Real-Time Security Information Management

[Bug 2911] Aladdin eSafe Log Format Modifications between Versions 4.0 and 4.2

Applies to: Net Report Version 3.12 Status: Patch available Last Review: Friday June 10, 2005

Symptoms

NetReport filter engine cannot parse eSafe log files which come from Aladdin eSafe 4.2.

Cause

This is due to the format changes which been made between versions 4.0 and 4.2 of Aladdin eSafe.

Please note the differences between the headers for the Aladdin eSafe log files for versions 4.0 and 4.2 $\,$

Aladdin eSafe Version 4.0 Log File Header: Date (yyyy-mm-dd HH:mm:ss)|FileName|FileType|ProtocolType|Source|Destination|Result|URL category|Details

Aladdin eSafe Version 4.2 Log File Header: Date (yyyy-mm-dd HH:mm:ss)|Protocol|Event|File Name\Mail Subject|Source|Destination|Details

The field names in the Aladdin eSafe version 4.2 log file have been changed and certain fields have disappeared entirely.

Solution

To resolve this problem, please perform the following tasks:

- Task 1: Launching the Net Report Management Console.
- **Task 2:** Creating an Aladdin eSafe Filter in the Net Report Management Console.
- Task 3: Downloading the Aladdin eSafe Support 4.2 Patch 2911 package in the Net Report Packages Server.
- **Task 4:** Creating an Aladdin eSafe Flat File Parser in the Net Report Management Console.
- Task 5: Creating the Data_eSafe_Mail table
- Task 6: Creating the Data_eSafe_Gateway table
- **Task 7:** Applying changes in the Universal Log Analyser in the Net Report Management console.
- **Task 8:** Downloading and Installing the Aladdin eSafe-related Device Report Project *.zip file from Net Report Web site's Device Report Projects page.

Task 1: Launching the Net Report Management Console

To launch the Net Report Management Console, please follow the steps below:

Steps

- 1. Select **Start> All Programs> Net Report> Management Console**. The **Login** dialog box appears.
- 2. Enter your Login and Password (as appropriate).

<mark>≪°</mark> Login			×
ی 6	Login :	netreport	OK
5	Password :	*********	Cancel

3. Click OK. The Net Report Management Console appears.

Task 2: Creating an Aladdin eSafe Filter in the Net Report Management Console.

This section only applies to those users who have not yet configured an Aladdin eSafe Filter. If you have already configured an Aladdin eSafe Filter, please skip this section and go directly to Task 3.

To create a Aladdin eSafe Filter, please follow the steps below:

Steps

1. Select Console root> Net Report> [Localhost]> ULA> Filters in the left Console root pane.



2. Select Aladdin eSafe in the Choose a Filter drop-down list.





3. Click the **New filter** icon \square . The **Aladdin eSafe** filter appears.

+ netreport - [Console root\NetReport\proxy\ULA*\Filters]					
💠 Eile Action View Favorites Window	Help	_ B ×			
⇔ → € 🖪 😫					
Console root Console root Proxy Packages Server CuLA* Settings Console root ULA* Console root Console roo	IIFilters Aladdin eSafe □ EngineEvent	Filters >NetReport/proxy/ULA/Filters<			
Ing Phig Redus Proxy Syslog Parser	D Selected Log Sources	Choose a Filter 💽 🖓 🛍 🛣			

4. Select **Console root> NetReport>[localhost]> ULA** in the left **Console root** pane. The **Universal Log Analyser** screen appears in the right pane.

Note: please note the asterisk adjacent to the **ULA** branch in the **Console root** tree structure. This asterisk indicates that you must save the changes you made to the filters. All the changes you made locally will be sent to the filters.



5. Click **Apply Changes**. Note that the asterisk disappears from the **ULA** branch in the left **Console root** pane.

Real-Time Security Information Management

Task 3: Downloading the Aladdin eSafe Support 4.2 Patch 2911 package in the Net Report Packages Server

To download the Aladdin eSafe Support 4.2 Patch 2911 package in the Net Report Packages Server, please follow the steps below:

Steps

1. Select **Console root> Net Report> [localhost]/ Packages Server** in the left **Console root** pane. The **Welcome to the NetReport Packages Server** screen appears in the right pane.



2. Enter the following address in the **Server Address** field: http://www.netreport.fr/packages/new

🚸 netreport - [Console root\NetReport\proxy\Packages Server]				
Eile Action View Favorites	Window Help			
← → 🗈 🖬 🔮				
Console root	Server Address: http://www.netreport.fr/packages/new			
E Proxy ☐ Packages Server E ↓ ULA E ↓ Agents	Welcome to NetReport Package Server			
	Here you can connect to a server in order to download new actions and upgrades. Simply enter the URL of your package server and click on You can also choose to connect to your local server by clicking <u>here</u>			
ļļ.				

5 Copyright © 2005 Net Report. All rights reserved. http://www.net-report.net 3. Click the **Connect to Server**[§] button. The **NetReport Packages** screen appears in the right pane.



4. Click the **Install this Package** icon. The **This will erase your previous configuration for this equipment** message appears.



Real-Time Security Information Management

5. Click OK. The Installation Complete dialog box appears.



- 6. Note the steps which you must perform to complete the patch installation if you haven't already installed the Aladdin eSafe device before:
 - Configure the Flat File Parser.
 - Create the Data_eSafe_Mail table.
 - Create the **Data_eSafe_Gateway** table.
 - Download the Device Report Project.

Please see Tasks 4, 5, 6 and 8 for further instructions.

7. Click **OK**.

Task 4: Creating an Aladdin eSafe Flat File Parser in the Net Report Management Console.

This section is only for those users who have not yet configured an Aladdin eSafe Flat File Parser. If you have already configured an Aladdin eSafe Flat File Parser, please skip this section and go directly to Task 4.

To create an Aladdin eSafe Flat File Parser, please follow the steps below:

Steps

1. Select Console root> Net Report> Localhost> Agents> Flat File Parser> Configurations in the left Console root pane.

🚸 netreport - [Console root\NetReport\proxy\Agents\Flat File Parser*\Configurations]				
🕸 File Action View Favorites Window Help				
← → 🗈 🖬 😫				
Console root	2	Flat F	File Agent Co	onfigurations
E A ULA*		>NetReport/p	roxy/Agents/Flat File	Parser/Configurations<
🖻 🛷 Agents 🕀 🗟 Check Point (Real Time)	🗄 Configu			
Event Scheduler	. Name	Spied Directory	File Name	ActiveDriver
 ☐ Flat File Parser* ☐ Gonfigurations ☐ Microsoft WMI ④ NetReport Communication ○ Ping ○ Radius Proxy ○ SQLServer Spyer ○ Syslog Parser 	0 Selected File spy	Choose a Driver		

2. Select Aladdin eSafe in the Choose a Driver drop-down list.

>> netreport - [Console root'\NetReport\proxy\Agents\Flat File Parser*\Configurations] X ● File Action View Favorites Window Help X				
Console root Console root Packages Server Packages Server Consoleration Con	Flat File Agent Configurations NetReport/proxy/Agents/Flat File Parser/Configurations Configuration			
Event Scheduler	. Name	Spied Directory	File Name	ActiveDriver
Brit Hie Parser* Brit Hie Parser* Arrow Horson WMI WetReport Communication Ping Ping Sulfarver Spyer Syslog Parser	0 Selected File spy	Choose a Driver Choose a Driver Aladdin eSafe (FR2 Format) Apache ARKOON Network Security Blue Coat Check Point FireWall-1 Cisco PX Clavister Fortinet FortiGate Generic Parser IBM Lotus Domino		
	r			

8 Copyright © 2005 Net Report. All rights reserved. http://www.net-report.net

3. Click the **New file spy** icon L. The **Aladdin eSafe** spy Configuration details appear in the **Configuration** sub-section table.



- 4. Enter the Directory you want Net Report to spy on in the **Spied Directory** column.
- 5. Select **Console root> NetReport> localhost> Agents> Flat File Parser** in the left **Console root** pane. The **Flat File Agent** screen appears in the right pane.

Note: please note the asterisk adjacent to the **Flat File Parser** branch in the **Console root** tree structure. This asterisk indicates that you must save the changes you made to the Flat File Agent. All the changes you made locally will be sent to the Flat File Agent.



Real-Time Security Information Management

6. Click **Apply Changes**. Note that the asterisk disappears from the **Flat File Parser** branch in the left **Console root** pane.

Task 5: Creating the Data_eSafe_Mail Table

This section is only for those users who have not yet configured the Aladdin eSafe device (during the configuration wizard for example). If you have already configured an Aladdin eSafe device, please skip this section and go directly to **Task 7**.

To create the **Data_eSafe_Mail** table, please follow the steps below:

Steps

1. Select Console root> Net Report> Localhost> ULA> Filters> Aladdin eSafe>Insert into Data_eSafe_Mail in the left Console root pane.

🚸 netreport - [Console root\NetReport\proxy\ULA\Filters\Aladdin eSafe\Actions\Insert into Data_eSafe_Mail]					
Eile Action View Favorites Window Help				_8	
Console root NetReport Proxy Packages Server ULA E	>NetReport/proxy/U	Insei JLA/Filters/Aladdin eS	rt into Data Safe/Actions/Insert	_eSafe_Mail	
E 😽 Filters	"Configuration 🔍				
	Connection : Dat	Connection : Database Connection			
	Table : □ Dron Table			✓ Create Table	
Count Events with the Same Viru	Source Field	Destination Field	Туре	Length Decimal	
Insert into Data_eSafe_Mail	😇 Orig	"Orig"	VarChar 💌	50 0	
Message Box	ອ Date	"Time"	DateTime 💌	15 0	
Stop Group	ອ FileName	"FileName"	VarChar 💌	235 0	
- 🙀 Update Aladdin eSafe records ar	ອ FileType	"FileType"	Char 💌	50 0	
Update Aladdin eSafe records ra	ProtocolType	"ProtocolType"	Char 💌	30 0	
Fields	ອ Result	"Result"	Char 💌	50 0	
Dictionary	Source	"Source"	Char 💌	80 0	
Agents Geek Point (Real Time)	🧧 From_Domain	"From_Domain"	VarChar 💌	128 0	
	Destination	"Destination"	VarChar 💌	180 0	
E Int File Parser	ອ To_Domain	"To_Domain"	VarChar 💌	128 0	
Image Configurations	ອ Details	"Details"	VarChar 💌	280 0	
🛨 📲 Microsoft WMI	😇 Virus	"Virus"	VarChar 💌	50 0	
	VirusFile	"VirusFile"	Char 🔽	15 0	
adius Proxy	Dst_Type	"Dst_Type"	Char 🔽	15 0	
E 🛃 SQLServer Spyer	Cat_Site	"Cat_Site"	VarChar 🔽	128 0	
	Family	"Family"	VarChar 💌	25 0	
	Reason	"Reason"	VarChar 🔻	30 0	
	😅 Туре	"Туре"	Char 🔽	15 0	
	No Fields Selected		bad_record	↑↓□ : : 3	
	J				

2. Click the Create Table icon.



3. Click the **OK** button. This will create a new **Data_eSafe_Mail** table in the **netreport** database.

Task 6: Creating the Data_eSafe_Gateway Table

This section is only for those users who have not yet configured the Aladdin eSafe device (during the Configuration Wizard for example). If you have already configured an Aladdin eSafe device, please skip this section and go directly to **Task 7**.

To create the **Data_eSafe_Gateway** table, please follow the steps below:

Steps

1. Select Console root> Net Report> Localhost> ULA> Filters> Aladdin eSafe>Insert into Data_eSafe_Gateway in the left Console root pane.

netreport - [Console root\NetReport\proxy\ULA\Filters\Aladdin eSafe\Actions\Insert into Data_eSafe_Gateway]						
🕸 Eile <u>A</u> ction <u>V</u> iew Fav <u>o</u> rites <u>W</u> indow <u>H</u> elp				_ <u>- 8 ×</u>		
Console root	.			4		
E wetReport	RN	Insert inte	o Data leS	afe Gateway		
⊡ froxy						
Packages Server		>NetReport/proxy/ULA/Filters/Aladdin eSafe/Actions/Insert into				
E Settings						
□ • • • Filters	8.0 (1)					
🗓 🞇 EngineEvent	aConfig	uration		\mathbf{w}		
🕀 😰 Database Aggregation	Connection : Dat	tabase Connection	•			
🖃 🥏 Aladdin eSafe	Det					
Count Events with the Same Viru	Table :	a_eSate_Gateway		✓ Create Table		
Insert into Data eSafe Gateway		Drop Table				
Insert into Data_eSafe_Mail	Source Field	Destination Field	Туре	Length Decimal		
Message Box	😂 Orig	"Orig"	VarChar 💌	50 0		
Stop All	ອ Date	"Time"	DateTime 💌	15 0		
Undate Aladdin eSafe records an	😑 FileName	"FileName"	VarChar 💌	235 0		
Update Aladdin eSafe records ra	FileType	"FileType"	Char 🔻	50 0		
	ProtocolType	"ProtocolType"	Char 💌	30 0		
Dictionary	Result	"Result"	Char 🔻	50 0		
Agents	Source	"Source"	Char 🔻	80 0		
⊡ Scheck Point (Real Time)	Destination	"Destination"	VarChar 💌	180 0		
	🧧 To_Domain	"To_Domain"	VarChar 💌	128 0		
Configurations	ອ Details	"Details"	VarChar 💌	280 0		
Microsoft WMI	😇 Dst_Type	"Dst_Type"	Char 💌	15 0		
NetReport Communication	🧧 Cat_Site	"Cat_Site"	VarChar 💌	128 0		
	No Fields Selected	l i i i i i i i i i i i i i i i i i i i	bad_record	- 🕈 🗸 🗅 🛍 🚦 😵		
🗄 런 SQLServer Spyer			,			
⊞⊶📰 Syslog Parser						

2. Click the **Create Table icon**.

Microsoft Internet Explorer					
?	This action will: - create new table 'Data_eSafe_Gateway'				
	Do you want to continue?				
	OK .	Cancel			

3. Click the **OK** button. This will create a new **Data_eSafe_Gateway** table in the **netreport** database.

Real-Time Security Information Management

Task 7: Apply changes to the Universal Log Analyser in the Net Report Management Console.

To apply changes to the Universal Log Analyser, please follow the steps below:

Steps

1. Select **Console root> NetReport>[localhost]> ULA** in the left **Console root** pane. The **Universal Log Analyser** screen appears in the right pane.

Note: please note the asterisk adjacent to the **ULA** branch in the **Console root** tree structure. This asterisk indicates that you must save the changes you made to the filters. All the changes you made locally will be sent to the filters.



2. Click **Apply Changes**. Note that the asterisk disappears from the **ULA** branch in the left **Console root** pane.

Task 8: Downloading and Installing the Aladdin eSafe-Related Device Report Project zip from Net Report Web Site's Device Report Projects Download Page.

To download and install the Device Report Project for the Aladdin eSafe patch, please follow the steps below:

Steps

- 1. Go to the Net Report **Device Report Projects Download** page, by clicking the link below: http://82.127.62.167/us/downloads/DOW_REPORT.asp
- 2. Select **3.12** as the Net Report Version in the drop-down list.



- Alto://82.127.62.167/us/HomePage/NetReportHome.htm
- 3. Select **Anti-Virus** as the device type in the drop-down list. The Device Report Projects which are available for Proxy Server Devices appear.
- 4. Select either the SQL Server or Oracle eSafe Statistics Report Project by clicking the adjacent zip icon.

Real-Time Security Information Management

- 5. Select the directory to save the Device Report Project *.zip file to.
- Extract the *.wfv files from the *.zip file to the following directory on the Net Report Web Portal host: c:\Program Files\NetReport\WebPortal\Runtime_Projects\enu (or equivalent).

Real-Time Security Information Management

Further Information

