

ARUBA OS EventTracker v8.x and above

Publication Date: February 25, 2019

Abstract

This guide provides instructions to configure Aruba OS to send the syslog events to EventTracker Enterprise.

Scope

The configurations detailed in this guide are consistent with **EventTracker Enterprise** version 8.x and later, and Aruba OS 6.5 and later.

Audience

Aruba OS users, who wish to forward syslog events to EventTracker manager.

The information contained in this document represents the current view of Netsurion. on the issues discussed as of the date of publication. Because Netsurion must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Netsurion, and Netsurion cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. Netsurion MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, this paper may be freely distributed without permission from Netsurion, if its content is unaltered, nothing is added to the content and credit to Netsurion is provided.

Netsurion may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Netsurion, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.

© 2019 Netsurion. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.



Table of Contents

Abstract	1
Scope	1
Audience	1
Overview	3
Pre-requisite	3
Integration of EventTracker with Aruba OS	3
EventTracker Knowledge Pack (KP)	4 4
Reports	5
Import Knowledge Pack into EventTracker Category	5 6
Alerts	7
Knowledge Objects	8
Templates	.0
Flex Reports	.1
Verify Knowledge Pack in EventTracker	.4 .4
Alerts 1	.4
Knowledge Object	.6
Flex Reports	.6
Templates	.7



Overview

The Aruba OS operating system for Aruba Mobility Controllers, Mobility Access Switches and access points (APs) perform security and system administration, as well as hardware-based routing, switching, firewall and data encryption capabilities.

EventTracker Enterprise supports Aruba OS, the syslog messages can be forwarded to EventTracker Enterprise and based on events, alerts and reports can be configured into EventTracker.

Pre-requisite

Prior to configuring Aruba OS and the EventTracker Enterprise, ensure that you meet the following prerequisites:

- EventTracker v8.x should be installed.
- Aruba OS should be installed.
- Port 514 must be opened on Aruba OS.
- Port 514 must not be used by other services of Aruba OS.
- An exception should be added into Windows Firewall on EventTracker machine for Syslog port 514.

Integration of EventTracker with Aruba OS

To configure Aruba OS to forward the log to EventTracker Enterprise:

- 1. Login to the Aruba Mobility Controller using Web User Interface.
- 2. Navigate to the **Configuration > Management > Logging > Servers** page.
- 3. To add an EventTracker Enterprise server, click New in the Logging Servers section.
- 4. Click **Add** to add the **EventTracker Enterprise server** to the list of logging servers. Ensure that the syslog server is enabled and configured on this host.
- 5. Click on Apply button.
- 6. To select the types of messages you want to log, select the Levels tab.
- 7. Select the category or subcategory to be logged.

8. To select the severity level for the category or subcategory, scroll to the bottom of the page. Select the level from the Logging Level drop-down menu. Click on **Done** button.

Logging Level	Description
Emergency	Panic conditions that occur when the system becomes unusable.
Alert	Any condition requiring immediate attention and correction.
Critical	Any critical conditions such as a hard drive error.
Error	Error conditions.
Warning	Warning messages.
Notification	Significant events of a non-critical and normal nature.
Informational	Messages of general interest to system users.
Debug	Messages containing information useful for debugging.

The default logging level for all categories is Warning.

9. Click **Apply** to apply the configuration.

The configuration is complete. Aruba Mobility Controller events are automatically discovered in EventTracker Enterprise. Events forwarded to EventTracker by Aruba OS are displayed on the Log Search tab of EventTracker Enterprise.

EventTracker Knowledge Pack (KP)

Once logs are received in EventTracker; alert, reports, knowledge object can be configured in EventTracker.

The following Knowledge Packs are available in EventTracker v8.x and later to support Aruba OS monitoring:

Alert

ArubaOS User authentication failure – This alert will trigger whenever user authentication failure happens.

ArubaOS: Attack detected – This alert will trigger whenever association flood DoS attack is detected, ARP-spoofing is detected.

ArubaOS: License expired – This alert will trigger whenever ArubaOS license is expired.



Reports

ArubaOS - **User Authentication Failure** -This report provides information related to the user authentication failure and authentication server out of service while serving request.

ArubaOS - **Connection failure** -This report provides information related to the connection failure with the profile manager.

ArubaOS - **Attack detected** – This report provides information related to the association flood DoS attack detected, detected ARP-spoofing, system detected MAC spoofing and frame dropped.

ArubaOS - **User login failure** – This report provides information related to the client authentication failure and User de-authenticated.

ArubaOS - **User login success** - This report provides information related to the Management user authentication completed successfully.

ArubaOS - **DHCP** activities - This report provides information related to the DHCP client disabled on the specified VLAN, request, release and decline.

ArubaOS - **Connection details** - This report provides information related to the Assoc connection success, Dis Assoc flood DoS attack detected and Assoc failure.

ArubaOS - **User authentication details** – This report provides information related to the user deauthenticated, log indicating that a user has been authenticated.

ArubaOS - **Firewall messages** – This report provides information related to the A firewall rule with log option as hit, as source IP address, source port, destination IP address, destination port details.

Import Knowledge Pack into EventTracker

- 1. Launch EventTracker Control Panel.
- 2. Double click **Export/Import Utility**, and then click the **Import** tab.



Figure 1

3. Import Tokens/Flex Reports as given below.

Category

1. Click **Category** option, and then click the **browse** button.

🐁 Export Import Utility	-		×
 Export Import Utility Export Import Provide the path and file nam Click the Import button. Options Category Filters Alerts Systems and Groups 	e of the Categories file. Use the '' button to browse and locate the import file. Location Source : F: EDEPODUCED Asks OF: NEW ADUDAGE 6.5. YE ITENS:		×
 Systems and Groups Token Value Reports Behavior Correlation 	Source : E:\PRODUCT\Aruba OS\NEW ARUBAOS 6.5x KP ITEMS\		
	Import	Clo	se



- 2. Locate Category_ArubaOS 6.5x.iscat file, and then click the Open button.
- 3. To import alerts, click the **Import** button.

EventTracker displays success message.





4. Click the **OK** button, and then click the **Close** button.

Alerts

1. Click **Alert** option, and then click the **browse** button.



🐁 Export Import Utility			
Export Import			
1. Provide the path and file nar 2. Click the Import button.	me of the Alerts file. Use the '' button	to browse and locate the import file.	
Options Category	Location		
Filters	Import E-mail settings		
Alerts	Set Active	This setting is applicable only for imports from Leg	gacy
Systems and Groups	 By default 	(v6x) Alert files. For v7, the active status will be so based on "Active" key available in the configural section	et tion
RSS Feeds		50000h.	
Reports	Source :		
Ø Behavior Rules	.isdit		
SCAP			
🔿 Token Value			
		Import	Close



- 2. Locate Alerts_ArubaOS 6.5x.isalt file, and then click the Open button.
- 3. To import alerts, click the **Import** button.

EventTracker displays success message.



Figure 5

4. Click the **OK** button, and then click the **Close** button.

Knowledge Objects

- 1. Click Knowledge objects under Admin option in the EventTracker manager page.
- 2. Locate the file named KO_ArubaOS 6.5x.etko.

Import			×
KO_ArubaOS6.5x.etko	🖀 Browse	Upload	
		[Close

Figure 6

3. Now select all the check box and then click on \mathbb{T} '**Import**' option.



Selec	t file	🗁 Browse.	. Upload
	Object name	Applies to	Group name
	Aruba OS All Other Message	Aruba OS 8.x and later	Aruba OS
	Aruba OS Attack Detected	Aruba OS 8.x and later	Aruba OS
\checkmark	Aruba OS Connection Details	Aruba OS 8.x and later	Aruba OS
	Aruba OS Connection Failed	Aruba OS 8.x and later	Aruba OS
\checkmark	Aruba OS DHCP Activities	Aruba OS 8.x and later	Aruba OS
	Aruba OS Login Success	Aruba OS 8.x and later	Aruba OS
\checkmark	Aruba OS User Authentication Details	Aruba OS 8.x and later	Aruba OS
\checkmark	ArubaOS Firewall Messages	ArubaOS 6.5x	Aruba OS
	ArubaOS User authentication failure	ArubaOS 6.5x	Aruba OS
			Import Close

4. Knowledge objects are now imported successfully.



Figure 8

Templates

- 1. Click Parsing Rules option, create group and click Import.
- 2. Locate the file name Token_ArubaOS 6.5x.ettd.



Import

select	ed file is: Token_ArubaOS 6.5x.ettd	🚰 Browse 📱				
\square	Template name	Separator	Template description	Added date	Added by	Group Name
	ArubaOS - Attack Detected	\n	Mar 07 07:42:47 192.168.200.53 Feb 16 22:43:37 1970 192.168.200.53 cli[[]37 80]: <522250> <192.168.200.53 AC:A3:1E:C7:BC:B4> Association Flood Do S attack detected - AP 9c:b6:d0:e5:12:41	Feb 18 05:45:52 PM	ETAdmin	ArubaOS
	ArubaOS - Connection Failed	\n	Mar 07 07:40:31 192.168.200.53 Feb 16 22:41:22 1970 192.168.200.53 cli[[]37 80]: <400144> <192.168.200.53 AC:A3:1E:C7:BC:B4> AP NAME: Station STA TIONNAME not found while clearing association	Feb 18 05:45:52 PM	ETAdmin	ArubaOS
	ArubaOS - Connection Success	\n	Mar 07 07:40:31 192.168.200.53 Feb 16 22:41:22 1970 192.168.200.53 cli[[]37 80]: <400189> <192.168.200.53 AC:A3:1E:C7:BC:B4> VPOOL:STA 9c:b6:d0:e 5:12:41 atAP 192.168.1.1-9c:b6:d0:e5:12:41-NAME assignedvlan value	Feb 18 05:45:52 PM	ETAdmin	ArubaOS
	ArubaOS - DHCP Activities	\n	Mar 07 07:42:47 192.168.200.53 Feb 16 22:43:37 1970 192.168.200.53 cli[[]37 80]: <202538> 9c:b6:d0:e5:12:41: RELEASE 9c:b6:d0:e5:12:41 Transaction ID: 208 clientIP=192.168.1.2	Feb 18 05:45:52 PM	ETAdmin	ArubaOS
	ArubaOS - Firewall Messages	\n	Feb 06 12:33:05 10.0.24.8 Feb 6 12:33:05 2019 ICDC-ARU-C16 authmgr[4195]: <124006> <4195> {7067743} TCP srcip=10.6.10.202 srcport=53219 dstip= 10.16.32.63 dstport=389, action=deny, role=nuskinemployeeinternet, poli cy=internetonly	Feb 18 05:50:02 PM	ETAdmin	ArubaOS
	ArubaOS - Login Failure	\n	Mar 07 07:42:47 192.168.200.53 Feb 16 22:43:37 1970 192.168.200.53 cli[[]37 80]: <541003> MAC=9c:b6:d0:e5:12:41 IP=192.168.1.1 User deauthenticate d:name=NAME, cause=REASON	Feb 18 05:45:52 PM	ETAdmin	ArubaOS
	ArubaOS - Login Success	\n	Mar 07 07:40:31 192.168.200.53 Feb 16 22:41:22 1970 192.168.200.53 cli[[]37 80]: <125024> <192.168.200.53 AC:A3:1F:C7:BC:B4> Authentication Succe	Feb 18 05:45:52 PM	ETAdmin	ArubaOS



3.Click the **Import** button to import the reports. EventTracker displays success message



Figure 10

Flex Reports

1. Click **Reports** option and select new (.etcrx) from the option.



ote : If report(s) contains template	e, first import template and proceed Location	with exportimport utility.	
) Category			
) Alerts	O Legacy (*.issch)	New (*.etcnx)	
) Systems and Groups	Source :		
) RSS Feeds	-issch		
Reports			
) Behavior Rules			
) SCAP			
) Token Value			



2. Locate the file named **Reports_ArubaOS 6.5x.etcrx** and select all the check box.



Preports Import X Note : If report(s) contains template, first import template and proceed with report import process. Select file Select file E:\PRODUCT\Aruba OS\NEW ARUBAOS 6.5x KP ITEMS\Reports_ArubaOS 6.5x.etcmx							
vaila	ble repo	rts					
îtle			Frequency Show all	- Q Q			
		Title	Sites	Groups	Systems	Frequency	
	EDIT	ArubaOS - Attack detected	NTPLDTBLR46			Undefined	
\square	EDIT	ArubaOS - Connection details	NTPLDTBLR46			Undefined	
\square	EDIT	ArubaOS - Connection failure	NTPLDTBLR46	Default	AnibaOS	Undefined	
	EDIT	ArubaOS - DHCP activities	NTPLDTBLR46			Undefined	
	EDIT	ArubaOS - Firewall messages	NTPLDTBLR46	Default	AnibaOS	Undefined	
\square	EDIT	ArubaOS - User authentication details	NTPLDTBLR46			Undefined	
\checkmark	EDIT	ArubaOS - User Authentication Failure	NTPLDTBLR46	Default	ArubaOS	Undefined	
\square	EDIT	ArubaOS - User login failure	NTPLDTBLR46			Undefined	
	EDIT	ArubaOS - User login success	NTPLDTBLR46			Undefined	
						\$	
Note	e: Set ru run tir	In time option is not applicable for Defined me for report(s) from A	Reports and Hourly Reports M • at interval of minu	tes Set		>	

Figure 12

3. Click the **Import** button to import the reports. EventTracker displays success message.



Figure 13



Verify Knowledge Pack in EventTracker

Category

- 1. Logon to EventTracker Enterprise.
- 2. Click the Admin menu, and then click Category.

≡	Event Tracker ⊕					🐥 Admin -	Tools 🛨 💿 Pavan Kumar Tirupat	thi 🛨
	Home		Active Watch Lists		Event Filters	💯 Parsing Rules	🔶 / Dashboard / Ho	ome
a		_	Alerts		Eventvault	Report Settings		_
	0	0	Behavior Correlation	Rules	FAQ Tile Configuration	Systems		
2			🗞 Behavior Correlation	Settings	Group Management	QQ Users		
	Potential Cyber Breaches Unsafe connections or processes, new TCP ent	Indicators of Cor USB activities, New	Casebook Configurat	ation	🔍 IP Lookup Configuration	r Weights	orting Systems of reporting since the last 24 hours	
			● Category		· 🔆 Knowledge Objects	Windows Agent Config		
	Attacker		Diagnostics	Knowledge knowledge	categories are used in reports, searcl are available. Users may create/edit (h and views. Pre-defined categories of categories.	F	-

Figure 14

3. In the **Search** box, type **'Aruba OS'**, and then click the **Go** button. Alert Management page will display all the imported alerts.

Category			Admin / Category
Category Tree Search	Total category groups: 24 Total categories: 336 Last 10 modified categories		
All categories	Name	Modified date	Modified by
(III) *All information events	Aruba OS: Firewall Messages	Feb 18 07:16:30 PM	
All warning events	ArubaOS: User authentication failure	Feb 18 07:14:50 PM	
Security: All security events	Aruba OS: Attack Detected	Feb 18 07:12:28 PM	
Aruba AirWaive	Aruba AirWave: AP Configuration Changes	Feb 18 07:11:06 PM	
Aruba OS	Aruba AirWave: Commands Executed	Feb 18 07:11:06 PM	
	Aruba AirWave: User Login Details	Feb 18 07:11:06 PM	
🗐 Aruba OS: Connection Failed	Aruba OS: Connection Details	Feb 18 07:11:06 PM	
Aruba OS: DHCP Activities	Aruba OS: Connection Failed	Feb 18 07:11:06 PM	
Aruba OS: Firewall Messages	Aruba OS: DHCP Activities	Feb 18 07:11:06 PM	
Aruba OS: Login Failure	Aruba OS: Login Failure	Feb 18 07:11:06 PM	
Aruba OS: User Authentication Deta			
ArubaOS: User authentication failu			



Alerts

- 1. Logon to EventTracker Enterprise.
- 2. Click the Admin menu, and then click Alerts.

≡	Event Tracker ⊕					🔎 🗛 Admin-	Tools +
	Home		Active Watch Lists	Collection Master	Group Management	Systems	🕈 / Dasht
a			Alerts	Correlation	Q IP Lookup Configuration	QQ Users	
	0	2	Behavior Correlation Rules	Diagnostics	Or Knowledge Objects	1 Weights	
			🗞 Behavior Correlation Settings	🔛 Event Filters	Manager	🔲 Windows Agent Config	
	Potential Cyber Breaches Unsafe connections or processes, new TCP entry point	Indicators of Co USB activities, New sen	Casebook Configuration	Eventvault	😥 Parsing Rules		
			📲 Category	FAQ Configuration	Report Settings		
	Attacker			- News			

Figure 16

3. In the **Search** box, type **'ArubaOS'**, and then click the **Go** button. Alert Management page will display all the imported alerts.

Alerts Admin / Alerts										
Show All		Search by Alert name V ArubaOS Q Q								
131 Available Alerts Total number of alerts available	36 Active Alerts Total number of active alerts	131 User 28 System/User Defined Alerts Count for system and user defined alerts					131 Alerts by Count of a	Critical 15 72 Low 15 16 Serious 19 s by Threat Level of alerts by threat level		
Activate Now Click 'Activate Now							Total: 3 Page Size 25 V			
Alert Name A	Threat	Active	E-mail	Forward as SNMP	Forward as Syslog	Remedial Action at Console	Remedial Action at Agent	Applies To		
□ 🖗 ArubaOS User authentication failure	•									
□ 🖗 ArubaOS: Attack detected	•							ArubaOS		
□ 🖗 ArubaOS: License expired	•							ArubaOS		

Figure 17

4. To activate the imported alerts, select the respective checkbox in the Active column.

EventTracker displays message box.

Successfully saved configuration.	
ОК	



5. Click **OK**, and then click the **Activate Now** button.

NOTE: Please specify appropriate **systems** in **Alert configuration** for better performance.



Knowledge Object

- 1. Logon to EventTracker Enterprise.
- 2. Click the Admin menu, and then click Knowledge Object.
- 3. In **Knowledge Object Group Tree** to view imported knowledge object, scroll down and click **Aruba OS** group folder.

Knowledge Object are displayed in the pane.

Knowledge Objects	↑ Admin / Knowledge Objects
Aruba OS Q Q Activate Now	Objects 🕀 ፒ 🏦 🌣
Groups 🕀 🗭 🗓 = Aruba OS	<u>٦</u>
Aruba OS All Other Mess Image: Constraint of the second se	Select Object from the left panel.

Figure 19

Flex Reports

- 1. Logon to EventTracker Enterprise.
- 2. Click the **Reports** menu, and then **Configuration**.
- 3. Select **Defined** in report type.
- 4. In **Report Groups Tree** to view imported Scheduled Reports, scroll down and click **Aruba OS** group folder.

Reports are displayed in the Reports configuration pane.

Report Configuration Areport Configuration / Defined													
O Scheduled O Queued Defined Queued Arubaos Q Q									Q	ť	i v		
Report Groups 🕒 🏭					orts config	uration: ArubaOS							
63	Security		^	÷	Ē 2,							Total:	: 9
{}}	Compliance					Title		Created on	Modified on				
63	Operations				£ \$ 3	ArubaOS - Firewall messages		Feb 18 06:47:17 PM	Feb 18 06:47:31 PM		(i)	5	+
83	Flex					ArubaOS - User Authentication Failure		Feb 18 06:37:32 PM	Feb 18 06:41:58 PM		(j)	5	+
Þ	All Compliance Repor	Ē	0		£	ArubaOS - User authentication details		Feb 18 05:52:43 PM	Jan 01 05:30:00 AM		(j)	5	+
	ArubaOS	Ű	0		E	ArubaOS - DHCP activities		Feb 18 05:52:43 PM	Jan 01 05:30:00 AM		i	5	+
	Bomgar	1	0		£3	ArubaOS - User login failure		Feb 18 05:52:43 PM	Jan 01 05:30:00 AM		(j)	5	+
	Dell Equallogic		0		213	ArubaOS - Connection details		Feb 18 05:52:43 PM	Jan 01 05:30:00 AM		(j)	2	+
	Dell Unity		Ø		555	ArubaOS - Connection failure		Feb 18 05:52:43 PM	Jan 01 05:30:00 AM		0		Ŧ
B	Domain Admin User Lo		Ø		~~			Fab 19 05:52:42 DM	Inc 01 05:20:00 AM				
	EventTracker		0		2.5	ArubaOS - Oser login success		Feb 18 05:52:43 PM	Jan 01 05:50:00 AM		0	ŏ	+
	HP ProCurve	Ú	0		£\$3	ArubaOS - Attack detected		Feb 18 05:52:43 PM	Jan 01 05:30:00 AM		(j)	ŏ	+
	IderaSQLCM	Ē	1										
	iis	Ī	Ø										

Figure 20

Templates

- 1. Logon to EventTracker Enterprise.
- 2. Click the Parsing Rules menu
- 3. Select **Template** and choose Group name.
- 4. In **Template** to view imported Templates, scroll down and click **ArubaOS** group folder.

Parsing Rules Parsing Rule Template	1								🕈 / Admi	n / Parsing Rules
Groups		÷	*	Group : ArubaOS	Search	Q				CIT
Accounts mediskid	Ŵ	Ø	I	Template Name	Template Description	Added By	Added Date	Active		^
Admin groups mediski	Ű	0		ArubaOS - Attack Detected	AurbaOS 6.5x	ETAdmin	Feb 18 05:45:52 PM		Ø	
AMediskid	Ü	0		ArubaOS - Connection Failed	AurbaOS 6.5x	ETAdmin	Feb 18 05:45:52 PM		Ø	
ArubaOS	Ē	0	I.	ArubaOS - Connection Success	AurbaOS 6.5x	ETAdmin	Feb 18 05:45:52 PM		0	
BMediskid	Ü	Ø	I.	ArubaOS - DHCP Activities	AurbaOS 6.5x	ETAdmin	Feb 18 05:45:52 PM	\checkmark	Ø	
Bomgar	Ü	0	ł	ArubaOS - Firewall Messages	AurbaOS 6.5x	FTAdmin	Feb 18 05:50:02 PM		Ø	
Dell Equallogic		Ø		ArubaOS - Login Failure	AurbaOS 6.5x	ETAdmin	Feb 18 05:45:52 PM	\checkmark	Ø	
Dell Unity		Ø		ArubaOS - Login Success	AurbaOS 6.5x	ETAdmin	Feb 18 05:45:52 PM		Ø	
EventTracker	<u>ال</u>	Ø		ArubaOS - User Authentication	AurbaOS 6.5x	ETAdmin	Feb 18 05:45:52 PM		1	- 1
Groups Mediskid	۳ ۳	© (#		ArubaOS - User Authentication	AurbaOS 6.5x	FTAdmin	Feb 18 05:50:02 PM			v
HP ProCurve	Ē	0	~	Autor of Automation					Delete Mo	ove to group



