

Solution Guide



Fortinet Solutions RSSO (RADIUS Single Sign On)

Author: David Oliver Consulting Systems Engineer

Contents

Introduction	3
Deployment Considerations	3
Requirements	3
RADIUS Accounting Direct to Fortigate (Fortigate RSSO)	4
Steps and related CLI / Configuration Example	5
Monitoring and Troubleshooting Examples	9
RADIUS Accounting via FortiAuthenticator to Fortigate (FortiAuthenticator RSSO to FS	SSO) 12
FortiAuthenticator Steps and related CLI / Configuration Example	13
FortiGate Steps and related CLI / Configuration Example	16
Monitoring and Troubleshooting Examples	19
RADIUS Accounting via FortiAuthenticator RADIUS Accounting Proxy to Fortigate	23
(FortiAuthenticator RSSO to RSSO)	23
FortiAuthenticator Steps and related CLI / Configuration Example	24
FortiGate Steps and related CLI / Configuration Example	
Related Information	



Change Log

Revision	Date	Change Description	Owner
1	2014-07-21	Initial Release	David Oliver



Introduction

FortiGate and FortiAuthenticator support the use of RADIUS Start, Stop, and Interim Update messages to authenticate and manage active users transparently. Carriers often use RADIUS servers tied into backend billing systems to record usage information. Enterprises often use RADIUS servers to authenticate VPN connections.

In both cases, the entities in question may want to provide UTM functions or other traffic restrictions to this traffic without having the user re-enter their credentials. Fortinet RSSO solutions can assist in deploying these solutions.

Deployment Considerations

The following are important aspects that need to be considered prior to using RSSO:

- RADIUS environment needs to be configured to send accounting records. How to configure every possible RADIUS server is beyond the scope of this document.
- For direct to Fortigate RSSO, RADIUS server needs to be configured with appropriate group names and users added to them.
- For RADIUS to FAC to FSSO, Your LDAP Directory needs to be configured with appropriate group names and users added to them.
- It is no longer necessary to import or utilize the Fortinet VSA dictionary
 We use the following default RADIUS attributes in Fortigate
 - User-Name (the username that logged in) Class (use this for the group name) Framed-IP-Address (the ip the user logged in from)

We use the following default RADIUS attributes in FortiAuthenticator User-Name (the username that logged in) Framed-IP-Address (the ip the user logged in from) Fortinet-Group-Name (use this for the group name.) {Group attribute is not entirely necessary as FAC will figure it out by querying the LDAP directory}

Requirements

FortiOS 5.0.6. This configuration example uses FortiOS 5.0.6 and FortiAuthenticator 3.0.1. Creation of RADIUS Accounting Records was performed using NTRADping.



RADIUS Accounting Direct to Fortigate (Fortigate RSSO)

FortiOS supports the use of RADIUS Start, Stop, and Interim Update messages to authenticate and manage active users transparently. Configuration of the Fortigate to receive and utilize these records is quite straight forward.



RADIUS Server

Steps and related CLI / Configuration Example

Step 1 – Configure Interface to receive RADIUS Accounting Records

It is required that at least one interface that can be reached by the RADIUS Server is configured to listen for RADIUS Accounting messages.

Figure 1 – Configure interface CLI.

е	dit "port4"
	set vdom "root"
	set ip 10.2.2.254 255.255.255.0
	set allowaccess ping radius-acct
	set type physical
	set explicit-web-proxy enable
	set alias "VMNet4"
	set snmp-index 4
n	ext

Figure 2 – Configure interface GUI.

FortiGate VM64			
Global		Edit Interface	
Clobal Virtual Domains Clobal Virtual Domains System Clobal System Clobal Clobal System Clobal System Clobal System Clobal System Clobal System Clobal System Clobal System Clobal System Clobal System Clobal System Clobal System Clobal System Clobal System Clobal System Clobal Clobal System Clobal Clobal System Clobal Clobal System System Clobal System Syst	Name Alias Link Status Type Virtual Domain Addressing mode IP/Network Mask IPv6 Address Administrative Access	Edit Interface port2(00:0C:29:75:FC:39) Inside_VMNet1 Up © Physical Interface root @ Manual DHCP Dedicate to FortIAP 172:16:245.132/255:255:25 ::/0 ::/0 # HTTPS Ø PING HTTP Ø FMG-Access CAPWAP Ø SSH Ø SNHØ TELNET FCT-Access	
	DHCP Server Security Mode Device Management Detect and Identify Devices	SSH SNMP TELNET	
	Enable Explicit Web Proxy Listen for RADIUS Accounting Messages Secondary IP Address Comments Administrative Status	V Virite a comment d: 0:	



Step 2 – Configure RSSO Agent

Only one RSSO agent is configurable per VDOM. Since the RSSO agent can receive records from any RADIUS server configured to send records to it, more than one is not required to receive from multiple RADIUS servers.

The RADIUS server must be configured to send the following Attributes in the Accounting Start, Accounting Stop and Interim Update messages

User-Name (the username that logged in) Class (The Fortigate uses this to determine the User Group name, Can be any attribute of type octetstring but "sso-attribute" must be set to whatever value you choose.) Framed-IP-Address (the ip the user logged in from)

These are standard RADIUS Attributes so the use of the Fortinet VSA Dictionary is not necessary

1 Idule $3 - 0000000000000000000000000000000000$
--

config user radius
edit "RSSO_Agent"
set rsso enable
set rsso-radius-response enable
set rsso-endpoint-attribute User-Name
next
end





Step 3 – Create User Groups

You will need to create User Groups for each class of user you want to authenticate. The RADIUS Attribute value is configured to match the Accounting Record value in the Attribute [Class].

Figure 5 – Create User Groups CLI

config user group
edit "RSSO_Restricted_Web"
set group-type rsso
set sso-attribute-value "restricted"
next
edit "RSSO_Unrestricted_Web"
set group-type rsso
set sso-attribute-value "unrestricted"
next
end

Figure 6 – Create User Groups GUI

FortiGate VM64				O Logout	F
Global			Edit User Group		
Virtual Domains	2000				
	ame	RSSO_Restricted_Web			
G A root	ype	Firewall O Fortinet	Single Sign-On (FSSO) (Guest) RADIUS Single Sign-On (RSSO)		
R System R	ADIUS Attribute Value	restricted	0		
a Tabadaaa			RADIUS Attribute Value		
E Evelicit Drevu			This value matches the value from the RADIUS Accounting-Start attribute "Class"		
- Explicit Proxy					
Packet Capture					
E Manitor					
R S Reuter					
Router					
Eravall Objects					
B Security Profiles					
E User & Device					
User Definition					
Device					
BO Authentication					
Single Sign-Or					
- + LDAP Servers					
RADIUS Server					
- * TACACS+ Serv					
* Settings					
🖲 🥅 Two-factor Auth					
Endpoint Protect					
🖲 🔍 Vulnerability Sca 🔔					

F: RTINET.

Step 4 – Configure Content Filter (if needed)

Refer to http://docs.fortinet.com for information on how to configure a content filter profile.

Step 5 - Configure Identity Based Firewall Policies

```
Figure 7 – Configure Identity Based Firewall Policies CLI
```

```
config firewall policy
    edit 1
       set srcintf "port2"
       set dstintf "port1"
        set srcaddr "all"
        set action accept
        set rsso enable
        set fall-through-unauthenticated enable
        set comments "For Use with RSSO"
        set identity-based enable
        set nat enable
            config identity-based-policy
                edit 1
                    set schedule "always"
                    set logtraffic all
                    set utm-status enable
                    set groups "RSSO Restricted Web"
                    set dstaddr "all"
                    set service "ALL"
                    set webfilter-profile "restricted"
                    set profile-protocol-options "default"
                next
                edit 2
                    set schedule "always"
                    set logtraffic all
                    set groups "RSSO Unrestricted Web"
                    set dstaddr "all"
                    set service "ALL"
                next
            end
    next
```



Figure 8 – Configure Identity Based Firewall Policies GUI

17-16						Image: Weight of the second	F
			Edit Po	licy			
Policy Type	Firewall VPN						
Policy Subtype	🔘 Address 🔘 User Identity 🔘	Device Identity					
Incoming Interface	port2 (Inside_VMNet1)	•					
Source Address	(all	0					
Outgoing Interface	port1 (Outside_VMNet0)	0					
 Enable NAT Use Destination Interface Address 	Fixed Port						
🔘 Use Dynamic IP Pool	Click to add]					
Enable Web cache							
Enable WAN Optimization							
Configure Authentication Rules							
🛇 Create New 📝 Edit 🎁 Delet							
User/Group	Destination Address	Service	Schedule	Security	Traffic Shaping	Logging	Action
SSO_Restricted_Web	all	ALL	always	WES	8	۵	✓ ACCEPT
& RSSO_Unrestricted_Web	all	ALL	always		8	٥	ACCEPT
ANY ANY	all	ALL	always		Q	w.	Ø DENT
 Skip this policy for unauthentia Disclaimer Customize Authentication Messages 	ated user						
Comments	For Use with RSSO			17/1023			
		I	ок	Cancel			
	Policy Type Policy Subbye Incoming Interface Source Address Outgoing Interface © Erable NAT © Use Destination Interface Address © Use Dynamic IP Pool © Fable WAN Optimization Configure Authentication Rules © Create New © User/Group © Rasso_Rastricted_Web © Rasso_Unrestricted_Web © Rasso_Unrestricted_Web © Rasso_Unrestricted_Web © Rasso_Unrestricted_Web © Rasso_Unrestricted_Web © Rasso_Unrestricted_Web © Rasso_Unrestricted_Web © Customize Authentication Messages Comments	Policy Type Policy Subtype Incoming Interface Source Address Outgoing Interface Outgoing Interface Incoming Interface Outgoing Interface Incoming Interface Interface Incoming Interface Inte	Policy Type Policy Subtype Incoming Interface Source Address @ User Identity Device Identity Incoming Interface Outgoing Interface Outgoing Interface Inable MAT Use Destination Interface Address Use Destination Interface Address Use Destination Interface Address Date Dynamic IP Pool Enable WAN Optimization Configure Athentication Rules Service Service Service Address Destination Address Service Service Service Address Destination Address Service Address Service Address Contemize Authentication Messages Comments For Use with RSSO	Edit Po Policy Type	Edit Policy Policy Type Policy Subtype Incoming Interface port2 (Inside_VMNet1) Source Address Outgoing Interface port2 (Inside_VMNet0) Insable NAT Use Destination Interface Address Enable Web cache Enable WAR Optimization Configure Authentication Rules Image Sectivided_Web ASSO_Unrestricted_Web all ALL always Asy and Asy and <td>Edit Policy Policy Type Policy Subtype Incoming Interface port2 (Inside_VMNet1) Source Address Outgoing Interface port2 (Inside_VMNet1) Outgoing Interface port2 (Inside_VMNet1) Outgoing Interface port2 (Inside_VMNet0) Inside NAT Outgoing Interface port2 (Inside_VMNet0) Inside NAT Outgoing Interface port2 (Inside_VMNet0) Inside NAT Outgoing Interface Pixed Port Address Dick to add Inable Web cache Enable WAR Optimization Description Address Skip this policy for unauthenticated user Issignment Outgoing Authenticated user Issignment Outgoing Authentication Massages Comments For Use wth RSSO For Use wth RSSO It 2000</td> <td>Edit Policy Policy Type</td>	Edit Policy Policy Type Policy Subtype Incoming Interface port2 (Inside_VMNet1) Source Address Outgoing Interface port2 (Inside_VMNet1) Outgoing Interface port2 (Inside_VMNet1) Outgoing Interface port2 (Inside_VMNet0) Inside NAT Outgoing Interface port2 (Inside_VMNet0) Inside NAT Outgoing Interface port2 (Inside_VMNet0) Inside NAT Outgoing Interface Pixed Port Address Dick to add Inable Web cache Enable WAR Optimization Description Address Skip this policy for unauthenticated user Issignment Outgoing Authenticated user Issignment Outgoing Authentication Massages Comments For Use wth RSSO For Use wth RSSO It 2000	Edit Policy Policy Type

Monitoring and Troubleshooting Examples

Figure 9 – Monitor Logged in Users GUI

lobal	2 Refresh	cate				P.c.	how all ESSO Logo
a tallor and	T User Name	Vser Group	T Policy ID	▼ Duration	TIP Address	Traffic Volume	T Method
irtual Domains	ftntunrestricted	RSSO_Unrestricted_Web		0 day(s) 0 hour(s) 3 minute(s)	172.16.245.10	3.02 M	E RSSO
Policy							
* IPv6 Policy							
DoS Policy							
IPv6 DoS Polic							
Proxy Options							
SSL/SSH Inspe							
Monitor							
General Objects							
B WON							
E C Ucor & Dovico							
User Definition							
User Groups							
Guest Manage							
Device							
B Authentication =							
* Single Sign-Or							
+ LDAP Servers							
* RADIUS Server							
TACACS+ Serv							
- Settings							
E I Two-factor Auth							
🖲 🛃 Endpoint Protect							
🖲 🔗 Vulnerability Sca							

You CANNOT deauthenticate a user via the GUI. It can only be done via CLI via the command "diag radiusd test 2". This however will clear the RADIUSD database of all RSSO users. To clear an individual user requires sending an Accounting Stop record for that user.



There are several commands in the CLI to monitor and query logged on users.

Figure 9 – Query Logged in Users CLI

diag rsso query	
allows you to query t	he rsso database by
carrier-endpoint	Query by End Point. (this is the equivalent of the User-name)
ip	Query by IP address.(this is the Framed-IP address(es). This should be the host ip address
rsso-key	Query by RSSO key. (this is the Class Attribute and relates to the Fortigate User Group name).
FortiGate-VM64-2 (g)	obal) # diag rsso query ip 172.16.245.10
Querying IP '172.16.	245.10'
Endpoint: ftntunrest	tricted
RSSO Key: unrest	tricted
IP Addresses:	
IP: 172.16.2	45.10, Time left (hh:mm:ss): 07:53:50 **

It is useful when you want to quickly look up who is at an IP, or list all the users in a specific Class (User Group) that are logged on.

Figure 10 – Query Logged in Users CLI and clear database

diag test app radiusd

allows you to query or clear the entire RADIUSD database

Radius Daemon Test Usage:

- -=-=-=2 : Clear RADIUS server database
 3 : Show RADIUS server database
 33 : Show RADIUS server database (with start time)
 - 4 : Show RADIUS server database info
 - 9 : Check HA context table checksums
 - 11 : Show HA sync connection status

 - 20 : Show RADIUS server configuration cache
 - 21 : Show RADIUS server interface configuration cache

99 : Restart



Figure 11 - debug RADIUSD events as the occur

diag debug enable diag debug app radiusd -1 allows you to debug RADIUSD events as they occur

FortiGate-VM64-2 (global) # diag debug app radiusd -1
FortiGate-VM64-2 (global) # diag debug en
FortiGate-VM64-2 (global) # DB 0 insert [ep='ftntrestricted' pg='restricted' ip='172.16.245.10'] success
DB 0 insert [ep='ftntrestricted' pg='restricted' ip='172.16.245.10'] success
DB 0 insert [ep='ftntrestricted' pg='restricted' ip='172.16.245.10'] success
vd 0:root Remove auth logon for IP 172.16.245.10 for user ftnturestricted
vd 0:root Add/Update auth logon for IP 172.16.245.15 for user ftnturestricted
DB 0 insert [ep='ftnturestricted' pg='unrestricted' ip='172.16.245.10'] success
vd 0:root Add/Update auth logon for IP 172.16.245.15 for user ftnturestricted
DB 0 insert [ep='ftnturestricted' pg='unrestricted' ip='172.16.245.15'] success
vd 0:root Remove auth logon for IP 172.16.245.10 for user ftnturestricted
DB 0 insert [ep='ftnturestricted' pg='unrestricted' ip='172.16.245.15'] success
vd 0:root Remove auth logon for IP 172.16.245.10 for user ftnturestricted
DB 0 insert [ep='ftnturestricted' pg='unrestricted' ip='172.16.245.15'] success
vd 0:root Remove auth logon for IP 172.16.245.10 for user ftnturestricted
DB 0 insert [ep='ftnturestricted' pg='unrestricted' ip='172.16.245.15'] success
vd 0:root Remove auth logon for IP 172.16.245.10 for user ftnturestricted
DB 0 insert [ep='ftntrestricted' pg='restricted' ip='172.16.245.10'] success
vd 0:root Remove auth logon for IP 172.16.245.10 for user ftnturestricted
DB 0 insert [ep='ftntrestricted' pg='restricted' ip='172.16.245.10'] success

RADIUS Accounting via FortiAuthenticator to Fortigate (FortiAuthenticator RSSO to FSSO)

FortiAuthenticator supports the use of RADIUS Start, Stop, and Interim Update messages to authenticate and manage active users transparently. It receives RADIUS accounting messages, Performs lookups against the LDAP server for Group Membership and then populates its FSSO cache with the correct information. This is then sent to the Fortigate as an FSSO login.

This is useful when Group membership information is handled by Active Directory or the RADIUS server is business-critical IT infrastructure, limiting the changes that can be made to the server configuration.





FortiAuthenticator Steps and related CLI / Configuration Example

Step 1 – Configure FortiAuthenticator as an FSSO Collector Agent

FSSO must already be configured between the FortiAuthenticator and the Fortigate(s)

For information on how to configure FortiAuthenticator for FSSO see http://docs-legacy.fortinet.com/auth/3-0-0/FAC-3.0-Admin-Guide.pdf

Step 2 – Configure remote LDAP server

Figure 11 – Configure Remote Auth Server

FortiAuthenticat	or					Logged in as admin	Melo Logour	FCBRTINET
System				Edit Remote LDA	P Server			A
Authentication	Name:	FTNT-AD						
- + Lockouts	Server name//P:	172.16.245.12	Port:	389				
Passwords Custom User Fields	Base distinguished name:	DC-ftnt,DC-local	<u>a</u>					
User Management I onal Users	Bind type:	Simple Regular						
Remote Users	Username:	on-Administrator.on-Users.do-fint.do-local	Password:					
Remote User Sync Rules User Groups	User object class:	person						
FortiTokens	Username attribute:	sAMAccountName						
	Group membership attribute:	memberOf						
Q Remote Auth. Servers LOAP	Secure Connection							
# 2 RADIUS Service	Enable							
- • General	Windows Active Directory	Domain Authentication						
Directory Tree FortiAuthenticator Agent	Varbans rasin rame							
	Deniele Mathian	FINILOCAL						
	Earth developed and better had BIOS assess	FINI						
	Portipulier totalor relation fame.	FortiAuthentica						
	Administrator usemame.	fint/Administrator						
	Administrator password							
	Remote LDAP Users Username			Token	Actions			
	Intrestricted				2 H			
	fintumestricted				2 H			
Fortinet SSO Methods	dollver				2 H			
Monitor	Import Users							
Certificate Management				OK	Cancel			



Step 3 – Enable FSSO and RADIUS accounting SSO Clients

Figure 12 – Enable RADIUS accounting SSO Clients



FHRTINET_®

Step 4 – Configure RADIUS Accounting SSO Client

LDAP server must be selected from the drop-down list. RADIUS Attributes Username Attribute (default User-Name) Client IP attribute (default Framed-IP-Address) are required. I recommend leaving at the defaults.

User group attribute is not required.

The LDAP server created earlier must be selected from the drop-down list as this is how the FortiAuthenticator establishes group membership.

Figure 13 – Create New RADIUS Accounting SSO Client

FortiAuthenticato	r				Logged in as admin	Help	Logout	FURTIDET
System			E	dit RADIUS Accounting SSO Client				
Authentication	Name:	Win2kSAD						
Portinet SSO Methods	Client name/IP:	172.16.245.12						
General Portal Services	Secret:	•••••						
Fine-grained Controls SPO Literre	Description:							
SSO Groups Domain Controllers RADIUS Accounting	SSO user type:	Edemal Cocal users Remote users						
FortiGate Group Filtering IP Filtering Rules	Remote LDAP server:	FTNT-AD (172.16.245.12.389)						
Tiered Architecture	Radius Attributes							
	Username attribute:	User-Name (Browse) (Default)						
	Client IP attribute:	Framed-IP-Address (Browse) (Default)						
	User group attribute:	Fortinet-Group-Name (Browse) (Default)						
				OK Cancel				
Monitor								
Certificate Management								
Logging								



FortiGate Steps and related CLI / Configuration Example

Step 1 – Configure FortiAuthenticator as an FSSO collector agent

Figure 14 – Configure FSSO agent CLI

config user fsso
edit "FAC"
set server "172.16.245.5
next
end

Figure 15 – Configure FSSO agent GUI

FortiGate VM64	and a						Image: Weight of the second	FCRTINET
Global				Edit Si	ngle Sign-On Server			
Virtual Domains Foncy - IPv6 Policy - DoS Policy - IPv6 DoS Polic - Proxy Options - SSL/SSH Inspe	Name Primary Agent IP/Name Secondary Agent IP/Name LDAP Server Users/Groups	FAC 172.16.245.5 Click to set View Users/Groups	Password Password v Edit Users/Groups	,	More FSSO agents			
B ■ Monitor B W Firewall Objects B Ø Ø Security Profiles B Ø VPN B 0 User & Device B 0 User		UNRESTRICTEDWE	28	Apply & Refresh	OK Cance	al		
Authentication Single Sign-Or LDAP Servers RADIUS Server TACACS+ Server								
Settings Settings Endpoint Protect Settings Settings Settings Settings Settings Settings Settings Settings								
Firewall Firewall FortiClient WNO pt. & Cache fill WIN pt. & Cache fill WiFi Controller t Cog & Report v								

Make certain to select groups.

F**;;**PTINET_®

Step 2 – Configure FSSO User Groups

Figure 16 – Configure FSSO user groups CLI

```
config user group
edit "FTNT_FSSO_RestrictedUsers"
set group-type fsso-service
set member "FTNT/RESTRICTEDWEB"
next
edit "FTNT_FSSO_UnRestrictedUsers"
set group-type fsso-service
set member "FTNT/UNRESTRICTEDWEB"
next
end
```

Figure 17 – Configure FSSO user groups GUI

FortiGate VM64	5		elp Logout	F
Global		Edit User Group		
Virtual Domains	Name	FAC_FSSO_Restricted		
Proxy Options	Туре	🔘 Firewall 🔘 Fortinet Single Sign-On (FSSO) 🔘 Guest 🔘 RADIUS Single Sign-On (RSSO)		
* SSL/SSH Inspe	Members	a CN=RESTRICTEDWEB,CN=USERS,DC ×		
🗄 🚽 Monitor		a FTNT/RESTRICTEDWEB X		
Firewall Objects		OK Cancel		
B C VON				
B User & Device				
B C User				
" User Definition				
User Groups				
Guest Manage				
🖲 🏹 Device				
authentication				
" Single Sign-Or				
* LDAP Servers				
* RADIUS Server				
TACACS+ Serv				
Settings				
B C Endpoint Protod				
B A Vulnerability Sca				
B Monitor				
- Firewall				
* Banned User				
- FortiClient				
🖲 😨 WAN Opt. & Cache				
🖲 👘 WiFi Controller				
🕀 🔛 Log & Report 🛛 👻				
< III >				

Step 3 – Configure Content Filter (if needed)

Refer to http://docs.fortinet.com for information on how to configure a content filter profile.



Step 4 – Configure Identity Based Firewall Policies

Figure 17 – Configure Firewall Policies CLI

config firewall policy
edit 2
set srcintf "port2"
set dstintf "port1"
set srcaddr "all"
set action accept
set status disable
set fsso enable
set comments "Use with FAC RSSO&FSSO"
set identity-based enable
set nat enable
config identity-based-policy
edit 1
set schedule "always"
set logtraffic all
set utm-status enable
set groups "FAC_FSSO_Restricted"
set dstaddr "all"
set service "ALL"
set webfilter-profile "restricted"
set profile-protocol-options "default"
next
edit 2
set schedule "always"
set logtraffic all
set groups "FAC_FSSO_UnRestricted"
set dstaddr "all"
set service "ALL"
next
end
next
end



Figure 18 – Configure Firewall Policies GUI

FortiGate VM64	5-1						ep Logout	FCBRTINET				
Global				Edit Poli	сy			-25				
Virtual Domains	Policy Type Policy Subtype Incoming Interface Source Address Outgoing Interface Image: Interface Image: Image: Ima	Firewall © VPN Address @ User Identity © port2 (Inside_VMNet1) all port1 (Outside_VMNet0) Fixed Port Click to add	Device Identity									
IPv6 Policy	Contraction rules											
- * DoS Policy - * IPv6 DoS Polic - * Proxy Options - * SSL/SSH Inspe	User/Group FAC_FSSO_Restricted FAC_FSSO_UnRestricted ANY	Destination Address all all all	Service ALL ALL ALL	Schedule always always always	Security wes	Traffic Shaping © ©	Logging Ø	Action ✓ ACCEPT ✓ ACCEPT Ø DENY				
SSL/SSH Inspe	 Skip this policy for unauthentil Disclaimer Customize Authentication Messages Comments 	user with FAC RSSO&FSSO		ок	्रा ३४/१२३३ Cancel							

Monitoring and Troubleshooting Examples

There is little in the way of troubleshooting on the FortiAuthenticator. The Monitor/SSO Sessions is the only way to determine who is logged on from where.

Figure 19 – Monitor Logged on Users FortiAuthenticator

FortiAuthentica	tor	
System	Retesh @Logoff All @Logoff Section: 0 of 1 selected	Q Search for SSO sessions Search
Authentication	Logon Time Update Time Workstation IP address Username Source	Group
Fortinet SSO Methods	Thu Mar 27 09:16:36 2014 Thu Mar 27 09:16:36 2014 172:16:245:12 172:16:245:12 FTNTRESTRICTED Radius Accounting CN	+FINTRESTRICTED, OL-RESTRICTEDWEB, DC+FINT, DC+LOCAL-CN+ADMINISTRATORS, CN-BULTIN, DC+FINT, DC-LOCAL-CN-BULTIN, DC+FINT, DC+LOCAL-CN+DDMAN, USERS, CN+USERS, DC+
Monitor	1 SSC session	
• Domains		
SSO Sessions Domain Controllers		
• FortiGates		
CH Authentication		
Certificate Management		
Logging	· · · · · · · · · · · · · · · · · · ·	•

A single user can be deauthenticated on the FortiAuthenticator.



The Fortigate provides more troubleshooting tools for comprehensive debugging

Figure 20 – Monitor Logged on Users Fortigate GUI

FortiGate VM64							Help	Logout F	BRTINET
Global	2 Refresh 🤴 De antendaria								Show all FSSO Logons
Virtual Domains	⊤ User Name	▼ User Group	T Policy ID	T Duration		TIP Address		Traffic Volume	T Method
Policy	FTNTRESTRICTED	FAC_FSSO_Restricted		0 day(s) 0 hour(s) 20 minute(s)	i i	172.16.245.12		N/A	FSSO
* IPv6 Policy									
- * DoS Policy									
* IPv6 DoS Polic									
Proxy Options									
SSL/SSH Inspe									
🕀 😾 Monitor									
Firewall Objects									
Gill Security Profiles									
W / VPN									
Guser & Device									
us 📆 User									
@ GO Device									
a Q Authentication									
- Single Sign-Or									
- CDAP Servers									
TACACS+ Server									
- Settings									
🖲 🥅 Two-factor Auth									
Endpoint Protect									
🖲 🤬 Vulnerability Sca									
🛛 💷 Monitor									
- Firewall									
Banned User									
= FortiClient									
🕫 🗓 WAN Opt. & Cache									
🖲 📢 WiFi Controller									
1 m	H								

You cannot deauthenticate an FSSO user from the Fortigate GUI.

Figure 21 – Monitor Logged on Users Fortigate CLI

diag debug authd fsso

allows you to query, clear, list and provide comprehensive information about the status of FSSO sessions. It supports filtering which makes searching through thousands of potential logins quite simple.

FortiGate-VM64-2 (global) # diag debug authd fsso

clear-logons Clear logon information.

filter Filters used for list or clear logons.

list List current logons.

refresh-groups Refresh group mappings.

refresh-logons Resync logon database.

server-status Show FSSO agent connection status.

summary Summary of current logons.

FortiGate-VM64-2 (global) # diag debug authd fsso filter

clear Clear all filters.

group Group name.

server FSSO agent name.

source Source IP address.

user User name.



diag debug authd fsso list

Unfiltered
FortiGate-VM64-2 (global) # diag debug authd fsso list
FSSO logons
IP: 172.16.245.12 User: FTNTRESTRICTED Groups: CN=RESTRICTEDWEB, CN=USERS, DC=FT
NT, DC=LOCAL Workstation: 172.16.245.12 MemberOf: FAC_FSSO_Restricted
Total number of logons listed: 1, filtered: 0
end of FSSO logons

diag debug authd fsso filter user FTNTUNRESTRICTED diag debug authd fsso list

Filtered

FortiGate-VM64-2 (global) # diag debug authd fsso filter user FTNTRESTRICTED FortiGate-VM64-2 (global) # diag debug authd fsso list ----FSSO logons----Total number of logons listed: 0, filtered: 1 ----end of FSSO logons----

You can deauthenticate a single FSSO user from the CLI using diag debug authd fsso filter user <username> diag debug authd fsso clear



Figure 22 – debug AUTHD events as the occur

diag debug enable diag debug app authd -1 allows you to debug FSSO events as the occur

FortiGate-VM64-2 (global) # diag debug app authd -1 FortiGate-VM64-2 (global) # message loop: checking timeouts event read[FAC]: received heartbeat 0 message loop: checking timeouts process logon[FAC]: FINTUNRESTRICTED(172.16.245.10) logged on with session id(), port range sz=0 process logon-883: can not find such a user, try to add it message loop: checking timeouts authd admin.c:636 authd admin read: called message loop: checking timeouts event read[FAC]: received heartbeat 0 message loop: checking timeouts message loop: checking timeouts event_read[FAC]: received heartbeat 0 message loop: checking timeouts [fsae db logoff user:453]: vfid 0, ip 172.16.245.10, FTNTUNRESTRICTED, sesion i (0), port range sz(0) [authd fp notify logoff:251]: vfid 0, ip 172.16.245.10, id 0 process_logoff[FAC]: FTNTUNRESTRICTED logged off message loop: checking timeouts authd admin.c:636 authd admin read: called authd del auth path: src ip = af510ac, vd = root Unknown sequence: 0af510ac message loop: checking timeouts process logon[FAC]: FTNTRESTRICTED(172.16.245.12) logged on with session id(0) port range sz=0 process logon-883: can not find such a user, try to add it message loop: checking timeouts authd admin.c:636 authd admin read: called message loop: checking timeouts event read[FAC]: received heartbeat 0 message loop: checking timeouts



RADIUS Accounting via FortiAuthenticator RADIUS Accounting Proxy to Fortigate (FortiAuthenticator RSSO to RSSO)

FortiAuthenticator supports the use of RADIUS Start, Stop, and Interim Update messages to authenticate and manage active users transparently. It receives RADIUS accounting messages, Performs lookups against the LDAP server for Group Membership and then forwards the RADIUS message to the Fortigate RSSO agent.

This is useful when Group membership information is handled by Active Directory or the RADIUS server is business-critical IT infrastructure, limiting the changes that can be made to the server configuration.





FortiAuthenticator Steps and related CLI / Configuration Example

Step 1 – Configure FortiAuthenticator as a RADIUS Accounting Proxy

Figure 23 – Configure Remote Auth Server

FortiAuthenticat	or					Logged in as admin	Help	Logout	F
System				Edit Remote Li	DAP Server				
Authentication	Name:	FTNT-AD	1						
 Lockouts 	Server name/IP:	172.16.245.12	Port:	309					
Custom User Fields	Base distinguished name:	DC-ftrt,DC-local	<u>a</u>						
User Management Incal Users	Bind type:	Simple Regular							
Remote Users	Username.	cn-Administrator.cn-Users.do-fint.do-local	Paseword.						
Remote User Sync Rules User Groups	User object class:	person							
- FortiTokens	Username attribute:	sAMAccountName							
MAC Devices	Group membership attribute:	memberOf							
Remote Auth. Servers	Secure Connection								
* 2 RADIUS Service	Enable								
LDAP Service General	Windows Active Directory	Domain Authentication					_	_	
Directory Tree	Enable								=
FortiAuthenticator Agent	Kerberos realm name.	FTNTLOCAL							
	Domain NetBIOS name:	FTNT							
	FortiAuthenticator NetBIOS name:	FortiAuthentica							
	Administrator username:	fintAdministrator							
	Administrator password:	•••••							
	Remote LDAP Users								
	Username			Token	Actions				
	fintrestricted				2 X				
	finiumestricted				/ #				
Fortinet SSO Methods	dollver				2 H				
Monitor	Import Users								
Certificate Management				ОК	Canoel				

Step 2 – Enable RADIUS Accounting SSO Clients

Figure 24 – Enable RADIUS accounting SSO Clients

FortiAuthenticat	or			Logged in as admin 🦉 📴 FCIRT	INET
System			Edit SSO Configuration		
Authentication	FortiGate				
Fortinet SSO Methods	Listening port:	8000			
SSO	Login expiry:	480 minutes			
Portal Services	Enable authentication				
 Fine-grained Controls SSO Users 	Fortinet Single Sign-On (FSSO)				
- SSO Groups	Maximum concurrent user sessions:	(Configure Per User(Group)			
RADIUS Accounting	Log level:	Debug			
FortiGate Group Filtering	Enable Windows Active Directory domain	controller polling			
Printening Rules Priered Architecture Accounting Proxy	Enable RADIUS Accounting SSO clients	•			
	Enable FortiClient SSO Mobility Agent S	ientoe			
	FortiClient listening port.	8001			
	Enable authentication				
	Keep-alive Internal:	5 minutes (1-60)			
	Idle timeout	10 minutes			
	Enable NTLM				
	NTLM authentication expiry:	480 minutes (1-10080)			
	Enable hierarchical FSSO tiering				
	Collector listening port:	8002			
	Enable DC/TS Agent Clients				
	DC/TS Agent listening port:	8003			
	Restrict auto-discovered domain controlle	ers to configured domain controllers			
	Enable Windows Active Directory worksta	ation IP verification			
	Enable IP change detection via D1	NS lookup			
Certificate Management	Restart SSO service				



Step 3 – Create a new Accounting Proxy source

Figure 25 – Create a new Accounting Proxy Source

FortiAuthenticat	or			Logged in as admin	(2) Help	Logout	FCRTINET
System			Edit RADIUS	Accounting Proxy Source	-	_	
Authentication	Name:	Win2k8AD					
Fortinet SSO Methods							
🖃 💽 SSO	Source name/IP:	172.16.245.12					
General	Secret:	•••••					
Portal Services	Description:						
Fine-grained Controls	Description:						
• SSO Users			OK	Cancel			
• SSO Groups			UN	Cancer			
• Domain Controllers							
• RADIUS Accounting							
• FortiGate Group Filtering							
··· • IP Filtering Rules							
Tiered Architecture							
E-M Accounting Proxy							
• General							
• Rule Sets							
Sources							
Destinations							

This information would be the RADIUS server.

Step 4 – Create a new Accounting Proxy Create a new Rule Set

Figure 26 – Create a new Rule Set

FortiAuthenticat	or				Logged in as admin	(2) Help	Logout	FCRTIN	ET
System				Edit Rule Set					
Authentication Fortinet SSO Methods	Name: Description:	RSSO							
General	Rules Rule: Add User-Na	me							0
- • Fine-grained Controls - • SSO Users - • SSO Groups	Action: Attribute:	Add User-Name	[Browse]						
	Value type: Username attribute:	Group names User-Name	[Browse]						
Tiered Architecture Accounting Proxy	Remote LDAP: Description:	FTNT-AD (172.16.245.12:389) Add attribute "User-Name" containing "Group name	es" from group membership	of "User-Name" attribute on rei	mote LDAP server "FTNT	-AD (172.16.2	245.12:389)"		
General Rule Sets Sources Destinations	Add another Rule		ОК	Cancel					

Select Action "Add" for a new attribute

Select Action "Modify" to translate an existent attribute

The attribute User-name is what the FortiAutheticator uses to parse group membership info from the LDAP Server.

The Value type is what we want FortiAuthenticator to add to the Accounting messages it forwards to the Fortigate. To add the user's group membership info select Group names.

Select the LDAP server that the FortiAuthenticator will run the group membership query on.



Step 5 – Create a New Destination

0 0 0

FortiAuthenticat	or		Logged in as admin	(2) Help	Logout	FCRTINET
System		E	dit RADIUS Accounting Proxy Destination			
Authentication	Name:	FGT				
Fortinet SSO Methods	Destination news (D)					
🕂 😭 sso	Desunation name/P:	172.16.245.132				
- • General	Secret:					
Portal Services	Source:	MERCHAR (170 16 045 10)				
- • Fine-grained Controls	Source.	WIN2K8AD (172.16.245.12)				
- • SSO Users	Rule set	RSSO .				
- • SSO Groups						
- • Domain Controllers			OK Cancel			
RADIUS Accounting						
PortiGate Group Filtering IR Eiltering Rules						
Tiered Architecture						
Accounting Proxy						
General						
- • Rule Sets						
• Sources						
Destinations						

This is the target for the translated Accounting message. Usually this is the Fortigate you wish to send the accounting message to but it can be any RADIUS Server configure to listen for Accounting messages.

Make certain you assign the rule set and source correctly.

FortiGate Steps and related CLI / Configuration Example

Configuration and debugging on the Fortigate is the same as what is describe at the beginning of this document under RADIUS Accounting Direct to Fortigate (Fortigate RSSO).



Related Information

FortiOS and FortiGate Technical Documentation <u>http://docs.fortinet.com/fgt.html</u>

Fortinet Knowledge Base <u>http://kb.fortinet.com/</u>

FortiGate appliances http://www.fortinet.com/products/fortigate/

FortiAuthenticator Technical Documentation <u>http://docs-legacy.fortinet.com/fauth.html</u>

Copyright© 2011 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, and FortiGuard®, are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance metrics contained herein were attained in internal lab tests under ideal conditions. Network variables, different network environments and other conditions may affect performance results, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding contract with a purchaser that expressly warrants that the identified product will perform according to the performance metrics herein. 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 guarantees. 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. Certain Fortinet products are licensed under U.S. Patent No. 5,623,600.