RSA Ready Implementation Guide for RSA Security Analytics

Hitachi ID Systems Privileged Access Manager/Password Manager 7.1.x, 7.2.x, 7.3.x

Daniel R. Pintal, RSA Partner Engineering Last Modified: February 29, 2016



Solution Summary

Hitachi ID Privileged Access Manager and Hitachi ID Password Manager leverage RSA Security Analytics to provide centralized reporting of audit logs as well as system errors, warnings & usage. This enables organizations to;

- act quickly when the system detects failures
- determine who was responsible
- ensure the product is being used effectively.

Examples of events reported to RSA Security Analytics include:

- Who signed into a privileged account, when and from where.
- Database replication errors and warnings, such as failure of one Hitachi ID Privileged Access Manager node to replicate new passwords to another, often in another data center.
- The number of users who reset their password using self-service password reset and/or enrolled security question/answer data into their profile.

This integration is achieved by configuring RSA Security Analytics to monitor Hitachi ID Privileged Access Manager's or Hitachi ID Password Manager's internal audit database tables.

RSA Security Analytics Features							
Privileged Access/Password Manager							
Integration package name	hitachiidmsuitepe.envision						
Device display name within Security Analytics	hitachiidmsuitepe						
Event source class	Access Control						
Collection method	ODBC						



RSA Security Analytics (SA) Community

The RSA Security Analytics (SA) Community is an online forum for customers and partners to exchange technical information and best practices with each other. The forum also contains the location to download the SA Integration Package for this guide. All Security Analytics customers and partners are invited to register and participate in the **RSA Security Analytics Community**.

Once you have downloaded the SA Integration Package, the next steps are to deploy this on all log decoders. For steps to disable or remove the Security Analytics Integration Package, please refer to the <u>Appendix</u> of this Guide.

The RSA Security Analytics package consists of the following files:

Filename	File Function
hitachiidsuitepe.envision	SA package deployed to parse events from device integrations.
hitachiidsuitepe.xml	A copy of the device xml contained within the SA package.
table-map-custom.xml	Enables Security Analytics variables disabled by default.

Release Notes

Release Date	What's New In This Release
12/05/2013	Initial support for Privileged Access Manager and Password Manager.
2/29/2016	RSA SA 10.5 Support.

RSA Security Analytics Configuration

Deploy the enVision Config File

In order to use RSA Partner created content, you must first deploy the *Envision Config File* from the **Security Analytics Live** module. Log into Security Analytics and perform the following actions:

Important: Using this procedure will overwrite the existing table_map.xml.

- 1. From the Security Analytics menu, select **Live > Search**.
- 2. In the keywords field, enter: **Envision**. Security Analytics will display the **Envision Config File** in Matching Resources.
- 3. Select the checkbox next to **Envision Config File**.

🖗 Live 💿 🔍 Search	🛠 Configure 🔊 Feeds					
Search Criteria	Matching Resources	5				
Keywords	📰 Show Results 🕙 📔 Deta	📰 Show Results 🏾 🗐 Details 🧊 Deploy 🦒 Subscribe 🧩 Package 🛇				
envision	Subscribed Name	Created	Updated	Туре	Description	
Resource Types	🗹 yes Envision Config	🗹 yes Envision Config File 2014-03-07 11:50 AM 2015-12-14 7:53 AM RSA Log Device This file is used to upd				
	~					

4. Click **Deploy** in the menu bar.

🔞 Live 🛛 🔍 Sear	ch 🛠 Config	gure 🔊 Fe	eeds				
Search Criteria		Matching	g Resources				
Keywords		📓 Show Results 🛛 📓 Details 🔯 Deploy 🔊 Subscribe 💥 Package 🛛					
envision		Subscribed	Name	Created	Updated	Туре	Description
Resource Types		🗹 yes	🗹 yes Envision Config File 2014-03-07 11:50 AM 2015-12-14 7:53 AM RSA Log Device This file is used to up				This file is used to update the Log Device ba
	~						

5. Select **Next**.

Deployment Wizard						
Resources	Services		Rev	view	Deplo	у
Total resources : 1						
Resource Names	F	Resource Type	D	ependency of		
Envision Config File	F	RSA Log Device				
					Cancel	Next

6. Select the **Log Decoder** and select **Next**.

Deploym	nent Wizard			
R	esources	Services	Review	Deploy
Service	es Groups			
	Name		Host	Туре
	SA - IPDB Extractor		SA	IPDB Extractor
I	vm3099_log_Decoder		vm3099_log_Decoder	Log Decoder
			Cancel	Previous Next

Important: In an environment with multiple Log Decoders, deploy the Envision Config File to each Log Decoder in your network.

7. Select **Deploy**.

Deployment Wiz	Deployment Wizard								
Resources		Services	Review	Deploy					
Service	Service Type	Resource Name		Resource Type					
vm3099_log_De	Log Decoder	Envision Config File		RSA Log Device					
			Cancel F	revious Deploy					

8. Select **Close**, to complete the deployment of the Envision Config file.

Deployment Wiz	ard					
Resources	5	Services		Review		Deploy
Live deployment t	task finished success	fully				
Service Name	Resource Name		Status		Progress	
vm3099_log_Dec	Envision Config Fil	e	1 of 1			
						Close



Deploy the Security Analytics Integration Package

After completing the previous section, <u>Deploy the enVision Config File</u>, you can now deploy the Security Analytics Integration Package. Download the appropriate RSA Partner Integration Package, then log into Security Analytics to perform the following actions:

1. From the Security Analytics menu, select **Administration > Services.**

Administration		🖴 Hosts	Services	Svent Sources		es 🔍 Health & Wellness		🞏 System	n 📑 Security	y
① Dashboard						! One	or more licen	ises have expir	ed. Please see <u>Lic</u>	ensing Overview for additional details.
Investigation		🔟 vm3099_log_	vm3099_log_Decoder Config ☉							
-∿- Incidents		Data Reter	ntion Scheduler	App Rules	Correlati	ion Rules	Feeds	Parsers	Data Privacy	Appliance Service Configuration
🏳 Alerts										
🕁 Reports				Live	Date	Installed				
🔊 Administration		🚔 Hosts		N/A						
🖗 Live		Services								
👤 Profile		 Event Sour Health & V 	rces Vellness							
ပံ Sign Out		😂 System								
	-	🔒 Security								

2. Select your Log Decoder from the list, select **View > Config**.

· · · · · · · · · · · · · · · · · · ·
View >
Delete Edit
Start
Stop Restart

Important: In an environment with multiple Log Decoders, repeat on the deployment of the RSA Partner Integration Package on each Log Decoder.

3. Next, select the **Parsers** tab and click the **Upload** button.

🔎 Admini	stration \odot	🖴 Hosts	Services	Sevent So	ources 🔍 Healt	Health & Wellness		n 📑 Security	y
One or more licenses have expired. Please see <u>Licensing Overview</u> for additional details									
🚠 Change Se	A Change Service vm3099_log_Decoder Config ☺								
General	Files	Data Reten	tion Scheduler	App Rules	Correlation Rules	Feeds	Parsers	Data Privacy	Appliance Service Configuration
- 🛓 Upload									

4. From the *Upload Parsers* window, click the **+ Add** button and select the *.envision* file.

Upload Parsers				×
+ -	- Delete			
File Name	Progress	Start Time	File Name	Status
			Cancel	Upload

Important: The .envision file is contained within the .zip file downloaded from the RSA Ready Community.

5. Under the file name column, select the integration package name and click **Upload**.

Upload Parsers					×
+ -	-				
File Name 🔨		Progress	Start Time	File Name	Status
hitachiidmsuitepe.envision					
	4				
				Cancel	Upload

READY

6. Upon completion of the upload click **Cancel**.

Upload Parsers				×
+ -	- Delete			
File Name	Progress	Start Time	File Name	Status
		2016-02-10 11:16:04	hitachiidmsuitep	Completed
			Cancel	Upload

 Connect to the Security Analytics Log Decoder Server using WinSCP. Copy the table-mapcustom.xml file from the contents of the .zip file to the /etc/netwitness/ng/envision/etc folder. If the table-map-custom.xml file already exists on the log decoder(s), enter only the contents between the <mappings>...</mappings>.

<mappings>

<mapping envisionName="result" nwName="result" flags="None" envisionDisplayName="Result|Volume|Information|Reason|Succeed/Failed"/><mapping envisionName="sessionid" nwName="log.session.id" flags="None"/>

</mappings>

8. Navigate to Administration > Services and check the Log Decoder(s) then click Restart.

•	vm3099_log_Decoder	0	vm3099_log_Decoder	Log Decoder	10.5.0.0.5307	• •
•	vm3101 - Concentrator	•	vm3101	Concentrator	10.5.0.0.5307	View >
0	vm3108.pe.rsa.net - Warehouse Connector	0	vm3108.pe.rsa.net	Warehouse Connector	onnector Edit	
0	vm3109.pe.rsa.net - Warehouse Connector	0	vm3109.pe.rsa.net	Warehouse Connector		Start
						Stop Restart

9. Navigate to Administration > Services and check the Log Decoder(s) then click View> Config.

2	vm3099_log_Decoder	9	vm3099_log_Decoder	Log Decoder	10.5.	0.0.5307		\$ •
	vm3101 - Concentrator	•	vm3101	Concentrator	10.	System	View	>
) vm3108.pe.rsa.net - Warehouse Connector	ause Connector O vm3108.pe.rsa.net Warehouse Connector		Warehouse Connector		Stats Config	Delete Edit	
□ c) vm3109,pe.rsa.net - Warehouse Connector	0	vm3109.pe.rsa.net	Warehouse Connector		Explore Logs Security	Start Stop Restart	

10. The new device is listed under the Log Decoder(s) General Tab within the Service Parsers Configuration.

Service Parsers Configuration		Enable All	Disable All
Name	Config Value		
hitachiidmsuitepe	\checkmark		•

11. The Log Decoder is now ready to parse events for this device. Below is an example of the RSA SA metadata collected from an Absolute DDS logfile.

Event Reconstr	uction						₿₽×
service 10.100.52.173	id 71354	type Log	service type hitachiidmsuite	service class Access Control	event source kevink-w2k864_default		
📳 View Meta	🔳 Viev	v Log	👜 Export Logs	📮 Open Event in Nev	v Tab		Cancel
sessionid		71354					
time	=	2016-0	2-10T11:20:34.0				
size	=	227					
device.ip	-	10.1	00.52.173 📀				
medium	=	32					
device.type	-	"hita	achiidmsuitepe" 💿				
device.class	=	"Acc	ess Control" 📀				
header.id	=	"0001"					
event.source	=	"kev	ink-w2k864_default"	\odot			
process	=	"psf	"				
log.session.id	=	"Se121	 f68c8-0a78-44d5-b3b	2-b5aca70d90ad"			
username	=	"sup	oeruser" 📀				
username	-	"sup	oeruser" 💿				
alias.host	=	"(nu	ID				
user.dst	=	"sup	eruser" 📀				
result	-	"\$INTE	ERNAL_password.pss				
ip.src	=	10.0	.35.1 🛞				
level	=	5					
msg.id	=	"ULC	GN1" ⊗				
event.cat.nam	e =	"Use	er.Activity.Failed Logi	ns" 💿			
< >	_	_				Viewing Log 📋 Show Rec	onstruction Log



Partner Product Configuration

Before You Begin

This section provides instructions for configuring the Hitachi ID Management Suite with RSA Security Analytics. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All Hitachi ID Management Suite components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Configuration

Deploy the ODBC Event Source Type XML

The ODBC Event Source Type XML, hitachiidmsuite.xml, is included in the partner package downloaded from the Security Analytics Community. The first step is to deploy this file to the Security Analytics Log Collector.

- 1. Log into the Log Collector via file transfer protocol (e.g. SFTP).
- Transfer the hitachiidmsuite.xml file to the following directory: /etc/netwitness/ng/logcollection/content/collection/odbc.
- 3. Change the file permissions on the file to **755**.
- 4. **Restart** the Log Collector service.

Configure an ODBC Event Source

After deploying the ODBC Event Source Type XML, add the Data Source Name (DSNs) to the configuration.

- 1. From the Security Analytics menu, select **Administration > Devices**.
- 2. In the Devices pane, select the **Log Collector** device.
- 3. In the toolbar, select **View > Config**.
- 4. Click the **Settings** tab.

5. From the left side menu, select **DSNs** and click **+**.

🧀 Administr	ation 💿	Devices	I⊟ Ta	sks 🖵 System						
嚞 Change Device 🗏 🖳 vm3093 💙 🌞 Config 💿										
General	Files	Event Sou	rces	Event Destinations	Settings	Appliance Service Configuration				
Lockbox Certificates DSNs	Lockbox DSNs Certificates + - Z									
SNMP v3 User	Manager	DSN ^	Par	ameters						

- 6. Enter a name in the **DSN Name** field.
- 7. Select the + and specify the value pairs and click **Save**.

Note: Refer to <u>ODBC Value Pairs</u> for a list of the value pairs for the ODBC event sources supported in this release.

Add DSN	8
DSN Name *	mssqlAudit
Parameters	
+ -	
Name ^	Value
Description	DataDirect 7.1 MS SQLServer Wire Protocol
√ database	audit
driver	/opt/netwitness/odbc/lib/R3sqls26.so
hostname	1.1.1.1
portnumber	12345
	Cancel Save

8. Select the **Event Sources** tab.

9. Select **ODBC** from the drop-down menu.

Administration	n E	🗄 Devices 📒	Tasks	Syst	tem		明の	RSA	Security Analytics
🛔 Change Device 🛛	🖳 Sand	dys Collector 🚿 👙	Config						
General F	iles	Event Sources	Ev	ent Destin	ations	Settings	Арр	liance Servio	e Configuration
ODBC	~								
Event Catego	ories								
+ -									
Name ^		DSN							al MaxEvents PerCy
mssql									5000

10. Click + the **Available Event Source Types** dialog is displayed. Select the Event Source Type which was deployed in the previous section, **Deploy the ODBC Event Source Type XML** and click **OK**. In this example we'll use a predefined event source, **mssql**.

Avai	Available Event Source Types									
	Туре ^									
	mckessonhpf	^								
	ms_forefront_uag									
	msnap									
✓	mssql									
	mswsus									
	netflowanalyzer_conversation	Ţ								
	Cancel									
	Cancel OK									



11. Under the Name column, **select** the Event Source Type that was added and click + in the DSNs pane.

Administration 🛛 🗏 Devices 🔚 Tasks 🖵 System										
🚠 Change Device 🕮 vm3093 👌 🌞 Config 👳										
General	General Files Event Sources Event Destinations Settings Appliance Service Configuration									
ODBC	~									
Event Cate	egories	DSNs								
+ -	+ - 🗹 🏝 Import DSN 🕐 Export DSN									
Name ^	Name ^ DSN Address									
🔽 mssql	V mssql									

12. Select the DSN you create from the drop down list, specify or modify the other parameters as required, and click **OK**.

Add DSN		8
DSN *	mssqlAudit	~
Address	127.0.0.1	
Username *	audit_reader	
Password	•••••	
Max Cell Size	2048	~
Nil Value	(null)	
Polling Interval	180	~ ~
Max Events PerCycle	5000	~ ~
Initial Tracking Id		
Enabled		
Debug	0	~
Filename	C:\MyTraceFiles	
	Cancel	OK



13. The newly defined DSN is displayed in the DSNs panel.

Event Sources	Security	Â	opliance Service						
Event Sources + - Z + Bulk Import DSN 🖄 Bulk Export DSN Z Bulk Edit DSN									
+ -			DSN	Address	Username	Max Cell Size	Nil Value	Polling Interval 🔨	Max Events PerCycle Initial Tracking Id
Name ^			mssqlAudit	127.0.0.1	audit_reader	2048	(null)	180	5000
🗹 mssql									

Start the ODBC Collection Service

The final configuration step is to start the ODBC Service within Security Analytics. For complete instructions, refer to *Configure Log Collection* in the SA online help documentation.

Certification Checklist for RSA Security Analytics

Date	Tested:	February	29,	201	6
------	---------	----------	-----	-----	---

Certification Environment							
Product Name	Version Information	Operating System					
RSA Security Analytics	10.5	Virtual Appliance					
Hitachi ID Privileged Access	7.1.X, 7.2.X, 7.3.x	Windows 2003/2008/2008 R2					
Manager							
Hitachi ID Password Manager	7.1.X, 7.2.X, 7.3.x	Windows 2003/2008/2008 R2					

Security Analytics Test Case	Result
Device Administration	
Partner's device name appears in Device Parsers Configuration	
Device can be enabled from Device Parsers Configuration	
Device can be disabled from Device Parsers Configuration	✓
Device can be removed from Device Parsers Configuration	
Investigation Device name displays properly from Device Type Displays Meta Data properly within Investigator	✓ ✓

✓ = Pass × = Fail N/A = Non-Available Function

Appendix

Security Analytics Disable Device Parser

To disable the Security Analytics Integration Package but not delete the XML from the system, perform the following:

1. Navigate to Administration > Services and check the Log Decoder(s) then click View > Config.

۷ .	vm3099_log_Decoder	0	vm3099_log_Decoder	Log Decoder	10.5.	0.0.5307	ی چ	
	vm3101 - Concentrator	۲	vm3101	Concentrator	10.	System	View >	
0	vm3108.pe.rsa.net - Warehouse Connector	0	vm3108.pe.rsa.net	Warehouse Connector		Stats Delete Config Edit		
00	vm3109,pe.rsa.net - Warehouse Connector	0	vm3109.pe.rsa.net	Warehouse Connector		Explore Logs Security	Start Stop Restart	

2. From the **Service Parses Configuration** window, scroll down to the device you wish to disable and uncheck the Config Value checkbox.

Service Parsers Configuration		Enable All	Disable All
Name	Config Value		
hitachiidmsuitepe	\checkmark		•

3. Click **Apply** to save settings.

Security Analytics Remove Device Parser

To remove the Security Analytics Integration Package files from the environment, perform the following:

- 1. Connect to the Security Analytics Log Decoder/Collector Server using SSH and open the /etc/netwitness/ng/envision/etc/devices folder.
- 2. Search for the device you are targeting for removal and delete the folder containing the device xml.
- 3. Returning the system to its original state will require either modifying or removing the **tablemap-custom.xml** based on your systems configuration. The table-map-custom.xml file is located in the **/etc/netwitness/ng/envision/etc** folder of the SA Log Decoder(s).