

# VOSS Insights Arbitrator Administration Guide

Release 22.2

Oct 18, 2022

## Legal Information

- Copyright © 2022 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: 20221018103412

# Contents

1	What's New           1.1         Arbitrator Administration Guide: Release 22.2	<b>1</b> 1
2	Getting Started         2.1       Introduction         2.2       Arbitrator Licensing	<b>2</b> 2 2
3	Correlate 3.1 Correlate	<b>4</b> 4
4	Configuration         4.1       Configuration	<b>28</b> 28
5	Backup and Restore         5.1       Backup and Restore the Arbitrator	<b>103</b> 103

# 1. What's New

## 1.1. Arbitrator Administration Guide: Release 22.2

• EKB-13343: Cannot run backup to external system. See: *Configuration* Added details on nfs option and new Check NFS buttons.

# 2. Getting Started

## 2.1. Introduction

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

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

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

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

This guide covers the following:

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

## 2.2. Arbitrator Licensing

#### 2.2.1. Overview

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

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



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

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

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

VOSS	🔺 🛞 🦨 iii	📰 🔧 🧏 🔒	📩 🚖 🄅 Days remaining: 17
ACCESS CONTROL	Permission Groups Users Node	s Realms Protected Subnets	Password Policy SAML
Group Name	Realm Context	Timeout	
Administrator	(local)		2
Typical	(local)	<b>V</b>	2
Permissions Users			
	Ana	alytiX :: 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	

### 2.2.3. View License Days Remaining

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

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

## 2.2.4. Load a License File

To load a license file:

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

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

## 3. Correlate

## 3.1. Correlate

#### 3.1.1. Menu Bar

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

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

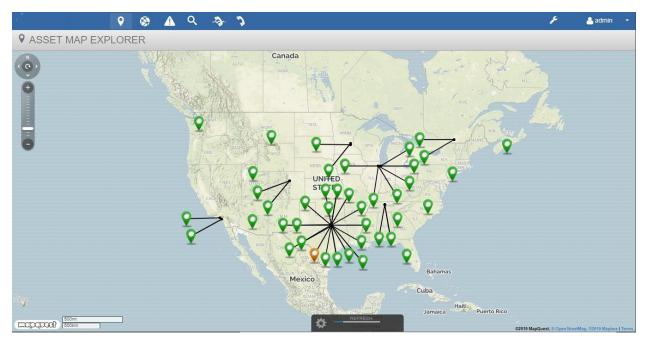
This menu is located at the top of the browser page and allows you to navigate to each of the Arbitrator views. Each are shown below:

	۰	4	îşi		٩	<u>\$</u>	£	*	🖻 🌣	👤 admin 🗸
1.	2.	3.	4.	5.	6.	7.	8.	9.	10.11.	12.

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

## 3.1.2. Assets

#### **Asset Map Explorer**



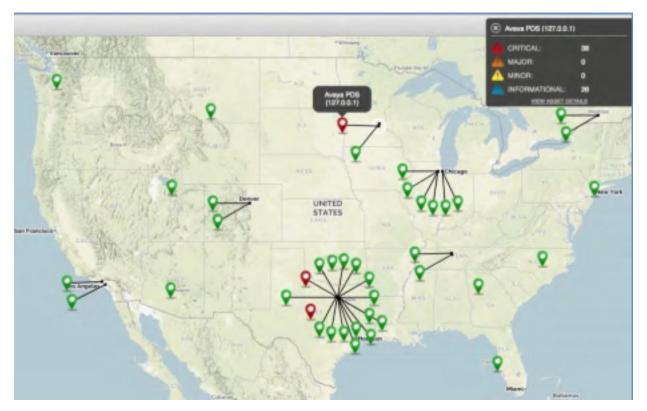
This view displays all of the defined assets in the system on a map for visual grouping according to their physical location. The location or address of the assets are input in the asset configuration section within the Configuration interface. This view is integrated with the MapQuest API (Internet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

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

#### **Asset Overview**

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

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



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

#### **Asset Explorer**

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

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

Alert Severity Levels:

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

ASSET EXPLORER	-								Deplaying 1 - 50 o	11778 <b>4 C</b>	<b>3 39</b> 00 €
STATUS	10.15.37.43	100.254.5.10	255.254.06	Aven FDS				192.105.103.	10.52.45.51	18.52-0.89	12.74.94
		-	10.13.07.0	10.13.37.100	10.13.07.100	10.13.37.140	10.15.57.20	14.10.27.000	16.10.37.200	11.13.37.290	10.15.27.40
ADDETS - 0	1115.17.48	10.15.37 M	10.12.57.80	-	-	1. Aven. 1817.	and the second	E Charles	and me	and the second	CLOMVILL.
P AJ P Arays P LayerX			and an		-	dia.	-	How			un de marte
LES BIP Phones     LES BIP Phones     LES BIP Phones     LES BIP Phones		una me	-	un alter		LALADATTA					
Dala Referre											
Genbard LayerX.Lab											
an Horted											
Ostua SiLo Instituto											
TELETRA TCC.CP											
Tolefonica											
Toiner											
UCHIX											
Vit Tech											
P P VOST CUCTH											

#### **Asset Filtering**



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

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

#### **Asset Explorer Navigation**



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

#### **Asset Details View**

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

- Alerts
- · Probes
- · Search

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

#### Asset Details: Alerts Tab

	T DETAILS	S = 10.13.3	37.43										X CLOSE
	ALIAS MAC	Unknown 10.13.37.43 Unknown Unknown	HOSTNAME 10.13.3 TIMEZONE Unknow VENDOR Unknow MODEL Unknow	In DESCRIPTIO	ON Unknown ON								
							Displaying 1 - 10 of 37	*	< >	*	10		STATUS -
	DATE	NODE	POLICY	RULE	STATUS	OWNER							
	DETALS	FERENCE ID 2 NODE d	JRNAL5 0000-01000005-00-01-36950- keyparb Joco Alerta : Universal	LAS	START 07/08/1						3	NEW RE	PORT
			Aajor Clisco Error	NEXT ES	SCALATION 07/06/11 EXPIRES IN 00:08:4 ROCEDURE Default	8 01-29-16 PM							
	D	OWNER U	Agor Claso Enor Inassigned OPEN •	NEXT ES	SCALATION 07/08/1 EXPIRES IN 00:09:4	8 01-29-16 PM							
A	07/08/18 11:08:21 AM	RULE OWNER U	Agor Claso Enor Inassigned OPEN •	NEXT ES	SCALATION 07/08/1 EXPIRES IN 00:09:4	8 01-29-16 PM							
•	07/08/18	AULE N OWNER U STATUS ESCRIPTION - desparts Crical Casco	Cisco Aints : Universal Cisco Aints : Universal Etter (<12-Jul 8 2018 16:08-21	NEXT ES RESPONSE PI Critical Cisco Error 10.13.37.43: <1853-82258: :	CALATION 07/08/1 EXPIRES IN 00:09/4 ROCEDURE Default DPEN : 34122: CUCM12.lag	II 01:29:16 PM D Unassigned Unassigned	08:21.207 UTC : %UC_/RIMT-I-RTM we of Cisco Tomoat Web Application(ar		%[Abort	NamouR	TMTSe	ssionsExc	(®) (
4	07/08/18 11:08:21 AM	AULE N OWNER U STATUS ESCRIPTION - desparts Crical Casco	Cisco Aints : Universal Cisco Aints : Universal Etter (<12-Jul 8 2018 16:08-21	NEXT ES RESPONSE PI Critical Cisco Error 10.13.37.43: <185-42258 : 018. slert RTMTSessionsExcl	CALATION 07/08/1 EXPIRES IN 00:09/4 ROCEDURE Default DPEN : 34122: CUCM12.lag	II 01:29:16 PM D Unassigned Unassigned			SijAlart	Name-R	TMTSe	ssionsExc	ceeds Threshold
A	07/08/18 11:08:21 AM OUTPUT: 07/08/18	RULE N OWNER U STATUS ESCRIPTION - Genpars Crical Careo I (AerOctain Genpars Major Careo I DeviceName	Cisco Alerta : Universal Cisco Alerta : Universal Etnor (<12x34 8 2018 16:08:21 On Sun Jul 08 11:08:21 CDT 28 Cisco Alerta : Universal Cisco Alerta : Universal	NEXT ES RESPONSE PT Critical Ciaco Enor 19.13.37.42: «185-822551: 018, alert RTMTSessionsExo Major Ciaco Enor 10.13.37.43: «178-820581: 1 88:*172.16.11]Protocolid	COLLATION OTOEN EXPIRES IN ODDA HOCEDUME Default OPEN 194122: CUCM12.lag exelsThreads has or OPEN COPEN COPEN COPEN	Unassigned Unassigned unexceptions: Jul DE 2018. 16 counter: SensioneAct Unassigned Layentents: com Jul 08 2018 Vagententsion-SEP03044005F		t) 1.3-EndPo	sintUnvi	benetropo			ceeds Threshold
4	07/08/18 11:08:21 AM OUTPUTE 07/08/18 09:25:15 AM	RULE N OWNER U STATUS ESCRIPTION - Genpars Crical Careo I (AerOctain Genpars Major Careo I DeviceName	Circo Akrts : Universal Circo Akrts : Universal Energ (-125-34) 8 2018 16:08:21 On Sun Jul 08 11:08:21 COT 2 Circo Akrts : Universal Dror (-125-34) 8 2018 14:25:15 	NEXT ES RESPONSE PI Critical Cisco Error 10.13.37.43: <186-82258 : 18, siert RTMTSessioneExo 1 Major Cisco Error 10.13.37.43: <178-85058 : 188-172.16.1.11[Protocolds discretification]?Node/D-CUC	COLLATION OTOEN EXPIRES IN ODDA HOCEDUME Default OPEN 194122: CUCM12.lag exelsThreads has or OPEN COPEN COPEN COPEN	Unassigned Unassigned unexceptions: Jul DE 2018. 16 counter: SensioneAct Unassigned Layentents: com Jul 08 2018 Vagententsion-SEP03044005F	ve of Cisco Torncat Web Application(ar 14/25-14 UTC : %UC_CALLMANAGE	t) 1.3-EndPo	sintUnvi	benetropo			ceeds Threshold

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

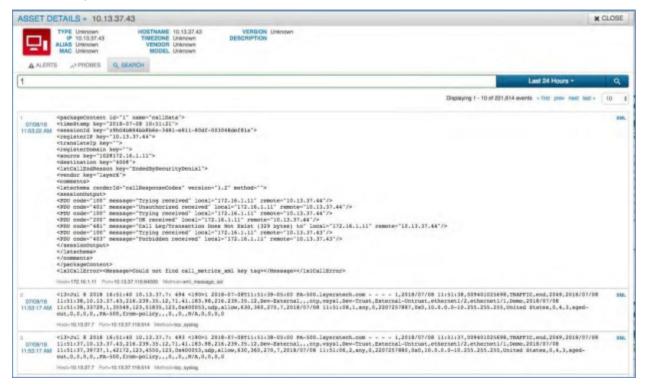
#### **Asset Details: Probes**

P 10.13.37.43 ALLAS Unknown MAC Unknown	HOSTNAME 10.13.37.43 TIMEZONE Unknown VENDOR Unknown MODEL Unknown	VERSION DESCRIPTION		
	Q, SEARCH			
Trunk Activity Call Manager PITMT Request Call Activity Call Manager Service Sisteway Activity CPU and Managry	Status: 200 c/trut/sension/15/25-c/PreCare Energian States/15/25/25/25/25/25/25/25/25/25/25/25/25/25	ndRepiles ReturnCode Ofikaster*1*s-Hoat M Rytes=30668*Cach Yoossor Name+5* Pe geCPU+8*/s-Process geCMdate-14* PercentageSot apather*197*PercentageSot apather*197*PercentageSot	to https://10.13.37.45/ast/4575aap.dt/?GetPreCannedinto&Nerre-getCpu4ndMerroryFloquest. ta-9° collecting/bate="0" AMC_"CLICENTMEREAGE": "SMERCENTS'-cogetCpu4ndMerroryFloquest. Bardio Course: "A second se	5° 52

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

#### Asset Details: Search

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



## 3.1.3. Alerts

#### Alert Analyzer

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

ALERT AN	IALYZER	1017	HER.					Displayer	ng 1 - 10 of 3,702 Alerts	4K K > >> 1	0 \$
AJERS	1	90	RT •	BULK DIS		STATUS .					
			DATE	NODE	POLICY	RULE	STATUS	OWNER			
		•	07/07/18 01:01:17 PM	(, <13×Jul NUC_RINT-1- RINTHESSION Value of 27 2016 17:56: RINT_ALENT: RINTSession	7 2018 17:56:48 10 RTHT_ALENT: %[Alex sExceedSThreshold 6#012 which is over 48 10.13.37.68; <] 8[Alex:Masse-STRT sExceedsThreshold	0.13.37.44: <185>1619 rtSame-#THTSessionabs has occured. Counter ar high threshold 350 (85>161906: = 1 11218 besionsExceedSThresh has occured. Counter	06: : : 112181: cume ceedsThreshold)[Aler SessionsActive of C ][AppED=Claco AMC Se 1: cume11.layerstech 06:[[AlertDeta1]= 0s SessionsActive of C	11.layerstech.com: thetail= On Sat Jul isco Tomcat Web App rvice](ClusterID=)) .com: Jul 07 2018 0 Bat Jul 07 12:56:4 isco Tomcat Web App	Jul 07 2018 05:56: 07 12:156:44 CDT 2: lication(ast) on n NodeD=cumcil): RT 5:156:44 PM.372 DTC 4 CDT 2018, elect lication(ast) on n	010, alert ode 10.13.37.44 has MT Alert', <130Jul 7 1 NUC_RIMT-1-	
			DETAILS	0. 3	URIVALS					VIEW REPORT	i -
				RULE (	Cisco Alerts : Universal Critical Cisco Error		ELAPSED TIME -				
			Di	STATUS	OPEN	* RESPC	EXPIRES IN Expi INSE PROCEDURE DAY				
		A	0101/18 01:01:29 PM	STATUS	OPEN	RESPO					
		A	07/07/18	STATUS	OPEN		INSE PROCEDURE Daily	ut IPP			
		<b>A</b>	07/07/18 01:01:29 PM	STATUS	OPEN	Catch all test	UNSE PROCEDURE DWA	ut IPP			
		A A	OTOTAS OTOTAS OUTPUT: OTOTAS	STATUS ESCRIPTION ONDARD	CIPEN Catch all test	Catch all test	UNSE PROCEDURE DWA	Unassigned			
		A A A	07/07/18 01:01:29 PM OUTPUT: 07/07/18 01:01:26 PM	STATUS ESCRIPTION ONDARD	CIPEN Catch all test	Catch all test	OPEN	Unassigned			
		A A A	OTOTAL OTOTAL OUTPUT: OTOTAL OTOTAL OUTPUT: OTOTAL	STATUS ESCRIPTION - exquarb exquarb devparb devparb Crical Caco Crical Caco	Canch all test Canch all test Cisco HCS PCA Cisco Alerts : Ur Efror (<13x340 7 2018 1	Catch all test RTMT_ALER Inventual Critical Catco 602:21 10.13.37.43: <1855	OPEN T OPEN Etter OPEN 78272 :: 52072 : CUCM12	Unassigned Unassigned Unassigned Unassigned			
		A A A	070718 01:01:29 PM 0007PUT; 07:0718 PM 0007PUT; 07:07/18 01:02:21 PM	STATUS ESCRIPTION - exquarb exquarb devparb devparb Crical Caco Crical Caco	Carch al test Carch al test Cisco HCS PCA Cisco Alorts : U Error (<13-Jul 7 2018 1 TMTTSesser Decedo	Catch all test RTMT_ALER IVernal Ortical Dato 60221101337-43-4385 Treekeld[AerDatal- Dr 1	DIPEN DIPEN T OPEN Errot OPEN Aparta :: saotra cocomita ar autor tacaza cotr ao	Unassigned Unassigned Unassigned Unassigned		NUC, IRTMT-1-IRTMT_ALERT: N curret: Courset: SessionaActive of	8 0 8 0
		•	01/01/20 PM OUTPUT: CROTHS 01/01/20 PM OUTPUT: CROTHS 01/02/21 PM OUTPUT: CROTHS	STATUS BECRIPTION - Devparb Sexparb Cricial Gaso Tomost Web	Carch of less Carch of less Carco HCS PCA Claco Alerts : U Energ (-13-Jul 7 2019) 1 PTM/Tilesscera Docedor Application(art)	Catch all test RTMT_ALER IVernal Ortical Dato 60221101337-43-4385 Treekeld[AerDatal- Dr 1	DIPEN DIPEN T OPEN Errot OPEN Aparta :: saotra cocomita ar autor tacaza cotr ao	Unassigned Unassigned Unassigned Isystech.com. JJ 07 20 18. elen RTM/TSessional		NUC, IRTMT-1-IRTMT_ALERT: N curret: Courset: SessionaActive of	® 0 ® 0
		•	01/01/20 PM 01/01/20 PM 00/07PUT: 01/01/20 PM 00/07PUT: 01/02/20 PM 00/07PUT: 07/07/18 01/02/20 PM	STATUS BECRIPTION - Devparb Sexparb Cricial Gaso Tomost Web	Carch of less Carch of less Carco HCS PCA Claco Alerts : U Energ (-13-Jul 7 2019) 1 PTM/Tilesscera Docedor Application(art)	Catch all test RTMT_ALER IVernal Ortical Dato 60221101337-43-4385 Treekeld[AerDatal- Dr 1	DIPEN DIPEN T OPEN Errot OPEN Aparta :: saotra cocomita ar autor tacaza cotr ao	Unassigned Unassigned Unassigned Isystech.com. JJ 07 20 18. elen RTM/TSessional		NUC, JETME-1-RETMET, ALERE: N curret: Courset: SessionsActive of	

#### **Alert Disposition**

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

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

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

ALERT AN	ALYZER		•				Displaying 1 - 10 o	( 3,899 Alens 40	< 1	* *	10 \$
PILTERS		SORT -	BULK DE	POSITION . STA	TUS -	STATUS	OWNER				
		A 070548	critical c pub.dimens Bervice op astdc-v-ce	isoo Ervor : Criical Cis Ional.com: Jul 10 2010 I erational status is DOMX s-pub-dimensional.com.[[] JUFRALS	oo mirror ( <i3>Jul 8 1:01:37 PM.154 UTC #012Cisco Califana</i3>	2018 12:81:37 169. NOC_RTHT-2-8THT_A per.#012The alert 1	254.5.16: <186>205685: 1 LERT: %:AlertRame-Critic a generated on Eun Jul (	alServiceDown][ 8 07:01:37 CDT	AlertDet 2018 en	a11+#012	®¢
			NODE POLICY RULE OWNER STATUS	2000-01000005-00-01-0044-1 departs Cace Akrts: Universal Ontical Cace Error Unatosigned OPEN UNDER REVIEW	L. NEXT	START 0700/16 IST CHANGE - APSED TIME - ESCALATION 0700/16 EXPIRES IN Expired PROCEDURE Delaut I	09/04:04 AM				
			devgarb	ACKNOWLEDGE RELEASE CLOSE		OPEN	Unassigned				≋≎
		CTORANS DTORESS AM OUTPUT:		DISREGARD CLOSE + LOCK The Scherological Service In Trade addc+-com-pub.dmension	Down[]AlertDetail=#012 S	envice operational status		er.A012The alert is g			
		CTOB18 07/02/25 AM OUTPUT:	desparb	Ciaco HCS PCA	RTMT_ALERT	OPEN	Unassigned				⊛≎



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

#### **Filtering by Disposition**

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

ALERT A	VALYZER	_ REPAIRS-					Displaying 1 - 10 of 246	Alerta de	¢	>	10 \$
PILTERS	1	SORT + BULK DISPOSITION +			STATUS .						
Test		DATE	NODE	POLICY	🗹 Open	STATUS	OWNER				
		CT/08/18 08:13:58 AM OUTPUT:		eb Cisco Alens : U @ Under Naview @ Astrowiedged Cisco Enrol (<13x-kd 6 2018 ,ALERT: Su/MerName-Citca	perational status	Unassigned on-pub.dmensional.com: Jul 08 2018 0 Is DOWN.4012Cisco CalManager 4012 (NodesD-astids +-com-pub); FITMT Area	The alert is (				
		A 07/08/18 08/14/44 AM	devparb	Cisco Allerts : U	CANCEL UPDATE	OPEN	Unassigned				80
		OUTPUT	(AlerName=Aut	harticationFailed[Ak		Failed events exceeds	yentach.com: Jul 08 2018 01:14:44 PM. configured threshold during configured in				

#### **Alert Filters**

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

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

FILTER MANAGER				✓ SAVE	* CANCEL
+ ADD - REMOVE		KEYWORDS SET	PERITY DATE & TIME		
Tost This is a test titler	ALLOW DISREGARD	NAME	Test		
		DESCRIPTION	This is a test filter		
		POLICY			
		RULE	Oritical Cisco Error		
		GROUP			
		CUSTOMER			
		SITE			
		NODE			
		MESSAGE			
		OWNER			

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

+ ADD - REMOVE	uniaumma	-			
	KEYWORDS	SEVERITY	DATE & TIME	~	©
Test ALLOW DISREGARD		ACTIVE	ESCALATED	ACKNOWLEDGED	EXPIRED
	A CRITICAL				
	A MAJOR				
	MINOR				

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

FILTER MANAGER		✓ SAVE	* CANCEL
+ ADD - REMOVE	KEYWORDS SEVERITY DATE & TIME		
Test ALLOW DISREGARD	DATE START DATE END DATE		
	TIME ALL DAY HOUR MINUTE HOUR MINUTE DAY OF WEEK SUNDAY MONDAY MONDAY MEDNESDAY FILIEDAY		

#### **Alert Journal**

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

To add an Alert Journal:

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

ALERT AN	to the Labor 1		TRESH					brapaying i	- 10 of 3,698 Alerts	a		/	*	10	•
FILTERS	+	SO	RT •	BULK D	SPOSITION	•	STATUS *								
Test			DATE	NODE	PC	DLICY	RUL	E	STATUS		OWN	ER			
		•	07/08/18 12:00:40 PM	1 1 203794 RTMT_ALERT DONN.#0120	4: astdo- 7: %[Aler Cisco Call cm-pub.dir	v-ccm-pub.d tName=Criti LManager.#0	imensional.com calServiceDown 12The alert is	m: Jul 08 2010 n][AlertDetsi) s generated of	018 17:00:40 169 8 05:00:37 PM.41 1=#012 Service o a Sun Jul 08 12: ce][ClusterID=][	0 UTC perat 00:37	ional CDT 2	RTMT statu 018 c	-2- s is n nod	(3	00
			DETAIL	S J	OURNALS						VI	EW R	EPOR	т	
			TINESTAMP	CR	EATOR	ACTION									
			07/08/18 12:	45.36 PM   sys	stem	devparb(127 <1865-20588 %UC_RTMT operational 1 12:00:37 CD	1.0.0.1) - Critical Gi 11: : 203794: astd 1-2-RTMT_ALERT: status is DOWN #0	isco Error : Criical fo-v-com-pub.dime %(AlertName=Cr 012Cisco CaliMan stdo-v-com-pub.di	autogenerated_sche Cisco Error (<13>Jul ensional.com: Jul 08 4 titcalServiceDown][Al ager.#012The alert is mensional.com.][App liert]	8 2018 2018 05 ertDeta genera	17:00: 00:37 F 1=#012 0ed on 3	40 169. PML410 Service Sun Jul	UTC: e 08		
			07/08/18 12	45:37 PM sys	storn	Incident Res	ponse - Method: A	LERT, Status: Su	ccess						
			07/08/18 12	45:37 PM svs	stem	Incident Res	oonse - Method: C	CONTROL Descri	ption: New Vodafone	Contro	. Status	: Succ	225		
			NEW JOURN	AL ENTRY						CI	LEAR		ADD		
			07/08/18 12:00:40 PM	devparb	ņ	500 HCS PCA	RTM	IT_ALERT	OPEN		Unas	signed		(8	03
			OUTPUT:												

#### **Alert Sorting**

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

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

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

ALERT AN		RETRICSH								<	-	*		+
FILTERS	F	SORT *	BULK D	SPOSITION	* STATU	S*	_							
Test		TIME TO EXPIRE/ESC	ALATE	ASCENDING	DESCENDING	~	~	-	STATUS		OV	VNER		
		ALERT SEVERITY		ASCENDING	DESCENDING	~	~	Error	OPEN		Un	assigne	d	(*
		ALERT DATE & TIME		ASCENDING	DESCENDING	UPDAT	~	>205881:::2 %(AlertName- ert is generate ClusterID=[N	CriticalSen d on Sun J	ul 08 12:	NertD 00:37 C	DT 2018	012 Se B an ne	IVICE
					GANGEL	UFUAI	-	Л	OPEN	D(0 11-		assigne		-
		12:00:40 PM												×
		OUTPUT:												
		A 07/08/18 d	evparb	Catch a	I test	Catch	all tes	t	OPEN		Un	assigne	d	()
		OUTPUT:												
		07/08/18 d	evparb	Catch a	l test	Catch	all tes	t	OPEN		Un	assigne	d	(*
		OUTPUT:												
		A 07/08/18 d	evparb	Cisco A	erts : Universal	Critical	Cisco	o Error	OPEN		Un	assigne	be	(8
		2	018 05:02 ssuerCN=	ASTDC-V-CCM-F	2018 17:02:03 16 %UC_ICSA-2-ICS UB][ErrorCode=2] t service detected	ACertifica AppID=Ci	teVali sco in	idationFailure: 1 itercluster Sync	%[SubjectC Agent][Clu	N=ASTD steriD=]	C-V-CC NodelD	M-PUB	1	
		A 07/08/18 d	evparb	Cisco H	CS PCA	RTMT	ALEF	ना	OPEN		Un	assigne	b	(*
		OUTPUT:												
		A 07/08/18 d	evparb	Catch a	Itest	Catch	all tes	t	OPEN		Un	assigne	be	*
		OUTPUT:												

### 3.1.4. Search

#### **Event Search**

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

#### Simple Searching

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

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

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



#### **Keyword Searching**

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

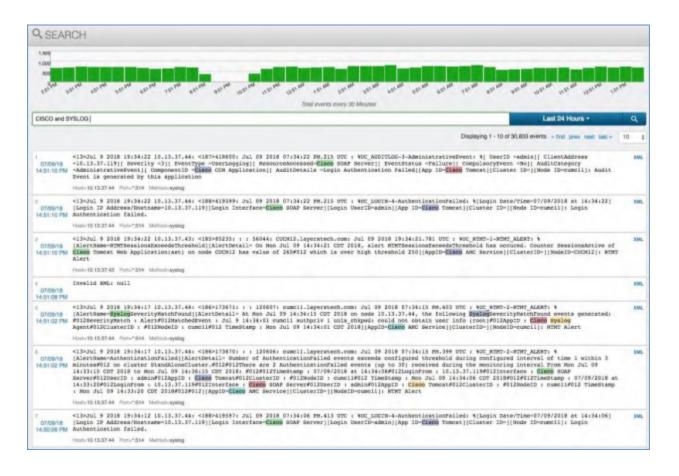
All log data that contains the keyword in the last 24 hours will be returned. The default number of logs per page is 10 but can be expanded by opening the drop-down box under the time bar and selecting the number desired.



#### **Utilizing Conjunctions with Searching**

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

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



#### **Date Range Searching**

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

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



#### Search Result Meta-Data

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



## 3.1.5. Call Path

#### **Call Path Monitor**

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

CALL PATH MONITOR									Displaying 1 - 5 of 5	*	< >	30	RANGE: 1 H	DUR •
								× search			Q,*	SOUT: TO	TAL DELAY DE	sc •
DATH	METHOD	DELAY	ANG DELAY	HOPS	ACALLS	LAST CALL	#PATHS							
LXLAB-RTR-1-eth1 Ciaco ASA	LX1	863.00	94.35	6	23	07/09/18 04 21 55 PM								8
- S												OFFINET	1 1	э
1		-					-	8		-			0	
7-		8	-	_		-				0			•	
						103								
-	/					8								
2 3	-					8								
	-					8								
2 VI AB STE Letter	LXI	62.00	33.92		12	07/09/18 04 13:15 PM								6
DXLAB-RTF-1-etti		62.00 36.00	33.92 34.25	5			8							

### **Sorting Call Paths**

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

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

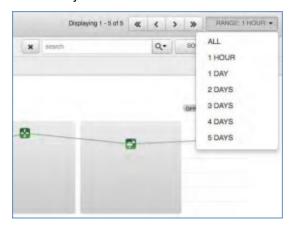
Each selection also has the choice of selecting ascending or descending order.

TAL DEL	AY (	▼ ASC	DESC
TAL HOP	PS		
			)

#### **Time Range for Call Paths**

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

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



#### **Expanding Call Paths**

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

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

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

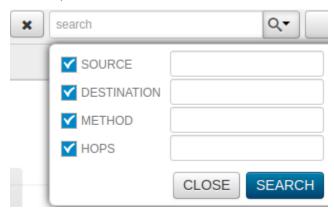
By default, the view will be in graph mode. To switch to the table view, simply choose the table view icon in the upper left corner of the now expanded call path.

CALL PATH N	ion in on									Displaying 1 - 5 of 5		> 27	RANGE: 1	
									× search		Q.	som	T TOTAL DELAY	DESC +
PATH	ME	THOD	DELAY	AVG	HOPS	PCALLS	LAST CALL	PATHS						
DXLAB-RTR-1-	eth1 Cisco ASA LX1		663.00	94.35	6	23	07/09/18 04:21:55 PM						Latency by Ho	
n <sup>4</sup> m												DEF N	-	2 3
													the state of the s	
1								_	8		-		0	
			8		_		0						-	
2	- 23													
	ebi		62.00	33.92		12	OTOBINE DEITOTIS PM	12						
LXLAB-RTR-1- LXLAB-RTR-4-	ebi			33.82 38.82		12	D705/18 D4:12:15 PM	[2]	JITTER		ON	NETWORK		
LXLAB-RTR-1-	ethi LXI					12		12	JITTER		ON			
LXLAB-RTR-1-	ethi LXI		AS			12	LATENCY	10				JE		
LXLAB-RTR-1-	eth1 LXI eth1 LXI IP ADORESS 172:16.1.11 (Endpe		AS , LX	SET NAVE	-ath1	12	LATENCY	42	0		TRI	JE SE		
LXLAB-RTR-1- LXLAB-RTR-4-	eth1 LX1 eth1 LX1 IP ADORESS 172.18.1.11 (Endp 172.18.1.1		AS - LX LX	LAB-RTR-1	-ath1	12	LATENCY 0 2.85	42	0		TRI	JE SE SE		
LXLAB-RTR-1- LXLAB-RTR-4-	eth1 LX1 eth1 LX1 IP ADORESS 172.16.1.11 (Endp 172.16.1.1 172.16.2.1		AS  LX LX	LAB-RTR-1-	-ath1 -ath1	12	LATENCY 0 2.86 7.67	10	0		TRI FAL	JE SE SE		

#### **Searching Call Paths**

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

- · Source
- · Destination
- · Method
- Hops



#### View Call Details from the Call Path

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

### 3.1.6. Call Details

#### **Call Details Explorer**

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



#### Filter by Date and Time

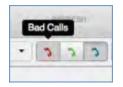
In the upper left corner there is a time bar. You can choose to search the call details by the various options presented. When you click inside the bar several options along with a calendar open up to select.

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

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

Jul 9, 2018 4:06 p	om - Jul 9, 3	2018 5	:08 p	m	•	3	3	3 4	8	C	×			
Last 5 Minutes	<	34		0	2018		>		Ju			201	8.0	>
Last 30 Minutes	Su	Mo	Tu	We	Th	Fr	Sa	Su	Mo	Tu	We	Th	Fr	Sa
Last Hour	24	25	25	27	28	29	30	24	25	26	27	28	29	30
Last 12 Hours	1	2	з	4	5	6	7	1	2	3	4	5	8	7
Last 24 Hours	8	9	10	11	12	13	14	8		10	11	12	13	14
	15	16	17	18	19	20	21	15	15	17	18	19	20	21
Last 7 Days	22	23	24	25	26	27	28	22	23	24	25	28	27	28
This Month	29	30	31	τ	2	3	4	29	30	31	1	z	3	4
Last Month	1		1:10	08		PM		5		:	08		PM	
Last 2 Months														
Last 3 Months														
Last 6 Months														
Last Year														

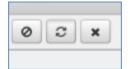
#### Filter by Call Quality



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

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

#### **Clear Filter, Update and Delete Call**



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

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

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

#### **Refresh Pause**

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



#### Sorting

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

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

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

Displaying 1 - 50 of 208	«	<	>	>>	SORT	LATENC	Y DESC -
	10		LATE	INCY	•	ASC	DESC
	1	TIM	IE				
		SO	URCE				
		DE	STINA	TION			
	-	VE	NDOR				
		LAT	ENC	(			
		HO	PS				

#### **Search Call Details**

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

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



## 3.1.7. Call Management Configuration

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

ARCHIVE OPTIONS	DAILY	WEEK	Y N	MONTHLY	QUARTERLY		
ALERTING OPTIONS	ALER	T ON AR	CHIVE	FAILURE	ALERT ON ARCH	HIVE SUCCESS	
HOST	,	NETHOD		METHO	DS PATH	CREDENTIAL	
		SCP 8	SFTP	SMB		admin	\$
		SCP S	SFTP	SMB		admin	\$

# 4. Configuration

## 4.1. Configuration

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

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



## 4.1.1. Policy Configuration

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

- Business Processes
- Infrastructure
- Security

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

olicies			Rules					
Name Failove	•		Name	Threshold	Window	Severity	Response Proces	fure
Avaya Call Monitor		4	Bitter Value Exceeded	1 time	1 minute	Critical	LinkCallToAlert	¥3 = Z
Avaya PDS SNMP Alarms		4	Name	Laterary littles From	- dad			21 = V
Avaya PDS SYSLOG Alarms		13		Latency Value Exce	6060			
Cisco Call Monitor		4	Description					
LATERX Agent Monitor		3						
Log Monitor		1						
LX1 Call Monitor v2		8	Туре	Simple		Action	Respond \$	
LX1 SIP Call Errors v2		8	Threshold	1	Respon	se Procedure	Reboot Machine \$	
Nortel Call Monitor		3	Window	1 minute	: Defi	nition Output		
PING Monitor		2	Severity	Critical		Enabled		
Powerwave SNMP Alarms		11	Jurenty	Catego			-	
SiLo training policy		2				nherit Output		
Test Alarm v1		Ŧ			H	alt Processing		
AJ ExperiMental	<b>V</b>	3	MOS Value LOW	1 time	1 minute	Critical	LinkCaliToAlert	A1 = Z
ALSTOYBARN : Austin - Alert Esa.		0	Packets Lost Value Excer	eded 1 time	1 minute	Critical	LinkCallToAlert	21 = 2
ALSTOVBARN : Dallas - Alert Exa.,		0						
ALSTOYBARN : NYC - Alert Examp.		9					Displaying 1 - 4 of	4 events + first prev next las

#### **Correlation Rules**

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

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

Parameter	Description
Severity	Indicates what is to appear in the Status field on the Alert Viewer monitor. Select the severity for this rule: • Informational • Minor • Major • Critical
Action	<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 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 menu to execute when conditions have been met.
Definition Output	Selects a single Correlation Definition's extracted value to be displayed with the Alert.
Enabled	Toggle to enable/disable the rule
Inherit Output	Toggle to enable/disable whether the rule will include the results of the filter attached to the policy module.
Halt Processing	Toggle to halt processing of logs to any other rules within the policy if the rule matches. This will highlight the Policy in Green to indicate that this function is in use.
Correlation Definitions	Click the wrench icon where you can define one or more definitions match and or extract the required data from a log or event. See Correlation Definitions.
Output Order	Sets the preferred order to output the extracted data from the Corre- lation 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 CONFIGUR/	ATION	Rules.	Fibers							Save
Policies Name Fail	over		Rules	Threshold	Wine	daw Severity	Response	Proced	re	
Arda.			Name	Jitter Value Exceede	d				23 E 🔽	
Aspect URP System Alerts	2		Description	-						
Asset Log Monitor										
Avaya Call Monitor	<b>2</b> 4									
Awaya PDS SNMP Alarms	2 4		Туре	Provide Name		Action	Barried	-1		
Avaya PDS SYSLOG Alarms	1	5		Simple	-		Respond	-		
Cisco Call Monitor	<b>2</b> 4		Threshold	1 2		Response Procedure	LinkCal/ToAlert			
LAYERX Agent Manitor	<b>2</b> 3		Window	1 minute	1	Definition Output				
Log Monitor			Severity	Critical	1	Enabled				
LX1 Call Monitor v2						Inherit Output				
LX1 SIP Call Errors v2						Halt Processing	2			
Nortel Call Monitor	<b>2</b> 3		-			ute 🕕 criscal				
ONG Manhor	20		Latency Value Exceeded	1 time	1 mir	Criscal	LinkCaliToP	GET	A3 = 1	

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.

POLICY CONFIGURA	ATION Rules	Filters		Save
Policies Failo	wee	Filters Pattern		
Arda	0	Name		
Aspect UIP System Alerts	1 T	Vendor Method		
Asset Log Monitor	0	Pattern		
Avaya Call Monitor		(method="cisco")	1	
-		Source Field		
Avaya PDS SNMP Alarms		Raw Log	~	
Avaya PDS SYSLOG Alarms	2	Pattern Type		
Cisco Call Monitor	<b>V</b> 2	Regular Expression Match/Extract	\$	
LAYERX Agent Monitor		Punction Value		
		None ¢	and the second se	
Log Monitor	0	Name		
UX1 Call Monitor v2		Call Manager Ip		
LX1 SIP Call Errors v2	0	Pattern		
Nortel Call Monitor	1	callManagerip="(,"7)"	1	
PING Monitor		Source Field		
	_	Raw Log	~	
Powenwave SNMP Alarms	2	Pattern Type		
SiLo training policy	1	Regular Expression Match/Extract		
Test Alarm v1	10	Function Value		
AJ ExperiMental		None ‡		

#### **Example: Policies and Alerts**

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

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

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

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

You can configure this definition in two ways:

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

#### **Correlation Definitions**

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

Parameter	Description
Name	Name this as close as possible to the data elements being extracted. That way the output matches the name once viewed in the alert text. It is also utilized in the key value pair within the alert text. 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
Function	If the extracted data is integer based, then you can apply the following functions that will allow you to compare the data: • None • Greater Than • Less Than • Same
Value	This field will only be available if the data extracted is an integer.

RULE DEF	INITIONS » Jitter Value Exce	eded	Changes made	Cancel Update
01800				Last 24 Hours - Q
Citch here for t	Build a New Defi		Displaying 1 - 10 of 154,94	2 events + first prev next last+ 10 t
Source Field	Raw Log	×		
2 07/11/18 16:54:10 PM		osts'11, "ReturnCode'1'0", "ErrorMessa AssotTpAddress", 10,13,37,43", "Mame"	ge","","AMU","CUCH12","Risbe","CUCH12","AssetName";"13.1 "CUCH12","ServiceMame","Cloce Trace Collection	(3.37.43","AssetRostname":"10.13
a 07/11/18 16:54:10 PM	/part2/jsil/arbitrator1/modules Stack traces 0 [internal function]: SoapCli #1 /part2/jail/arbitrator1/modu #2 /part2/jail/arbitrator1/modu #3 (main)	les/sxec/cisco/axlGetPhoneInventory_	<pre>ds.php100 ', 'http://idhemas,', i, 01 creds.php(00): BoapClient-&gt;eall('SelectAbevice', Array) creds.php(00): BoapClient-&gt;SelectAbevice('', Array)</pre>	(1)

RULE DEFINITIONS * Jitter Value Exce	eeded		Please fill in all Name and Pattern fields	Cancel	Update
dieco			Last 2	4 Hours +	٩
Click here for help building rules Build a New Defi	inition Manually		Displaying 1 - 10 of 154,942 events + Re	t prev next last	10 8
Events CALL_METRICS_IO Ø Hitter Ø	CALL_ID · (rem) ·				
Name	Pattern		1		
(new)					
Source Reid					
Raw Log					
Pattern Type	Function	Value			
Plegular Expression Match/Extract	I Norw	1			
(13×241 11 2018 21:51:01 logger 07/11/18 16:54:10 PM *: "Ciaco Trace Collection Servi B Extracted Value:	<pre>:: {'CIBCO_RTHT_SERVICE': bota':1, "ReturnCode':'0', "ErrorMessage':' ce', "ElapsedTime':2958218, "ServiceStatus':</pre>	,"ANC"+"CUCH12","H14 "1"})	ICC'1'CUCM12','AssetName'1'10.13.37.43','A	asetfostname":	10.13.37.,

Regex Wizard		Cancel	Update	Regex Wizard	Cancel Update
1) Select a Log 2) Create Riges				1 (Select et al., 2) Dense Reger	
Search for logs:				classi vermines'1.0' encodings '85.85011'70-85095-0209 -0200170-20005-02011-0200177_20007-0/207111_08207-02 -020070-02018-020070-020177_20007-0207000-02070-020	EV3CE-2808-0108000-00-814/DEV10E>
- Dis	Last 24 Hou playing 1 - 10 of 2,961,353 events is finite pre		Q.	<ul> <li>CONTRACT, CONTRACT, Second Struct CONTRACT, CONTRACT,</li></ul>	ORDEREN-2008-0200081-34-MEDIEF-4/MEDIEF- METS-ARTOREN-127,0.4.1-MEDIEF METS-ARTOREN-4/ARTOREN-MEDIEF MEDIEF-ARTOREN-4/ARTOREN-1000-4/DEALER MEDIEF-ARTOREN-135-241.11.2018.2016-35
<pre><entity>2000//INTITY&gt;<entity 014/DEVICE&gt;<endup>LATERE//OND &lt;10&gt;127.0.0.34/IE&gt;</endup></entity </entity></pre>	* 08-8621 * Profectings - Dards - Robert - Barty Barty - Alaritity - Galaxy - David Co-2000 - 01 Dars - Content - Salar - Content - Salar - Sa	000005-80- vparb=/%8,800 g>=//MODULE>		[13] J. A. G. H. (210). Alth. J. D. (Construction of a construction of the construc	PER-CALENT MARK ITEMPENDED COMPANY VERITOR COMPANY CALENT MERICIPA
«PORT>127.0.0.11514*/PORT>4AD 10070-000020 4TRAKEPORT>4087 400PERT>4/00PERT>4ADJUE 4808000>40EFERENCE13>4/REFERENCE 4808000>40EFERENCE13>4/REFERENCE 4808000>40EFERENCE13>4/REFERENCE 4808000>40EFERENCE13>4/REFERENCE 48080000>40EFERENCE13>4/REFERENCE 48080000>40EFERENCE 48080000>40EFERENCE 48080000>40EFERENCE 48080000000000000000000000000000000000	IDREES-127.0.0.1*/ADDRESS-4/IDDAL_2P+ COMPANIE-/DRVICEDATE-4/DC+4TART-15111 TED-4/ADJREES-4/UTC-4/TRANSPORT-4/NON GEIDE	VURDAL 194 446354/STARS DK-OKOULEDE	D-GEBD> ITAIL>	WHERE DOES THE WATCH REGIST Is there any test that investigating proceeds your search? (5a), ensure in here or eline leave this field block.	and white the start on the paper we
3018 22/03/05 127.5.5.17 (/RAMIDO-ARTER_ARTER14//ARTE ARTERT_INSTRUMENTIAL/ARTER ARTERT_INSTRUMENTIAL/ARTERNAL (ARTERT_ARTER15) (ARTERT_MCADER55) (ARTERT_MCADEF55) (ARTERT_MCADEF55) (ARTERT_MCADEF555) (ARTERT_MCADEF5555) (ARTERT_MCADEF555555) (ARTERT_MCADE555555555555555555555555555555555555	HE YELTSTEINE DATTER MALE / MODINE (AND AND AND AND AND AND AND AND AND AND	ull)]))##ak, HE> AGGET_HOGTHU DATA/ABGET_V GE>		LIST ALL PHEASES YOU ARE TRANSIG TO MATCH	**
Select log from the list above or pass				Even a phrase or realize phrases you some to realize, "I provident to realize any presses before this field blanck."	lociale the test after these physics
	α <sup>+1</sup> 1.8. AUCL1         1.7. PERCEPTING CARPENDER           1.1.         CARPEZ-VENTER         CARPEZ-VENTER         CARPEZ-VENTER           1.1.         CARPEZ-VENTER         CARPEZ-VENTER         CARPEZ-VENTER           1.1.         CARPEZ-VENTER         CARPEZ-VENTER         CARPEZ-VENTER           1.1.         CARPEZ-VENTER         CARPEZ-VENTER         CARPEZ-VENTER           1.1.         CARPEZ-VENTER-VENTER         CARPEZ-VENTER         CARPEZ-VENTER           1.1.         CARPEZ-VENTER-VENTER         CARPEZ-VENTER         CARPEZ-VENTER           1.1.         CARPEZ-VENTER         CARPEZ-VENTER         CARPEZ-VENTER           1.1.         <	00-01080085 MENDENCH ACOULENC/HO 004/HETHODN 180-(/WINTHODN 180-(/WINTHO NCHIDN HOHIDN	00- //WARE>- OULE> ML_IP>	ETEP 4: WHERE DOCK THE SAFE() ETCEI is there are ser list that investigately follows prov answch? If is, onter 4 here ar eiter some tild, find bland, BEETER ELEMERATED : 6-70	accure that test is my capture () Match with end of low_

## **Creating a Policy**

To Create a Policy:

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

POLICY CONFIGURAT	ION	Rules	Filters	Change	s have been	made					Save
Policies Name Failove	•		Rules Name		T	reshold	Window	5	leverity		Response Procedure
Asterisk Basic	-	5									
Clsco CUCMv8 to 11.5	$\mathbf{M}$	447									
Cisca CUCMV8, r2 up	$\mathbf{M}$	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)	$\mathbf{\mathbf{v}}$	215									
Sample Events	$\checkmark$	1									
Example Policy									No re	cords rules	+ first prev next last =

## **Creating a Correlation Rule**

To Create a new Correlation Rule:

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

		. 🕲 🗸	( 前		۹ ۹	, <b>6</b> -	± 1	••	1 admin+
POLICY CONFIGURATI	ION Min	Filters	Film at fee	ts before saving a	nd make sure at	rules have at least	t pefinitio	n	Save
Policies		Rules							
Norne Failmer		Name		Threshold	Window	Severity		Response Proce	dure
Avaya POS ShallP Alarma		D per tatus	Exceeded	1.674	t minute	() cm	of.	LinkcatfloAkers	×1 = Z
Aviga PDS SPSLDG Alarms	-	Lateray Tal	Le Dorerted	1674	1 minute	() Cris	al .	UniCalification	21 - 2
Case Call Member	<b>El 3</b>	MOSTAN	LOW	1.8me	1 minute	() cm	al	LinkCalifisAlert	21 - 2
LAVERT Agent Monitor		-							
Log Monitor	2 (T)	Packets Lo	e tolue Gicen	fed 1 pre	1 minute	O Cris	Cal.	LinkCallfloWert	A) = 2
LKI Call Monitor v2	<b>2 3</b>		Norre	(real)					A0 = 5
Lift SIP Call Briors val		De	ecquan						
Nortei Call Monitor	<b>2</b> 3								
PING Manitar									
Powerwave Shall? Marvis	1 m		Type	Simple		Action	Thack	Tespont 8	
SLatraining policy	12		hended	1		sponse Procedure	Detail	100 4	
Test Alarm v1	TT		Window						
Al OperMental	<b>2</b> (1)			1 minute		Definition Output		:	
ALSTOYBARN : Austin - Aiert Ess.			Severity	International		Enabled			
ASTOYBAIN Dalas - Nert Exa.						Inherit Output	2		
ALSTOYBARN : NITC - Alert Damp.						Halt Processing			
APC Powernet MIB Traps	-								
APEX SOLID Alarm Test	<b>2 •</b>							Displaying 1 - 4 of 4	rules + first prev next last -
	-								

## **Creating a Definition**

To create a new definition:

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

OLICY CONFIGURATION Rules Fibers				~	
olicies Rule	s				
Name Failover	Name Th	weshold Wind	law Severity	Response Proce	dure
Cipco Call Monitor	Itter Value Exceeded 1 t	time 1 min	rute 🕕 Critical	LinkCaliToAlert	P3 =
I ADDRESS AND ADDRESS MILL ADDRESS					
LE DEFINITIONS + Jitter Value Exceeded		Overges	ude .	Cancel Update	
ina			Last	24 Hours - Q	
a have for help building rules Build a New Definition Manually			Diplaying 1 - 10 of 154,042 events + 1	tel pres sent lint = 10	
EVENTS EALL_METRICE_D @ JEW @ CALL_D @					
arce field Real Log					1
	NET:		117- Teaching (173) 13-15-15	Section and a sector sector sector	1
Chindal II 2000 Electric Lagree ("CINCL, NEW", NEW" ("Theorem," "INJECTOR Data ("Lagree", "Lagreed and Solid PM 30, 45", "Association (Lagreed Data ("Lagreed Data ("Lagreed Data Barvice", "Klapsed Lagr. (2010).	1.13.37.43", "Masse"1"0003012", "Me	ericelane": "Claco Tra	ce dullaction		
mostri 127.8/0,1 Post-Vervilleg Microsoft Bedract P	wid .				
ARTIKEBBS-Socket, Created, Skill FM					1
4/METURNARD>	cel Seve				1
Hee-12720.1					
RULE DEFINITIONS > Jitter Value Exceeded	d		Peace fill in all Name and Pa	Dam Sekts	Cancel Update
ciace				Last 24 Hours	1+ Q
Click here for herp building rules Build a New Definition	Manually		Personal Mar		
			Different 1 - 10 -	F154.542 events + first prev	real last + 10 - a
THERE'S CALL_WETRICS_ID @ BOOM CAL	1,0 ° (res) °				
Name Patt				1.81	
(vex)					
a second s					
Source Reld					
Reviag	-	The			
		Value 1		1	
Nav Log V Pattern Type Pure Pepalar Expression Matth/Estruct 8 No	ne.			)	
Raw Log Million Type Pure	ne.		1°, "Numer of Octors", "Assessment	(*1.1.1.1.1.1.), Teneda	riame"+"18,13,33,-
Raw Ling view Pattern Type Runn Pepter Dynemote MathyTothat & Non *13-294, 11 2018 21:51:55 Longgers (*C EXPLOYING *126-8748 51349823, "Randfibrars" *154599 **248 5149823, "Randfibrars" *154599 **248 5149823	ne.	0 0400*********************************		······································	
Rev Log View Pattern Type Rune Pequire Dynesson Mattry Estruct 6 No +129-201, 11, 2018, 21:51:65, Loggers, 6*C Extratage -1512.524.822, "Badd Dense (656-000, **C-124-0 Table Section-7)	ne.	*	ex Waard		etaam"s"18.13.33.+ Cancel Update
Revelang veri Rathern Type Runn Pequer Dypression MathyTothast & Non *12*-2NL 11 2018 21:51:65 Longgers (*C EDV11018 (*Classical value) *155-2NL 12 2018 21:51:51:24:22, "BaddTarts" *154-500 **Classical value	ne 1903_WTMD_KERVICE": 13_"NoturBOdd":"1";"Erschwe ElapsedTime":1918219,"Terviced	1 10 10 10 10 10 10 10 10 10 1	en Wizard Fron et og. 2) Onser Regar		Carcel Update
Anno Log Puttern Type Puttern Type Puttern Type Puttern Type Puttern Type (*12-Vic) 15 2018 21:151:05 Loger: (*C EMVINE (*12-Vic) 15 2018 21:151:05 Loger: (*C EMVINE (*12-Vic) 15 2018 21:151:05 Loger: (*C EMVINE *Calence Trace Calencian Berline*,*T Extended Volume Regent Wizard Tytewer alog 2) Science Regent	ne 1903_WTMD_KERVICE": 13_"NoturBOdd":"1";"Erschwe ElapsedTime":1918219,"Terviced	1 10 10 10 10 10 10 10 10 10 1	en Wizard Fron et og. 2) Onser Regar		Carcel Update
Revelag view Pattern Type Rank Pepter Types Name Pepter Types View Pepter Types View 1554/00 PM ***Class Trace Collection Service**** Regex Wizard 1556/00 PM ***Class Trace Collection Service****	ne 1903_WTMD_KERVICE": 13_"NoturBOdd":"1";"Erschwe ElapsedTime":1918219,"Terviced	1 10 10 10 10 10 10 10 10 10 1	en Wizard Fron et og. 2) Onser Regar		Carcel Update
Revelag Version States	ns 2005 Artiser, JERWITER** 1-2 - Tentore Scheff * 1*** - Terrecolmen Cancel Update Cancel Update et 24 Hours - Q	1 1 1 1 1 1 1 1 1 1 1 1 1 1	ex Wizard Inno.ing. 2/Oran Ages a) services '1.0' exceeding '01-001 Inno.ing. (10' exceeding '01-001) Inno.ing. (10' exceeding '01-001) Control (10) (10) (10' exceeding '01-001) Control (10) (10) (10' exceeding '01-001) Control (10) (10) (10) (10) (10) (10) (10) (10)		Cancel Update Trijetio- 20 anije - 4 - 4 - 20 - 20 - 20 - 20 - 20 - 20 -
Region Ing View Region States (* 1000) Region Type Russ Pastern Type Russ Pastern Type Russ *159-201, 11, 2018, 21:01:151, longers; (* 0) EDVTUTE (* 118:01:83, 11:01:151, longers; (* 0) EDVTUTE (* 118:01:83, 11:01:151, longers; (* 0) EDVTUTE (* 118:01:83, 11:01:151, longers; (* 0) Region Wilcard 1) forest atog Science Region * EDVTUTE (* 118:01:83, 11:01:151, longers; (* 0) Edverts for Riges * EDVERSE * EDVERSE	ns 100 Arter Janvicz** ), hetersolati **** Transfer Laponities ***** Cancel Updat 1224 Hours • Q, •for prev next late 19	1 1 1 1 1 1 1 1 1 1 1 1 1 1	ex Wizard Inno.ing. 2/Oran Ages a) services '1.0' exceeding '01-001 Inno.ing. (10' exceeding '01-001) Inno.ing. (10' exceeding '01-001) Control (10) (10) (10' exceeding '01-001) Control (10) (10) (10' exceeding '01-001) Control (10) (10) (10) (10) (10) (10) (10) (10)		Cancel Equilation TELETION 2010/00- 2010/00- 2010/00-2010-00- 2010/00- 2
Regist Wizard  Physics "Job Section 100 (100 - 100 (100	ns 100 Arms JEWICE** ), Tentersolutie**** Cancel Update 124 Hours • Q • first prev rect last+ 33 Ben-derrications	1 1 1 1 1 1 1 1 1 1 1 1 1 1	ex Wizard Inno.ing. 2/Oran Ages a) services '1.0' exceeding '01-001 Inno.ing. (10' exceeding '01-001) Inno.ing. (10' exceeding '01-001) Control (10) (10) (10' exceeding '01-001) Control (10) (10) (10' exceeding '01-001) Control (10) (10) (10) (10) (10) (10) (10) (10)		Cancel Equilation TELETION 2010/00- 2010/00- 2010/00-2010-00- 2010/00- 2
Partiam Type Pattern Type Patt	na 1903 HTML JERVICE": 1. "Interschaft" ("1", "Interchant Cancel Updat 82.24 Hours • Q, •fing province last • 70 BR-600119712190- 10000-100005-01- •70000-100005-01- *70000-100005-01-	1 1 1 1 1 1 1 1 1 1 1 1 1 1	en Wizard Fron et og. 2) Onser Regar		Cancel Equilation TELETION 2010/00- 2010/00- 2010/00-2010-00- 2010/00- 2
Register Type     Fastern Type	ns 100, Arter, SERVICE** ), "Reteriseded" ***, "Erreschere Legenetiter ************************************	1 1 1 1 1 1 1 1 1 1 1 1 1 1	ex Wizard Inner III, 21 Onner Report III dentified (1), 21 Onner Report IIII dentified (1), 21 Onner Report III dentified (1), 21 Onner III dentifi		Cancel Update Trijetio- 20 anije - 4 - 4 - 20 - 20 - 20 - 20 - 20 - 20 -
Res Log     Image: Common Matter Status     Image: Common Matter Status <td< td=""><td>na 100, Artine, JERVICE** 1, - Retroit Scholt****, * Terreichen Laponettine*********************************</td><td>1 1 1 1 1 1 1 1 1 1 1 1 1 1</td><td>ex Witand Internet II. 21 Dears Expo Internet II. 21 Dears Expo Internet II. 21 Dears Expo Internet II. 21 Dears Expo Internet II. 21 Dears II. Internet II. Intern</td><td></td><td>Cancel Update</td></td<>	na 100, Artine, JERVICE** 1, - Retroit Scholt****, * Terreichen Laponettine*********************************	1 1 1 1 1 1 1 1 1 1 1 1 1 1	ex Witand Internet II. 21 Dears Expo Internet II. 21 Dears Expo Internet II. 21 Dears Expo Internet II. 21 Dears Expo Internet II. 21 Dears II. Internet II. Intern		Cancel Update
Res Log     Image: Common Matter Status     Image: Common Matter Status <td< td=""><td>na 100, Artine, JERVICE** 1, - Retroit Scholt****, * Terreichen Laponettine*********************************</td><td>8 1000 (100</td><td>ex Wizard Inner III, 21 Onner Report III dentified (1), 21 Onner Report IIII dentified (1), 21 Onner Report III dentified (1), 21 Onner III dentifi</td><td></td><td>Cancel Update</td></td<>	na 100, Artine, JERVICE** 1, - Retroit Scholt****, * Terreichen Laponettine*********************************	8 1000 (100	ex Wizard Inner III, 21 Onner Report III dentified (1), 21 Onner Report IIII dentified (1), 21 Onner Report III dentified (1), 21 Onner III dentifi		Cancel Update
Register Type         Partieren Type         Parieren Type         Partieren	100_HING_BENVICE**     1 TensesSubd******     1 TensesSubd******     Cancel Update     Concel	8 1000 (100	ex Wizard Sector 2 Course Fage al sector 2 C		Cancel Update
Rev Log     Image: Compression Management Status: Compression Management Mana	100_HING_BENVICE**     1 TensesSubd******     1 TensesSubd******     Cancel Update     Concel	8 1000 (100	ex Wizard Sector 2 Course Fage al sector 2 C		Cancel Update
Register Type         Partieren Type         Parieren Type         Partieren	Initial State (Section 1)         Initial State (Section 1)           1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,	8 1000 (100	ex Wizard Sector 2 Course Fage al sector 2 C		Cancel Update
Res Lag     Image: Comment Name       Pattern Type     Pattern Type       Pattern Type	Interface         Interface           1.1. Interface         Interface           1.2. Interface         Interface	8 Reger * *** *****************************	ex Wizard Sector 2 Course Fage al sector 2 C		Cancel Update
Register Type     Partieren Type	A The second of the secon	8 Regel *, * *, * (Ref*, * CERE) Regel *, * *, * (Ref*, * CERE) 8 8 8 8 8 8 8 8 8 8 8 8 8	Winard     All Const Equal     All Const		Салка Ориана 1999 - Салка Ор
Register Type     Fastern Type	A      BOD ATTAC JERVICE**     A      The set of body **** *     Cancel     Update     Cancel     Update     Cancel     Update     Set 24 Hours *     Q	8 Regel *, * *, * (Ref*, * CERE) Regel *, * *, * (Ref*, * CERE) 8 8 8 8 8 8 8 8 8 8 8 8 8	ex Wizard Inner 2 Orace Report al semanary 2 Orace Repor		Cancel Syndrome Property in the second syndrome of the second syndr
Register Type     Fara       Parame Type     Fara       <	Intersection         Intersection           1.1. The transmission         1.1. The transmission           1.2. The transmission         1.1. The transmission           1.3. The transmission         Intersection           Cancel         Update           22.24 Hours         Q.           • first preveneot late         30           Ben-Martin Transmission         30           Ben-Mart	8 Regel *, * *, */RC* * * COOKL Regel *, * *, */RC* * * COOKL ************************************	Winard     All Const Equal     All Const		Салка Ориана противо проти
Register Type     Fastern Type	Interface         Interface           1000_PTMC_LERVICE*	8 Reger * * * * * * * * * * * * * * * * * * *	Winard     Constraints		Cancel Syndrome Property in the second syndrome of the second syndr

## **Deleting a Correlation Rule**

To delete a Correlation Rule:

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

POLICY CONFIGUR	ATION	Rules	Filters					Save
Policies			Rules					1
	over		Name	Threshold	Window	Severity	Response Procedure	
Cisco Call Monitor	<b>X</b> 4		CLEARED - RITE Alarm	1 time	1 minute	() Informational	AlertClear	¥7 = Z
LAYERK Agent Monitor	1							
Log Monitor			CRITICAL - RPTR Alarm	1 dme	20 minutes	Critical	AlertHold	¥7 = /
DK1 Call Monitor v2	<b>1</b> 3		DISREGARD - FailedNodes	1 time	1 minute	() Informational	DoNotAlert	A1 = Z
LX1 SIP Call Errors v2	<b>1</b> 6	-	DISREGARD - UnableToRun	1 time	1 minute		DoNotAlen	×1 = ×
Nortel Call Monitor			IN STERMINATE - RPTR Ala	10.00	15 seconds		DoNotAlert.	
PING Monitor	2		and the second second	- 1011	12 Million Para	W monautre	Somerari.	
Powerwave SNMP Alarms		T)	ISG Alarm trap - INDETERMI	1 dme	1 minute		DaNotAlers	×1 = ×
SiLo training policy	1 (3		ISG Alarm trap - MAJOR	1 time	1 minute	() Major	DoNotAlert.	×1 = ×
Test Alarm v1	11		_			-		
AJ ExperiMental	V (1		-				Displaying 1 - 11	of 11 events + first prev next last
- +			- + C					

#### **Deleting a Policy**

To delete a Policy:

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

Policies			Rules					
Name Faile	over		Name	Threshold	Window	Severity	Response Procedure	
Cisco Call Monitor		4	CLEARED - RPTR Alarm	1 time	1 minute		NertClear	127 =
LATERX Agent Monitor		3	-	10.2				
Log Monitor		1	CRITICAL - RPTR Alarm	1 time	20 minutes	Critical	AlertHold	A1 = 1
UK1 Call Monitor v2		5	DISREGARD - FailedNodes	1 time	1 ininute		DoNotAiert	A1 = 1
UK1 SIP Call Errors v2		6	DISREGARD - UnableToRun	1 time	1 minute	() Informational	DoNotAlert	1 = 1
Nortel Call Monitor		3	INDETERMINATE - RPTR Ala	1.1100	15 seconds	() Informational	DoNotAlert	
PING Monitor		2		Tume	19 seconds	U montabonal	DONODIET	
Powerwave SNMP Alarms		n	ISG Alarm trap - INDETERMI.	1 time	1 minute	Informational	DoNotAlert	<u> 21 = 2</u>
Sto 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		3		Tume	Timeque	() Major	DONOPIET	A1 = 2
ALSTOYBARN Austin - Alert E		3				0	Displaying 1 - 11 of 11 events	efirst prev next last

## **Disabling and Enabling a Policy**

To Disable and Enable a Policy:

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

Policies			Rules					
Name Failove	r		Name	Threshold	Window	Severity	Response Procedure	
Cisco Cali Monitor		4	CLEARED - RPTR Alarm	1 time	1 minute	() Informational	AlertOear	27 = 2
LAYERX Agent Mankar		3	CRITICAL - RPTR Alarm	1 time	3D minutes	Critical	AlertHold	
Log Monitor		1	CRITICAL - RPTR Alarm	1 Line	au minutes	Concar	Aerona	×7 = ×
LX1 Call Monitor v2		5	DISREGARD - FailedNodes	1 time	1 minute	() Informational	DoNotAlert	×1 = Z
LXT SIP Call Errors v2		6	DISREGARD - UnableToRun	1 time	1 minute	() Informational	DoNotAlert	21 - 2
Nortel Call Monitor		1	INDETERMINATE - RPTR ALL	1 time	15 seconds	() Informational	DoNotAlert	21 = 2
PING Manitor		1				- monitore	DOMONON T	
Powerware SMMP-Alpres		11	ISG Alarm trap - INDETERM	L. 1 lime	1 minute	() Informational	DoNotAlart	A1 = 4
to training porty		1	156 Alarm trap - MAJOR	1 time	1 minute	() Major	DoNotAlert	1 = 1
TestAlaresvt		T	ISG Alarm trap - MAJOR	1 time	1 minute	D Major	DeNotAlart	A1 = Z
Aj ExperiMental		1	- interest in a state of the st	( how		C mater	Domarson L	
ALSTOYBARN : Aut IT - Alert Exe.		9				C	Splaying 1 - 11 of 11 events	«first prev next last»

## **Cloning a Policy**

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

To Clone a Policy:

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

Policies		Rules					
Name Fa	ilover	Name	Threshold	Window	Severity	Response Procedure	1
Cisco Call Monitor		CLEARED - RPTR Alarm	1 time	1 minute		AlentOear	17 - 2
LAFERX Agent Monitor	2	The second second second		Contract of	Critical		
Log Monitor		CRITICAL - RPTR Alarm	1 time	20 minutes	Critical	AlertHold	¥7 = Z
LX1 Call Monitor v2	5	DISREGARD - FailedNodes	1 sime	1 minute	Informational	DoNotAlert	<u> 21 = 2</u>
LX1 SIP Call Errors v2	<b>2</b>	DISREGARD - UnableToRun	1 time	1 minute	() Informational	DoNotAlert	21 = 2
Nortel Call Monitor	3	INDETERMINATE - RPTR Ala	1.000	15 seconds	() Informational	DoNotAlert	
PING Monitor	1	INDETERMINATE - 10/18 ALL.	. I sime	13 seconds	() imprimational	DONDOVER	×1 = Z
Rowerwave SHMP Algeres	<b>2</b> 11	ISG Alarm trap - INDETERMI.	. 1 time	1 minute	() Informational	DoNosAlert	P1 = 2
Lo training policy	1 2	15G Alarm trap - MAJOR	1 time	1 minute	() Major	DoNotAlert	21 = 2
Test Alarm V1	107	ISG Alarm trap - MAJOR	1 sime	1 minute	(D) Major	DoNotAlert	41 - 21
Aj ExperiMental	1 3	- conservation and any and out	1000	Chinada	C major	Domorout	×1 = ×
ALSTOYBARN : Austin - ert	Exa. 2 9					Displaying 1 - 11 of 11 events	« first prev next last

### **Export and Import a Policy**

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

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

See the:

Log Search Section in the Dashboard and Reporting Administration Guide.

Sys	tem log								\$
se Se	arch 🕶								e
*	lxt_timestamp_epoch (America/Chicago)	username 🔺	action 🔺	area 🔺	status 🔺	duration	A.,	details	-
7	03/09/22 9:24:49 am	admin	import	asset	SUMMARY	1	19	{"csvRows":1, "numInsert":0, "numUpdate":2, "numDelete":0}	
8	03/09/22 9:19:31 am	admin	import	asset	SUMMARY	1	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	1	14	{"csvRows":6, "numInsert":0, "numUpdate":6, "numDelete":0}	
10	03/09/22 9:13:30 am	admin	import	asset	SUMMARY	1	11	{"csvRows":6, "numInsert":1, "numUpdate":4, "numDelete":0}	
6	03/09/22 9:25:13 am	admin	import	asset	SUMMARY	4	43	{"csvRows":6, "numInsert":1, "numUpdate":5, "numDelete":0}	
3	03/09/22 10:03:12 am	admin	export	policy	SUMMARY		0	{"numExportPolicyGroups":1, "csvRows":4}	
2	03/09/22 10:05:50 am	admin	export	policy	SUMMARY		0	{"numExportPolicyGroups":3, "csvRows":28}	

To Export a Policy:

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

To Import a Policy:

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

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

### **Policy CSV Format**

The following columns are in an exported CSV file:

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

#### Note:

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

See: Response Procedure Configuration.

voss 🎇 🚺	
POLICY CONFIGURATION	Import Policies
Policies       Name     Failover       AA-E1-Layer1     Image: Constraint of the second sec	Select file to import Choose file No file chosen Critical
Cisco Cube DSPRM	Cancel Import
Cisco Cube VOICE_FILE_ACCT	4
Cisco Cube VOIPAAA	
Cisco Cube Call Treat No Signal	<b>7</b> 29
Cisco Cube CCM	24
	8
Cisco Cube DSMP	8 Filter All → Filter Sort Column Halt / E

# 4.1.2. Asset Configuration

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

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

See the:

Log Search Section in the Dashboard and Reporting Administration Guide.

## **Creating an Asset Group**

To create a new Asset Group:

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

Groups	Assets						
Group Name	IP Address	Asset Name	Description	Туре	Monitor Profile		
BB All groups							
CIRAL CO.							
in 1 and Arda Asset Group 1							
I Aspect (1)							
The Avenue T							
T a Cace CM							
- Data Network 15							
The ETISALAT T							
a Gerband							
GreatWest 74							
T a GROUP NAME							
E BELAYERX 5							
E Interest Lab 12							
BILKI SIP Phones 2							
i iii Nortel 8							
mill Optus							
> a Bit SLo training							
Talafonica 1							
🛄 📾 Telmax 🗇							
TELSTRA TCC-CP 1							
E NUCHAR 1							
WM Tech 1							
» m voss cucom 2							
🗌 🇰 Windows T							
🗍 🇰 Zain Bahrain 💿							
ill Zein Kuwait							
(mm)	Filter		Sort IP Address			No seconds a	esets + first prev mext last

## Adding an Asset to an Existing Group

To add a new Asset to a Group:

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

ASSET CONFIGURATION		Errors exist	Save
Groups	Assets		
Group Name	IP Address Asset Name Descriptio	n Type	Monitor Profile
All groups	10.1.1.1 AE_NAME DESCO	Unknown	No profiles set 🖌 🖌
13 MAJ 13	Properties Interfaces		
- Arda Asset Group 0			
Aspect 4	Enabled	Model	
Awaya 2	Maintenance Mode	Version	
Cisco CM	IP Address	MAC Address	
Data Network 15	Asset Name	Alias	
ETISALAT	Description	Manufacturer	
Genband 1	Host Name	Time Zone	итс
GreatWest 74		Customer	
GROUP NAME 1			
i LayerX S	Address	Site	
LayerX_Lab 12	External URL		
LX1 SIP Phones 2			
Nortel 5			
Optus 1	Filter Sort IP Addres		Displaying 1 - 2 of 2 assets + first prev next last
Group Name	Assets IP Address Asset Name Descriptio	а Туре	Monitor Profile
I Al groups	T 101.1.1 AL NAME DESCO	Unknown	No profiles set
THAT D			
- Arda Asset Group 0	Properties Interfaces		
Aspect 4	Name IP Address MAC Add	ness Vendor	Model Version
Maraya 2			
Cisco CM 4			
· Data Network 13	1		
ETISALAT 1			
GreatWest 74			
E GROUP,NAME			
W LayerX 1			
LayerX Lab 12			
I LAT SP Phones 2			
Nortel 5			
Dim Optus	and the second se		
	Filter Sort IP Address	•	Displaying 1 - 2 of 2 assets + first, prev next last

## **Deleting an Asset**

To delete an Asset:

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

ASSET CONFIGURATION				Errors exist	Save
Groups Group Name	Assets IP Address	Asset Name	Description	Туре	Monitor Profile
Data Network 15	10.13.37.119	Local System	Local Arbitrator Platform	LayerX Node	7 profiles set 🖌 🖌
	10.13.37.194	LOLAB03		LayerX Node	No profiles set 🕜 🖉
Genband T	1010-37.206	TempAlert	Temperature Monitor	Unknown	1 profile set
GreatWest 76	10.13.37.48	PeodP	PeoliP System	Unknown	t profile sot
GROUP NAME 1	10.99.99.99	LinkIPToAlertTest	LinkiPToAlertTest	Unknown	No profiles set
LayerX (30) 12     KX1 SIP Phones     Nortel S     Optus 1     SLo training 2     Telefonica 3     Telefonica 3     Telefonica 1     UCtriX 2     WM Tech 1	Fitter		Sort IP Address \$	Displaying	ç1-5 of5 assets ∉ñnst prev next læst+
WM Tech 1	Piner		Sort IP Address ¢	Uispiaying	g1-5 or 5 assets a nist prev next lasta

# **Deleting an Asset Group**

To delete an Asset Group:

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

ASSET CONFIGURATION			6	mors exist	Save
Groups Group Name	Assets IP Address	Asset Name	Description	Туре	Monitor Profile
P Data Network 15	10.1.1.1	test	test	Unknown	No profiles set 🛛 🖌 🗾
	10.199.161.11	is-prd/ms01a.gwl.com	VP DRS	Unknown	No profiles set 🖌 🖌
Genband 3	10.199.161.130	is acrmaina!	DRS Main recorder	Unknown	No profiles set 🖌 🖌
GreatWest 74	10.199.161.131	is-acreeca1	DRS Secondary recorder	Unknown	No profiles set. 🔺 🖌
LayerX 5	10.199.161.132	is-crsbrdigdra1	DRS CRS/Biridge	Unknown	No profiles set 🖌 🖌
LayerX_Lab 12	10.199.161.21	madr-ess-cm	Drs-ess	Unknown	No profiles set 🖌 🖌
LX1 SIP Phones 2	10.199.161.46	madr-sesmgr	DRS session Manager	Unknown	No profiles set 🔹 🗾
Die Optus	10.199.161.50	dr-aes-crm	CRM TSAPIS	Unknown	No profiles set 🖌 🖌
> SLo training 2	10.199.161.57	dr-aam3-msging	DRS VM app srvr	Unknown	No profiles set 🖌 🗾
Telefonica	10.199.161.58	is-assmalinat	DR Main AES	Unknown	No profiles set 🛛 🖌 🖌
THISTRATECCP T	Fiter	9	ort IP Address \$	Displaying	1 - 20 of 74 assets « first prev next las

### Assigning a Probe to an Asset

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

To assign a Probe to an Asset:

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

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

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

ASSET CONFIGURATION	1			Char	nges have been made	Save
Groups		Assets		Calanda	-	
Group Name		IP Address	Asset Name Nortel_CS1K_BM	Description Nortel CS 1000 BM	Type Server voice	Monitor Profile 1 profile set
# Data Network 15						
ETISALAT 1		192.168.1.3	Nortel_CS1K_DAL	Nortei CS 1000 Dallas	Server voice	1 profile set
GreatWest 74		192.168.1.3	Nortel_CS1K_SF	Nortel CS 1000 SF	Server voice	1 profile set 🥜 💋
GROUP, NAME 1		192.168.1.3	Nortel_CS1K_SU	Nortel CS 1000 SU	Server voice	1 profile see 🔺 🖌 🖉
all LayerX S		192.168.1.3	Nonel_CS1K_SW	Nortel CS 1000 SW	Server voice	stofiester A
LayerX Lab 12						
ELX1 Phones 2						
in Nortel 5		Fiter		Sort IP Address 0	Displaying 1 - 5	of 5 assets + first prev next last +
						Court STREET
MONITOR PROFILE * Nort Groups	el_CS1/	K_BM Templates/Profi	ller			Cancel Update
Probe Group		Name	Frequency	Credentials 1 & 2	2 Enabled	
> AA	(3)	PING Probe	\$ Minutes	None & None	22	×
						-
- Application sah probe	7				/	/
- Application sah probe	デー				/	
					/	
- Aspect alarm demo	Ť				/	
- Aspect alarm demo	т Т				/	

MONITOR PROFILE » North	el_CS1	K_BM				Cancel	Update
Groups		Templates/Profiles					
Probe Group		Name	Frequency	Credentials 1 & 2	Enabled		
= AA	3	Name PING Probe		Fruitiked Start Time			
Annilleption sch metho		Frequency		V Immediate?			
<ul> <li>Application ssh probe</li> </ul>	1	5 Minutes		Days			
Aspect alarm demo	T	Credential 1		Sun V Mon V Tue V Wed V Thu			
		None					
Aspect CallCenter Service Probes	3	Credential 2					
- Asset Probe Test	T	None	•				

#### Assigning a Customer to an Asset

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

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

ASSET CONFIGURATION				Changes have been mu	ide Save
Group Name	Assets IP Address As	set Name Descr	iption Type	Monitor Profile	
Arda Asset Group	Properties Interfa				v.
Aspect 4	Enabled		Model	Unknown	
a Avaya 2	Maintenance Mode		Version	Unknown	
Gisco CM	IP Address	192.168.1.3	MAC Address	Unknown	
> 🗌 🎟 Data Network 15	Asset Name	Nartel_CS1K_BM	Alias	Unknown	
ETISALAT 1	Description	Nortel CS 1000 BM	Manufacturer	Nortel	
Genband 1	Host Name	nortel_SW	Time Zone	UTC	
CreatWest 74 Crea	Type Address External URL	Server volco Billinge, Montana	: Customer Site	Anda Virtual Customer 1 Anda Virtual Customer 2 Anda Virtual Customer 3 LayerX Virtual Customer SiLo Custoemr 1	8
Nortel 3	Riter	Sort IP Ad	idress ‡	Displayir	ng 1 - 5 of 5 assets + first prev next last +

### Placing an Asset in Maintenance Mode

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

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

ASSET CONFIGURATION					Charges	have been made	Save
Groups Group Name	Assets IP Address Ad	set Name	Description	Туре	Ma	mitar Profile	
AJ 13     Arda Asset Group 0	Properties Interfa	tes	/				-
Aspect 4	Enabled		-	Model	Unknown		
Avaya 2	Maintenance Mode			Version	Unknown		
Cisco CM	IP Address	192.168.1.3		MAC Address	Unknown		
> Data Network 15	Asset Name	Nortel_CS1K_BM		Alias	Unknown		
ETISALAT T	Description	Nortel CS 1000 BM		Manufacturer	Nortel		
Genband 1	Host Name	nortel_SW		Time Zone	UTC		
GreatWest 74	Туре	Server voice	0	Customer		8	
GROUP_NAME 1	Address	Billings, Montana		Site		*	
a LayerX Lab 12	External URL						
IN LX1 SIP Phones 2							
IN Nortel 3	Fitter	So	rt IP Address			Displaying 1 - 5 of 5 asset	s « first prev next last »

## **Export and Import an Asset**

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

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

To Export an Asset:

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

To Import an Asset:

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

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

#### **Asset CSV Format**

The following columns are in an exported CSV file:

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

Note:

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

voss 🎇 🔥		Days remaining: 1	admin <del>-</del>
ASSET CONFIGURATION	Import Assets		Save
Groups	Select files to import		
Group Name	Choose file No file chosen	Туре	Monitor Profile
The 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			
NEXTWAVE 2			
PANDABANK 0	← Filter All ← Filter Sort column	IP Address 🗸 🕨	No records assets « first prev

# 4.1.3. Probe Configuration

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

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

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

Arbitrator Cisco PRI and SIP Probe Configuration

## **Creating a Probe Group**

To create a new Probe Group:

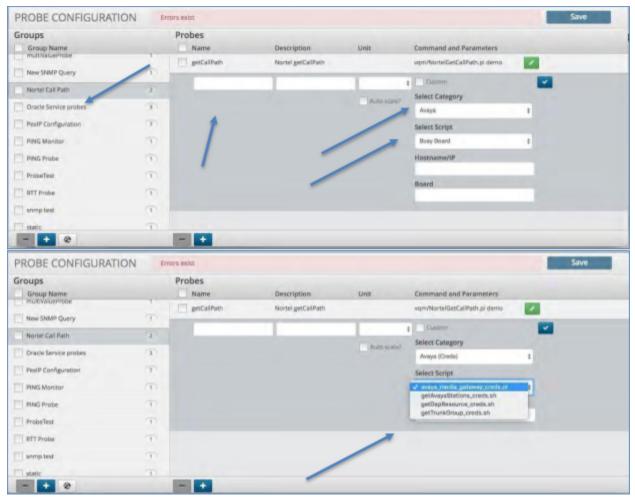
- 1. Click the Probe icon from the Menu bar.
- 2. Click the "Plus" icon within the Groups pane in the bottom left corner.
- 3. Enter the "Group" name and press Enter.
- 4. Click the "Save" icon in the upper right corner.

voss 🎇 🔥 🛕	8	1	ţţţ		٩	Ŀ	A	<b>±</b>	Ē	٥	Days remaining: 173	admin 🕶
PROBE CONFIGURATION	Cha	nges have	been ma	de								Save
Groups Group Name		Probes Nan			Des	cription		Unit		Co	mmand and Parameters	
Polycom VMWARE-CPU-MEM												
vmwarev3	D											
Voss CPT CUCM Perfmon AXL Counters												
Voss USA CUCM Perfmon AXL Counters				/								
Voss USA CUCXN Perfmon AXL Counters			/									
- + 0 ± ±			-	+								

## **Creating a Probe**

To create a new Probe:

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



## **Creating a Custom Probe**

To create a new Probe:

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

PROBE CONFIGURATION	En	rors 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 pl 4000 6000	2
Avaya VQM RTCP Demo	2	Pre Policy OB Pkts	Pre Policy OB Picts		genRandom pl 4000 6000	
Avaya VQM Statistics	8	Dit Rate	Bit Rate		genRandom pi 2100 2400	12
CCMM 6	7	Drop Packets	Orop Packets	×B.	genRandom.pl 200 350	
CCMS 6	41	Urop Packets	Urop Packets	×0		-
CCT 6	7			_	t Custom	
CDR Ndx Demo	3		-	ALCO	40	
Cisco ASA SNMP Table Probe	1					
Cisco ASA Stats	2					`
Cisco CBQos	5			-		
Cisco CUCM Device Location	-					
Cisco CUCM LX-RTMT	6					
Cisco CUCM PerfMon Counters						
Cisco CUCM Phone Inventory - 10.13.37	1					
Cisco CUCM Phone Inventory - 10.13.37	1					
Cisco Finesse	2	-				
- + 0		-				

## **Deleting a Probe Group**

To delete a Probe Group:

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

		۲		†å†		•	-	â	*	•	٠		👤 admin <del>-</del>
PROBE CONFIGURATION	Err	ors exist											Save
Groups Group Name		Probes			Descriptio	•	Unit		Comm	and and Par	ameters		
Awaya Utilization Demo	1	Pre Pol	icy IB Plets		Pre Policy I	Pies			genRan	dom.pl 4000 6	6000		
Awaya VQM RTCP Demo	2	T Pre Pol	ity OB Pies		Pre Polky C	e Pies			perdan	dom pi 4000 t	000	1	
Awaya VQM Statistics	(6)	Eit Rate			Bit Rate				perflan	dom pl 2100 ;	400	1	
CCMM 6	2								-				
COMS 6	41	Drop P	acate		Orop Packet		k8		Bergau	dom.pl 200.35	90	1	
CCT 6	7											1	
CDR Ndx Demo	1												
Cisco ASA CIAMP Table Probe	P												
Csco ASA Stats	2												
Cisco CBQos	3												
Cisco COCM Device Location	P												
Cisco CUCM LX-RTMT	Ŧ												

# **Deleting a Probe**

To delete a Probe:

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

	A	۲	1	†††		٩	2	A	*	9	٠		👤 admin 🗸
PROBE CONFIGURATION	N En	fors exist											Save
Groups Group Name		Probes			Descriptio	n	Unit		Comma	nd and Par	ameters		
Awaya Utilization Demo	T	Pre Po	nicy IB Plets		Pre Policy I	Piets			genRand	lam.pl 4000	6000	1	
Awaya VQM RTCP Demo	1	Pre Po	liky OB Pies		Pre Policy C	8 Piets			geniland	om.pl 4000	1000	1	
Awaya VQM Statistics	6	E Bit Ra			Dit Rate				-	om.pl 2100.	1411	1	
CCMM 6	3	-										_	
CCMS 6	41	2 Day	Packets		Orop Packet	5	10		ten Auno	lam. pl 200 3	50		
CCT6	1												
CDR Ndx Demo	1												
Cisco ASA SNMP Table Probe	T												
Cisco ASA Stats	2												
Cisco CBQos	18		/										
Cisco CUCM Device Location	1	-											
	6												

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

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

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

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

See the:

Log Search Section in the Dashboard and Reporting Administration Guide.

To Export a Profile:

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

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

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

To Import a Profile:

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

#### **Profile CSV Format**

The following columns are in an exported CSV file:

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

#### Note:

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

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
$(\underline{\mathbb{X}})$	
-+ @ ± ±	

## Assignment of a probe to an asset

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

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

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			
▶ Cisco Expressway	3	Test Probe	1 Minute	None & loc		1			
CISCO Expressway		PING Monitor	1 Minute	ray & loc	M	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	Templates/Profiles							
Probe Group		Name	Frequency	Credentials 1 & 2	Enabled					
Cisco CUCM Version	1	Local System Stats	1 Minute	None & touy		1				
Cisco Expressway	3 <b>L</b>	Test Probe	1 Minute	None & loc		1				
CISCO Expressway	3	PING Monitor	1 Minute	ray & loc						
Cisco Telepresence API - Call Details	1	Cisco CUCM Version	1 Minute	ray & loc		1				

# 4.1.4. Controls

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

## **Creating a Control**

To create a new Control:

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

ONTROLS	Errors exist Pr	obes		Save
	Name	Command and Parameters	Protection	
	PEAK-AspectDB	aspect/bidwAlertInsert.pl	off 🛛	×
	PushToZenass	zenoss/zenossNew.php '1.1.1.1' 'abc123' 'abc123' '0'	off	
	Reboot machine	generic_ssh.exp %s 'reboot' '22'	off 🛛	
	ReporterPush	ReporterPush 10.13.37.128:65515 true	off	-
	SendToEM7	sciencelogic/apiAlertToEm7_creds.pl *10.1.1.1*	off	
	show running	cisco_pix_cli.exp '76.198.119.129' show running'	off	
	Test Fiber Link	avaya/command.pl %s testfiber %s	off	2
	Trace Route	avaya/command.pl %s tracent %s %s	On	-
	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.php193.35.222.39 smartpoint@cambridgecom	isultants Off	2
	VossQuery	voss/vos8.sh	Off	2
		Custom		-
		Select Category	_	
~		Aspect ¢		
		Select Script	_	
		Aspect BIDW Event Queue Insert #		

## **Deleting a Control**

To delete a Control:

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

Name	Command and Parameters	Protection	
AlertClear	alerts/ackAlert.php	Off	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.sh	Off	
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

# 4.1.5. Response Procedure Configuration

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

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

## **Creating a Response Procedure**

To create a response procedure:

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

<u> </u>	⑧ 🖌 销 🗐 🥄 🧏 🔒 📥 👄 🌣	1 adr
ESPONSE PROCEDURE C	NFIGURATION	Save
esponse Procedures	Response Procedure Details	
CEMS Stat Test	Alert Disable on Fallover	
Default IRP	Methods	
DoNotAiert	From: arbitratordiayentech.com To: supportiliayentech.com Smtp Server	email
Small wstrobel	Control Reboot machine # Driay Disconds	1
Erral,Arda	Credential 1 admin 1 Confirm Timeout 30 seconds	
Deceletion Example		Controls
Fallover ACTIVE	Control LinkPTpAlen # Credental 1 admn #	
Fallover STANDBY	Credental 2 None # Confirm Timeout 30 seconds	1
Fest Bank 34x7	Destination: 10.10.2.10 As Swert?	Forward
Just Alert		
LeyerX Support		
UniCalPathToAlert		
UNCHTORES	+ Email + Control + Forwarder	
UniPlaten	Do Not Run Windows	
LiniaPToAlert - Do Not Post Alert	Start Priday 0 12am 0 00 0	
LinkPToAlert - Post Alert	End Sunday 2 12am 2 00 2	
LinkProbeToAlert		
Local Alert ONLY		
PANI OS Decrypt		
PEAKtoAspect08		
Rush to Reporter		
Rebost Machine		
SendfoEM7		
Svit burgle		
Tracy, ResProdecure		
USAN Response		
Test		
- 0		

### Assigning an Alert to a Response Procedure

To assign the Alert function to a response procedure:

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

S 👔 🔺 🥼	🔊 🦨 🕷	1	2 (	a 🛓	• •	1 admin -
RESPONSE PROCEDURE CON	FIGURATION					Save
Response Procedures	Response Proce	dure Details				
CEMS Sue Text	Alert	Daabi	e on Fallover			
C Default IIIF	Methods	farmer an	Tr supportil	avendech.com	Smip Server	
Dukesker	Current	Rebool machine				
Cital estate	Course 1	admin		Delay	0 seconds	
Dral,Ada	Credential 2	None		2 Confirm Tim	eout 30 seconds	
Disalation Example	Cantral	Link975Aiet				
Palover ACTIVE	Credential 1	admin		B Delay	0 seconds eout 30 seconds	
Falser STANDBY	Credential 2	None		2	eour 30 seconds	
First Bark 24x7	Destructors 1	0.10.2.10	As	trent 🖬 🔽		
Dat Alert						
Layert Support						
UnicalParticiper						
UNCETARE	- + Im	ell + Control	+ Forwards	er i		
Unit7ToAlant	Do Not Run W	rutinent				
LinkePflaAlert - Dis Nat Pest Alert	Start Frid		8 00 B		_	
LindPToAlen - Post Alen	End Sur	_	8 00 8			
C LisiProteToAlet						
Local Alert ONLY						
TAN 05 Decrypt						
PEAKtoAspect08						
Auth to Reporter						
Rebost Machine						
SendfotM7						
Suit burigie						
Trag, Risholaure						
USAN Response						
Test.						

#### **Deleting a Response Procedure**

To delete a Response Procedure:

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

Response Procedures Name	Response Procedure Details				
Avaya Fix MED-GTWY	Alert	Disable on Failover			
CCMS-Stat-Test	Methods				
Default IRP	C Email	From: arbitrator@layerstech.com	To: tier1@company.com	×.	
DoNotAlert					
Email wetrobel					
Email Anna	- + Ema	all + Control + Forwarder			
Escalation Example	Do Not Run Wi	ndows			
Failover ACTIVE					
Failover STANDBY					
First Bank 24x7					
Just Alert					
LayerX Support	-				
LinkEmPathTaAlert					

# 4.1.6. How to Enable ServiceNow Intergration

Name	Command and Parameters	Protection
LINKIPTOAlert	LInkIPToAlert	off 🗾 🖊
ReporterPush Reading	ReporterPush 172.30.15.121:65515 true	off 🗾 🗾
ReporterPush-GC	ReporterPush 172.25.87.6:65515 true	off 🗾 🚺
VpnSyslog	vpnSyslogAlert.sh	off 🗾 🗾
	Custom	
	Select Category	
	ServiceNow 🗸	
	Select Script	
	PushToServiceNow	
	Service Now IP Address / Hostname	
	Service Now Username	
	Service Now Password	

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

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

# 4.1.7. ServiceNow One Way Incident Integration

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

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

#### **ServiceNow Requirements**

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

## Arbitrator Correlation Configuration

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

## Screenshots From ServiceNow

Service Million Service Million	anagement			System Administrator 🝷	< 다 @ 🕸
Filter navigator	< Incident INC0010023			Follow - Update Rese	olve Delete 🛧 🗸
■ ★ C	Configuration item	Q	Assignment group	Q	
My Assets			Assigned to	Q	
My Notification Preferences	*  Short description	LXTALERT: ARB_REFERENCEID=20000-01009001-00-0	1-7134-14 ARB_POLICY_MODULE=MultiTest ARB_C	ORRELATION_RULE=Some Rule	8
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	Preview Attach
Incident	Firewall Rule Change	Cisco Firewall Appliance			Preview 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		
Assigned to me	About Windows 10	the microphone to talk with her instead, kulle	ne web with microsoft cage microsoft cage is the hi	st browser	Preview Attach
Open R	Notes Related Records	Closure Information			
K Open - Unassigned	Watch list	<b>a e</b>	Work notes list	2	
5 Resolved					
<sup>je</sup> all	Additional comments (Customer visible)				
er Overview				Work notes Post	
Critical Incidents Map					
Problem	Activity	😨 System Administrator		2016-12-13 12:52:14	$\overline{\mathbf{Y}}$
Change		LXTALERT: ARB_REFERENCEID=20000-01009001-00-01 ARB_MESSAGE=Some Rule : Multitest (2)	7134-14 ARB_POLICY_MODULE=MultiTest ARB_CORREI	.ATION_RULE=Some Rule	
Configuration					
Password Reset		System Administrator		2016-12-13 12:52:14	
Service Catalog		Incident state New Opened by System Administrator			
Item Designer		Priority 1 - Critical			
	inagement			👰 System Administrator 🝷	୧ ୮ ୩ ଊ
Filter navigator	Incidents New	Go to Number V Search	]	√ ◀◀ ◀ 1	to 20 of 75 🕨 🕨
■ ★ ①	⊘ ■ Numl	Der ▼	■ Caller ■ Priority ■ State	■ Category ■ Assignment group	■ Assigned to     ■
My Assets	(i) INC00200	01 2016-08-10 09:14:29 test	System Administrator 3 - Moderate New	Inquiry / Help	20 H
My Notification Preferences		LXTALERT: ARB_REFERENCEID=20000-			
Guided Setup	(i) <u>INC00100</u>	2016-12-12 01009001-00-01-7124-14	• 1 - Critical New	Software	20 15
Service Desk		ARB_CORRELATION_RULE=Si Rule			
Incident		LXTALERT: ARB_REFERENCEID=20000-			
Create New	(i) <u>INC00100</u>	2016-12-12 01009001-00-01-7124-16	est • 2 - High New	Software	20 12
Assigned to me		ARB_CORRELATION_RULE=So Rule Major	ome		
RE Open		LXTALERT: ARB_REFERENCEID=20000-			
V Open - Unassigned	(i) <u>INC00100</u>	2016-12-13 01009001-00-01-7134-19 12:52:08 ARB_POLICY_MODULE=Multi		Software	20 12
5 Resolved		ARB_CORRELATION_RULE=Se Rule Info	me		
ge All		LXTALERT: ARB_REFERENCEID=20000-			
er Overview	(i) <u>INC00100</u>	12:52:04 ARB_POLICY_MODULE=Multi		Software	20 12
57 Critical Incidents Map		ARB_CORRELATION_RULE=Si Rule Minor	me		
		I XTALERT-			

# 4.1.8. Credential Configuration

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

## **Creating a Credential**

To create a Credential:

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

. 🔺	🛛 🦨 ili	🗏 ° 🧏	ê 🚣 🖻	🔅 👤 admin -
CREDENTIAL CONFIGURATI	ON Errors exist	/		Save
Name	Username	Password	Confirm	-
LXTREADONLY				2
SILo Test Cred				× 1
snmp community public	*******			1
SNMP RO String		*******	*******	<b>2</b>
Tandburg	*******	*******	********	× .
UCAXLAPI				1
VOSS API	*******	*******	********	1
Windows Agent probe		*******	********	× .
				× .

## **Deleting a Credential**

To delete a Credential:

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

Name		Username	Password	Confirm	
Labrimic	eas				~
LxtAutoGer	1489019854046	********	********	********	1
LXTREADO	NLY	********	********		1
SiLo Test C	red	********	********		1
snmp com	munity public	********	********		1
SNMP RO S	tring	********	********		1
Tandburg		*******	********	*******	
UCAXLAPI		*******			1
VOSS API		********	********	********	1
Windows A	gent probe	********	********	********	1

# 4.1.9. Customer Configuration

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

(See: Asset Configuration, Access Control Configuration).

#### **Creating a Customer**

To create a Customer:

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

CUSTOMER CONFIG	URATION		Save
Customers		Sites	
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		

## **Creating a Customer Site**

To create a site for a Customer:

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

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

## **Deleting a Customer**

To delete a Customer:

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

CUSTOMER CONFIGURATION			Save
Customers		Sites	
Arda Virtual customer 1	1	Mountain View	
Arda Virtual Customer 2	2	Los Angeles	
Arda Virtual Customer 3	2		
LayerX Virtual Customer	1		
SiLo Custoemr 1	1		
		-	

#### **Deleting a Customer Site**

To delete a site for a Customer:

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

CUSTOMER CONFIGURATION			Save
Customers		Sites	
Name		Name	
Arda Virtual Customer	2	Mountain View	
Arda Virtual Orstomer 2	2	Los Angeles	
Arda Virtual Customer 3	2		
LayerX Virtual Customer	1		
SiLo Custoemr 1	1	/	
-			

# 4.1.10. Access Control

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

### **Permission Groups**

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

## **Creating a Permission Group**

To create a Permission Group:

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

Group Name	Realm Context	Timeout		
Science Logic	(local)			1
SuperUser	(local)			1
Admin	(local)			1
SiLo Test	(local)			1
Guesz	(local)			1
Typical	(local)	22		1
Monitor	(local)	2		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	An: VIEW - Asset Explorer	alytiX :: Correlate VIEW - Alarm Analyzer		
Permissions Users VIEW - Main Application VIEW - Policy Monitor	Anie VIEW - Asset Explorer VIEW - Asset Map Explorer ACTION - Delete Paths	alytiX :: Correlate VIEW - Alarm Analyzer VIEW - Cail Details		
Permissions Users VIEW - Main Application VIEW - Policy Monitor	Anie 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	Ana VIEW - Asset Explorer VIEW - Asset Map Explorer ACTION - Delete Paths Ana	alytiX :: Correlate VIEW - Alarm Analyzer VIEW - Call Details ACTION - Disposition Alerts ayltiX :: Configure	VIEW - Call Path Monitor	

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

To Assign a User to a Permission Group:

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

Group Name	Realm Context	Timeout	
Science Logic	(local)		1
SuperUser	(local)		1
Admin	(local)		1
SiLo Test	(local)		1
Guest	(local)		1
Typical	(local)	12	1
Manitor	(local)	12	1
Test	(local)	- 1	1
Permissions Users	Users in Group	All Users	
testing		Administrator	
		Alain jansen	
1		Andrew Freisch	
		Arda Savran	
	Dra	Guest Account	
		layerx	
		testing2	
		View Only	
		Vodafone	

#### Users

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

#### **Creating a New User**

To create a new User:

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

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

Full Name Administrator Nain Jansen Andrew Frosch Arda Savran Guest Account	Username admin ajansen afrosch esavran	Password	Confirm	Email afrosch@layenstech.com ajansen@layenstech.com	Super-User	Force Password Change	
Alain Jansen Andrew Frosch Arda Savran	ajansen afrosch						
Andrew Frosch	afrosch			ajansen@layerxtech.com	23		
Arda Savran		********					1
	asavran			afrosch@layerxtech.com			-
Guest Account		********	********	asavran@layerxtech.com	23		1
	guest	********	********	support@layerxtech.com			
layers	layerx	*******	********	support@layerxtech.com	12		1
testing	testing	*******	********	support@layerxtech.com	53		
testing2	testing2	*******		support@layerxtech.com	22		1
View Only	viewonly	*******		view@layerxtech.com			-
Vodafone	voda	*******	********	support@layerxtech.com			
wstrobel	wstrobel	********	********	wstrobel@layerxtech.com	53		1
Customer		± Disa	ble multi tenancy				/

#### **Deleting a User**

To delete a User:

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

#### Nodes

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

#### Creating a Node

To create a Node:

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

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

#### **Deleting a Node**

To delete a Node:

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

#### Realms

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

#### **Creating a Realm**

To create a Realm:

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

Name	
Deployment	× 1
LayerxDev	2
1.000	
/	
-	-
	1
Devices in Realm	All Devices
	devarb
Drag /	demoarb
/	ePius
	trab

#### **Deleting a Realm**

To delete a Realm:

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

#### **Protected Subnets**

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

#### **Creating a Protected Subnet**

To create a Protected Subnet:

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

#### **Deleting a Protected Subnet**

To delete a Protected Subnet:

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

Name	IP Address	Mask	
internal_172_16	172.15.0.0	255.255.0.0	×
ANA1918_192_168	192.168.0.0	255.255.0.0	2
Google (subnet 5)	66.102.0.0	255.255.240.0	2
Google (subset 4)	72.14.192.0	255.255.192.0	
internal_1	192.168.103.0	255.255.255.0	
Internal_114	192.168.114.0	255.255.255.0	
internal_103	192.168.103.0	255.255.255.0	
Google (subset 1)	64,233,160.0	255.255.224.0	
Internal_141	192.168.141.0	255.255.255.0	2
Google (subset 2)	209.185.108.129	255.255.255.128	2
IANA_10	10.0.0.0	255.0.0.0	2
Google (subset 3)	64.68.88.0	255.255.248.0	
LOOPBACK	127.0.0.0	255.0.0.0	2
ANA1918_172_16	172.16.0.0	255.240.0.0	
Internal_135	192.168.135.0	255.255.255.0	× .
68.91.38.98	68.91.38.98	255 255 255 255	22
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	

#### **Password Policy**

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

#### **Creating a Password Policy**

To create a Password Policy:

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

Minimum Length	7
Minimum Uppercase	1 A-Z
Minimum Lowercase	1 🔷 a-z
Minimum Numeric	1 0-9
Minimum Special	1 0#\$%^&*()[]
Password Lifespan	0 days
Maximum Login Attempts	20
	Save

#### SAML

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

#### Creating single sign-on via SAML

To create single sign-on via SAML:

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

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

Disable Multi Tenancy AML Signature Algorithm		
AML Signature Algorithm	<u> </u>	
	sha1	•
Attribute Mappings		
mail (Optional):		
Isername (Optional):		
irst or Display Name (Optional):		
ast Name (Optional):		
dentity Provider Metadata XML		
Required		
laste your metadata XML here		
ervice Provider Information rovide this information to your Ide	ntity Provider	
		om/sami2/module.php/saml/sp/metadata.php/default-sp
rovide this information to your Ide	http://demoarb.layendech.com	om/sami2/module.php/sami/sp/metadata.php/default-sp om/sami2/module.php/sami/sp/sami2-acs.php/default-sp
rovide this information to your Ide udience URI (SP Entity ID):	http://demoarb.layerxtech.com http://demoarb.layerxtech.com	

Disable Multi Tenancy	
AML Signature Algorithm	sha1 +
Attribute Mappings	
imail (Optional):	
lsername (Optional);	
irst or Display Name (Optional)	
ast Name (Optional):	SAML Metadata
dentity Provider Metadata XM	xml version=*1.0*?
Required	cmd:EntityDescriptor xmins:md="um:oasis:names:tc:SAML:2.0:metadata" xmins:ds="http://www.w3.org/2000/09/xmldsig#"
laste your metadata XML here	<md:spssodescriptor protocolsupportenumeration="um:casis:names:tc:SAML1.1:protocol&lt;br&gt;um:casis:names:tc:SAML2.0:protocol"> <md:keydescriptor use="signing"> <ds:keyinfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#"> <ds:x509data> <ds:x509certificate>MIID52CCAs+gAwIBAgLJAly0+0SPIFX0MA0GCSqGSlb3DQEBCwUAMIGJMQ9wl QYDV20QEwx/U22E0MAwGA1UECAwFVGV4YXMxDzANBgNVBAcMBkhydmlu2zEPMA0GA1UECgw0 QF5ZXJ4MQ8wDQYDVQQLDAZsYXIcngxEDA0BgNVBAMB2RidnBhcmitxJTAjBgkqhkiG9w0BCQEW nN1cHBvcnRAbGF5ZXJ4dQijac5jp20wHhcMNTgwMTE3MjkMx2Q3WhcMlgwmTE3MjkMzC3WyCBE ELMAkGA1UEBMCVMkDjAMBgNVBagMPRIeGF2M08wDQTVDQQHDAZ.JcnZpbmcxD2ANBgNV AoMBmxheWvyeDEPMA0GA1UECwwGbGF5ZXJ4MRAwDgYDVQQDDAdkZX2wYXJIMSUJwhvYJKoZI vcNAQkBFh2zdKBw53J0QGxheWVyeHRY2gu292MiIBiJANBgkqhkG9w0B4QGFA0CA6A8MiBCq5 DPBIMfikdBiJIbiK4V3L0TCoaCq5u0fJ09YLSeVAMsm0aFFX1dTAb3Ls9VqMceh7PsvMh9CqCImJ- 3J2BvAGS78OC68UUhD4d8UH45VWsJ+x1wECeYsRQN16c7Ai56O6YP8BeVU000pgdmk8rX0C6XWI HvYDVR0jBBgwFoAUUrDDaBSaubH6fUtzgbEVEm8v8tbwDAYDVDJ7DLSspfd1DbVmFJRCla7LgkGdq/+ hB0KVtjOpVG225w2T5xlwwbdwIDAQA8b1AwTjAdBgNVHQ4EFgQUUVDB8BauHi6fUtzgbEVEm8v8tb GsFAACCAQEAyk084TvcTg2zuoNncX2019T6v7IIt2O1280UBydBsWbNmP9vXP68JAgdzImiaTLHDu Izt×K65G25G5NAUKKdnTep4yngtcKHJUbXhzWVbDI/QJZFk+D7yDLSspfd1DbVmFJRCla7LgkGdq/+ hB0KVtjOpVG225w2T5xlwwbdwIDAQA8b1AwTjAdBgNVHQ4EFgQUUVDB8BgkqhkG9w0B4 GsFAACCAQEAyk084TvcTg2zuoNncX2019T6v7IIt2O1280UBydBsWbNmP9vXP68JAgdzImiaTLHDu Izt×K55750DC6BT2JuN8Jz(QSUr1MbJz)gQSUr1M3878Z+EltKLULk1zGLWs9HNttp2PFbK866KBsJum6GC Gyf9wG2EnmjwHYQGW==/ds:X509Certificate&gt; <dtkc55750c62fitzjun8jz(qsur1mbjz)z60cbfitydbyd81w0bygvb1fyg8++t lt06l2fec<br="" qgjluocqr="">Cgf9wG2EnmjwHYQGW==/ds:X509Certificate&gt; <dtkc55750dc84ewdapa< td=""></dtkc55750dc84ewdapa<></dtkc55750c62fitzjun8jz(qsur1mbjz)z60cbfitydbyd81w0bygvb1fyg8++t></ds:x509certificate></ds:x509data></ds:keyinfo></md:keydescriptor></md:spssodescriptor>

nable SAML		
isable Multi Tenancy		
AML Signature Algorithm	sha1 +	
ttribute Mappings		
mail (Optional):		
sername (Optional):		
irst or Display Name (Optional		
ast Name (Optional):	SAML Certificate	×
ientity Provider Metadata XM	BEGIN CERTIFICATE	
Required	MIID5zCCAs+gAwiBAgIJAly0+0SPIFX0MA0GCSqGSlb3DQEBCwU	
oste your metadata XML here	VQQGEwJVUzEOMAwGA1UECAwFVGV4YXMxDzANBgNVBAcMBk CgwGbGF5ZXJ4MQ8wDQYDVQQLDAZsYXIcngxEDAOBgNVBAM	MB2RidnBhcmbuTAj
	BgkqhkiG9w0BCQEWFnN1cHBvcnRAbGF5ZXJ4dGVjaC5jb20wHk MzQ3WhcNMjgwMTE3MjkMzQ3WjCBITELMAkGA1UEBhMCVVMx	
	eGFzMQ8wDQYDVQQHDAZJcnZpbmcxDzANBgNVBAoMBmxheW bGF5zXJ4MRAwDgYDVQQDDAdkZXZwYXJIMSUwIwYJKoZIhvcNA	
	QGxheWVyeHRIY2guY29tMIIBIJANBgkqhkiG9w0BAQEFAAOCAQ8/ 4ZgbuCZEgq3E/RrHvoMyyjhYtcsGiTvqvuKmbkmD9eP75vBS4tQy1	AMIIBCgKCAQEA
	GrjGqsjrpk55DPBIMf6kBUIMIUDK4V3L0TCoaCq5u0rjD8YLSeVAMs dTAb3Lc9VgMceh7PsvMn9CqCImJ+x3J2BvAGS78OC6BUUhD4d8	m0aNF/X1
	ECeYsRGN16c7Ai56O6Yr9Bel/U000pq6mk6xYXiC6XWNvLTKt8G5	ZeG5NAUtKKdn
	Tep4yhgtckRJUbXh2wVbD/rOJZFk+D7yDLSspfc41DbVmFJRCla7L KVtjOpVQ5Z6w2T5xlwwbdwIDAQABo1AwTjAdBgNVHQ4EFgQUUv	fDaBSaubH6fUtz
	gbEVEm8vBttwHwYDVR0jBBgwFoAUUvtDaBSaubH6fUtzgbEVEm8 BAUwAwEB/zANBgkqhkiG9w0BAQsFAAOCAQEAyk094TvcTgZxuo	NhcX2019T6v171
	RzOt280Uh8ydBSwbNmP9vXP68IA9dzImI4TUHfDwJqElz+M/4HKzt NWZIXnodxFzuYATrdsVkEZn+BXT+vD3w9fPNmxpPPFbK8e5X/8eJu	
	yVS7750VDQPBT2JuIV8JlzI)QSUrI1MDIr3R9Z+EltiKUrJIt4CLVsn9h4 br315XKoJeDISq7Vy9WEYXP00IHm6nkEvUs95jyLxsXcjw3NTbt2Qe	i0tzDYo
	GValEWIgIFyg8++t/qGJluoCQn/LT06LzFek2rCg/19wGzEnmjnwHYp/ END CERTIFICATE	
		- 0
ervice Provider Information		
rovide this information to your I	dentity Provider	
udlence URI (SP Entity ID);	http://demoarb.layanstech.com/samt2/module.php/samt/sp/metad	lata.php/default-sp
ingle Login URLS	http://demoarb.layendech.com/sami2/mbdule.php/sami/sp/sami2	-acs.php/default-sp
ingle Logout URL:	http://demoarb.layen/tech.com/sami2/module.php/sami/sp/sami2	-logout.php/default-sp
	View Details Download	
Netadata:	Yiew Details 1 Download	

# 4.1.11. Import & Export

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

#### Exporting

To export configuration items:

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

IMPORT & EXPORT Export	Import	
Configuration Items	Export	
Arbitrator Nodes 4	-	
Asset Entries 2030		
Asset Groups 25		
Eustomers 5		
> Controls 36		
Permission Groups 7		
► ■ Policy Modules 116		
Probe Groups 80		
► m Protected Subnets 20		
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	

#### 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.

T Export Import	The second second	-	
Load a configuration package:	Choose File No file chosen	C Upload	
			No file chosen
			No file chosen
		Ø Import	

# 4.1.12. Archive Management

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

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

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

API Config	Archive	Blue Jeans Config	Cisco SDL	Collect
Creation				
DEM Config				
Webex Config				
Zoom Config				

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

#### Webex API Configuration Steps

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

voss 💭 🔒	🛞 🖌 🕅 🗐 🥄 🛓 🔒	📩 宣 🌣 Days remaining: Unlimited ad
ARCHIVE MANAGEMENT	Configuration Management Log Management	
API Config Archive Blue Je	eans Config Cisco SDL Collect Import LDAP Pro	obe SNMP Syslog Tunnel
Creation DEM Config Webex Config Zoom Config	Changes have been made to this configuration Item Webex Config Allows the enable and configuration of Webex monitoring. Create Access Token Create Access Token	Command: Webex Config: Create Access Token Status: Finished Output: succzss
	This step is required to allow the creation of an access token.  Enabled enabled Capture Webex's statistics using the Access Token provided from https://marketplace.webex.us/ Recommendation: Manually overwrite the ExpirationTime to a much greater time.	Close View Output
	CUSTOMER ABC Telecom Name of Customer.	
	AccessToken ["access_token":"ZjIyZjAyYmEtYTYyNS00YWZiLWizOGEt AccessToken to be used for requests.	

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

#### Archive

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

#### Setup

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

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

Vertifie       Celled       UAV       SNMP       System    Serve         Serve    Arbitrator Backup    Casco Files    Casco SQL    Paragia Files Remote Scorage    The system does a backup daily, for the most part, there is nothing for the user activitied case and configurations that exists on the system are activited configurations that exists on the system are activited case and configurations that exists on the system are activited configurations that exists on the system are activited scorefigurations that exists on the system are activited configurations that exists on the system are activited scorefigurations that exists on the system are activited score removing the NIS mount will NOT score the system set option to mount a NIS drive to the system. All activited files will then get activited to the NIS mounted drive. Nece: removing the NIS mount will NOT score the system will use the system will use the system file score file to score and to score the system will use the system of the source of the subscurate of the subscurate of the subscurate of the subscurate of the subupace of the subscurate of the subscurate of t	
Serie       Charges have been made to this configuration item         Arbitrator Backup       Disco Files         Osco SQL       Files         Presign Files       Disconfigure, 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 cache found on the individual Archive folies you page. The user also achive do to the NFS mount will NDT together to the system. All archived files will then get archived to the NFS mount and to the NFS mount will NDT together to the system. All archived files will then get archived to the NFS mount and the individual. Archive group pages. The user also the together to the system. All archived files will then get archived to the NFS mount and NFS drive to the system. All archived files will then get archived to the NFS mount and the to the NFS mount will NDT together to the system. All archived files will then get archived to the NFS mount and the to the system. All archived files will then get archived to the NFS mount and NFS drive to the system. All archived files will then get archived to the NFS mount and the Stange. Only NFS V3 mounts are current together to the system. All archived files will then get archived to the NFS mount and NFS drive to the system. All archived files will then get archived to the NFS mount and the system will use its disflaut archive foccion for of together.	
Arbitrator Backup         Cisco Files         Cisco SQL         Pexip Files         Remote Scorage         State and configurations that exists on the system are archived files locally on the box. There is a separate page for each Archive group. Nore dealed information about each Archive group can be found on the individual Archive group pages. The user also has the option to mount a NFS drive to the system. All archived files will then get archived to the NFS mounted drive. Note: removing the NFS mounts will NOT copy the NFS contents back to local storage. Only NFS v3 mounts will NOT copy the NFS contents back to local storage. Only NFS v3 mounts will NOT copy the NFS contents back to local storage. Only NFS v3 mounts will NOT copy the NFS contents back to local storage. Only NFS v3 mounts will NOT copy the NFS contents back to local storage. Only NFS v3 mounts will NOT copy the NFS contents back to local storage. Only NFS v3 mounts will NOT copy the NFS contents back to local storage. Only NFS v3 mounts are currently copy the NFS contents back to local storage. Only NFS v3 mounts are currently copy the NFS contents back to local storage. Only NFS v3 mounts are currently copy the NFS contents back to local storage. Only NFS v3 mounts are currently copy the NFS contents back to local storage. Only NFS v3 mounts are currently copy the NFS contents back to local storage. Only NFS v3 mounts are currently copy the NFS contents back to local storage. Only NFS v3 mounts are currently copy the NFS contents back to local storage. Only NFS v3 mounts are currently copy the NFS contents back to local storage. Only NFS v3 mounts are currently copy the NFS contents back to local storage. Only NFS v3 mounts are currently copy the NFS contents back to local storage. Only NFS v3 mounts are currently copy the NFS contents back to local storage. Only NFS v3 mounts arecur	
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 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 and easi be found on the individual Archive group pages. The user also has the option to mount a NFS drive to the system. All archived files will then get archived to the NFS mount will NDT copy the NFS contents back to local storage. Only NFS v3 mounts will NDT copy the NFS contents back to local storage. Only NFS v3 mounts are currently copt the NFS contents back to local storage. Only NFS v3 mounts are currently copt the NFS contents back to local storage. Only NFS v3 mounts are currently copt the NFS contents back to local storage. Only NFS v3 mounts are currently copt the NFS contents back to local storage. Only NFS v3 mounts are currently copt the NFS contents back to local storage. Only NFS v3 mounts are currently copt the NFS contents back to local storage. Only NFS v3 mounts are currently copt the NFS contents back to local storage. Only NFS v3 mounts are currently copt the NFS contents back to local storage. Only NFS v3 mounts are currently copt the NFS contents back to local storage. Only NFS v3 mounts are currently copt the NFS contents back to local storage. Only NFS v3 mounts are currently copt the NFS contents back to local storage. Only NFS v3 mounts are currently copt the NFS contents back to local storage. Only NFS v3 mounts are currently copt the NFS mount set of the NFS mount setof set of the NFS mount setof the NFS mount set of the NFS	
Cisco SQL Paxip Files Remote Storage The system does a backup daily. For the most part, there is nothing for the user to configure. All data and configurations that earlas on the system are archived automatically on a daily basis. Anthived data are logically grouped together and by default stored into separate archived files locally on the box. There is a separate page for each Archive group. More detailed information about each Archive group can be found on the individual Archive group pages. The user also has the option to mount a NFS drive to the system. All archived files will then get archived to the NFS mounted drive. Note: removing the NFS mount will NOT couported today. Storage Type Standard means the system will use its default archive location for of bookups. Tys' means the system will use its default archive location for of bookups. Tys' means the system will use the ngt mount specified to store all	
Decision Sqlit       to configure. All data and configurations that exists on the system are archived automatically on a daily basis. Archived data are logically groups 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 mounts a MS's drive to the system. All archived tiles will then get archived to the NFS mounted to the NFS mounted drive. Note: removing the NFS mounts will NOT coupy the MS contents back to local storage. Only NFS v3 mounts are currently supported today.         Storage Type	
Pexip Files       automaticaly on a daily basis. Archived data are logically grouped together and by default stored into separate archived files localy on the box. There is a separate page for each Archive group. More detailed information about each Archive group can be found on the individual Archive group pages. The user also has the option to mount a NFS drive to the system. All archived files will then get archived to local storage. Only NFS v3 mounts will NOT copy the NFS contents back to local storage. Only NFS v3 mounts will NOT copy the NFS contents back to local storage. Only NFS v3 mounts are currently supported today.         Storage Type       standard       a)         Optionsit. Storadord' means the system will use its default orthive location for all bockups. Xg5 'means the system will use the right mount specified to store all	
Remote Storage separate page for each Archive group. More detailed information about each Archive group can be found on the individual Archive group pages. The user also has the option to mount a NPS drive to the system. All archived files will then get archive to the NPS drive to the system. All archived files will be ng get archive to the NPS drive to local storage. Only NPS v3 mounts are currently supported today. Storage Type standard Optionsit. Stondord means the system will use its disfort archive location for all bockups. %b' means the system will use the rds mount specified to store all	
has the option to mount a NPS drive to the system. All archived files will then get archivel to the NPS mounted drive. Note: removing the NPS mounts will NDT copy the NPS contents back to local storage. Only NPS v3 mounts are currently supportined today.         Storage Type         standard         Optionsit. Storadord' means the system will use its disfout orchive location for all bockups. https://doi.org/10.0000/000000000000000000000000000000	
copy the NFS contants back to local storage. Only NFS v3 mounts are currently supportized today. Storage Type stanstand = Optionsit, strandors' means the system will use its disfort archive location for all backups. rgb' means the system will use the rgb mount specified to store all	
Storage Type standard = Optionsi: Stondord' means the system will use its disfout archive location for all backups: http://means.the.system.will.use.the.nfs.roount.specified to store all	
standard = Optional. Standard' means the system will use its disfault anthive location for all backups. http://means.the.system.will.use.the.nft mount specified to store all	
Optional, standard means the system will use its disfault archive location for all backups, http://means.the.system.will use the rifs roount specified to store all	
bookups. Info' means the system will use the rifs mount specified to store all	
orchives	
Remote Location	
Required only for infs' option. Specify remote offs to 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.

	ination Management Log Management	
Archive Collect LDAP SNMP	Syslog Tunnel Save	
Setup	Changes have been made to this configuration item	
Arbitrator Backup	and a second	
Cisco Files	Arbitrator Backup	
Osco 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, Away 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/CVAR 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	
	/chrool/scp/pub/txt_arch/ve	
	monthsKept	

#### **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.

HIVE MANAGEMENT Con	ifiguration Management Log Management	
Archive Collect LDAP SNI	MP Syslog Tunnel	
	Save	
Setup	Changes have been made to this configuration item	
Arbitrator Backup		
Osco Files	Cisco Files	
Cisco SQL	Archival for Cisco files. This Archive group will backup all Cisco CDR and Cisco	
	CMR raw files. These are the files that are sftpid to the system by the Cisco Call	
Pexip Files	Manager. The settings here are for informational purposes only. However, the user may disable the storage of raw Cisco COR and Cisco CMR raw files on the	
Remote Storage	system. This option could be used to conserve disk space.	
	status	
	enabled t	
	'enabled' - keep original cisco calr/cmr files, 'bisabled' - remove original cisco	
	calriomr files. The latsablest apaton will cause all calrionr files to be deleted	
	from the system. This is a permanent deletion.	
	archive_interval	
	daily	
	method	
	local	
	destination	
	/chroci/scp/publid, 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.

Arbba Celect UAV Systeg Turnel     Setup   Arbba Changes have been made to this configuration taen:     Arbba Changes have been made to this configuration taen:     Arbba Changes have been made to this configuration taen:     Arbba Changes have been made to this configuration taen:     Arbba Changes have been made to this configuration taen:     Arbba Changes have been made to this configuration taen:     Arbba Changes have been made to this configuration taen:     Arbba Changes have been made to this configuration taen:     Arbba Changes have been made to this configuration taen:     Arbba Changes have been made to this configuration taen:     Changes have been made to this configuration taen:     Arbba   Case SQL   Peop Files   Bemote Storage  Peop Files  Bemote Storage  arbba   Benote Storage  Betwee betwe	AGEMENT Configuration Mar	nagement. Log Management	
Setup       Autrastor Backup         Cases Files       Cases SQL         Peep Files       Autrastor Backup been tracke to this configuration tem.         Remote Scorage       Cases SQL data. This is the data that has already been processed by the system. There is nothing to edit here. The settings here are for information processed by the system. There is nothing to edit here. The settings there are for information processed by the system. There is nothing to edit here. The settings there are for information processed by the system. There is nothing to edit here. The settings there are for information processed by the system. There is allower for more granular control on which Call Manager data to insport.         Immediate       Immediate         Immediate       Immediate <th>offect LDAP SNMP Sysiog</th> <th>Turnel</th> <th></th>	offect LDAP SNMP Sysiog	Turnel	
Arbitrator Backup         Cases Files         Cases SQL         Peop Files         Remote Storage		Save	
Cisco Files       Cisco SQL         Penip Files       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 Spitem. There is in orbing to eith here. The settings here are for information 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.         achive_interval       daily         method       box         iccut       box         cistonation       cistonation         cistonation       box         cistonation       cistonation         cistonation       cistonation         cistonation       cistonation		Changes have been made to this configuration item	
Cases SQL       Archival for Cisco SQL data. This Archiva group will backup all Cisco data in the database tables. This is the data that has already been processed by the system. There is nothing to edit here. The settings here are for information purposes only. The data here is grouped together by the Cisco Call Manager lp Accesses. This allows for more granular control on which Call Manager data to import.         accive_interval       data/         meetod       isoai         destination       control isop/publiket, archive	p		
Perip Files       database tables. This is the data that has already been processed by the system. There is nothing to edit here. The settings here are for information purposes only. The data here is grouped together by the Cisco Call Manager ip Address. This allows for more granular control on which Call Manager data to import.         archive_interval       database tables. This is the data that has already been processed by the system. There is grouped together by the Cisco Call Manager ip Address. This allows for more granular control on which Call Manager data to import.         archive_interval       database tables. This is the data there is grouped together by the Cisco Call Manager data to import.         archive_interval       database         destination       tectoritispipub/lite, archive	0	Disco SQL	
Pesip Files Remote Storage 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 (p Address. This allows for more granular control on which Call Manager data to inport. achive_interval datay method boal destination .chronot/sop/publikt_achive			
Remote Storage     Address. This allows for more granular control on which Call Manager data to import.       archive_interval     data/       method     local       destination     Address. Archive	5	ystem. There is nothing to edit here. The settings here are for information	
archive_interval daty method boal destination Attroat/sop/pub/ht_archive	A	kddress. This allows for more granular control on which Call Manager data to	
method local destination /chroat/sop/js.dz/art.archive			
destination Actrost/scp/pub/kt, anthive		daly	
destination Actrost/scp/pub/kt, anthive			
destination /chrost/scp/pub/kt, archive			
Achroot/scp/pub/lat_archive			
		destination	
		(chroat/scp/pub/sc_anchive	
		monthsKept	
infinite			

#### Ndx

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

is scre	en can be used to manage Ndx files on the system.
max n	dx file size
1	
The ma	nximum size the ndx searchable file should be. Once the max size is hit, the ndx server will create a new ndx file.
max_s	earchable_days
1	
	iximum number of days that should be searchable. Ndx files greater than this time will still live on the system but will not l able from the UI.
month	sKept
6	
The ma	ximum number of months to keep ndx archives around. Each archived ndx will take up disk space. Warning, increasing th
numba	r too large may require customer to also increase the hard disk size.

#### **Pexip Files**

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

Archive Collect LDAP SN	MP 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	
Pexip 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	
	ensbled \$	
	'enabled' - keep original pexip files, thisabled' - remove original pexip files.	
	This 'disabled' option should be used to conserve disk space. The 'disabled'	
	option will cause all pexip files to be removed. This is a permanent change.	
	archive_interval	
	dally	
	method	
	look	
	destination	
	/chroot/scp/pub/bt_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).

#### archive\_interval

This can be set on a schedule of:

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

Selecting this option enables additional controls:



- \* Check NFS Host: Click and use the View Output button to see verification output.
- \* Check NFS Mount: Check the destination location (entered below) *after* saving the configuration. View Output shows disk usage on the destination of the NFS host.
- rsync System will sync the archive directory to remote system. The remote system must have rsync installed for this to work.
- rsyncToArb System will sync the archives directory to a remote Arbitrator. This utilizes the rsync protocol so both Arbitrators will always be in sync.
- scp System will copy archives to a remote location. Scp is not a sync. To reduce load on system and network, system only copies new / changing archives over to the scp location.
- sftp System will copy archives to a remote location. Sftp is not a sync. To reduce load on system and network, system only copies new / changing archives over to the sftp location.
- IP location

IP address. Also add username and password.

destination

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

ARCHIVE MANAGEMENT Configuration Management	Log Management
API Config Archive Blue Jeans Config Clisco SDL	Collect Import LDAP Probe SNMP Syslog Tunnel
	Save Delete
Remote Storage	Changes have been made to this configuration Item
Arbitrator Backup	
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 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.
Cisco SQL	archive_interval
Cisco Expressway SQL	daily V
Cisco RTMT SQL	
Ndx	Select an option
Pexip Files	disabled
Pexip SQL	rsync
Webex SQL	rsyncToArb
UHE SQL	scp
Vdf Clsco	'disabled'- keep archives locally, 'nfs'- Will mount a network file system as a local drive, which preserves local device disk
Vdf Gsip	space, 'scp' - System will copy archives to a remote location. Scp is not a sync. In order to reduce load on system and
	network, system only copies new / changing archives over to the scp location, 'sftp'- System will copy archives to a remote
	location. Sftp is not a sync. In order to reduce load on system and network, system only caples new / changing archives over
	to the sftp location, 'rsync' - System will sync archive directory to remote system. The remote system must have rsync
	installed for this to work, 'rsyncToArb' - System will sync archives directory to a remote Arbitrator. This utilizes the rsync
	protocol so both Arbitrators will always be in sync
	IP location
	192.168.123.123
	username admin
	password
	destination
	/mstrd
	monthsKept
	infinite V

See also: Backup and Restore the Arbitrator.

#### Collect

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

ARCHIVE MANAGEMENT	omert Lig Management	
Anthive Collect LDAP SNVP Systeg	fund	
	Save	
Classo CDR	Changes have been made to this configuration item	
	Cisco CDR Use this to configure where the collection of cisco of/ cmr files should be stored. "local" is the default location. Cisco CDR / CMR files will be processed and maned on local arbitrator. Choose "remote arbitrator." And the processed Cisco CDR / CMR files will be stored to the dictabase of a remote arbitrator. The 'remote join reads to be filed in with the jo address of the 'remote arbitrator'. If configured.	
	remote.jp	
	Addrator P	

#### LDAP External Config

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

; 🔺 🎯 🖌 111 📰	< a a ± • •	
NE MANAGEMENT Column Reasons - and reasons		
antes fater and beet space fater		
	lie .	
and larg	Ourges have been to a stand and and greater have	
	Exerved Cordig	
	The segment are shown from a strength drawneds. The same are specific advectange and an external discussion server. The advected documed Notices of the process and containing to or it and to the process and the section of discussion. These strength makes the test documed for another the section of a set of the process and the process and the process and the section of the process and the process and the process and the process and the process and the process and the process and the process and the process and the process and the process and the p	
	another as one were applied and a start region and applied and a boost the first and threads the part and the applied and the applied and a first and the	
	Beau, brieffite yr neg annal wy neg annal a yng wydar faethar yng ang wyg a'n gallan yn gall y sannaffit y gan a gall y sannaf yn gallan yn gal Gallan yn gallan yn g	
	Taxi LiteFuerRevision	
	Next class configuration	
	ou mu lanai toren fa sulgumen da sultar e fo, ten laño	
	Connect 1.047 configuration	
	the first internet to contrar por comparison in the particular approximation and contractions.	
	Entered File	
	64 F	
	Tool - on the pains series the same - ansates' - can not not disconfidence from any order. The out report additional from informations a leaf test	
	10	
	Instantini (in sense) wite for a nut ( linear). Also freeny many after senses	
	Insurativey (it lands), areay (publics c), iterativates intervy	
	Shifted	
	Report (m) provident listing the elements to an Jun Replan Annual Annu	
	In given	
	2 percent	
	Angelesistics), de landeal wing, Anada personnin any te laip senit. This laip can mai tany shilige to senit this kili. The controlatal landeal to perform any	
	Aparte approved and construction of the second se	
	and the second se	
	Repared only for strategy among Jaman is use with comment.	
	*	
	Anguint and, for whether wentige Associated Diff for expressionless or group. Lynem will use the Different hearts for all users under the lane 2016	
	unt .	
	unamental and a second s	
	Reparks sighter westwar witting through the interpretation for start and the same if it your Microsoft Ad Vaporagian Subsectionment's a Lineman	
	adjud talenadj slipengeng. The game will ensure a matering local sing-are for each care under the lane 2016. The game will can the property so the local care its	
	Nome Statement	
	Repaires who have a strip them meet the importance was the standard terms of the same to the interface the same to the interface the same to the interface to the interface to the same to the interface to the interface to the same to the interface to	
	stimuly dijunyany. Despans all evan a materia laar inpuas ja vant van wier de taan 2016. De passe all van dit property is de nam je de taan je d	
	end in the second se	
	M	
	Arguinal only for windows' wating. Though the in-matrix the day property same that shortful for any or Wessagh followy algues must be a same adjust Manualy	
	Al property. The general diversals in earth optimal shape care for each care only the base 2000. The quines will can the property in the send solaters, for the basic care of	
	Reparts of the visiting writing the double same any sole interpret film. The prime will same by all same such the test diff group. The task 200 mp constraines	
	many groups. Service is and quely integrated piller that contents and the groups that are abound Design (the Server ( ) previously/Contactinue). Do for any	
	desigs_30-dipensest_20' vorige-androph/Ch-chardroug1.20-beavily-designs20-dipensest20' vorige	
	Barlyan	
	where	
	Anguant and, for windows' unling. Charge Machine and it the billing progenty some than sideslifes by treasters of fast or your Missingh Kill Way states. Invention of a common Angland Microsoft Accounting	
	substantine	
	Regard and the water atting the behave to prevent party and the test and the section (right particulation or an effective or and a spectra	
	ansat it an ilute metotoogs	

#### **SNMP V3 User Config**

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

CHIVE MANAGEMENT	Configuration Management Log Management	
Archive Collect LDAP	SNMP Syslog Tunnel	
	Save	
SNMPv3 User Config	Changes have been made to this configuration zem	
	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 Server

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

ARCHIVE MANAGEMENT Configuration Management	general - Log Mangement	
Archive Collect LDAP SNMP System	Turnel	
	Silver	
Byslag Server	Changes have seen mapping this configuration item	
	Syslag Server	
	Use this screen to configure the ip address of your central systog server. This is a system wide setting, if an ip address is specified the system will send any internal Layer X messages onto- the specified systog server. Only one central systog server can be specified at this time. These validate firewall settings are open to allow incoming messages on the specified ip address and port.	
	external_splag.jp	
	Optionel. Enter in the ip address of your argunization's control tysilig server. A single (p Address or a single Damain name. Note, Domain name entries must resolve through its system	
	configured DMS (sam specified in system DMS settings)	
	protocol	
	top 8 Systeg prototori to use in systeg transport. Systeg server must also sort the same protocol.	
	there become in one or there a makeur that much some way way on a more become	
	external_systag_port	
	814	
	Optionui. Enter in the port, Default systag port is 514	

#### Tunnel

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

#### Creation

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

CHIVE MANAGEMENT Configuration Mar	Augenunz Log Musapoment	
Anthwa Collect LDAP SNMP Sysleg	tund	
	Save	
Creation	Changes have been made to this configuration tiers	
Managemeré		
Request History	Creation	
	Allows the creation of SSH tunnel to the specified endpoint, including interim hops needed.	
	Create Turtnel	
	Create Tunnel	
	Create a tunnel to the requested device, and optional port.	
	remateAddress	
	172.30.11.106	
	remotePort	
	3389	
	InterimDevice	
	169.254.5.12	
	Fetch InterimOevices	
	Fetch InterimDevices List	
	Petch a init of possible interim devices. This is required when the Arbitrator is connected to	
	multiple VPMs, and the IP address specified in the 'remoteAddress' field is reused within the	
	different VPRa.	

### Management

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

ARCHIVE MANAGEMENT Configuration	Aanagement Log Masagement	
Archive Collect LDAP SVAVP Syste	18 Tunnel	
	Save	
Creation	Changes have been made to this configuration term	
Management		
Request History	Management	
	Allows the listing, and management of existing tunnels.	
	List Active: Tunnels	
	List Active Tunnels	
	List only active durinels.	
	Remove Specified Tunnel	
	Remove and close the tunnel specified	
	Close the active nummel, by requestion	
	requestid	
javäss/lat.;		

#### **Request History**

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

RCHIVE MANAGEMEN	T Configuration Management Log Management
Archive Collect LDAP	SNMP Syslog Tunnel
	Save
Creation	Changes have been made to this configuration item
Management	
Request History	Request History
	Allows the listing of tunnel requests, and management
	of those requests.
	List Requests
	List all tunnel requests, and their status.
	List bill turmen requests, bind bren stolids.

# 4.1.13. Log Management

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

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

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

Archive Methods	
IP Address	Method
0.0.0	SCP
	SCP SFTP SMP

nive Settings				
• Used Space (570 GB) •	Free Space (375 GB)	Current Intervals 4 GB 10 Days Last Archive Time Aug 19, 2018 13:50	/	Archive Index Every 4 t GB 10 t Days Alerting Options Alert on archive success V Alert on archive failure
thive Methods				
IP Address	Method	Path	Credentials	
	SCP	+	None	: 2

# 4.1.14. Tools

#### **SNMP Tools**

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

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

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

3. Scroll through and select the desired MIB.

!	1	A	8	1	181		٩	4	£.	*	•	٠				👤 admin -
TOOLS	MIB Browser															
Load MIB	Import MIBs	SNM	P Connecti	« N0	Host					© Con	nection					
					OID									Operation	1	
					1.3.6								~	Get	0	Run
			Sele	ct a	MIB						×					
			Search													
				HOS	nmp DGE-MIB	CES-TYPE	ES	IS-MIB								
Name			Re-pa	arse					Can	cel Se	lect					
OID			_					_								
Syntax																
Access																
Status																
Description																

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

TOOLS Mill Browser							
Load MIB Import MIBs Si	NMP Connection »	Host 10.13.37.80		© Connection			
a 📄 iso a 📄 org		OID 1.3.6.1.4.1.6876.1			~	Operation Get	Run
<ul> <li>internet</li> <li>internet</li> <li>directory</li> <li>mgmt</li> <li>experimental</li> <li>private</li> <li>enterpris</li> <li>wmw</li> </ul>	Community	ptions	Cancel	Ok			
	vmwResources vmwProductSpecific vmwLdap vmwTraps vmwSRM vmwSRM			SNMP Options			
Name vmwSystem				Security Level auth/Nrv 8 Auth Protocol			
OID 1.3.6.1.4.1.6876.1 Syntax				SHA 8 Auth Passphrase			
Access				Privacy Protocol AES 8 Privacy Passphrase			
Status			6				
Description Parent of all managed of system software identified							

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

8

DID				Operation	
	.6.1.4.1.6876.1 ults		~	✓ Get Get Next Walk	
q	Text OID Toggle Numeric/Text OID Cre	ate Probe			
	Text OID	Value		Туре	
0	VMWARE-SYSTEM-MIB::vmwProdName.0	VMware ESXi	STRING		
7	VMWARE-SYSTEM-MIB::vmwProdVersion.0	6.0.0	STRING		
n	VMWARE-SYSTEM-MIB::vmwProdBuild.0	2494585	STRING		
5	VMWARE-SYSTEM-MIB::vmwProdUpdate.0	0	STRING		
-	VMWARE-SYSTEM-MIB::vmwProdPatch.0	0		STRING	

OID:

.1.3.6.1.4.1.6876.1.1.0 Probe Name:

Add to existing probe group Application ssh probe

Probe Group Name:	
	Cancel Create

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

# 5. Backup and Restore

# 5.1. Backup and Restore the Arbitrator

# 5.1.1. Step 1: Backup

To configure the Arbitrator backup, see Archive.

#### **Next steps**

Restore

## 5.1.2. Step 2: Restore

This procedure restores a backup of the Insights Arbitrator.

#### Pre-requisites:

• Backup (see see: Archive)

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

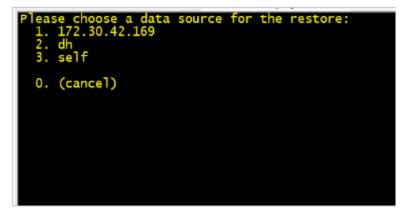
- 1. Log in to CLI as an admin
- 2. Go to **Backup Restore** and click **OK**.

+	from the following options.	
-	Network Configuration Time Configuration	
	Advanced ARB Options	
	ackup Restore	
	Change Arbitrator Branding Change Passwords	
	Fix Corrupt Ndx	
	Log Snapshot	
	NRS	
	Resize Disk Restart openldap	
	Upgrade	
	VPN Client Configuration	
+v(+)		68%+

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



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



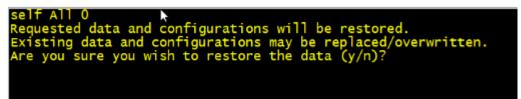
5. Select the data types to restore.

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

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



7. Confirm the restore.



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