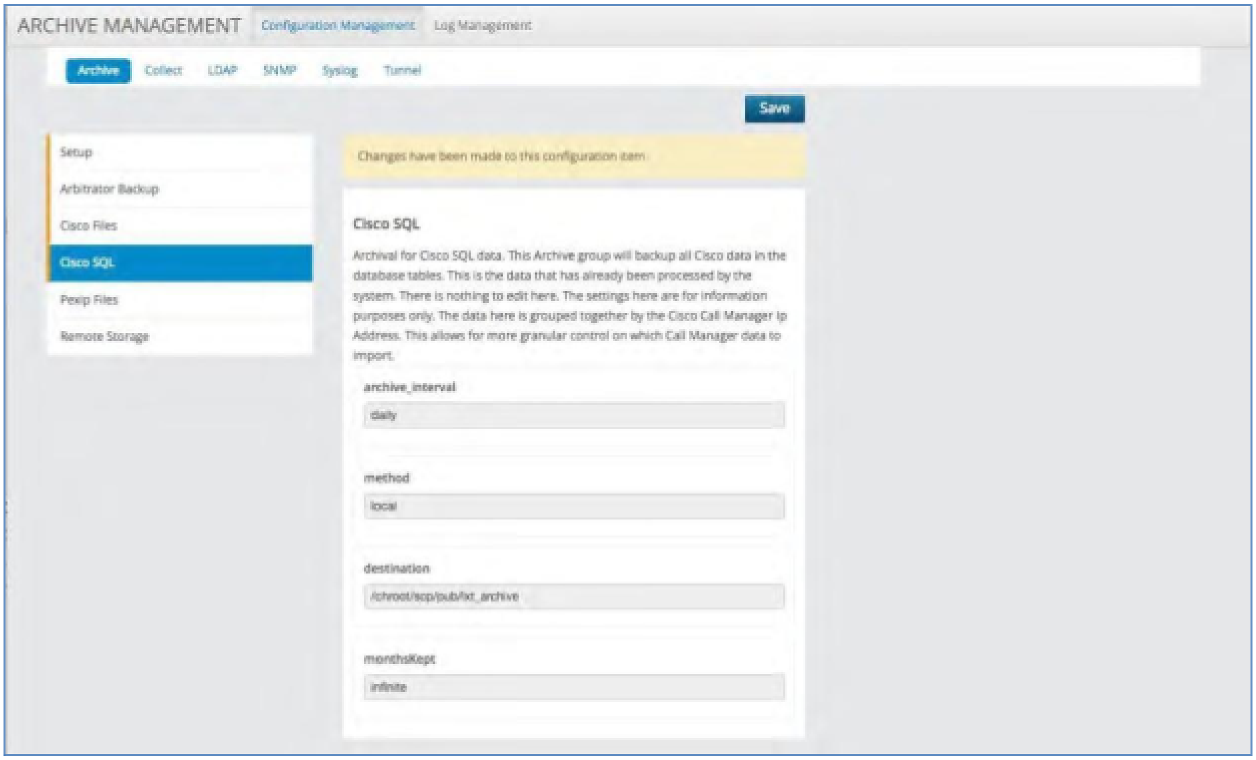
method: local

destination: /chroot/scp/pub/txt_archive

monthsKept: notSupported

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.



Changes have been made to this configuration item

Cisco SQL

Archival for Cisco SQL data. This Archive group will backup 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.

archive_interval: daily

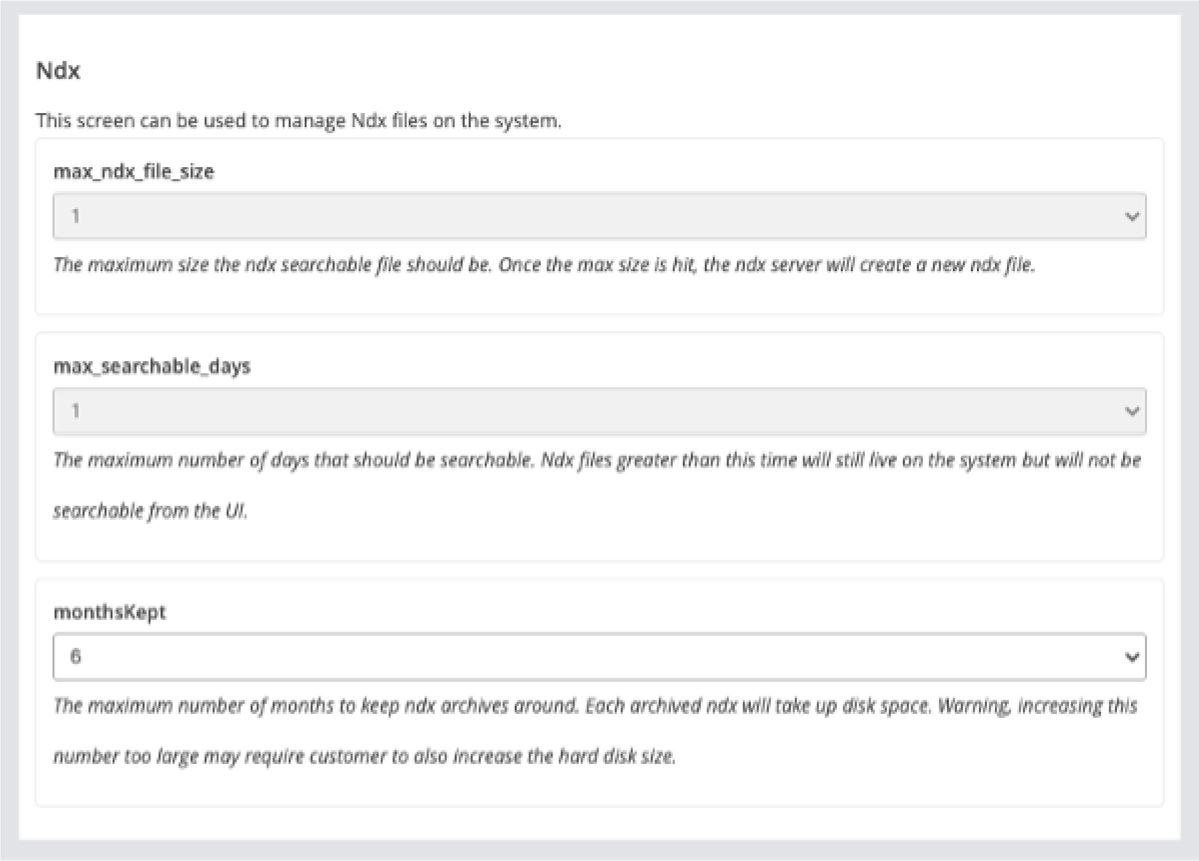
method: local

destination: /chroot/scp/pub/lxt_archive

monthsKept: infinite

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.

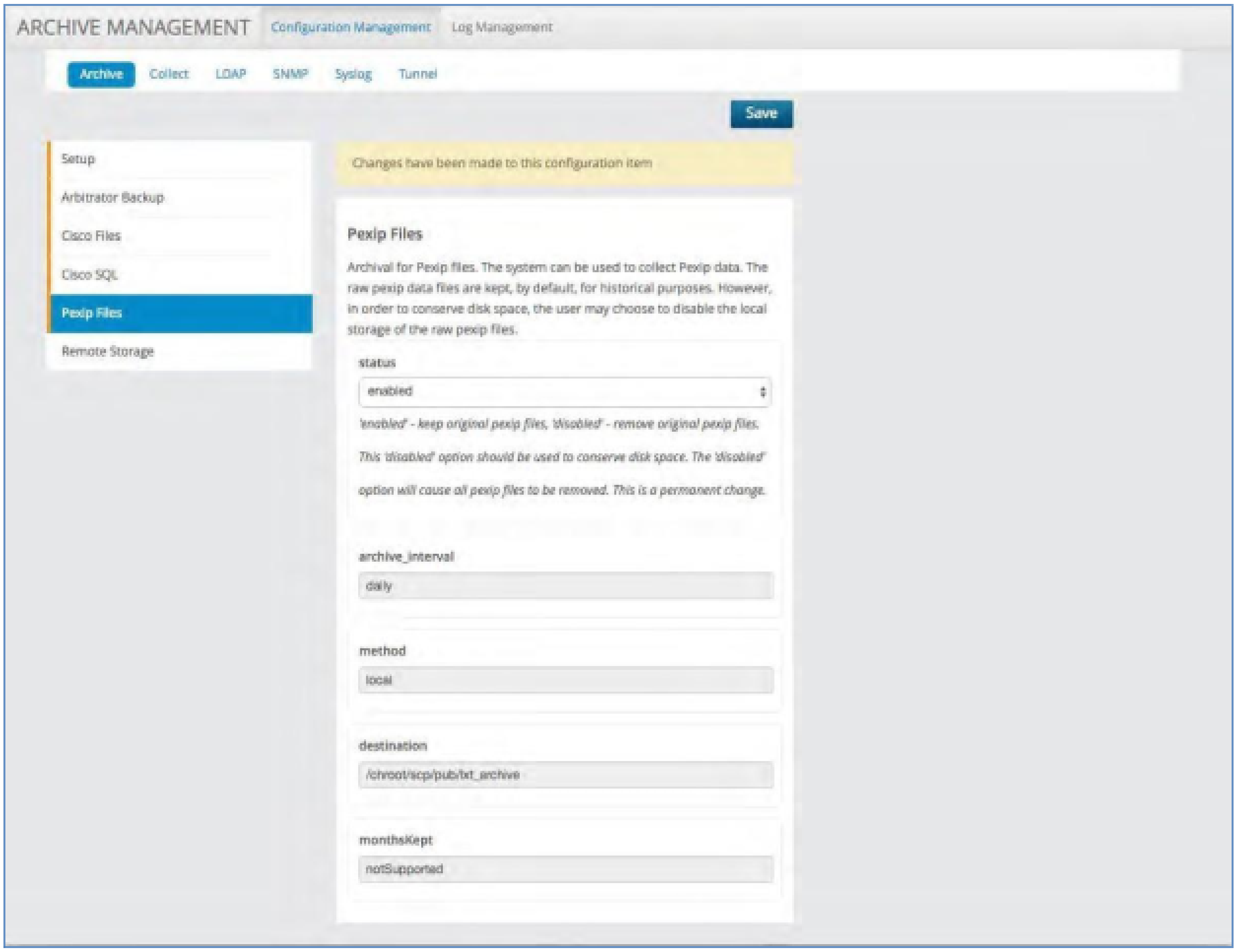
monthsKept

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.



Changes have been made to this configuration item

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.

status: enabled

'enabled' - keep original pexip files, 'disabled' - remove original pexip files.

This 'disabled' option should be used to conserve disk space. The 'disabled'

option will cause all pexip files to be removed. This is a permanent change.

archive_interval: daily

method: local

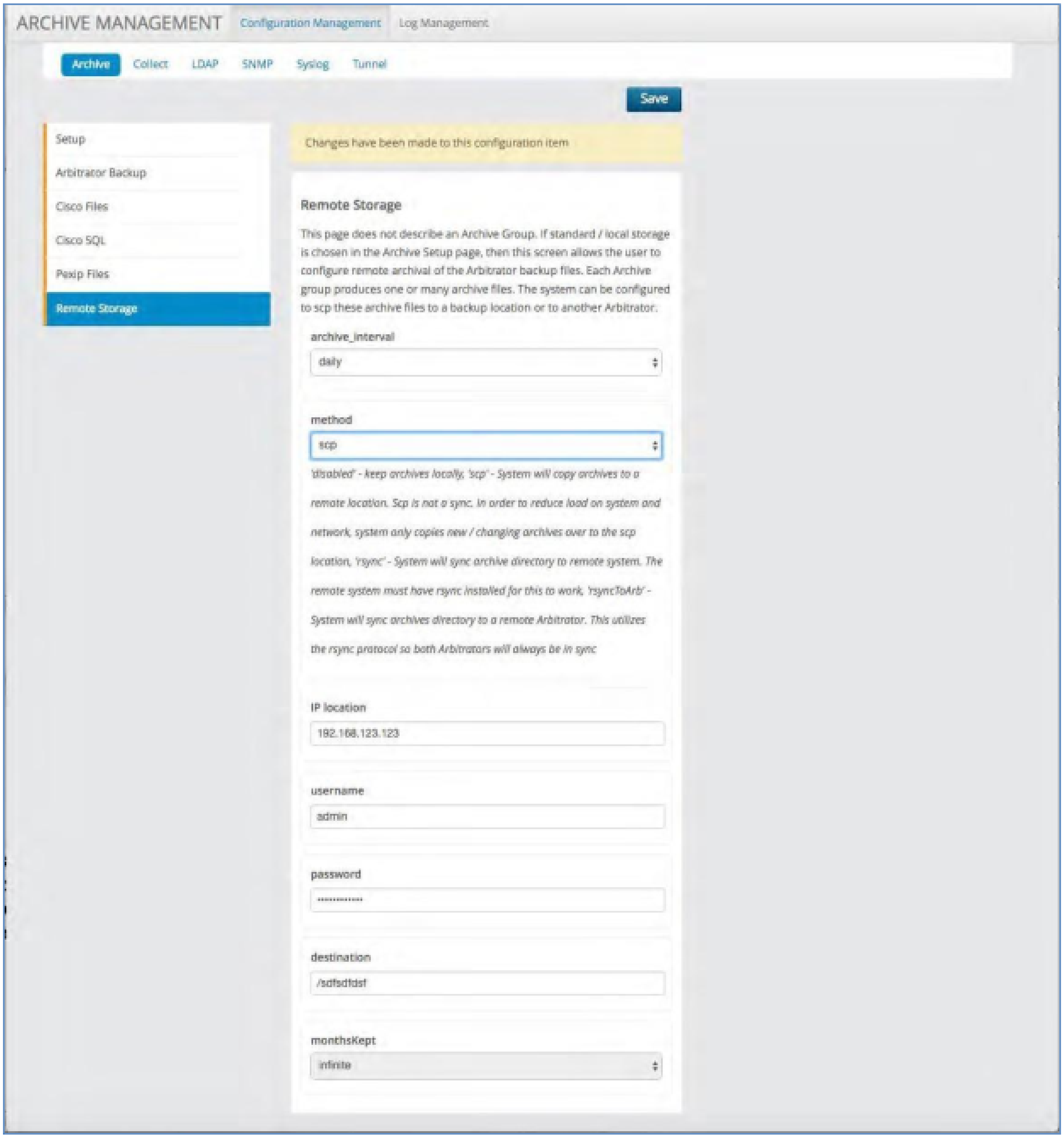
destination: /chroot/scp/pub/txt_archive

monthsKept: notSupported

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 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.



Changes have been made to this configuration item

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 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.

archive_interval: daily

method: scp

'disabled' - keep archives locally, '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, 'rsync' - System will sync archive directory to remote system. The remote system must have rsync installed for this to work, 'rsyncToArb' - System will sync archives directory to a remote Arbitrator. This utilizes the rsync protocol so both Arbitrators will always be in sync

IP location: 192.168.123.123

username: admin

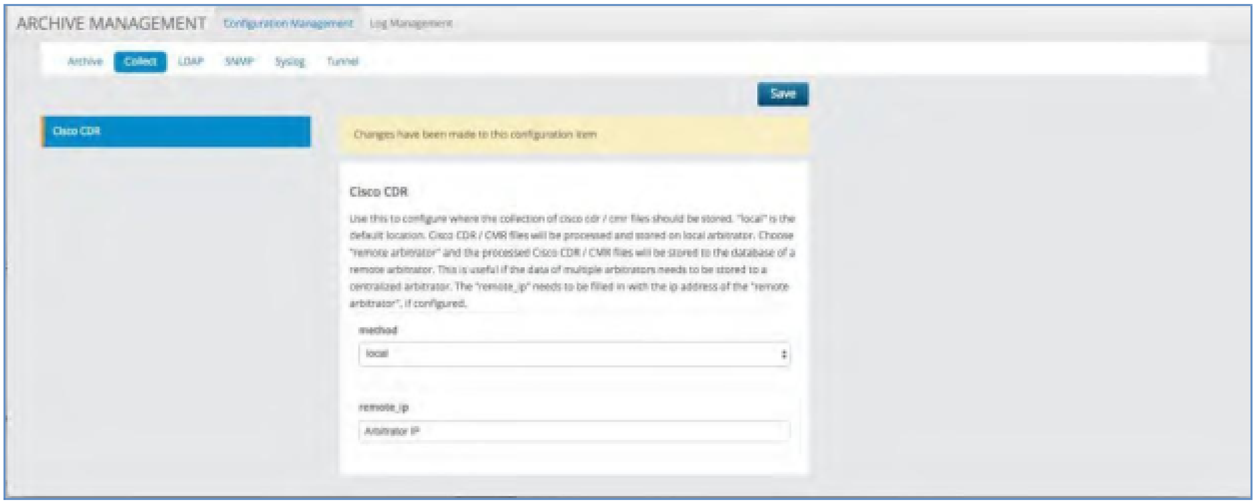
password: ••••••••••••

destination: /sdfsdfdsf

monthsKept: infinite

5.12.2. Collect

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



Changes have been made to this configuration item

Cisco CDR

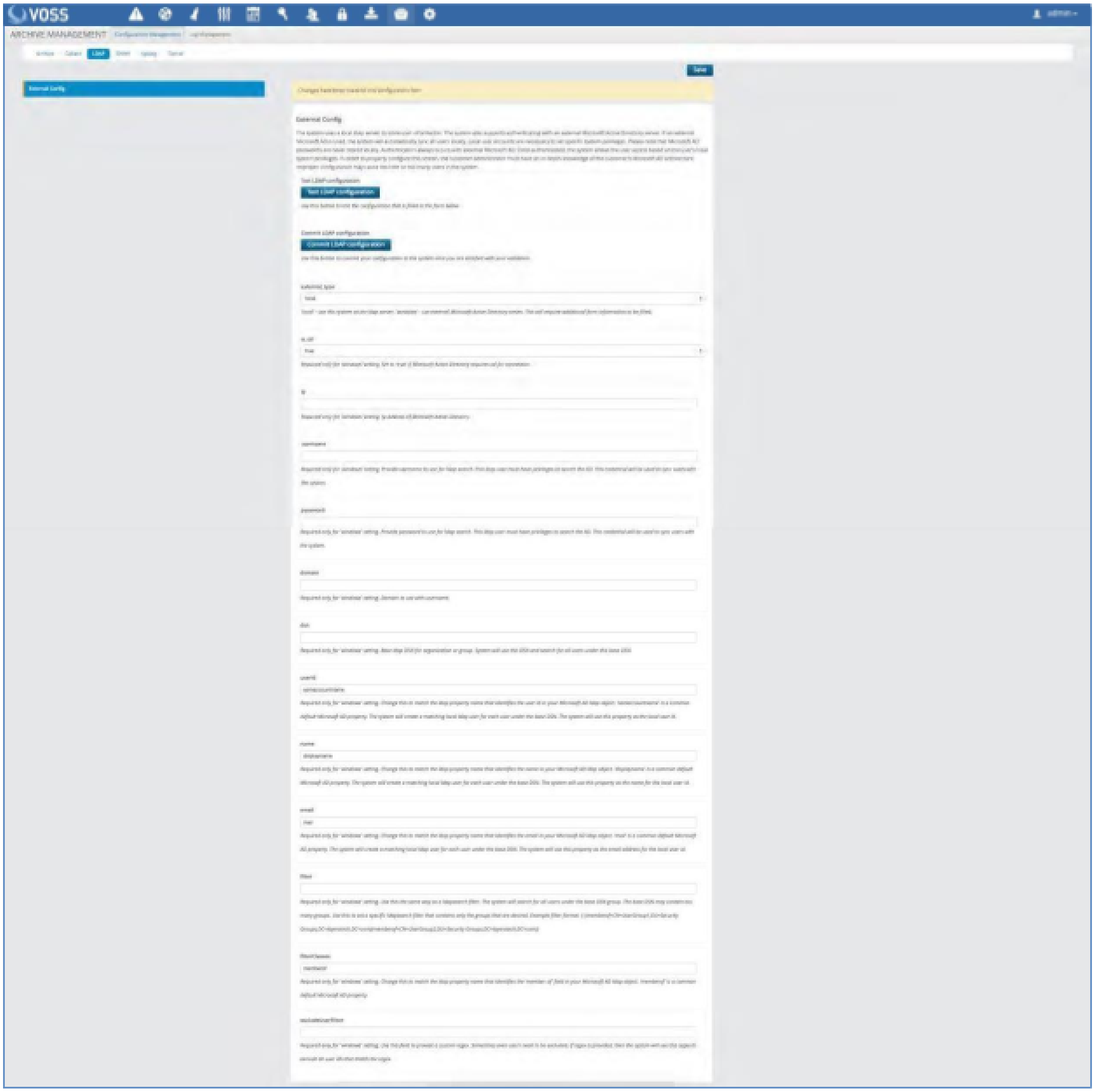
Use this to configure where the collection of cisco cdr / cmr files should be stored. "local" is the default location. Cisco CDR / CMR files will be processed and stored on local arbitrator. Choose "remote arbitrator" and the processed Cisco CDR / CMR files will be stored to the database of a remote 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.

method: local

remote_ip: Arbitrator IP

5.12.3. LDAP External Config

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



External Config

external_type: local

is_ad: true

ip

username

password

domain

dn

userid: samaccountname

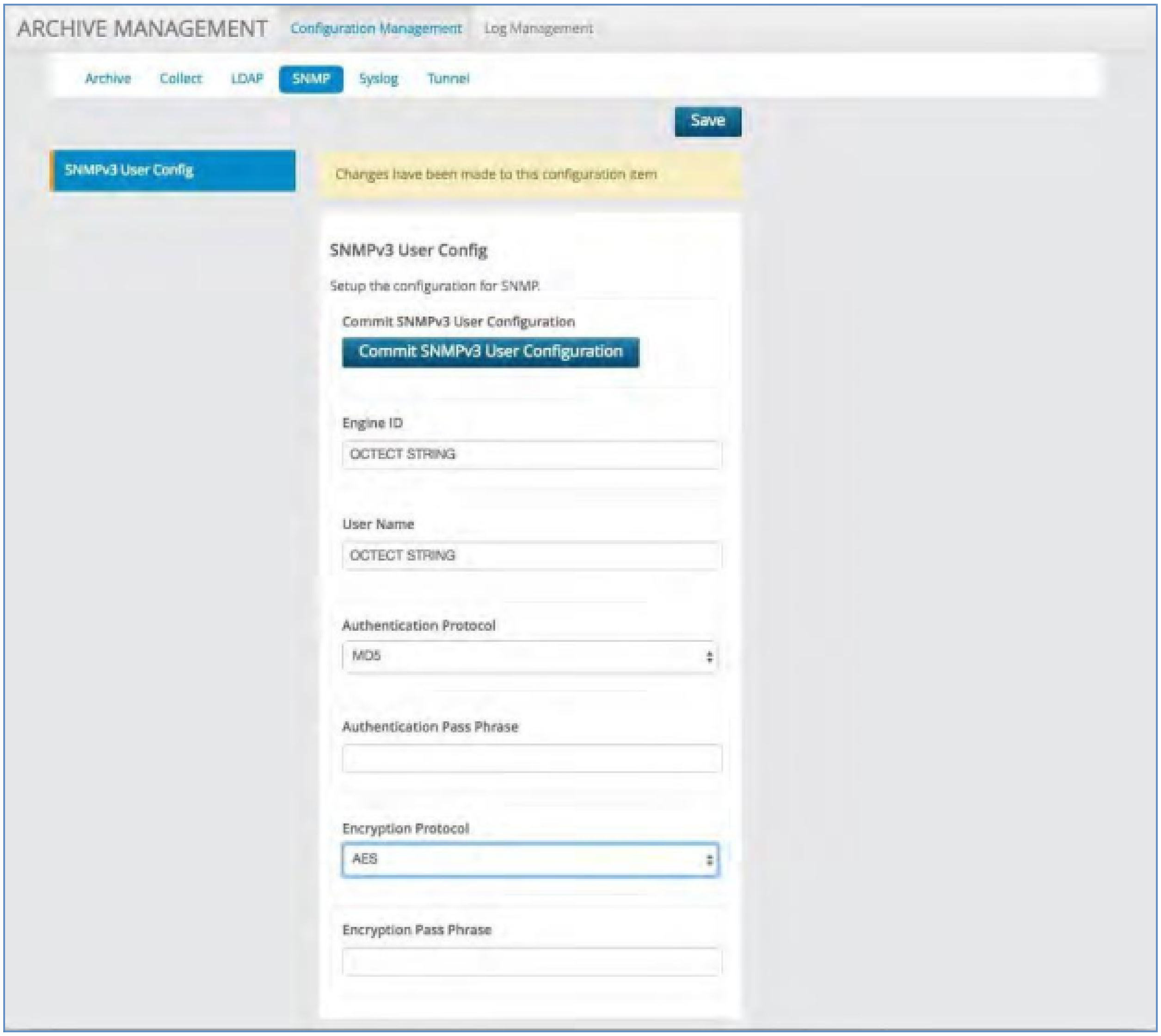
name: displayname

email: mail

filter

5.12.4. SNMP V3 User Config

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



Changes have been made to this configuration item

SNMPv3 User Config

Setup the configuration for SNMP.

Commit SNMPv3 User Configuration

Engine ID: OCTECT STRING

User Name: OCTECT STRING

Authentication Protocol: MD5

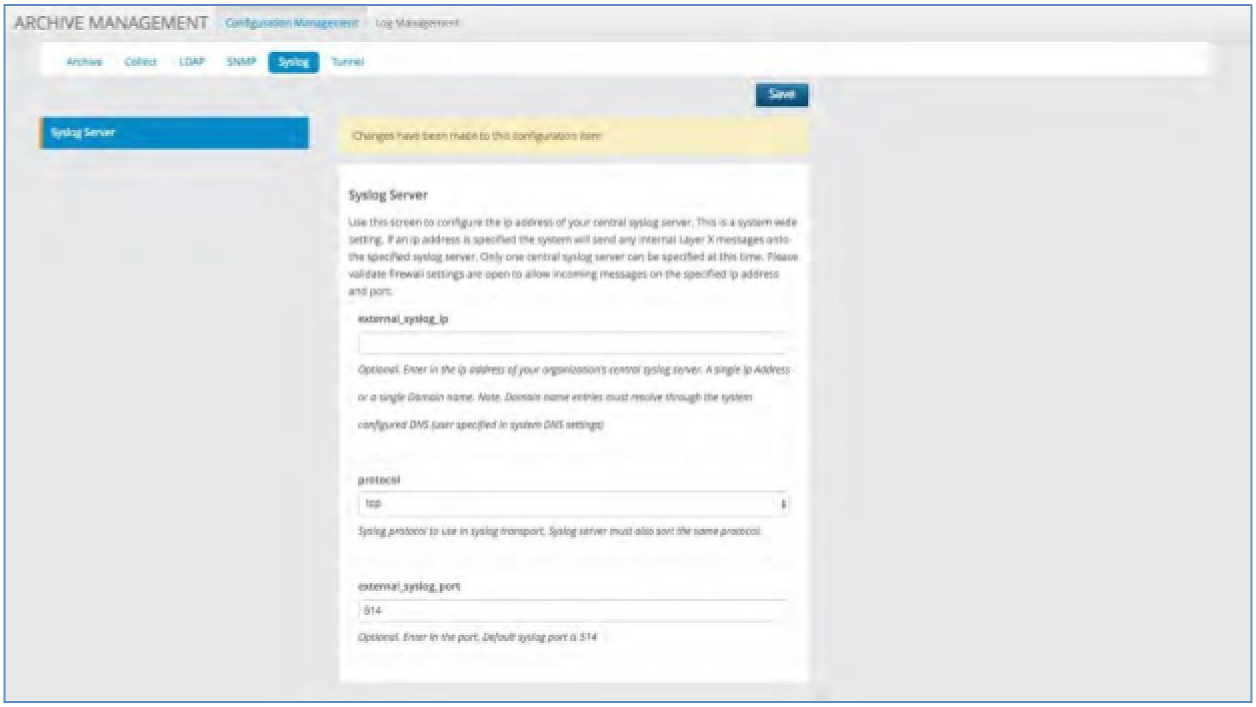
Authentication Pass Phrase:

Encryption Protocol: AES

Encryption Pass Phrase:

5.12.5. Syslog Server

The system has the ability to send out syslog messages about several of the internal functions including backup and archival success. Use this screen to configure the IP address of your central syslog server. This is a system wide setting. If an IP address is specified, the system will send any internal VOSS Assurance 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.



Changes have been made to this configuration item

Syslog Server

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.

external_syslog_ip

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 (user specified in system DNS settings)

protocol

tcp

Syslog protocol to use in syslog transport. Syslog server must also sort the same protocol.

external_syslog_port

514

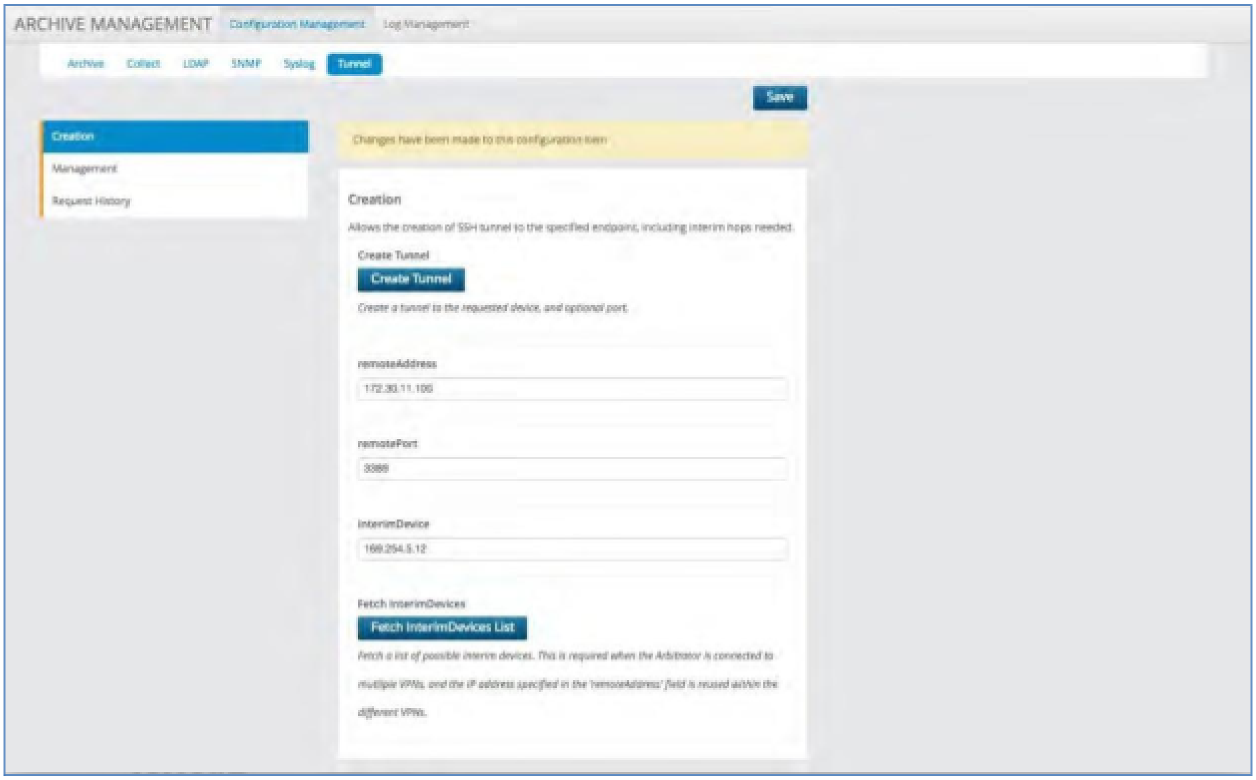
Optional. Enter in the port. Default syslog port is 514

5.12.6. Tunnel

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

Creation

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



Changes have been made to this configuration item

Creation

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

Create Tunnel

Create a tunnel to the requested device, and optional port.

remoteAddress: 172.30.11.100

remotePort: 3389

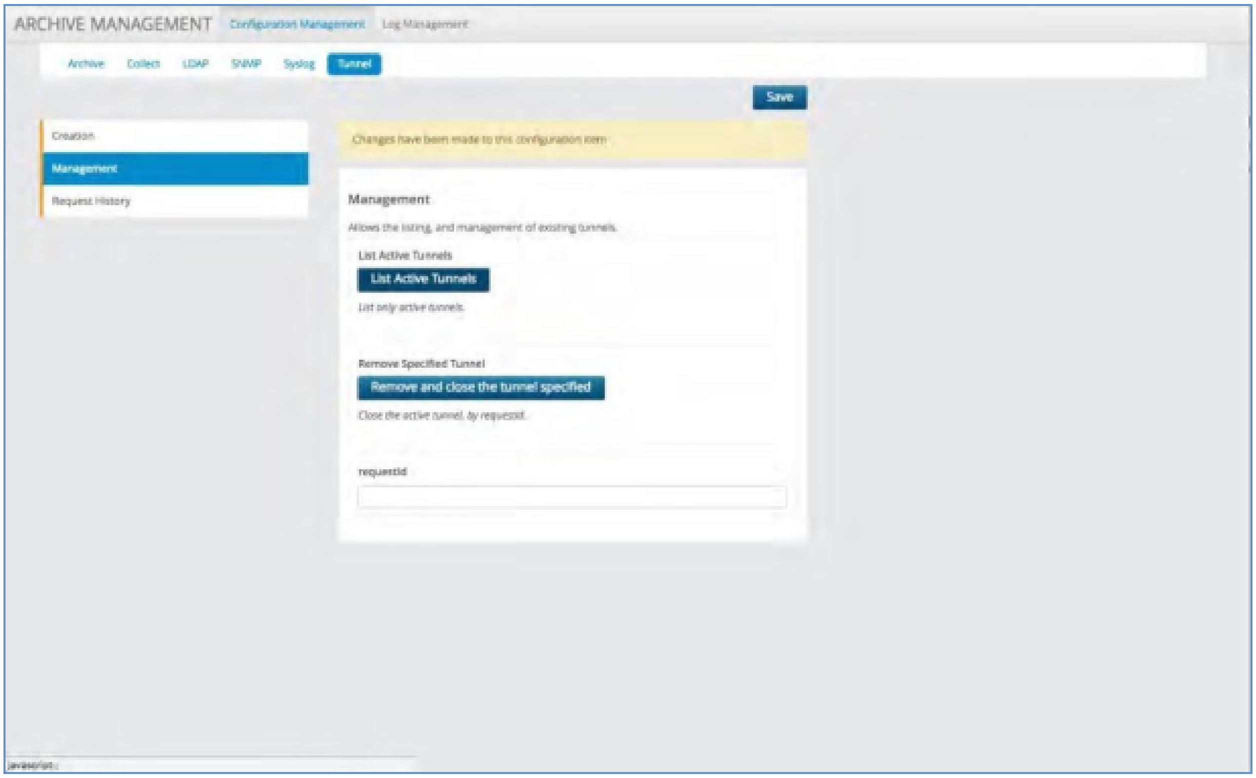
interimDevice: 169.254.5.12

Fetch InterimDevices

Fetch a list of possible interim devices. This is required when the Arbitrator is connected to multiple VPNs, and the IP address specified in the 'remoteAddress' field is reused within the different VPNs.

Management

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



Changes have been made to this configuration item

Management

Allows the listing, and management of existing tunnels.

List Active Tunnels

List only active tunnels.

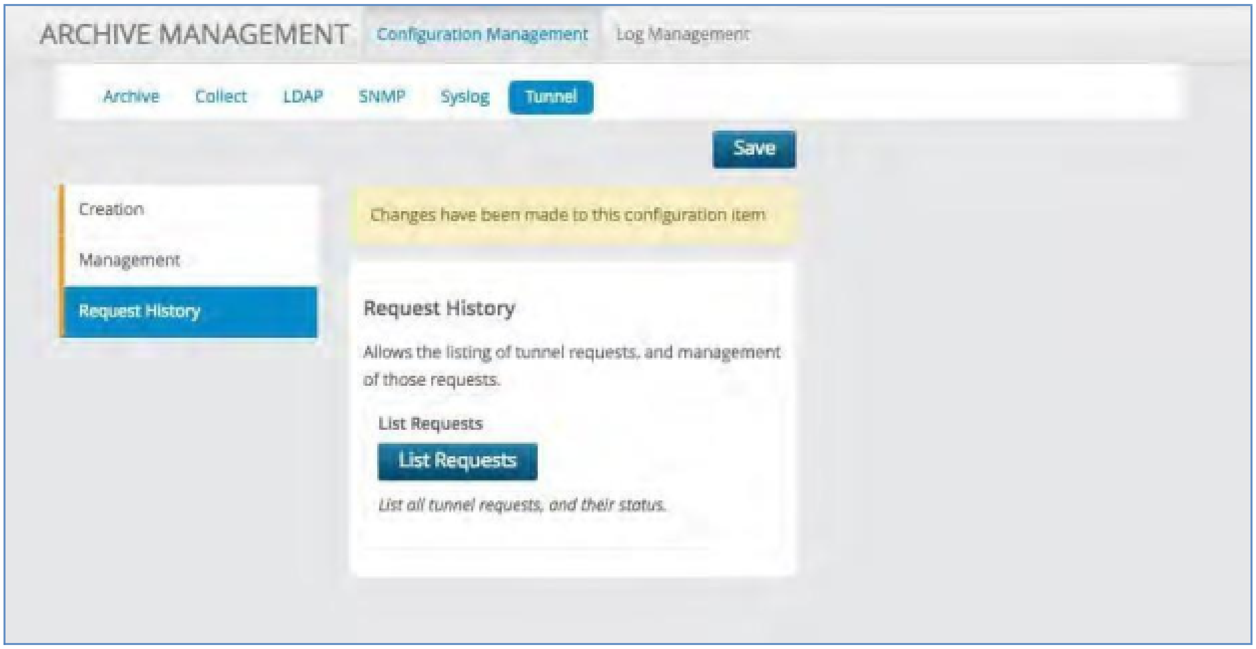
Remove Specified Tunnel

Close the active tunnel, by requestId.

requestId:

Request History

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



Changes have been made to this configuration item

Request History

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

List Requests

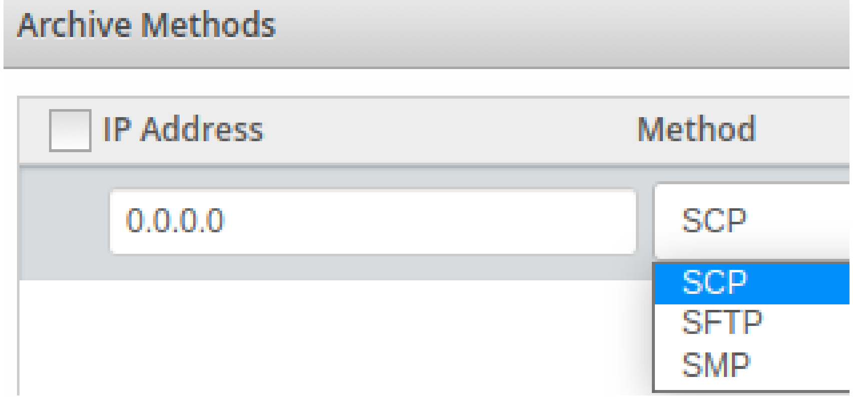
List all tunnel requests, and their status.

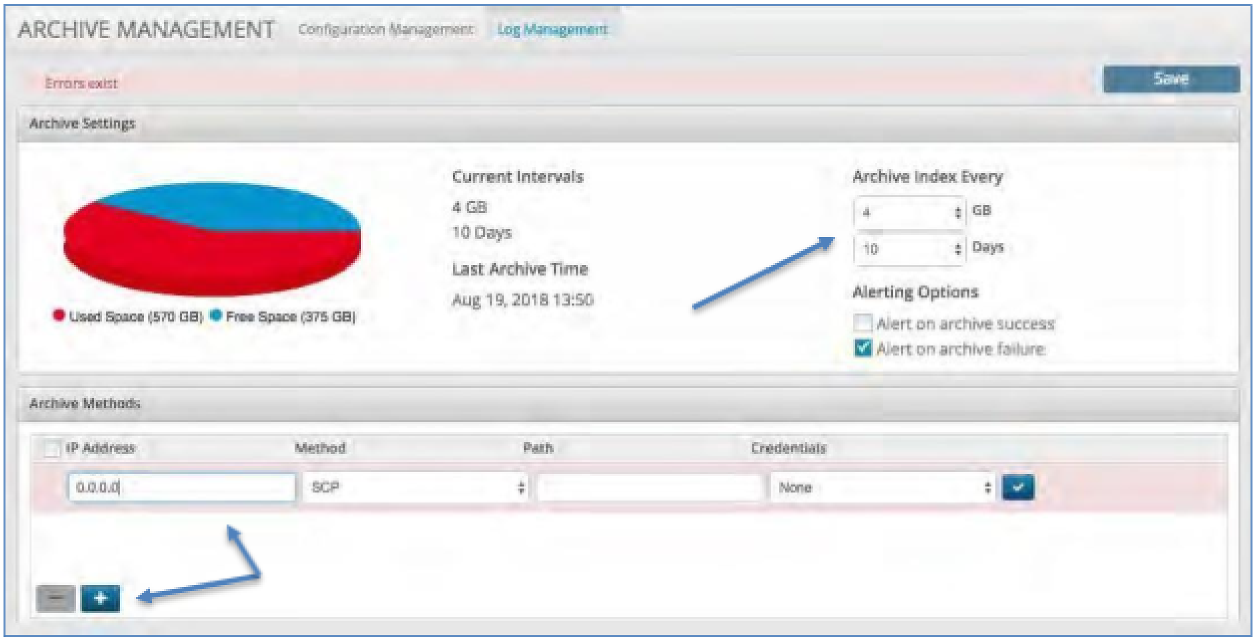
5.13. Log Management

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

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

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





Errors exist

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

☐ IP Address	Method	Path	Credentials
0.0.0.0	SCP		None

5.14. Tools

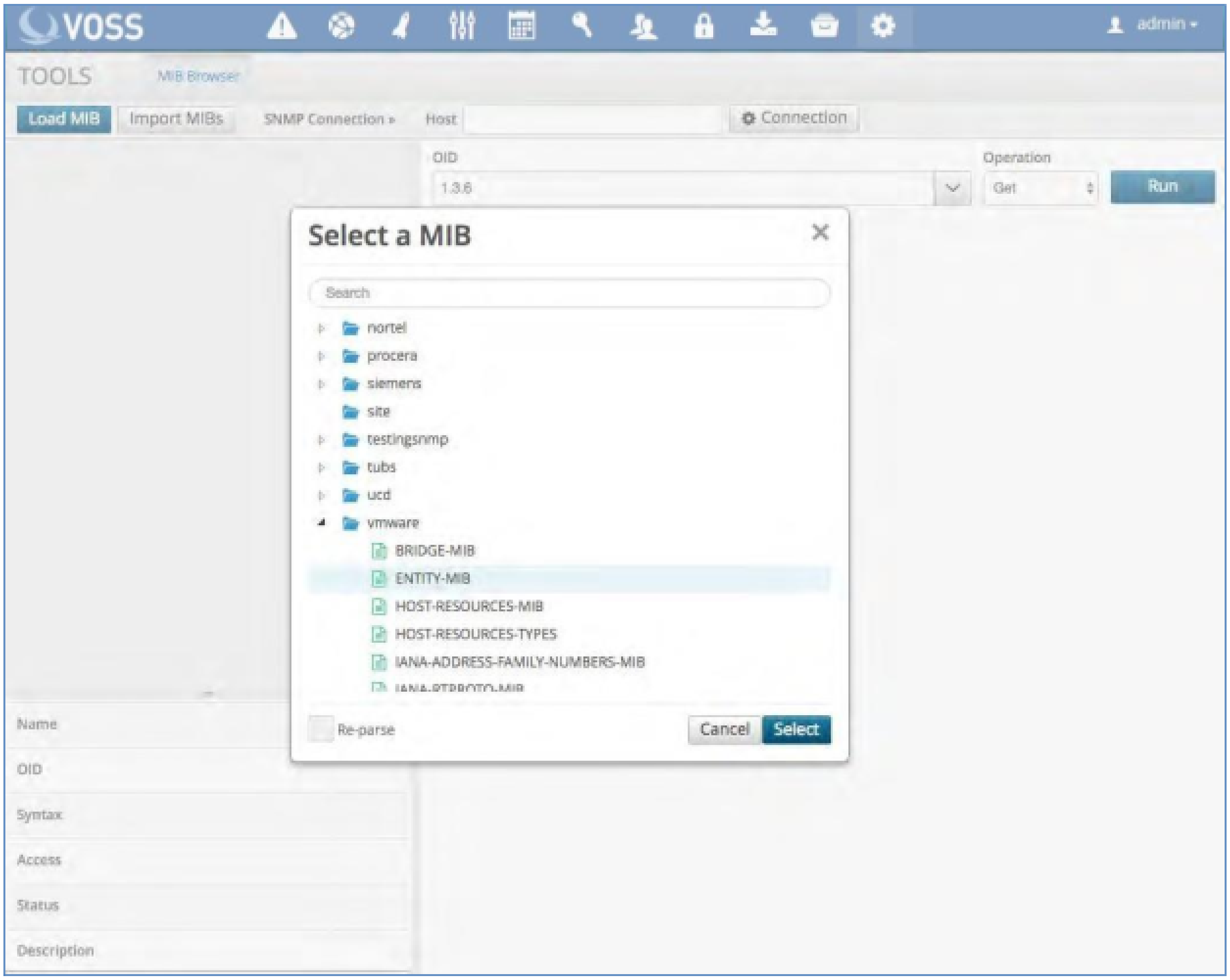
5.14.1. SNMP Tools

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

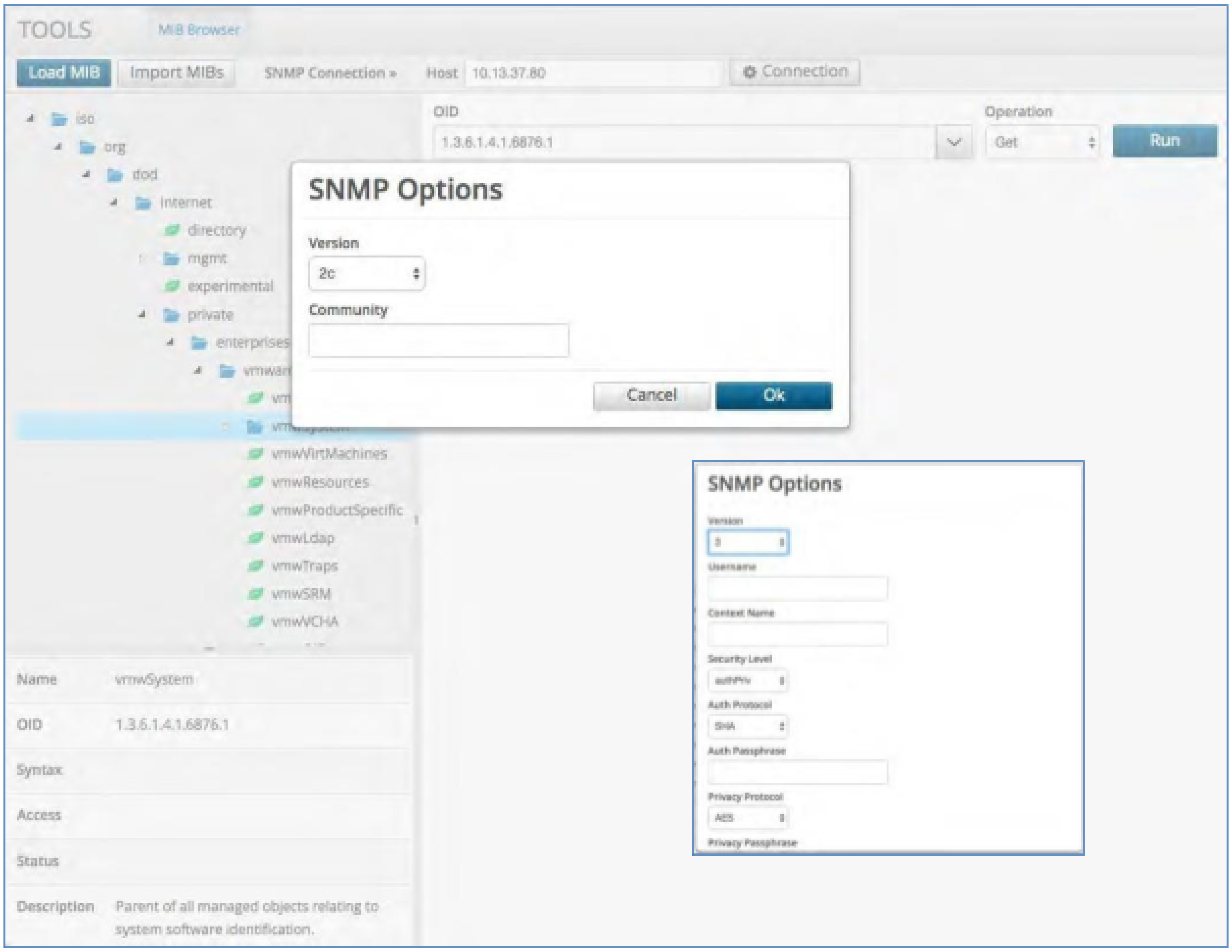
The system comes with a library of MIBs that can be opened by selecting the Load button. Click the Tools Tab:

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

3. Scroll through and select the desired MIB.



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



Host 10.13.37.80

OID 1.3.6.1.4.1.6876.1

Operation Get

SNMP Options

Version 2c

Community

Name	vmwSystem
OID	1.3.6.1.4.1.6876.1
Syntax	
Access	
Status	
Description	Parent of all managed objects relating to system software identification.

SNMP Options

Version 3

Username

Context Name

Security Level authPriv

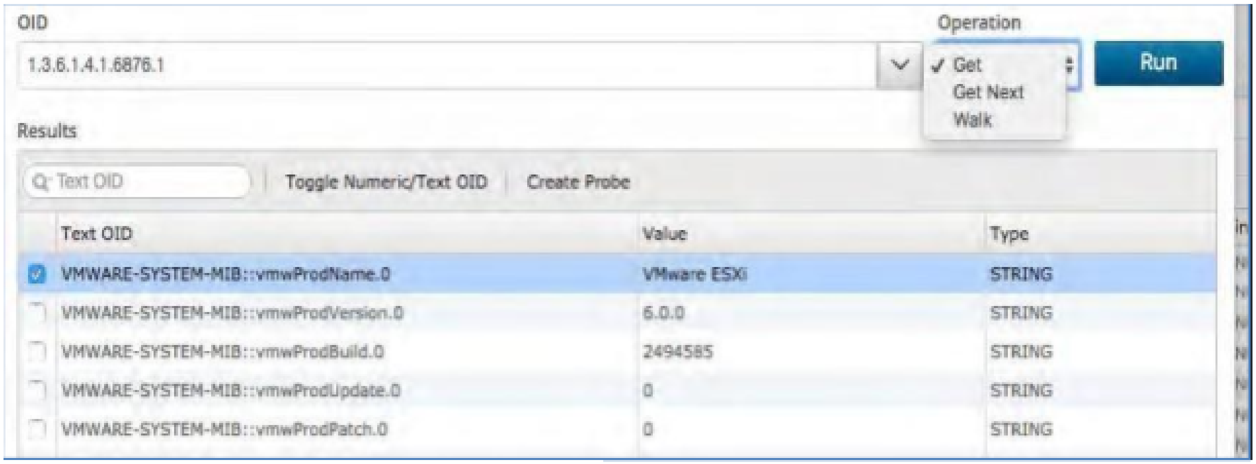
Auth Protocol SHA

Auth Passphrase

Privacy Protocol AES

Privacy Passphrase

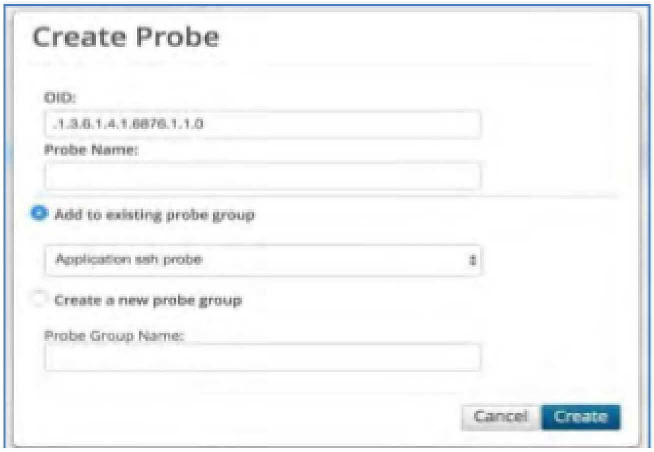
7. Choose the operation to perform: GET, GET NEXT or WALK
8. The operation will return the values of the OID you query in the field below it. Checking any of the boxes beside the field will un-gray the “Create Probe” box.
9. Do this for each Probe you want to create.



OID: 1.3.6.1.4.1.6876.1

Operation: ✓ Get

	Text OID	Value	Type
☑	VMWARE-SYSTEM-MIB::vmwProdName.0	VMware ESXi	STRING
□	VMWARE-SYSTEM-MIB::vmwProdVersion.0	6.0.0	STRING
□	VMWARE-SYSTEM-MIB::vmwProdBuild.0	2494585	STRING
□	VMWARE-SYSTEM-MIB::vmwProdUpdate.0	0	STRING
□	VMWARE-SYSTEM-MIB::vmwProdPatch.0	0	STRING



Create Probe

OID: .1.3.6.1.4.1.6876.1.1.0

Probe Name:

● Add to existing probe group

Application ssh probe

○ Create a new probe group

Probe Group Name:

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