

Legal Information

Please take careful note of the following legal notices:

- Copyright © 2021 VisionOSS Limited. All rights reserved.
- VOSS, VisionOSS and VOSS-4-UC are trademarks of VisionOSS Limited.
- No part of this document may be reproduced or transmitted in any form without the prior written permission of VOSS.
- VOSS does not guarantee that this document is technically correct, complete, or that the product is free from
 minor flaws. VOSS endeavors to ensure that the information contained in this document is correct, whilst every
 effort is made to ensure the accuracy of such information, VOSS accepts no liability for any loss (however caused)
 sustained as a result of any error or omission in the same.
- This document is used entirely at the users own risk. VOSS cannot be held responsible or liable for any damage to property, loss of income, and or business disruption arising from the use of this document.
- The product capabilities described in this document and the actual capabilities of the product provided by VOSS are subject to change without notice.
- · VOSS reserves the right to publish corrections to this document whenever VOSS deems it necessary.
- All vendor/product names mentioned in this document are registered trademarks and belong to their respective
 owners. VOSS does not own, nor is related to, these products and vendors. These terms have been included to
 showcase the potential of the VOSS solution and to simplify the deployment of these products with VOSS should
 you select to utilize them.

Security Information

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

Contents

1	What's New 1 1.1 Arbitrator Data Correlation Administration and User Guide: Release SP23 1
2	Introduction 2 2.1 Purpose 2.2 Intended Audience 2.3 Organization
3	Arbitrator Licensing
4	Correlate 4 4.1 Menu Bar 4 4.2 Assets 5 4.3 Alerts 10 4.4 Search 16 4.5 Call Path 21 4.6 Call Details 25 4.7 Call Management Configuration 25
5	Configuration315.1Policy Configuration315.2Asset Configuration435.3Probe Configuration435.4Controls535.5Response Procedure Configuration555.6How to Enable ServiceNow Intergration565.7ServiceNow One Way Incident Integration565.8Credential Configuration565.9Customer Configuration615.9Customer Configuration625.10Access Control645.11Import & Export765.12Archive Management785.13Log Management915.14Tools92

1. What's New

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

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

2. Introduction

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

2.1. Purpose

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

2.2. Intended Audience

The audience intended for this User's Guide includes system administrators and users responsible for configuring and monitoring the Correlation platform. Users should have a working knowledge of operating systems, software applications, and network elements.

2.3. Organization

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

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

3. Arbitrator Licensing

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



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

Voss	🛕 🛞 🦨 👫	📰 🔧 🚣 🔒	📩 🖻 🔅 Days remaining: 170
ACCESS CONTROL	Permission Groups Users Nodes	s Realms Protected Subnets	Password Policy SAML
Group Name	Realm Context	Timeout	
Administrator	(local)		2
Typical	(local)		× .
Permissions Users			
	Ana	lytiX :: Correlate	
VIEW - Main Application	VIEW - Asset Explorer	VIEW - Alarm Analyzer	VIEW - Punq Search
VIEW - Asset Map Explorer	VIEW - Call Details	VIEW - Call Path Monitor	VIEW - License Expiration
ACTION - Delete Calls	ACTION - Delete Paths	ACTION - Disposition Alerts	

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

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

To load a license file:

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

4. Correlate

4.1. Menu Bar

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

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

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



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

4.2. Assets

4.2.1. Asset Map Explorer



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

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

4.2.2. Asset Overview

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

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



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

4.2.3. Asset Explorer

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

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

Alert Severity Levels:

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

ASSET EXPLORER	-								Deplaying 1 - 50 c	11779 4 ¢	3 39 50 5
STATUS	10.12.07.40	10.24.5.10		Avera POS	LaperX HDS.	Lever HCS.	Local System	102.100.100.	18.52.45.51	18.52.028	0.7.569
Thre		-	18.18.87.1	10 13 37 100	10.13.07.190	10.10.07.000	10.11.37.20		16.10.37.000	11.13.37.298	10.10.07.40
400ETS - 0	-	10.13.37.60					the second	-	ante	and the	-
P Aurya P LayerX	-		- Bankar	P.	-	dia.		-	Lawrit Ope-	Littent	
LET BIP Phones LET BIP Phones LET BIP Phones LET BIP Phones LET BIP Phones		USABATTAR	-	ULABOTTAS		LULADITTA					
 Dais Nature Emission 											
F De Gerband											
+ E Hortel											
P 🖿 Ostar											
P 📷 SiLe Inshing											
P TELETRA TCO-CP											
P Tolefonica											
P Toiner											
P De las fact											

4.2.4. Asset Filtering



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

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

4.2.5. Asset Explorer Navigation



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

4.2.6. Asset Details View

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

- Alerts
- · Probes
- · Search

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

4.2.7. Asset Details: Alerts Tab

ET DETAILS	5 = 10.13	.37.43												X CLOS
ALIAS UMAC U	Unknown 15.13.37.43 Unknown Unknown	HOSTNAME TIMEZONE VENDOR MODEL	10.13.37.43 Unknown Unknown	VERSION DESCRIPTION	Unknown									
Transition Mail	THOUSE .	of sectors.					Displaying 1 - 10 of 37	40	<	>	30	10		STATUS
DATE	NODE	POLICY		ULE	STATUS	OWNER								
DETALS	FERENCE ID NODE POLICY RULE OWNER STATUS	DURNAL5 20000-01000005-00-01 dexparb Class Alerts : Universal Mager Class Ener Unassigned OPEN	-39950-34843	LAST ELAST NEXTESC/ EXI RESPONSE PROV	START 07/06/18 250 TIME 0 Days 0 LLATION 07/06/19 PIRES IN 00/06/40 CEDURE Default I	11:57:00 AM 1:22:30 01:39:16 PM 10						V	IEW R	EPORT
DE	ESCRIPTION													
on maker	dexparb	Cisco Alerts : I	Universal C	rtical Cisco Error	OPEN	Unassigned								
11:08:21 AM										and the second	ne-RT	MTSer	isionsE:	coelds Thresho
UTPUT:	Crical Cao (AlerDetail-	e Errer (<125Jul 8 2018 • On Sun Jul 08 11:08:2	16:08:21 10.13.3 11 CDT 2018, aler	17.43: <185>82258: ::5 FRTMTSessionsExceed	4123: CUCM12.lay	entiech.com: Jul 08 2018 16:0 cured. Counter SessionsActiv	8:21.207 UTC : %UC_RTMT-1-RTM e of Cisco Tomcat Web Application(ar	r_ALER Ø	E SA	acrea.				
07/08/18 11:09:21 AM OUTPUT: 07/08/18 09:25:15 AM	Crical Cao (AlerDetail desparb	e Errer (<12sJul 8 2018 • On Sun Jul 08 11:08:2 Cisco Alerts : 1	16:08:21 10:13.3 11 CDT 2018, aler Universal M	17.43: <185-412258: :: 5 t RTMTSessionsExceet lajor Cisco Error	4122: CUCM12.lay SThreshold has ou OPEN	entech.com: Jul 08 2018-16:0 oured. Counter SessionsActiv Unassigned	8:21.207 UTC : %UC_ITTMT-1-RTM e of Cisco Torncat Web Application(ar	r_ALER Ø	E SAA	der Page				
OUTPUTE OUTPUTE OTOD/18 OF/25:15 AM	Crical Cao (AlerDetail devparb Major Cisco (DeviceNan (AppID+Cis	o Error (<125-Jul 8 2018 = On Sun Jul 08 11:08:2 Claco Alerts : 1 = Error (<13-Jul 8 2018 se-SEP003048DEF81A co CaliManager()Cluster	16:08:21 10:13.3 11 CDT 2018, alex Universal M 14:25:15 10:13.37 (JPAddress=172: 10=StandAloneC	17.43: <185.402258: :: 5 1 RTMTSessionsExcees lajor Cisco Error 14.0: <179.402558: : con 16.1.11]Protocol-SIP[0 lister[Piode/D-CUCM1	4122: CUCM12.lay IsThreshold has on OPEN t 52775: CUCM12. DeviceType=336(D 2): An endpoint has	entech.com: Jul 08 2018 18:4 ured. Counter SessionsActiv Unassigned layendech.com Jul 08 2018 1 excription-SEP030048DEF8 unregistered)	82:1287 UTC : %UC, RTMT-I-RTM e of Cisco Tomost Web Application(ar 425:14 UTC : %UC, CALLMANAGE (A)[Rasson=10][PAddrAstrbutes=0](t_ALER #) 1-3-End 2aliState	PointU He402-1	rengia call_de	larad: 1 Evered	5. 16,402-6	ual_del	(Herechi)
07/08/18 11:09:21 AM OUTPUT: 07/08/18 09:25:15 AM OUTPUT: 07/06/18 09:19:21 AM	Critcal Care (AlenDetail devparb Major Cisco (DeviceNan (AppID+Cisc devparb	o Error (<12-Jul 8 2018 = On Sun Jul 08 11:08:2 Claco Alerts : 1 = Error (<13-Jul 8 2018 ns-SEP003048DEF81A co CaliManage/[Cluster Claco Alerts : 1	16.08.21 10.13.3 21 CDT 2018, alex Universal M 14.25: 15 10.13.3 (UPAddress=172, 10=StandWoreC Universal C	17-43: <185-482-58: ::5 It RTMTSestionsExceet lajor Cisco Error 7.43: <178-82058: : con 16.1.11[Protocol-SIP][kater][Node/D=CUCM1 ritical Cisco Error	4122: CUCM12.lay dsThreshold has oo OPEN t: 52775: CUCM12. Device Type=338[[D 2] An endpoint has OPEN	ennech.com: Jul 08 2018 16:5 oured: Courter SessionsActiv Unassigned layendech.com Jul 08 2018 1 encription-SEP0030480EF8 urvegistered) Unassigned	9:21.207 UTC : NUC, INTER-1-IRTM e d' Cisco Tomani Web Application(ar 4:25:14 UTC : NUC, CALLMANAGE A)[Plasson=10][PladdAtributes=0][0	r_ALER r) H-3-End JaliState	PointU w402-s	neegia call_de	tered: 1 Evered	5 K,402-	call_del	(8 Iveredit)

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

4.2.8. Asset Details: Probes

ASSET DETAILS + 10.1	3.37.43	# CLOS
TYPE Unknown P 10.13.37.43 ALLAS Unknown MAC Unknown ALLERTS AV PROBES	HOSTNAME 10.13.57.43 TIMEZONE Unknown VENDOR Unknown MODEL Unknown	VERSION Unknown DESCRIPTION
Trunk Activity Call Manager RTMT Hequest Call Activity Call Manager Service Galeway Activity Call Manager Service Galeway Activity CIPU and Memory	CPU and Memory HAW DETAILS Ormate this tools 0.061254 secon Shatas: 200 Chord versions"1.072-cPreClarine Timestamp-11072-07167* Auto ShureKolyteen *25376* Suffreyor Mercentage/Killer *1 Processing Percentage/Killer *1 Processing Percentage/Killer *	di to send a request to https://16.13.37.45/ast/ASTIsapi.dt//Get/PecCannedinto&iterse-getCpu4ndMemoryRequest edRepter ReturnCode=*0* CollectingRete=*30* AMD=*CULOM12* RetDe=*CULOM12*cgetCpu4ndMemoryRept ReturnCode=*0* EnroMessage=** Becate=*10+60* CollectingRete=*30* AMD=*CULOM12* RetDe=*000000000000000000000000000000000000

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

4.2.9. Asset Details: Search

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

ASSET DE	ETAILS = 10.13.37.43	×	CLOSE
Q.	TYPE Unknown HOSTNAME 10.13.37.43 IP 10.13.37.43 TIMEZONE Unknown VENDOR Unknown MAC Unknown MODEL Unknown	VERSION LINKOWN DESCRIPTION	
A ALERTI	8 ANPROBES Q SEARCH		
1		Last 24 Hours +	9
		Displaying 1 - 10 of 221,814 events + first prev next last +	10 0
0708/18 11:53:22 AM	<pre>cpackapeContent 16"1" name"callatta"> cpackapeContent 16"1" name"callatta"> cinaditamp (www?"2018-07-08 10:31:21") caesalcontd keye" Th041064100106-3481-4811-4811 completers heye"10:24172.14.11"> clocallattag keye""> clocallattag keye" clocallattag keye" clocallattag keyet"> clocallattag keyettag keyett</pre>	<pre>if-0010000000000000000000000000000000000</pre>	244.
2 07/08/18 11:53:17 AM	<pre><13>341 8 2018 14:51:40 10.13.37,7: 494 <190 11:51:38,10.13.37.43,216.239.35.12,71.41.85 11:51:83,23728,1.3544,123,5185,123,2440005 out,0,0,0,0,78-500,from-policy,.,3.0,,37/8,0</pre>	1 2518-57-38711151:39-55:60 FA-500.layerxteeh.com = = = 1,2018/07/08 11:51:38,039401025698,TMAFFIC.end,2049,2018/07/08 39,216.239.35.12,Bev-External.,.ntg.vays1,Bev-Trust,Extornal-Ontrust,othernet1/2,othernet1/1,Demo,2018/07/08 1,0dp,810w,630,366,275,7,2018/07/08 11:51:08,1,any,0,2207257887,Ex0,10.8.0.0-10.235.255.255.United States,0.4.3,aged- 1,0,9.0	XML.
	Host=10,13.37.7 Port=10.13.37.119.514 Michoci=tep_systeg		
07/08/18 11:52:17 AM	<pre><li< td=""><th>1 2018-07-08711151138-05100 PA-500.1ayerxteeh.com = 1,2018/07/00 11151137,004401025690,TMAFFIC.end,2049,2018/07/00 30,216.239.35.12.Dev-External.,.rtg.vays1.Dev-Trust.Extornal-Untrust.ethernet1/2.ethernet1/1.Deme,2018/07/00 100,allow.630,360,270,7,2018/07/00 11151106,2.any.0,2207257000,0x0,10.0.6.0-10.255.255.255.United States.0.4,3.aged- 1,0,9.0</th><td>XML.</td></li<></pre>	1 2018-07-08711151138-05100 PA-500.1ayerxteeh.com = 1,2018/07/00 11151137,004401025690,TMAFFIC.end,2049,2018/07/00 30,216.239.35.12.Dev-External.,.rtg.vays1.Dev-Trust.Extornal-Untrust.ethernet1/2.ethernet1/1.Deme,2018/07/00 100,allow.630,360,270,7,2018/07/00 11151106,2.any.0,2207257000,0x0,10.0.6.0-10.255.255.255.United States.0.4,3.aged- 1,0,9.0	XML.
	Line of the P. P. Don, 45 49 49 410 514 (American mains)		

4.3. Alerts

4.3.1. Alert Analyzer

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

ALERT ANALY	ZER	100710(2)					Displaying 1 - 10 of 3,702 /	Werts 42 4 3 30 10 2
PLJERS	1	SORT .	BULK DISE		rus •			
		DATE	NODE	POLICY	RULE	STATUS	OWNER	
		67/07/18 01:01:17 PM	Critical Cin (, <13×Jul 7 NCC_RIMT-1-3 MINTREssion value of 27 2018 17:56:0 NTMT_ALENT: NIMTSession value of 27	eo Error : Criical Cise 2018 17:15:48 [0.13,37 CTMT_ALERT: N[AlertSame- micceedeThreshold has on #012 which is over high 5[AlertHame-STMTDession EnceedeThreshold has on #012 which is over high	<pre>b Error (source:'cost .44: 4185-161396: : : @PHTeessionsEcreedsTh orared. Counter Seesie (threshold 330):AppET storeedsThreshold ()A storeedsThreshold ()A storeedsThreshold ()A threshold 230)(AppET</pre>	rol engine" mean 112181: cumell. roahold JAIerthe mahetive of Ciso >Claco AMC Servi 11.1ayerstech.co erthetall- Os Ea meantive of Ciso >Claco AMC Servi	agenAttempting Control Method Leperstech.com. Jul 07 2018 07 tol 00 Sat Jul 07 12:16:14 of Context Jul 07 12:16:14 of [ClasserID-1]SodoIS-cumel] t Jul 07 20:8 03:16:14 407.J7 t Jul 07 12:16:14 Cort 2018, al 0 Tomost Web Application(ast) 0 Tomost Web Application(ast)	(LiokipToAlert) Farameters ist6:44 FM.312 UTC : 207 2018, slert on node 10.11.37.44 has ; KTT Alert', <13-041 ? UTC : NUC_KTHT-1- Att os node 10.13.37.44 has : KTT Alert) code:90010)
		DETAILS	JOL 8	RNALS				VIEW REPORT
		5	NODE d POLICY C RULE C OWNER U STATUS	wpars soo Alens : Universal Intol Caso Error nassigned OPEN •	LAS ELAS NEXT ES RESPONSE PR	T CHANGE - SED TIME - CALATION GROTINE CALATION GROTINE DOCEDURE Danuit P	03.01.30 PM	
		01:01:29 PM	devparb	Catch all leaf.	Catch all test.	OPEN	Unassigned	(B) \$
		OUTPUT:						
		01:01:26 PM	devparb	Cisco HCS PCA	RTMT_ALERT	OPEN	Unassigned	۵۵
		OUTPUT:						
		A 01/02/21 PM	devparb	Cisco Alerts : Universal	Critical Cisco Error	OPEN	Unassigned	
		OUTPUT:	Crical Claco I (AlertName-JP Tomcat Web /	(mor (<135Jul 7 2018 18:02:21 TMTSisseions Exceeds Threshol (pplication(ast)	10.13.37.43: <185>79373: : c[[AlertDetail= On Sat Jul 07	52072: CUCM12 Jaye 13:02:20 CDT 2018. (nstech.com: Jul 07 2016 18:02:20.641 U alert RTMTSessionsExceedsThreshold ?	ITC : %UC_ITTMT-1-ITTMT_ALERT: % has occurred. Counter SessionsActive of Cisco
		01/02/28 PM	devparb	Cisco HOS PCA	RTMT_ALERT	OPEN	Unassigned	⊛≎
		OUTPUT:						
		01/02:40 PM	devparb	Catch all test	Catch all test	OPEN	Unassigned	
		OUTPUT:						

4.3.2. Alert Disposition

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

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

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

ALERT AN	VALYZER						Displaying 1 - 10	of 3,099 Alerts 4	<	> >>	10 0
FLIERS		SORT + DATE	BULK DI NODE	POLICY	ATUS - RULE	STATUS	OWNER				
		COCCANS CT21-27 AM DETAL	Critical C pub.dimens Bervice op astdc-v-ot S X FFERENCE ID NODE POLICY RULE OWNER STATUS	Linon Firzar i Crilinal CL Linnal.com. Jul 18 2018 errational status 15 DOM m-pubdimensionsal.com.) DUFPALS 20000-01000005-00-01-3004- departb Como Adots : Universal Defical Caso Enor Unanged OffEN UNDER REVIEW	NOB TETOT (<13-JPL 4 12-05147 PR.154 UTC KUDICIAGO CALIMANA (AppID-CLASO AND DET 100 1100 RESPONSE	2018 12:01:37 169. WOL PATET-2-MERT, A WOL PATET-2-MERT, A START 07:00-18 START 07:00-18	254.5.16: <186>20568: LERT: X[AlerURserClas generated on Bun Jul odoT3=solder-V-ecm-pub] 107:01:37 AM 109:04:04 AM RP	: 4 202500: ant icalServiceDown J 08 07:03,37 CDT - RTMT Alert)	ke-v-ccm AlertDe 2018 on VIE	w REPOR	© ©
			ESCRIPTION	ACKNOWLEDGE							
		COURSES AN	069940	CLOSE		OPEN	Unassigned				€\$
	DTOINS despare DTS238 AM OUTF2138 AM OUTF211 OUTF211 RTMT_ALERT: %(Avenue RTMT_ALERT: %(Avenue	DISREGARD CLOSE + LOCK AT: %/Aer/Name=OnticeServe	sDown(jAlerDetail-4012 S	OPEN 88: : : 202602: antido-v-o milor operational status MC Gascal/Dumer Dul	Unassigned m-pub.dimensional.com, Jul 1 Is DOWN #012Cisco Califian Nordel Duration of 15	26 2016 12:02:37 PM-4 sger.#012The sleet is g	ian UTC : prevaied i	SUIC_ATMT In Sun Jul 0	® \$		
		CTOB18 07/02/39 AM OUTPUT:	degañ	Ciboo HCS PCA	RTMT_ALERT	OPEN	Unastigned				©¢



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

4.3.3. Filtering by Disposition

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

ALERT AN	VALYZER		REFYERE					Displaying 1 - 10 of 248	Alerta dC C > 30 10 0
PILTERS	1		SORT -	BULK DIS		STATUS .	-		
Test			DATE	NODE	POLICY	Open	STATUS	OWNER	
		1	OT/OB/18 OB 13:36 AM OUTPUT:	dexparb Crical Cace RIMT_ALER CDT 2018 on	Cisco Alerts : U Error (<135.Jul 8 2018 11 Sc/AlertName-Ortica node astdo v-com pub	Under Review Acknowledged Released Cosed	DPEN 50566: asido-v perational statu vice@ClusterID	Unassigned -com-pub.dimensional.com: Jul 88 2018 0 as is DOWN.4012Cisco CalManager.4015 -([NobibD-satids +com-pub]; FTIMT Aler	(8) \$ 01:13:27 PM 381 UTC : NUC_ NTMT-2- 27% alleft is generated on 5un Jul 08 08:13:37 6
		1	07/08/18 08/14/44 AM	devparb	Cisce Allerts : U	CANGEL	OPEN	Unassigned	® \$
			OUTPUT	Crisel Cisco (AlertName=/ StandAloneC	Error (<13-Jul 8 2018 1 AuthenticationFailed [Ak Juster #012#012There a	2:14:44 10.13.37.44: <186>1961 ertDetail+ Number of Authenticat are 2 AuthenticationFailed events	19: 1115893. cume11.8 IonFailed events exceed Jup to 30	layentach.com: Jul 08 2018 01:14:44 PM Is configured threshold during configured	1563 UTC 1 %UC_RTMT-2-RTMT_ALERT; % interval of time 1 within 3 minutes#012 on duster

4.3.4. Alert Filters

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

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

FILTER MANAGER				✓ SAVE	* CANCEL
+ ADD - REMO	VE	KEYWORDS SET	VERITY DATE & TIME		
Test This is a test titler	ALLOW DISREGARD	NAME	Test		
		DESCRIPTION	This is a test filter		
		POLICY			
		RULE	Critical 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

FILTER MANAGER					✓ S	AVE X CANCEL
+ ADD - REMOVE		KEYWORDS	SEVERITY	DATE & TIME		
Test This is a test litter	ALLOW DISREGARD		ACTIVE	+ ESCALATED		O EXPIRED
		A MAJOR				
			NAL 🗹			

• 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 X CANCEL
+ ADD - REMOVE	KEYWORDS SEVERITY DATE & TIME
This is a test filter	DISREGARD DATE END DATE
	TIME ALL DAY START HOUR MINUTE START O C O C End O O O O O O O O O O O O O O O O O O O

4.3.5. Alert Journal

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

To add an Alert Journal:

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

- ALLINI A	INCLER		The state of the s					Lisbeying i	- TO GI S, GRO PORTS		<	,	11	10	-
FILTERS	+	SO	RT +	BUI	K DISPOSITI	ON .	STATUS *								
Test			DATE	NODE		POLICY	RUL	E	STATUS		OW	NER			
		A	07/08/18 12:00:40 PM	Critic 1 1 20 RCWT_A DOWN.# astdc- pub]:	al Cisco E: 3794: astd LERT: %[Al 012Cisco C: V-OCM-pub. RTMT Alert	rror : Criic c-V-ccm-pab. ertName=Crit allManager.) dimensional.	al Cisco Error dimensional.co cicalServiceDow 012The alert i com. [AppID=Ci	<pre>(<13>Jul 8 2 m: Jul 08 201: m)[AlertDetai s generated or sco AMC Servir</pre>	018 17:00:40 169 8 05:00:37 PM.41 1=#012 Service o a Sun Jul 08 12: ce][ClusterID=][.254. 0 UTC perat 00:37 Nodel	5.16: i 80 ional CDT D-ast	<196 C_RTM stat 2018 dc-V-	>20688 T-2- us is on nod com-	1: (H	9:
			DETAIL	S	JOURNAL	S					V	IEW P	REPOR	т	
			TINESTAMP		CREATOR	ACTION									
			07/08/18 12:	45:36 PM	system	Alert Creat devparb(12 <186>205 %UC_RTM operationa 12:00:S7 C [ClusterID	ed. Response: Defa 27.0.0.1) - Oritical C 3811: : : 203794: asto 17-2-RTIMT_ALERT: 1 status is DOWN # 2012 2018 on node a @Node(D=astdo-v-d	ault IRP Schedule: iseo Error : Criical de-v-com-pub.dime : %(AlertName=Cr 012Cisco CallMan istde-v-com-pub.di com-pub]: RTMT A	: autogenerated_sche I Cisco Error (<13>Jul ensional.com: Jul 08 2 rticalServiceDown]/Ai lager.#012The alert is imensional.com.][App Vert)	dule_2 8 2018 2018 05 entDetz genern ID=Cis	4x7 No 8 17:00 5:00:37 al=#01 ated on co AM	de: 140 161 PML41 2 Servi 1 Sun J C Servi	9.254.5. 10 UTC : ce ul 08 ice]	16:	
			07/08/18 12:	45:37 PM	system	Incident Re	sponse - Method: /	ALERT, Status: Su	00855						
		07/08/18 12:45:37 PM system Incident Resconse - Method: CONTROL, Description: New Vodalone								Contro	d. Stati	IS: Suo	cess	_	
			NEW JOURN	AL ENTR	Ý					C	LEAR		ADD		
	07/08/18 devparb		rb	Cisco HCS PC	A RTM	T_ALERT	OPEN		Una	ssigned	8	(8	0:		
			OUTPUT:												

4.3.6. Alert Sorting

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

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

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

FILTERS	+	SORT . BULK	DISPOSITION . STAT	US *			
Test		TIME TO EXPIRE/ESCALAT	E ASCENDING DESCENDING		STATUS	OWNER	
		ALERT SEVERITY	ASCENDING DESCENDING		Error OPEN	Unassigned	×
		ALERT DATE & TIME	ASCENDING DESCENDING	~ ~	cm-pub.dimensional.com own[[AlertDetail=#012 S	m: Jul iervice	
			CANGEL	UPDATE	ClusterID=[NodeID=astdo-v-o:	am-pub[: RTMT Alert)	node
		12:00:40 PM			T OPEN	Unassigned	×
		OUTPUT:	Prof. 1911				_
		4 07/08/18 devparb	Catch all test	Catch all tes	It OPEN	Unassigned	×
		OUTPUT:					
		A 07/08/18 devparb	Catch all test	Catch all tes	it OPEN	Unassigned	×
		OUTPUT:					
		07/08/18 devparb	Cisco Alerts : Universal	Critical Cisc	o Error OPEN	Unassigned	×
		OUTPUT: Crical C 2018 05 [IssuerC Claco In	isco Error (<13-Jul 8 2018 17:02:03 1 :02:03 PM.181 UTC : %UC_ICSA-2-K N=ASTDC-V-CCM-PUB][ErrorCode=0 tercluster Sync Agent service detected	69.254.5.16: <16 CSACertificateVal 2][AppID=Cisco In 4 a validation error	16>4940: : : 1386: astof-v-imp-pu lidationFailure: %[SubjectCN-AS intercluster Sync Agent][Cluster/D or on the certificate being process	b.dimensional.com: Jul STDC-V-CCM-PUB) D=[[NodelD=astof-v-imp- sed)	08 pub]:
		07/08/18 devparb	Cisco HCS PCA	RTMT_ALE	RT OPEN	Unassigned	
		OUTPUT:					
		07/08/18 devparb	Catch all test	Catch all tes	st OPEN	Unassigned	*
		OUTPUT:					

4.4. Search

4.4.1. Event Search

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

4.4.2. Simple Searching

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

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

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



4.4.3. Keyword Searching

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

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



4.4.4. Utilizing Conjunctions with Searching

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

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



4.4.5. Date Range Searching

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

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



4.4.6. Search Result Meta-Data

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

Q SEARCH	
1.500	
	and and a state way and a state and a state
CISCO and SYSLOG	Last 24 Hours - Q,
	Displaying 1 - 10 of 30,833 events + first prev read last + 10 s
xml version='1.0' encoding='US-ASCI1'?	Tax
07/09/18 <sc018> 14.51.10 PM <ibpo></ibpo></sc018>	
<body <butiting></butiting></body 	
<entity>20000</entity>	
<td></td>	
<device>20000-01000005-00-01</device> <oroup-layers< oroup=""></oroup-layers<>	
<td></td>	
<813100× <8097>	
<rdme>devparbs/RDME> <ip>127.0.0.1</ip></rdme>	
<td></td>	
<pre>«HODMEY>20000-01000003-1</pre>	
<3802	
<pre><hithop <br="" hithop="" myslog=""><port>*+\$14</port></hithop></pre> //HITHOP/ <port>*+\$14</port>	
<address>10,13,37,44</address>	
<30003>	
<devicepate></devicepate>	
 <uzc></uzc>	
<start>1531164962</start>	
<offset> </offset>	
(ADJUSTED)	
<ncouledetail></ncouledetail>	
(REFERENCEID)	
<p< td=""><td></td></p<>	
800082</td <td></td>	
<13>201 9 2018 19:34:22 10.13.37.44: <187>419600: 201 09 2018 07:34:22 FM.215 UTC : 4	OC_AUDITLOG-3-AdministrativeEvent: %; UserID =admin;; ClientAddress
=10.13.37.113][Severity =3][EventType =UserLogging][ResourceAccessed=Class SOAP Server][Ev =AdministrativeEvent][ComponentID =Class CCM Application][AuditDetails =Login Authentication	estStatus =Failure [CompulsoryEvest =So] AuditCategory Failed)(App ID=Ciaco Tomcat)(Cluster ID=)(Node ID=cumcil): Audit
Event is generated by this application	
<asset_name>LayerX BCS Pub</asset_name>	
<pre><asset_ipaddrese>10.13.37.44</asset_ipaddrese></pre> /ASSET_IPADDRESE> <pre><asset_bostname>publ1.corp.lsyerxtech.com/ASSET_BOSTNAME></asset_bostname></pre>	
CASSET DESCRIPTION>	
<a>ASSET_VERSION=CIMOD Call Manager SET_VERSION>	
<abbet_aliab>URRNOWS/ABBET_ALIAB> <asset_vendos asset_vendos="" cincos=""></asset_vendos></abbet_aliab>	
<pre>(ASSET MODEL=Unknown(ASSET TIMETORYND) ADDAUS(ASSET TIMETORY)</pre>	
<asset_racadoress>Unknown</asset_racadoress>	
<asset_raintenance_node>O</asset_raintenance_node> 	
<isdexid>6c02b5180b12b91f249e79af5b43b8bf</isdexid>	
Human 10.11.17.44 Horse' 114 Married ayaog	

4.5. Call Path

4.5.1. Call Path Monitor

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

CALL PATH MONITOR									Displa	aying 1 - 5 of 1	*	< >	>>	RANGE	1 HOUR +
									earch			Q,*	sont	TOTAL DELA	W DESC +
PATH	METHOD	DELAY	ANG DELAY	HOPS	PCALLS	LAST CALL	#PATHS								
a 🔄 LXLAB-RTR-1-eth1 🚥 Cisco ASA	LX1	883.00	94.35	6	23	07/09/18 04 21 55 PM									۲
n ⁴ =													OFFICE	D at a	- 2
1		-					-	8			-			0	
5-	-	-0	-	-		83					a				
						-									
0															
	_								_						
LXLAB-RTR-1-eth1	LX1	62.00	33.92		12	07/09/18 04:13:15 PM	-								۲
▶	LXI	35.00	34.25	5	4	07/09/18 03:53:38 PM									۲
▶ 🔄 10.13.37.238 192.168.103.38	LX1	7.00	2.66	2	32	07/05/18 04:18:01 PM									

4.5.2. Sorting Call Paths

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

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

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



4.5.3. Time Range for Call Paths

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

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

	> > RANGE: 1 HOUR *
x search Q.	ALL 1 HOUR 1 DAY 2 DAYS 3 DAYS 4 DAYS 5 DAYS

4.5.4. Expanding Call Paths

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

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

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

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

CALL PATH N	NONITOR				Displayin	g1-5ol5 🛠 <	> > RANGE: 1 HOUR
					× search	Q.•	SORT TOTAL DELAY DESC
PATH	METHOD	DELAY DELAY HOPS	ACALLS L	AST CALL PATHS			
DXLAB-RTR-1	eth1 Cisco ASA LX1	663.60 94.36 6	23 07/09/1	18 04:21:55 PM			Latincy by Hop
8- 7-		8	- 50	/	8	8	0
*	8						
LXLAB-RTR-1 LXLAB-RTR-4		62.00 33.92 5 ASSET NAME	12 07/08/ LAT	18 Dd:10:15 PM 42	лтек	08	NETWORK
DALAB-RTR-1 LXLAB-RTR-1 LXLAB-RTR-4	481 LX1 481 LX1 IP ADORESS 172.161.11 (Endport)	62.00 33.52 5 ASSET NAVE	12 07/08/ LAT	18 DL10:15 PM (2)	JITTER	ON	NETWORK
LXLAB-RTR-1 LXLAB-RTR-4	eth1 LX1 IP ADORESS 172.161.11 (Endpoint) 172.161.1	82.00 33.92 5 ASSET NAVE 	12 0708/ LAT 0 2.84	18 DL1215 FM 22 EMCY	атея 0 0	ON THI FAL	NETWORK JE SE
LXLAB-RTR-1 LXLAB-RTR-4		82.00 33.82 5 ASSET NAME LXLAB-RTR-1-ath1 LXLAB-RTR-3-ath1 LXLAB-RTR-3-ath1	12 07/08/ 0 2.68 7.67	18 De113:15 7M 23	JITTER 0 0	ON TRU FAL	NETWORK JE SE
DXLAB-RTR-1 LXLAB-RTR-4		5200 33.92 5 ASSET MANE - USLAB-RTR-1-abh1 USLAB-RTR-3-abh1 USLAB-RTR-3-abh1	12 07/08/ 0 2.85 7.87 5.42	18 Dd 10:15 PM 22 TENCY	0 0 0	08 THL FAL FAL FAL	NETWORK JE SE SE
DXLAB-RTR-3 LXLAB-RTR-4		62.00 33.82 5 ASSET NAVE 	12 07/08/ 0 2.86 7.87 5.43 5.43 5.43 5.43	18 Del 10 115 PM (12)	UTTER 0 0 0 0	0N TRI FAL FAL FAL	NETWORK JE SE SE SE SE

4.5.5. Searching Call Paths

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

- Source
- Destination
- Method
- Hops

×	search		٩.
	SOURCE		
	METHOD		
	MOPS		
		CLOSE	SEARCH

4.5.6. View Call Details from the Call Path

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

4.6. Call Details

4.6.1. Call Details Explorer

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

							Displaying	1-5df5 46 6	> 30 RA	NGE. 1 HOUR +
						×	sourch	Q.+	SORT TOTAL	OELAY DEBC +
PATH	METHOD	DELAY DE	NG HOPS	ACALLS	LAST CALL	PATHS				
u LXLAB-RTR-1	LXI	666.00 36	0.00 5	2	07/06/18 04:53:28 PM				OPF MET	View Calls
10 10 10	-	-	-	_		•		8		0
2		-								
CALL DETAILS EXPLORER	- interaction						Displaying 1 - 2	2 of 2 at 2 at 2	30 SONT.	ATENCY DESC +
Jul 5, 2018 4:03 pm - Jul 5, 2018 5:03 pm		30	C ×					· teach		Q,*
TIME BOURCE					DESTINATION			VENDOR	LATENCY	HOPS
07/08/18 04.46/36 PM 101@192.166.10	0.56				10248172.16.1.11			Litt	600	
att 07/06/16 04:53:36 PM 101/01/92:166.10	0.56				102/0172.16.1.11			LXC9	34	
DIRAKED CALL PATH	010918-04-49-39	Paul I	01	PHET AL	FORWARD CAL	METRICS				

4.6.2. Filter by Date and Time

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

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

Jul 9, 2018 4:06 p	pm - Jul 9, 2	018 5	:08 p	m	-	3	3	3 4	9	C	×			
ast 5 Minutes	<	34		.0	201	8.0	>		Ju	1		2018		>
ast 30 Minutes	Su	Мо	Tu	We	Th	Fr	Sa	Su	Mo	Ти	We	Th	Fr	5a
ast Hour	24	25	25	27	28	29	30	24	25	26	27	28	29	30
ast 12 Hours	1	2	3	4	5	6	7	1	2	3	4	5	8	7
and the library	8	9	10	11	12	13	14	8	9	10	11	12	13	14
Last 24 Piburs	15	16	17	18	19	20	21	15	15	17	18	19	20	21
ast 7 Days	22	23	24	25	26	27	28	22	23	24	25	28	27	26
This Month	29	30	31	1	2	3	4	29	30	31	1	z	3	4
last Month	4		a):[08		PM		1	5	:	08		PM	
ast 2 Months														
ast 3 Months														
aat 6 Months														
ast Vear														

4.6.3. Filter by Call Quality



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

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

4.6.4. Clear Filter, Update and Delete Call



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

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

4.6.5. Refresh Pause

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



4.6.6. Sorting

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

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

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

Displaying 1 - 50 of 208	*	<	>	>>	SORT	LATENC	Y DESC -
	10		LATE	ENCY	•	ASC	DESC
	1	TIM	E				
		SO	URCE				
		DE	STINA	TION			
		VEN	NDOR	1			
		LAT	ENC	Y			
		HO	PS				

4.6.7. Search Call Details

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

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



4.7. Call Management Configuration

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

ARCHIVE OPTIONS	DAILY	WEEK	LY	MONTHLY			
ALERTING OPTIONS		ti Oli Ar	CHIVE	TAILUAL		11VE 3000E33	
HOST		METHOD		метно	DS PATH	CREDENTIAL	
		SCP	SFTP	SMB		admin	\$
		SCP	SFTP	SMB		admin	\$

5. Configuration

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

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

	۲	4	îşi		٩	<u>\$</u>	A	₹	🖻 🌻	🡤 admin 🗸
1.	2.	3.	4.	5.	6.	7.	8.	9.	10.11.	12.

5.1. Policy Configuration

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

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

- Network behavior
- Metrics and Threshold Violations

Policias			Bular					
None			Rules	Thursdayla	International	The local days	Research Research	
Name Fallove	1	-	Name	Threshold	Window	Severity	Response Proced	ture
Poregra Care nederator	-	-	jitter Value Exceeded	1 time	1 minute	Critical	LinkCallToAlert	¥3 = Z
Avaya PDS SNMP Alarms	⊻.	4	Name	Latency Velue Danas	eded			A1 = V
Avaya PDS SYSLOG Alarms		13	Description	Latercy value Exceeded				
Cisco Call Monitor		4						
LAPERX Agent Monitor		3						
Log Monitor		1						
LX1 Call Monitor v2		3	Туре	Simple		Action	Respond \$	
LX1 SIP Call Errors v2		8	Threshold	1	Respo	nse Procedure	Reboot Machine \$	
Nortel Call Monitor		3	Window	1 minute	t Def	Inition Output		
PING Monitor		2	Severity	Different		Enabled	2	
Powerwave SNMP Alarms		15		Critca		Inhard Cutaut		
SiLo training policy		2			Main D	tale Descension		
Test Narm v1		T			,	this Processing		
AJ ExperiMental	•	3	MOS Value LOW	1 time	1 minute	Critical	LinkCallToAlert	A1 = Z
ALSTOYBARN : Austin - Alert Esa	•	9	Packets Lost Value Excer	eded 1 time	1 minute	① Critical	LinkCallToAlert	1 = 1
ALSTOYBARN : Dallas - Alert Exa.,		0						
ALSTOYBARN : NYC - Alert Examp.	1	9					Displaying 1 - 4 of 4	4 events + first prev next las

5.1.1. Correlation Rules

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

Parameter	Description
Name	Descriptive name for the correlation rule which will be displayed within an Alert and viewed in Alert Analyzer.
Description	Enter a complete description of the problem that created the alert along with any specific remediation steps that should be taken to resolve the problem.
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	 Choose the action that is to occur for this rule, based on the selection in the Severity field Respond - If the condition is met, set a marker and send an alert. Track - If the condition is met, track the event, but do not post it to the Alert Analyzer. Track/Respond - If the condition is met, send an alert and continue to monitor. Respond on Expire – If the condition is met, wait to send an alert until the window time has expired. Submit - Submit the results of a correlation event back into the Correlated. Submit/Respond - Submit this alert back into the Correlation Engine so that the event can be analyzed and re-correlated. Then set a marker and send an alert. 									
Response Procedure	For any rule that is satisfied, an Incident Response Procedure occurs and an event is posted to the Alert Analyzer. Select the Response Procedure from the drop-down menu to execute when conditions have been met.									
Definition Output	Selects a single Correlation Definition's extracted value to be displayed with the Alert.									
Enabled	Toggle to enable/disable the rule									
Inherit Output	Toggle to enable/disable whether the rule will include the results of the filter attached to the policy module.									
Halt Processing	Toggle to halt processing of logs to any other rules within the policy if the rule matches. This will highlight the Policy in Green to indicate that this function is in use.									
Correlation Definitions	Click the wrench icon where you can define one or more definitions match and or extract the required data from a log or event. See Correlation Definitions.									
Output Order	Sets the preferred order to output the extracted data from the Correlation Definitions.									
Done	Click the Done box when the rule is complete									
Save	Be sure to click the Save button so your rule (or changes) are saved and committed.									
POLICY CONFIGUR	ATION	Rules	Fibers							Save
--------------------------	-------	-------	------------------------	----------------------	-------	--------------------	----------------	-----------	--------	------
Policies Name Fail	over		Rules	Threshold	Wine	daw Severity	Response	Procedure		
Arda		1	Name	Jitter Value Exceede	d			1	3 🔳 🛃	
Aspect UIP System Alerts		2	Description					-		
Asset Log Monitor		1								
Avaya Call Monitor		4								
Awaya PDS SNMP Alarms		4	Turne	-		Action	-			
Avaya PDS SYSLOG Alarms		13		Drube	-		respond			
Cisto Call Monitor		4	Threshold	1 2		Response Procedure	LinkCalTsAlert			
LAYERK Agent Manitor		3	Window	1 minute	1	Definition Output				
Log Monitor		1	Severity	Critical	1	Enabled				
UX1 Call Monitor v2		8				Inherit Output	2			
LX1 SIP Call Errors v2		6				Halt Processing	2			
Nortel Call Monitor		3	-							
Obst Manhart	100	3	Latency Value Exceeded	1 6/16	1 min	ute O Criscal	LinkCalifo	Alert	×1 - ×	

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

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

Within the Regex Wizard there are 2 sections:

- 1. Select a Log: In the top section you can search and select the log or data set you will be utilizing. That will then show up in the bottom portion under the phrase "Select log from the list above or paste log here:". As the phrase indicates you can copy and paste a log into this section as well.
- 2. Create Regex: Once you have your log then go to this section. Here you can utilize the wizard to create the Regular Expression required. Close the wizard and copy this pattern the Regex into the box under Pattern.
- Source Field: In the drop-down box select the source from which the data is being extracted.
- Pattern Type: Select from the drop-down box the type of expression you want to utilize:
 - String Match
 - Regular Expression Match
 - Regular Expression Match/Extract (Most Often Used)
 - Regular Expression Multi-Valued Extract
- Function: If the extracted data is integer based then you can apply the following functions that will allow you to compare the data:
 - None
 - Greater Than
 - Less Than
 - Same
- Value: This field will only be available if the data extracted is an integer.

POLICY CONFIGURA	ATION Rules	Filters		Save
Policies		Filters		
Name Failo	wer	Name Pattern		
Arda	0	Name	· · ·	
Aspect UIP System Alerts		Vendor Method		
Asset Log Monitor	0	Pattern		
Avenue Call Monitor		(method="cisco")	1	
- maje car montos	-	Source Field		
Avaya PD5 SNMP Alarms	2 3	Raw Log	~	
Awaya PDS SYSLOG Alarms	2	Pattern Type	and the second	
Cisco Call Monitor	2	Regular Expression Match/Extract	0	
LAVERX Agent Monitor	1 T	Function Value		
Log Monitor	0	News		
UKI Call Monitor v2		Call Manager lp		
LX1 SIP Call Errors v2	0	Pattern		
Nortel Call Monitor	1	callManagerip="(,"7)"	1	
PING Monitor	1	Source Field	141	
Powermave SNMP Alarms		Pattern Type		
SiLo training policy		Regular Expression Match/Extract		
Test Alarm v1	0	Function Value		
AJ ExperiMental		None +		

5.1.2. Correlation Definitions

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

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

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

RULE DEF	INITIONS » Jitter Value Exce	reded	Changes made	Cancel Update
0900				Last 24 Hours - Q
Chick here for t	es CALL_METRICS_ID O Jour O	nition Manually CALL JD ⁶⁹	Displaying 1 - 10 of 154,942 i	events + first prev next last + 10 t
Source Field	Raw Log	V		
2 07/11/18 16:54:10 PM	<pre><li< td=""><td>: (*CISCO_RTMT_SERVICE*: cots *:1,*"neturpOode*: *0*, "Errorthessape*:**,*/ AssetTpAddrees*: *10:13:37.43*, "Mame*: *CUCH.2 DetractField Name this field: IP Address Cancel Save</td><td>AND","CUCH12","Histe","CUCH12","AssetName","10.13</td><td>.37.43","AssetRostname":"10.13</td></li<></pre>	: (*CISCO_RTMT_SERVICE*: cots *:1,*"neturpOode*: *0*, "Errorthessape*:**,*/ AssetTpAddrees*: *10:13:37.43*, "Mame*: *CUCH.2 DetractField Name this field: IP Address Cancel Save	AND","CUCH12","Histe","CUCH12","AssetName","10.13	.37.43","AssetRostname":"10.13
3 67711718 16(54:10 PM	<pre>«HETURNEGG>PEP Fatal error: Uso /parts/jail/arbitratus/modules bteck traces #0 [internal Numotion]: Boagdij #1 /parts/jail/arbitratus/modu #2 /parts/jail/arbitratus/modu #3 (pain) thrown in /parts/jail/arbitratus /METURNEGS/METUR</pre>	aught ScapFault exception: [HTTP] Unauthoriz- /www/ulscu/axlobtPhoneInventory_creds.php4 ent->_domoguest(' mail versions"', 'http<br les/wee/clsco/axlGetPhoneInventory_creds.ph les/exec/clsco/axlGetPhoneInventory_creds.ph rl/modules/exec/clsco/axlGetPhoneInventory_cr	ed in 8 6://10.13.5', 'bttp://schemas', 1, 0) p(00): BoapClient->call('SelectEmbevice', Array p(00): BoapClient->BelectEmbevice('', Array) reds.php on line 00	,

RULE DEFINITIONS * Jitter Value Exce	reded	Please fill in all Name and Pattern	Telds Cancel	Update
dieco			Last 24 Hours +	٩
Click here for help building rules Build a New Defi	nition Manually	Displaying 1 - 10 of 154	942 events + first prev next last -	10 8
Events CALL_METRICS_IO @ Jitter @	CALL_JO · (new) ·			
Name	Pattern		10	
(new)				
Source Field				
Raw Log				
Pattern Type	Function	Value		
Plegular Expression Match/Extract 0	Norw			
(13×Jul 11 2018 21:51:01 Logger (77.54:0 PM (15:4:10 PM (15:4:20 PM (15:4:10 PM (15:4:10) P	<pre>: {'CINCD_NTMT_BERWICE': bata':1, "ReturnCode':'0', 'IzrozMessage':'',' ce', 'ElapsedTime':2958219, 'ServiceStatus':'1</pre>	UNC":"CUCM12","RisOe":"CUCM12","AssetName":"1 '}}	0.13.37.43°,'AssetDostzame'ı'	10.13.37.,

Regex Wizard		Cancel	Update	Regex Wizard	Cancel Update
1) Select a Log 2) Create Régis				1 Select et al. 2) Dense Reger	
Search for logs:				check versions 1.1 enough at ABO11 TookINTS-CIEFO employee the second	
• Disp	Last 24 Hour	n - mot last -	9	 CONSTRUME - CONSTRUCT Second style of CONSTRUME - SecONDLAR - CONSTRUME - - SECONDSTRUCTURE - Specification (CONSTRUME) - SecONDLAR - CONSTRUME - CONSTRUME - - SECONDSTRUME, SECONDST	Contract - Control -
<pre>47ml varsion*'1.0' secoding* 4EMTITY>20004*/INTITY>4EMTITY 01*/DEVICE>4EMOUPLARERX*/UND 4TP>137.0.0.3*/IN>-/WEMT>*/WEM 9ED0EVY>2000-1000085.1*/WEMT</pre>	08-84011 ****40015***1989***08000***88017* 08009**/28112** (08009**02112**000**010** 1954/28112**890**3112****001**************************	(18/0» (00015-80- parter/88/80 p- 4002149-</td <td></td> <td>[13] J. J. G. H. (201). Alth. J. M. (201). 207 (Controller tradies '11' '01' '01' '01' '01' '01' '01' '01</td> <td>ULD (1) PER-VALUET_MARK ETHNER-Lock IC (MERT_REPEARES VEREIDED (MERSAN) (MERT_VEREIDED und (MERT_VEREIDES</td>		[13] J. J. G. H. (201). Alth. J. M. (201). 207 (Controller tradies '11' '01' '01' '01' '01' '01' '01' '01	ULD (1) PER-VALUET_MARK ETHNER-Lock IC (MERT_REPEARES VEREIDED (MERSAN) (MERT_VEREIDED und (MERT_VEREIDES
<pre>«PORT»127.5.0.1:514«/INFO»400008><transport>400/0 «/END>400/PERT>4/0/PERT>4A3/04T «NONCO»40/PERT>4/0/PERT>4A3/04T «NONCO»40/PERT>4/0/PERT>4A3/04T</transport></pre>	SREEGE 127.0.0.14/ACCOREGOE (VINTOAL, 1994) CERENTING (ANNO CERETING (VICC) (VIANTO 1331) CERENG/ALTOITECH (VICC) (VIANTO 2001) SEIDE (ALTOITECH (VICC) (VIANTO 2001) SEIDE (ALTOITECH (VICC) (VIANTO 2001)	VIRTUAL IP REDS-/BIAR	H/BRN D-SBRD MADD	WHERE DOES THE WATCH REGIST Is there any test that investediotaly precedes your search? (Fa), enset in here or else leave this field block.	actude this test in my represent
GRADEN SOE TO STATE TO SERVICE TO CONTROL TO THE OWNER SOLAR 20 CONTROL TO THE OWNER SOLAR TO THE OWNER ADDRESS OF THE OWNER SOLAR TO THE OWNER ADDRESS OF THE OWNER OWNER SOLAR TO THE OWNER ADDRESS OF THE OWNER OWNER ADDRESS OF THE OWNER ADDRESS OF THE OWNER ADDRESS OF THE OWNER	b) 121 (2019) doi:10.1011/JALINE/KORDON-OMMELAS 10.81 (2011) doi:10.1011/JALINE/KORDON-OMMELAS 1.84 (2011) doi:10.1011/JALINE/KOMPLEAS 1.84 (2011) doi:10.1011/JALI	Pals;138(5. il););#48, ED GOUT_HOUTH MON*/ABBUT_N ED000 ED0	AND IN ANY ANY ANY ANY ANY ANY ANY ANY ANY AN	LIST ALL PHEASES YOU ARE TRANSG TO MATCH	**
Select log from the list above or paste	e log here:			Even a photose or resultable photoset you want to reacch. If you want to realch any photose leave this fixed balank.	lociale the test after their physics
Класски четалог (1, ° вноеццо) Класски ч	- UF-MALL (***00010**1.870**1.880*1.880*1. (************************************	0-01000000 0-01000000 000000 000000 000000 000000 00000		ETEP 4: WHERE BOOK THE SATISF ENDI is there are less that intervalidately follows provi anarch? If is, used here are else lesser this, field bland, BEERE	actuals that that as any capture () statch watt and of low (

5.1.3. Creating a Policy

To Create a Policy:

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

POLICY CONFIGUR	ATION	Rules	Filters		Chang	es have b	een mad	e .				Save
Policies Name Fail	over		Rule	s iame			Thresh	old	Window	Severity		Response Procedure
Asterisk Basic	-	5										
Cisco CUCMv8 to 11.5		447										
Cisca CUCMv8_r2 up		413										
Custom Security Policy		3										
Do NOT Delete - AJ		1										
LayerX LX1 SIP Error Messages		5										
Nortel 4.5 IPTFM (08/03/2010 1	9:45]	215										
Nortel 5+ IPTFM (08/03/2010 15	R(45) 🔽	215										
Sample Events		T										
Example Policy										Nor	ecords rules	+ first prev next last

5.1.4. Creating a Correlation Rule

To Create a new Correlation Rule:

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

WOSS		⊗ 4 1	精 🗐 🖞	۹. ۹	ê 🕹	••	👤 admin +
POLICY CONFIGURATIO	N Bules	Films Filmald	leids before saving an	nd make sure at rul	es have at least 1 de	finition	Save
Policies Name Failurer		Rules	Threshold	Window	Severity	Response Procedur	
Anna 201 Shall Amera		Differ Value Exceeded	16me	t minute	Crew	UHRCatToAlert	A1 = Z
Avaya PDS SPSLDG Alarms	11	Latercy Talue Excertion	d 16me	teritule	Creat	UniCalification	21
Case Cal Member	5	MOS NAME LOW	1846	1 minute	C Crisical	UniCalificAlert	21 - 2
LAVERt Agent Monitor		C Barrense for	and all the second	1.000	(D) const	a loss of the loss	
Log Monitor	T	Papers Los retor to	and and the second	1.0010	O costa	Crecartoven	
UII Call Monitor v2	5	Name	(real)				A0 = 4
Litt SIP Call Briefs val	6	Description					
Nortei Call Monitor	1						
PING Manitar	T						
Powerwave Shall? Narws	TT.	Type	Simple		Action	Track/Respond 8	
SLatraining policy	T	Threshold	1 10	Respo	nae Procedure	Select PP 4	
Test Alarm v1	T	Winter	1.000				
Al OperMental	5		1 100.00		manos Cospor	-	
ALSTOYBARN : Audin - Alert Exa.	(1)	Severity	International	-	Enabled		
ALSTOYBAIN : Galas - Nert Exa.	· 🐨				Inherit Output		
ALSTONBARN : NHC - Alert Dump.	10				iak Processing		
APC Powernet MIS Traps	-						
APER SOLID Alarm Test	T					Displaying 1 - 4 of 4 rul	es + first prev next last+
		-	c				

5.1.5. Creating a Definition

To create a new definition:

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

- No. 10.1 No.	Y CONFIGURA		the second se					
olicies			Rules					
Nam	e Failo	wer	Name	Threshold	Window	Severity	Response Proc	edure
Ciaco	Call Monitor		Jitter Value Exceeded	1 time	1 minute	Critical	LinkCal/ToAlert	23 -
	F Land Limiter	-						
LE DE	INITIONS = Jitter Va	ive Exceeded		-	Charges made		Cancel Updat	-
60						Last 2419	awa - Q	
here her	help builting rules Build a	New Definition M	unualy		Distant	1.10 of 156 bill month a first in	-	
1.00	TALL METHOD O	and CALL	0.0					
or ce ri ere	<130-241 11 2010 23-51-	di loggero d'ere	OD ATME SERVICE".					1
82410 PM	('Timestamp':155134583 .37.43', "AssetDescript	2, Wasofficers 11	Midgreen '1'10.13.37.43', 'Hanne'1'000	","AHC"+"CDOM13","N: N12","BHLYLOHBANH":"	inde":"COUNLI", "Ann "Clano Trace Collar	ert/have": "10.13.37.43", "have crises	(Bestrame") *10-13	
	man 127.8.0.1 Port-Meeting	Merrudola	Extract Field					
£2011/08	-METHODOG-Socket Cree	ited. Name I	Pris field					1
85410 PM	4/HETUMMAD		Statement Street					1
	August 27.8-0.1		1000					
67/11/18	RULE DEFINITIONS	S . Jitter Value	e Exceeded			Rease fill in all Name and Pattern 1	LADS .	Cancel Update
	cieco						Last 24 Hou	a- Q
		and the second	P. Company and C.					
	Chick here for herp building	ndes Duitd a Na	ne Definition Manually			Displaying 1 - 10 of 154	942 events + fint prev	rest lats 10 a
	Events CALL	METRICSJO	izer CALLUD (real					
	Name		Pattern.				181	
	(1004)							
	Source Reld		Local Contractions					
	Source Reld Raw Log		v.		Video			
	Source Field Raw Log Pattern Type Repair Expression Values 1 EXHIVES (*129-02) 1 EXHIVES (*129-02) 1	Torbact 1 2018 21:51141 ap 1151145422."	Function 1 Nove Longers (*C1000_HTMC_ADWICC*) MadCEbasts*1,2, *Meturibode*,***,1	1	Value	er" 1 "CHCH13" , "Ansen Same" 1 "1		ataan": 10.13.33.4
Income V	Source Held Rawing Pattern Type Popular Expression March 1556-0704 1556-0704 1556-0704 Extransf Extransf Extransf Extransf	Tednast 1 2018 21:51:61 mg*1151:36:822.* Trace Collection Fvalue:	Partition 1 Toris Degen: (*1000, Mrtd, samitict*) Martines*(*1*, *11.epsel1e*,*1*,*11.epsel1e*,*1*) Derent		Value K"+"CROKL3", "BLACK) Browny Wilson	e" 1"05003" , "AssertSame" (* 3) rd		arcane"; "(3,13,3),-
Regex V	Source Held Rate Log Pattern Type Repaire Expression March 1654-00 Mt 41 1654-00 Mt 41 1656-00 Mt 41	Totout 1. 2018 21:51:65 Trace Collection Twine:	Partition 1 Toris Degrees (* 12100, Arms, samvists*, Matchass*, *, * Bagenetites* (* 1319213,*) Dervice*, * Bagenetites* (* 1319213,*)	Toronoona and a star	Value ef * * CHOKLP*, * Russes Jo Rogens Witzer	e" : "05003" , "Assert Same" ; "3) rd 3) Onum Finger	. 13. 17. 47°, "Assertio	excess"+"18.13.33 Cancel Openet
Regex V	Source Held Res Lag Pattern Type Repair Expression March Source & Status Source & Status Source & Status Source & Status Source Held Vizard	Totout 1 2018 21:51:61 mp*1153:34:6422,* Trade Gellentian I Value:	Pantise 1 Tors J Tor	Trachesays", ",", "M Breekeekkas", "1", Update	Value R ⁺⁺ *CHORL2 ⁺ , *Runos Regex Witzer Classes etc., C	er" 1 "CRCRCL", "Assert Sume" 1" 21 rd 2) Over Fague	1.13.37.47°, 'teams	exame"+" 3.13.3) Cancel Upende
Regex V 1) Select 2	Source Held Rev Log Pattern Type Pegdar Expression March 155400 Mt 15720000 155400 Mt 1572000 Bottom 155400 Mt 1572000 Bottom Vizand	Tatsut 1 2018 21:51:61 ng: 1133 300822," Trate Gullernian Poline:	Pantise Pan	Trachuseys", ".", "M Bereloutestatus", ".", " Update	Value R ⁺ + ⁺ CHORE2 ⁺ , *Rank Person Value Commission of the second second second second second second second second secon	er" 1 "CRCCUU", "Assert Jame" 1" 1 nd 2) Conver Enger er 1.4" energinger "Okaditijt "Fort Schaff og den tijt, dender og det tij Schaff og den tijt, dender og det tij	1.13.37.43°, "Reserve (1.13.37.43°, "Reserve (1.13.17.43°), "Reserve (1.13.17.43°, "Reserve (1.13.17.43°), "Reserve (1.13.17.43°, "Reserve (1.13.17.43°), "Reserve (1.13.17.43°, "Reserve (1.13.17.43°), "Reserve (1.13.17.43°, "Reserve (1.13.17.43°), "Reserve (1.13.17.43°)	Cancel Upstale
Regex V 1) Select - Search for	Source Held Rev Log Pattern Type Pegalar Expression March 155400 Mt 15720000 155400 Mt 1572000 Bibliotom Vizand Nago	Fatuer 1 2018 21:51:61 ng: 11313.404022," Trates Gullerian Futues	Puntise 1 Torn J Tor	Transbusseys" - (* * * * *) Bereicheld aus * * 1 * * Update	Value R***cuck12*,*kuo Progen Witan *Chair second second action second action second second action second action s	er" ; "CICICLU", "Assert Jame" ; " u nd 2) Conver Enger = 1.4" assessing - Vik.Mitt ; "and conver enger = 1.4" assessing - Vik.Mitt ; and conver enger =		Cancel Upstale
Regex V 1) Select of Select her	Source Held Rev Log Pattern Type Pegdar Expression March 15000000 41574000 5 15000000 415740000 Wizard Nage Dep	Totaat 1 POIst 21:51:61 97:153336482," Trace Gullerijan Toblac	Puntise 1 Torn J Tor	Transbusseys" 1 ",", " M Bereicost Attan "," 1 ") Update Q 10 1	Value R ⁺ **cool.2*,**k.abo People Wiza *Chel wereas -description -	er" 1 "CICICLU", "Assert June" 1 "J nd 2) Conver Exper 2) Conver 2) Conver Exper 2) Conver 2) Conver		Cancel Upcole
Rogex V 1) Select A Search for *	Source Held Res Log Pattern Type Pegdar Expression March 1500000 41574000 5 1500000 41574000 5 Bibliog 250000 Allogo Nizard Dop Pegdar Schware Allogo Dag	Estruct 1. 2018 21:51:61 mp*1:51:14:1422,* Trainat: Trainat: trainat:	Puntise 1 Torn 1 Torn Longers (* 1200, Arm, 3800155*) Methods (* 17, 1800, Arm, 1800155*) Methods (* 120, 1800, Arm, 1800	Update CQ.	Value R ⁺ 1 ⁺ CROBL ²⁺ , *Rush Regex Wiza Regex Wiza Construction Regex Wiza Regex Wiza	er" (* "COOLU" - , "Anneet Jones" (* 1) nd 2) Onese Exper er 1. 4" anneeting - 10 Add(1) - Ford Construction Add(1) - Monta - Add(1) - Add(1) - Toront Construction Add(1) - Monta - Add(1) - Add(1) - Toront Construction Add(1) - Monta - Add(1) - Add(1) - Toront Construction Add	CTTO - (2010 - 40000 - 4011 - 13. 37. 42", " Marantum - 10. 13. 17. 42", " Marantum - 10. 12. 17. 42", " Marantum - 10. 12. 17. 42", " Marantum - 10. 17. 17. 17. 17. 17. 17. 17. 17. 17. 17	Cancel Upcole Cancel Upcole Cancel Upcole Control Co
Regex V 1) Second Search for emergence Standard of the emergence	Source Held Res Log Pattern Type Pegdar Expression Varus 1500000 41570000 100000 1500000 41570000 Bibliog 2500000 Allogo Dage excluse-1,11 escediage 2000000000000000000000000000000000000	Estruct 1. POIR 21:51:11 Trans Collection Prober Seging 1 - 15 of 2.56 desember - Sector 2.56 desember - Sector 2.56 desember - Sector 2.56	Puntise 1 Torn 1 Torn Longers (* 1200, Mm, 3800155*) Meditass*, * Trageontine* (* 3948135,*) Cancel Last 24 Hours - Cancel 1.253 Avents - fing pro-mod fast - 1.253 Avents - fing pro-mod fast -	Territowith at us ****	Value R***caceti2****kace * Regex Wiza * Linear to: * Check second * Chec	er" (* "COOLD" - "Anseet Jone" (* "J nd 2) Onese Exper er 1. 4" anseeding - 10 Add(1) - Teel Contractor Add(1) - March - 2001 (* 1. 4" anseeding - 10 Add(1) - Teel Contractor Add(1) - March - 2001 (* 1. 4" anseeding - 10 Add(1) - Teel Contractor Add(1) - March - 2001 (* 1. 4" anseeding - 10 Add(1) - Teel (* 1. 4" anseeding - 10 Add(1) - Teel (* 1. 4" anseeding - 10 Add(1) - Teel (* 1. 4" and 1) - Te		Cancel Upperform Cancel Upperform Statistics - Statistics Statistics
People V 1) Second V Second V Company V	Source Held Ret Lag Pattern Type Pegdar Expression Varus 1500000 41570000 Varus 1500000 41570000 Varus 1500000 41570000 Varus Ret Lag Ret L	Tatsud 1. Pole Jack of Annual Probations Probations Reging 1 - 10 of 2.06 off-annual to the second second second second second second second second second second second second second second second	Puntises Pun	Transformation (* 1977) Terrefordination (* 1977) Update Ol	Value ****cacoti2*****Lao ************************************	er"; "COOCUL", "Asseet Jame"; ", "J nd 2) Once Fage er 1.4" assesting "Or Addition Terrer Control of the State of the		Cancel Upperform Cancel Upperform Upperfor
Regex V I) Select a Second for the selection of the selection of the selection of the selection of the selection of the selection of the selection of the selection of the selection of the selection of the selection of the selection of the selection of the selection of the selec	Source Held Return Type Pettern Type Pettern Type Source Higher Expression Varus Source Higher Expression Varus Source Higher Higher Source Higher Higher Return Higher Return Higher Higher Return Higher	Tatsut 1. Pole Particle printi Statuto printi Statuto printi Statuto printi Statuto printi Statuto Statu	Purchas Purcha	Terricolousays"; ***, * Ma Terricolousau ***** Update	Value R ¹ ⁺	er"; "CICULI", "Asseet Jame"; ", "J nd 2) Charles Exper 2) Char	CITICA CONTRACTOR OF CONTRACTO	entraneer = 1 = 1, 3, 3) = + Cancel Upperform Upperfo
Regex V ty select of selects for selections select	Source Held Ret Log Pattern Type Pagain Typesons Marco 1500000 4150000 10000 1500000 4150000 10000 150000 4150000 Ret Log 250000 400000 Ret Log 250000 400000 Ret Log 250000 400000 Ret Log 250000 400000 Ret Log 250000 400000 Ret Log 250000 40000 Ret Log 250000 Ret Log 250000 250000 Ret Log 250000 Ret Log 2500000 Ret Log 2500000 Ret Log 2500000 Ret Log 25000000000000000000000000000000000000	Totsust 1. Pole Parsing 1. Pole Parsin	Purchas Purcha	Trachesays", " " " " Terricettatus" " " " " Update Q 19 19 10 10 10 10 10 10 10 10 10 10 10 10 10	Value R ¹¹ ¹ ¹ ¹ ¹ ¹ ²	w"," "CICULI", "Assert Jame", "," J rd 2) Charle Experimental States, "," J with 2) Charle Experimental States, "," J with 2) Charle Experimental States, ", States, and		ARTINGUE (* 18.13.3) Cancal Upperformation
Provide a second	Source Held Return Type Pettern Type Pettern Type Pettern Type Source Held Source Held So	Totsust 1. POINT PLANTER PLA	Purchas Purcha	Trachusaya", " " " " " Bereloethatus" " " " " Update Q 9 9 9 10 10 10 10 10 10 10 10 10 10 10 10 10	Value R ¹¹ ***********************************	e* + * * * * * * * * * * * * * * * * * *	CTTO - (2010) - (2010) - (2010) - (1) - (2) - (ers aaner ***13.13.33.* ers aaner ***13.13.33.* Ers aan ers
Pagetx V 1) Select - Search for emergence 4/DBCP * * * * * * * * * * * * *	Source Held Return Type Pattern Type Pagain Typesons Marco Source Held Source	Totsust 1. POINT PLANTER 1. POINT PLANTER PLA	Purchas Purcha	Trachesage"; " * " * " * * * * * * * * * * * * * *	Value R ^{ar} ²	e* + * * * * * * * * * * * * * * * * * *	CTT OF C (2010) 478 (2	ers aaner ***13.13.33.+ ers aaner ***13.13.33.+ ers aaner ***13.13.33.+ ers aaner ***13.13.33.+ ers aaner ************************************
Pani, v Pani, v Pan	Source Held Return Type Pettern Type Pettern Type Pettern Type Source Held Source Held So	Totsust 1. POINT PLANTER 1. POINT PLANTER Print Planter Print Planter Print Planter Print Planter Print Planter	Purchas Purcha	Trachesaar", " " " " Beretoetheter" " " " " Update Q 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Value R ^{ar} + ¹ ² (2001.2 ¹² , ⁴ Rada ¹) Internet ¹) Internet ¹ (Internet ¹) Internet ¹ (Internet ¹) Internet ¹) Intern	e* + * COOLS * * * * * * * * * * * * * * * * * * *	CTT OF 4 (2010) 497 (2	ers aanse" s "13, 13, 33, 4 ers aanse" s "13, 13, 33, 4 ers aanse" s "13, 13, 33, 4 ers aanse " s "13, 13, 13, 4 ers aanse " s "13, 13, 13, 13, 4 ers aanse " s "13, 13, 13, 13, 4 ers aanse " s "13, 13, 13, 13, 13, 13, 13, 13, 13, 13,
**************************************	Source Held Return Type Pettern Type Pettern Type Pettern Type Source Held Source Held So	Totsust 1. POINT STATES 1. POINT STATES Print States P	Parettee Parett	Update C. SectoreBatter * 3 * 1 Update C. S. SectoreBatter SectoreBatter Sectore	Value	** + * *******************************	CTTO - (2007) - (2007) - (2007) CTTO - (2007) - (2007) - (2007) CTTO - (2007) -	ertanse" (* 13. 13. 33. 4 ertanse" (* 13. 13. 33. 4 ertanse" (* 13. 13. 33. 4 ertanse ert
Phose ************************************	Source Held Return Type Pattern Type Pagain Typesons March Source Held Source	Totsust 1 0018 21:51:05 1 0018 21:51:05 Trace Oxileration (wider 1/wider 1/wid	Partition Partition	Update Reconstructions Reconstructions Update Update Update Update Update Update Update Update	Value	e* + * COOLS * * * Assert Keen* * * 21 rd 2: Charter Regin ** 1.4* assertion of the Add of 1 * Pert ** Table ** assertion of the Add of 1 * Pert ** Table ** assertion of the Add of 1 * Pert ** Table ** assertion of the Add of 1 * Pert ** Table ** assertion of the Add of 1 * Pert ** Table ** assertion of the Add of 1 * Pert ** Table ** assertion of the Add of 1 * Pert ** Table ** assertion of the Add of 1 * Pert ** Table ** assertion of the Add of 1 * Pert ** Table ** assertion of the Add of 1 * Pert ** Table ** assertion of the Add of 1 * Pert ** Table ** assertion of the Add of 1 * Pert ** Table ** assertion of the Add of 1 * Pert ** assertion of th	COLOR - 120-07 - 1 A REFERENCE COLOR - 120-07 - 1 A REFERENCE COLOR - 120-07 - 120-07 - 120-07 COLOR - 120-07 - 120-07 COLOR - 120-07 - 120-07 COLOR - 12	entranses" = "13, 13, 33, 4 Carrier Update Carrier Update C
Passi v ************************************	Source Held Return Type Pattern Type Pagain Typesons March Source Held Source	Tatuat 1 0018 2115110 1 0018 2115100 1 0018 2115100 10008 10	Partition Partition	C Tractionsature "1" Revoluced at us" "1" Update C TRECS States Manual P RESS States Non Manual P RESS States Non Manual P RESS States Non Manual P RESS States Non Manual P RESS States Non Manual Manual Manua	Value	e" + "COOLS", "Assert Same" + "J rd 2: Crase Report ** 1.4" assertion of the second	1. 13. 17. 47°, * Keneroli (1. 13. 17. 47°, * Keneroli (1. 13. 17. 47°, * Keneroli (1. 13. 17. 47°), * Keneroli (1. 13. 17°, * Keneroli (1. 1	entranses" = "13, 13, 33, 4 Carrier Update Carrier Update C
Press. v	Source Held Return Type Pattern Type Pagain Typeson Murity Source Held Source	Tatuat 1 0018 21151161 1 0018 21151161 Trace Collection 1000et 001-0011 Preference 001-0011 Preference 001-	Partition Partition	C Tractionsates ReveloceBatter * 1 * 1 Update C 1 1 1 1 1 1 1 1 1 1 1 1 1	Value	e* + * COOOL* * * Assert Same* * * 21 ed 20 Crase Report a* 1.4* seconds on * 04.4001* * etc 20 Crase Report a* 1.4* seconds on * 04.4001* * etc 20 Crase Report a* 1.4* seconds on * 04.4001* * etc 20 Crase Report a* 1.4* seconds on * 04.4001* * etc 20 Crase Report a* 1.4* seconds on * 04.4001* * etc 20 Crase Report a* 1.4* seconds on * 04.4001* * etc 20 Crase Report a* 1.4* seconds on * 04.4001* * etc 20 Crase Report a* 1.4* seconds on * 04.4001* * etc 20 Crase Report a* 1.4* seconds on * 04.4001* * etc 20 Crase Report a* 1.4* seconds on * 04.4001* * etc 20 Crase Report a* 1.4* seconds on * 04.4001* * etc 20 Crase Report a* 1.4* seconds on * 04.4001* * etc 20 Crase Report a* 1.4* seconds on * 04.4001* * etc 20 Crase Report a* 1.4* seconds on * 04.4001* * etc 20 Crase Report a* 1.4* seconds on * 04.4001* * etc 20 Crase Report a* 1.4* seconds on * 0.4* seconds a* seconds of the Report Report a* 1.4* seconds on * 0.4* seconds a* seconds of the Report Report a* 1.4* seconds on * 0.4* seconds a* seconds of the Report Report a* seconds of the R	1. 13. 17. 47. * Kennet (17. 10. 17. 47. * Kennet (17. 10. 17. 47. * Kennet (17. 10. 17. 17. 17. 17. 17. 17. 17. 17. 17. 17	entransee" = "13, 13, 33, 3 Carrier Update Carrier Update C
Press. v	Source Held Return Type Pattern Type Pagain Typeson Murity Source Held Source	Tatuat 1 2018 21:51:05 1 2018 21:51:05 Trace Collection 1/00/00 1/00/0	Partition Partition	Update Reconstructions Reconstructions Update Updat	Value	e" + "COOLS", " Assert See", * "J rd @Crase Segm * 1.4" second of the second second second * The second second second second * The second second second second second second * The second second second second second second * The second se	1. 13. 37. 47°, * Assertin 1. 13. 37. 47°, * Assertin 1. 13. 17. 47°, * Assertin 1. 13. 17. 47°, * Assertin 1. 11. 10. 17°, * 10. 17°, * 10. 18°, * 10°,	entransee" = "13, 13, 3, 3, 4 Carrier Upton Carrier Upton Carri

5.1.6. Deleting a Correlation Rule

To delete a Correlation Rule:

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

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

POLICY CONFIGURA	TION	ules	Filters					Save
Policies			Rules					
Name Failo	wer.		Name	Threshold	Window	Severity	Response Procedure	
Cisco Call Monitor	4		CLEARED - RFTR Alarm	1 time	1 minute	() Informational	AlertClear	27 = 2
LAYERK Agent Monitor	1			A Marco	10	(D) com	Alexandrated	
Log Monitor			CHINCAL - HPTR Adarm	Tone	20 minutes	Criedai	Merthold	
LICI Cali Monitor v2	3		DISREGARD - FailedNodes	16me	1 minute	() informational	DoNotAlert.	A1 = 2
LX1 SIP Call Errors v2	6		DISREGARD - UnableitoRun	16me	1 minute		DoNotAlen	×1 = ×
Nortel Call Monitor	20		INCOTTOMINATE, DOTO AL	1.000	15 seconda		Dalvethiert	
PING Monitor	2		and the second second					
Powerwave SNIVP Alarms	1		ISG Alarm trap - INDETERMI.	1 6me	1 minute	() Informational	DaNosAlert	×1 = <
SiLo training policy	1 12		ISG Alarm trap - MAJOR	1 time	1 minute	() Major	DoNotAlert.	P1 = 2
Test Alarm v1	DI		_	_		-		
AJ ExperiMental	V ()		-				Displaying 1 - 11	of 11 events + first prev next last +
- +			- + -					

5.1.7. Deleting a Policy

To delete a Policy:

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

allelas		Bules					
rolicies		Kules					
Name Fallove		Name	Threshold	Window	Sevenity	Response Procedure	
Cisco Call Monitor	4	CLEARED - RPTR Alarm	1 time	1 minute	D Informational	AlertClear	A1 = 2
LAVERX Agent Monitor	1	The second second stress		10.000	0	-	Contraction of the local division of the loc
Log Monitor	1	CRITEAL - HPTR Adarm	1 Dine	20 minutes	Critical	Merthold	
LX1 Call Monitor v2	1	OISREGARD - FailedNodes	1 time	1 minute	() Informational	DoNotAiert	25 E Z
LX1 SIP Call Errors v2		DISREGARD - UnableToRun	1 time	1 minute	() Informational	DoNotAiert	1 = 1
Nortel Call Monitor		INDETERMINATE - RPTR Ala	1 time	15 seconds		DoNotAlert	
PING Monitor	2				-		
Powerwave SNMP Alarms	1 n	ISG Alarm trap - INDETERMIL	1 time	1 minute	Informational	DoNotAlert	N1 = N
Sup training policy	1	ISG Alarm trap - MAJOR	1 time	1 minute	() Major	DoNotAlert	71 = 7
Test Alarm v1	1	ISS Alarm trag. MAIOR	Ltime	Louisute	(D) Marine	Dobotélect	
AJ ExperiMental	•	- isa warm dap i souton	1 price	1 mardine	a major	DONODICE	
ALSTOYBADN - Austin - Alert Exa.					0	Sisplaying 1 - 11 of 11 events	« first prev next last

5.1.8. Disabling and Enabling a Policy

To Disable and Enable a Policy:

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

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

POLICY CONFIGURATIO	ON Rules	Fitters Changes have b	een made				Save
Policies Name Fallover		Rules	Threshold	Window	Severity	Response Procedure	
Cisco Call Monitor		CLEARED - RPTR Alarm	1 time	1 minute	() Informational	AlertClear	27 = 2
LAYERX Agent Monitor	3	CONTRAL OPTO Alarm	1.000	10 minutes	(D) contract	Alexander	
Log Monitor		C CALIFOR INFINITION	1 1000	au menunes	Contract (Alterations	
LK1 Call Monitor v2	V 8	DISREGARD - FailedNodes	1 time	1 minute	() Informational	DoNotAlert	×1 = Z
LXT SIP Call Errors v2	6	DISRDGARD - UnableToRun	1 time	1 minute	() Informational	DoNotAlert	×1 = Z
Nortel Call Monitor			1 time	15 seconds		DoNotAlert	
PING Manitor	1	T mension a material			-		Content of
Powerware SNMP Alpres	11	ISG Alarm trap - INDETERML.	1 time	1 minute	() Informational	DoNotAlert	×1 = ×
Lo training porty	1.1	156 Alarm trap - MAJOR	1 time	1 minute	() Major	DoNotAlert	21 = 2
Testificares v1	T	ISG Alarm trap - MAJOR	1 time	1 minute	D Major	DoNotAlert	
Aj ExperiMental	Y ()	Per second and a second					
ALSTOYBARN : Aut IT - Alert Exa.					C	isplaying 1 - 11 of 11 events	+ first prev next last+
- +		- + -					

5.1.9. Cloning a Policy

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

To Clone a Policy:

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

olicies Name Faile	wer		Rules	Threshold	Window	Severity	Response Procedure	1
Cisco Call Monitor		(4)	CLEARED - RPTR A	arm 1 time	1 minute		NertOear	17 - 2
LAYERX Agent Monitor		3			20	(D) control	Alteretized	
Log Monitor		1	CHIRAL - HPIRA	arm 1 proe	20 minutes	Cribbas	Aleronolo	
LX1 Call Monitor v2		5	DISREGARD - Falle	dNodes 1 time	1 minute	Informational	DoNotAlert	<u>21</u> = <u>2</u>
LX1 SIP Call Errors v2		6	DISREGARD - Unat	sieToRun 1 time	1 minute	() Informational	DoNotAlert	21 = 2
Nortel Call Monitor		3		BOTD Ala 1 time	15 seconds		Doblethiart	A1 - 23
PING Monitor	V	1	- merrenerer.		14 1000 140			
Powerwave SHMP Algeres		11	ISG Alarm trap - IN	DETERML_ 1 time	1 minute	() Informational	DoNotAlert	A1 = 4
Lo training policy		1	15G Alarm trap - M	AJOR 1 time	1 minute	() Major	DoNotAlert	21 = 2
Test Alarm VI	,	T	ISC Alarm tran - M	A ICR 1 Sime	1 minute	(D) Malor	Doblocklast	41 - 23
AJ ExperiMental		3	- I recommended in	Ann i faur		Constant and a second s	Providence of the	
ALSTOYBARN : Austin - Det Et		-				0	Asplaying 1 - 11 of 11 events	« first prev next last

5.1.10. Import a Policy

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

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

POLICY CONFIGURATION	es Alters	Save
Policies Name Failover	Rules Name Threshold Window Severity Response Procedure	
Arda 🗹 1	Default AP	#2 = ×
Aspect UIP System Alerts 🛛 🗹 💈	Import Policies	
Asset Log Monitor	Select file to import	
Awaya Call Monitor	Choose File No file chosen	
Avaya PDS SNMP Alarms 🛛 👔 A		
Awaya PDS SYSLOG Alarms 🛛 13	Cancel Import	
Cisco Call Monitor		
LAYERX Agent Monitor		
Log Monitor		
Dtf Call Monitor v2		
DX1 SIP Call Errors v2		
Nortel Call Monitor		
PING Monitor		
Powerwave SNMP Alarms 11		
SiLo training policy 2		
Test Alarm VI		
A) ExperiMental		
ALSTOYBARN : Austin - Alert Exa 🗹 🤋		
ALSTOYBARN : Dalas - Alert Exa. 🗹 🤉	Disclosing 1, 1 of 1 m	IPS a first new part lists
		and a max pror these tools

5.2. Asset Configuration

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

5.2.1. Creating an Asset Group

To create a new Asset Group:

1. Click the Asset icon from the Menu bar.

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

ASSET CONFIGURATION					D	anges have been made	Save
Groups	Assets						
Group Name	IP Address	Auset Name	Description	Туря	Monitor Profile		
· BR All groups							
T BAL (S)							
> 🔄 🏭 Anda Asset Group 🔞							
a Aspect							
E Araya T							
Esco CM							
> Cate Network 15							
mattalar T							
Br Genhand							
GreatWest 24							
BE GROUP NAME							
E BayerX 3							
Bill LayerX, Lab 12							
BB LICI SIP Phones 2							
Bill Nortel 5							
B Optus							
> a Bu SLa training							
🔄 🏭 Telefonica 🚯							
in Televex (T)							
TELSTRA TCC-CP							
BB UCHOK 2							
all VM Tech 1							
> THE VOSS CUEDM 2							
🗌 🇰 Windows T							
🛄 🇰 Zain Babtain 💿							
i in Zein Kuwait							
(mm)	Filter		Sort IP Address			No records a	assets + first prev next last +

5.2.2. Adding an Asset to an Existing Group

To add a new Asset to a Group:

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

Group Name All groups All group Anda Asset Group Asset 4 Anda Asset 4 Anda Asset 4 Anda Asset 5 Cloco CM A	Assets IP Address 10.1.1.1 Properties Inat Maintenance M IP Addr	Asset Name AE_NAME terfaces	Description DESC0	Type Unknown	Monitor Profile No profiles set	22
Group Name All groups All groups All groups Arda Asset Group Asset 4 Avays 2 Cisco CM 4	IP Address	Asset Name AE_NAME rienfaces	Description DESCD	Type Unknown	Monitor Profile No profiles set	
All groups All groups All groups All groups Arda Asset Group Avays Avays Cisco CM Cisco	To.1.1.1	AE_NAME tierfaces	DESCO	Unknown	No profiles set	11
Arda Asset Group 3 Arda Asset 4 Avays 2 Cisco CM 4 Data Network 15	Properties In Ernet Maintenance M	nterfaces				
Arda Asset Group 3 Aspect 4 Aspect 2 Cisco CM 4 Data Network 15	Enab Maintenance M	Ned 🗹				
Aspect 4 Avaya 2 Cisco CM 4 Data Network 15	Enab Maintenance M	iled 🗹				-
Avaya 2 Bar Cisco CM 4 Bar Data Network 15	Maintenance M			Model		
Cisco CM	IP Add	ode		Version		
🕨 🗍 📷 Data Network 🛛 15	and the second sec	1855		MAC Address		
	Asset Na	ime		Alias		
ETISALAT 1	Descript	tion		Manufacturer		
Genband 1	Host Na	ime		Time Zone	UTC	
GreatWest 74		upe Uniconen		Customer		
I GROUP NAME		The Distribution				-
LayerX S	Addr	193		Sibe		-
LayerX Lab 12	External	URL				
ILX1 SIP Phones 2						
Nortel 5	/					
Optus 1	Elter		Sout IP Advises		interior 1 - 2 of 2 seasts . 6	et any and lar
				-		
Groups	Assets	A	Description	Time	Marches ProFile	
In All proves	TP ADDRESS	Asset Name	Description	type	Monitor Pronie	
The state	100.00	ALANNE	DISCO	Linknown	No protives set	
	Properties in	nerfaces				
P B Ards Asset Group 0	Name	IP Address	MAC Address	Vendor N	Iodel Version	-
Aspect 4	1					~
Awaya 2						
Cisco CM 4		+ -				
F Data Network 15						
ETISALAT 1						
Genband 1						
GreatWest 74						
B GROUP NAME						
_ @ LayerX 1						
ElayerX_Lab 12						
LX1 SP Phones 2						
Nortel 5						
E Optus 1	Filter		Sort IP Address 4	D	splaying 1 - 2 of 2 assets • fir	st prev next last

5.2.3. Deleting an Asset

To delete an Asset:

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

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	1 1
	10.13.37.194	LOLABO3		LayerX Node	No profiles set	1
Genband 1	10.12.37.206	TempAlert	Temperature Monitor	Unknown	1 profile set.	1 🖬
GreatWest 76	10.13.37.48	PextP	PeoriP System	Unknown	1 profile set	1 1
GROUP NAME 1	10.99.99.99	LinkIPToAlertTest	LinkdPToAlertTest	Unknown	No profiles set	
LayerX Lau 12						
Nortel S						
Optus 1						
> 🔁 🎒 SiLo training 🔞						
Telefonica 3						
Telmex 1	/					
TELSTRA TCC-CP						
UCtriX 2						
	Thurs .		Court 10 Automate A	Displayin	nel. 5 of 5 accest a fuel	new next last -

5.2.4. Deleting an Asset Group

To delete an Asset Group:

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

ASSET CONFIGURATION			6	mors exist	Save
Groups Group Name	Assets IP Address	Asset Name	Description	Type	Monitor Profile
P Data Network 15	10.5.7.3	test	test	Unknown	No profiles set 🛛 🗲 🗾
ETISALAT 1	10.199.161.11	is-prdimsD1a.gwl.com	VP DRS	Unknown	No profiles set 🖌 🖌
Genband 1	10.199.161.130	is-acrimaina1	DRS Main recorder	Unknown	No profiles set 🖌 🖌
GreatWest 74	10.199.161.131	is-acraeca1	DRS Secondary recorder	Unknown	No profiles set 🖌 🖌
LayerX 5	10.199.161.132	is-crsbrdigdra1	DRS CRS/Bridge	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 🖌 🗾
Dptus 1	10.199.161.50	dr-aes-crm	CRM TSAPIS	Unknown	No profiles set 🖌 🖌
> Esto training	10.199.161.57	dr-aam3-msging	DRS VM app srvr	Unknown	Nó profiles set 🖌 🗾
🖂 📾 Telefonica	10.199.161.58	is-assmaina1	DR Main AES	Unknown	No profiles set 🖌 🖌
Televis 1	Filter	9	ort IP Address 🕴	Displaying	1-20 of 74 assets + first prev next last+

5.2.5. Assigning a Probe to an Asset

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

To assign a Probe to an Asset:

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



MONITOR PROFILE » Norte	LCS1	K_BM				Cancel	Update
Groups		Templates/Profiles					
Probe Group		Name	Frequency	Credentials 1 & 2	Enabled		
= AA)	Name PING Probe		Finabled			
		Frequency		Minnediate?			
 Application ssh probe 	- 1	5 Minutes		Days			
- Aspect alarm demo	T	Credential 1		Sun V Mon V Tue V Wed V Thu	Pri 🔽 Sat		
		None					
Aspect CallCenter Service Probes	3	Credential 2					
- Asset Probe Test	T	None	+				

5.2.6. Assigning a Customer to an Asset

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

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

ASSET CONFIGURATION				Changes have been made	Save
Groups Group Name	Assets IP Address As	set Name Description	Туре	Monitor Profile	
Ards Asset Group Ards Asset Asset Asset Asset Coco CM A	Properties Interfa Enabled Maintenance Mode IP Address	122.168.1.3	Model Version MAC Address	Unknown Unknown Unknown	
Elisada Network 15	Description Host Name	Nortel CS 1000 BM	Manufacturer Time Zone	Nortel UTC	
	Type Address External URL	Server volos 8 Billings, Montana	Customer	Arda Virtual Customer 1 Arda Virtual Customer 2 Arda Virtual Customer 3 LayerX Virtual Customer 3 SiLo Custoemr 1	
Nortel 5	Filter	Sort IP Address		Displaying 1 - 5	of 5 assets + first prev next last
- +					

5.2.7. Placing an Asset in Maintenance Mode

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

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

ASSET CONFIGURATION					Charges have bee	m made	Save
Groups Group Name AJ 13	Assets IP Address Ad	set Name De	escription	Туре	Monitor Pri	offe	
Ards Asset Group 0 Aspect 4 Aspect 4 Claco CM 4 Cl	Enabled Maintenance Mode IP Address Asset Name Description Host Name Type Address External URL	I 192.168.1.3 Nortel, CS1K, BM Nortel CS 1000 BM nortel, SW Server voice Billings, Montana		Model Version MAC Address Allas Manufacturer Time Zone Customer Site	Unknown Unknown Unknown Unknown Nortel UTC		
Nortel 5	Filter	Sort IP	Address 8		Disp	playing 1 - 5 of 5 asset	s « first prev next last »

5.3. Probe Configuration

The Probes Configuration panel allows you to assign a group of scripts to an asset that can run on a set interval. These scripts will allow for data collection from many types of devices. The protocols can be API, SNMP or custom CLI scripts. The return data from the Probes can then be injected into the system for correlation or can be stored in the database to allow for analysis on the Dashboard/Reporting server.

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

Arbitrator Cisco PRI and SIP Probe Configuration

5.3.1. Creating a Probe Group

To create a new Probe Group:

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

VOSS		▲	۲	1	îţi		٩	1	Ĥ	*	-	٠	👤 admin v
PROBE CONFIGURATION		Errors exis	6										Save
Groups Group Name MUNY3LIPHODE		Prob	Name		Descripti	en	Unit		Command a	and Paramete	***		
New SNMP Query	17												
Nortel Call Path	$\langle \overline{v} \rangle$												
Cracle Service probes	3												
PexiP Configuration	17												
PING Monitor	1												
PING Probe	1												
ProbeTest	-												
RTT Probe	$\langle T \rangle$												
inmp test	5												
Static	T												
Temperature	5												
test	(\overline{r})												
Tracy PG	1												
Trunk Utilization	1												
Twitter	Ŧ												
Verware	5												
VmwareCreds	1												
Vess CUCDM	ĩ												
Windows Stats	14												
Tent													
0			•										

5.3.2. Creating a Probe

To create a new Probe:

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

	ON E	mors exist				Save
Groups		Probes				
Group Name mult/ValueProbe		Name	Description	Unit	Command and Parameters	
New SNMP Query	1	getCalPath	Nortel getCallPath		vqm/NortelGetCallPath.pl demo	1
Nortel Call Path	12				Custern	2
Oracle Service ombes	100			Auto-scale?	Select Category	
Deale Service probes	-	4			Avaya	0
Pesil' Computation		I			Select Script	
PING Monitor			/		Buey Doard	
PING Probe	(1)	/			Hostname/IP	
ProbeTest			/		Board	
ITT Probe						
sromp test	1					
static	T					
PROBE CONFIGURATION	ON E	mors exist				Sava
Groups		Probes				
Groups Group Name MUTOVAUEPHODE		Probes	Description	Unit	Command and Parameters	
Groups Group Name Mutovaue/wobe	t. Tr	Probes Name perCalPern	Description Nortel getCalPath	Unit	Command and Parameters	2
Groups Group Name MUEVAUEPROE New SMMP Query Nortel Call Path	T T	Probes Name getCalPoth	Description Notel getCalPath	Unit	Command and Parameters vom/Norte/GetCalPath.pl demo	
Groups Group Name MUEVAUEMODE New SNMP Query Nortel Carl Path Dracis Service protes	1. T T	Probes Name getCalPoth	Description Nortel getCalPath	Unit Auto-sceles ¹	Command and Parameters vom/Norte/GetCalPath.pl demo Custom Select Category	
Groups Group Name MUDVAULEWODE New SHMP Query Nortel Call Path Cracle Service probes Decth Configuration	1 (1) (1) (1)	Probes Name	Description Nortel getCaliPath	Unit Nuto scale?	Command and Parameters vgm/NortelGetCaliPath.pl demo Custom Select Category Awaya (Crede)	
Groups Group Name MUDVAUAHYODE New SNMP Query New SNMP Query Cracle Service probes PedP Configuration Class Measure	1 1 2 3 7	Probes Name	Description Notel getCalPath	Unit Auto-scale?	Command and Parameters vom/NortelGetCalPath of demo Custom Select Category Awaya (Crede) Select Script	
Groups Group Name FullSvalueProbe New SNMP Query Nertal Call Path Cracle Service probes PeodP Configuration PliNG Monitor	1 T T T T	Probes Name	Description Nortel getCalPath	Unit Autoscoleč	Command and Parameters vom/NortelGetCaliPath ol demo Custom Select Category Avras (Crodo) Select Script V arsas, roods softemay, Credo d/ getAvayaStations, credo sh	
Groups Group Name Rucovauerrose New ShMP Query Nortel Call Path Oracle Service probes Ped P Configuration PING Monitor PING Probe	1 7 2 3 7 1 1 7	Probes Name getCalPeth	Description Nortel getCalPath	Unit Auto scale?	Command and Parameters vom/Norte/GetCal/Path.pl demo Custom Select Category Avaya (Crode) Select Script V avaya, noise judiening, Crede.of getAvayaStations, crede.of getAvayaStations, crede.of getAvayaStationa, crede.of getTupResource, crede.of	
Groups Group Name MUDVAUEPPODE New SHMP Query Nortel Call Path Dractel Service probes PedP Configuration PING Monitor PING Probe ProbeTest	1 (1) (2) (3) (3) (4) (4) (4) (4) (4) (4) (4) (4) (4) (4	Probes Name gerCalPoth	Description Nortel getCaliPath	Unit Auto-scale?	Command and Parameters vom/NortelGetCalPath pl demo Custom Select Category Awaya (Crede) Select Script V arays, tracts, screte, sh getDynastations, screte, sh getDynastations, screds, sh getThunkGroup, creds, sh	
Groups Group Name WubvaueWooe New SHMP Query Nortel Call Path Coracle Service probes PedP Configuration PHNG Monitor PHNG Probe ProbeTest RTT Probe	1 1 2 3 3 1 1 1 1 1 1 1 1 1 1 1 1 1	Probes Name	Description Nortel getCaliPath	Unit Nutro scate?	Command and Parameters vgm/NortelGetCalPath pl demo Custom Select Category Awaya (Crede) Select Script V getAwayStations, creds. sh getThurkGroup, creds. sh	
Groups Group Name PrubNoueHode New SNMP Query Nortal Cal Path Dracte Service probes PedP Configuration PING Monitor PING Monitor PING Probe ProbeTest RTT Probe somp test		Probes Name	Description Nortel getCalPath	Unit Auto-scalee	Command and Parameters vgm/NortelGetCaliPath pi demo Custom Select Category Avaya (Crede) Select Script V avaya (Crede) Select Script V avaya stations, creds.sh getDapResource_creds.sh	

5.3.3. Creating a Custom Probe

To create a new Probe:

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

PROBE CONFIGURATION	Er	rrors exist				Save
Groups Group Name		Probes Name	Description	Unit	Command and Parameters	
Awaya Utilization Demo	1	Pre Policy IB Pkts	Pre Policy IB Pkts		genRandom pi 4000 6000	1
Avaya VQM Statistics	6	Pre Policy OB Picts	Pre Policy OB Picts		genRandom pi 4000 6000	
	7	Drop Packets	Drop Packets	kB	genRandom pl 200 350	2
	7			1	t 🗹 Cussom	
CDR Ndx Demo	3		/	Alton		
Cisco ASA SMMP Table Probe	1	/	-		/	1
Cisco CBQos	5			-		
Cisco CUCM Device Location	-					
Gisco CUCM PerfMon Counters	(0)					
Cisco CUCM Phone Inventory - 10.13.37.	(T)					
Cisco Finesse	2	-				

5.3.4. Deleting a Probe Group

To delete a Probe Group:

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

Q V0SS	4	8	4	î ļ î		٩	2	Ĥ	*	2	٠		👤 admin -
PROBE CONFIGURATIO	N D	mors exist											Save
Groups Group Name		Probes		D	escription		Unit		Comma	nd and Par	ameters		
Avaya Utilization Demo	1	Pre P	olicy IB Piets	P	e Policy IB	Pies			gerRand	iom.pl 4000	6000	1	
Awaya VQM RTCP Demo	(2)	E PreP	olicy OB Pies		e Polky OB	Pies			genRand	lom pi 4000	0000	1	
Awaya VQM Statistics	(6)	-			Rate				perfland	om pl 2100 :	400		
CCMM 6	2						14						
CCMS 6	41	Drop	Packets	0	rop Packets		10		genRand	iom.pl 200 3	10	1	
СТ 6	7											1	
CDR Ndx Demo	1												
Cisco ASA SIAMP Table Probe	T												
Cisco ASA Stats	2												
Cisco CBQos	5												
Cisco ROCM Device Location	T												
CISCO CUCM LX-RTMT		-											
- + @		- +											

5.3.5. Deleting a Probe

To delete a Probe:

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

QV0SS	▲	۲	4	†††		٩	2	Ĥ	*		٠		👤 admin 🗸
PROBE CONFIGURATION	Err	ors exist											Save
Groups Group Name		Probes			Descriptio	n	Unit		Comma	ind and Para	ameters		
Aveya Utilization Demo	T	Pre Po	licy IB Plets		Pre Policy I	Piets			genRand	tom.pl 4000 6	000	1	
Awaya VQM RECP Demo	2	Pre Po	iky OB Pie		Pre Policy C	8 Piets			genRand	tem. pl 4000 6	000	1	
Awaya VQM Statistics	6				Dit Rate				gentland	lam.al 2100 2	400	-	
CCMM 6	1	-	a linte		Dana Bastin				-			-	
CCMS 6	41	-	acard		Undp Hacke				Towns	10m.pr 200 85	N	-	
CCT 6	7											1	
CDR Ndx Demo	(1)												
Cisco ASA SNMP Table Probe	1												
Cisco ASA Stats	2			1	r .								
Cisco CBQos	5		/										
Cisco CUCM Device Location	1	-											
Cisco CUCM LX-RTMT	-	-											

5.4. Controls

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

5.4.1. Creating a Control

To create a new Control:

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

8. Click Save icon.

V 0SS	🔺 🛞	4 १८१	III 🥄	<u>a</u> 🔒	2 🖬	٠	👤 admin-
CONTROLS	Errors exist	robes					Save
	Name	Command and	d Parameters		Protection		
	PEAK-AspectDB	aspect/bidwAler	tinsert.pl		Off	1	
	PushToZenoss	zenoss/zenossN	lew.php '1.1.1.1' 'abc12	3' 'abc123' '0'	Off	1	
	Reboot machine	generic_ssh.exp	%s 'reboot' '22'		Off	1	
	ReporterPush	ReporterPush 10	0.13.37.128:65515 tru		off	1	
	SendToEM7	sciencelogic/api	AlertToEm7_creds.pl **	0.1.1.1"	off	1	
	show running	cisco_pix_cli.exp	76.198.119.129' 'sho	v running'	off	1	
	Test Fiber Link	avaya/command	d.pl %s testfiber %s		off	1	
	Trace Route	avaya/command	d.pl %s tracert %s %s		On	1	
	Tracy_Control	avaya/command	d.pl '10.13.37.241' 'pin	ip' '10.13.37.241' '2'	off	1	
	USAN Reporter Forward	ReporterPush 10	0.10.100.101:65515 tr	e	Off	1	
	Voice-Email	alert2Email.ph	193.35.222.39 smartp	oint@cambridgeconsu	itants Off	1	
	VossQuery	voss/vras8.sh			Off	1	
		Custom				-	
		Select Category	r		_	10.000	
		Aspect		1	_		
		Select Script			_		
		Aspect BIDW E	vent Queue Insert				
javascript.;							

5.4.2. Deleting a Control

To delete a Control:

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

Name	Command and Parameters	Protection	
AlertClear	alerts/ackAlert.php	Off	1
AlertClear	alerts/ackAlert.php	Off	1
AlertHold	alerts/checkAlert.php	Off	1
AlertHold	alerts/checkAlert.php	Off	1
Aspect SalesForce	aspect/aspectForceInsert5oap.php 'filename.wsdi' 'username' 'pas	Off	1
Avaya FD' MED-GTWY	avaya/fix_avaya_MED-GTWY.pl %s %s %s %s	Off	1
Blink	blink.siv	017	
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

5.5. Response Procedure Configuration

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

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

5.5.1. Creating a Response Procedure

To create a response procedure:

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

- 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.

🔍 VOSS 🛛 🔺	8 / 11 🗐 🥄 Jz 🔒 📥 👄 🗢	1 admin
ESPONSE PROCEDURE C	INFIGURATION	Save
esponse Procedures	A second sector to the second s	
Name	Anguine muchane verans	
CENS-Stan Test	Aert Disable on Fallover	
Default IRP	Methods	
DukesAiert	From: arbitrator@layendach.com Tix support@layendach.com Smp Server:	email email
Gruil estrobel	Control Reboot machine # Delay Desconds #	
Enal, Arda	Credential 1 admin 1 Confirm Timeout 30 seconds 1	
Deceletion Dumple	Untertain 2 Note 1	Controls
Falover ACTIVE	Control LinkPTpAlert 2 Delay Diseconds 8	
Falover STANDBY	Credential 2 None 2 Centre Timeout 30 seconds 8	
Fest Bank 26x7	Destination 10.00.010 As Land 2	Forward
Just Airt	And a state of the	101111
LayerX Support		
UniCalifumToAlert		
UNCATINET	+ Email + Control + Rowarder	
UniPlatet	and Restored Relationed	
LinksPToAlert - Do Not Post Alert	Do Not Run Windows	
LinkPToAlett - Post Alett	See Proof 5 100 5	
LinkProbeToAlert		
Local Alert ONLY		
PAN OS Decrypt		
PEAKtoAspect08		
Push to Reporter		
Rebost Machine		
SendfoEM7		
Svit Isarigie		
Tracy, ResProdecure		
USAN Response		
Test		

5.5.2. Assigning an Alert to a Response Procedure

To assign the Alert function to a response procedure:

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

SVOSS 🛛	▲ ⑧ / 餠 圖 < 注 A 土 @ ◇	1 admin -
RESPONSE PROCEDURE	CONFIGURATION	Save
Response Procedures	Response Procedure Details	
	Alert Disable on Fallover	
CCMS-Sue fest	Methods	
Default inte	Fram arbitrary drayentech.com Ta: supportiliayentech.com Smtp Server:	
Durenter	formal financiana a	
Cruil estrobel	Createry 1 admin 2 Delay Diseconds 1	
Drai,Ada	Credential 2 Nane 8 Confirm Timeout 30 seconds 8	
Disalution Exemple	Central LossPfloRet 8	
Talover ACTM	Despertar 1 admin 8 Cardian Tenning Desay	
Falser STANDBY	Dedential 2 Name 8 Control Interior ad Michael 4	
End Bank 24x7	Destination: 10.10.2.10 As Event? 🗹 🔽	
Distant.		
C Layert Support		
UnCirtumfuter		
UniceTokint	+ Email + Control + Forwarder	
UnitToAint	Particle Sections	
LinkePflaAlert - Dis Not Pest Alert	Ban Frita 1 Jan 1 00 1	
UnitPlaAen-Post Aen	Feel Surviver 8 12am 8 00 8	
LinkProbellaRet	and manual and manual and an	
Crical Alert DRLY		
TANK OS Decrypt		
PEAKDAspect08		
Push to Reporter		
Rebost Machine		
SendfotM7		
Dift.buriyie		
Tray, Reshoteoure		
USAN Response		
Test.		

5.5.3. Deleting a Response Procedure

To delete a Response Procedure:

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

Response Procedures	Response Proces	dure Details			
Avaya Fix MED-GTWY CCMS Stat-Test Default 188	Methods	Disable on Fallover	To: tier1@company.com	2	
DoNotAlert Email vebrobel Email Ages	+ Ema	il + Control + Forwarder			
Failover ACTIVE Failover STANDBY First Bank 24x7	Do Not Run Wi	ndows			
Just Alert					

5.6. How to Enable ServiceNow Intergration

Name	Command and Parameters	Protection
LINKIPTOAlert	LINKIPTOAlert	off 🥒
Reporter Push Reading	ReporterPush 172.30.15.121:65515 true	Off 🖉
ReporterPush-GC	ReporterPush 172.25.87.6:65515 true	off 🖉
VpnSyslog	vpnSyslogAlert.sh	Off 🖉
	Custom	
	Select Category	
	ServiceNow 🗸	
	Select Script	
	PushToServiceNow V	
	Service Now IP Address / Hostname	
	Service Now Username	
	Service Now Password	

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

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

5.7. ServiceNow One Way Incident Integration

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

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

5.7.1. ServiceNow Requirements

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

5.7.2. Arbitrator Correlation Configuration

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

- PASSWORD

5.7.3. Scree	enshots From	ServiceNow
--------------	--------------	------------

	lanagement	🤀 System Administrator 👻	< 다 ? 🕸				
Filter navigator	< Incident INC0010023	● 小 芸 ∞∞ Follow ■ Update Resol	ve Delete 🔨 🔨				
	Configuration item	Q Assignment group Q					
My Assets		Assigned to Q					
My Notification Preferences	* Short description	LXTALERT: ARB_REFERENCEID=20000-01009001-00-01-7134-14 ARB_POLICY_MODULE=MultiTest ARB_CORRELATION_RULE=Some Rule	8				
Guided Setup		Related Search Results V					
Service Desk	vice 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						
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	Preview Attach				
i Assigned to me			Autor				
Open K	Notes Related Records	Closure Information					
Open - Unassigned	Watch list	B B Work notes list B					
Resolved	Additional comments						
All	(Customer visible)						
Critical Incidents Man		Work notes Post					
Problem	Activity	System Administrator 2016-12-13 12:52:14	∇				
1 Change		XTALERT: ARB_REFERENCEID=20000.01009001.00.01.7134-14 ARB_POLICY_MODULE=MultiTest ARB_CORRELATION_RULE=Some Rule ARB_MESSAGE=Some Rule : Multitest (2)					
Configuration							
Password Reset		Image: System Administrator 2016-12-13 12:52:14					
Service Catalog		Impact 1-High Incident state New Description State Sta					
Item Designer		Opened by System Administrator Priority 1- Critical					
	anagement	🤤 System Administrator 👻	< 다 () 🕸				
Filter navigator	E Incidents New G	io to Number V Search V 44 4 11 t	o 20 of 75 🕨 🕨				
	Ø ■ Numb	er ▼ ≡ Opened ≡ Short description ≡ Caller ≡ Priority ≡ State ≡ Category ≡ Assignment group	■ Assigned to =				

, 🕎 Filter navigator)	■ In	cidents	New Go to	Number	▼ Search				\checkmark	44 4 1 to	20 of 75	••	
• * ()		Ø		■ Number ▼	■ Opened	■ Short description	Caller	■ Priority	≡ State	■ Category	■ Assignment group	■ Assigned to	.0 .	
My Assets			(j)	INC0020001	2016-08-10 09:14:29	test	<u>System</u> Administrator	3 - Moderate	New	Inquiry / Help			20 09	
My Notification Preferences						LXTALERT: ARB_REFERENCEID=20000-								I
Guided Setup			(i)	INC0010023	2016-12-13 12:52:14	01009001-00-01-7134-14 ARB_POLICY_MODULE=MultiTest		• 1 - Critical	New	Software			20 12	
Service Desk						ARB_CORRELATION_RULE=Some Rule								
Incident	L					LXTALERT: ARB_REFERENCEID=20000-								
Create New			i	INC0010022	2016-12-13 12:52:11	01009001-00-01-7134-16 ARB_POLICY_MODULE=MultiTest		😐 2 - High	New	Software			20 12	;
Assigned to me						ARB_CORRELATION_RULE=Some Rule Major								
Open						LXTALERT: ARB_REFERENCEID=20000-								
Open - Unassigned			(i)	INC0010021	2016-12-13 12:52:08	01009001-00-01-7134-19 ARB_POLICY_MODULE=MultiTest		5 - Planning	New	Software			20 12	
Resolved						Rule Info								
All						LXTALERT: ARB_REFERENCEID=20000-								
Overview			(i)	INC0010020	2016-12-13 12:52:04	01009001-00-01-7134-18 ARB_POLICY_MODULE=MultiTest		4 - Low	New	Software			20 17	
Critical Incidents Map						Rule Minor								
Problem						LXTALERT:								

5.8. Credential Configuration

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

5.8.1. Creating a Credential

To create a Credential:

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

REDENTIAL CONFIGURATIO	UN CITUIS CARSE			
Name	Username	Password	Confirm	-
	*******	*******		2
SiLo Test Cred		*******	*******	
snmp community public	*******	*******	*******	1
SNMP RO String	*******	*******	*******	× .
Tandburg	********	*******	*******	1
UCAXLAPI	*******	********	*******	× .
VOSS API	*******	********	*******	1
Windows Agent probe	*******		*******	× .
				~

5.8.2. Deleting a Credential

To delete a Credential:

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

Labert M Tcreas	Username	Password	Confirm	
LxtAutoGen 1489019854046		********		-
LXTREADONLY	********	********	********	1
SiLo Test Cred	*******	********	********	1
snmp community public	*******	********	********	1
SNMP RO String	********	********	********	1
Tandburg	*******	********	*******	-
UCAXLAPI	*******			1
VOSS API	*******	********	********	1
Windows Agent probe	*******	********	*******	1

5.9. Customer Configuration

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

(See: Asset Configuration, Access Control Configuration).

5.9.1. Creating a Customer

To create a Customer:

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

CUSTOMER CONFIG	URATION		Save
Customers		Sites	
Ardia Virtual Customer 1	2		
Arda Virtual Customer 2	2		
Arda Virtual Customer 3	2		
LayerX Virtual Customer	1		
SLo Custoemr 1	7		
test	1		
1/			
E 1		E •	

5.9.2. Creating a Customer Site

To create a site for a Customer:

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

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

5.9.3. Deleting a Customer

To delete a Customer:

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

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

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

5.9.4. Deleting a Customer Site

To delete a site for a Customer:

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

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

5.10. Access Control

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

5.10.1. Permission Groups

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

Creating a Permission Group

To create a Permission Group:

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

Group Name	Realm Context	Timeout		
Science Logic	(local)			1
SuperUser	(local)			1
Admin	(local)			1
SiLo Test	(local)			1
Guest	(local)			1
Typical	(local)	2		1
Monitor	(local)	2		1
Test Permissions Users	(local)	1 -	/	
Test Permissions Users	(local)	alytiX :: Correlate	/	
Test Permissions Users VIEW - Main Application	(local) And VIEW - Asset Explorer	alytiX :: Correlate	VIEW - Pung Search	
Test Permissions Users VIEW - Main Application VIEW - Policy Monitor	(local) Ani VIEW - Asset Explorer VIEW - Asset Map Explorer	alytiX :: Correlate VIEW - Alarm Analyzer VIEW - Call Details	VIEW - Pung Search VIEW - Call Path Monitor	
Test Permissions Users VIEW - Main Application VIEW - Policy Monitor ACTION - Delete Calls	(local) And VIEW - Asset Explorer VIEW - Asset Map Explorer ACTION - Delete Paths	alytiX :: Correlate VIEW - Alarm Analyzer VIEW - Call Details ACTION - Disposition Alerts	VIEW - Pung Search VIEW - Call Path Monitor	
Test Permissions Users VIEW - Main Application VIEW - Policy Monitor ACTION - Delete Calls	(local) And VIEW - Asset Explorer VIEW - Asset Map Explorer ACTION - Delete Paths And	alytiX :: Correlate VIEW - Alarm Analyzer VIEW - Call Details ACTION - Disposition Alerts ayltIX :: Configure	VIEW - Pung Search VIEW - Call Path Monitor	
Test Permissions Users VIEW - Main Application VIEW - Policy Monitor ACTION - Delete Calls VIEW - Main Application	(local) Ani VIEW - Asset Explorer VIEW - Asset Map Explorer ACTION - Delete Paths Ania VIEW - Policies	alytiX :: Correlate VIEW - Alarm Analyzer VIEW - Call Details ACTION - Disposition Alerts ayltIX :: Configure VIEW - Assets	VIEW - Pung Search VIEW - Call Path Monitor VIEW - Probes	
Test Permissions Users VIEW - Main Application VIEW - Policy Monitor ACTION - Delete Calls VIEW - Main Application VIEW - Controls	(local) And VIEW - Asset Explorer VIEW - Asset Map Explorer ACTION - Delete Paths And VIEW - Policies VIEW - Response Procedures	alytiX :: Correlate VIEW - Alarm Analyzer VIEW - Call Details ACTION - Disposition Alerts ayltiX :: Configure VIEW - Assets VIEW - Credentials	VIEW - Pung Search VIEW - Call Path Monitor VIEW - Probes VIEW - Customers	

Assigning and Removing Users to and from a Permission Group

To Assign a User to a Permission Group:

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

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

5.10.2. Users

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

Creating a New User

To create a new User:

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

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

Full Name Username Password Confirm Email Super-User Force Password Change Locked Out Administrator admin ******** afrosch@layerstech.com ******** afrosch@layerstech.com ******** ******** afrosch@layerstech.com ********* ************ ******** ******** ******** ******** ************************************	ilte	4		Sort Fu	II Name 🕴	-	1	1	
Administrator admin ******** afrosch@ilayerstech.com Image: Comment of the second of the seco		Full Name	Username	Password	Confirm	Email	Super-User	Force Password Change	Locked Out
Alain Jansen ajansen ******** ajansen@layerxtech.com Image: Customer afrosch@layerxtech.com Image: Customer Imag		Administrator	admin	******	********	afrosch@layerxtech.com	5		
Andrew Frosch afrosch ••••••••• afrosch Ølayerstech.com Image: Customer asavran@layerstech.com Image: Customer I	1	Alain Jansen	ajansen	*******	********	ajansen@layerxtech.com	1		
Arda Savran asavran@layerxtech.com Image: Comment of the savran@layerxtech.com Ima		Andrew Frosch	afrosch	********	********	afrosch@layerxtech.com			1
Guest Account guest ******** support@layerstech.com Image: Comparison of Compar	1	Arda Savran	asavram	********	********	asavran@layerxtech.com	23		
layerx layerx ******** support@layerxtech.com Image: Comparison of the support@layerxtech.com Image: Comparison o		Guest Account	guest	********	********	support@layerxtech.com			1
testing testing2 testing2 support@layerxtech.com Image: Comparison of the compariso	1	layers	layerx	********	********	support@layerxtech.com	12		1
testing2 testing2 <td< td=""><td>3</td><td>testing</td><td>testing</td><td>*******</td><td>********</td><td>support@layerxtech.com</td><td>5</td><td></td><td></td></td<>	3	testing	testing	*******	********	support@layerxtech.com	5		
View Dnly viewonly •••••••• view@layerxtech.com Image: Comparison of the second	1	testing2	testing2	*******		support@layerxtech.com	23		1
Vodafone voda ******** support@layerxtech.com Image: Customer ******** wstrobel@layerxtech.com Image: Customer Image: Customer </td <td>3</td> <td>View Only</td> <td>viewonly</td> <td></td> <td>********</td> <td>view@layerxtech.com</td> <td></td> <td></td> <td></td>	3	View Only	viewonly		********	view@layerxtech.com			
wstrobel wstrobel ******* wstrobel@layerxtech.com 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	1	Vodafone	voda	*******	********	support@layerxtech.com			
Customer	1	wstrobei	wstrobel	********	********	wstrobel@layerxtech.com	22		1
Customer									
		Customer		± Disa	ble multi tenancy				/
	ber	-Users can do an	sything in any co	ntext.					

Deleting a User

To delete a User:

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

5.10.3. Nodes

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

Creating a Node

To create a Node:

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

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

5.10.4. Realms

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

Creating a Realm

To create a Realm:

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

Name	
Deployment	× 1
LayerxDev	
	V
/	/
Devices in Realm	All Devices
	devarb
- Drag	demoarb
	ePlus
	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.

5.10.5. Protected Subnets

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

Creating a Protected Subnet

To create a Protected Subnet:

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

5. Click the Save button to save your changes.

Deleting a Protected Subnet

To delete a Protected Subnet:

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

Name	IP Address	Mask	
internal_172_16	172.16.0.0	255.255.0.0	× .
ANA1918_192_168	192.168.0.0	255.255.0.0	
Google (subnet 5)	66.102.0.0	255.255.240.0	1
Google (subset 4)	72.14.192.0	255.255.192.0	1
internal_1	192.168.103.0	255.255.255.0	 Image: A set of the set of the
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	2
internal_141	192.168.141.0	255.255.255.0	1
Google (subset 2)	209.185.108.129	255.255.255.128	1
IANA_10	10.0.0.0	255.0.0.0	× .
Google (subset 3)	64.68.88.0	255.255.248.0	2
LOOPBACK	127.0.0.0	255.0.0.0	× .
ANA1918_172_16	172.16.0.0	255.240.0.0	2 C
internal_135	192.168.135.0	255.255.255.0	2
68.91.33.96	68.91.38.98	255 255 255 255	
76.198.119.129	255.255.255.128	255.255.255.128	
APIPA_168_254	169.254.0.0	255.255.0.0	
internal_3	192.168.1.0	255 255 255.0	1
internal_125	192.168.125.0	255.255.255.0	
		255.255.255.255 \$	

5.10.6. Password Policy

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

Creating a Password Policy

To create a Password Policy:

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

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

5.10.7. SAML

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

Creating single sign-on via SAML

To create single sign-on via SAML:

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

Enable SAML	
Disable Multi Tenancy	
SAML Signature Algorithm	shat +
Attribute Mappings	
Email (Optional):	
Username (Optional):	
First or Display Name (Optional):	
Last Name (Optional):	
Identity Provider Metadata XML * Required	
Paste your metadata XML here	
Service Provider Information Provide this information to your ide	ntity Provider
Service Provider Information Provide this information to your ide Audience URI (SP Entity ID):	ntily Provider
Service Provider Information Provide this information to your Ide Audience URI (SP Entity ID): Single Login URL:	ntity Provider http://demoarb.layerxtech.com/sami2/module.php/sami/sp/metadata.php/default-sp http://demoarb.layerxtech.com/sami2/module.php/sami/sp/metadata.php/default-sp
Service Provider Information Provide this information to your ide Audience URI (SP Entity ID): Single Login URL: Single Login URL:	ntily: Provider http://demoarb.layerxtech.com/sami2/module.php/sami/sp/metadata.php/default-sp http://demoarb.layerxtech.com/sami2/module.php/sami/sp/sami2-acs.php/default-sp http://demoarb.layerxtech.com/sami2/module.php/sami/sp/sami2-logout.php/default-sp

Iseable Multi Tenancy Image: Seable Multi Tenancy MML Signature Algorithm sha1 Attribute Mappings sha1 mail (Optional): sername (Optional): rst or Display Name (Optional): SAML Metadata XV Primit Westions *1.0*2* Control (Control): exit Nome (Optional): SAML Metadata XV Primit Westions *1.0*2* Control (Control): exit your metadata XV Contro): <th>Enable SAML</th> <th></th> <th></th> <th></th>	Enable SAML			
AML Signature Algorithm sha1 ttribute Mappings mail (Optional): sername (Optional): set Name (Optional): ast Name (Optional): CondEntity Provider Metadata XI Required ast Name (Optional): CondEntityOpeor/plotr xmins:md="um:casis:names:tc:SAML:2.0:metadata" xmd::ds:ds:ds:ds:ds:ds:ds:ds:ds:ds:ds:ds:d	isable Multi Tenancy			
ttribute Mappings mail (Optional): seemame (Optional): seemame (Optional): seemame (Optional): set or Display Name (Optional):	AML Signature Algorithm	sha1		
mail (Optional): sername (Optional): rst or Display Name (Optional): SAML Metadata XI Required set Name (Optional): SAML Metadata XI Required set your metadata XIML here	ttribute Mappings			
sername (Optional): rst or Display Name (Optional): ast Name (Optional): Itentity Provider Metadata XIR Recuired aste your metadota XML here	imail (Optional):			
rst or Display Name (Optional): Ast Name (Optional): SAML Metadata XM Required sate your metadata XML here Commensation XML here Com	Username (Optional):			
ast Name (Optional): SAML Metadata XIX Required	First or Display Name (Optional			
<pre>sete your metadata XX Required paste your metadata XXIL here <??mti version="1.0"?> cmd:EntityDescriptor xmtins:md="um:oasis:names:tc:SAML:2.0:metadata" xmins:ds="http://www.w3.org/2000/09/xmtidsig#" entityID="nttp://demoarb.layerxtech.com/sam2/module.php/sami/sp/metadata.php/default-sp"> cmd:SPSSODescriptor protocol/supportEnumeration="um:oasis:names:tc:SAML:1.1:protocol um:ossis:names:tc:SAML:2.0:protocol/supportEnumeration="um:oasis:names:tc:SAML:2.1:protocol um:SPSSODescriptor use="signing"> cds:K509Deta: cds:X509Deta: cds:X509Deta: cds:X509DotA23YLUEEOMAwGA1UECAwFVGV4YXMDzANBgMVBAcMBR/NdzANBgMvHacMBR/ndBR/ndBR/ndBR/ndBR/ndBR/ndBR/ndBR/nd</pre>	Last Name (Optional):	SAML Metadata		×
Required aste your metadota XML here c-rdd:EntityDescriptor xmins:md="um:basis:names:tc:SAML:2.0:metadata" xmins:ds="http://www.w3.org/2000/09/xmidsig#" - rdd:SPSSODescriptor protocolSupportEnumeration="um:basis:names:tc:SAML:1.1:protocol um:basis:names:tc:SAML:2.0:metadata_php/default-sp"> - rdd:SPSSODescriptor protocolSupportEnumeration="um:basis:names:tc:SAML:1.1:protocol um:basis:names:tc:SAML:2.0:metadata_php/default-sp"> - rdd:SPSSODescriptor use="signing" - rdd:KeyDescriptor use="signi	dentity Provider Metadata XN	xml version=*1.0"?		
entitylo="nitp://demoarb.layerxtech.com/sami2/module.php/sami/sp/metadata.php/default-sp"> <pre> <md:spssodescriptor protocolsupportenumeration="um:coasis:names:tc:SAML:1.1:protocol
um:coasis:names:tc:SAML:2.0:protocol"> <pre> <md:spssodescriptor protocolsupportenumeration="um:coasis:names:tc:SAML:1.1:protocol
um:coasis:names:tc:SAML:2.0:protocol"> <pre> <md:keyoescriptor usa="silpning"> <ds:x509data> </ds:x509data></md:keyoescriptor></pre> </md:spssodescriptor></pre> </md:spssodescriptor></pre> <pre> </pre> <	* Required	<md:entitydescriptor signing<br="" xmins:md="u</td><td>rn:oasis:names:tc:SAML:2.0:metadata*</td><td></td></tr><tr><td></td><td></td><td> and:SPSSODescriptor protocols,
um:oasisnamestc:SAML:2.0:proto
and:KeyDescriptor use="><ds:keyinfo um:casis:names:tc:sa<br="" xmins:ds="http://w
<ds:X509Centificates-MIID5zCCAs+
QYDVQGEw,JU2EDMAwGA1UEI
GF5zXJ4MQ8wDQYDVQQLDAZsY;
nN1cH8vcnRAbGF5ZXJ4GVjaCSJ
ELMAkGA1UEEhMCVWbdJAMBgj
AoMBmcheWyeDEPMA0GA1UEC
voNACkBFh2zdXBwb3J00GxheWY
CAQEA4ZgbuCZEgg3E/Rri+lvoMyyj
DPBIMf5kBJIM[UbK4V5L0TCoaCc
3J28vAGS780C68UUhD4d8UH455
LTKIBG5zCd5NAUfKKnTep4yhgto
hB0KYlQpVQ5Z6w2T5xlwvbdwlD/
HwYDVR0jB8gwFoAUUtPD8BSaub
GsFAACCAQEAyk094TvcTg2xuoNi
E1z+M4HK207D22h60LW+2NW2IX
8Kbd4yV57750VDQPBT2JuV8JzQj
WEYXP00IHm6nkeVUs95J/LxsXqlw
Cg/I19wG2EnnjinwHYpGw==d/ds:Xi
 </td><td>upportEnumeration=">col"> ()> www.w3.org/2000/09/xmidsig#"> gAw/BAgLAIy0+05PIFX0MA0GCSqGSIb3D CAnFVGV4YXMxD2ANBgNVBAcMBklydmit XicngxEDAOBgNVBAMMB2RidnBkombuT b20wihncNATgwMTE3NjkMzG3WncNMjg wwGbGF52X.14MRAwDgYDVQQDH0AZJ wwGbGF52X.14MRAwDgYDVQQDDA4K2/G yyeHRIY2guY29ItMIBIJANBgkqhkiG9w0BAG jhYtasGTvqvuKmbkmD9eP75vB54t0yTT55 j50d1D9YL3eVAMsm0aNF/X1dTAb3Lc9Vq iXMsJa+1 wECeYsRQN16c7Al56C9Yr9BeHU xRLUbXh2wVbD/rOJZFk+D7yDLSapte410b AQABo1 AwTJAdBgNVHQ4EFgQUUvtDaB5s HiBrUtzgbEVEm8V8thwOAYDVR0TBALUwAw hcX2019T6v17IR201280LN8ydBswbNmP9vX incdx?zuYATtdsWEZn+BXT+vDSw9IPNmxp QSUr11MD1/3R9Z+EtitKUrJIN4CLVsn8h40r2D v3NTbtzQeMBppuVOByGVaIEWIgiFyg8++t/i 509Certificate></ds:keyinfo></md:entitydescriptor>	ML11.1:protocol QEBCwUAMIGJIMQswC IZ2EPMA0GA1UECgwGb NBgkqhkiG9w0BCQEWF WTE3M[IxMzC3WJG8iT ec72pbmcxD2ANBgNVB WYXJIMSUWWYJKoZIh EFAACCAQBAMIBCgK MY7DW722Gr[Gqsjrpk5s Moch7PsvMnBCqCImJ+x 000pq6mk6xYXIC6XWVv VmFJRCIa7LgkGdqV+R UdH6fUtzgbEVEm8vBtw EB/2ANBgkqhkiG9w0BA PPFDkBe6K/BsJum63c1 Yobr315XKoJeDISq7Vy9 qGJIuoCQrt/LT06LzFek2r	
	Service Provider Information	death Dravidas		
ervice Provider Information	erowae this information to your I	aenuty Provider		
ervice Provider Information rovide this information to your identity Provider	Audience URI (SP Ender 10):	http://demoarb.layerxtech.com/sa	ami2/module.php/sami/sp/metadata.php/de	fault-sp
ervice Provider Information ravide this information to your identity Provider udience URI (SP Entry ID): http://demoarb.layerxtech.com/samt2/module.php/saml/sp/metadata.php/default-sp	Single Login URL:	http://demoarb.layendech.com/aa	aml2/module.php/saml/sp/saml2-acs.php/d	sfault-sp
ervice Provider Information rowide this information to your identity Provider udience URI (SP Enter 10): http://demoarb.layerxtech.com/samt2/module.php/sami/sp/metadata.php/defauit-sp ingle Login URL: http://demoarb.layerxtech.com/samt2/module.php/sami/sp/samt2-acs.php/defauit-sp	Single Logout URL:	http://demoarb.layen/tech.com/aa	ami2/module.php/sami/sp/sami2-logout.php	/default-sp
ervice Provider Information rovide this information to your identity' Provider udience URI (SP Entry ID): http://demoarb.layerxtech.com/samt2/module.php/samt/sp/metadata.php/default-sp ingle Login URL: http://demoarb.layerxtech.com/samt2/module.php/samt/sp/samt2-acs.php/default-sp ingle Logout URL: http://demoarb.layerxtech.com/samt2/module.php/samt/sp/samt2-logout.php/default-sp	Metadata:	View Details Download		
ervice Provider Information rovide Information rovide this information to your identity' Provider udience URI (SP Entry ID): http://demoarb.layendech.com/samt2/module.php/samt/sp/metadata.php/default-sp ingle Login URL: http://demoarb.layendech.com/samt2/module.php/samt/sp/samt2-acs.php/default-sp ingle Logout URL: http://demoarb.layendech.com/samt2/module.php/samt/sp/samt2-acs.php/default-sp ingle Logout URL: http://demoarb.layendech.com/samt2/module.php/samt/sp/samt2-acs.php/default-sp ingle Logout URL: http://demoarb.layendech.com/samt2/module.php/samt/sp/samt2-acs.php/default-sp ingle Logout URL: http://demoarb.layendech.com/samt2/module.php/samt/sp/samt2-logout.php/default-sp ingle Logout URL: http://demoarb.layendech.com/samt2/module.php/samt/sp/samt2-logout.php/default-sp ingle Logout URL: http://demoarb.layendech.com/samt2/module.php/samt/sp/samt2-logout.php/default-sp ingle Logout URL: http://demoarb.layendech.com/samt2/module.php/samt2-logout.php/default-sp ingle Logout URL: http://demoarb.layendech.com/samt2/module.php/samt2-logout.php/default-sp ingle Logout URL: http://demoarb.layendech.com/samt2/module.php/samt2-logout.php/default-sp ingle Logout URL: http://demoarb.layendech.com/samt2/module.php/samt2-logout.php/default-sp ingle Logout URL: http://demoarb.layendech.com/samt2/module.php/samt2-logout.php/samt2-logout.php/default-sp ingle Logout URL: http://demoarb.layendech.com/samt2/module.php/samt2-logout.php/sam				

Enable SAML		
Disable Multi Tenancy		
SAML Signature Algorithm	sha1 +	
Attribute Mappings		
Email (Optional):		
Username (Optional):		
First or Display Name (Optional)		
Last Name (Optional):	SAML Certificate	×
Identity Provider Metadata XM * Required Poste your metadata XML here	BEGIN CERTIFICATE MID5zCCAs-gAwiBAgLAIyo-0SPIFX0MADGCSqGSIb3D00 VOQGEwUVJzEOM&GA1UECAwFVGV4YXMxDzANBgNV CgwGbGF52XJ4MQ8wDQYDVQQLDAZsYXIIcngxEDA0BgN BgkqhklG8w0BQCEWFnN1cH8vcnAbGF52XJ4dQVaCBV BgkqhklG8w0BQCEWFnN1cH8vcnAbGF52XJ4MQ8wDQYDVQQHDAZJcnZpbmcxDzANBgNVBAoMB bGF52XJ4MRAwDgYDVQQHDAZJcnZpbmcxDzANBgNVBAoMB bGF52XJ4MRAwDgYDVQQHDAZJcnZpbmcxDzANBgNVBAOC6BU bGF52XJ4MRAwDgYDVQHDAZJcnZpbmcXDZAABG1AwTJAdBgNVHADEF gbEVEm8vBtwHwYDVRDIBBgWCBAQsFAAOCAQEAyK094Tvc Rz0c280UBsydBswbNmP9xXF68UA9dzin4TUHDwJqEIz-H NVZZNnodxfzryYATrdsVEZn-BXT+v03w9fPNmxpPFFbK8 yVS7750VDQPBT2JuIV8JizJQSUr11MDi3R9Z+E1IKUJII4CL br315XKoJeDISq7Vy9WEYXPO0IHm6nkeVJ985yLxsXcjw33 GValEWIgFygB++v1qGJluoCQn/LT06LzFek2rCg/19wGzEnmjEND CERTIFICATE	EBCwUAMIGJIMQswCQYD AcMBRIydmiuZ2EPMAAQGATUE VBAMMB2PidnBhcmbuTAj 20wHnchMfgwMTE3Mjix CVVMxDjAMB9NVBAgMBVRI mxheWVyeDEPMA0GATUEOwwG 21mvDAAQKBFhZz0XBwb3J0 CAQBAMIBCgKCAQEA S4fQyIT55HY7DW722 3eVAMsm0aNF/X1 UnDA48UH45CWSJ+x1W K18G5ZcGSNAUHKKdn RCIa7LgkGdqV-RhB0 gQUUVDaSBaubH6fUtz 4VEm8vBthwDAYDVR0T TgZxuoNhcX2019T6vI7I M4HK207DZ2h60UW+Z 6X/BaJum63cII8Kbd4 X9nBh40t2Y6 TbtzQeMBppuV0By nwHYpGW=
Service Provider Information		
Provide this information to your l	lentity Provider	
Audience URI (SP Entity ID):	http://demoarb.layendech.com/sami2/module.php/sami/sa	o/metadata.php/default-sp
Single Login URL	http://demoarb.layenttech.com/sami2/module.php/sami/sr	o/sami2-acs.php/default-sp
Single Logout URL:	http://demoarb.layen/tech.com/sami2/module.php/sami/sr	s/sami2-logout.php/default-sp
Metadata:	View Details Download	
The state of the s		

5.11. Import & Export

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

5.11.1. Exporting

To export configuration items:

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

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		
> I Protected Subnets 20		
Realms 2		
E Response Procedures 37		
⊨ 🗑 Users 📊	Package Name	Must be between 1 and 32 characters long
	Package Description	Must be between 1 and 172 characters long
	Export	

5.11.2. Importing

To import configuration items:

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

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

5.12. Archive Management

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

5.12.1. Archive

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

Setup

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

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

LHIVE MANAGEMENT	ntguration wanagement, Log wanagement	
Archive Collect LOAP SN	MP Syslog Tunnel	
	Save	
Setup	Changes have been made to this configuration item	
Arbitrator Backup		
Cisco Files	Setup	
Cisco SQL	The system does a backup daily. For the most part, there is nothing for the user	
Pexip Files	automatically on a daily basis. Archived data are logically grouped together and	
Remote Storage	by default stored into separate archived files locally on the box. There is a separate page for each Archive group. More detailed information about each	
	Archive group can be found on the individual Archive group pages. The user also has the option to mount a NFS drive to the system. All archived files will then get	
	archived to the NFS mounted drive. Note: removing the NFS mount will NOT copy the NFS contents back to local storage. Only NFS v3 mounts are currently	
	supported today.	
	Storage Type	
	standard :	
	Optional Standard' means the system will use its default archive location for all	
	backups. http://means.the.system.wili use the nfs mount specified to store all	
	orchives	
	Remote Location	
	Required anly for infs' option. Specify remote nfs ip and path location	

Arbitrator Backup

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

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

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

Archive Collect LDAP SNMP	Systog Tunnel	
	Save	
Setup	Changes have been made to this configuration item	
Arbitrator Backup		
Cisco Files	Arbitrator Backup	
Cisco SQL	Arbitrator configuration and data backup. This page contains the settings for the backup of the Arbitrator. There is nothing to edit here. The settings	
Pexip Files	are simply displayed for informational purposes only. This Archive group contains the following data: Arbitrator Configuration settings (Database:	
Remote Storage	Assets, Alerts, Policies, Rules, Probe Groups, Response Procedures, Controls), User Permissions settings (Idap), NDX files, Awaya data, Pexip data, and all other data currently being collected in the Arbitrator database. The backup excludes data from the CALL table, Cisco Tables, and raw Cisco CDR/CMR files. Data in the CALL table can be very large and is expendable. Cisco Tables and raw Cisco CDR/CMR files are part of a separate Archive group.	
	archive_interval	
	daily	
	method	
	local	
	destination	
	/chroot/scp/pub/tut_archive	
	monthsKept	
	notSupported	

Cisco Files

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

Archive Collect LDAP SN	IMP Syslog Tunnel	
	Save	
Setup	Changes have been made to this configuration item	
Arbitrator Backup		
Osco Files	Cisco Files	
Cisco SOL	Archival for Cisco files. This Archive group will backup all Cisco CDR and Cisco	
and ste	CMR raw files. These are the files that are sfip'd to the system by the Cisco Call	
Pexip Files	Manager. The settings here are for informational purposes only. However, the	
Remote Storage	user may disable the storage of raw clico COM and clico CMM raw files on the system. This option could be used to conserve disk space.	
	status	
	enabled \$	
	'enabled' - keep original cisco cdr/cmr files, 'disabled' - remove original cisco	
	reference files. The Wendeled' antion will ensure all existence files to be deleted	
	carcun pres. The doubled option we cause an carcun pres to be based	
	from the system. This is a permanent deletion.	
	archive_interval	
	cuty	
	method	
	inal	
	destination	
	/chroot/scp/pub/vd_archive	
	monnswept	
	notSupported	

Cisco SQL

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

CHIVE MANAGEMENT Configu	ration Management Log Management	
Archive Collect LDAP SNMP	Syslog Turnel	
	Save	
Setup	Changes have been made to this configuration item	
Arbitrator Backup		
Cisco Files	Cisco SQL	
Claco SQL	Archival for Cisco SQL data. This Archive group will backup all Cisco data in the database tables. This is the data that has already been processed by the	
Pexip Files	system. There is nothing to edit here. The settings here are for information	
Remote Storage	purposes only. The data here is grouped together by the Gisco Call Manager (p Address. This allows for more granular control on which Call Manager data to import.	
	archive_interval	
	daily	
	method	
	local	
	destination	
	/ctroot/scp/pub/st_anthive	
	monthsKept	
	révite	
	infeste	

Ndx

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

nis scr	een can be used to manage Ndx files on the system.
	ndy file size
max_	nax_me_size
1	
The m	vaximum size the ndx searchable file should be. Once the max size is hit, the ndx server will create a new ndx file.
	correbable dave
max_	searchable_days
1	
The m searcl	aximum number of days that should be searchable. Ndx files greater than this time will still live on the system but will not b hable from the UI.
mont	hsKept
6	
The m	aximum number of months to keep ndx archives around. Each archived ndx will take up disk space. Warning, increasing th
numb	er 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.

RCHIVE MANAGEMENT	Rguration Management Log Management	
Archive Collect LOAP SNN	NP Syslag 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 peep data fiels 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 peep files.	
Remote Storage	status	
	enabled \$	
	knabled - keep original pexip files, Wisabled - remove original pexip files.	
	This 'disabled' option should be used to conserve disk space. The 'disabled'	
	option will cause all peeip files to be removed. This is a permanent change.	
	archive_interval	
	daily	
	method	
	local	
	destination	
	/chroot/scp/pub/bt_archive	
	monthskept	
	natsupponed	

Remote Storage

This page does not describe an Archive Group. If standard / local storage is chosen in the

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

Archive Collect LDAP SNMP	Syslog Tunnel	
	Save	
Setup	Changes have been made to this configuration item	
Arbitrator Backup		
Cisco Files	Remote Storage	
Cisco SQL	This page does not describe an Archive Group. If standard / local storage	
Pexip Files	configure remote archival of the Arbitrator backup files. Each Archive	
Remote Storage	group produces one or many archive files. The system can be configured to scp these archive files to a backup location or to another Arbitrator.	
	archive interval	
	daily \$	
	method	
	scp ÷	
	'disabled' - keep archives locally, 'scp' - System will copy archives to a	
	remate location. Scp is nat a sync. In order to reduce load on system and	
	network, system anly copies new / changing archives over to the scp	
	location, 'rsync' - System will sync archive directory to remote system. The	
	remote system must have raync installed for this to work, 'rsyncToArb' -	
	System will sync archives directory to a remote Arbitrator. This utilizes	
	the rsync pratocol so both Arbitrators will always be in sync	
	IP location	
	192.168.123.123	
	username	
	admin	
	password	
	destination	
	/sdfsdtdst	
	monthsKept	
	infinite +	

5.12.2. Collect

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

ARCHIVE MANAGEMENT Configuration Man	gemeint Log Management	
Archive Collect LDAP SNVP Systeg	fund	
	Save	
Cisco CDR	Oranges have been made to this configuration item	
	Clisco CDR	
	Use this to configure where the collection of cisco cdr / one files should be stored. "local" is the debuilt location. Click CDR / CVHS files will be processed and stared on local arbitrator. Thorose "remote arbitrator" and the processed clock CDR / CVM files will be stored to the kitabase of a remote arbitrator. That is useful if the data of multiple arbitrators needs to be stored to a certratabal arbitrator. The 'remote, jp' needs to be filed in with the lp address af the 'remote arbitrator'. If configured.	
	method	
	remote,p	
	Addrator IP	

5.12.3. LDAP External Config

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

Image: Control of the control of th	
Section 1 Section 2	all control on the difference par-
Image: Section of the sec	
	net, he preserved a conserved procedures and program and according or overcompart, and press memory Me
	an month way. Anthersport-space spaces portion power becaute the mone affected to the power present the determinant and an end of the space and the space of the determinant of the space o
	Annue under anne annue anne a service anne a service annee.
	Apresent
Even the second seco	And the second s
Image: Section and the section and	
Image: Control of the second seco	angle and
per la de la contra per per gargene y en la generar per la magne de la contra per la mañe de la mañe	AP configuration
Image: Image	n sanna par seligarena e na polini alegar alegar alegar adolare.
Image: Image	
Interpretation provide press, source or provide database bases parts in the strenge additional phones to parts it. Image: Image: <td></td>	
Note Note <t< td=""><td>yalem autor lag annes "annanend Alimagh Anne Tonnoy neins. Na ant report additional Jone optimistics a le (194)</td></t<>	yalem autor lag annes "annanend Alimagh Anne Tonnoy neins. Na ant report additional Jone optimistics a le (194)
Note 1 Note 1 <td></td>	
Image Image	
<pre>key a set of a local set of a l</pre>	10
Image: Image	e sensegi beling fer is trat (Blessel) Ann Einney maarmal/in sponten
*	
Sector by it shows years years of densate the point is not in t	
wwwwwwwwwwwwwwolawawawawawawawawawawawaw	H landan jumiy (julatan di Amathan Ana Janar)
www sparse type is adout intog have accessed, top is less ands intog a sector is the its the statematic parameters are stated in a sector is a	
Approximate integet inside integet inside integet inside inside integet inside insi	
Adverture for another large of another l	
<pre>strain stra</pre>	2 ander settig freidrierenses sied her and her an der der Antigenitieren felse fils setting an einer eine verset
parents parents pa	
Appendix on by several wang, having person to using a well his bigs our in a tota young person to it is a well as	
aligned by Surface and production and production and the subgroups are not to subgroups a series of the subscription are not production are not pr	
<pre>result</pre>	2 metalen alleng feldelig generative op in tige and the dig and had been program and the dig the control and the dig table. The dig and had been program and the dig table of the dig table of the dig table.
Intell State	
Report of y be invested a star of planetic a star of the star of t	
Mail Sector Sector </td <td>r Westen' etting Janesi is uit uth-consent.</td>	r Westen' etting Janesi is uit uth-consent.
International and a second of the species of the provide of the provide of the second	
beginned only, by whether yamp, have top (2015) arguments or group (percental and this allow thread on 1011 and it ments insurements ins	
aveil aveiled av	production ranning. Amonthip 1937 (in regeneration or group: Agent wall use the 1933 excitation in the all uses under the lases 1934
week impoundement dependency derivative ander dans privative store das privatives store das dasselptions are und angeband store under in dasselptions are under indexed points are under indexed poin	
I and a set of the second set	
Application of the present of and present present of a state present present of a state p	n
An experting of any party in any part of a standard stand	e wedawi atting ihang tilain metri da ing propery nona diaraketija de aar iti o paa blonad Al kiga agan tamenaamanari na konsta.
mem Register 10 Register 10 Register 10 Register 10 Register 10 <td>) wily engering. The spaces will some a matching local blog user for such some and was the groups and user its property on the local such its</td>) wily engering. The spaces will some a matching local blog user for such some and was the groups and user its property on the local such its
Minimum Anglewine	
Append of the sense sense in the field parameter sense in the field parameter sense in the sense of parameter device of the sense of th	
ational dispares for yours at investor sector by least top out out out out of the spectra allow at its pares	e wholey amy those must be depayory more for whether to some a partition of site departition on commendation
Mode Mode Applied by Setters and plane plane and the flag synaph wate developed to is wate applied by the setter applied	gamp. The paints and remain to place hidp ware for each ware write the tase 2016. The paints all was the paperty as the same for the local war int.
Intel	
Image:	
All pages 1, for some states, grand pages than a most in the pages some that develops in and a state develops of and a state of the sta	
Mai Approxit only, for waters' andiag, and decision and approxit dates that perform all assess that and the second interpret of source and and the second interpret of source and the second i	
Appropriet by for matter and gains the design and pains them the type of and serve for at anno set in the DD gains. The second is a pain type of the second is a	
Angeland chy far watered wetting and index watere up as a signature filter. In provide all water in the test Byres in Neuron 2016 responses, many paper, far Wetting and the paper of the test watered of the paper filter for all and the paper filter	
sangapa, Junita kas pagi Agalamin Jain ka sana ung kagupat kas na anak Annag Bar Jainer (panakan)-Dinasaling (Dinasa) Barataan Barataan Insense Agalamin Agala ang Jainer Jaine Andre Kasagalan kasi kasi kasi kasi kasi kasi kasi kasi	en verselander vertrige, van de hullen van een wegen en bekenweren (deren. Der gedeen waart van er vertrijk van aander vie twaat bijd genaag. De kaans 2001 mag constant van
Drugs/Dr dynamits/Dr volgeneenderg/Chr-dwinning/Dirichardy Organisti/Dr lange Hardhami (mettal) Re-parts pf, for stratest withing. Drugs fritune match for its property size withing for the your Minning fill they depict in revising? In a summer Relyhold Winning fill they apply fritune match for its property search dire strategies for searcher of forter space Minning fill they depict in revising? In a summer Relyhold Winning fill they apply fill the strategies for the strategies for searcher of forter space Minning fill they depict in revising? In a summer Relyhold Winning fill they apply fill the shared of Lanet days. Winning was apply apply for the strategies for the strategies apply of the strategies of the strategies of the strategies for the strategies for the strategies of the strategies for the strategies of the strat	and the tax test space (b) Stag Standard (Bloc that an option of the groups (Bloc Jacob) (Dermit Standard) (Derivated Strange), (De
Nonlineau I month Angel of the Antheorem and the Antheorem Anthe	next, NovergrandersphOn-Jandraug, 20-dar angl-Angenet Al-samp
Managana Januarian Rapital tanja, la matema naling Sanga Malan nakti tha dagi ayaang sawa dini sherijita tin vanane (fulti a yaar Malang) Ki dagi agasi, teretang ti sa samane anjaratikanyak tanjangan matamatanakatikan Managana Tanja Sanga Malan ku kanada Janati aga, Kanatan ana saha and Sa anjaka Pana, sabada ter da ganta ana da kanadi	
Alignet of the first sections which we also needs the day property sears that sheeply the researce of plot of large space. The section of the day property search and section of the section of the day property search and section of the section of	
Adult de long d'a superior Malance Mar Anna de la company de la co	e windower antrag. Stage House medit her big graanty voor des steeldes de meeter of het is over Michael Al big dated. Herderer () is service
mulation from the second s	hit years and a second s
Associations for watting with data to constrain communication and wait is for an interaction of the second	
	structurer setting the the Andre to grower a good structure over our hole and we projected at the good with an do agent
annual to and all new tests to regar	al no not no upo

5.12.4. SNMP V3 User Config

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

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

5.12.5. Syslog Server

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

ARCHIVE MANAGEMENT Configuration Man	agenerer Log Mangement	
Archive Collect LDAP SNMP System	Turni	
	See	
Syndag Server	Changes have been much to this configuration item	
	Syslag Server	
	Use this screen to configure the ip address of your control spring 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 systag server. Only one central spring server can be specified at this time. These validate firewall settings are open to allow incoming messages on the specified ip address and port.	
	sxternal_spilag_b	
	Optional, Enter in the lp. address of your organization's control gislig server. A single to Address	
	or a ungle Ganatin name. Note, Donatin name entries must resolve through the system canfigured DNG (part specified in system DNS settings)	
	protocol	
	122 E	
	dand become is on a dead another the Basic source on an and here became	
	external_systeg_port	
	614	
	Optional. Enser in the port, Default systag port is 514	

5.12.6. Tunnel

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

Creation

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

ARCHIVE MANAGEMENT Configuration Man	nagement log Wasapersent
Archive Collect LDAP SNMP Sysleg	Tirred
	Save
Creation	Changes have been made to the configuration teen
Management	
Request History	Creation
	Allows the creation of SSH surnel to the specified endpoint, including interim hops needed.
	Create Tunnel
	Create Tunnel
	Clease a shore in the subhetter search are obtained built
	remateAddress
	172.30.11.106
	remataPort
	3389
	Defention Theorem
	169.254.5.12
	Fetch InterimDevices
	Fetch InterimDevices List
	Petch a list of possible interim devices. This is required when the Arbitrator Is connected to
	multiple events and the or advertisis specified in the hermoder/adverse field is recised without the efficience company
	uguna ma

Management

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

Anthive Collect LDAP SVMP Sys	ag Turnel	
	Sive	
Creation	Changes have been made to this configuration com	
Management		
Bequest History	Management	
medaner unend	Allows the listing, and management of existing tunnels,	
	Les Arther Turnels	
	List Active Tunnels	
	List only at the Annels.	
	Berness Startiked Turned	
	Remove and close the tunnel specified	
	Core the artise surged to request it	
	Cana per anter malarita da regurante	
	requerds	

Request History

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

RCHIVE MANAGEMEN	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
	List Bequests
	List Requests
	List all tunnel requests, and their status.

5.13. Log Management

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

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

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

Archiv	ve Methods		
	IP Address	N	lethod
	0.0.00		SCP
			SCP SFTP SMP

hive 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 Alert on archive failure
chive Methods				
IP Address	Method	Path	Credentials	
There are a second seco	SCP	+	None	:

5.14. Tools

5.14.1. SNMP Tools

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

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

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

3. Scroll through and select the desired MIB.

W V0SS	A ③ 1 前 🕮 🥄 4 品 🕹 👄 🗢	👤 admin -
TOOLS MIB Browser		
Load MIB Import MIBs	SNMP Connection » Host @ Connection	
	OID	Operation
	13.6	✓ Get ¢ Run
	Select a MIB ×	
	Search	
Name	Re-parse Cancel Select	
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 MIB Browser							
Load MIB Import MIBs SN	MP Connection » Host 10.13.37.80		© Connection				
4 📄 iso 4 📄 org	OID 1.3.6.1.4.1.6876.1			~	Operation	e Ru	un
a 🐌 dod a 📄 Internet	SNMP Options						
 directory mgmt experimental private 	Version 2c ‡ Community						
 enterproc ymwa ymwa ym ym 	2 д П	Cancel	Ok				
	nwWirtMachines nwResources nwProductSpecific nwLdap nwTraps nwSRM nwVCHA	SN vers cont	IMP Options				
Name vmwSystem		Secur auth Auth	nty Lavel http://www.all Protocol				
010 1.3.6.1.4.1.6876.1		Su	A 2 Passphrase				
Access		Priva	cy Protocol 5 B				
Status		- Priva	ng - andphase				
Description Parent of all managed obj system software identifica	ects relating to ition.						

- 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.

DID				Operation	
1.3 Resi	.6.1.4.1.6876.1 ults		~	Get + Run Get Next Walk	
q	Text OID Toggle Numeric/Text OID Crea	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	
VMWARE-SYSTEM-MIB::vmwProdBuild.0		2494585	STRING		
VMWARE-SYSTEM-MIB::vmwProdUpdate.0		0	STRING		
-	VMWARE-SYSTEM-MIB::vmwProdPatch.0	0		STRING	

create Probe	
OID:	
.1.3.6.1.4.1.6876.1.1.0	
Probe Name:	
Add to existing probe group	
Application sah probe	
Create a new probe group	
Probe Group Name:	

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