

## Legal Information

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

DOCUMENT ID: 20241122150123

# Contents

1	What's New       1         1.1       Arbitrator Administration Guide: Release 24.2       1
2	Getting Started       2         2.1       Welcome to Insights Arbitrator       2         2.2       Arbitrator and Dashboard Licensing       3         2.3       License Auditing       6
3	Arbitrator Main Interface103.1Arbitrator Main Interface10
4	Configuration324.1System Configuration324.2Policy Configuration334.3Asset Configuration494.4Probe Configuration614.5Controls704.6Response Procedure Configuration724.7Credential Configuration724.8Customer Configuration794.9Access Control834.10Import & Export984.11Archive Management1004.12Tools1244.13Agent Configuration124
5	Arbitrator Maintenance1335.1Backup and Restore Arbitrator1335.2System Recovery1355.3Network Observability136

# 1. What's New

## 1.1. Arbitrator Administration Guide: Release 24.2

- EKB-12958: Allow a 7-day courtesy license on OVA install. See: *Arbitrator and Dashboard Licensing* Docs updated for the 7-day courtesy license applied on ISO install.
- EKB-20657: VOSS Insights ping probe does not forward to Consolidator. See: *Archive Management* Arbitrator docs updated for the new ping probe configuration functionality.
- EKB-20658: Kafka cleanup automation. See: *System Recovery* Docs updated for a new Kafka recovery option on the Arbitrator Admin menu.
- EKB-21117: Add cleanup of more Arbitrator db tables. See: *Archive Management* Updated the Archive settings for Arbitrator.
- VOSS-1277: Allow the forwarding of alarms via API to 3rd parties. See: *Response Procedure Configuration*

Added a note about updated support around forwarding alarms.

• VOSS-1388: Insights Agent improvements. See: Agent Configuration

Doc added for how to install and manage the improved Insights agent in Arbitrator, including creating and assigning profiles, and where to view agent data.

# 2. Getting Started

## 2.1. Welcome to Insights Arbitrator

#### 2.1.1. Overview

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

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

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

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

This guide covers the following:

- Main interface allows you to visualize the monitored systems and to manage alerts for these systems. The views within this workspace are constantly updating with newly gathered data.
- System Configuration admin users only, this is the workspace used to install and set up the platform.

#### 2.1.2. Conventions Used in this Guide

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

admin-users-only

## 2.2. Arbitrator and Dashboard Licensing

admin-users-only

#### 2.2.1. Overview

The VOSS Insights product and features are activated via a product key (license file) that is loaded on to every Arbitrator and Dashboard server.

### 2.2.2. Courtesy Product Key (License) on Install

When installing with an ISO file (new install), a 7-day courtesy product key (license) is automatically applied.

The courtesy product key allows you to log in and access the system user interface until you've received your official product key from VOSS.

You'll need to replace the courtesy product key via the **About** page within 7 days from install with your valid product key.

ABOUT		
Version 24.1.20		EDIT PRODUCT KEY
RELEASE	sp24.2	
PRODUCT ID	3Y9ED-RDH9A-439349Q09AX965888	
PRODUCT KEY	Courtesy license applied.	
DAYS LICENSED	7	
DAYS REMAINING	7	

### 2.2.3. Load Product Key (License)

To load your Insights product key (license):

- 1. Obtain the product key from VOSS.
- 2. Click the System Configuration (Cog) icon on the toolbar, then select About
- 3. Click EDIT PRODUCT KEY and replace the existing product key with the new product key.

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

## 2.2.4. Update Expired Product Key (License)

The VOSS Insights product key (license) contains an expiry date. You'll need to activate and add a new product key once the expiry date is reached.

- 1. As an admin user, log in to the GUI.
- 2. View the activation window, which displays the product key.
- 3. Copy the product key for each individual server.
- 4. Provide details to the VOSS representative.
- 5. The VOSS representative provides the product key to activate the server.
- 6. The admin user applies the product key on the server (Arbitrator and Dashboard servers), accepts the license terms, and clicks Submit.

PRODUCT REGISTRATION	
Enter your product key:	
I accept the End User License Agreement	SUBMIT
To purchase a new license, contact our sales department. <u>Voss Solutions</u>	
Provide this product id: 3 JTT-3 7R7X-PJ4EK	

## 2.2.5. View License Days Remaining

The days remaining for the product key (license) display in the UI when logging in, or via the **About** menu. You can enable or hide the **View License Expiration** setting from the **Permissions** tab in **Access Controls**:

≡ vo	> s s 🎎 🛛	« Back VOSS Ins	ights	۹	Search Dashboar	ds
Permissions	Users Roles	Customers SAML	Password Policy			
+ Perr	nissions					
						Delete Save
Reporter P	Permissions	Group name				
		Reporter Permissions				
		Permissions				
		Select All				
		View				
		View Application	View Search	Vie	w License Expiration	
		Action				
		Edit Dashboards	Edit Datasources	Edi	t Definitions	Edit Field Groupings
		Edit Reports	Edit Permissions	Edi	t Users & Customers	Edit SAML

View "license days remaining" via the About menu:

- 1. Click the System Configuration (Cog) icon on the toolbar, then select About.
- 2. View the DAYS LICENSED and DAYS REMAINING values.

Enable or disable display of "license days remaining" on the GUI:

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

Voss	🔺 🛞 🦨 iii	📰 🥄 🧏 🔒	📩 💼 🔅 Days remaining: 170
ACCESS CONTROL	Permission Groups Users Nodes	Realms Protected Subnets I	Password Policy SAML
Group Name	Realm Context	Timeout	
Administrator	(local)		2
ТурісаІ	(local)	<b>V</b>	2
Permissions Users			
	Ana	lytiX :: Correlate	
VIEW - Main Application	VIEW - Asset Explorer	VIEW - Alarm Analyzer	VIEW - Punq Search
VIEW - Asset Map Explorer	VIEW - Call Details	VIEW - Call Path Monitor	VIEW - License Expiration
ACTION - Delete Calls	ACTION - Delete Paths	ACTION - Disposition Alerts	

## 2.3. License Auditing

### 2.3.1. Overview

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

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

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

- data\_user\_view
- standalone\_count\_view
- meeting\_room\_count\_view

😑 voss 💭 data_user		cə 🖏 admin •
LICENSES		Days remaining: 305
CUCM USERS   CUCM_LICENSE_USER DATA_USER MSTEAMS Users   UNITY USERS   WEBEX Users		
+ Global Filters ( 0 applied )	Click to Refresh Data	Oct 2, 2023 12:00 am - Nov 1, 2023 10:14 am
DATA_USER_VIEW 👻 🕸	STANDALONE_COUNT_VIEW	MEETING_ROOM_COUNT_VIEW
DATA_USER_VIEW (Count)	STANDALONE_COUNT_VIEW (Sum)	MEETING_ROOM_COUNT_VIEW (Sum)
237	11	8

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

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

#### **Related Topics**

• License Tab

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

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

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

#### Before you start

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

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

#### Register and upload license file

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

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

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

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

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

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

API Config	Archive	Cisco SDL	Collect	Data Use	er Import	LDAP	License	Probe	Ртоку	SNMP	Syslog	Tunnel
											1	Save
License					Changes have	ve been mad	le to this con	figuration	tem			
					License							
					This screen n	nanages lice	nsing with V	OSS. This	screen ma	be used to	o enable the	periodic lic
					delivery to VC solutions.com	ISS. If applic	able, please	update fire	wall polici	es to allow	interaction	with platfor
					enabled	n. Additiona	ny, prease co	reigure pro	ky settingi	for excern	ai connectiv	nty, il neces
					false							
					Opt-in/Enab	ble the autom	natic sharing	of the lice	sø file.			
					organizatio	n id						
					adsf							
					The VOSS of	rganization	id associate	d with this o	fevice.			
					environme	nt type						
					productio	n						
					The VOSS a	eccount id (o	rganisation i	d) associat	ed with thi	device.		
					description							
					A descript	tion						
					A description	on of this de	vice.					

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

#### Alternative steps:

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

## **Related Topics**

• Archive Management (Proxy) in the VOSS Insights Arbitrator Administration Guide.

# 3. Arbitrator Main Interface

## 3.1. Arbitrator Main Interface

#### 3.1.1. Overview

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



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

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

#### **Related Topics**

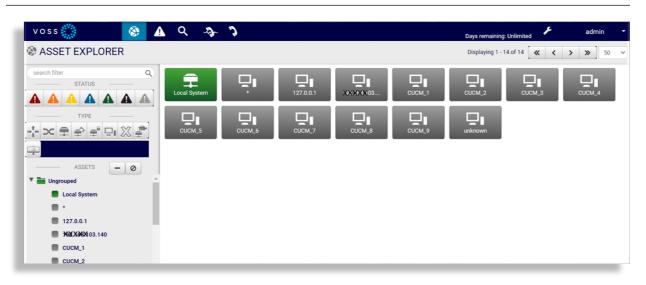
• System Configuration

## 3.1.2. Asset Explorer

#### Overview

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

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



#### **Asset Alert Severity Status**

Assets display the color of the current highest-level alert for that asset in the system. Color coding is used to indicate the alert severity status of each asset:

sear	ch filte	ATUS	Norma		C
	A	A	Å	A	

· Critical (Red)

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

#### **Assets Search Filter**

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

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



#### **Asset Details**

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

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

- Alerts
- · Probes
- · Search

#### **Asset Details - Alerts Tab**

The **Alerts** tab displays all alerts associated with the asset and allows you to disposition, add alert journal entries for the alert, and see a report of the alert and events.

(See Alert Disposition, Alert Journal and View Report within the :ref:`arb-alert-analyzer`section)

ē	A.40	Unknown 10, 13, 37, 43 Unknown Unknown	HOSTNAME 10.15.37 TINEZONE Unknow VENDOR Unknow MODEL Unknow	DESC	REASON Unknown									
-	LEATS 10	PROBES Q	SEARCH											
							De	daying 1 - 10 at 37	æ	< >		10 0	0.6	STATUS
	DATE	NODE	POLICY	NAE	STATUS	OWNER								
	DETAL	PERENCE ID 21 NODE 01 POLICY C	Phys. 5		START OTO LAST CHANGE - ELAPSED TIME O DI ENT ESCALATION OTO							VE	W REP	ORT
		STATUS	OPEN •	RESPO	EXPINES IN 000	8.40								
4	27/09/18 11/08/21 AM		OPEN .	Ortical Cardo E	NEE PROCEDURE DAY	8.40								(8
•	070918	STATUS ESCRIPTION - departs Ontoni Crean I	OPEN .	Ortical Disco 5	INST OPEN	Unassigned				- Charth	1000-JETS	( Jacobia	rybos	(8)
•	07/08/18 11:08:21 AM	STATUS ESCRIPTION - departs Ontoni Crean I	Cherr Alers - Universal	Ortical Disco 5	INSE PROCEDURE DAY	Unassigned				Stan	area	("Second	ration	-
<b>A</b>	CTICANS TTORICS AND OUTPUT: CTICANS	STATUS ESCRIPTION - desparts Oncol Cases I JAIPTORES desparts Mage Cases II DeviceMarrie	Checo Alleris : Drevenuel Checo Alleris : Drevenuel Dreve (x10-xx1 & 2018 16:08:01 In Sun Junite 11:08:21 (CDT 20	Ontonal Dates & 16.13.37 AD -c1850-4 (6, seer RTM/TSensis Mager Cauto for 0.13.37 AD -c1780-40 mc172, 16.117[Press	INFOCEDURE Des Inscr OPES InfoceDes Clones Infocedes Invested has or OPEN Infocedes InfoceDes Infocedes InfoceDes Infocedes InfoceDes Infocedes InfoceDes	Unansgred Unansgred Separatech Iom Jul 2010 Unansgred Unansgred PC2 Jepartech Iom Jul 20 20	Active of Classo Tomose	Ret Application(a	136.00	ont.heat	interest %			(8
A A	CTION/18 11:08:21 ANN OUTPUTE CTION/18 CR:25:15 ANN	STATUS ESCRIPTION - desparts Oncol Cases I JAIPTORES desparts Mage Cases II DeviceMarrie	Cardo Alarto - Dimensial Deser Julio Alarto - Dimensial Deser Julio Alarto - Dimensial Cardo Alarto - Dimensial mar (utilica) & 2018 142 25:15 1 - Gardo Alarto - Dimensial	Ontonal Dates & 16.13.37 AD -c1850-4 (6, seer RTM/TSensis Mager Cauto for 0.13.37 AD -c1780-40 mc172, 16.117[Press	NER PROCEDURE Des Ner OPEN Instructure des CLOMIG Instructure des CL	Unansgred Unansgred Separatech Iom Jul 2010 Unansgred Unansgred PC2 Jepartech Iom Jul 20 20	Active of Classo Tomose	Ret Application(a	136.00	ont.heat	interest %			(8

#### Asset Details - Probes Tab

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

ASSET DETAILS = 10.1	3.37.43		¥ CLO
ALERTS ALERTS	HOETNAME 10.13.57.43 TIBEZONE Unecom VENCOM MODEL Unecom MODEL Unecom	VERSION University DESCRIPTION	
Truns Activity Call Manager RTMT Request Call Activity Call Manager Service Gammay Activity CPPU and Memory	Batas 200 «Deni sensori 1 STD-dhaGay Terestenyo-1 S2001 (41) Standikura-1 (234) Suhrain Sandikura-1 (234) Suhrain Mesensyaki (234) Percensyaki (234) Percensya	nds to tend & request to https://16.11.57 45/tap/A5/hapi.d1/Cer/McCanedintol/htms-ge/Cpu/rol/HerroryRepart additation Refundades: ** Called by Back ** 2000*** Refundation *** 2000******************************	k64" Total/Option="10128812" Total:Total/Instantiage(Jand="22" Percentage(Jand="2" Recentage(Jand="2" Recentage(Jand="2" Recentage(Jand="2") Recentage(Jand="2") Recentage(Jand="2")

#### **Asset Details - Search Tab**

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

ASSET D	ETALS = 10.13.37.43	LOSE
	TYPE Unicoun HOTTLAME 15 (3.37.45 VERSON Unicoun P 15 (1.37.45) TEREZON Unicoun DESCRIPTION ALLS Unicoun HEXICOL Unicoun MAC Unicoun HODEL Unicoun S _^PROPER 0, BEARD	
1	Last 24 Hours -	٩
	Displaying 1 - 10 of 221,014 events + Toor provi next last + 1	10 0
andere In SLEE Aw	<pre>sparkageContent is'1' same"'sallista''&gt; slameLage Expr":12:13:13-13-14 ibil:12:'' stansing Expr":13:13:13:'' stansing Expr":13:13:13:'' stansing Expr":13:13:'' stansing Exp":13:13:'' stansing Exp::13:'' stansing Exp::13:'' stansing Exp::13:'' stansing Exp::13:'' stansing Exp::13</pre>	-
070818 11.53 17 AM	C1D201 8 2018 16:01:40 10.13.37.71 604 (100) 2010-07-00101010-05-00 Ph-500.Lapertoch.com > = = 1,2010/07/08 11:51:10.00401015600.7002707.eod.2014.2010/17/08 11:51:00.00401015600.7002707.eod.2014.2010/17/08 11:51:00.0010000000000000000000000000000	-
	Huand(15)27 Pund(15)2720334 Metuolog.galig	
-	11:51:37,39737,1,42172,123,4550,123,0s40053,asp.allow,430,340,270,7,2018/07/04 11:51:04,2,any,6,2207257880,0a0,10.0.0.4-10.255.255.255.255.051ad States,0,4.3,apd-	-
11.52 17 AM	eut.0.0.0.0., #8-900_Erom-pmliey0., 0., N(8.0.0.0.0.)	

## 3.1.3. Alert Analyzer

#### Overview

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

NJBB P	- 50	• 19	BULK DIS	POSITION . ST	ATUS -				
		DATE	NODE	POLICY	RAE	614708	OWNER		
	•	DE DE STOPHE	1, <13×3x1 NUC_RENT-1- HTMTHemmion value of 21 2018 17×16× HTMT_ALERTY HTMTSemmion	7 2018 17:58:48 10.13. -R797_ALBET: V[Alertian substandeffictualed has 16912 which is over hi 168 10.13.27.461 (1895) • (Alertiane-Strengthered substances)	37.44: *185+161904: ; er=27%TiessionsTateedat accured. Counter Resai gh threahold 2102(App 61906: ; i 112181: em instancedsThreahold () occured. Counter Resai	: 112101: euseil. Troosholdjjklartbe insaketive of Class ID-Class ARE Beryi mil.layerstach.co Klartbetall- On De ionsketive of Class	sage intempting Control Net Layerstack.com/ 04/19/201 compared to the set of the set compared to the set of the set compared to the set of the	18 05:56:44 PM.372 UTC 144 CDT 2010, slort mat) on node 15.13.37.4 Melli: MTMT Alert', 41 8.372 UTC : Not_MCMT-1- 6, slort Mat] on node 10.13.37.4	a haa bobul 7
		DETAUS	.0	URNALS				VIEW	V REPORT
				Cisco Alerts : Universal Circual Cisco Error		APSED TINE - BCALATION DISTRICT	03:01:30 PM		
			STRTUS	OPEN -		DOMES IN Expert INCCEDURE Delate			
		010118 010128 PM	STRTUS	OPEN					
		CTOTAS CLOL28 PM OUTPUT		CHEN IF HE	Cash al tas	OPEN	Descynt		
	*	010118 010128 PM	STRTUS BORFTON	0701	RESPONDE	NOCEDURE Dubuit			
	A A	CTOTAS CTOTAS OUTPUT		CHEN IF HE	Cash al tas	OPEN	Descynt		
	A A A	orome cloude PM ovmut chome cloude PM		CHEN IF HE	Cash in we	OPEN	Descynt		
	A A A	CTOTING CLOLOS PM OVTPUT: CTOTING CLOLOS PM CLOLOS PM OVTPUT: DTOTING	angan degan degan degan degan	Crept al test Casts al test Casts HCB PCA Casts Rosts Universi Cherr (c1bull / 2018 18/022	Cash al tes Cash al tes FINIT, ALERT d Ortical Case Ever In 16133742 eteb-7805	OPEN OPEN OPEN OPEN	Descyred Descyred Descyred		(
	A A A	CTOTAN CLOLES PM OUTPUT CHOTAL CLOLES PM OUTPUT DOUTPUT CLOLES PM	angan degan degan degan degan	Cesh al wa Cesh al wa Cesh HOB PCA Ceso Kots Universit Chru (chual / 2014 1902)	Cash al tes Cash al tes FINIT, ALERT d Ortical Case Ever In 16133742 eteb-7805	OPEN OPEN OPEN OPEN	Dreasgred Dreasgred Dreasgred Dreasgred		(
	A A A	Create Create OWTPUT Create Cr	STATUS SCRIPTON Began Segan Segan Chos Date Tamos Vet	CHDS Cech at less Cech at less Cech HCB PCA Cech Alors : Drever Dreve (-Chu Jal 7 2014) 1602 (-Threshouth Church Theat Application(ant)	Costn kit we     Costn kit we     FINIT_ALEPT     Critical Dates Enver     It 15:1337.43 critic-2005     set Jun	OPEN OPEN OPEN OPEN SATO COCHICAN DI SATO COCHICAN	Disasgred Disasgred Disasgred Disasgred settert. 34 07 2016 (18:02-20) ant RTMT Sesternitizaset/Theor		MT, ALBRY S HELITARDIN D
	A A A A	Chenny Charles Print OwnPublic Charles Print OwnPublic Charles Print OwnPublic Charles Print OwnPublic Charles Print OwnPublic Charles Print OwnPublic	STATUS SCRIPTON Began Segan Segan Chos Date Tamos Vet	CHDS Cech at less Cech at less Cech HCB PCA Cech Alors : Drever Dreve (-Chu Jal 7 2014) 1602 (-Threshouth Church Theat Application(ant)	Costn kit we     Costn kit we     FINIT_ALEPT     Critical Dates Enver     It 15:1337.43 critic-2005     set July	OPEN OPEN OPEN OPEN SATO COCHICAN DI SATO COCHICAN	Disasgred Disasgred Disasgred Disasgred settert. 34 07 2016 (18:02-20) ant RTMT Sesternitizaset/Theor		MT, ALBRY S HELITARDIN D

#### Disposition

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

The table describes the options for alert dispositions:

Option	Description
Open	Default status for a new alert.
Under Review	The assigned owner is working on the alert.
Acknowledge	Alert has been seen, but is not currently being worked on.
Release	The assigned owner has released the alert to be worked on by others.
Close	The alert has been resolved, but the alert journal can still be edited.
Disregard	The alert is deleted from the system.
Close + Lock	Alert has moved to a Closed state and the alert journal cannot be edited.

#### **Disposition a Single Alert**

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

FLIERS	1 3	• TROS	BULK DR	sposition . St	ATUS *			
		DATE	NODE	POLICY	NALE	814748	OWNER	
	-		pab.dimens Service op	ional.com- Jul 08 2018 erational status is DDM	12+01+37 PR.154 UTC S.FULDCIAGO CallMan	+ NOC_RONT-2-RONT_A	256.5.26: <106205885: : : 2015 E297: 4(AlertHame-CriticalDervi a generated on But 2w1 04 07:01 ode22-eachdr-v-erm-pub): KTMT Al	nebownijskiertbetall-Milz (8) (
		DETALS	5	DURVALS				VIEW REPORT
			HODE POLICY RULE	2000-0100005-00-01-38644 deeparb Cisco Alerta: Universal Ottical Cisco Error Unessigned		START CROAME - LAST CROAME - ELAPSED THE - T ESCALATION ERISTS EXPIRES IN Expired		
			STATUS	OPEN .	RESPONS	E PROCEDURE Delast P	*	
			ISCAPTION	UNDER REVIEW ACKNOWLEDGE				
	4	010815 010225 AW	despart	RELEASE		OPEN	Unansigned	
		OUTPUT	(most)	DISREGARD		OPEN	Uramignet	
		07:02:38.494		CLOSE + LOCK			the second s	2:37 PM.431 LTC : SUC_RTMT-2-
	1	OUTPUT:		AT Scherthame-OrticalSenie	sCowrijAierDetail-4012	Service operational status		e siert is generated on Sun Jul DE 07:02-07
			RTMT_ALE	AT Scherthame-OrticalSenie	sCowrijAierDetail-4012	Service operational status	a DOWN #012Circle Califirmager #012Th	e sier is generated in Sun Jul DE (Fill 2)

#### **Bulk Disposition Multiple Alerts**

This procedure dispositions a group of alerts at once.

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

#### **Filter by Disposition**

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

PETERS	1	* 1908	BULK DR	ercemon +	STATUS .			
Test E		DATE.	MODE	POLICY	Cipen .	STATUS	Owner	
		A	decado	Case Alerts	Creber Review Actorowiedged Reteremit	OPEN	Unampred	
		007		e Error (+13-Jul 8 2018 PT: %/HertName-Critic in note adds ++com-put	Cinet		om publidmanelonal aten: Au 08 2016 01 10:07 is DOMR.#012Class-CallManager.#012The all [Node/D-astdo +-com-pub] #7547 Aler()	
		A 0000	na degato	Caro Alerts 1	CANCEL OF CARE	OPEN	Unanigred	
		007	Put Crical Case		13 14 44 13 13 37 44 +180-186719 IntEntal- Number of Authentication? pl are 2 Authentication? plind events (up to		ventextucions. Jul 18 2018 21 14, 44 PM-363 UT configured threshold during configured interval	C I NUC, RIMITERIME, ALEREI N. d'Eme 1 witter 3 minuter/C12 on chat

#### **Filter Manager**

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

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

FILTER MANAGER				✓ SAVE	# CANCE
+ ADD - REMO	WE	KEYWORDS DEV	ERITY DATE & TIME		
Test Trea is a test ther	ALLOW DIBREGARD	NAME	Test		
		DESCRIPTION	This is a test filter		
		POLICY			
		PULE	Critical Cisco Error		
		GROUP			
		CUSTOMER			
		SITE			
		NODE			
		MESSAGE			
		OWNER			

- · On the Severity tab, select one or more severity states:
  - Active: Alert is currently in one of the active states
  - Escalated: Alert has been escalated based on the timer in the correlation rule
  - Acknowledged: Alert is in an acknowledged disposition state
  - Expired: Alert has expired based on the timer set in the correlation rule

+ ADD - REMOVE	KEYWORDS	SEVERITY	DATE & TIME		
Test DisRegard ALLOW DISREGARD	Þ	ET ACTIVE	1 TECALATED		() EXPARED
	A CRITICAL		2	2	2
	A MAJOR		2		
	A MINOR				
		NAL 🖬			

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

FILTER MANAGER		✓ SAVE	* CANCEL
+ ADD - REMOVE		KEYWORDS SEVERITY DATE & TIME	
Test This is a test titler	ALLOW DISREGARD	DATE START DATE END DATE	
		TIME ALL DAY HOUR MINUTE HOUR MINUTE START 0 me 0 me End 0 me 0 me DAY OF WEEK SUNDAY MONDAY MONDAY MEDNESDAY MEDNESDAY MEDNESDAY MEDNESDAY MEDNESDAY MEDNESDAY MEDNESDAY MEDNESDAY	

#### **Alert Journal**

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

#### Add an Alert Journal

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

FILTERS	1	50	RT .	BU.	UK DISPOSITIO	N * S1	ATUS *							
Test			DATE	NODE		OLICY	RULE		STATUS		OWNER			
		•	07/08/18 12:00:40 PM	H H 20 HTHE_A DONG.# ABLGO-	3794: astdo LEN7: %[Ale 012Cisco Ca	rur : Crilcal Ci -v-com-pub-dimen rtNama-Critical llManager.#01211 imensional.com.;	sional.com: Ju erviceDown)[A1 # alert is gen	al 00 2018 05:0 ertDetail-#013 wrated on Dun	01:37 Pm.410 Service of Jul 08 12:0	peration	WOC_R soal st	tus is a on no	G	0:
			DETAIL	8	JOUFMALS	4. T					VIEV	REPO	AT.	
			THESTAMP		CREATOR	ACTION								
			07/06/18 12:	45:36 PM	system	devparb(127.0.0.1 <186x205881 %UC_FITMT-2-RT operational status 12:00.57 CDT 20	Iponse: Default IVI () - Ortical Claco El 200794. astdo-v-co TMT_ALEITT: NJAle Is DOWN #012Cla I8 on node astdo-v (D-astdo-v-corr pu	inor : Orlical Oscol on pub.dimensiona etName-OrlicalDe co CalManager #0 -con-pub.dimensio	Error (<13×Jul 1 Loom: Jul 08 2 nviceDown[[Aia 112The allert is	8 2018 1 018 05 0 mDetal- generate	17:00:40 10:27 PM 4012 Se 1d on Sur	A10 UTC NOS		
			07/06/18 12	45:37 PM	system	Incident Response	- Method ALERT	Status: Success						
			07/06/18 12	45.37 PM	maters	Incident Response	- Method CONTR	NOL Description N	New Vodatone (	Cormol.	Status: 5	LOORES		
			NEW JOURN	AL ENTR	¥					CLI	RAS	A00		
			07/08/18 12:00:40 PM	despa	•	Disco HCS PCA	RTMT_AL	ERT	OPEN		Unessig	red	0	0
			OUTPUT											

#### **Alert Sort**

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

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

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

FILTERS	1	SORT +	BULK D	SPOSITION . STATU	IS *			
Test		TIME TO EXPIRE/E	SCALATE	ASCENDING DESCENDING	~~	STATUS	OWNER	
		ALERT SEVERITY		ASCENDING DESCENDING	~ ~	Error OPEN	Unessigned	0
		ALERT DATE & TIM	E	ASCENDING DESCENDING	C. C	»206881::: 203794: astdo-v-oo N/AlertName=OnticalServiceDo et is generated on Sun Jul 08 1 DuaterID=[NodeID=astdo-v-co	wn[[AlertDetail-#012 S 2:00:37 CDT 2018 on r	Service
		12:00:40 PM				T OPEN	Unassigned	6
		OUTPUT:						
		A 07/08/18 12:00:52 PM	devparb	Catch all test	Catch all test	OPEN	Unassigned	6
		OUTPUT:						
		C7/08/18 12:01:53 PM	desparb	Catch all test	Catch all test	OPEN	Unassigned	6
		OUTPUT:						
		C7/08/18 12:02:03 PM	devparb	Cisco Alerts : Universal	Critical Cisco	Error OPEN	Unassigned	6
		OUTPUT:	2018 05:00 [lssuerCN/	co Error (<13-Jul 8 2018 17:02:03 18 2:03 PM:181 UTC : %UC_ICSA-2-IC ASTDC-V-CCM-PUB[[ErrorCode+2] cluster Sync Agent service detected	SACertificateValid (AppID=Cisco Inte	ationFailure: %(SubjectCN=AS) arcluster Sync Agent[(OusterID	IDC-V-CCM-PUB] -[NodelD-astol-v-imp	
		A 07/06/18 12/02/07 PM	devparb	Cisco HCS PCA	RTMT_ALER	T OPEN	Unassigned	6
		OUTPUT:						
		A 07/08/18 12/02:57 PM	devparb	Catch all test	Catch all test	OPEN	Unassigned	6
		OUTPUT:						

## 3.1.4. Search

#### **Overview**

Arbitrator's main interface provides the following search options:

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

#### **Event Search**

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

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

#### **Simple Search**

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

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

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

9. SEAR	
25.000	
23750 25	
-	Last 24 Hours +
	Displaying 1 - 10 of 3,208,343 events + that prev next last - v 1
0100-18	<10-32. 9 2018 14:17:07 geordi: 09-322018 14:17:07.084 client: debug 3: client 192.169.103.115945690 (29.02136.vpmen.com): view Internal: mendto inscing apping
0705/18 14.51.12 PM	Invalid RMLs coll
And all the second seco	<13>241 9 2018 14:17:07 geordi: D9-241-2018 14:17:07.084 client: debug 3: client 182.168.103.113445680 (29.or136.voxeo.com): view Internal: mend Inter-182.988 92:05 2 2019 14:17:02:04 Intercolog_apping
07/09/18 14/51:12 PM	<pre>4180-01 # 2018 19:34:23 Lepers-security-listener: LEL-cons 1531164853.049378 (j3sb#14TmaltEngPe 10.10.10.223 41225 0.0.0.5 53 udp dos 0.057516 37 77 87 - 0 06 1 65 1 105 (409ty) Han-60702220 Patr-554 Hartal-sping</pre>
076915 143112 PM	<pre>gydytime "32:15:31:18.51", enterprises.5265.2.1.3.1.109:1365 , enterprises.5205.2.1.3.1.101:19 , enterprises.5205.2.1.3.1.102:"2018/07/09 14:144:18", enterprises.5205.2.1.3.1.101:"00:00:0.00", enterprises.5205.2.1.3.1.104:"avg", enterprises.5205.2.1.3.1.102:"2018/07/09 14:144:18", enterprises.5205.2.1.3.1.101:"00:00:0.00", enterprises.5205.2.1.3.1.104:"avg", enterprises.5205.2.1.3.1.101:"100-01", enterprises.5205.2.1.3.1.101:"00:00:0.00", enterprises.5205.2.1.3.1.101:"00:00:0.00", enterprises.5205.2.1.3.1.104:"avg", enterprises.5205.2.1.3.1.101", enterprises.5205.2.1.3.1.5.100", enterprises.5205.2.1.3.1.104:"avg", enterprises.5205.2.1.3.1.51", enterprises.5205.2.1.3.1.51", enterprises.5205.2.1.3.1.101", enterprises.5205.2.1.3.1.51", enterprises.5205.2.1.3.1.51", enterprises.5205.2.1.3.1.101", enterprises.5205.2.1.3.1.51", enterprises.5205.2.1.3.1.51", enterprises.5205.2.1.3.1.51", enterprises.5205.2.1.3.1.51", enterprises.5205.2.1.3.1.51", enterprises.5205.2.1.3.1.51", enterprises.5205.2.1.3.1.51", enterprises.5205.2.1.3.1.51", enterprises.5205.2.1.3.1.51", enterprises.5205.2.1.3.1.51", enterprises.5205.2.1.3.1.51", enterprises.5205.2.1.3.1.51", enterprises.5205.2.1.3.1.51", enterprises.5205.2.1.3.1.51", enterprises.5205.2.1.3.1.51.51", enterprises.5205.2.1.3.1.51", enterprises.5205.2.1.3.1.51.51", enterprises.5205.2.1.3.1.51", enterprises.5205.2.1.3.1.51.51", enterprises.5205.2.1.3.1.51", enterprises.5205.2.1.3.1.51.51", enterprises.5205.2.1.3.1.51", enterprises.5205.2.1.3.1.51.51", enterprises.5205.2.1.3.1.51", enterprises.5205.2.1.3.1.51.51", enterprises.5205.2.1.3.1.51", enterprises.5205.2.1.3.1.51.51", enterprises.5205.2.1.3.1.51", enterprises.5205.2.1.3.1.51.51", enterprises.5205.2.1.3.1.1.51", enterprises.5205.3.1.3.1.51.51", enterprises.5205.3.1.3.1.51.51", enterprises.5205.3.1.3.1.51.51", enterprises.5205.3.1.3.1.51.51", enterprises.5205.3.1.3.1.51.51", enterprises.5205.3.1.3.1.51.51", enterprises.5205.3.1.3.1.51.51", enterprises.5205.3.1.3.1.51.51", enterprises.5205.3.1.3.1.51.51", enterprises.52</pre>

#### **Keyword Search**

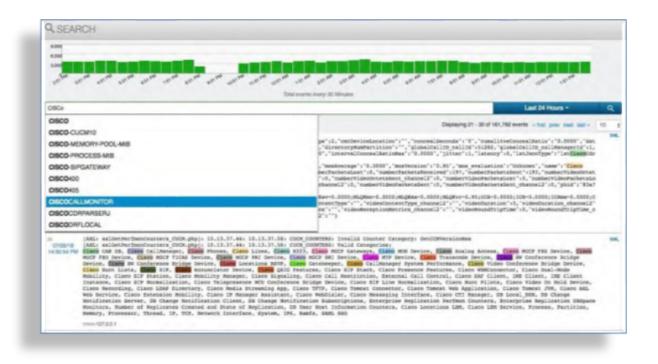
To perform a keyword search across all logs based on the default time of "Last 24 Hours":

1. Fill out a word or part of a word that you know is present in your data, such as "Cisco".

The event search auto suggests a keyword as you type, based on data the Arbitrator has collected.

- 2. Press Enter to select the auto-suggested word, or click the Magnifier icon to run the search.
- 3. View search results, which displays all log data from the past 24 hours that contains the specified criteria.

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



#### **Use Operators with Search**

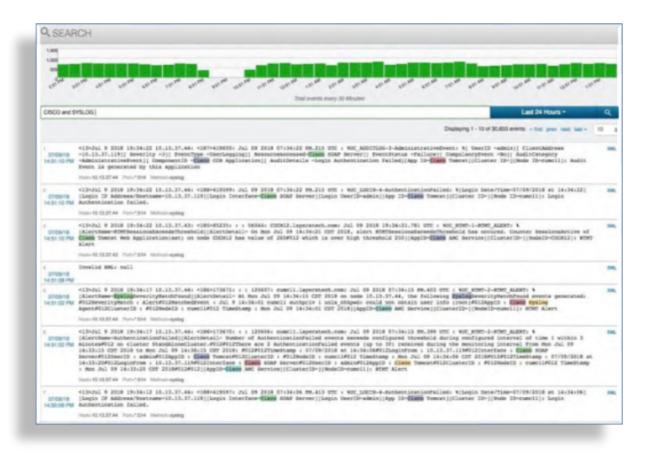
The Event Search allows the use of operators (AND, OR, NOT) to combine keywords that you know are present in your data for a more granular search. A search with operators searches across all logs based on the default time of "Last 24 Hours".

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

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

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

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



#### **Date Range Search**

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

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

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



#### Search Result Metadata

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

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

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



## 3.1.5. Call Path Monitor

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

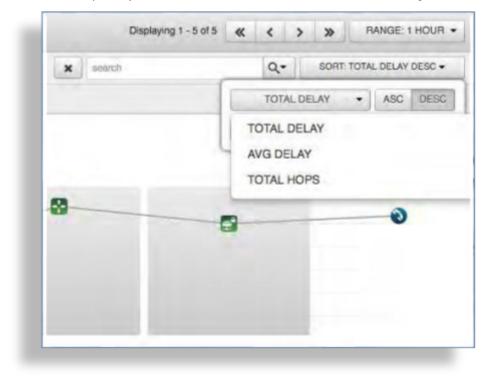


#### **Sorting Call Paths**

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

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

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



#### **Call Path Time Range**

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

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

admin	Days remaining: Unlimited		<u>ک</u>	ર	<u> </u>	$\otimes$	•	voss 🎇
RANGE: 1 HOUR	No records					OR	ATH MONI	
ALL	Q. st	search	•					
1 HOUR	#CALLS LAST CALL	AVG DELAY HOPS	DELAY	THOD	M			PATH
1 DAY 2 DAYS								
3 DAYS								
4 DAYS								
5 DAYS								

#### **Expanded Call Path View**

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

To expand a call path and toggle between graph and table views, click the arrow adjacent to the relevant call path.

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

				A wath	Q.* SDRT TOTAL DELAY DESC
D PATH	METHOD	DELAY DELAY HOPS ACA	LS LAST CALL MAD	15	
JULAS-RTR-1-ett Q	NO ASA LIN	663.00 94.36 6 2	070916 0421.55 PM		Latency by Hup
a <sup>2</sup> m					INVERT IN 12
-		9	-	8	a 0
LIXLAB-RTR-1 4651	un	N2.00 33.07 5 5			
LIXLAB-RTR-1-sets	LEI	42.00 33.92 5 4			OR INSTRUCTOR
			1990-1912 PM		
LUCLAB-RTR-1 etht == LUCLAB-RTR-4 etht == A m crocts == B = 1	ADDRESS	ASSET NAME	LATENCY	ATTER	ON NETWORK
USLAB-RTR-1-etti     USLAB-RTR-1-etti     USLAB-RTR-1-etti     OFODER     OFODER	ACCRESS 12.16.1.11 (Endport)	ASSET NAME	CTOBITE DECISION 4	JITTER	ON NETWORK TRUE
USLAB-RTR-3-end     USLAB-RTR-4-end     CROEN     CROEN     CROEN     CROEN     T     T     T     T	P ADCINESS 72.16.1.11 (Endpoint) 72.16.1.1	ASSET NAME	LATENEY 2.05	4775A 0 0	ON NETWORK TRUE FALSE
LXLAB-RTR-1-e81     LXLAB-RTR-4-e81     LXLAB-RTR-4-e81     CROER     C	P ADCRESS 72 16.1 11 (Endport) 72 16.1 1 72 16.2 1	ASSET NAME - UKUAB-RTR-1-emi UKUAB-RTR-2-emi	CTIGSHESEKONS 794 42 0 2.85 7.87	2000A	ON NETWORK TRUE FRUSE FRUSE

### **Searching Call Paths**

Each call path has several fields you can use to search and filter for a relevant call (one or more).

- · Source
- Destination
- · Method
- Hops



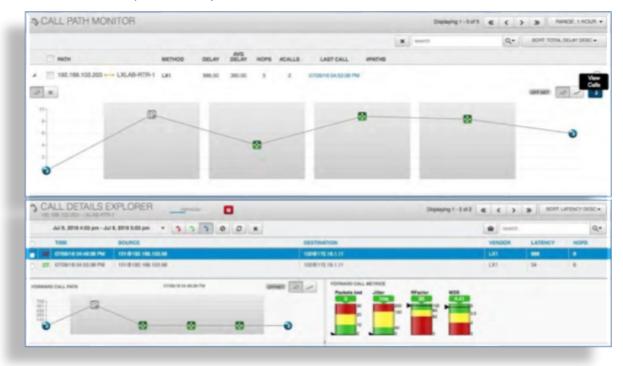
#### View Call Details from the Call Path

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

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

## 3.1.6. Call Details Explorer

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



#### **Call Details Explorer Toolbar**

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

voss 🎇	🛞 🛕 Q 🤘	<u>ک</u>	Days remaining: Unlimited 🔑 admir	1 <sup>-</sup>
CALL DET	AILS EXPLORER	н 🕕	No records ( 🕻 💙 🚿 SORT: LATENCY I	ESC 🕶
Apr 22, 202	24 5:53 pm - Apr 22, 2024 6:53 pm 🌖	<i>&gt; ~</i> 0 3 ×	search	Q

Element	Description					
Filter by date and time	The date and time calendar allows you to search call details for a spec- ified date and time range. You can select a date and time from the calendar, or select from a range of predefined options, from Last 5 Minutes, to Last 12 Months, or for the previous hour, day, or week.					
Filter by call quality	The Phone icons allow you to filter your data to view only good calls, only bad calls, or view both good and bad calls. <ul> <li>Bad Calls (Red)</li> <li>Good Calls (Green)</li> <li>Bad and Good Calls (Blue)</li> </ul> CALL DETAILS EXPLORER Calls Apr 22, 2024 5:53 pm - Apr 22, 2024 6:53 pm Last 5 Minutes Apr 2024  Apr 2024					
Clear Filters	Removes all applied filters and displays call details in the default display mode.					
Update	Applies a predefined refresh timer to the page. Click <b>Update</b> to request new data, on demand.					
Delete Selected Calls	Deletes any call selected on the page.					
Refresh, Play, or Pause Data	Click the Pause/Play icon to pause or restart the data refresh cycle. This is useful when reviewing a specific call.					
Sort	<ul> <li>Provides the following sort options for call details. You can sort by:</li> <li>The time the call was placed</li> <li>The source that placed the call</li> <li>The call destination</li> <li>The vendor, which identifies the method that created the call. The only options are LX1 (the VOSS Raptor Call Path generator) and RTCP (Avaya-specific RTCP and call path data)</li> <li>Latency - the aggregate latency recorded on the call</li> <li>The total number of hops the call took</li> <li>You can sort each option in ascending or descending order.</li> </ul>					
Search	<ul> <li>A free text search field that also has options to use predefined criteria, either of the following: <ul> <li>Search by the source IP that made the call</li> <li>Search by the destination IP that received the call</li> <li>Search by vendor, which identifies the method that created the call. Options are LX1 (the VOSS Raptor Call Path generator) and RTCP (Avaya-specific RTCP and call path data)</li> </ul></li></ul>					

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

The image shows the Call Management Configuration dialog:

Apr 22, 2024	6:56 pm - Apr 22, 2024 7:56 pm	2 2 2 0	2 ×	Ē	search		
TIME	CALL MANAG	EMENT CONFI	GURATION		×	LATENCY	HOPS
	ARCHIVE OPTIONS	DAILY WEEKLY MONT	HLY QUARTERLY				
	ALERTING OPTIONS	ALERT ON ARCHIVE FAILU	IRE ALERT ON ARCHIV	E SUCCESS			
	HOST	METHOD	PATH	CREDENTIAL			

# 4. Configuration

# 4.1. System Configuration

#### 4.1.1. Overview

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

voss 🎇		Q	-?}-	3			Days	remaining: 313	P	admin	-
S ASSET EXPLORER							Displ	aying 1 - 32 of Syste	em Configuration	<b>»</b> 50	~
search filter	 ۹)			<b>D</b> I			<b>D</b> I		Ē		
· · · · · · · · · · · · · · · · · · ·		179 20 4	0 77	170 00 40 04	172 20 42 90	173 20 42 00	00000	David Surday	Land Conta		

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

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

voss 🎇		8	_	îļî		٩	<u>\</u>	Ĥ	<b>.</b>	ē	٠		Days remaining: 313	admin
POLICY CONFI	GURATION	Rules	Filters											Save
Policies Name	Failover		Rules Nar	ne		Thr	eshold	Wir	ndow	Sev	erity	Response Procedure		
Cucm_CmCat_Cm		146 ^	Alarm	ID: 50506	(DChannelO	) 1 time		1 min	ute	()	Critical	Default IRP		
Touy Ack Alert			Alarm	ID: 50500	(CallManag	1 time		1 min	ute	0	Critical	Default IRP	¥2 = 🖌	
Demo2			Alarm	ID: 50501	(SDLLinkIS)	/) 1 time		1 min	ute		Minor	Default IRP	¥2 = 🖌	
Infinity			Alarm	ID: 50502	(SDLLinkOC	) 1 time		1 min	ute	0	Critical	Default IRP	J 2 ≡ 🖌	
Ping Second Dchannel			Alarm	ID: 50503	(CMVersion	1 time		1 min	ute	()	Informational	Default IRP	≠2 ≡ Z	

#### **Related Topics**

• Arbitrator Main Interface

# 4.2. Policy Configuration

#### 4.2.1. Overview

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

- · Business processes
- Infrastructure
- Security
- Applications
- Unified communications
- · Network behavior
- · Metrics and threshold violations

voss 🎇		🗿 🦨 🕴	i 🔳	<u> </u>	L 🔒 i	* •		Days remaining: 313	admin
POLICY CONFIG		s Filters							Save
Policies		Rules							
Name	Failover	Name		Threshold	Window	Severity	Response Proced	lure	
Cucm_CmCat_Cm	146	Alarm ID: 50	06 (DChannelO	1 time	1 minute	Critical	Default IRP	J≠2 ≡ 🗸	
Touy	9	Alarm ID: 50	00 (CallManag.	1.600	1 minute	Critical	Default IRP		
Ack Alert	2	Alarm ID: 50	oo (Calimanag.	i ume	1 minute	Crisical	Default IRP	¥2 = /	
Demo2	= 1	Alarm ID: 50	01 (SDLLinkISV	) 1 time	1 minute	(!) Minor	Default IRP	≠2 ≡ 🖊	
Infinity	= 1	Alarm ID: 50	502 (SDLLinkOO	1 time	1 minute	() Critical	Default IRP	≠2 <b>=</b> ∕	
Ping	. 1								
Second Dchannel	1	Alarm ID: 50	503 (CMVersion	1 time	1 minute	🕛 Informati	onal Default IRP	J 2 ≡ 🖌	

# 4.2.2. Correlation Rules

A correlation rule extracts data from the various sources and then defines the parameters for creating an alert within a policy. It may contain one or more correlation definitions along with specific actions and response procedures. Each correlation rule consists of the following parameters:

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

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

POLICY CONFIGURA	ATION	RURS.	roes						Save
Policies Name Faile			Rules	Threshold	Wind	tow Severity	Response	Proced	
Arda		1	Name	Jitter Value Exceed	ed.				23 8 2
Aspect UIP System Alerts		2	Description					-	
Asset Log Monitor		1							
Avaya Call Monitor	2	4							
Avaya PDS SMMP Alarms	2	6	7,004	Simple		Artist	Respond	-1	
Avaya PDS SHSLOG Alarms		10					respons	-	
Caro Cal Monitor		4	Threshold	1		Response Procedure	UnicalToAlert		
LAVERS Agent Manitor		3	Window	1 minute	- 1	Definition Output			
LogMonitor		1	Severity	Ontoal	-	Enabled	2		
UR1 Call Monitor v2		1				Inherit Output			
LIST SEP Call Errors v2		6				Halt Processing	-		
Nortel Call Monkor		3	Latency Value Decented	15me	1.000	ute 🕐 Croud	LINCHTON		100 IN 100
DBC Monitor		3	Latency Value Domested	1.000	1 100	O CHAR	Linkcarno	oers.	AT # 5

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

Each filter has the following options:

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

Policies		Filters		
Name Fals	wer	Name Pattern		
Arda		Name		
Aspect UP System Alerts		Vendor Method		
Asset Log Monitor	1	Pattern		
Avaya Call Monitor		(method="cinco")	1	
		Source Field		
Avays POS SNMP Alarms		Raw Log	· ·	
Avaya POS SYSLOG Alarms		Pattern Type		
Caro Call Monitor		Regular Expression Match/Extract Runction Value	1	
LANCER Agent Monitor		Puection Volue		
Log Munitor		Kama		
UR Cal Monitor v2		Call Manager to		
LKI SP Calibrons v2	0.7	Pattern		
Nortal Call Munitor	I T	callManager(ps/1,=1)*	1	
PING Manikar	D T	Source Field		
	_	Raw Log	~	
Powerwave ShMP Aarms		Pattern Type		
Site training policy		Regular Expression Match/Extract	8	
Test Alarm v1	10	Function Value		
Aj DeperMental	<b>2</b> (1)	None 8		

### 4.2.3. Example - Policies and Alerts

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

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

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

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

You can configure this definition in two ways:

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

#### 4.2.4. Correlation Definitions

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

Parameter	Description
Name	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	<ul> <li>Within the Regex Wizard there are 2 sections:</li> <li>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.</li> <li>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.</li> </ul>

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 Note: The "Extract" pattern types above will cause the correlation engine to include the definition name and the matched value in the Alert Message.
Function	<ul> <li>The functions below may be used to change what the correlation engine counts as a "match" in the log. Alerts are only triggered if the specific number of matches are found.</li> <li>None - Default. Only use Pattern type matching to trigger a match.</li> <li>Greater Than - Should only be applied to integer values. If the extracted value is greater than the configured value, then a "match" is made.</li> <li>Less Than - should on be applied to integer values. If the extracted value is less than the configured value, then a "match" is made.</li> <li>Same - Can be applied to both Text or Integer. If the extracted value is the same as previous occurrences, a match triggered. For example, if multiple devices are sending an error message, only the first error will trigger an alert. If the desired goal is to trigger an alert for unique IP address, then the IP address definition should have the Same function applied.</li> </ul>
Value	This field will only be available if the function selected is either "Greater Than" or "Less Than".

		_
0806	Last 24 Hours -	
Click have for help building rules   Build a New Definition Manually	Displaying 1 - 10 of 154,942 events + first prev next	-
Nerro CALLMETRICLUS B RUN B CALLUS B		
Seurce Reld Raw Log		
(37)118 (37)11	'ANC', 'COCK12', 'Kiste', 'COCK12', 'AssetSame', '18.13.37.41', 'AssetSmatner 2', 'ServiceName', 'Cisco Trace Collection	et'-'10.
Hunt-127.0.0.1 Fort-Idealog Method-1 Detract Field		
EXAMPLE Socket Connected. IP Address		
165435 PM «/истокимно»		
Hugh127.0.01 Cancel Save		
<pre>CDMINE /pert#/jeil/etbitetsit/modules/ween/visos/adderFissettorentory_treads.gdpr 155500FW East tream #0 [internal function]: BoogClientsdBMoguest["<table version",",","<br="">#1 /pert2/jeil/Arbitrari/modules/ween/visos/adderFissetTorentory_treads.g #2 /pert2/jeil/Arbitrari/modules/ween/visos/adderFissetTorentory_treads.g #3 [binom is /pert2/jeil/Arbitratori/modules/ween/visos/adderFissetTorentory_treads.g modules/setTorentory_treads.g modules/setTorentory_treads.g</table></pre>	ps://10.13.5', 'bitp://echemas', 1, 01 hp(00): SompClimst->_call('SelectOmbeviow', Array) hp(00): SompClimst->GelectOmbeviow('', Array)	
RULE DEFINITIONS * Jitter Value Exceeded	Please 63 th all Name and Pattern fields Ca	ncel 🚺
tince .	Last 24 Hours -	
Disk hars for help building rules Build a New Definition Manually	Displaying 1 - 10 of 154,942 events a first previous	-
	subside it is a christ second such that see	-
Invents CALL-METRICE_ID * Ittan * CALL_ID * (read) *		
Name Pattern		
band		
Secure Date		
Seurce Field		
Raw Log	-	
Rew Log Viteration Revealed Reve Revealed Revealed Reve	No.	
Rose Log V Factors Type Function Regular Expression Match/Extract 8 None	Nine .	
Ren Log Function Pattern Type Pattern Type Pattern Type Paper Expression Match/Extract Paper Expression Match/Extract Pattern	1	
Park Log Pattern Type Pattern	1	
Rev Log Pattern Type Function Repaire Expression Math/Extract	1	
Rate Log Pattern Type Pattern	0 "And","COCH13","Hisbo","COCH12","AssertAsser","10.13.37.43","AssertAssets "733	_
Park Log Pattern Type Pattern	0 "ANC", "COURLE", "Risbe", "COURLE", "Assert/Asser", "LB.13.37.43", "Assert/Assert/ "')) Regres Wizard	aurori 👔
Rate Log Pattern Type Pattern	0 "And","COCH13","Hisbo","COCH12","AssertAsser","10.13.37.43","AssertAssets "733	_
Res Log Pattern Type Function	0 "ANC", "COURLE", "Risbe", "COURLE", "Assert/Asser", "LB.13.37.43", "Assert/Assert/ "')) Regres Wizard	Cannool Cannoo
Res Lag Pataen Type Pataen Typ	B           "Sett" * "CODELL" * "Riado" * "CODELL" * "Aspentikases" * "Lit. Lit. Lit. 47 + 43 * "Aspentikases" * "Lit. Lit. 17 + 43 * "Aspentikases" * "Lit. Lit. 17 + 43 * "Aspentikases" * "Lit. Lit. 17 + 43 * "Aspentikases" * Lit. Lit. 17 + 43 * "Aspentikases * Lit. 10 * 10 * 10 * 10 * 10 * 10 * 10 * 10	Canadal Lo Coleccione Material Material Deve 700 Deve 700
Res Lag Pattern Type Pattern Ty	B           "Sett" * "CODELL" * "Riado" * "CODELL" * "Aspentikases" * "Lit. Lit. Lit. 47 + 43 * "Aspentikases" * "Lit. Lit. 17 + 43 * "Aspentikases" * "Lit. Lit. 17 + 43 * "Aspentikases" * "Lit. Lit. 17 + 43 * "Aspentikases" * Lit. Lit. 17 + 43 * "Aspentikases * Lit. 10 * 10 * 10 * 10 * 10 * 10 * 10 * 10	Cannool Cannoo
Res Lag Pattern Type Pattern	B           "word" a "COCREGT", "Raised" a "COCREGT", "Assert/Rame" a "Life.15.17.43", "Assert/Rame" a "Life.15.17", "Assert/Rame" a "Life.15", "Assert/Ram	Carsoni C Consulation 
Res Lag Pattern Type Pattern	The second	Connord Connor
Res Lag Pattarm Type Pattarm	B           "word" a "COCREGT", "Raised" a "COCREGT", "Assert/Rame" a "Life.15.17.43", "Assert/Rame" a "Life.15.17", "Assert/Rame" a "Life.15", "Assert/Ram	Connord Connor
Res Lag Patients Type Patients Typ	The second	Carrol Constraint Cons
New Long     Function       Particine     Function <tr< td=""><td>Terres and an an</td><td>Cancel Construction Lancentration Construction Research R</td></tr<>	Terres and an	Cancel Construction Lancentration Construction Research R
New Log     Function       Pattern Type	Terres and an	Carrol Constraint Cons

# 4.2.5. Add a Policy

To add a policy:

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

POLICY CONFIGURATI	ON	Rules	Filters	Chan	iges have l	been made					Save
Policies Name Failover	0		Rules Name			Threshold	Window	3	severity		Response Procedure
Asterisk Basic		5									
Cisco CUCHv8 to 11.5	2	447									
Cisca CUCMV8_r2 up	7	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	7	T									
Example Policy									No re	cords rules	+ first prev next last

### 4.2.6. Add a Correlation Rule

To add a new correlation rule:

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

		8 ·	【 销		۹ ۹	L 🔒 🛓	2 0 1	•	👤 admin -
POLICY CONFIGURATIO	N Rules	Filters	Fil to all feet	is before saving a	nd make sure a	el rules have at least	1 definition		Save
Policies		Rules							
Norte Falipart		Name		Threshold	Window	Severity	Respon	nse Proced	PR
Avays POS ShallP Alarms	100	per tela	Connected	1.674	t minute	O crea	al LinkCal	numers	×1 = Z
Avaya PDS SYSLDG Alarms	1 10	Latersym	the Downed	1674	1 minute	() Cres	al UNACA	floAlein	21 - 2
Clace Call Member	3 5	MOS NAME	e UDW	1.8me	1 minute	() creat	al LHACA	nuklen	21 - 2
LAVERT Agent Monitor		-							
Log Monitor	1	Packers Li	nt Volue Excen	fed 1 bre	1 minute	Cress	al LinkCal	noven	
UIT Call Monitor vil	1 1		Norre	(read)					A6 = 5
UR SP Call Briors val	•	0	escription						
Nortei Call Montor	1 1								
PING Manitar	1 1								
Powerwave Statt? Narms	11		Type	Simple		Action	Track/Tempond		
SLo training policy	12		Threshold	1 10		Insponse Procedure	Default PP		
Test Alarm vt	T		Window				-	-	
Aj OperMental	10			1 minute		Definition Output		-	
ALSTOYBARN : Auton - Alet Ess.	(P)		Severity	International		Enabled	2		
ALSTOYBAIN : Dalas - Nert Exa.						Inherit Output	2		
ALSTOYBARN : NHC - Alert Dump.	1					Halt Processing			
APC Powernet MIB Traps	-								
APEX SOLID Alarm Test	5						Discission	1-4-14+	ules + first prev next last+

### 4.2.7. Add a Definition

To add a new definition:

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

	CY CONFIGUR	RATION	PLINES FILLY	rs					
olicie	5		Rul	es					
Nan	ne Fa	ilover		Name	Threshold	Window	Sevenity	Response Proc	edure
Cieco	Call Monitor		* <u> </u>	Jitter Value Exceeded	1 time	1 minute	Critical	LinkCaliToAlert	P3 =
_	TR Assess Manuface	1973							-
ALE DE	FINITIONS = jitter	Value Excee	eded			Ourges made		Cancel Upter	-
808							Last 24	Have G	
h here for	Telp building rules Buil	ld a New Definit	tion Manually			Diploying	1-10-01154,042 events + Feat	pres next list = 10	4
P.4	CALL_METRICS_O	0 <sub>jipr</sub> 0	CALLO 0						
roe Tield	Rew Log		~						
-	<12-341 11 2010 21-1	Alath Loggers	("class, seve_ast	WICE's		Lade"+"000412", "And		and an	
65410 PA	.37.43', "AssetDeatr. Bervice", "ElapsedTic	1041000'1'', Ad	esen i pAddresse" i "	10.13.37.43", "Mame" 1"000	(NL2", "Bervicebane"	"Class Trace Gulla	ntilaan"+"10.13.57.43", "Aa nijaa		
	mont127.8.0.1 Port-Mex		Extract Name this field	rield					
67/11/18 8:54:10 PA	-RETERONG-Godket C. Bochat Cansetted.	reated.	(P Address						
			6	ancel Save					
		-							A DESCRIPTION OF
57/11/18 554.10 PA	RULE DEFINITIO	NS » Jitter \	Value Exceed	ed			fease fill in all harne and Pather		Cancel Update
	cieco							Last 24 Hou	m- q
	Click here for help build	ing notes Balls	d a New Definitio	n Manually			Displaying 1 - 10 of 15	54.542 events + first pre-	rest late 10 a
	Events ICA	L. METRICS JO	0 par 0 2	ALLO O great O					
	_								
	Name			diare.					
	Source Field								
	Raw Log		1.90						
	Plane Long								
	Pattern Type			retter		Value		•	
		novExtract						`	
	Pattern Type Regular Expression Via		1	tone			n' - ' OKCHIJ' - ' Assert Renn' - '	10.13.17.47.1544	ant same " - " (\$ . 13 . 17
	Pattern Type Regular Expression Val 1 50/10/18 15:54:00 PM 1:12444	1 11 2018 21:5 Hamp':1331345 Ho Trace Culle	1	tone			r" - "000012" - "Asset Jame" -	11.13.3 <sup>7</sup> .47 <sup>°</sup> , <sup>1</sup> 88893	101.1000° 1° 10.13.37.4
Inners	Pattern Type Repair Expresson Mar SM1V18 1654:00 PM * 17 Care * Tates		1	Vone C1803_MTHT_BERWICE": '13_"BetweeGode":"8',"E "81apsedTume":2918219,"	CrescHousept","","A "BervLoethatus","L	MC","COCHL3","%LHD		18.13.17.43°, 'Asserti	
	Pattern Type Pepular Expression Mat SM11/18 1654:50 PM * 2014 * 2014 * 2014 * 2014 * 2014 * 2014	1 11 2018 21:5 stang":1331345 re Trace Colle cod Value:	1	tone	CrescHousept","","A "BervLoethatus","L	Reges Wita	rd	18.13.17.47°,* <b>1</b> 0000	Cancel System
	Pattern Type Repair Expresson Mar SM1V18 1654:00 PM * 17 Care * Tates	1 11 2018 21:5 stang":1331345 re Trace Colle cod Value:	1	Vone C1803_MTHT_BERWICE": '13_"BetweeGode":"8',"E "81apsedTume":2918219,"	CrescHousept","","A "BervLoethatus","L	Reges With	rd 2) Onever Region		Cancel Update
	Autorn Type Popular Expression Mar SUTURE S	1 11 2018 21:5 stang":1331345 re Trace Colle cod Value:	Fu 4 1 51:05 Longers (* 622, "Band Dervice",	tone CEROL ATMET, REMATCH' '11, "Retro HEARD' 1"1", " "El aprocettane" - 1914123, Cancel	CrescHousept","","A "BervLoethatus","L	Reges With	rd 2) Onever Region		Cancel Update
1) Select	Autorn Type Popular Expression Mar SUTURE S	1 11 2018 21:5 stang":1331345 re Trace Colle cod Value:	Fu 4 1 51:05 Longers (* 622, "Band Dervice",	Vone C1803_MTHT_BERWICE": '13_"BetweeGode":"8',"E "81apsedTume":2918219,"	CrescHousept","","A "BervLoethatus","L	Regex Wita Regex Wita (1) Ment of the description	nd 2) Onuse Regus 1.67 annual agus 100.40011 1 1.07 annual 117 annual 118 1.08001111 annual 118 1.08001111 annual 118		Carcol Update
1) Select	Mattern Type Pegular Expression Mar SD11118 4120000 SD11118 4120000 41000 Witzand Alog 2500 are Magoo Pingo	i il 2018 21:5 namo fillila no Trace Colle ctmd Value.	Pu 1 1 51:61 Lopper ( 5422 - "MadCharts etian Dervice",	tone CEROL ATMET, REMATCH' '11, "Retro HEARD' 1"1", " "El aprocettane" - 1914123, Cancel	Update	Regen Waa Post of the second	nd 2) Oncer Engen 11,45° executions 101-060111° to realize the second second second second 101-06000000, 1010 1010000000000000000000000		Cancel Dystems 1990/05-6-6-9-9/09/100- 000-01-01-1-6-6-9-9/09/100- 000-01-01-1-6-6-9-9/09/100- 000-01-01-1-6-6-9-9/09/100- 000-01-01-01-01-01-01-01-01- 000-01-01-01-01-01-01-01-01-01-01-01-01-
T) Salers	Mattern Type Pegular Expression Mar SUTURE 123-040 15:50-040 17:10:00 Wizard Alog 2:50-ore Report Mar Mar Data 10:50-000 10:00 10:50-000 10:5	111 2018 21:5 neargy 1131346 re Trace Colle cred Value:	Pu 1 1 hiddi Looppers (* 1422, "Austitusta setian Bervise", af 2 501 313 even	tere CERCO, PENE, SERVICE** *13. *Returnicule****** *Expenditure**24440 Cancel ant 2444005 + * figst, prov. mod. lat.+ returnicule*	Update	Regen Waa Post of the second	nd 2) Oncer Engen 11,45° executions 101-060111° to realize the second second second second 101-06000000, 1010 1010000000000000000000000		Cancel Dystems 1990/05-6-6-9-9/09/100- 000-01-01-1-6-6-9-9/09/100- 000-01-01-1-6-6-9-9/09/100- 000-01-01-1-6-6-9-9/09/100- 000-01-01-01-01-01-01-01-01- 000-01-01-01-01-01-01-01-01-01-01-01-01-
1) Salert Search fo *	Mattern Type Popular Expression Mar EDMONT EDMONT EDMONT EDMONT Popular Mizzard Alog Pipular	L L POIR DIES Hangy (1933) He re Trace Golle and Value:	Fu	tere CISO, PTRT, SERVICE** *13, "Returnicate" * ** ** *Expenditure**24440 Cancel ant 2444005 • * * first, prev mod. lat.* Resource************************************	Update	Regen Waa Post of the second	nd 2) Oncer Engen 11,45° executions 101-060111° to realize the second second second second 101-06000000, 1010 1010000000000000000000000		Cancel Dystems 1990/05-6-6-9-9/09/100- 000-01-01-1-6-6-9-9/09/100- 000-01-01-1-6-6-9-9/09/100- 000-01-01-1-6-6-9-9/09/100- 000-01-01-01-01-01-01-01-01- 000-01-01-01-01-01-01-01-01-01-01-01-01-
*	Mattern Type Popular Expression Val Schrönin 413/4/01 Schrönin 413/4/01 Richard 41 Alog 3:Schward Magoo Pings Versions- 1.6.7 secolistic Vice-Accession 400000	L LL DOIN 2115 Hangy 1131340 to Trace Collected Value: Land Value:	Fu         1         1           1         1         1         1           1         1         1         1         1           1         1         1         1         1           1         1         1         1         1           1         1         1         1         1           1         1         1         1         1           1         1         1         1         1           1         1         1         1         1           1         1         1         1         1         1           1         1         1         1         1         1         1           1	NYS. CIACO, JAYNE, LENVICE** *1, - Terrescode******* Cancel and 24 Hours + + frs: pro: necf. last+ manufactures - + frs: pro: necf. last+ manufactures - manufactures	Update Q, 19 1	ART + "COOLS", "Rush Topological and the second an	nd 2. Occur form 1. Second s		Carcol Update
1) Select Search fo * * * * * * * * * * * *	Mattern Type Popular Expression Var SUTUR SUTUR SEASON Wizard Alog SCENER Ange Wextore' Laf excellance Wextore' Laf excellance NOR SUTUR	L 11 2018 2015 Kangr (132240) to Trace Daile training (1-100 m) (1	Гу 1 1 51:151 Loppers (* 422, "MadClassis etilian Bertine", 072.000.353 енето ебото - дото на объект 12.000 2007.0000000000000000000000000000000000	NYM CIACO, JAYNE, JARWYICK** *1, January Content of the second Cancel And 24 Hours + * • Fry prov mod last + NAME - 2601 (1910) NAME - 2601		ARTY CROKET, "Rush 33 Regen Willa Chail accord description Chail accord description descr	nd 2) Cream Fague 11 J. Cream Fague 11 J. Cream Fague 12 J. Cream Fague 13 J. Cream Fague 14 J. Cream		Cancel Dystems 1990/05-6-6-9-9/09/100- 000-01-01-1-6-6-9-9/09/100- 000-01-01-1-6-6-9-9/09/100- 000-01-01-1-6-6-9-9/09/100- 000-01-01-01-01-01-01-01-01- 000-01-01-01-01-01-01-01-01-01-01-01-01-
1) Saler Searth fo * * * * * * * * * * * * *	Autorn Type Popular Expression Var Expression Var Expression Var Wizard Aug Convertinger Popular	L 12 2018 2015 Camp <sup>2</sup> (132) Mit or Trans Dollar Campbolic Control Control Control Viller Control Viller Control Contr	Fig.         1         1           S1161         Loppers         4         1           S122         "BudClassis         6         1           S1161         Loppers         4         1         1           S122         "BudClassis         6         1         1         1           S125         "BudClassis         6         1 <td>true     Clancel     Clan</td> <td>Update 90</td> <td>ART**CROAL2*,*Rush Itegers Watan Clamma et al. Check and the second of the second second second second second of the second second second second second second second of the second secon</td> <td>d - December 2000 - 1.4.5 Construction - 1.4.5 Construction -</td> <td>Contraint (1990) (1000) (1000) (1000)     Contraint (1990) (1000) (1000)     Contraint (1990) (1990) (1990)     Contraint (1990) (1990) (1990)     Contraint (1990) (1990)     Contraint (1990) (1990)     Contraint (1990)     Contraint (1990) (1990)     Contraint (1990)     Cont</td> <td>Cancel Update 101712000 10170100 10170100 101701 101701 101701 10170 10170 10170 10170 1017</td>	true     Clancel     Clan	Update 90	ART**CROAL2*,*Rush Itegers Watan Clamma et al. Check and the second of the second second second second second of the second second second second second second second of the second secon	d - December 2000 - 1.4.5 Construction -	Contraint (1990) (1000) (1000) (1000)     Contraint (1990) (1000) (1000)     Contraint (1990) (1990) (1990)     Contraint (1990) (1990) (1990)     Contraint (1990) (1990)     Contraint (1990) (1990)     Contraint (1990)     Contraint (1990) (1990)     Contraint (1990)     Cont	Cancel Update 101712000 10170100 10170100 101701 101701 101701 10170 10170 10170 10170 1017
1) Select Searth fo * * * * * * * * * * * * * * * * * * *	Autarn Type Popular Expression Var SUITIN S	L 11 2018 2015 Kamp <sup>2</sup> (132) MD or Trans 052 MD or Trans 052 MD or Trans 052 MD or Money 100 M	Гу 1 1 51161 Loppers (* 1422, "hadClasss 4422, "hadClasss 4428, "hadClasss 4429, "hadClass 4429, "ha	Kins     Classe, Jimm, Jasseviczi, *, *, *, *, *, *, *, *, *, *, *, *, *,	Creationsage" - ", ", ", " Terrelocitation" - ", " Update 20 10 10 10 10 10 10 10 10 10 10 10 10 10	ART**CROAL2*,*Rush Itegers Watan Clamma et al. Check and the second of the second second second second second of the second second second second second second second of the second secon	nd 2) Cream Fague 11 J. Cream Fague 11 J. Cream Fague 12 J. Cream Fague 13 J. Cream Fague 14 J. Cream		Cancel Update 101712000 10170100 10170100 101701 101701 101701 10170 10170 10170 10170 1017
1) Salvers Saurach fo * * * * * * * * * * * * * * * * * * *	Vectors Type Popular Expression Var SUTION	L 12 2018 2011 Kang' (13 13 14) er Treve folle rand Value angeleging 1 - 12 of ap 48-480213 Th Tr. Jander- Verst and Status (13 100-1997) 11 11 11 11 11 11 11 11 11 11 11 11 11	Го 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	EVEN CERCOL PEYER, REAVICE * (*), *, * * Expenditions * (*) * *, * * Expenditions * (*) * *, * Cancel act 24 Hours • * Forg pro reaf last • Reav-Ref[]*(1899- Reav-Ref[]*(1899- Reav-Ref[]*(1899- Reav-Ref[]*(1899- Reav-Ref])*(1899- Reav-Ref])*(1899- Reav-Ref])*(1899- Reav-Ref])*(1899- Reav-Ref])*(1899- Reav-Ref])*(1899- Reav-Ref])*(1899- Reav-Ref])*(1899- Reav-Ref])*(1899- Reav-Ref])*(1899- Reav-Ref))*(1899- Reav-Reav-Ref))*(1899- Reav-Ref))*(1899- Reav-Ref))*(1	Transformation (1997)	ART**CROAL2*,*Rush Itegers Watan Clamma et al. Check and the second of the second second second second second of the second second second second second second second of the second secon	d Di David Ingue 1-16: Constituto di Administrativa 1-16: Const	Contraint (1990) (1000) (1000) (1000)     Contraint (1990) (1000) (1000)     Contraint (1990) (1990) (1990)     Contraint (1990) (1990) (1990)     Contraint (1990) (1990)     Contraint (1990) (1990)     Contraint (1990)     Contraint (1990) (1990)     Contraint (1990)     Cont	Cancel Update 101712000 10170100 10170100 101701 101701 101701 10170 10170 10170 10170 1017
1) Select Search fo * * * * * * * * * * * * * * * * * * *	Autom Type Popular Expression Val SUITING SUI	L 12 2018 2015 Cargo (1332) 504 cargo (1352) 504 control (1352) 505 control (1352) control (1352) contro	Fig.         1         1           S1161         Loppers         4         1           S122         "BudClassis         6         1           S123         "BudClassis         6         1         1           S124         S1         BudClassis         6         1         1           S125         S1         BudClassis         6         1	Kins     (1), Not according to the second of the seco	Transformation (1997)	ART**CROAL2*,*Rush Itegers Watan Clamma et al. Check and the second of the second second second second second of the second second second second second second second of the second secon	d Di David Ingue 1-16: Constituto di Administrativa 1-16: Const	Contraint (1990) (1000) (1000) (1000)     Contraint (1990) (1000) (1000)     Contraint (1990) (1990) (1990)     Contraint (1990) (1990) (1990)     Contraint (1990) (1990)     Contraint (1990) (1990)     Contraint (1990)     Contraint (1990) (1990)     Contraint (1990)     Cont	Cancel Update 101712000 10170100 10170100 101701 101701 101701 10170 10170 10170 10170 1017
1) Select Search fo * * * * * * * * * * * * * * * * * * *	Vectors Type Popular Expression Var SUTION	L 12 2018 2015 Cargo (1332) 504 cargo (1352) 504 control (1352) 505 control (1352) control (1352) contro	Fig.         1         1           S1161         Loppers         4         1           S122         "BudClassis         6         1           S123         "BudClassis         6         1         1           S124         S1         BudClassis         6         1         1           S125         S1         BudClassis         6         1	Kins     (1), Not according to the second of the seco	Transformation (1997)	ART**CROAL2*,*Rush Itegers Watan Clamma et al. Check and the second of the second second second second second of the second second second second second second second of the second secon	d Di David Ingue 1-16: Constituto di Administrativa 1-16: Const	Contraint (1990) (1000) (1000) (1000)     Contraint (1990) (1000) (1000)     Contraint (1990) (1990) (1990)     Contraint (1990) (1990) (1990)     Contraint (1990) (1990)     Contraint (1990) (1990)     Contraint (1990)     Contraint (1990) (1990)     Contraint (1990)     Cont	Салка Ористи
1) Salari Salari 1) Salari 1) Salari	Nations Type People Expression Via 151-002 15	L 1 2018 2019 Lange (113) 1930 or Traces (014) or trac	Калана         Калана           1         1           1 <t< td=""><td>Non           C1000_PTMBERNITCH*           *1.5_Restarbide*           *1.5_Restarbide*           Cancel           Cancel           and 244 Hours =           * = Free prov mod_last*           * = Free prov modelast*           *</td><td>Update 90 10000000000000000000000000000000000</td><td>All "+" CROKE", "Rush 33 Regen Wiza Climenter, "Check and the service distribution of the distribution of th</td><td>d Di David Ingue 1-16: Constituto di Administrativa 1-16: Const</td><td></td><td>Cancel Update 101712000 10170100 10170100 101701 101701 101701 10170 10170 10170 10170 1017</td></t<>	Non           C1000_PTMBERNITCH*           *1.5_Restarbide*           *1.5_Restarbide*           Cancel           Cancel           and 244 Hours =           * = Free prov mod_last*           * = Free prov modelast*           *	Update 90 10000000000000000000000000000000000	All "+" CROKE", "Rush 33 Regen Wiza Climenter, "Check and the service distribution of the distribution of th	d Di David Ingue 1-16: Constituto di Administrativa 1-16: Const		Cancel Update 101712000 10170100 10170100 101701 101701 101701 10170 10170 10170 10170 1017
1) Seventh for Seventh for 400000 2014000 400000 400000 400000 400000 400000 20180 4000000	Nations Type Popular Expressions Mar #13-0/02 School of These Research of These Wizard alog Converting Popular P	L 1 2018 2019 Lange (1) 113 Lange (1) 113 Transformer (1) Transformer	Городина	Non.           C1000_PTMBERVICE**           *1ReturnSchaft*******           *1	Update Q 10 10 10 10 10 10 10 10 10 10	All"+"CROKEF", "Rank Brigger, William Control of the second secon	d		Салка Ористи
1) Second 1 Second 1 (1) Second	Nations Type Popular Expressions Variation 15.54.0.002 William Allow Statements of the William Network Statements of the William Network Statements of the Weekslope - 1.4 * execution NEEKS Statements of the Weekslope - 1.4 * execution NEEKS Statements of the NEEKS Statements of the NEEKS Statements of the NEEKS Statements of the NEEKS Statement of the NEEKS Statements of the NEEKS Statement of	L 1 2018 2019 Kang T 125 193 to Trace foile control value 	Fig.         1           1         1	Non           C1000_Presservices           '1	Transformation ****	All"+"CROKL", "Rush Brigger, Walah ("Lines: chap of the lines:	A Description 1.1.2.2.2.2.2.2.2.2.2.2.2.2.2.2.2.2.2.2	AND THE CONTRACT OF A STATE OF A	Careca Under Careca Under Ca
1) Second Search for	Addam Type Pepdar Expression Val 151-001 151-	L 1 2018 2017 Kang' (1313) Mo	Fig.         1           1         1	Viris  C100, Jrynt, Lawyick, *  C200, Jrynt, Lawyick, *  T, Japanetrise, *  Cancel  Cancel Cancel Cancel Cancel  Cancel  Cancel Cancel  Cance	Contractions and a set of the set	All"+"CROKL", "Rush Brigger, Walah ("Lines: chap of the lines:	d	AND THE CONTRACT OF A STATE OF A	Careet Under Terrapione and and the set of the set of the set of the and the set of the set of the set of the and the set of the set of the set of the and the set of the set of the set of the and the set of the set of the set of the and the set of the set of the set of the and the set of the set of the set of the and the set of the set of the set of the and the set of the set of the set of the and the set of the set of the set of the and the set of the set of the set of the and the set of the set of the set of the and the set of the set of the set of the and the set of the set of the set of the and the set of the set of the set of the and the set of the set of the set of the and the set of the set of the set of the set of the and the set of the set of the set of the set of the and the set of the set of the set of the set of the and the set of the set of the set of the set of the and the set of the set of the set of the set of the and the set of the set of the set of the set of the and the set of the set of the set of the set of the and the set of the and the set of the and the set of the and the set of the and the set of the and the set of the and the set of th

# 4.2.8. Delete a Correlation Rule

To delete a correlation rule:

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

POLICY CONFIGURA	TION	Rules	Filters					Save
olicies			Rules					
Name Fallow	er 🔄		Name	Threshold	Window	Severity	Response Procedure	
Cisco Call Monitor	<b>V</b>	4	CLEARED - RPTR Alarm	1 time	1 minute	() Informational	AlertClear	27 = 2
LAYERK Agent Monitor		3	CRITICAL - RPTR Alarm	1 dime	20 minutes	Criscal		
Log Monitor		T	CHITCAL - HPTH Marm	Tome	20 minutes	Cristal	AlertHold	F1 = 1
LX1 Call Monitor v2		5	DISREGARD - FailedNodes	1time	1 minute	() Informational	DoNotAlert.	A1 = 1
LX1 SIP Call Errors v2		6	DISREGARD - UnableToRun	1 time	1 minute		DaNotAlen	¥1 = Z
Nortel Call Monitor		3	INDETERMINATE - RPTR Ala.	Tama	15 seconds		DoNotAlert	
PING Monitor		2			12 angun jua	C monadora	Domain and	
Powerwave SNMP Alarms		71	ISG Alarm trap - INDETERMI.		1 minute	() Informational	DoNotAlert	×1 = ×
SiLo training policy		2	ISG Alarm trap - MAJOR	1 time	1 minute	() Major	DoNotAlert	P1 = 2
Test Alarm v1	1	1		-		-		
AJ ExperiMental		T	-	-			Displaying 1 - 11	of 11 events + first prev next last +

### 4.2.9. Delete a Policy

To delete a policy:

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

Policies		Rules					
Name Fa	lover	Name	Threshold	Window	Sevenity	Response Procedure	
Cisco Call Monitor		CLEARED - RPTR Alarm	1 time	1 minute		NertClear	17 =
LAVERX Agent Monitor	<b>2</b> 3		1000		0		
Log Monitor		CRITICAL - RPTR Alarm	1 time	20 minutes	Critical	AlertHold	27 = 2
LX1 Call Monitor v2	1	DISREGARD - FailedNodes	1 time	1 minute	() Informational	DoNotAiert	25 E 2
UX1 SIP Call Errors v2	<b>2</b> 6	DISREGARD - UnableToRun	1 time	1 minute	() Informational	DoNotAlert	1 = 1
Nortel Call Monitor		INDETERMINATE - RPTR Ala	1.1100	15 seconds	() Informational	DoNotAlert	
PING Monitor	2		1 Dine	19 seconds	() montabonat	DONODIET	
Powerwave SNMP Alarma	<b>2</b> 11	ISG Alarm trap - INDETERMI.	. 1 time	1 minute		DoNotAlert	N1 = N
Sko training policy	2	ISG Alarm trap - MAJOR	1 time	1 minute	() Major	DoNotAiert	×1 = /
Test Alarm v1	1	ISG Alarm trap - MAJOR	1 time	1 minute	(D) Major	DoNotAlert	
AJ ExperiMental	<b>Z</b> 3	_ isa wanin cap i awyon	Tume	THINKILE	C major	DONODIEL	
ALSTOYBADN Austin - Alert	Exa. V 9				0	isplaying 1 - 11 of 11 events	e first prev next last

# 4.2.10. Disable or Enable a Policy

To Disable and Enable a Policy:

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

Policies		Rules					
Name Fallover	-	Name	Threshold	Window	Severity	Response Procedure	
Cisco Call Monitor		CLEARED - RPTR Alarm	1 time	1 minute	() Informational	AlertClear	27 = 2
LAYERX Agent Monitor	2	CRITICAL - RPTR Alarm	1 time	30 minutes	Critical	AlertHold	Logical Sector
Log Monitor		C COURSE INFINIATION	1 Mar	au menunes	Contan	Automas	¥7 = /
LX1 Call Monitor v2	1	DISREGARD - FailedNodes	1 time	1 minute	() Informational	DoNotAlert	21 = 2
LX1 SIP Call Errors v2	0	DISREGARD - UnableToRun	1 time	1 minute	() Informational	DoNotAlert	A1 = Z
Nonel Call Monitor		INDETERMINATE - RPTR Ala-	Lune	15 seconds	() Informational	DoNotAlart	21 = 2
PING Manitor	1				C monatore		
Powerware SNAP Alarma	<b>1</b> 1	ISG Alarm trap - INDETERMI.	. 1 time	1 minute	() Informational	DoNotAlart	A1 = 5
Lo training policy	11	15G Alarm trap - MAJOR	1 time	1 minute	() Major	DoNotAlert	21 = 2
Test Alares v1	TT	ISG Alarm trap - MAJOR	1 time	1 minute	(D) Major	DoNotAlart	
Aj ExperiMental		- no com nati undra	(1000	( manage	( major	DURIDURI	A1 = 2
ALSTOVEARN : Aut - Alert Exe.					(	Splaying 1 - 11 of 11 events	«first prev next last»

# 4.2.11. Clone a Policy

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

To clone a policy:

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

Policies		Rules					
Name Fails	wer	Name	Threshold	Window	Severity	Response Procedure	1
Cisco Call Monitor		CLEARED - RPTR Alarm	1 time	1 minute		AlertGear	#7 F Z
LAYERX Agent Monitor	2			Contact of	C Critical	-	
Log Monitor		CRITICAL - RPTR Alarm	1 time	20 minutes	Critical	AlertHold	¥7 = Z
LX1 Call Monitor v2	<b>X</b> 5	DISREGARD - FalledNodes	1 sime	1 minute	Informational	DoNotAlert	×1 = Z
LX1 SIP Call Errors v2		DISREGARD - UnableToRun	1 time	1 minute	() Informational	DoNotAlert	21 = 2
Nortel Call Monitor	<b>2</b> 3	INDETERMINATE - RPTR A/A	1.000	15 seconda		DoNotAlert.	
PING Monitor	1	INDETERMINATE - RPTR ALL.	. 1 teme	15 seconds	() imprimational	DONDOVER	1 = 1
Rowerwave SNMP Alarms	<b>2</b> 11	ISG Alarm trap - INDETERML	1 time	1 minute	() Informational	DoNosAlert	21 = 2
Lo training policy	1 2	ISG Alarm trap - MAJOR	1 time	1 minute	() Major	DoNotAlert	F1 = Z
Test Alarm v1	107	ISG Alarm trap - MAJOR	1 sine	t minute	(D) Major	DoNotAlert	
AJ ExperiMental	3	- ise wern wap mayon	( une	Chinage	C major	DONODAEL	1 = 2
ALSTOYBARN : Austin - Tert D						Displaying 1 - 11 of 11 events	« first prev next last

### 4.2.12. Export or Import a Policy

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

A new system log table insights\_system\_log has also been added to log user actions and a user can create a dashboard to view these actions.

See the:

Log Search Section in the Dashboard and Reporting Administration Guide.

#### + Global Filters ( 0 applied )

Click to Refresh Data 📋 Mar 9, 2022 9:09 am - Mar 9, 2022 10:09 am

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

#### **Export a Policy**

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

#### **Import a Policy**

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

#### **Policy CSV Format**

The following columns are in an exported CSV file:

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

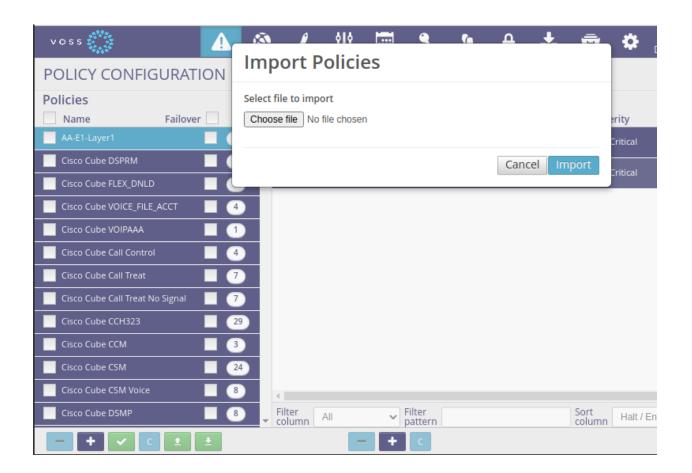
#### Note:

- The "row action" column is used when importing and if it contains "delete", then the row will be deleted upon import.
- The "respond procedure" column can be used when importing and should then contain the Response Procedure name *exactly* as it exists on the system. If a procedure is found, then it will be assigned

to the associated rule. If a new value is entered, a new Response Procedure is created. The default Response Procedure is used if no value is entered.

• The combination: "policy group name", "name", "respond procedure" should be unique in CSV row. If a policy found, its data will be updated. If not found, new policy will be inserted. The "name" has to be unique. If a rule is found, its data will be updated. If not found, new rule will be inserted to the policy indicated in "policy group name".

See: Response Procedure Configuration.



# 4.3. Asset Configuration

### 4.3.1. Overview

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

Assets can be any devices that are either sending data or from which data is being retrieved. Each asset can be assigned to a specific customer to create a multi-tenant environment.

voss 🎇 🔥 🚹	🥸 🦨 ili	🗏 🥄 🧕	🔒 📩 🖻	\$	Days remaining: Unlimited admin
ASSET CONFIGURATION					Save
Groups	Assets				
Group Name	IP Address	Asset Name	Description	Туре	Monitor Profile
All groups	• •			Unknown	No profiles set 🛛 🗡
Ungrouped 14	<b>XXXXX</b> 7.173	Local System	Local Arbitrator Platform	Server	1 profile set 🥜 💋
	127.0.0.1	127.0.0.1		Unknown	No profiles set 🕜 📝
	<b>XXXXX</b> 3.140	XXXXXXXXX140		Unknown	No profiles set 🛛 🥕 📝
	CUCM_1	CUCM_1		Unknown	No profiles set 🥜 🧪
	CUCM_2	CUCM_2		Unknown	No profiles set 🥜 💋
	CUCM_3	CUCM_3		Unknown	No profiles set 🥜 💋
	CUCM_4	CUCM_4		Unknown	No profiles set 🥜 💋
	CUCM_5	CUCM_5		Unknown	No profiles set 🥜 💋
		CUCM_6		Unknown	No profiles set 🛛 🥕 📝
	Filter All	✓ Filter pattern	Sort	IP Address 🗸 🗸	Displaying 1 - 14 of 14 assets « first prev next last » 20
- +	- + 1	±			

**Note:** A system log table (insights\_system\_log) logs user actions, and a user can create a dashboard to view these actions.

#### **Related Topics**

Log Search in the Dashboard Administration Guide

### 4.3.2. Add an Asset Group

To add a new asset group:

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

ASSET CONFIGURATION					Ch	anges have be	en made		Save	
Groups Group Name	As	sets IP Addres	s Ass	et Name	Descript	ion	Туре		Monitor Pr	ofile
All groups										
Expressway 0										
UCCE 1										
UNITY 5										
NEW GROUP										
Ungrouped 29										
Add Group	Filte	mn All	~	Filter pattern		Sort	IP Address	~	No records assets	« first

### 4.3.3. Add an Asset to a Group

To add a new asset to a group:

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

Group Name	Assets IP Address Asse	t Name	Description	Туре	Monitor Profile	
All groups	Properties Interface	5				- 1
CUCM 5	Enabled	✓		Model		
Expressway 0	Maintenance Mode			Version		
	IP Address			MAC Address		
	Asset Name			Alies		
Ungrouped 29	Description			Manufacturer		
	Host Name			Time Zone	UTC	
	Туре	Unknown	~	Customer	~	
	Address			Site	×	
	External URL					
	Filter All Y P	ilter attern		mn IP Address V		

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

Groups Group Nar	ne
🖮 All groups	
🗌 💼 DS9	s 2
📃 🏢 Exa	mpleName 1
Exan	npleName 💿
🗌 💼 Vos	s (1)
E Ungrouped	51

#### 4.3.4. Delete Assets

To delete assets in an asset group:

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

			Errors exist		Save
Assets IP Address	Asset Name	Description	Туре	Monitor Profile	
011.52.5.0 T	Local System	Local Arbitrator Platform	LaperX Node	7 profiles set	1
D 10.13.37.194	URABOS		LaperX Node	No profiles set	1 2
12/01/2.206	TempAlert	Temperature Manitor	Unknown	1 profile set	1 2
1212.27.48	1407	Paul# System	Uningen	1 profile set	1
12.99.99.99	LinkPloAetTest	LinkPlakertTest	Unknown	No profiles set	1
_		Sort IP Address 1	Displayi	ng 1 - 3 of 5 assets a fing	prev next last
Filter		Sort IP Address \$	Displaye	ng 1-5 of 5 assets + first	prev next las
	<ul> <li>IP Address</li> <li>16.13.37.199</li> <li>16.13.37.194</li> <li>16.13.37.194</li> <li>16.13.37.194</li> <li>16.13.37.48</li> <li>16.13.37.48</li> <li>16.13.37.48</li> <li>16.13.37.48</li> </ul>	IP Address         Asset Name           10.13.37.19         Local System           10.13.37.194         UXLARCS           10.13.37.194         UXLARCS           10.13.37.194         UXLARCS           10.13.37.194         UXLARCS           10.13.37.194         UXLARCS           10.13.37.40         PeaP           10.08.39.30         UnixPTtpAlectText	Assets       IP Address     Asset Name     Description       ID 13.13.17.19     Local System     Local Address       ID 13.13.17.19     Local System     Temperature Monitor       ID 13.13.17.10     PeelP     PeelP System       ID 15.18.19.19     LockPTpAlienthen     LockPTpAlenthen	Assets       IP Address     Asset Name     Description     Type       1013131719     Local System     Local Arbitrator Plation     LaperS Note       1013137194     UEAMS     Local Arbitrator Plation     LaperS Note       1013137194     UEAMS     Bengristant Manilar     Unicease       101313704     UEAMS     Bengristant Manilar     Unicease       1010137205     Bengrist     Bengristant Manilar     Unicease       1010137205     Bengristant     Bengristant Manilar     Unicease       1010137205     Bengristant     Description     Unicease       1010137205     Bengristant     Unicease     Unicease       1010137205     Local Platenties     Unicease     Unicease	IP Address     Asset Name     Description     Type     Montor Profile       1015333119     Local Address     Local Address     LopeX Node     7 profiles set       1015333119     Local Address     LopeX Node     No profiles set       1015333119     Local Address     LopeX Node     No profiles set       101532206     TempAtert     Temperasure Monitor     Unknown     1 profile set       10153233     TempAtert     Temperasure Monitor     Unknown     1 profile set       10153234     Peet     PeetP System     Unknown     1 profile set       10153344     PeetP     PeetP System     Unknown     No profiles set

# 4.3.5. Delete an Asset Group

To delete an asset group:

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

voss 🞇 🔥 🚹	1	†ļ†		٩	<u>\$</u>	Ĥ	<b>±</b>
ASSET CONFIGURATION							
Groups Group Name	Assets	ddress	Asse	et Name		Desc	ription
All groups CUCM 5 Expressway 0 CUCE 1 UNITY 5 NEW GROUP 0 Ungrouped 29							
move Group	ilter olumn	All		filter battern			So
	- 5	2	1				_

### 4.3.6. Assign a Probe to an Asset

A probe is a script or set of commands that are saved in the system and can be used to gather data, to issue commands to systems, and to auto repair or send data.

Assigning a probe to an asset is typically done to retrieve data from that asset. Commands such as an SNMP GET or an API call are used to retrieve data from a particular asset.

To assign a probe to an asset:

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

		Templates/Profiles					
Probe Group		Name	Frequency	Credentials 1 & 2	Enabled		
API System stats	1	ucce anmp	5 Minutes	anmp & None	$\checkmark$		
▶ cisco axl counters	6	ucce api	1 Minute	admin & None			
P cisco axi counters		UCCE Publish 172.30.42.	76 5 Minutes	admin & None	V	×	
cisco cucmrisphone	4						
CUCM Publish 172.30.42.73	cisco ci	sco_snmp	5				Drop Zone

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

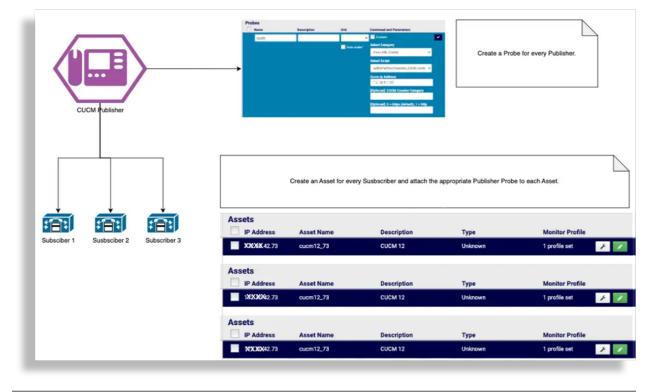
Note: For SP25, the frequency for Polycom devices is set at 5 minutes.

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

**Note:** In order to configure performance monitor probes for CUCM publishers and their related subscribers, the publisher IP address is used to create a probe with that **Cucm IP Address** value.

Each related subscriber is then created as an asset and this probe is attached to each asset.

Refer to the diagram below:



# 4.3.7. Bulk Assign Probes to an Asset

1. In the Arbitrator System Configuration Gui, select the Probes icon to open the PROBE CONFIGU-RATION tab.

voss	A	<b>(</b>	1	tiit	٩	<u>_</u>	Ĥ	₹	Ē	\$
PROBE CONFIGURA	TION									
Groups Group Name			Probes Nam		Des	cription		Unit		Command and Parameters
API System stats		1	cheo	kurl						checkURL.php
cisco axl counters		6								
cisco cisco_snmp		5								
cisco cucmrisphone		4								
CUCM Publish 177 XXXXXX/32/3		1								
CUCM Publish 1%22%XXX77		1								

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

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

ASSIGN PROBES	TO ASSETS		
Assets	Durks Assigned to Asset?	Configure	
All groups     All groups     All Groups     Groups     Groups     Groups     Groups	Probe Assigned to Asset?	<ol> <li>Select a probe group</li> <li>Select assets from list on left</li> <li>Create profile for probe</li> </ol>	
Cycle-cucm-pu Cycle-ucxn-pu Cycle-ucxn-pul		Probe Group 1b-PING Monitor	~
PANDABANK		Create Profile Frequency	Start T
V4UC      Video End Poir	nts	15 Seconds V Credential 1 None V	Days
VM HOSTS  Voice Gateway  VOSS NETWO		Credential 2 None	Duratio
VOSS SOLUTIO		Save	

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

### 4.3.8. Assign a Customer to an Asset

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

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

To assign a customer to an asset:

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

5. Click Save.

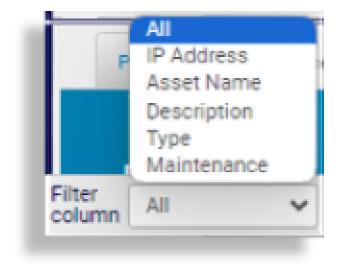
	см <b>ХХХХ</b> 73	cription Type Unknown	1 profile set	
			r prome sec	+ /
Properties Interface	15			
Enabled		Model		
Maintenance Mode	•	Version		
IP Address	V718142.77	MAC Address		
Asset Name	CUCM172.59.42.77	Alias		
Description		Manufacturer		
Host Name		Time Zone	UTC	
Туре	Unknown	✓ Customer	Customer1	<b>~</b>
Address		Site		<b>~</b>
External URL				
	Maintenance Mode IP Address Asset Name Description Host Name Type	Maintenance Mode IP Address 77.53342.77 Asset Name CUOM V72.50.42.77 Description Host Name Type Unknown Address	Maintenance Mode     Version       IP Address     \$7223142.77       MAC Address     CUCM 1723042.77       Asset Name     CUCM 1723042.77       Description     Manufacturer       Host Name     Time Zone       Type     Unknown       Address     Size	Maintenance Mode     Version       IP Address     ?71513/2.77       Asset Name     CUCM 172:50.42.77       Asset Name     CUCM 172:50.42.77       Aiss     Manufacturer       Description     Manufacturer       Host Name     Unknown       Version     Customer       Customer     Site

### 4.3.9. Place an Asset in Maintenance Mode

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

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

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



### 4.3.10. Export and Import Assets

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

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

#### **Export Assets**

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

#### **Import Assets**

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

voss 👯 🔶		Days remaining: 173	admin 🕶
ASSET CONFIGURATION	Import Assets		Save
Groups Group Name	Select files to import Choose file No file chosen	Туре	Monitor Profile
🐨 🚞 All groups			
AAAGlobal 0	Importing assets will overwrite any assets in the system.		
AcmeCorp 1			
AFD 0	Cancel Import		
AUDIO CODES 1			
BODYSHOX 5			
CSP Shared Architecture 3			
CUCM14 1			
CYCLETRONIC 5			
ELITETECHS 5			
GENCORP 0			
NEXTWAVE 2			
PANDABANK 0	Filter All V Filter Sort column	IP Address V No	records assets « first prev
- +	- + 1 1		

#### 3. Click Import.

#### **Next steps**

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

#### **Asset CSV Format**

The following columns are in an exported CSV file:

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

Note:

- Mandatory fields are: Asset Name, IP Addres.
- The "Row Action" column is used when importing and if it contains "delete", then the row will be deleted upon import.
- Row uniqueness is the combination of: "IP Address", "Customer Name", "Site Name". If an asset found, its data will be updated. if not, new asset will be inserted under the asset group indicated in column "Asset Group Name".
- The column "Asset Group Name" has to be unique. if an asset group is found, its data will be updated. If not, a new asset group will be inserted.
- There are 2 entries in the import CSV:
  - An asset with data in all columns. Most important is the very first column "Asset Name".

 An interface is a property of an asset. An interface only has data in from column "Description" to "Host Name". Most important is that it does not have data on the very first column "Asset Name". All CSV interface row(s) will be under an asset just right above it(them).

# 4.4. Probe Configuration

### 4.4.1. Overview

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

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

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

Arbitrator Cisco PRI and SIP Probe Configuration

### 4.4.2. Add a Probe Group

To create a new Probe Group:

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

voss 🎇 🔥 🛕	8	1	î₿î		٩	Ł	A	2	Ē	Days remaining: 173	admin 🕶
PROBE CONFIGURATION	Chan	ges have b	peen ma	de							Save
Groups Group Name		Probes Nam	e		Des	cription		Unit		Command and Parameters	
Polycom											
VMWARE-CPU-MEM											
vmwarev3											
Voss CPT CUCM Perfmon AXL Counters											
Voss CPT CUCXN Perfmon AXL Counters											
Voss UK CUCM Perfmon AXL Counters											
Voss UK CUCXN Perfmon AXL Counters											
Voss UK IMP Perfmon AXL Counters											
Voss USA CUCM Perfmon AXL Counters				/							
Voss USA CUCXN Perfmon AXL Counters			/								
WIGGO-Cisco Unity AXL (WIGGO-CUC-CL											
Gencorp	•										
- + 🛛 ± ±			-	+							

# 4.4.3. Clone a Probe Group

To clone an existing Probe Group:

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

voss 🎇	<b>A</b> (		🦨 🕴		٩	1	A	<b>.</b>	Ē	Days remaining: 1684	admin •
PROBE CONFIGURATIO	N									Save	
Groups Group Name		Pro	bes Name		Des	cription		Unit		Command and Parameters	
1-Cisco CUCM RIS CmDevice_creds	3	Î	RIS API data		pho	ne, media re	sources, s	SIP		cisco/cucmrisphone/collectrisphones	1
1b-PING Monitor	1		SIP Trunk							cisco/cucmrissiptrunk/collectrissiptru	1
4-Cisco CUCM Version	1		Media Resour	ces						cisco/cucmrismediaresources/collectr	1
5-Cisco RTMT	1										_
6.Cisco Expressway-API	2										
6a.Cisco Expressway Call Detail-API	1										
6b.Cisco Expressway - SNMP	2			clo	one						
7.CUCM Perfmon AXL Counters	1			/	١						
8.Cisco Unity Perfmon AXL Counters	1				<b>\</b>						
9.Cisco IMP Perfmon AXL Counters	1										
9a.CUCM-END USER	1				_ <b>\</b>						
9b.VOSS4UC	1	*		-	+						

### 4.4.4. Create a Probe

To create a new Probe:

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

PROBE CONFIGURATION	V EI	rors exist				Save
Groups		Probes				
Group Name mult/ValueProbe		Name	Description	Unit	Command and Parameters	
New SNMP Query	1	getCalPath	Nortel getCallPath		vqm/NortelGetCallPath.pl demo	1
Nortel Call Path	1				Custom	
Oracle Service probes	31			Auto-scano?	Select Category	
PexIP Configuration	T	4			Avaya	0
PING Monitor	1			/ .	Select Script Buey Doard	
	1		/		Hostname/IP	
PING Probe		/			ridschamerie	
ProbeTest	0		/		Board	
RTT Probe	0					
snmp test	1					
static 🗧 🕂 🥹	T					
						Save
PROBE CONFIGURATION		rors exist				Save
PROBE CONFIGURATION Groups Group Name			Description	Unit	Command and Parameters	Save
PROBE CONFIGURATION Groups Group Name MultivaueProbe	N D	Probes	Description Notel getCalPath	Unit	Command and Parameters	Save
PROBE CONFIGURATION Groups Group Name MILEVAULEPROSE New SHMP Query	1	Probes		Unx		Save
PROBE CONFIGURATION Groups Group Name MultivaueProbe	N D	Probes			vgm/NortelGetCaliPath.pl demo	Save 2
PROBE CONFIGURATION Groups Group Name MILEVAULEPROSE New SHMP Query	1	Probes		Unit Auto-scale?	vgm/NortelGetCaliPath.pl demo	Save Z
	N P	Probes			vom/NortelGetCaliPath.pl.demo  Custom Select Category	
	N P + (+ (2) (3)	Probes			vgm/Norte/GetCal/Path.pl.demo  Custom Select Category Avaya (Crede) Select Script  v oneya, moda, gateway, credu.d/	
PROBE CONFIGURATION Groups Group Name TrutitivalueProce New SNMP Query Nortal Call Path Cracle Service probes PedP Configuration PING Monitor	N D	Probes			vgm/NortelGetCalPath.pl.demo  Custom Select Category Awaya (Crede) Select Script  C responses customery.creds.aft getDap3Stations.creds.aft	
	N P	Probes			vgm/Norte/GetCal/Path.pl.demo  Clustom Select Category Awaya (Crede) Select Script  C anaya,mer.Siz, gataway,creda.d/ getAvayaStations,creds.sh	
		Probes			vgm/NortelGetCalPath.pl.demo  Custom Select Category Awaya (Crede) Select Script  C responses customery.creds.aft getDap3Stations.creds.aft	
PROBE CONFIGURATION      Groups      Group Name      MUEVAUEPPORE      New SNMP Query      Nortal Call Path      Dracte Service probes      PedP Configuration      PING Monitor      PING Probe		Probes			vgm/NortelGetCalPath.pl.demo  Custom Select Category Awaya (Crede) Select Script  C responses customery.creds.aft getDap3Stations.creds.aft	

### 4.4.5. Clone a Probe

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

To clone a probe:

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

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

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

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

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

#### 4.4.6. Create a Custom Probe

To create a new Probe:

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

PROBE CONFIGURATION	Erro	ors exist				Save
Groups		Probes				
Group Name		Name	Description	Unit	Command and Parameters	
Awaya Utilization Demo	1	Pre Policy IB Pkts	Pre Policy IB Pkts		genRandom pi 4000 6000	1
Awaya VQM RTCP Demo	2	Pre Policy OB Pids	Pre Policy OB Pits		genRandom pl 4000 6000	
Awaya VQM Statistics	8	Dit Rate	Bit Rate		genRandom pl 2100 2400	-
CCMM 6	7	Drop Packets	Orop Packets	kB	genRandom.pl 200 350	
CCMS 6	(41)	Urop Packets	Urop Packets	KD	-	-
CCT 6	7			_	t Custom	-
CDR Ndx Demo	1		-	Arth	ale l	
Cisco ASA SNMP Table Probe	1					
Cisco ASA Stats	2	/				`
Cisco CBQos	5			-		
Cisco CUCM Device Location	-					
Cisco CUCM LX-RTMT	8					
Cisco CUCM PerfMon Counters	6					
Cisco CUCM Phone Inventory - 10.13.37	1					
Cisco CUCM Phone Inventory - 10.13.37	1					
Cisco Finesse	2	-				
- + 0						

# 4.4.7. Delete a Probe Group

To delete a Probe Group:

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

( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( )	▲	۲	4	†↓†		٩	2	£	*	2	٠		👤 admin <del>v</del>
PROBE CONFIGURATION	Erm	ors exist											Save
Groups Group Name		Probes			Descriptio	n	Unit		Comma	and and Paran	neters		
Awaya Utilization Demo	1	Pre Po	iky 18 Piets		Pre Policy I	Pies			genRand	form.pl 4000 60	00		
Awaya VQM RTCP Demo	2	T Pre Po	ity OB Pies		Pre Policy C	to Pies			genhand	iom.pl 4000 60	00	1	
Awaya VQM Statistics	(6)	Bit Rat			Bit Rate				eardinos	form.pl 2100 24	00		
CCMM 6	7												
CCMS 6	41	Drop I	fackets		Orop Packet	0	k8		gerRand	iom.pl 200 350		1	
CCT 6	7											1	
CDR Ndx Demo	1												
Cisco ASA GAMP Table Probe	1												
Cisco ASA Stats	2												
Cisco CBQos	5												
Cist Location	P												
Cisco CUCM LX: RTMT	-												

### 4.4.8. Delete a Probe

To delete a Probe:

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

9	A	۲	4	îţî		٩	2	Ĥ	*	•	٠		1 admin -
PROBE CONFIGURATION	Err	ors exist											Save
Groups Group Name		Probes			Descriptio	n	Unit		Comma	nd and Par	ameters		
Aveya Utilization Demo	1	Pre Po			Pre Policy I				genRand	tom.pl 4000 (	6000	1	
Awaya VQM RTCP Demo	2	Pre Po	iky OB Pies		Pre Policy C	oli Pieta			geniland	tem pl 4000 (	6000	1	
Awaya VQM Statistics	6	E Bit Rat			Bit Rate				andian	lam.pl 2100.	2400	1	
CCMM 6	1	-										_	
CCMS 6	41		Accerts		Orop Packe	8	10		genkand	tern pi 200 31	50		
CCT 6	7											<b>1</b>	
CDR Ndx Demo	1												
Cisco ASA SNMP Table Probe	T												
Cisco ASA Stats	2												
Cisco CBQos	8												
Cisco CUCM Device Location	1	-											
Caso CUCM DARTMT	-												

# 4.4.9. Export and Import a Profile

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

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

A new system log table insights\_system\_log has also been added to log user actions and a user can create a dashboard to view these actions.

See the:

Log Search Section in the Dashboard and Reporting Administration Guide.

#### **Export a Profile**

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

Since this is a probe configuration, we cannot select individual profiles, so it will export all profiles in the system.

- 2. The **Export CSV** dialog opens. Enter a **CSV file name** (You do not have to add the .csv file extension) and click **Export**.
- 3. The **Export finished** dialog shows when the export file has been created. Click **Download** to save the CSV file to your selected download location.

#### **Import a Profile**

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

#### **Profile CSV Format**

The following columns are in an exported CSV file:

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

#### Note:

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

VOSS 🔅 🏠 PROBE CONFIGURATION	Import Profiles     Import Profiles     Import Profiles     Import Profiles     Import Profiles
Groups Group Name	Select files to import         Command and Parameters
	Cancel Import
- + 🛞 ± ±	

#### Assign a Probe to an Asset

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

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

MONITOR PROFILE » Local S	System											
Groups		Templates/Profiles										
Probe Group		Name	Frequency	Credentials 1 & 2	Enabled							
Cisco CUCM Version	1	Local System Stats	1 Minute	None & touy	$\checkmark$	1						
Ciana Evenenuuu	3	Test Probe	1 Minute	None & loc								
Cisco Expressway		PING Monitor	1 Minute	ray & loc	V	1						
▶ Cisco Telepresence API - Call Details	1											

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

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

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

#### MONITOR PROFILE » Local System

Groups		Templates/Profiles				
Probe Group		Name	Frequency	Credentials 1 & 2	Enabled	
Cisco CUCM Version	1	Local System Stats	1 Minute	None & touy	$\checkmark$	1
		Test Probe	1 Minute	None & loc		1
Cisco Expressway	3	PING Monitor	1 Minute	ray & loc		1
Cisco Telepresence API - Call Details	1	Cisco CUCM Version	1 Minute	ray & loc		

# 4.5. Controls

#### 4.5.1. Overview

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

### 4.5.2. Create a Control

To create a new Control:

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

NTROLS	Errors exist Pr	obes		Save
	Name	Command and Parameters	Protection	
	PEAK-AspectDB	aspect/bidwAlertInsert.pl	Off	× 1
	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	<b>2</b>
	Test Fiber Link	avaya/command.pl %s testfiber %s	off	1
	Trace Route	avaya/command.pl %s tracert %s %s	On	2
	Tracy_Control	avaya/command.pl '10.13.37.241' 'pingip' '10.13.37.241' '2'	Off	2
	USAN Reporter Forward	ReporterPush 10.10.100.101:65515 true	Off	
	Voice-Email	alert2Email.ph/193.35.222.39 smartpoint@cambridgeconsultants	L. Off	
	VossQuery	voss/gas8.sh	Off	2
		Custom		
		Select Category		
		Aspect 0		
		Select Script		
		Aspect BIDW Event Queue Insert #		

## 4.5.3. Delete a Control

To delete a Control:

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

Name	Command and Parameters	Protection	
AlertClear	alerts/ackAlert.php	off	1
AlertClear	alerts/ackAlert.php	Off	1
AlertHold	alerts/checkAlert.php	Off	1
AlertHold	alerts/checkAlert.php	Off	1
Aspect SalesForce	aspect/aspectForceInsert5oap.php 'filename.wsdi' 'username' 'pas	Off	1
Avaya FD' MED-GTWY	avaya/fix_avaya_MED-GTWY.pl %s %s %s %s	Off	1
Blink	blink.siv	Off	1
Check IP	ipinfo-aj.php %s	Off	1
Data-Email	alert2Email.php 193.35.222.39 smartpoint@carouselindustries.co	Off	1
Disable Policy	policystatus.php "POLICYNAME" disable	Off	1
Enable Policy	policystatus.php "POLICYNAME" enable	Off	1

# 4.6. Response Procedure Configuration

## 4.6.1. Overview

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

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

From release 24.2, alert details can be sent to platforms like Slack, MS Teams and Webex Teams - providing improved visibility and allowing instant collaboration.

# 4.6.2. Create a Response Procedure

To create a response procedure:

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

i 👔 🔺	🛛 🖉 🖌 🛞	🗐 🎙 🎍	A 📥 🖻	• •		1 admin-
RESPONSE PROCEDURE C	ONFIGURATION					Save
Response Procedures	Response Procedu	re Details				
CEMS State Text	Aiert Methods	Disable on Faile	MET			
Default RP Dokotiert		Bayendech.com To: su	pportBlayentech.com 5	mp Server:		email
Brail estrate	Carerai	Reboot machine	0 Delay	0 seconds	-	ciiiii
Erral,Arda	Credential 1 Credential 2	admin None	Confirm Timeout	30 seconds		Control
Deceletion Example	Control Credental 1	Link/PToAlert admin	e Delay	© seconds		Controls
Ralisver STANDBY	Credential 2	None	Confirm Timeout	30 seconds		
First Bank 24x7	Destination: 10.1	02.10	As Event? 🗹 🕑			Forward
LeyerX Support						
Unicalitation	+ Enal	+ Control + Fo	rwarder			
UnitPloAiet	De Not Run Wind					
UnkiPToAlen - Do Not Post Alen	Start Hoay					
UnitProbeToAlert	End Sunda	y 8 12am 8 00	0 0			
Local Alert DNLY						
RAKIDAspect08						
Rush to Reporter						
Rebost Machine						
Svit (hariple						
Tracy, ResProdecure						
1.04						

# 4.6.3. Assign an Alert to a Response Procedure

To assign the Alert function to a response procedure:

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

i 🔺	⊗ 1 iii iii < ½ A ± a ≎	1 admin+
RESPONSE PROCEDURE CO	NFIGURATION	Save
Response Procedures	Response Procedure Details	
CEMS Stati Text	Alert Disable on Failover	
Default IRP	Methods	
Difestion	From arbitrary Bayentech.com To: support/Blayentech.com Smitp Server:	
C Gital astrobal	Cartesi Reboot machine 8 briay Diseconds 8	
Erel,Atla	Confirm Timeout 30 seconds 1	
Decalation Example		
Talaver ACTVE	Control LinkPToNet 1 Credential 1 admin 2 Driay 0 seconds 1	
Falser STANDBY	Conform Timeout 30 seconds 4	
Ent Bank 24/7	Destruction 10.15.2.10 Autwent V	
Datket.		
Layerk Support		
Uncirentwet		
UnCeltofert	+ Email + Control + Forwarder	
Unit Unit to Airt	Do Not Run Windows	
LinketToAart - Dis Not Pest Alert	Sart Price & 12am 2 00 2	
UnitPlaten-PostAlen	End Sunday & 12am # 00 #	
UsPubelsket		
Local Alert ONLY		
TAN 05 Decrypt		
FEAKDApect08		
Push to Reporter		
Rebot Machine		
SendfotM7		
Dift.bariple		
Trag, RisProtecure		
USAN Response		
Test.		
-		

# 4.6.4. Delete a Response Procedure

To delete a Response Procedure:

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

RESPONSE PROCEDURE C	ONFIGURATION	Save
Response Procedures	Response Procedure Details	
Avaya Fix MED-GTWY CCMS-Stat-Test Default IRP DoNotAlert Email waterbei	Methods           Imail         From: arbitrator@layerstech.com         To: tier1@company.com	om 🗾
Email April Email April Escalation Example Failover ACTIVE Failover STANDBY First Bank 24x7 Just Alert LayerX Support Linic unpathToAlert		

# 4.6.5. Enable ServiceNow Integration

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 V	
	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. Uncheck Custom.
- 5. Fill in the following details:
  - Select Category: ServiceNow
  - Select Script: PushToServiceNow
  - Service Now IP Address / Hostname:
  - Service Now Username:
  - Service Now Password:
- 6. Tick the blue tick box.
- 7. Click the Save.
- 8. Navigate to the Response Procedure Configuration menu.
- 9. Apply the control to the required IRP, such as the default IRP.

### ServiceNow One Way Incident Integration

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

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

### **ServiceNow Requirements**

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

### Arbitrator Correlation Configuration

- Version Required: 4.0001-15b
- Script: servicenow/PushToServiceNow.pl
- parameters:
  - URL\_TO\_SERVICENOW\_INSTANCE
  - USERNAME
  - PASSWORD

### ServiceNow images:

Servicendw service	ice Management 🤤 System Administrator 🔹 🔍	₽ (? \$
Filter navigator	Incident <i>w</i> ↓ ↓ 00000023           Follow ↓ Update Resolve	Delete 🔨 🦊
	Configuration item         Q_         Assignment group         Q_	
My Assets	Assigned to Q	
My Notification Preferences	* Short description LXTALERT: ARB_REFERENCEID=20000-01009001-00-01-7134-14 ARB_POLICY_MODULE=MultiTest ARB_CORRELATION_RULE=Some Rule	
Guided Setup	Related Search Results 🗸	
Service Desk	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	iew Attach
Incident	Firewall Rule Change Cisco Firewall Appliance Prev	iew Order
Create New	About Windows 10 the microphone to talk with her instead. Rule the web with Microsoft Edge Microsoft Edge is the first browser Prev	iew Attach
i Assigned to me		
Open K	Notes Related Records Closure Information	
Open - Unassigned	Watch list	
Resolved	Additional comments	
All Pr Overview	(Customer visible)	
Critical Incidents Map	Work notes Post	
Problem	Activity System Administrator 2016-12-13 12-52:14	
n Change	LXTALERT: ARB.REFERENCEID=20000-01009001-00-01-7134-14 ARB_POLICY_MODULE=MultiTest ARB_CORRELATION_RULE=Some Rule ARB_MESSAGE=Some Rule: Multitest (2)	
configuration		
Password Reset	Image: System Administrator         2016-12-13 12:52:14	
Service Catalog	Impact 1 - High Incident state New	
ltem Designer	Opened by System Administrator Priority 1 - Critical	

Servicendw service	Managem	ent								system Administrator 🔻	< 급 ③	\$ \$
Filter navigator		ncidents	New Go to	Number	▼ Search					• • • • 1	to 20 of 75 🕨	••
■ ★ (0)	۵		■ Number ▼	■ Opened	■ Short description	■ Caller	■ Priority	<b>≡</b> State	■ Category	■ Assignment group	■ Assigned to	
My Assets		í	INC0020001	2016-08-10 09:14:29	test	<u>System</u> Administrator	3 - Moderate	New	Inquiry / Help			2( 05 #
My Notification Preferences Guided Setup		<b>()</b>	INC0010023	2016-12-13 12:52:14	LXTALERT: ARB_REFERENCEID=20000- 01009001-00-01-7134-14 ARB_POLICY_MODULE=MultiTest ARB_CORRELATION_RULE=Some		• 1 - Critical	New	Software			2( 12
Service Desk				2016-12-13	Rule LXTALERT: ARB_REFERENCEID=20000- 01009001-00-01-7134-16							2(
Create New Assigned to me		()	<u>INC0010022</u>	2016-12-13 12:52:11	ARB_POLICY_MODULE=MultiTest ARB_CORRELATION_RULE=Some Rule Major		• 2 - High	New	Software			12
8 Open R Open - Unassigned Resolved		(j)	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			20 12
P <sup>C</sup> All T Overview Critical Incidents Map		<b>(</b> )	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			20 12
Problem					LXTALERT:							

# 4.7. Credential Configuration

## 4.7.1. Overview

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

# 4.7.2. Create a Credential

To create a Credential:

- 1. Click the "key" icon in the menu bar at the top.
- 2. Click the plus icon in the bottom left corner.
- 3. Enter the name to be assigned to the Credential.
- 4. Enter the Username, Password and Confirm fields.

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

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

Name	Username	Password	Confirm	
	Username	Password	Commit	-
LXTREADONLY	*******	********		1
SiLo Test Cred	*******	********		1
snmp community public	********	********		1
SNMP RO String	********	********	********	1
Tandburg	********	********	********	1
UCAXLAPI	*******	********		1
VOSS API	********	********	********	1
Windows Agent probe	*******	********	********	1
				~

# 4.7.3. Delete a Credential

To delete a Credential:

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

Labrimicreos	Username	Password	Confirm	-
LxtAutoGen 1489019854046	********	********		1
LXTREADONLY	********		********	1
SiLo Test Cred	*******	********	********	1
snmp community public	********	********	********	1
SNMP RO String	********	********	********	<ul> <li>Image: A set of the set of the</li></ul>
Tandburg	*******	********	********	
UCAXLAPI	*******		*******	1
VOSS API	********	********	********	1
Windows Agent probe	********	********	*******	1

# 4.8. Customer Configuration

## 4.8.1. Overview

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

(See: Asset Configuration, Access Control Configuration).

# 4.8.2. Create a Customer

To create a Customer:

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

CUSTOMER CONFIG	URATION		Save
Customers		Sites Name	
Arda Virtual Customer 1	2		
Arda Virtual Customer 2	2		
Arda Virtual Customer 3	2		
LayerX Virtual Customer	1		
SiLo Custoemr 1	T		
test	1		

### 4.8.3. Create a Customer Site

To create a site for a Customer:

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

CUSTOMER CONFIG	URATION	Errors exist	Save
Customers		Sites	
Name		Name	
Arda Virtual Customer 1	2		
Arda Virtual Customer 2	2		
Arda Virtual Customer 3	2		
LayerX Virtual Customer	1		
SiLo Custoemr 1	(T)		
test	2		
-			

# 4.8.4. Delete a Customer

To delete a Customer:

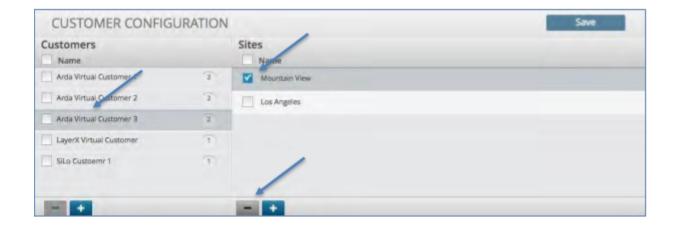
- 1. Click the check box of the customer you wish to delete.
- 2. Click the minus icon in the bottom of the site panel.
- 3. Click the Save icon to in the upper right corner.

CUSTOMER CONFIG	URATION		Save
Customers		Sites	
Arda Virtual Customer 1 Arda Virtual Customer 2 Arda Virtual Customer 3 LayerX Virtual Customer SiLo Custoemr 1	2 2 1 1 1	Mountain View Los Angeles	
- 0			

# 4.8.5. Delete a Customer Site

To delete a site for a Customer:

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



# 4.9. Access Control

### 4.9.1. Overview

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

You can select the following tabs on this page:

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

# 4.9.2. Permission Groups Tab

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

### **Create a Permission Group**

To create a Permission Group:

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

Group Name	Realm Context	Timeout		
Science Logic	(local)			1
SuperUser	(local)			1
Admin	(local)			1
SiLo Test	(local)			1
Guest	(local)			1
Typical	(local)	22		1
Monitor	(local)			1
Test Permissions Users	/		/	
Permissions. Users	Ani	alytiX :: Correlate	/	
	/	-	VIEW - Pung Search	
Permissions. Users	Ani	alytiX :: Correlate	VIEW - Pung Search VIEW - Call Path Monitor	
Permissions Users VIEW - Main Application	Ani VIEW - Asset Explorer	alytiX :: Correlate VIEW - Alarm Analyzer		
Permissions Upers VIEW - Main Application VIEW - Policy Monitor	Ani VIEW - Asset Explorer VIEW - Asset Map Explorer ACTION - Delete Paths	alytiX :: Correlate VIEW - Alarm Analyzer VIEW - Cail Details		
Permissions Upers VIEW - Main Application VIEW - Policy Monitor	Ani VIEW - Asset Explorer VIEW - Asset Map Explorer ACTION - Delete Paths	alytiX :: Correlate VIEW - Alarm Analyzer VIEW - Call Details ACTION - Disposition Alerts		
Permissions Users VIEW - Main Application VIEW - Policy Monitor ACTION - Delete Calls	Ani VIEW - Asset Explorer VIEW - Asset Map Explorer ACTION - Delete Paths Anie	alytiX :: Correlate VIEW - Alarm Analyzer VIEW - Call Details ACTION - Disposition Alerts ayltiX :: Configure	VIEW - Call Path Monitor	

#### Assign and remove users to/from a permission group

#### Assign a User to a Permission Group

**Note:** From release 24.1, a permission group API has been added for the new voss\_agent\_api\_user. This group has no permissions. Refer to the *Users Tab* for details on the new user in this group.

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

Group Name	Realm Context	Timeout	
Science Logic	(local)		
SuperUser	(local)		
Admin	(local)		1
SiLo Test	(local)		
Guest	(local)		
Typical	(local)		
Manitor	(local)		
Test	(local)		
	Users in Group	All Users	
testing		Administrator	
		Alain Jansen	
		Andrew Freisch	
	1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 -	Arda Savran	
	Dra	Guest Account	
		layerx	
		testing2	
		View Only	
		Vodafone	

# 4.9.3. Users Tab

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

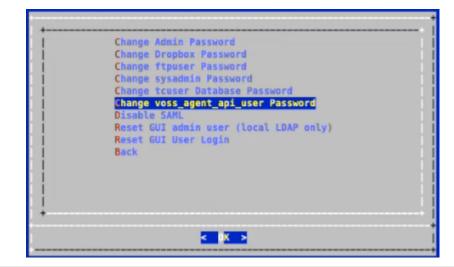
**Note:** From release 24.1, a new user voss\_agent\_api\_user has been added that is specifically used by the VOSS Insights Forwarder - an agent that collects statistics such as latency and response times on various cloud endpoints, along with system CPU statistics, which is sent by means of the API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

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

· Editing the user on the Users form.

#### or

• Using the administrator console menu: Administration > Change Passwords.



#### Add a new user

To create a new User:

- 1. Click the User tab at the top of the screen next to Permission Groups.
- 2. Click the blue plus icon at the bottom of the screen.
- 3. Fill in the required fields. (Full Name, Username, Password, Confirm and Email).
- 4. Check the Super-User box if applicable.
- 5. Check the Force Password Change if you want this user to follow the Password Policy.
- 6. Click the Locked Out box if you want this user to time on inactivity on the UI.
- 7. Select the Customer drop-down box and assign the user to a customer.
- 8. Check the Disable multi-tenancy if this is a single customer and multi-tenancy does not apply.
- 9. Click the Blue check icon to set the user.
- 10. Click the Save button to save the user.

Full Name       Username       Password       Confirm       Email       Super-User       Force Password Change       Locked Out         Administrator       admin       ********       afrosch@layenstech.com       *******       afrosch@layenstech.com       *******       *******       ajansen@layenstech.com       *******       *******       afrosch@layenstech.com       *******       *******       afrosch@layenstech.com       *******       *******       afrosch@layenstech.com       ********       *******       *******       *******       *******       *******       *******       *******       *******       *******       *******       *******       ********       ********       ********       ********       ********       ********       ************************************	iter			Sort Fu	I Name \$	-	1	1		
Alain Jansen       ajansen       ********       ajansen@layerstech.com       Image: Comparison of the compa	Full Na	me	Username	Password	Confirm	Email	Super-User	Force Password Char	nge Locked Out	t
Andrew Frosch       afrosch       ••••••••       afrosch@layerxtech.com       Image: Commentation of the commentation o	Adminis	trator	admin	******	********	afrosch@layerxtech.com	5			1
Arda Sawran       asavran       ********       asavran@layerxtech.com       Image: Comparison of Compar	Alain Jan	isen	ajansen	********	********	ajansen@layerxtech.com	23			1
Guest Account       guest       ********       support@layerxtech.com       Image: Comparison of Compar	Andrew	Frosch	afrosch	********	********	afrosch@layerxtech.com				1
layerx       layerx       ********       support@layerxtech.com       Image: Comparison of the support@layerxtech.com         testing       testing2       testing2       ********       support@layerxtech.com       Image: Comparison of the support@layerxtech.com         View Only       viewonly       ********       support@layerxtech.com       Image: Comparison of the support@layerxtech.com         View Only       viewonly       ********       support@layerxtech.com       Image: Comparison of the support@layerxtech.com         Vodafone       voda       ********       support@layerxtech.com       Image: Comparison of the support@layerxtech.com         wstrobel       wstrobel@layerxtech.com       Image: Comparison of the support@layerxtech.com       Image: Comparison of the support@layerxtech.com	Arda Sav	vran	asavram	********	********	asavran@layerxtech.com	23			1
testing       testing       ********       support@layerxtech.com       Image: Comparison of Comparison	Guest A	ccount	guest	********	********	support@layerxtech.com				1
testing2       testing2       ********       support@layerxtech.com       Image: Comparison of the comparis	layers		layerx	********	********	support@layerxtech.com	23			1
View Only       viewonly       ********       view@layerxtech.com       Image: Common Com	testing		testing	*******		support@layerxtech.com	53			1
Vodafone       voda       *******       support@layerxtech.com       Image: Comparison of the comparison of	testing2		testing2	********		support@layerxtech.com	22			1
wstrobel wstrobel wstrobel@layerxtech.com	View On	by .	viewonly	*******	********	view@layerxtech.com				1
	Vodafor	e	voda	*******	********	support@layerxtech.com				1
	wstrobe		wstrobel	********	********	wstrobel@layerxtech.com	5			1
Customer								10		~
	Custome	er		‡ Disa	ble multi tenancy				/	
	per-Users o	an do an	ything in any cor	ntext.						

#### Delete a user

To delete a User:

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

# 4.9.4. Nodes Tab

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

### Create a node

To create a Node:

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

System	GUI IP Address 10.13.37.5	Username	Password	Direct	Secure	Appliance	
devarb	10.14.37.5	admin				Arbitrator	1
demoarb	10.13.37.119	admin	********		22	Arbitrator	1
ePlus	10.13.37.160:62001	admin	********		12	Arbitrator	1
trab	10.13.37.12	admin	********		122	Arbitrator	1
						✓ Arbitrator Reporter	

#### Delete a node

To delete a Node:

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

# 4.9.5. Realms Tab

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

### Create a realm

To create a Realm:

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

Name	
Deployment LayerxDev	
/	
Devices in Realm	All Devices
	devarb
, Drag /	demoarb
	ePlus
	trab

#### Delete a realm

To delete a Realm:

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

# 4.9.6. Protected Subnets Tab

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

#### Create a protected subnet

To create a Protected Subnet:

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

### Delete a protected subnet

To delete a Protected Subnet:

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

	Name	IP Address	Mask	
	internal_172_16	172.16.0.0	255.255.0.0	
	ANA1918_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	2
	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	<b>2</b>
	Google (subset 2)	209.185.108.129	255.255.255.128	
	IANA_10	10.0.0.0	255.0.0.0	2
	Google (subset 3)	64.68.88.0	255.255.248.0	<b>2</b>
	LOOPBACK	127.0.0.0	255.0.0.0	2
	ANA1918_172_16	172.16.0.0	255.240.0.0	2
	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	2
	APIPA_168_254	169.254.0.0	255.255.0.0	2
	Internal_3	192.168.1.0	255 255 255 0	2
	Internal_125	192.168.125.0	255.255.255.0	
_	*		255 255 255 255 1	

# 4.9.7. Password Policy Tab

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

#### Create a password policy

To create a Password Policy:

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

CCESS CONTROL Pe	rmission Groups Users No				Password Policy	
	Minimum Length	7	*			
	Minimum Uppercase	1	< ×	A-Z		
	Minimum Lowercase	1	*	a-z		
	Minimum Numeric	t	×	0-9		
	Minimum Special	1	× ×	!@#\$%^&*()[]		
	Password Lifespan	0	* *	days		
	Maximum Login Attempts	20	*			
	F	Save				

# 4.9.8. SAML Tab

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

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

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

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

#### Set up SSO via SAML

To create single sign-on via SAML:

- 1. Click the SAML tab at the top of the screen (adjacent to Password Policy). The attributes on this page require you to interact with your administrator of allowed users.
- 2. Click the box next to Enable SAML.

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

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

Enable SAML	
Disable Multi Tenancy	
SAML Signature Algorithm	sha1 ¢
Attribute Mappings	
Email (Optional):	
Username (Optional):	
First or Display Name (Optional):	
Last Name (Optional):	
Identity Beneddae Matadata VIII	
Identity Provider Metadata XML * Required	
Paste your metadata XML here	
Service Provider Information	
	ntily Provider
Service Provider Information Provide this information to your Idea Audience URI (SP Entity ID):	ntly: Provider http://demoarb.layentech.com/sami2/module.php/sami/sp/metadata.php/default-sp
Provide this information to your Ider	
Provide this information to your ider Audience URI (SP Entity ID):	http://demoarb.layerxtech.com/sami2/module.php/sami/sp/metadata.php/default-sp
Provide this information to your Ider Audience URI (SP Entity ID): Single Login URL:	http://demoarb.layenxtech.com/sami2/module.php/sami/sp/metadata.php/default-sp http://demoarb.layenxtech.com/sami2/module.php/sami/sp/sami2-acs.php/default-sp

inable SAML	
isable Multi Tenancy	
SAML Signature Algorithm	shat ‡
Attribute Mappings	
imail (Optional):	
Jsername (Optional):	
irst or Display Name (Optional	
ast Name (Optional):	SAML Metadata
* Required Poste your metadota XML here	<md:entitydescriptor <="" p="" xminsmd="um:oasis:names:tc:SAML:2.0:metadata"> xmins:ds="http://www.w3.org/2000/09/xmidsig#" entityID="http://www.w3.org/2000/09/xmidsig#" entityID="http://www.w3.org/2000/09/xmidsig#" end:SPSSODescriptor protocolSupportEnumeration="um:oasis:names:tc:SAML:1.1:protocol um:oasis:names:tc:SAML:2.0protocol"&gt; cmd:SPSSODescriptor use="signing"&gt; cds:KeyInfo xmins:ds="http://www.w3.org/2000/09/xmidsig#"&gt; cds:X509Centificate&gt;MIID5zCCAs+pAwIBAgLIAIy0+0SPIFX0MADGCSqGSIb3DQEBCwUAMIGJMOswC QYDVQQGEw.JVUzEOMAwGA1UECAwFVGV4YXMxDzANBgNVBAcMBkhydmiuZzEPMA0GA1UECgwG GF5ZXJ4MQ&amp;wDQYDVQQLDAZYXIIcngxEDA0BgNVBACMBkhydmiuZzEPMA0GA1UECgwG GF5ZXJ4MQ&amp;wDQYDVQQLDAZYXIIcngxEDA0BgNVBACMBkhydmiuZzEPMA0GA1UECgwG GF5ZXJ4MQ&amp;wDQYDVQQLDAZYXIIcngxEDA0BgNVBACMBkhydmiuZzEPMA0GA1UECgwG GF5ZXJ4MQ&amp;wDQYDVQQLDAZYXIIcngxEDA0BgNVBACMBkhydmiuZzEPMA0GA1UECgwG GF5ZXJ4MQ&amp;wDQYDVQQLDAZYXIIcngxEDA0BgNVBACMBkhydmiuZzEPMA0GA1UECgwG GF5ZXJ4MQ&amp;wDQYDVQQLDAZYXIICngxEDA0BgNVBACMBkhydmiuZzEPMA0GA1UECgwG GGF2XJ4MQ&amp;wDQYDVQQLDAZYXIICngxEDA0BgNVBACMBkhydmiuZzEPMA0GA1UECgwG GGF2XJ4MQ&amp;wDQYDVQQLDAZYXIICngxEDA0BgNVBACMBpVDVQDDDAUZJcnZpbmcxDzANBgNVB AdMBmxheWVyeDEPMA0GA1UECwwGbGF5ZXJ4MRAwDgYDVQDDDAUZZwYXJIMSUwWYJK02DI vNAQKBF7zzXBw0xbUDQ48UWYeHIFIZJY2WY2MIBJNNBGA0EFAAOCA08AMIBCgK CAQEA42gbuCZEgq3E/RirivoMyyiPYtcsGiTvqvuKmbkmD9eP75vBS4fQvIT55HY7DW722GrjGqsipKss DPBIMBkBJIMJUDK4V3L0TCoa5Q5u0rjD9YLSeVAMsm0aNF/X1dTAb3LcSWqMoen7PsMnBCQclmL HxB6K5ZcGSNAUfKKdnTep4yngtckRJUbXh2wVbD/r0JZFk+D7yDLSapte41DbVmFJRCia7LgkGdvH1 hB0KV0JQ0PV02252w2T5xiwwbdwIDAQA801AwTjAdBgNVHQ4EFgQUUVDA8BaubH6IUtzgbEVEm8w8IB QsFAAOCAQEAyk094TvcTgZxuoNhcX2019T6v171R2U280UB94BswbNmP9vXP68IA9dzImi4TUH1DyJ E2-M44Hcz07D2zh6DUH2ZWWZIXn0dxFzuYATidsWEZn+BXT+vOSW9IPDTBAUwAwEBZANBgknkMi6Bw0BA QsFAAOCAQEAyk094TvcTgZxuoNhcX2019T6v171R2U280UB94BswbNmP9vXP68IA9dzImi4TUH1DyJ E2-W44Hcz07D2zh6DUH2ZWWZIX00dxF</md:entitydescriptor>
Service Provider Information	
Provide this information to your I	dentity Provider
1	
Audience URI (SP Ender 10):	http://demoarb.layendech.com/samt2/module.php/samt/sp/metadata.php/default-sp
Single Login URL:	http://demoarb.layendach.com/saml2/module.php/saml/sp/saml2-acs.php/default-sp
Single Logout URL: Metadata:	http://demoarb.layenxtech.com/saml2/module.php/saml/sp/saml2-logout.php/default-sp View Details Download

Disable Multi Tenancy	Enable SAML		
Attribute Mappings Enail (Optional): Username (Optional): Istr or Display Name (Optional): Ist Name (Optional): Is	Disable Multi Tenancy		
Email (Optional): Username (Optional): Erst or Display Name (Optional):  Asst Name (Optional):  Casst	SAML Signature Algorithm	sha1	+
Username (Optional); First or Display Name (Optional): Last Name (Optional): Identity Provider Metadata XM * Required Poste your metadata XML here Big Not Certificate Poste your metadata XML here Gif 2MOBWO CYDVQCIDAZ3WICBITELMAKGA1UEBhMCVVMxDJAMBgNVBAQMBZVBI Ggr SMOBWO CYDVQCIDAZ3WICBITELMAKGA1UEBhMCVVMxDJAMBgNVBAQMBZVBI Ggr SMOBWO CYDVQCIDAZ3WICBITELMAKGA1UEBhMCVVMxDJAMBgNVBAQMBZVBI GGF SXL4MMRAW DQYDVQDDDAZ3WICBITELMAKGA1UEBhMCVVMxDJAMBgNVBAQMBZVBI GGF SXL4MMRAW DQYDVQDDDAZ3WICBITELMAKGA1UEBhMCVVMxDJAMBgNVBAQMBZVBI GGF SXL4MMRAW DQYDVQDDDAZ3WICBITELMAKGA1UEBhMCVVMxDJAMBgNVBAQMBZVBI GGF SXL4MMRAW DQYDVQDDDAZ3WICBITELMAKGA1UEBhMCVVMxDJAMBgNVBAQMBZVBI GGF SXL4MMRAW DQYDVQDDDAZ3WICBITELMAKGA1UEBhMCVVMxDJAMBgNVBAQMBZVBI GGF SXL4MMRAW DQYDVQDDDAZ3WICBITELMAKGA1UEBhMCVVMxDJAMBgNVBAQMBZVBI GGF SXL4MMRAW DQYDVQDDDAZ3WICBITELMAKGA1UEBhMCVVMxDJAMBgNVBAQMBVBI GGF SXL4MMRAW DQYDVQDDDAZ3WICBITELMAKGA1UEBhMCVVMxDJAMBgNVBAQMBVBI GGF SXL4MMRAW DQYDVQDDDAZ3WICBITELMAKGA1UEBhMCVVMxDJAMBgNVBAQMBVBI GGF SXL4MMRAW DQYDVQDDDAZ3WICBITCACAQBAMIBCQKCAQEA 42gbVCZEgg3E/FirthvoMyJNM1SGGTRQUKMBAWGABACEFAAQCACABAMIBCQKCAQEA 42gbVCZEgg3E/FirthvoMyJNM1SGGTRQUKMBAWGABACEFAAQCACBAMIBCGKCAQEA 42gbVCZEgg3E/FirthvoMyJNM1SGGTRQUKMBAWGABACEFAAQCACBAMIBCGKCAQEA 42gbVCZEgg3E/FirthvoMyJNM1SGGTRQUKMBAWGABACEFAAQCACBAMIBCGKCAQEA 42gbVCZEgg3E/FirthvoMyJNM1SGGTRQUKMBAWGABACEFAAQCACBAMIBCGKCAQEA 42gbVCZEgg3E/FirthvoMyJNM1SGGTRQUKMBAWGABACEFAAQCACBAMIBKGWVYSCEGSINAUHKKBW ECeYSRBMHKWYVYDDICAZEA+DTY, VDLSsgtr6411bWmFJRC137_gkSdqV+FhB0 KV1QVQCSZ8WZT3WWbDMNPWZPBBAUUVDDBSswVHCHEEBWEBWDAVDVPDT BAUwAwEB/ZANBgkqkkiG9w0BAQEFAAQCAQEAkW094TvcTgZxu0NhcX2019T6v171 RCC280UIb3ydBSWNNPMPWZPBBABAZImi4TUHDWJEEEHKBKDA4 VySZ770dVCQPBTZJUVSBLIZJQUVFR00HIm6nkEVUS98JVLXSXQiv3NTbtzQeVBBpUVOBy GYBEVGBPVSHLWHYVYVPODIHm6nkEVUS98JVLXSXQiv3NTbtzQeVBBpUVOBy BAUWAWEB/ZANBgkqkkiG9W0BAQEFAAQCAQEAWBZEHMTUHDW3GEFEABCYCByWBBHDADAVDVPDT	Attribute Mappings		
First or Display Name (Optional):       SAML Certificate       X         Identity Provider Metadata XM * Required	Email (Optional):		
Last Name (Optional):       SAML Certificate       X         Identity Provider Metadata XIX       "Required       MIDS2CCAs+gAwIBAGIJAb()+05PIFX0MA0GCSgGSIb3DCEBC//UAMIGJI/QawCOYD       X         Poste your metadoto XML here       MIDS2CCAs+gAwIBAGIJAb()+05PIFX0MA0GCSgGSIb3DCEBC//UAMIGJI/QawCOYD       X         VQCgBwi/VU2EOMAwGA1UECAWFVGV4YXMx0zANBgNVBAc/MBkiydmiu2EPMA0GA1UE       GwdBicF52X,44MCBw0DQ/DVQQLDA2sYXIIcngxEDA0BgNVBAc/MBkiydmiu2EPMA0GA1UE       X         MIDS2CC22gg3E/RFNVCHWBW/DQUDDA2dx2XxYXIIcngxEDA0BgNVBACMBBiydBACMBBVPII       GgC3zdQBw0QO/DVQQLDA2sYXIIcngxEDA0BgNVBACMBBVPII/QEDPMA0GA1UECOwG       GwdBicF52X,44MCBw0QYDVQQLDA2sYXIIcngxEDA0BgNVBACMBBVPII/QEDPMA0GA1UECOwG         GgC3zdQBw0QO/DVQQQDDAdxZzczpbmcxDzANBgNVBACMBBVPII/QET2xBMb0AJD       GgCxheWVQeHDY2gy2929HIIBIJABgqchkiG9w0BACEFAACCAQBAMIBCGKCAQEA         AzgbuC2Egg3GFRHvoMyjNY15SGTQuVUKmbkmD9eP75vB54tQ)T55HY7DW72z       Grigajpisk5sDPBIMtBkBUMIUbX4V3L0TC0acq5u0rj09YLSeVAMsm0aNFX1       dtAb3Le9VqMceh7PsvMn9QQCImJ+x3J2BvAGS780C6BUUhD4d8U4E5MsJ+x1W       ECY5RBN16c74550C9Y9B8UU000qgBmkBXYXICCXWNVLYXBG52cG3NAUHKKAN       Tep4yhgtckRLUbXh2wVbD/0XJZFk-D7yDL3Sgto41DbVmF_JRCla7LgkGdqV-AFB0       KY107VQ0Q55w275siwwbdwIDAQABS7AVCGACAACAAK90A1VCTgZbSouADH6Ut22pf0UVF2       MV2DN00H2BSgto41B9VXP6BiABgto111HUHDX4X2UT022F00UVF2       KY107VQ0GBSgto41HW7VN0BBBWNMP9VXP6BiABgto111HUHDX4X2UT022F00UVF2       KY107VACB52V31HMBWBWABABAHBWBWABABAHBWBWABABABABBWBBWBBBBBBBB	Username (Optional);		
Identity Provider Metadata XM * Required BEGIN CERTIFICATE MIIO5zCCAs-gAwlBAgIJAIy0+0SPIFX0MA0GCSqGSIb3DQEBCwUAMIGJIMQswCQYD VQQ6EwJVUzEOMAwGA1UECAwFVGV4YXMDzANBgNVBAcMBKvdmiuZzEPMA0GA1UE GwGbGF5ZXJ4MQ8w0QYDVQQLDAZsYXItorgxDaABgNVBAMMB2RidnBhomkuTAj BgkqhkiG9w0BCQEWFnN1CHBvonRAbGF5ZXJ44GVjaC5jb2CWHcNNMgWNTE3M[jx MzQ3WhcNMigwMTE3M[jxMzQ3W)CBTELMAkGA1UEBhMCVVMxDJAMBgNVBAgMBVPI eGFzMQBw0DQYDVQQDDAdkZX2VYXJIMSUMWAJKoZINvcNAQk8FhZzdXBw0J30 QGxheWVyeHRIY2guY29MIIBJANBgkqhkiG8w0BAQEFXAQCAQBAMIBCGKCAQEA 4ZgbuC2Egg3FrRHvhvMyyNtresfTvquuKmbkmDaPF7x9B34V0/T55HYT0W7zz Gr[Gqs]ptk5sDPBIMt6kBUIMIUbK4V3L0TCoaCq5u0rjD9YLSeVAMsmDaNF/X1 dTAb3Lc9VqMceh7Ys9MM9CQCImu+x3J2BVMAGS780CG8ULhD4d8U4E5WsJ+x1 w ECeYsFRGN16e7X550CF9B6L/D00pqEmk6xYXICCKXWNVLTKIK5GZcGSNUHKKin Tep4yhgtckRJUbXhzwVbD/rQJZFk+D7yDLSspfc41DbVmFJRCla7LgkGdqV+RhB0 KVTQDVQSZ6w2T5xlxWbdwIDAQAB01Awr1Ad5g1VHQ4EFgQUUvfDaBSaubH6IUtz gEVEm8v8timVaYDVP0T BAUwwE8iZANBgkqhkiG9W0BAQsFAACCAQEA/W094TreTgZxuoNhcX209T6VTI R20280UB9d58xbNmP9vXP69IA8dzImI4TUHTDWqEIzeLMW4HZ07DZzh60UW+z NW2XmodxFzuYXHd8VKEZ+BXK+033w8IPNmgPPFbK86XX6Jum682D9V0By GN15XXJabDISg7V/9WEYXP00IHm6nkEVJ8V82F8UK5gLWMSTbt2D0MBpuVDBy GN15XXJabDISg7V9WEYXP00IHm0nkEV2D895JLxXcjw3NTbt2Q0MBpuVDBy GN15XXJabDISg7V9WEYXP00IHm6nkEV2B85jLc8Xcjw3NTbt2Q0MBpuVDBy GN15XXJabDISg7V9WEYXP00IHm6nkEv2B85jLc8Xcjw3NTbt2	First or Display Name (Optional		
* Required MIDStCCAs+gAwiBAgLAIy0+0SPIFX0MA0GCSqGSIb3DQEBCwUAMIGJMQswCQYD VQQGEwJVUzEOMAwGA1UECAwFVGV4YXMDzANBgNVBAcMBkiydmiuZzEPMA0GA1UE CgwdbdF5ZSU4M0GM0QYDVQUDAZsYXIiongxEDA0BgNVBACMBkiydmiuZzEPMA0GA1UE CgwdbdF5ZSU4M0GM0QYDVQUDAZsYXIiongxEDA0BgNVBACMBkiydmiuZzEPMA0GA1UE CgwdbdF5ZSU4M0GM0QYDVQUDAZsYXIiongxEDA0BgNVBACMBkiydmiuZzEPMA0GA1UE CgwdbdF5ZSU4M0GMVCBICEAwFVGV4YXMDzANBgNVBACMBkiydmiuZzEPMA0GA1UE CgwdbdF5ZSU4M0GMVCBICEAwFVGV4YXMDzANBgNVBACMBkiydmiuZzEPMA0GA1UE CgwdbdF5ZSU4M0GMVCBICEAWFN1cHBvcmAbGF5ZSU4dQSjbCSbVHncNMTgWTE3M[ix Mz03WhcNMgwMTE3M[ixMZ03W)CBITELMAkGA1UEBhMCVVMxDJAMBgNVBAgMBVFI e6F2M0GW0DQVDVQDDAZLczDpbmcxbzANBgNVBAMBXVBAQMBAQBFAAQCAQBAMIBCgKCAQEA 42gbuCZEgdE7RH+MVMyNJYNtsoSiTrayuKmbkmDaeP75xBs4rdVJT55HYT0W7Zz GrjGqsjrpK5sDPBIMt6kBUMIUbK4V3L0TCoaCq5u0rj09YLSeVAMsmDaNF/X1 d1Tab3Lc3VqMoen7PsvMn9CqCImu+x3J2BWAGS780C68UUhD4d8U455WsJ+x1w ECer¥BrGIN167A1560FYB8LUD00pqEmk8xYXIC6XWNULTXt8G5ZcGSNLHKkdn Tep4yhgtcKRJUbXh2wVbD/rOJZFk+D7yDLSept41DbVmFJRCla7LgkGdqV+RhB0 KV1Q0VQ5Z6w2T5xiwwbdwIDAQAB01AwTJAd5gVHQ4EF2gQUUVD2BSaubH60Utz gbVEm8w8timM4Y0VDPIT BAUwawEE/2ANBgkqhkiG9w0BAQEFAAQCAQEAyk094TvcTgZxuoNhcX20f9T6VT1 R20280Uh9VdBSwbNimP9vXP69IA962imi4TUHTDwJqEIz+MM4HK207D2Zh60UW+Z NW2XhondxFzuYATidsWPXP69IA962imi4TUHTDwJgEIz+MM4HK207D22h60UW+Z NW2XhondxFzuYATidsWF2YP00Hm6nkEvUg9SyLxsXcjw3NTbtz0eMBpuVOBy GVBIEVGP984-100Hm6nkEvUg9SyLxsZcjw3NTbtz0eMBpuVOBy GVBIEVGP984-100Hm6nkEvUg9SyLxsZcjw3NTbtz0eMBpuVOBy GVBIEVGP984-100Hm6nkEvUg9SyLxsZcjw3NTbtz0eMBpuVOBy GVBIEVGP984-100Hm6nkEvUg9SyLxsZcjw3NTbtz0eMBpuVOBy GVBIEVGP394	ast Name (Optional):	SAML Certificate	×
	* Required	MID5rCCAs+gAwiBAgLIAIy0-05PIFXDMA0GCSGSIb3 VQQGEwJVUzEOMAwGA1UECAwFVGV4YXMDzANBgi CgwGbGF52XLI4MQ3wDQYDVQQLDA2sYXIcngxEDA0G BgkqhkiG3w0BCQEWFnN1cHBvcrAbQF52XLI4(GylgC MzQ3WhcNMigwMTE3MjkMzQ3WjCGiTELMAkGA1UEB GF2XLJ4MRAwDgYDVQQDDAdc2X2wYXLIMSUwhwYJ QGxheWVyeHRIY2grY29tMIBIJANBgkqhkiG3w0BAQEF 42gbuC2Egq3E/RHv0MyJhYtscSiTvqukkmbkmD39P72 GrjGqsjpk5sDPBIMf8kBUIMUbK4V3LDTCacQsUnJp9 diTAb3Lc9VqMceh7PsvMn9CqCImJ+x3J28vAGS780C6 ECaYsRGN16c7AJ6505Yr9BeUU000pq6mk8xYXIC68WN Tep4yngtckFJUbXh2wVb0/rQJZFk+D7yDL5spfc41DbVn KVtj0pVQ5Z5w2T5xlwwbdwIDAQaEAA0CAC2EAk054 gbEVEm8v8ttwHwYDV90jBBgwFoAUUvDaBSaubH8fUU BAUwAwEB/2ANBgkqhkiG9w0BAQEFAA0CAC2EAk094 R20t280Uh8ydBSwbNmP9vXP68LA92Ini4TUH7bwJqE1 WV2XhodxF2UYA11tdsVkE2n+BXT+vQ3w9fPnmgPFbb yVS7750VDCPBT2Julv8Li2QGUri1MDi3R92+EtitKUrlit br315XKoJaDISq7V9WEYXP00IHm6nkEvU885yJLxsXcj GWaIEWjGFyg8++v3qJluoC0L17bL2Fek2rCg/9w62zF	NVBAcMBklydmiu2zEPMA0GA1UE 3gNVBAMMB2RidzEPMA0GA1UE 3gNVBAMMB2RiddnBhombuTAj 5jb20wHncNMTgwMTESMjtx hMCVVIMxDjAMBgNVBAgMBVRI MBmxheWVyeDEPMA0GA1UECowuG KoZihvpNA0KBFhz2x0KBwb3J0 AAOCAQBAMIIBCgKCAQEA wBS4f0yIT55HYT7DW72z YU.SVAMsm0aNF/X1 BUUhD4d8Uf4E5/WsJ+x1W MUTKIBG5ZcdSNAUHKKdn hFJRClarLgkGdqV+RhB0 1EFgQUUvfDaBSaubH6fUtz 2gbEVEm8v8thwDAYDVR0T Tv=TgZxu0NhcX20915w171 tv=TgZxU0NhcX20915w171 tv=M4HKz07DzZh60UW+Z &B6XV8eJum63cill8Kbd4 4CUVsn9h40tzDY0 aNTbtzDeMBppuVOBy
	Single Login URL:	http://demoarb.layerxtech.com/sami2/module.php/sam	
		View Details Download	and an in adhemic of a against the
Single Logout URL: http://demoarb.layen.tech.com/sami2/mcdule.php/sami/sp/sami2-logout.php/default-sp	reconstruction.	title and a second second second	

# 4.10. Import & Export

## 4.10.1. Overview

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

# 4.10.2. Exporting

To export configuration items:

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

IMPORT & EXPORT	Export Import		
Configuration Items	~	Export	
Arbitrator Nodes 4	-		
Asset Entries 2030			
Asset Groups 25			
Eustomers 5			
F Controls 36		_	
Permission Groups			
Policy Modules 116			
Probe Groups 80			
Protected Subnets 20			
P Realms 2		\	
Response Procedures 37			
Users 11		Package Name	Must be between 1 and 32 characters long
		Package Description	 Must be between 1 and 172 characters long
		Export	

# 4.10.3. Importing

To import configuration items:

- 1. Click the Import tab at the top of the screen.
- 2. Select the file you wish to import by clicking the "choose file" button. This will open up your local file system to select the file from where you have it stored on your computer.
- 3. Double click the file or highlight it and click "Open".
- 4. Click the Upload button. This will open up all of the configuration items you are importing.
- 5. Make any changes to the settings as required.
- 6. Click Import.
- 7. A progress screen will pop up. Once complete click OK.

IMPORT & EXPORT	Export Import			
	Load a configuration package:	Choose File No file chosen	C Upload	
				No file chosen
			Ø Import	

# 4.11. Archive Management

# 4.11.1. Overview

#### admin-users-only

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

You can select the following tabs on this page:

- Configuration Management Tab
- Log Management Tab

Note: Archive Management is only accessible to admin users.

/oss 🤮 🔥 🔅	4 W 🗐 🥄 🧕 🔒 📥 🧰 🌣	Days remaining: 132
RCHIVE MANAGEMENT Configuration	Management Log Management	
API Config Archive Cisco SDL Col	ct Data-User Import LDAP License Probe Proxy SNMP Syslog	Tunnel
	Save Delete	
Creation	Changes have been made to this configuration item	
DEM Config		
MS Teams Config-42e49b74-b877-4b29- b2d9-e521b8067c57	Creation Allows the creation of periodic monitoring of remote APIs.	
MS Teams Config	remoteAddress	
Webex Config		
Zoom Config	Specify the URL hosting the JSON formatted data. The data retrieved will be	
	used to populate a local table.	
	headerLine	
	[Optional] Specify a headerLine to be used with the API requests. This field	
	may be required by the API's author(s) for security or identification reasons.	
	Ex: x-lxt-api-token:1234abc	

# 4.11.2. Configuration Management Tab

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

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

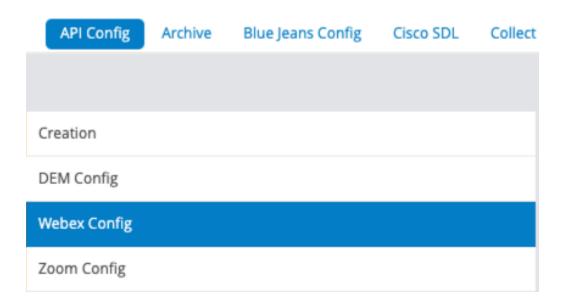
- Import Tab
- LDAP Tab
- License Tab
- Probe Tab
- Proxy Tab
- SNMP Tab
- Syslog Tab

#### **API Config Tab**

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

#### Webex Config

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



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

Copyright o 2024 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

To configure Webex API:

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

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

- e. Click Verify Access Token and to verify, inspect the output in View Output.
- f. Click Save Access Token, which will create a new Customer-specific "Webex Config <XYZ>" entry. under the API Config list. (You need to click away and return to Configuration Management to reload with the new entry.)

voss 💭	A 🛞 .	l 189		٩	<u>1</u>	A 1	2	Days remaining: Unlimi
ARCHIVE MANAGEME	NT Configuration	Management	Log Ma	nagement				
API Config Archive	Blue Jeans Config	Cisco SDL	Collect	Import	LDAP	Probe	SNMP	Syslog
Creation DEM Config Webex Config Zoom Config	Webex ( Allows the Create This step Enable enabl Copture from http://www.com/com/com/com/com/com/com/com/com/com/	e enable and o Access Token Ite Access To b is required to	onfiguration oken allow the c trics using the trice.webex.u	on of Webes reation of a reation of a reation of a reation of a reation of a	k monitorin n access tok ken provided indation:	en.	Comma Status: Output:	Token Finished SUCCESS
	Name o Access1 {*acce	elecom ( Customer.			WZILWIZOG	iEt		

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

#### **MS Teams Config**

MS Teams Config settings configure MS Teams monitoring for Insights.

The MS Teams API configuration requires an initial application registration on Microsoft Azure.

To set up Microsoft Teams integration and monitoring for Insights, see *Microsoft Teams Integration Guide for Insights*.

#### **Zoom Config**

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

Zoom Config

Allows the enable and configuration of Zoom monitoring.

Create Access Token

Create Access Token

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

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

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

#### **Archive Tab**

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

Note: From release 24.2, new configuration options are available for the archive of:

- Cisco SNMP SQL
- Network Observability SQL
- VMWARE SQL

#### 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.

ARCHIVE MANAGEMENT Centigu	ation Management Log Management	
Archive Collect LOAP SNMP	Syslog Tunnel	
Setup	Changes have been made to this configuration item	
Arbitrator Backup		
Cisco Files	Setup	
Cisco SQL	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	
Pexip Files	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	
Remote Storage	by senance 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 mourt a NPS drive to the system. All archived files will then get archived to the NPS mounted drive. Note: removing the NPS mount will NOT copy the NPS contents back to local storage. Only NPS v3 mounts are currently supported today. Storage Type	
	standard :	
	Optional, 'standard' means the system will use its diffault archive location for all backups. 'sfs' means the system will use the rifs roound specified to store all archives	
	Remote Location	
	Required any 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

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

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

CHIVE MANAGEMENT	nfiguration Management Log Management	
Archive Collect LDAP SN	MP Syslog Tunnel	
	Save	
Setup	Changes have been made to this configuration item	
Arbitrator Backup		
Cisco Files	Arbitrator Backup	
Cisco SQL	Arbitrator configuration and data backup. This page contains the settings for the backup of the Arbitrator. There is nothing to edit here. The settings	
Pexip Files	are simply displayed for informational purposes only. This Archive group contains the following data: Arbitrator Configuration settings (Database:	
Remote Storage	Assets, Alerts, Policies, Rules, Probe Groups, Response Procedures, Controls), User Permissions settings (Idap), NDX files, Awaya data, Pesip 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/tit_archive	
	monthsKept	
	netSupported	

# **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.

Archive Collect LDAP SN	MP Syslog Tunnel	
	Save	
Setup	Changes have been made to this configuration item	
Arbitrator Backup		
Clsco Files	Cisco Files	
Cisco SQL	Archival for Cisco files. This Archive group will backup all Cisco CDR and Cisco	
Pexip Files	CMR raw files. These are the files that are shipld to the system by the Cisco Call Manager. The settings here are for informational purposes only. However, the	
Remote Storage	user may disable the storage of raw Cisco COR and Cisco CMR raw files on the system. This option could be used to conserve disk space.	
Nemore storage	status	
	enabled 4	
	'enabled' - keep original cisco catricmr files, trisabled' - remove original cisco	
	calritomr files. The bisobled' option will cause all calritomr files to be deleted	
	from the system. This is a permanent deletion.	
	archive_interval	
	daily	
	method	
	local	
	destination	
	/chroot/scp/pub/td_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.

CHIVE MANAGEMENT cont	guration Management Log Management					
Arabive Collect LDAP SNM	P Syslag Tunnel					
	Save					
Secup	Changes have been made to this configuration item					
Arbitrator Backup						
Cisco Riles	Cisco SQL					
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					
Pexip Files	system. There is nothing to edit here. The settings here are for information					
Remote Storage	purposes only. The data here is grouped together by the Cisco Call Manager (p Address. This allows for more granular control on which Call Manager data to import.					
	archive_interval					
	daily					
	method					
	local					
	destination					
	Actroat/scp/pub/st_antiwe					
	monthsKept					
	infortane pt					

#### Ndx

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

nax_ndx	le size
1	10_010.0
'he maxim	m size the ndx searchable file should be. Once the max size is hit, the ndx server will create a new ndx file.
nax_sear	hable_days
1	
	im number of days that should be searchable. Ndx files greater than this time will still live on the system but will not from the UI.
nonthsKe	st
6	
'he maxim	im number of months to keep ndx archives around. Each archived ndx will take up disk space. Warning, increasing ti
	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.

Archive Collect LDAP SN	IMP Syslog Tunnel	
	Save	
Setup	Changes have been made to this configuration item	
Arbitrator Backup		
Cisco Files	Pexip Files	
Cisco SQL	Archival for Pexip files. The system can be used to collect Pexip data. The	
Peolp Files	raw pexip data files are kept, by default, for historical purposes. However, in order to conserve disk space, the user may choose to disable the local storage of the raw pexip files.	
Remote Storage	status	
	enabled \$	
	'enabled' - keep original pexip files, Wisobled' - remove original pexip files.	
	This trisabled' 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**

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

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

Avaya SQL	Remote Storage
Cisco Files	This page does not describe an Archive Group, if standard / local storage is chosen in the Archive Setup page, then this soreen allows the user to configure remote archival of the system's backup lifes. Each Archive group produces one or many archive files. The system can be configured to spo these archive lifes to a backup location or to another system.
Cisco SQL	archine_interval
Cisco Expressway SQL	daily
Cisco RIS SQL	
Cisco RTMT SQL	Select an option drashed
MSTeams SQLi (legacy data)	nfs
Ndx	C rayno
Oracle Filea	
Oracle SQL	Sup sta
Pexip Files	Waabled - keep archives locally, hts'- Will mount a network file system as a local drive, which preserves local device disk space, 'sop' - System will copy archives to a remote
Pexip SOL	location. Scp is not a sync. In order to reduce load on system and network, system only copies new / changing archives over to the acp location, 'shp' - System will copy archives
Polycom SQL	a remote location. Ship is not a sync. In order to reduce load on system and nervork, system only copies new / changing archives over to the ship location, 'sync'. System will sy
UHESOL	archive directory to remote system. The remote system must have rayno installed for this to work, 'raynoToArb'- System will sync archives directory to a remote system. This util
Vef Cisco	the rayno protocol so both systems will eliways be in sync
Vdf Geip	IP location
Webex SOL	172.00.42.175
Remote Storage	usemame
	stpuser
	password
	options
	destination
	/beckups

#### archive\_interval

This can be set on a schedule of:

- i. Daily
- ii. Weekly
- iii. Monthly
- · Method: Select an option
  - disable System will reset storage options, e.g. archives locations are reset to the local system if these were previously on a remote host.
  - nfs System will mount the filesystem as a local drive. The system drop/lxt\_archive directory is linked with a symbolic link to /mnt/nfsshare on a host, thereby saving space on the system.

Selecting this option enables additional controls:

Check NFS Host	
Check NFS Host	
Check NFS Mount	
Check NFS Mount	1

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

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

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

See also: Backup and Restore Arbitrator.

### **Collect Tab**

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

# Control

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

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

DEM	Enables/disables Digital Experience Monitoring (DEM) collection on the Arbitrator. DEM provides the ability to test connectivity to web-based systems, such as Microsoft Teams, and to deliver metrics for the following: • Overall round-trip times to the application • The number of hops taken • Best and worst latency • The connection path, displayed hop-by-hop DEM agents on the Arbitrator provide connectivity and performance statistics to various MS Teams in- ternet endpoints, including Microsoft Graph. When enabled, the job runs every 5 minutes, and poli- cies (rules) imported to Arbitrator fire incident alerts when any of the DEM-collected metrics are out of the permitted thresholds. To verify that the Arbitra- tor policies are firing alerts and to view the logs, you can search in Arbitrator for either "dem_connectivity"
	or "dem_web_performance".
Cisco UCM	
Oracle SBC	
Pexip	
NGIN	Enables/disables NGIN-XML processing
Palladion	
NMR	
Infovista GSIP	
Infovista IPSLA	

HIVE MANAGEMENT Configuratio	n Management Log Management
API Config Archive Cisco SDL Coll	ect Data User Import LDAP License Probe Proxy SNMP Syslog
	Save Delete
Control	Changes have been made to this configuration item
Avaya Datastore	
Cisco	Control
Cisco Remote Copy	This screen allows the file processing mechanism to be suspended. The system will still receive files, but the file contents will not be processed until re-enabled.
Oracle Microsoft Operator Connect	DEM
Vdf	disabled 🗸
Voss Analytics	Enable/Disable Digital Experience Monitoring processing.
	Cisco UCM
	enabled V
	Enable/Disable Cisco Unified Call Manager processing.
	Cisco ME
	enabled V
	Enable/Disable Cisco ME processing.
	Oracle SBC
	enabled 🗸
	Enable/Disable Oracle Session Border Controller processing.
	Pexip
	enabled 🗸

# **Cisco Remote Copy**

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

The default location is "local", which is the local Arbitrator Correlation platform. Choose "remote arbitrator" and the processed Cisco CDR/CMR files will be stored to the database of a remote arbitrator. This is useful if the data of multiple arbitrators needs to be stored to a centralized arbitrator. The "remote\_ip" needs to be filled in with the IP address of the "remote arbitrator", if configured.

V	oss 🎇				4	îţi		٩	£	A	2	
AR	CHIVE MAN	AGEME	NT	Configurat	ion Manaç	gement	Log Mana	igement				
	API Config	Archive	Blue Je	eans Config	Cisc	o SDL	Collect	Import	LDAP	Probe	SN	IMP
										Save	Dele	te
	Avaya Datastore				Changes I	have beer	n made to th	his configu	uration iter	n		
	Cisco											
	Cisco Remote Co	ру		0	lisco Re	mote Co	ору					
	Oracle Microsoft	Operator Co	nnect	L			e CDR/CMR	forwardin	ig to a rem	tote system	n.	
	Vdf				10.13.3							
	Voss Analytics				Specify t	he IP add	ress of the I	remote loc	ation.			
					drop	e						
					Specify t	he userna	ame to be u	sed to acce	ess the rer	note locati	lon.	
					passwor							
							ord to be us	sed to acce	ess the ren	note locati	ion.	
					destinati							
						/scp/pub	n the remot	e system				
					Speeny I	ne patri 0	in the remot	e ayateni.				
					Verify Co	onfig						

# **Oracle Microsoft Operator Connect**

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

vos	s 👬		A	۲	1	łł		٩	Ł	<b>A</b>	* 6	<b>a</b>	
ARCH	IVE MAN	AGEME	NT	Configuratio	n Managem	ent	Log Mana	gement					
	API Config	Archive	Blue J	eans Config	Cisco Si	DL	Collect	Import	LDAP	Probe	SNMP	Syslog	Tun
A	vaya Datastore						Change	es have be	en made te	o this confi	guration iter	n	
С	isco												
c	isco Remote Co	ору							-	tor Conne			
0	racle Microsoft	Operator Co	nnect				Client	-	ire SBC for	rwarding to	Microsoft 0	perator Cor	inect.
V	df						Cilent	ib.					
V	oss Analytics						Specif	fy the clien	t_id to be a	used to accu	ess the rem	ote location.	
							Client	Secret					
							Specil	ly the clien	t_secret to	be used to	access the	remote loca	tion.
							Tenar	ıt					
							Specil	ly the tena	nt to be us	ed to acces	s the remot	e location.	
							Resou	irce					

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

# **Ping Probe**

This page configures ping probes to define the location to store the collection of ping probe results. By default, the storage location is "local", and all ping probe results are processed and stored on a local arbitrator.

You can configure the ping probe to store results remotely. This is useful if the data of multiple arbitrators should be stored in a central location.

- 1. At method, select remote arbitrator.
- 2. Fill out the remote IP address of the arbitrator.
- 3. Save your changes.

**Note:** Even if configuring the results of the ping probe to be stored to a remote arbitrator, results are stored both to the remote location as well as to the local storage location (the default).

API Config Archive Cisco SDL Collect Data	ent Log Management	e Probe Proxy SNMP Syslog
		Save
Control		Changes have been made to this configuration item
Avaya Datastore		
Cisco		Ping Probe
Cisco Remote Copy		Ping probes are configured through the Arbitrator configuration screens. This screen is solely to configure where the collection of the pring probe results should stored. "local" is the default location. By default, all ping probe results will be processed and stored on local arbitrator. Choose "remote arbitrator" and the proce-
Oracle Microsoft Operator Connect		data 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 place. The "remote, needs to be filled in with the remote ip address of the arbitrator.
Ping Probe		method
Vdf		remote arbitrator
Voss Automate		
		remote_ip

## **Import Tab**

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

Note: Only csv file imports are supported	Note: O	ly csv fil	e imports	are sup	ported
---	---------	------------	-----------	---------	--------

### LDAP Tab

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

1010										-			
API Config	Archive	Cisco SDL	Collect	Data User	Import	LDAP	License	Probe	Proxy	SNMP	Syslog	Tunnel	
													Save
External Config						Cha	anges have be	en made to	this config	guration iter	m		
						Exte	ernal Config	1					
													uthenticating with an external M
													ync all users locally. Local user a are never stored locally. Authent
													access based on the user's loca
												oo little or too many users ir	e an in depth knowledge of the c n the system.
						Те	st LDAP conf	guration					
							Test LDAP	configura	tion				
						Us	e this button t	o test the c	onfiguratio	n that is fill	ed in the for	m below.	
							ternal_type						
							local						
										ver, 'windov	vs' - use exte	ernal Microsoft Active Directo	ory server. This will require additi
						fo	rm informatio	n to be filled	1.				
							<b>.ssl</b> true						
								r 'windows'	setting, Se	t to 'true' if	Microsoft A	ctive Directory requires ssl fo	or connection.

# License Tab

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

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

API Config	Archive	Cisco SDL	Collect	Data Use	r Import	LDAP	License	Probe	Ртоку	SNMP	Syslog	Tunnel
												Save
License					Channes ha	ve been mar	de to this con	fouration	tem			
					Consequences on	THE EXCENTION	00 10 0111 000					
					License							
					This screen r	nanages lice	ensing with V	OSS. This	icreen may	be used to	enable the	periodic li
					delivery to Vi solutions.com							
					enabled							
					false							
					Opt-in/Enal	ble the autor	matic sharing	of the licer	se file.			
					organization ads/	on id						
						organization	id associate	f with this o	feuice.			
					environme	nt type						
					production	on						
					The VOSS (	account id (d	organisation i	d) associat	ed with this	device.		
					description	•						
					A descrip	tion						
					A descripti	on of this de	vice.					
			-		Fetch Lice	na File						

# **Related Topics**

• License Auditing

# **Proxy Tab**

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

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

voss 🎇 🧴	S 🛞 🦼	វដុះ 📰	۰. ا	<u> </u>		<b>•</b>	ŧ	
ARCHIVE MANAGEMENT	Configuration Manage	ement Log Ma	nagement					
API Config Archive Blue	Jeans Config Cisco	o SDL Collect	Import	LDAP	Probe Pro	xy SNMP	Syslog	Tunnel
							Save	Delete
Proxy Config		Changes hav	ve been made	to this conf	iguration item			
		Proxy Conf		v use in ext	ernal data creat	tion.		
		ipAddress		*				
		10.0.0.1	6.4					
		IP Address	of the proxy se	rver.				
		proxyPort						
		19001	proxy server.					
		r on or une p	broxy server.					
		userName						
		UserX User for the	proxy accoun	t for externa	al access.			
		password						
		Password fo	or the proxy us	er account	for external acc	ess.		
		Set Proxy Set Pro	xv					
		<u></u>		ings above.	(Values must b	e saved first.)		
		Remove Pro	-					
				ioving any p	preiously configu	ired proxy.		

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

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

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

#### **SNMP** Tab

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

ARCHIVE MANAGEMENT	Configuration Management Log Management	
Archive Collect LDAP	SNMP Syslog Tunnel	
	Save	
SNMPv3 User Config	Changes have been made to this configuration item	
	SNMPv3 User Config	
	Setup the configuration for SNMP.	
	Commit SNMPv3 User Configuration	
	Commit SNMPv3 User Configuration	
	Engine ID	
	OCTECT STRING	
	User Name	
	OCTECT STRING	
	Authentication Protocol	
	MDS \$	
	Authentication Pass Phrase	
	Encryption Protocol	
	AES	
	Encryption Pass Phrase	

# Syslog Tab

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

**Note:** This is a system-wide setting.

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

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

ARCHIVE MANAGEMENT Contgurates Man	general Log Masagement	
Archive Collect LDAP SNMP System	Turnel	
	See	
Systag Server	Changes have been made to this torfiguration time	
	Syslag Server	
	Use this screen to configure the ip address of your central splag server. This is a system welle setting, if an ip address is specified the system will send any internal Layer X messages acto- the specified systeg server. Only one central splag server can be specified at this time. These validate freewall settings are open to allow incoming messages on the specified by address and port.	
	external_system_lp	
	Optional. Ever in the ip address of your organizations central typing sover: A single ip Address or a single Danain name. Note, Donain name entries must resolve through the system	
	configured DMS (saar specified in system DMS antings)	
	protocol	
	top 8	
	Systeg protocol to use in systeg transport, Systeg server must also sort the same protocol:	
	estensal systag, port	
	614	
	Optional. Enser in the part, Default systag port is \$14	

# 4.11.3. Log Management Tab

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

# Set the archival process

This procedure sets up the archival process.

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

Archive Methods	
IP Address	Method
0.0.0.0	SCP
	SCP SFTP SMP

mors exist				
hive Settings				
		Current Intervals		Archive Index Every
		4 GB		4 ‡ GB
		10 Days		10 ‡ Days
		Last Archive Time Aug 19, 2018 13:50		Alerting Options
<ul> <li>Used Space (570 GB)</li> </ul>	Free Space (375 GB)	Aug 15, 2010 15.50	-	Alert on archive success
				Alert on archive failure
chive Methods				
IP Address	Method	Path	Credentials	
0.0.0.0	SCP	+	None	: 2

# 4.12. Tools

# 4.12.1. Overview

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

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

# 4.12.2. Load a MIB

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

1			۲	1	161	٩	4	£	*	-	٠				👤 admi	
TOOLS	MIB Browser															
Load MIB	Import MIBs	SNMP	Connectio	« nc	Host				O Con	nection						
					OID								Operation	n	_	
		1			1.3.6							~	Get	0	Run	
			Sele	t a	MIB					×						
			Search													
			•	nortel procera												
			-													
				estings: ubs	nmp											
				ucd												
				mware												
					DGE-MIB											
				ENT												
				_	ST-RESOUR	e										
					A-ADDRES		S-MIB									
	-			-	A.PTPROT		e nie									
Name			Re-pa	arse				Can	cel Se	elect						
OID		-		-		 										
Syntax.																
Access																
Status																
Description																

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

5. Select the Connection button, input the host name or IP and choose the SNMP version. If selecting V3 then a set of different parameters will pop up and you will need to fill these in.

	MP Connection » Host 10.13.37.80	© Connection		
a 📻 iso	OID		Operation	
a 🍙 org	1.3.6.1.4.1.6876.1		✓ Get ‡	Run
a 🎦 dod a 🚞 internet	SNMP Options			
<ul> <li>directory</li> <li>mgmt</li> <li>experimental</li> <li>private</li> <li>enterprises</li> </ul>	Version 2c ‡			
	Community			
<ul> <li>enterprise</li> <li>image: second second</li></ul>				
<b></b>		Cancel Ok		
	nwVirtMachines nwResources	SNMP Options		
	nwProductSpecific	Version		
	nwLdap	8 8		
	mwTraps	Usersame		
🖉 vr	nwSRM mwVCHA	Context Name		
🖉 vr	mwSRM mwVCHA			
		Context Name Security Level extPrix 8		
ame vrrwSystem		Security Level outPrix 8 Auth Protocol		
9 v 9 v		Security Level authPhy 8		
ame vrrwSystem ID 1.3.6.1.4.1.6876.1		Security Level extRPN 8 Auth Protocol SNA 2 Auth Prosphrase		
ame vmwSystem ID 1.3.6.1.4.1.6876.1 yntax		Security Level extPrive 8 Auth Protocol SIVA 5		
ame vmwSystem		Security Level outPriv 8 Auth Protocol DolA 2 Auth Possphrase Privacy Protocol		

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

OID				Operation	_			
	3.6.1.4.1.6876.1 ults	~	✓ Get Get Next Walk		Run			
q	Text OID Toggle Numeric/Text OID Cr	eate Probe						
	Text OID	Value		Туре				
0	VMWARE-SYSTEM-MIB::vmwProdName.0	VMware ESXi		STRING	ING			
7	VMWARE-SYSTEM-MIB::vmwProdVersion.0	6.0.0	STRING					
D	VMWARE-SYSTEM-MIB::vmwProdBuild.0	2494585		STRING	3			
h	VMWARE-SYSTEM-MIB::vmwProdUpdate.0	0		STRING				
0	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 sah probe	
Create a new probe group	
Probe Group Name:	
	Cancel Create

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

# 4.13. Agent Configuration

# 4.13.1. Overview

Insights Arbitrator agents are Linux service testing bots that enable synthetic connectivity and performance testing of a range of UC and business applications for greater visibility of the user experience in your environment.

The agents test connectivity to UC resources, such as Teams and Zoom, and perform synthetic testing to validate that the infrastructure can reach the application resource or a specified URL. For example, you may want to monitor the route and connectivity across a WAN link for mission-critical applications to verify jitter and per hop latency. Alerts can be set up to notify you immediately when your systems experience connectivity or performance issues. This is especially important for systems where it's important that they're up and running at all times.

Each agent makes regular (5 minute interval) API calls to the Arbitrator for updates.

You can view and configure registered Insights agents and agent profiles via the **Agent Configuration** tab in Arbitrator's **System Configuration** interface.



# 4.13.2. Install Insights Agent

This procedure installs and registers an Insights agent with the Arbitrator.

# System Requirements

- Minimal Linux installation on your network that can install .deb files on any of: VM, (mini)computer, Raspberry PI
- Linux should have installed: jq, curl, sysstat, mtr-tiny, util-linux
- · Minimal space required: .deb file size less than 17KB
- 1. Download the installation package via the Arbitrator GUI or directly via the Arbitrator IP address:

https://[Arbitrator IP Address]/insights-agent/insights-agent-[release version]-all.
deb

**Note:** You can verify the file against the sha value, also available at the download location: insights-agent-[release version]-all.deb.sha256

tname System I	P Prof

- 2. Install the software: \$ sudo apt-get install ./insights-agent-24.2-all.deb
- 3. Enter the IP address or FQDN of the Arbitrator where you're deploying the agent.
- 4. Fill out credentials, user and password, and wait for authentication.

**Note:** Typically, these are the VOSS Agent API credentials - user can be the default, voss\_agent\_api\_user. You can also use the admin, or your own user. Once the credentials are set up for the agent, they're not exposed again. The credentials are centrally managed on Arbitrator's *Credential Configuration* page, so that you can share them between the profiles. Users and their passwords can be added and configured in Arbitrator's *Access Control* page.

- 5. Fill out the customer name.
- 6. Fill out a name for the agent.
- 7. The agent registers with the Arbitrator. A UUID is required to be able to register so that the Arbitrator can identify the agent in its interactions.

Confirm that the agent status is "registered".

- 8. At the prompt, restart services.
- 9. Verify that the agent has been added:
  - · Log in to Arbitrator.
  - · Click the toolbar Wrench icon to open the System Configuration GUI.
  - Click the Agents icon to open the Agent Configuration page.
  - Select the Agents tab to view the agent you added.

**Note:** If you need to upgrade the agent for a new version of Arbitrator, you can re-run the Agent installation package.

# 4.13.3. View and Configure Agents and Profiles

# Agents

The **Agent Configuration** page provides a centralized management interface for agents and their profiles, where you can:

• Add or delete agents and their profiles

Note: It is expected that an organization will have just one agent per site (location).

· Add tests for the agent to run and specify test attributes (destination, ports, protocol)

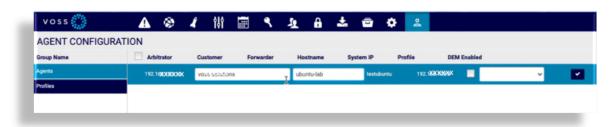
**Note:** Credentials for connecting to a destination can be configured via Arbitrator's *Credential Configuration* page.

- · Manage the tests the agent runs, for example, to remove or disable existing tests
- Manage the agent code, for example, to view agents and their description or purpose, their versions, and their enabled tests, and to update one or more agents
- Enable or disable agents

**Note:** When disabling an agent on the Arbitrator, the agent still runs all its jobs (5 minute intervals), but it won't run its tests or report to the Arbitrator until it's enabled again.

• Select a profile for the agent, and update the agent or its profile - for example, you can change the customer name or the hostname, and enable or disable collection

Note: The system IP is a read-only value as it's assigned by the system.



### Assign a profile to an agent

- 1. On the **Agents** group, click the green Pencil icon to edit the agent.
- 2. In the **Profile** drop-down for the relevant agent, choose a profile.
- 3. Save your changes.

# Profiles

You can add one or more profiles. An agent can only have one profile assigned to it. One profile may be assigned to one or more agents.

# Add a custom profile

Insights ships with a default profile, which is assigned to an agent on install. The default can be cloned and customized in Arbitrator.

To clone a profile:

- 1. On the **Profiles** group, select the checkbox at the profile name.
- 2. Click the taskbar Clone Profile button (C)
- 3. Give the profile a new name and description.
- 4. Add or remove tasks for the connectivity tests and/or the performance tests. You can also clone existing tasks then customize the clone for your requirements for example, change the task name, specify a destination and port. Save your changes.

# **Configure profile**

Click the green Edit icon (Pencil) to edit a profile.

A	<b>\$</b>	4	îţî		٩	<u>.</u>	A	*	5	۰	2	
TION												
Pro	file Name			Des	cription					Tests		<b>b</b>
Def	ault Profile			Prof	ile for con	nectivity an	d perform	ance testin	g	9	1	
			TION Profile Name	TION Profile Name	TION Profile Name Des	TION Profile Name Description	TION Profile Name Description	TION Profile Name Description	TION Description	TION Profile Name Description	ATION Description Tests	TION Profile Name Description Tests

You can edit the various connectivity and performance tests for the profile. Once the profile is updated, the next time the agent checks for changes, the new settings are retrieved from the Arbitrator and the agent runs the profile with these settings against the Arbitrator.

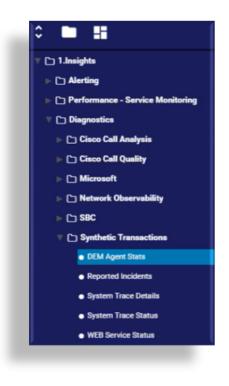
Group Name	Profile Name	Description		Tests				
Agents	Default Profile	Profile for connectivity	and performance	testing 9				
Profiles	Connectivity Tests			_				
	Task Name	Destination	Interation Co	unt Protocol	Port	ToS Max	TTL Packet Size	
	Trace graph.microsoft.com/	. graph.microsoft.com	3	3	0	0	30 64	
	Trace teams microsoft.com/.	teams.microsoft.com	3	3				
	Trace graph.microsoft.com/	. graph.microsoft.com	3	3 tcp	443			
	Trace teams.microsoft.com	teams.microsoft.com	3	3 top	443			
	Performance Tests							
	Task Name	Destination		k Authentication Type	Username	Password	Certificate	
	Test Service graph.microsoft.	https://graph.microsoft.com/v1.0/tea	ims	none				
	Test Service teams.microsof.	https://teams.microsoft.com						
	Test Service login.microsoft	https://login.microsoftonline.com		basicauth	someuser	somepass	-BEGIN CERTI	
	Test Service outlook office.c.	https://outlook.office.com		none				
	Test Service outlook office3	https://outlook.office365.com		none				

# View Agent Data on the Dashboards

You can view the results of agent tests on the collection of Synthetic Transactions dashboards.

When adding the agent, the system provides a unique ID (UID) to the agent, which remains associated to the agent if you uninstall and reinstall the agent. The UID comes from the Linux system, which has a unique ID. You can identify the agent data on the dashboard from the UID.

- 1. Log in to Insights Dashboard.
- 2. In the Dashboard folders, navigate to **Diagnostics > Synthetic Transactions**.



Note: See Synthetic Transactions Dashboards in the Dashboard Admin Guide.

3. Select a dashboard to view and inspect agent data.

# **Related Topics**

· Insights Reference Dashboards - Synthetic Transactions Dashboards in the Dashboard Admin Guide

# 5. Arbitrator Maintenance

# 5.1. Backup and Restore Arbitrator

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

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



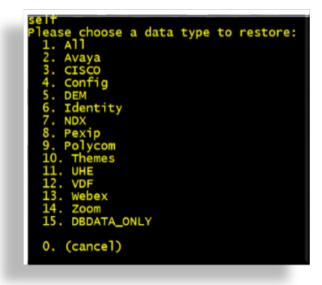
3. Select Restore a backup.



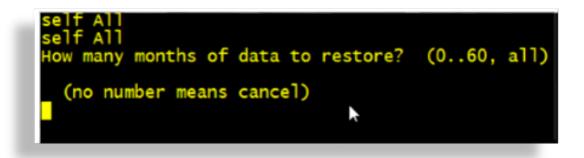
- 4. Optionally, run the Fetch command to retrieve backup files.
- 5. Select the local backup you wish to restore. Choose an option:
  - To restore data from the nightly backups, select self.
  - To restore from another source, including a remote backup of this device, select the relevant source.

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

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



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



8. Confirm the restore.



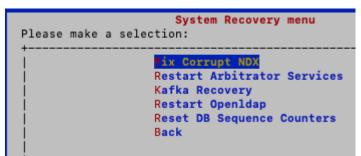
9. Monitor restore progress. A system message confirms when the restore is complete.

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

# 5.2. System Recovery

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

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



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

May be used to repair the NDX. The NDX is the backbone of the "Search" screen in the user interface. If the "Search" screen displays zero results, the NDX may be corrupt. This option terminates the current NDX files and start a new NDX set of files.

Restart Arbitrator services

Allows you to restart the Arbitrator's core services involved in collection, correlation, and alerting. This option is useful when attempting to debug a scenario where alerts are not firing.

Kafka Recovery

Arbitrator uses Kafka for communication between different processes. This menu option stops and starts the Kafka process and restarts Arbitrator services. Use this option when Kafka is slow and impacting Arbitrator system performance.



Restart OpenLDAP

Used specifically for restarting the OpenLDAP service. This option is useful when attempting to debug authentication issues in the user interface.

Reset DB Sequence Counters

This option provides an optional (last resort) method for resolving a rare scenario when alerts stop firing. If you've exhausted the normal troubleshooting checks for alerting, this option may be used as a final resort. This method has been shown to fix rare issues in the past, and is provided an an option until the issue may be auto-detected and automatically repaired.

# 5.3. Network Observability

# 5.3.1. Overview

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

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

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

# **Related Topics**

- Probe Configuration
- Asset Configuration
- Insights Reference Dashboards in the Dashboard Administration Guide

# 5.3.2. Configure Network Observability Probe Groups

This procedure configures network observability probe groups in Arbitrator.

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

**Important:** We have provided a recommended configuration of the following four probe groups, including a recommended naming convention and probe configuration parameters, in *Network Observability*:

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

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

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

**Note:** It is recommended that you use the probe configuration parameters provided in the table, in *Network Observability*.

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

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

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

Groups		Pro	bes				
Group Name			Name	Description	Unit		Command and Parameters
CUCM RIS	1		network_obs cbqoscm			~	Custom
Local System Stats	5				Auto-scale?		Select Category
Network Obs 10min	1	1					Network Observability 🗸
Network Obs 5min	2	1					Select Script
Network Obs SNMP 10min	1						netob-alarm-probe-cbqoscm-stats.sh 🗸
Network Obs SNMP 5min	1						IP address list (default = all)
Ping Probe	1						IP address exclude list (default = none)
Voss Automate Data	1	1					
							Interval in seconds (default = 900)

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

### Next steps:

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

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

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

Repeat this step to add other probe groups, and to configure their frequency.

- Click Update.

# 5.3.3. Recommended Network Observability Probe Group Configuration

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

The table describes the recommended network observability probe group configuration:

Probe Group	Configuration
1. Network Observabil- ity 5 min	<ul> <li>There are two probes to set up for this probe group: <ol> <li>Network Observability Asset Impact</li> <li>This probe detects the impact of network observability alarms on locations.</li> <li>Scripts to use with this probe: <ul> <li>netob-asset-impact-assessment.sh</li> <li>Category: Network Observability</li> <li>Parameters: N/A</li> <li>Applied to: Arbitrator</li> <li>Frequency: 5 minutes</li> <li>Credentials: N/A</li> </ul> </li> <li>Network Observability Interface Event Detections <ul> <li>This probe detects the interface counter changes for discards and errors.</li> <li>Script to use with this probe: <ul> <li>netob-alarm-probe-interface-stats.sh</li> </ul> </li> <li>Category: Network Observability</li> <li>Parameters: Use defaults, unless customization is required.</li> <li>Applied to: Arbitrator</li> <li>Frequency: 5 minutes</li> </ul> </li> </ol></li></ul>
2. Network Observabil- ity 10 min	<ul> <li>This probe group contains one probe. The probe detects the cbqoscm counter changes.</li> <li>Probe name: Network Observability CB QoS Event Detections</li> <li>Script to use with this probe: <ul> <li>netob-alarm-probe-cbqoscm-stats.sh</li> </ul> </li> <li>Category: Network Observability</li> <li>Parameters: Use defaults, unless customization is required.</li> <li>Applied to: Arbitrator</li> <li>Frequency: 10 minutes</li> <li>Credentials: N/A</li> </ul>
3. Network Observabil- ity SNMP 10 min	<ul> <li>This probe group contains one probe. The probe is used for netob-cisco-cbq-mib-stats-snmpv3 collection for group01.</li> <li>Probe name: Network Observability CBQ</li> <li>Script to use with this probe - either of the following: <ul> <li>netob-cisco-cbq-mib-stats-snmpv3.sh</li> <li>netob-cisco-cbq-mib-stats-snmpv2c.sh</li> </ul> </li> <li>Category: Network Observability</li> <li>Parameters: Supply appropriate credentials, where applicable.</li> <li>Applied to: Asset</li> <li>Frequency: 10 minutes</li> <li>Credentials: SNMP</li> </ul>

Probe Group	Configuration
4. Network Observabil-	<ul> <li>This probe group contains one probe. The probe is used for netob-ifmib-</li></ul>
ity SNMP 5 min	interface-stats-snmpv3 collection for group01. <li>Probe name: Network Observability Interface</li> <li>Script to use with this probe - either of the following: <ul> <li>netob-ifmib-interface-stats-snmpv3.sh</li> <li>netob-ifmib-interface-stats-snmpv2c.sh</li> </ul> </li> <li>Category: Network Observability</li> <li>Parameters: Supply appropriate credentials, where applicable.</li> <li>Applied to: Asset</li> <li>Frequency: 5 minutes</li> <li>Credentials: SNMP</li>