

DEPLOYMENT GUIDE

Fortinet and IBM Resilient



Fortinet and IBM Resilient

Overview	3
Deployment Prerequisites	3
Architecture Overview	3
FortiAnalyzer Configuration	4
IBM Resilient Configuration	6
Summary	9

Overview

Fortinet (NASDAQ: FTNT) secures the largest enterprise, service provider, and government organizations around the world. Fortinet empowers its customers with intelligent, seamless protection across the expanding attack surface and the power to take on ever-increasing performance requirements of the borderless network—today and into the future. Only the Fortinet Security Fabric architecture can deliver security features without compromise to address the most critical security challenges, whether in networked, application, cloud, or mobile environments. Fortinet ranks #1 in the most security appliances shipped worldwide and more than 400,000 customers trust Fortinet to protect their businesses. Learn more at https://www.fortinet.com, the Fortinet Blog, or FortiGuard Labs.

About IBM Resilient

IBM Resilient Incident Response Platform (IRP) is the leading platform for orchestrating and automating incident response processes. IBM Resilient IRP quickly and easily integrates with your organization's existing security and IT investments. It makes security alerts instantly actionable, provides valuable intelligence and incident context, and enables adaptive response to complex cyber threats.

Architecture Overview



- Fortinet FortiAnalyzer version
 (tested with version 6.0.0)
- 2.IBM Resilient version 30.x (tested with version 30.0.3476)
- With Email Connector version 2.2 installed





FortiAnalyzer Configuration

Create and configure an Email Server. From System Settings, go to **Mail Server > Create New**.

System Settings 🛩						v ninte 🔝 0
(Cashboard	+ Create New @ Eat: @ D	wlata 🕎 Tact				9
CLOSER'S Topology	C Seq.#	SMTP Server Name	SMTP Server	SMTP Server Port	E-Mail Account	
@ AILADOMs	01	fectivet	wait.fortiset.com	25	kgalaugher@fortinet.com	
C Storage Iv/o	0 2	LabMall	10.101.32.68	25	fortbiere@win2008.lab.lac	
O Network						
A 14						
1 Admin	*					
Administrators						
Prohio						
Remote Authentication Server	2					
Admin Settings						
EB Certificates	*					
Local Certificates						
CA Certificates						
CRL						
# Log Forwarding						
El Patather Management						
E Event Lag						
Task Menitor						
By Advanced	v					
SNMP						
Mal Server						
Sysing Server						
Meta Flaids						
Device Lag Settings						
File Management						
Advanced Settings						

Enter a name to identify the mail server, the hostname, or IP address of your mail server and the SMTP port (typically 25). Be sure to enable Authentication if your mail server requires it. Then, enter a valid Email address and password for the Account. Click **OK** when done.

System Settings 🗸				🕄 🕖 🙆 admin 🗸
(B Destributed	Create New Mail Server Settings			
Eff Exhan Sublega v Orbantoord Scharpte Produce DefA 20056 Orbane Strange Min Orbane Annin Sublema Blantend Blantend Blantend Blantend Blantend Shift Fata Brane Sublema Su	Create Hole Mail Server Setting DATT Server Name Hail Server SatT Server Port (Trainte Antheniation Planmad Planmad	Corpland Industrations 26 D Interedignetalisane.com 10 Interedignetalisane.com		🕄 🗭 遵 sinin -
Advanced Settings				
			OK Cavel	

The screen shot should look like the image below.

	NAMES AND POST OFFICE ADDRESS OF TAXABLE PARTY.				
() Deshboard	+ Create New G Edit 1	Doleta 🛃 Test			
■ÉLogging Tepelogr	D Seq#	SMTP Server Name	SMTP Server	SMTP Server Port	E-Mail Account
B AI ADOMs	01	Sartinat	realLifortinet.com	25	kgslaugher@fertinet.com
O Starsge Info	0 2	LabMell	10.101.32.40	25	for tisiere@wix2000 lab.los
Q Network	0 9	CorpEnall	setavnymaloerve.com	25	far finet@mynailserver.vem
Ана					
L Admin *					
Administrators					
Profile					
Remote Authentication Server					
Admin Sattings					
RD Certificates *					
Local Certificates					
CA Certificates					
CRL					
# Log Forwarding					
Retcher Management					
BENT Log					
Task Monitor					
h Advanced v					
SNMP					
Mail Server					
Syslog Server					
Meta Fields					
Device Log Settings					
File Management					
Advanced Settines					

Configure FortiAnalyzer to send Email Alerts when certain Events occur. Click **System Settings** from the top left then choose **Event Manager**.



From this view you can see there was an HTTP Event specifically about Application Control. On the right, the Handler is where Email Alerting is configured.

Event Manager 🗸										🖸 🖉 🙆 admin 🗸
Event Monitor	~	Add	filer		🔍 🗘 Refresh + 🛛 Last 7 Days	Collapse All	Show Acknowled	ged		± & m -
All Events			Event	Event Status	Event Type	Count	Severity	¥ Last Update	Additional Info	Handler
Calendar View		0 1	~Proxy.HTTP (335)					16 minutes ago		
& Custom View	>		app:Proxy.HTTP		Application Control	2	Critical	2018-06-06 10:10:58		UTM App Ctrl Event
Event Handler List	1	0	app:Proxy.HTTP		Application Control	2	Critical	2018-06-06 09:40:48		UTM App Ctrl Event
f Incidents	¥ 1		app:Proxy.HTTP		Application Control	2	Critical	2018-06-06 09:10:48		UTM App Ctrl Event
fl All Incidents		D	app:Proxy.HTTP		Application Control	3	Critical	2018-06-06 08:57:48		UTM App Ctrl Event
E FortiGate Event Handlers			app:Proxy.HTTP		Application Control	2	Critical	2018-06-06 08:10:38		UTM App Ctrl Event
CT CONCERNMENT OF STOLES	1		app:Proxy.HTTP		Application Control	12	Critical	2018-06-06 07:57:36		UTM App Ctrl Event
			app:Proxy.HTTP		Application Control	2	Critical	2018-06-06 07:10:28		UTM App Ctrl Event
		0	app:Proxy.HTTP		Application Control	2	Critical	2018-06-06 06:40:18		UTM App Ctrl Event
			app:Proxy.HTTP		Application Control	2	Critical	2018-06-06 06:10:18		UTM App Ctrl Event
	3		app:Proxy.HTTP		Application Control	2	Critical	2018-06-06 05:40:08		UTM App Ctrl Event

In this example, we will configure an Email Alert to be sent when there is an Admin logon failure via SSH. Click Collapse All.

Event Manager 🗸										🖸 🖉 🚺 admin 🗸
Event Monitor	~	Add	Rer		🔍 💭 Refresh + 🛛 Last 7 Days +	Collapse All	Show Acknowled	land		1 A 🖩 -
All Events			Event	Event Status	Event Type	Count	Severity	▼ Last Update	Additional Info	Handler
Calendar View	0	1	✓Proxy.HTTP (335)					21 minutes ago		
& Custom View	> 0	2	app:Proxy.HTTP		Application Control	2	Critical	2018-06-06 10:10:58		UTM App Ctrl Event
Event Handler List	C	1	app:Proxy.HTTP		Application Control	2	Critical	2018-06-06 09:40:48		UTM App Ctrl Event
Incidents	~ [3	app:Proxy.HTTP		Application Control	2	Critical	2018-06-06 09:10:48		UTM App Ctrl Event
I All Incidents	1	3	app:Proxy.HTTP		Application Control	3	Critical	2018-06-06 08:57:48		UTM App Ctrl Event
III FortiGate Event Handlers	0	2	app:Proxy.HTTP		Application Control	2	Critical	2018-06-06 08:10:38		UTM App Ctrl Event
	C	3	app:Proxy.HTTP		Application Control	12	Critical	2018-06-06 07:57:36		UTM App Ctrl Event
	C	3	app:Proxy.HTTP		Application Control	2	Critical	2018-06-06 07:10:28		UTM App Ctrl Event
	0	2	app:Proxy.HTTP		Application Control	2	Critical	2018-06-06 06:40:18		UTM App Ctrl Event
	C	3	app:Proxy.HTTP		Application Control	2	Critical	2018-06-06 06:10:18		UTM App Ctrl Event

Then locate the Event User login from SSH. Click Local Device Event under the Handler.

Event Manager ~										[] Ø 😡 admin 🗸
Event Monitor	×	Add F	itor	c	🗈 💭 Refresh + 🛛 La	st 7 Days	- ,* Exp	and All 🔲 Show Ackne	owiedged	± & m -
All Events	C		Event	Event Status	Event Type	Count	Severity	▼ Last Update	Additional Info	Handler
Calendar View		1	> Proxy.HTTP (335)		Application Control	1371	Critical	23 minutes ago		UTM App Ctrl Event
& Custom View	> 0	2	> Remove local db (14)		Event	14	Medium	3 hours ago	-	Local Device Event
Event Handler List		3	> Trim local db (14)		Event	14	Medium	3 hours ago	Requested to trim database tables older than 60 days to enforce the retention policy of Adom root	Local Device Event
@ Incidents	~ 0	4	> SSL Message Authentication Code corrupted (7)		Event	49	Medium	12 hours ago	Corrupted MAC packet detected	FOS Event Log Higher T
All Incidents		5	> User login/logout failed (7)		Event	21	Medium	12 hours ago	user () [;;]; echo Piugin output: \$((1+' login failed from teinet(10.101.32.173)	Local Device Event
E FortiGate Event Handlers		6	> User login from SSH (7)		Event	7	Medium	12 hours ago	A user login failed from ssh	Local Device Event
		7	> User login failed (7)		Event	7	Medium	18 hours ago	Device FGVMD40000101072 login failed for restapi request due to empty user name.	Local Device Event
	0	8	> User login from SSH failed (2)		Event	9	Medium	18 hours ago	-	Local Device Event
		9	> Admin login failed (2)		Event	4	Medium	18 hours ago	-	FOS Event Log Higher T
		10	logdesc:Admin login disabled		Event	1	Medium	2018-06-05 16:18:43	Login disabled from IP 10.101.32.254 for 60 seconds because of 3 bad attempts	FOS Event Log Higher T
		11	> Files dropped by quarantine daemon (12)		Event	20	Medium	A day ago	-	FOS Event Log Higher T
		12	desc:Send mail failed		Event	1	Medium	2018-06-04 16:26:46	Failed to send a test email to igailaugher@fortinet.com through LabMail.	Local Device Event
		13	logdesc:FortiGate update failed		Event	1	Medium	2018-06-03 08:43:56	Fortigate scheduled update failed	FOS Event Log Higher T
		14	>Malicious Websites (16)		O Web Filter	45	Medium	6 days ago		UTM Web Filter Event

Enable **Send Email Alert** under Notifications. Enter the Email address you want to send Alerts to. Enter the Email address you want to use as the sender address. Enter a Subject for the Email. Lastly, under Email Server, choose the Email Server created previously.

	ON	
Name	Local Device Event	
Description	Default local device event handler	
Devices	OAII Devices OSpecify	
Filters		+
Filter 1		>
Send Alert Email	resilient@mymailserver.com fortianalvzer@mymailserver.com	
	User Logon failed via SSH	
Subject		
Subject Email Server	CorpEmail: smtp.mymailserver.com	- +
Subject Email Server □Send SNMP(v1/v2) Trap	CorpEmail: smtp.mymailserver.com fortinet: mail.fortinet.com	• +
Subject Email Server Send SNMP(v1/v2) Trap	CorpEmail: smtp.mymailserver.com fortinet: mail.fortinet.com LabMail: 10.101.32.68	• +
Subject Email Server Send SNMP(v1/v2) Trap Send SNMP(v3) Trap	CorpEmail: smtp.mymailserver.com fortinet: mail.fortinet.com LabMail: 10.101.32.68 CorpEmail: smtp.mymailserver.com	. +

The FortiAnalyzer Configuration is complete.

IBM Resilient Configuration

This guide assumes that the IBM Resilient IRHub is already installed and configured. Refer to Resilient Email Connector Config Guide v2.x for more details. Install the Email Connector package using the following command, where <version> is the run file version.



If using the IMAP protocol, run the IMAP script to configure the email account to monitor by entering the following command and following the prompts.

Last login: Tue Jun 5 16:21:27 2018 from 10.101.32.254 -bash-4.2\$ sudo irhub-imap-cfg

As prompted, enter the following information:

- IMAP mail server host name; for example, mail.example.com
- Trust the certificate (only prompted if the certificate is untrusted)
- IMAP username; for example, resilient@example.com
- IMAP user password

The script concludes by stating the location of the configuration file. For example: Selecting mailbox INBOX OK IMAP configuration settings were written to /usr/share/irhub/etc/irhub.mail.cfg. If using the EWS protocol, run the EWS script to configure the email account to monitor by entering the following command and following the prompts.

Last login: Tue Jun 5 16:21:27 2018 from 10.101.32.254 -bash-4.2\$ sudo irhub-ews-cfg

As prompted, enter the following information:

- nEWS endpoint; for example, https://mail.example.com/ews/exchange.asmx
- nTrust the certificate (only prompted if the certificate is untrusted)
- nEWS username; for example, resilient@example.com
- NOTE: It must be in email format. Domain/Username format does not work.
- nEWS user password

The EWS script automatically sets the mail_protocol property to EWS. If using the EWS script to make changes after the initial installation, make sure to restart the IRHub for the updates to take effect. The script concludes by stating the location of the configuration file. For example: Using the following settings: Endpoint = https://mail.example.com/ews/exchange.asmx, Mailbox = Inbox EWS configuration settings were written to /usr/share/irhub/etc/irhub.mail.cfg.

Restart IRHub as follows:

```
Last login: Tue Jun 5 16:21:27 2018 from 10.101.32.254
-bash-4.2$ sudo systemctl restart irhub
[sudo] password for resadmin:
-bash-4.2$
```

At this point FortiAnalyzer will send an Email Alert to Resilient when there is a failed Admin logon via SSH.

You can test this by making several failed authentication attempts to the FortiAnalyzer CLI:



Now log in to the Resilient GUI and check List Incidents. It should look like the image below:

AI	0	pen	Incidents time T	- Save Ae 🕞 👹 (Shared)						8	= batoola
	Inci	Sent 1	Disposition: Confirmed, U	0 Nama Ali+ O Status: Active O						Nore.	•
37	7963		Show 900 ±							c	- annulo
0		1	None 2	Description	Data Discovered	Net Due Dete	Eulo Crusted	Owner	Plana	Beverity.	these if
n	2	131	Uner Logon failed via 53H (medium event alert desc:Remove local do FAZYM64)	Subject desc Remove local do Device: FAZIVAH Severity: maclum Prant: FAZIVAH4XAZ-VMX0000101910] Trissen: Local Device Event	95/06/2018	-	06/05/2018	A Kavin Galaugher	Respond	-	Active
0	2	130	User Logon falled via SBH (modium event ålert desc:Trim local do FAZVM64)	Subject desc/Trim local db Device: FAZ/M64 Severity: matteri Franc FAZ/Me4/M2/M40000101010 Tribaer: Local Device Event	96/06/2018	H.	66/05/2018	A Kavin Galaugher	Respond	-	Active
0	2	129	User Logon falled via BSH (reclam event aler) descrüser login/logout taled rikzvMMH	Bubject deec User login/logiost taled Device: FA2/M64 Eleventy: modium France KA2/Media/SA2/Media/D10101 Tribate: Funal Device Event	96/05/2018	5	06/05/2018	A Kevin Giataugher	Respond	-	Active
0	2	120	User Lopon falled via 55H (rectum event alert descuber login from 55H (NZVM5H)	Subject describer login from 85H Device: FAZIMMH Severity: medium Financ Load Device Fuent	96-05-2018	-	06/25/2018	A Kavin Galaugher	Respond	-	Active
0	2	127	User Logon falled via SBH (readium event alert cesc:Remove local do FAZVM64)	Subject deed Remove local do Device: FAZIMMA Severity: motion Feare: FAZIMMA/SAZ-VMA2020101010 Timore: Local Device Fount	96/05/2018	5:	06/05/2018	A Kavin Galeugher	Respond	7	Active
0	2	126	User Logon failed via SBH (medium event alert desc:Trim local do f/AZVW64)	Subject descritern local db Devlox: FADrM64 Beverity: modium Ferer: FADVM64FAD VM0000101010	96/05/2018	2	06/05/2018	& Kevin Galeugher	Respond	-	Active

Notice that the Incident Name is populated by the Email Subject and a description of the Incident is included.



Click on an Incident Name to view details.

Jser Logon failed via SS	SH (medium event alert desc:User logi	ctions +
Summary	Description	
ID 2129	Subject: desc: User login/logout failed	
Phase Respond	Severity: medium	
Severity -	From: FAZVM64(FAZ-VM0000101910)	
Date Created 06/05/2018	Filter:	
Date Occurr	Log message:	
ata Dianati OF OF POIR	log_id=0.01010019 type=event subtype=system pri-alert desc="User login/logout failed" user="() { :;}; echo Plugin output: s()	1+1
Jace Discov 06/06/2016	userfrom=teinet, msg="user '0 { ;;}; echo Plugin output; \$((1+' login failed from teinet(10.101.32.173)" userfrom="" msg=""	
Data Compr Unknown	userfrom=teinst, msg="user '() { ;;}; echo Plugin output: \$([1+' login failed from teinet(10.101.32.173)" userfrom="" msg="" adminprof="" devid=FAZ-VM0000101910 itime=1528263225 date=2018-06-05 time=22:33:45	
Data Compr Unknown	userfrom=teinet, msg="user () { ;;}; echo Plugin output: \$((1+' login failed from teinet(10.101.32.173)" userfrom="" msg="" adminprof="" devid=FAZ-VM0000101910 itime=1528263225 date=2018-06-05 time=22:33:45 Tasks Details Breach Notes Members News Feed Attachments Stats Timeline Attachments	
aas Discov Vever2018 Nata Compr Unknown Incident Type — People	userfrom=teinet, msg="user () { ;;}; echo Plugin output: \$([1+' login failed from teinet(10.101.32.173)" userfrom="" msg="" adminprof="" devid=FAZ-VM0000101910 itime=1528263225 date=2018-06-05 time=22:33:45 Tasks Details Breach Notes Members News Feed Attachments State Timeline Attracts Tasks	
Data Compr Unknown Incident Type - People Created By <u>Kevin Gallaugher</u>	userfrom=teinet, msg="user () { ;;}; echo Plugin output: \$([1+' login failed from teinet(10.101.32.173)" userfrom="" msg="" adminprof="" devid=FAZ-VM0000101910 litme=1528263225 date=2018-06-05 time=22:33:45 Tasks Datais Breach Notes Members News Feed Attachments Stats Timeline Attracts Tasks Oth Complete Filter All - Selected - Add	Task
Aate Oriscov Unknown Incident Type – People Created By & Kevin Gallaugher Owner & Kevin Gallaugher	userfrom=teinet, msg="user () { ;;}; echo Plugin output: \$([1+' login failed from teinet(10.101.32.173)" userfrom="" msg="" adminprof="" devid=FAZ-VM0000101910 litme=1528263225 date=2018-06-05 time=22:33:45 Tasks Datais Breach Notes Members News Feed Attachments Stats Timeine Artifacts Tasks 0% Complete Filter: All + Selected + Add 1	Task
Aate Discov Vokvo/2016 Data Compr Unknown Incident Type — People Created By & Kevin Gallaugher Owner & Kevin Gallaugher Members There are no members.	userfrom=teinet, msg="user () { ;;}; echo Plugin output: \$([1+' login failed from teinet(10.101.32.173)" userfrom="" msg="" adminprof="" devid=FAZ-VM0000101910 itime=1528263225 date=2018-06-05 time=22:33:45 Tasks Details Breach Notes Members News Feed Attachments Stats Timeline Attacts Tasks 01% Complete 01% Complete Task Name Owner Due Date Flags Activ	Task
Data Compr Unknown Incident Type – People Created By <u>Kevin Gallaugher</u> Owner <u>Kevin Gallaugher</u> Members <i>There are no members</i> .	userfrom=teinet, msg="user () { ;;}; echo Plugin output: \$([1+' login failed from teinet(10.101.32.173)" userfrom="" msg="" adminprof="" devid=FAZ-VM0000101910 ltime=1528263225 date=2018-06-05 time=22:33:45 Tasks Dttals Breach Notes Members News Feed Attachments Stats Timeline Atthacts Tasks Of% Complete Filter: All - Selected - Add Task Name Owner Due Date Flags Active Respond	Task
Alle Discov Vever2018 Data Compr Unknown Incident Type — People Created By <u>Kevin Gallaugher</u> Owner <u>Kevin Gallaugher</u> Members There are no members. Related Incidents	userfrom=teinet, msg="user () { ;;}; echo Plugin output: \$([1+' login failed from teinet(10.101.32.173)" userfrom="" msg="" adminprof="" devid=FAZ-VM0000101910 ltime=1528263225 date=2018-06-05 time=22:33:45 Tasks Datals Breach Notes Members News Feed Attachments Stats Timeline Attracts Tasks Of% Complete Filter: All + Selected + Add Task Name Owner Due Date Flags Active Respond	Task ons
Alle Discov Oliver2018 Data Compr Unknown Incident Type – People Created By & Kevin Gallaugher Dwner & Kevin Gallaugher Members There are no members. Related Incidents Incidents.	userfrom-teinet, msg-"user () { ;; }; echo Plugin output: \$([1+' login failed from teinet(10.101.32.173)" userfrom="" msg="" adminprof="" devid=FAZ-VM0000101910 ltime=1528263225 date=2018-06-05 time=22:33:45 Tasks Datais Breach Notes Members News Feed Attachments Stats Timeine Attfacts Tasks Of% Complete Filter: All - Selected - Add date Task Name Owner Due Date Flags Active Respond Respond - (Data Breach - Organizational)	Task ons
Alle Discov Oliver2015 Data Compr Unknown Incident Type – People Created By <u>Kevin Gallaugher</u> Owner <u>Kevin Gallaugher</u> Members There are no members. Nealated Incidents Io related incidents.	userfrom=teinet, msg="user () { ;;}; echo Plugin output: \$([1+' login failed from teinet(10.101.32.173)" userfrom=** msg=** adminprof=** devid=FAZ-VM0000101910 Itime=1528263225 date=2018-06-05 time=22:33:45 Tasks Datais Breach Notes Members News Feed Attachments Stats Timeline Atthacts Tasks Of% Complete Filter: All - Selected - Add Task Name Owner Due Date Flags Active Respond Respond - (Data Breach - Organizational)	Task ons

Notice that an ID Number is automatically assigned to the Incident.

The Incident indicates which device the Incident came from, in this case FAZ-VM0000101910.

The full Log message is also included in the Incident.

Summary

Fortinet and IBM Resilient.

FortiAnalyzer Administration Guide: https://docs.fortinet.com/uploaded/files/4379/FortiAnalyzer-6.0.0-Administration-Guide.pdf



www.fortinet.com

Copyright © 2021 Fortinet, Inc. All rights reserved. Fortinet^{*}, FortiGate^{*}, FortiGate^{*}, FortiCare^{*} and FortiGate^{*}, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Tortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinets General Counsel, with a purchaser that expressly warrants that the identified product will perform accerding to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

October 29, 2021 1:19 PM

Macintosh HD-Users:austin:Dropbox (Red Rider):Clients:Fortinet:Solution Brief Updates:Working Group 7:DG-Fortinet-IBM-Resilient-102021:DG-Fortinet-IBM-Resilient