RADIUS SINGLE-ON [RSSO]

When the user is connected to LAN and is successfully authenticated by Active Directory, DC's security event log can be polled for logon events and this information is sent to Fortigate to record the IP address, Username and Group information associated to that event. Users may have a static IP or may have DHCP server assigning the IP address. If this is a laptop, for example, most of the times authentication request are made using the Ethernet interface (default setting). What happens when the user is disconnected from wired connection? Fortigate does not know the IP address of the wireless interface on this laptop and now the user is no longer authenticated to the firewall. User may have to sign out and sign back in to make the authentication request via wireless IP.

This is where RSSO comes into picture. RSSO uses the wireless authentication(802.1x) request from the Radius server authenticating that request via Radius Accounting. We will discuss more about this in a bit. Typically, RSSO is solution when third party AP is used but that does not restrict the administrator from using this solution with FortiAP.

AUTHENTICATION FLOW:

When third-party AP is deployed:



- 1. WiFi Users connects to \$SID.
- 2. AP sends Username and Password to the Radius Server.
- Radius Server authenticates the user and sends Access-Accept message back to the AP.
 Users is now connected to SSID and IP address is assigned by
- 4. Users is now connected to SSID and IP address is assigned by DHCP Server.
- 5. AP sends Accounting-Request message to the Radius Server.
- Radius server forwards this Accounting-request including the Username, Framed-IP-Address and Class attribute values to the Fortigate.
 Fortigate matches the user to correct RSSO user group using the Class value
- Fortigate matches the user to correct RSSO user gi and inserts this information into its Radius DB.
- User traffic is now matched to the correct identidy policy and can access the network resources as per the policy with a single sign-on, without the need to re-authenticate to the Fortigate.

When FortiAP is deployed: (802.1x is used to authenticate the WiFi users) 101 Host 2 Username : Sam "port2 92.168.1.99/24 10.10.100.99/24 1. WiFi Users connects to \$\$ID. 2. Fortigate(WLC) sends Username and Password to the Radius Server. 3. Radius Server authenticates the user and sends Access-Accept Host 1 Username : John message back to the Fortigate 4. Users is now connected to \$\$ID and IP address is assigned by DHCP Server. FortiAP 5. Fortigate sends Accounting-Request message to the Radius Server. SSID: RSSO port1 6. Radius server forwards this Accounting-request including the N/W: 192.168.80.0/24 10.10.100.119/24 Username, Framed-IP-Address and Class attribute values to the Fortigate. 7. Fortigate matches the user to correct RSSO user group using the Class value and inserts this information into its Radius DB. port2 8. User traffic is now matched to the correct identidy policy and can access the 192.168.50.0/24 network resources as per the policy with a single sign-on, without the need to re-authenticate AD/ Radius to the Fortigate. The configuration components we will be working are show below:

- 1. RSSO Accounting Listener which listens on port 1813 for accounting packets
- 2. Radius Accounting and Fortigate Radius Server
- 3. Configuring RSSO user group
- 4. Configuring WiFi SSID
- 5. Configuring NPS (Windows server 2019) for authentication and authorization

RSSO Accounting Listener which listens on port 1813 for accounting packets

- 1. Login to the Fortigate and Click on Security Fabric > Fabric Connectors > Create New and select "Radius Single Sign-On Agent"
- 2. Enable "Use RADIUS Shared Secret" and provide the Shared Secret configured in the NPS
- 3. Enable "Send RADIUS Responses" and click on OK

Dashboard	>		config us	er radius
X Security Fabric	~	SSO/Identity	edit	"RSSO Agent"
Physical Topology			S	et rsso enable
Logical Tapalagy			S	et rsso-radius-response enable
Logical topology			s	et rsso-validate-request-secret enable
Settings			s	et rsso-secret ENC TAlcudAKY2tuXibXTiBKOsgZ
Fabric Connectors	☆	RADIUS Single		ot race endpoint attribute Haer Name
🖿 FortiView	>	Sign-On Agent	5	et isso-enapoint-attribute oser-Mame
+ Network	>		S	et rsso-context-timeout 0
A Sustan		Connector Settings	S	et rsso-flush-ip-session enable
System	1	Name RSSO Agent	next	
Policy & Objects	~		end	
Security Profiles	>	Use RADIUS Shared Secret	CIIG	
므 VPN	>	Send RADIUS Responses		

4. Connect to the CLI and add the above show configuration to the "RSSO Agent"

Please note that the FortiAP uses the attribute "User-Name" to denote the user. Please refer to other vendor's documentation for corresponding attribute for this field in their accounting packets.

"rsso-context-timeout" can be used to clear authentication after 'x' number of seconds (when set to 0, it never times out)

Radius Accounting and Fortigate Radius Server

1. Create radius server on the Fortigate and enable "Radius Accounting" on the interface connecting to the NPS.

Edit RADIUS Server		config user radius
Name	NPS	set server "10.10.100.119"
Authentication method	Default Specify	set secret ENC ZuFofpwEhC5IM2U1my9fRVa
	MS-CHAP-v2	<pre>set auth-type ms_chap_v2</pre>
NAS IP		config accounting-server
Include in every user group 🕥		edit 1 set status enable
Primary Server		set server "10.10.100.119"
IP/Name	10.10.100.119	set source-ip "10.10.100.99"
Secret	•••••	next
Connection status	Successful	end
Test Connectivity		next
Test User Credentials		end

- 2. From the CLI, add the above show configuration to send accounting packets for any connection that uses this server.
- 3. Accounting packets will now be sent to port 1813 of the radius server

Configuring RSSO user group

- 1. From User & Device > User Group, Click Create New
- 2. Provide the name for the group and select "Radius Single Sign-On(RSSO)"
- 3. Enter the "Radius Attribute Value" for this group. This is the value which the NPS should send to Foritgate (sent in HEX) and Fortigate will use this value to map the correct group and identity policy.

Name	Restricted		
ype	Firewall		
	Fortinet Single Sign-On (FSSO)		
	RADIUS Single Sign-On (RSSO)		
	Guest		
RADIUS Attribute Value 🜖	Restrict		
		ОК	Ca
		ОК	Cá

Configuring WiFi SSID

- 1. Click on WiFi & Switch Controller > SSID > Create New SSID
- 2. Provide name for the interface, IP/Netmask and enable DHCP Server
- 3. Enter the name for the SSID and select "WPA2 Enterprise"
- 4. Now for the authentication select "Radius Server" and choose the Radius server created earlier in this article and click OK

WiFi Settings			
SSID		do not connect	
Security mode		WPA2 Enterprise	•
Client limit			
Authentication		Local RADIUS Server	
		la NPS	-
Dynamic VLAN assignme	nt 🔿		
Broadcast SSID			
Schedule 🚯		lo always	×
		+	
Block intra-SSID traffic			
Broadcast suppression		ARPs for known clients	×
		DHCP unicast	×
		DHCP uplink	×
		+	

Before proceeding with the NPS configuration, I would like to explain a bit about Protected EAP. Protected EAP with MS-CHAPv2 is an EAP type which is more easily deployed with EAP-TLS or PEAP-TLS because user authentication is accomplished by using password-based credentials (an AD Username and Password) instead of digital certificates or smart cards. Only server running the NPS are required to have a certificate (we will see this in the NPS configuration). Administrator can choose not to use "Server Validation" in the wireless properties in the end-user's pc, however that is not recommended. When "Server Validation" is enabled, NPS will present its certificate to the client and the client after examining the certificate will have to Trust it. This certificate used by NPS can be issued by a public CA or by the private trust root CA deployed in the network.

Configuring NPS (Windows server 2019) for authentication and authorization

Goal here is to authenticate user and return the correct attribute based on user group membership and forward the Radius Accounting packets to Fortigate for RSSO.

Client and Remote Radius Server Group Configuration.

- 1. Make sure the NPS service is started and registered to the Active Directory
- 2. Right-Click on "Radius Clients", select New and populate the fields Friendly Name, Address (Fortigate IP) and shared secret which must match Fortigate Radius server/RSSO agent configuration

	RADIUS Clients					
RADIUS Clients and Servers RADIUS Clients RADIUS Clients Remote RADIUS Server RADIUS clients allow you to specify FGT-RSSO Properties FGT-RSSO Properties	×					
Settings Advanced						
Connection request Po						
Accounting for the second seco						
Template Management						
> Templates Management	\sim					
Name and Address						
Friendly name:						
FGT-RSSO						
Address (IP or DNS):	14.15					
10.10.100.39	Venty					
Shared Secret						
Select an existing Shared Secrets template:						
None	\sim					
To manually type a shared secret, click Manual. To automatically genera secret, click Generate. You must configure the RADIUS client with the s secret entered here. Shared secrets are case-sensitive.	ite a shared ame shared					
Manual Generate						
Shared secret:						
Confirm shared secret:						
OK Cancel	Apply					

3. Right-Click "Remote RADIUS Server", select "New", enter the group name and click on "Add"

	s		
Remote RADIUS server gro	oups allow you to specify wh	Address Authentication/Accounting Load Balancing	
rver		Select an existing Remote RADIUS Servers template: None	
st Po Group Name Group	×	Type the name or IP address of the RADIUS server you want to add.	
	1	Server:	
		10.10.100.99	Verify
Priority Weight	Add Edit Remove		
ОК	Cancel		
	Vers Remote RADIUS server gro ver t Po Group Name Group Priority Weight	Vers Remote RADIUS server groups allow you to specify wh ver t Po Group X Priority Weight Add Edt Remove OK Cancel	Address Authentication/Accounting Load Balancing Address Authentication/Accounting Load Balancing Address Authentication/Accounting Load Balancing Select an existing Remote RADIUS Servers template: None Type the name or IP address of the RADIUS server you want to add. Server: 10.10.100.99 OK Cancel

- 4. Use the IP Address of the Fortigate Interface that was configured to listed for "Radius Accounting" in the previous step
- 5. Navigate to "Authentication/Accounting" tab:
 - a. Un-check "Use the same shared secret for the authentication and accounting"
 - b. Enter the shared secret configured on the forigate for the Radius server/Rsso Agent and click OK

ddress	Authentication/Accounting	Load Balanci	ing
Authent	tication port:		1812
Select a	an existing Shared Secrets ten	nplate:	
None			`
Shared	secret:		
Confirm	shared secret:		
Req	uest must contain the messag	e authenticato	r attribute
Δ	unities of		
ACCOL	unung		
Acco	unting port:		1813
Accol	unting port: se the same shared secret for	authentication	1813 and accounting.
	unting port: se the same shared secret for elect an existing Shared Secre	authentication	1813 and accounting.
	unting port: lse the same shared secret for elect an existing Shared Secr None	authentication	1813 and accounting.
Acco Acco U S S	unting port: se the same shared secret for elect an existing Shared Secre None hared secret:	authentication	1813 and accounting.
Acco Acco U S I C	unting port: ise the same shared secret for elect an existing Shared Secre None hared secret: ionfirm shared secret:	authentication	1813 and accounting.
Accol	unting port: ise the same shared secret for elect an existing Shared Secre None hared secret: ionfim shared secret: prward network access server	authentication ets template :	1813 and accounting. ******** ******** motifications to this server
Acco Acco U S S C F C	unting port: ise the same shared secret for elect an existing Shared Secre None hared secret: ionfirm shared secret: prward network access server	ets template:	1813 and accounting. •••••••• •••••••• •••••••• •••••••• •••••••• ••••••• ••••••• •••••••
Acco Acco U S C C F	unting port: se the same shared secret for elect an existing Shared Secre None hared secret: ionfirm shared secret: prward network access server	authentication ets template: start and stop	1813 and accounting. ••••••• ••••••• ••••••• ••••••• ••••••• ••••••• ••••••• ••••••• ••••••• ••••••• ••••••• •••••••
Acco Acco U S C C	unting port: se the same shared secret for elect an existing Shared Secre None hared secret: onfirm shared secret: onward network access server	authentication ets template:	1813 and accounting.

Configuring Connection Request Policy

- 1. Right-Click on "Connection Request Policy" and select New
- 2. Provide a name for the policy and navigate to "Conditions" tab by clicking "Next"

lew Connecti	ion Request Policy		×
	Specify Connection Requ	est Policy Name and Conn	ection Type
	You can specify a name for your connec	tion request policy and the type of connect	ions to which the policy is applied
olicy name	:		
RSSO-POLIC	Y-CONNECTION		
letwork copp	action method		
Select the type ype or Vendo select Unspec	e of network access server that sends the cc r specific, but neither is required. If your netv ified.	onnection request to NPS. You can select eith work access server is an 802.1X authenticating	er the network access server g switch or wireless access point,
) Type of ne	twork access server: ed	~	
Vendor spe	ecific:		
10			
-			

3. Click "Add" and select a condition. Adding "Client IPv4 Address" binds this connect policy to the network policy in the next step. Provide the IP address of the Foritgate and Click 'OK' and "Add"

🐌 Network Policy Server		1			л — Ф
File Action View Help		Select condition	Client IPv4 Address	×	×
← → 2 📧 2 🖬	New Connection Reques	Select a condition, and then clic	Specify the IPv4 address of the RADIUS client. Yo syntax.	u can use pattern matching	^
 RADIUS Clients and Serv RADIUS Clients RADIUS Clients Remote RADIUS Serv Policies Connection Request 	Specif Specify th minimum	Day and Time Restri Day and Time Restric restrictions are based RADIUS Client Properties Calling Station ID Calling Station ID	10.10.100.99	OK Cancel	These
 Network Policies Accounting Templates Management 	Conditions:	Client Friendly Name The Client Friendly Name The Client Friendly Na NPS.	condition specifies the network access server telep me condition specifies the name of the RADIUS clie	ent that forwarded the connection	on request to
		The Client IP Address to NPS.	condition specifies the IP address of the RADIUS cl	ient that forwarded the connec	tion request ❤
				Add.	Cancel
	Condition description:				
			Add Edit.	Remove	
			Previous Next Finish	Cancel	

4. Next step in to Specify the Connection Request Forwarding. For Authentication, leave as default (Authenticate requests on this server). Click Accounting and check "Forward accounting requests to this remote RADIUS server group" and the select the remote radius server group created earlier. Click on Next.

New Connect	ion Request Policy		×
	Specify Conn The connection requ remote RADIUS serv	nection Request Forwarding lest can be authenticated by the local server or it can be forwarded to RADIUS servers ver group.	in a
If the policy co	onditions match the conr	nection request, these settings are applied.	
Forwardin Request → Authen	g Connection tication hting	RADIUS accounting allows you to record user authentication and accounting requests in log file or to a SQL Server database. To forward accounting requests to remote RADIUS servers, specify a remote RADIUS server group. Forward accounting requests to this remote RADIUS server group Acc-grp	ı a
		Previous Next Finish Can	cel

- 5. Leave Specify Authentication Methods to default and Click on Next
- 6. Click Next on Configure Settings dialogue
- 7. Click Finish on the Completing connection request policy

Configuring Network Policies

- 1. Right-Click on "Network Policies" and select New
- 2. Provide a name for the policy and navigate to "Conditions" tab by clicking "Next"
- 3. Click "Add" and select a condition. Select "User Groups" and the group for the restricted users. Click OK and Add.

New Netw	vork Policy			×	
	Specify Condition	I S determine whether this i	network policy is evaluated for a connection reque	st. A minimum	s Type Source Access Unspecified Access Unspecified Access Unspecified
Conditio	ns:		Select Group		×
Con	ndition Value	User Groups	Select this object type:		
:	Select condition	Specify the grou	Group		Object Types
	Select a condition, and then click A	dd. Groups	fortilab.local		Locations
	Windows Groups The Windows Groups cor groups. Machine Groups	dition	Enter the object name to select (<u>examples</u>): Restricted User		Check Names
Conditio	User Groups The User Groups condition	on spe	Advanced	0	K Cancel
	Day and time restrictions Day and Time Restriction Day and Time Restriction Day and Time Restriction restrictions are based on Connection Properties	ns sspe the ti	ОК Са	incel	word after it ha
			A	dd Ca	incel
		[Previous Next Finish	Cancel	

- 4. Leave Specify Access Permission to default (Access Granted) and click on Next
- 5. Next few steps are important because this is where the NPS certificate is linked. In the configure Authentication Methods page-

a.	Select Add and Click on Protect EAP (PEAP)						
	Configure Authentication Methods Configure one or more authentication methods required for the connection request to match this policy. authentication, you must configure an EAP type.						
	EAP types are negotiated betwee EAP Types:	Add EAP Authentication methods: Microsoft: Smart Card or other certif Microsoft: Protected EAP (PEAP) Microsoft: Secured password (EAP	Cate				
	Add Edt Less secure authenticatio Microsoft Encrypted Authent User can change passw Microsoft Encrypted Authent User can change passw Encrypted authentication (C) Unencrypted authentication (C) Hencrypted authentication (C) Allow clients to connect with	n methods: ication version 2 (MS-CHAP-v2) rd after it has expired ication (MS-CHAP) rd after it has expired 14P) (PAP, SPAP) out negotiating an authentication meth	od.				
			Previous Next	Rnish Cancel			

b. Click on PEAP and click on Edit, select the certificate that the server should use to prove its identity to the client.

New Network Policy	Edit Protected EAP Prop	erties		×
Configure Authentication Me Configure one or more authentication method authentication, you must configure an EAP ty	Select the certificate the A certificate that is config Policy will override this ce Certificate issued to:	ve its identity to the n Connection Reque	e dient. est	
EAP types are negotiated between NPS and the client in the order EAP Types: Microsoft: Protected EAP (PEAP)	Friendly name: Issuer: Expiration date:	dc1 dc1 9/17/2025 9:53:53 PM		
Add Edt Remove	Enable Fast Reconnect Disconnect Clients with Eap Types Secured password (EAP-4	Move Up Move Down		
Microsoft Encrypted Authentication version 2 (MS-CHAP-v2) User can change password after t has expired Microsoft Encrypted Authentication (MS-CHAP) User can change password after t has expired Encrypted authentication (CHAP)	Add Edit	Remove	ОК	Cancel
Unencrypted authentication (PAP, SPAP) Allow clients to connect without negotiating an authentication n	nethod.			hange passwon
	Previous N	lext Finish	Cancel	

- 6. Leave Configure Constrains to default
- 7. In Configure settings, Add a **Standard Radius Attribute Class**, provide the value for the string. This value should match the sso attribute value in the rsso user group. (case-sensitive). Click OK>Add>Next.

• 🔿 🖄 🔂 🔽					
NPS (Local) RADIUS Clients and Servers	work Policies	:	Attribute Information	×	
RADIUS Clients	Network p	olicies allow you to designate who Add Standard RADIUS Attrib	Attribute name: Class		they can or c ×
Configure Se NPS applies settings matched.	ttings to the connect	To add an attribute to the settin To add a custom or predefined Add. Access type: All	Attribute number: 25 Attribute format: Octet String Enter the attribute value in:		ien click
If conditions and constraints match the connection req		Attributes:	String O Hexadecimal		^
RADIUS Attributes Standard Vendor Specific Routing and Remote Access Multilink and Bandwidth Allocation Protocol (BAP) IP Filters Encryption IP Settings	To send add then click Ec your RADIU: Attributes: Name Framed-Prr Service-Ty	Acct-Interim-Interval Callback-Number Class Filter-Id Framed-Apple Talk-Link Framed-Apple Talk-Network C Description: Specifies the classification of a	Restrict	OK Cancel	> >
	Add	Edit Remove	8	hange password after	it has expired)
		Previous	Next Finish Ca	ncel	

8. Verify and click on Finish.