



ClearPass 6.5

Tech Note: ClearPass

Integration with 3rd Party Enforcement Points

ClearPass & Fortinet utilizing RESTful API and RADIUS Accounting

<u>Version</u>	<u>Date</u>	<u>Modified By</u>	<u>Comments</u>
0.1 / 0.2	Jan /Feb 2015	Danny Jump	Early Draft Versions
1.0	March 2015	Danny Jump	First Published Version
1.1	April 2015	Danny Jump	Calculating dynamically the user-role that is sent from TIPS role.

Introduction	4
Audience	5
CPPM 6.5 Post Auth Framework Changes	6
Configuring Fortinet & ClearPass.....	7
ClearPass Configuration	7
Fortinet Configuration for RESTful Integration	9
Manually Creating Users on Forti-Authenticator for integration testing	14
Curl Forti-Authenticator Login Example	14
Configuring Radius Accounting Proxy.....	16
Configuring RADIUS Accounting on Fortinet (Authenticator & FortiGate)	18
Figure 1 - ClearPass Attributes sent to Firewalls	4
Figure 2 - New Session Notification Enforcement Profile	6
Figure 3 - Adding a Generic HTTP Context Server	7
Figure 4 – Adding the Endpoint Server to the Server Action's	8
Figure 5 - Configuring SMTP on Forti-Authenticator	9
Figure 6 - Adding a LOCAL user to be used by the API.....	10
Figure 7 - Changing the user to an Administrator and enable API service	10
Figure 8 - Confirmation of WEB password for API service	11
Figure 9 - Example of email sent with PSK password	11
Figure 10 - Adding an AD server to Forti-Authenticator	11
Figure 11 - Viewing Logs in Logfile for user	12
Figure 12 - Checking SSO sessions in Forti-Authenticator for non-AD user	12
Figure 13 - Viewing Logs in Logfile for user	12
Figure 14 - Checking SSO sessions in Forti-Authenticator for AD user	13
Figure 15 - Running a Login with a curl command in verbose mode.....	15
Figure 16 - Running a Login with a curl command in normal mode	15
Figure 17 - SSO Logged in users	15
Figure 18 - Adding a PROXY Target.....	16
Figure 19 - Enabling Accounting Proxy Configuration	17
Figure 20 - Configuring Accounting Proxy on an example service	17
Figure 21 - Setting RADIUS accounting attribute Filter-Id = 'geek-group'	18
Figure 22 - Calculating the TIPS role from AD memberOf.....	19
Figure 23 - Using TIPS role as the bases for User-Role in Fortinet	20
Figure 24 - Checking RADIUS Accounting listen service is enabled on the interface	21
Figure 25 - Enable RADIUS SSO client on Forti-Authenticator	22
Figure 26 - Setting RADIUS Accounting source and remapping attributes	22
Figure 27 - Adding a RADIUS Accounting source [ClearPass]	23
Figure 28 - Adding ClearPass as a RADIUS Accounting source	23
Figure 29 - Configuring the Forti-Authenticator Accounting Target/Destinations	24
Figure 30 - Monitor RADIUS SSO Sessions in Forti-Authenticator	24

Figure 31 - Enabling RADIUS Accounting listener on FortiGate	25
Figure 32 - Configuring RADIUS SSO on FortiGate.....	25
Figure 33 - FortiGate RADIUS default configuration.....	26
Figure 34 - Setting the FortiGate to use User-Name as the authenticator	26
Figure 35 - FortiGate RADIUS configuration after changes.....	26
Figure 36 - FortiGate using RADIUS accounting 'class' to parse 'user-role'	27
Figure 37 - Changing FortiGate to use a different AVP than class for 'user-role'	27
Figure 38 - FortiGate RADIUS configuration.....	28
Figure 39 – Defining a GROUP within FortiGate to match CPPM 'role' for user	28
Figure 40 - FortiGate User groups.....	29
Figure 41 - Adding a rule referencing the group 'geek-group'	29
Figure 42 - FortiGate showing differentiated users User-Group.....	30

Introduction

This series of TechNotes describes the integration with 3rd Party firewall vendors. Within this document we have captured the integration with Fortinet. There are two methods of integration between ClearPass Policy Manager and Fortinet. One uses HTTP JSON encoded RESTful API's the other uses RADIUS Accounting. In the table below we have captured the features and restrictions of different vendors and the capabilities they support.

Note that the framework we have developed is **not** limited to only the below vendors.

Similar to the integration that exists between ClearPass and other vendors, Fortinet supports at a basic level the ability to pass username and source IP address attributes. But other attributes shown below can also be passed. As a summary this is a list of the attributes we pass from CPPM 6.5 to the vendors we have tested.

Feature/ Firewall	CheckPoint	Fortinet	SonicWall	Palo Alto
Source IP	✓	✓	✓	✓
Username	✓	✓	✓	✓
User Role	✓	✓ [a]	✗	✗
Domain	✓	✗	✗	✓
Device Type	✗	✗	✗	✓
Machine OS	✗	✗	✗	✓
Machine Name	✓ [b]	✗	✗	✓
Health/Posture	✗	✗	✗	✓



Figure 1 - ClearPass Attributes sent to Firewalls

[a] = Available from RADIUS Accounting, not from HTTP REST API calls

[b] = Available from HTTP REST API calls not from RADIUS Accounting.

The intent is to document the integration between CPPM and Fortinet. This document focuses on testing and integration specifically Fortinet Authenticator 3.x and FortiGate 5.x or later and covers the integration using RESTful API and RADUS Accounting.

Where it is practical, best practices will be documented, although not every conceivable use case or deployment can or will be covered here in this document.

 **Note:** Within this document where you see a red-chili  this is used to signify a **'hot'** important point and highlights that this point is to be taken as a best-practice recommendation.

Audience

The reader is assumed to be familiar with the ClearPass family of products. Basic knowledge of IP networks and wide-area networking is also assumed. A general understanding and previous experience in the deployment/configuration of Fortinet products is also assumed. We also make the assumption that the firewall is already deployed. We will not cover the firewall deployment or configuration beyond the steps to integrate ClearPass.

CPPM 6.5 Post Auth Framework Changes

Historically the Post Auth framework has provided multiple functions such as Palo Alto Networks Integration, RADIUS Accounting, Session Restrictions such as Bandwidth Usage or Multiple Device Enforcement, etc. Starting in CPPM 6.5 we released an enhancement to the Post Auth framework. This will allow ClearPass to provide an enhanced level of integration and possibly allow the enduser/customer the ability to add additional 3rd party systems without Aruba having to specifically add support for the vendor directly in to ClearPass. This follows a similar approach to ClearPass Exchange where the flexibility of ClearPass Exchange encourages and allows for the integration into 3rd party system supporting HTTP RESTful frameworks.



The new Enforcement Profile is a '**Session Notification Enforcement**'. Through the next few sections we will cover this in detail. This new Enforcement Profile enhances the functionality we previously provided within the 'Session Restriction Enforcement Profile'.

Configuration » Enforcement

Enforcement Profile

Profile | Attributes

Template:

Name:

Description:

Type: Post_Authentication

Action: ☒ Accept ☐ Reject ☐ Drop

Device Group List:

Remove View Details Modify

Agent Enforcement
CLI Based Enforcement
ClearPass Entity Update Enforcement
Generic Application Enforcement
HTTP Based Enforcement
SNMP Based Enforcement
✓ Session Notification Enforcement
Session Restrictions Enforcement
TACACS+ Based Enforcement

Figure 2 - New Session Notification Enforcement Profile



Note: When you migrate a system from a previous CPPM 6.x software level (6.4.x and lower), if previously you had configured integration with a Palo Alto Networks firewall, this would have been defined using a Session Restriction Enforcement Profile [Type – Session Check IP-Address-Change-Notify]. These Enforcement Profiles are **NOT** supported under CPPM 6.5 and any configuration using these profiles is migrated as you upgrade to CPPM 6.5.

Configuring Fortinet & ClearPass

Configuration is required on both the ClearPass and Forti-Authenticator to accomplish the integration. We DO NOT document the configuration between Forti-Authenticator and the FortiGate Firewalls. The Forti-Authenticator unit can integrate with external NAD such as RADIUS (CPPM) and LDAP to gather user logon information and send it to the FortiGate units. The integration discussed below uses a Fortinet exposed RESTful API within the Forti-Authenticator product.

Within ClearPass, the integration with Fortinet falls under the ClearPass Exchange Framework, this framework allows for an extremely flexible and vendor agnostic solution architecture. At the heart of ClearPass Exchange are Context-Servers [endpoints we interoperate with] and Context-Server-Actions [functions performed against the Context Servers]. Starting in ClearPass 6.5 released in February 2015 we have supplied two Fortinet context server actions templates, Login and Logout. We recommend that these default templates are copied and then modified as appropriate when configuring the context server actions for your own installation.

The following two sections walk you through the ClearPass and Fortinet configuration.

ClearPass Configuration

HTTP Context Server: First you need to add a HTTP Context Server (this is the Fortinet Authenticator endpoint). Follow the below directions to add the Context Server:-

Administration -> External Servers -> Endpoint Context Servers [Add]

Administration » External Servers » Endpoint Context Servers

Endpoint Context Servers

Modify Endpoint Context Server

Server Actions

Server Type: Generic HTTP

Server Name: 10.10.10.10

Server Base URL: https://10.10.10.10

Username: admin

Password: Verify Password:

Validate Server: ☐ Enable to validate the server certificate

Enable Server: ☒ Enable to fetch endpoints from the server

Bypass Proxy: ☐ Enable to bypass proxy server

Show 100 records

Name	Status	Actions
all	Enabled	
	Enabled	
	Enabled	
	Enabled	
	Enabled	

Export Delete

Figure 3 - Adding a Generic HTTP Context Server

Add the appropriate Server Name (IP Address), this will be translated in to the Server Base URL. Add the Username/Password credentials used to communicate with the Forti-Authenticator firewall. The process of obtaining the username/password are discussed below in section '[Fortinet Configuration/ Configuring HTTP API Access](#)'.

Context Server Actions: Now that we have defined the Forti-Authenticator endpoint, we need to amend the Fortinet context server actions '**Login & Logout**' to use this Generic HTTP endpoint just configured.

It's very important that you modify **both** the Login and Logout Server Actions. These are what update the Firewall of a users session going active/de-active. ClearPass will then update the Forti-Authenticator, this in turn will permit/deny this user. We don't want to update the firewall of a session starting and never clear this session down.

Note: Its recommended that you copy the supplied/original **Fortinet Login/Logout** context server actions templates and modify the copied items.

Within the 'Action' tab the 'Server Name' must be changed to that of the HTTP server you added in the previous section. The default will be localhost, select the HTTP context server added previously in the drop-down.

Action	Header	Content	Attributes
Server Type:	Generic HTTP		
Server Name:	10.2.100.35		
Action Name:	LAB-Fortinet Login		
Description:	Inform Fortinet that user logged in.		
HTTP Method:	POST		
Skip HTTP Auth:	<input type="checkbox"/> Enable to skip HTTP Basic Authentication		
URL:	/api/v1/ssoauth/		

Save Cancel

Figure 4 – Adding the Endpoint Server to the Server Action's

Note: Nothing needs to be changed on the Fortinet Login/Logout Context Server Actions **beyond** ensuring the correct Server has been selected as shown above by selecting the Context Server defined previously on the Action Tab. The above shows the **Login** Context Server Action, the process is exactly the same for the **Logout** Context server action.

Fortinet Configuration for RESTful Integration

Configuration needs to be completed within the Forti-Authenticator. Several items need to be configured. Follow the steps below to complete the configuration.

Configuring HTTP API Access: To allow CPPM to send username info into Forti-Authenticator requires that we use a username/password that is enabled for this function. Firstly you need to configure SMTP as the password that will be used in conjunction with the username must be emailed to a user configured as shown below e.g. a GMAIL account.

First setup your SMTP server... **System -> Messaging -> SMTP Servers**... then click on 'Create now' below is an example of using GMAIL server as a mail-relay Your SMTP configuration will likely differ.

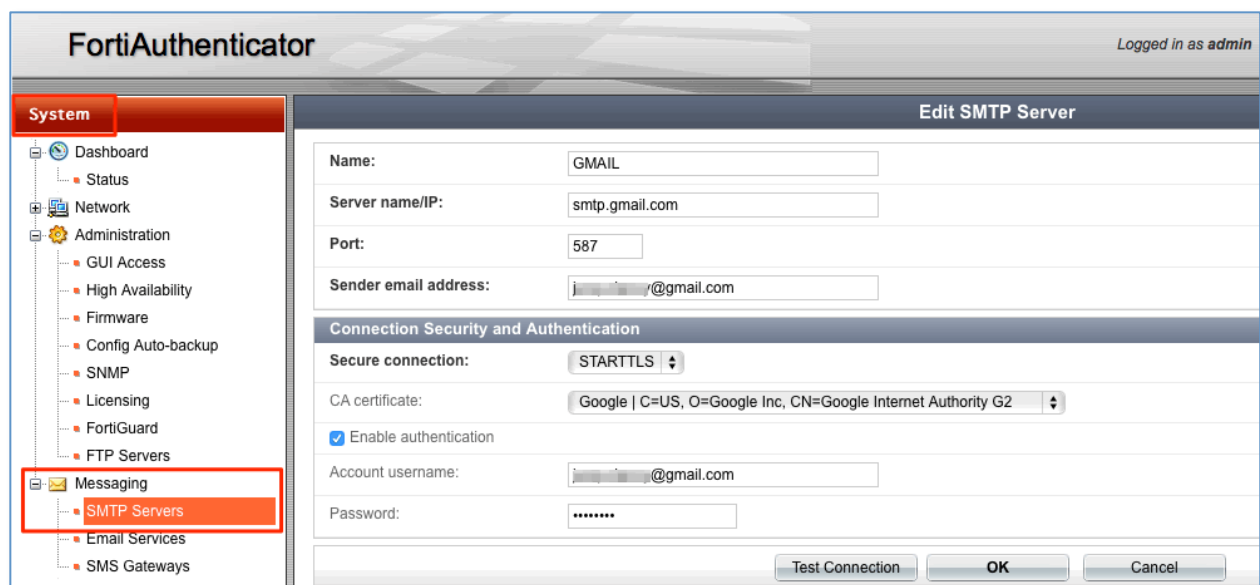


Figure 5 - Configuring SMTP on Forti-Authenticator

Next you need to create a local on box account that you will later configure within CPPM to be used by the RESTful integration. Go to **Authentication -> User Management -> Local Users** then click on 'Create now'



Note: The password specified below is **not** the password configured in CPPM for the HTTP Context Server admin-user definition. That Password is sent out via the SMTP configured above as we previously mentioned.

Figure 6 - Adding a LOCAL user to be used by the API

Following the creation of the account, it needs to be modified to enable the API service. The account will likely have been created as a 'User', change the account to 'Administrator' and enable the 'Web service access'. Ensure that you enter a VALID email address in the User Information. Forti-Authenticator will email the PSK to this email address. This is the PSK configured as the password in CPPM that will be used to communicate using the RESTful API.

Figure 7 - Changing the user to an Administrator and enable API service

Having made the above changes, the below confirmation shows the account has been changed, more importantly the confirmation of the email with the password has been sent.

<div> <div>Create New</div> <div>Import</div> <div>Export Users</div> <div>Edit</div> <div>Delete</div> <div>0 of 3 selected</div> </div>							
<div> <div>✓</div> <div>User "admin-cppm" has been given an access to the web service. An email containing the web service secret key has been sent to the user.</div> </div>							
	User	First name	Last name	Email address	Admin	Status	T
<input type="checkbox"/>	admin	danny	Jump	danny@arubanetworks.com	✓	✓	
<input type="checkbox"/>	admin-cppm			admin-cppm@ns-tme.com	✓	✓	
<input type="checkbox"/>	aruba	danny	jump	djump@arubanetworks.com	✓	✓	

Figure 8 - Confirmation of WEB password for API service

Below is an example of the email sent by Forti-Authenticator with the PSK password.

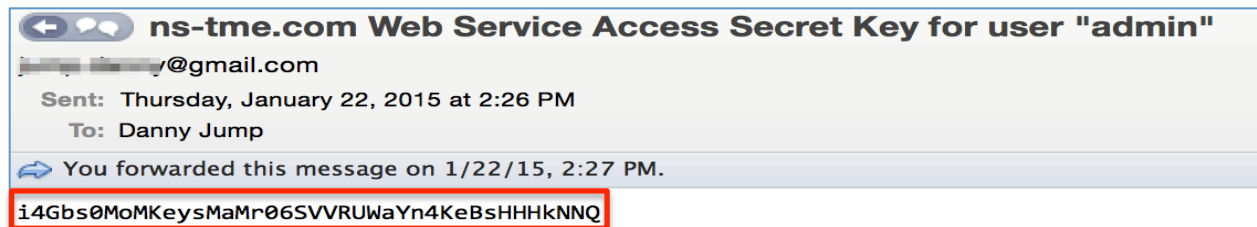


Figure 9 - Example of email sent with PSK password

Adding Active-Directory Server: You may have a need to add an Active-Directory server to the Forti-Authenticator. Complete this step from **Authentication -> Remote Auth. Servers -> LDAP**. Add the AD server as required. An example is below. Set your IP address, etc.

Edit LDAP Server	
Name:	win28k
Primary server name/IP:	Port: 389
<input type="checkbox"/> Use secondary server	
Base distinguished name:	DC=ns-tme,DC=com Set base DN as required
Bind type:	<input type="radio"/> Simple <input checked="" type="radio"/> Regular
Username:	Password: *****
User object class:	person Default Values
Username attribute:	sAMAccountName Default Values
Group membership attribute:	memberOf Default Values

Figure 10 - Adding an AD server to Forti-Authenticator

Adding the AD server allows Forti-Authenticator to validate the username sent by ClearPass. Within the Forti-Authenticator you can monitor the usernames received from in the **Logging -> Log Access -> Logs**. In this Log-file you can see the usernames.

FortiAuthenticator										Logged in as admin	Help	Logout	F
System													
Authentication													
Fortinet SSO Methods													
Monitor													
Certificate Management													
Logging													
ID	Timestamp	Level	Category	Sub category	Type id	Action	Status	NAS name/IP	Short message				
1068	Fri Jan 23 17:30:44 2015	information	Event	Web Service	50501				SSO logon request sent for user "danny_jump" with IP 10.1.73.175				
1067	Fri Jan 23 15:41:43 2015	information	Event	Web Service	50501				SSO logoff request sent for user "verytemp" with IP 10.1.73.175				
1066	Fri Jan 23 15:39:42 2015	information	Event	Web Service	50501				SSO logon request sent for user "verytemp" with IP 10.1.73.175				
1065	Fri Jan 23 15:38:53 2015	information	Event	Authentication	20994	Login	Success		Local administrator authentication with no token successful				
1064	Fri Jan 23 15:37:16 2015	information	Event	Web Service	50501				SSO logon request sent for user "fred" with IP 10.1.73.175				
1063	Fri Jan 23 15:36:32 2015	information	Event	Web Service	50500				Sent API secret key via email to user "admin"				
1062	Fri Jan 23 15:36:32 2015	information	Event	System	30908				smt				
1061	Fri Jan 23 15:36:30 2015	information	Event	Admin Configuration	10001	Add			Added Web Service Access: admin				
1060	Fri Jan 23 15:36:30 2015	information	Event	Admin Configuration	10002	Edit			Edited Local User Profile: admin (changed fields: FortiToken authentic				
1059	Fri Jan 23 15:36:30 2015	information	Event	Admin Configuration	10002	Edit			Edited Local User Profile: admin (changed fields: FortiToken authentic				

Figure 11 - Viewing Logs in Logfile for user

Now, the username sessions here do not necessarily translate to an SSO valid session that can be seen in **Monitor -> SSO -> SSO Sessions**. The above log file shows a user 'danny_jump'.... But there is no valid SSO session for this user as danny_jump is **not** in the Active Directory that Forti-Authenticator is joined to. See below, '0 SSO sessions' shown.

FortiAuthenticator		Refresh
0 SSO sessions		

Figure 12 - Checking SSO sessions in Forti-Authenticator for non-AD user

Again we see the user 'danny' in the Log file below,... but this time we also see the user in the SSO Sessions log as this user 'danny', is also in the Active Directory that Forti-Authenticator is joined to and thus can be verified by the Forti-Authenticator.

FortiAuthenticator										Logged in as admin	Help	Logout	F
System													
Authentication													
Fortinet SSO Methods													
Monitor													
Certificate Management													
Logging													
ID	Timestamp	Level	Category	Sub category	Type id	Action	Status	NAS name/IP	Short message				
1069	Fri Jan 23 17:42:37 2015	information	Event	Web Service	50501				SSO logon request sent for user "danny" with IP 10.1.73.175				
1068	Fri Jan 23 17:30:44 2015	information	Event	Web Service	50501				SSO logon request sent for user "danny_jump" with IP 10.1.73.175				
1067	Fri Jan 23 15:41:43 2015	information	Event	Web Service	50501				SSO logoff request sent for user "verytemp" with IP 10.1.73.175				
1066	Fri Jan 23 15:39:42 2015	information	Event	Web Service	50501				SSO logon request sent for user "verytemp" with IP 10.1.73.175				
1065	Fri Jan 23 15:38:53 2015	information	Event	Authentication	20994	Login	Success		Local administrator authentication with no token successful				
1064	Fri Jan 23 15:37:16 2015	information	Event	Web Service	50501				SSO logon request sent for user "fred" with IP 10.1.73.175				
1063	Fri Jan 23 15:36:32 2015	information	Event	Web Service	50500				Sent API secret key via email to user "admin"				
1062	Fri Jan 23 15:36:32 2015	information	Event	System	30908				smt				
1061	Fri Jan 23 15:36:30 2015	information	Event	Admin Configuration	10001	Add			Added Web Service Access: admin				

Figure 13 - Viewing Logs in Logfile for user

User 'danny' logged as a valid SSO session in the **Monitor -> SSO -> SSO Sessions**.

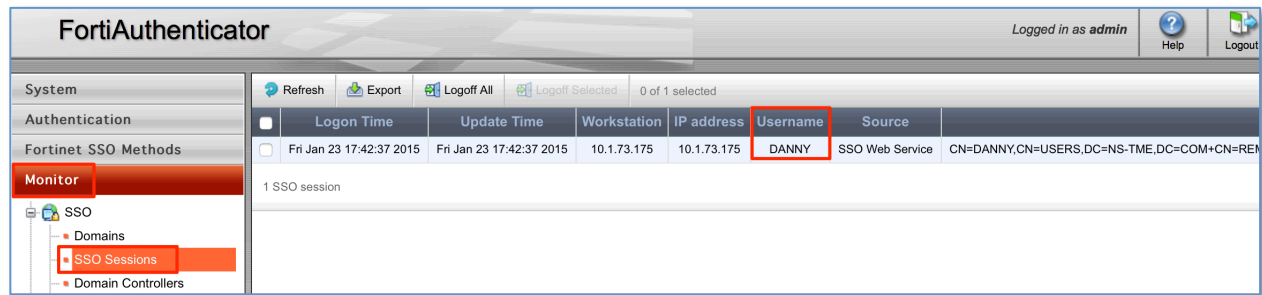


Figure 14 - Checking SSO sessions in Forti-Authenticator for AD user



Manually Creating Users on Forti-Authenticator for integration testing

Forti-Authenticator has the ability via curl/wget to manually create test users within the Forti-Authenticator system. This is a great feature to allow us to test the configuration.

Note: You need to have the PSK password that was discussed earlier as this is used to authenticate the curl/wget HTTP session.

Below are examples of a Login. Logout is very similar and explained below. I'm not going to provide a detailed description of the curl cmd beyond what relates to the Login/Logout.

Curl Forti-Authenticator Login Example

```
curl -k -v -u "admin:pKAHp8kLJXPQt2fQXmKrvYeIxMdAggfmOXLGGqbx" -d
'{"event":"1","username":"danny","user_ip":"10.1.73.175"}' -H "Content-Type:
application/json" https://IP\_of\_Forti-Authenticator/api/v1/ssoauth/
```

What's important from the above example...

"admin:followed_by_the_PSK" this is the PSK we discussed that must be emailed out.

"event":1 this makes this command effectively a **LOGIN** command. Change the **1** to a **0** to make this command function as a **LOGOUT**.

"username":"danny" Pretty obvious, this is the username sent from CPPM..!!

"user_ip":"10.1.73.175" Pretty obvious, this is the IP addresses of the endpoint..!!

[https:// IP_of_Forti-Authenticator /api/v1/ssoauth/](https://IP_of_Forti-Authenticator/api/v1/ssoauth/) This is the IP address of the Forti-Authenticator, you should also recognize the path after the IP address as that matching within the Context Server Action URL for Fortinet Login.

Below is a verbose example of running the Login command using the curl command. The -v option shows all the dialogue. You can see the curl command connecting to Forti-Authenticator, then the server authenticating the admin and then a successful POST of the user-data with the HTTP 200 OK status-code.

```
danny-jump:~ djump$ curl -k -v -u
"admin:pKAHp8kLJXPQt2fQXmKrvYeIxMdAggfmOXLGGqbx" -d
'{"event":"1","username":"danny","user_ip":"10.1.73.175"}' -H "Con
tent-Type: application/json" https:// IP_of_Forti-Authenticator
/api/v1/ssoauth/
* Hostname was NOT found in DNS cache
*   Trying IP_of_Forti-Authentocator...
* Connected to IP_of_Forti-Authenticator port 443 (#0)
* TLS 1.2 connection using TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
* Server certificate: FAC-VM0A14000265
* Server certificate: support
```

```

* Server auth using Basic with user 'admin'
> POST /api/v1/ssoauth/ HTTP/1.1
> Authorization: Basic
YWRtaW46cEtBSHA4a0xKWFB RdDJmUVhtS3J2WWVJeE1kQWdnZm1PWExHR3FieA==
> User-Agent: curl/7.37.1
> Host: IP_of_Forti-Authenticator
> Accept: */*
> Content-Type: application/json
> Content-Length: 56
>
* upload completely sent off: 56 out of 56 bytes
< HTTP/1.1 200 OK
< Date: Sat, 24 Jan 2015 02:29:23 GMT
* Server Apache is not blacklisted
< Server: Apache
< Vary: Accept,Accept-Language, Cookie
< X-Frame-Options: SAMEORIGIN
< Content-Language: en
< Content-Length: 0
< Content-Type: text/html; charset=utf-8

```

Figure 15 - Running a Login with a curl command in verbose mode

As an example of the same command run without the verbose [-v] option.....

```

danny-jump:~ djump$ curl -k -u
"admin:pKAHp8kLJXPQt2fQXmKrvYeIxMdAggfmOXLGGqbx" -d
'{"event": "1", "username": "danny", "user_ip": "10.1.73.176"}' -H "Content-Type: application/json" https:// IP_of_Forti-Authenticator
/api/v1/ssoauth/
danny-jump:~ djump$

```

Figure 16 - Running a Login with a curl command in normal mode

Two users 'danny' from different IP address's 10.1.73.175 & 176 from the above two curl cmds.

<div> Refresh Export Logoff All Logoff Selected 0 of 2 selected Search for SSO sessions </div>							
<input type="checkbox"/>	Logon Time	Update Time	Workstation	IP address	Username	Source	
<input type="checkbox"/>	Fri Jan 23 19:29:44 2015	Fri Jan 23 19:29:44 2015	10.1.73.176	10.1.73.176	DANNY	SSO Web Service	CN=DANNY,CN=USERS,DC=NS-TME,DC=COM+CN=REMOTE DESKTOP USERS,CN=BUILTIN,DC=NS
<input type="checkbox"/>	Fri Jan 23 19:25:50 2015	Fri Jan 23 19:25:50 2015	10.1.73.175	10.1.73.175	DANNY	SSO Web Service	CN=DANNY,CN=USERS,DC=NS-TME,DC=COM+CN=REMOTE DESKTOP USERS,CN=BUILTIN,DC=NS
2 SSO sessions							

Figure 17 - SSO Logged in users

Configuring Radius Accounting Proxy

An additional integration method to support 3rd Party vendors was also added to the CPPM 6.5 release. We now support the ability to configure a RADIUS Accounting Proxy. This allows CPPM to proxy the RADIUS accounting data that is received to an external system. When CPPM processes an authentication, as part of the session configuration on CPPM a RADIUS Accounting Proxy target can also be configured. This then allows CPPM to forward the interim accounting updates it receives from the NAS to this external target.

Configure Accounting Proxy on CPPM as shown below First configure your targets, under **Configuration-> Network -> Proxy Targets** just like you would previously if you were configuring RADIUS authentication proxy-ing.

The screenshot displays the 'Proxy Targets' configuration page in the Fortinet ClearPass interface. The breadcrumb navigation at the top reads 'Configuration » Network » Proxy Targets'. Below this, there is a filter section with a dropdown menu set to 'Name', a search box containing 'contains', and buttons for 'Go' and 'Clear Filter'. A table lists existing proxy targets:

#	Name	Hostname	Description
1.	checkpoint-pr		
2.	fortinet-proxy		

Below the table, it says 'Showing 1-2 of 2'. An 'Add Proxy Target' dialog box is open in the foreground. The dialog contains the following fields:

- Name: test-proxy
- Description: (empty)
- Hostname: 1.1.1.1 (highlighted with a red box)
- Shared Secret: (masked with dots)
- Verify Shared Secret: (masked with dots)
- RADIUS Authentication Port: 1812 (Default is 1812)
- RADIUS Accounting Port: 1813 (Default is 1813)

At the bottom of the dialog are 'Save' and 'Cancel' buttons. A red arrow points to the 'Save' button.

Figure 18 - Adding a PROXY Target

By default the Account Proxy Tab is not shown, you must enable it in the Service Definition as highlighted below.

Configuration » Services » Edit - Enforcement-TEST

Services - Enforcement-TEST

Summary	Service	Authentication	Roles	Enforcement
Name:	Enforcement-TEST			
Description:	Aruba 802.1X Wireless Access Service			
Type:	Aruba 802.1X Wireless			
Status:	Enabled			
Monitor Mode:	<input type="checkbox"/> Enable to monitor network access without enforcement			
More Options:	<input type="checkbox"/> Authorization <input type="checkbox"/> Posture Compliance <input type="checkbox"/> Audit End-hosts <input type="checkbox"/> Profile Endpoints <input type="checkbox"/> Accounting Proxy			

Figure 19 - Enabling Accounting Proxy Configuration

Now that the target is defined and the Accounting Proxy is enabled the remaining configuration can be completed.

Below is an example of adding the Accounting Proxy to the above service definition. We added a proxy target from one of the targets configured in the previous step.

Configuration » Services » Edit - Enforcement-TEST

Services - Enforcement-TEST

Summary	Service	Authentication	Roles	Enforcement	Profiler	Accounting Proxy
Accounting Proxy Targets :						
RADIUS-acc-proxy-trg				Move Up Move Down Remove View Details Modify		
--Select to Add--						
RADIUS attributes to be added for Accounting proxy						
Type	Name	=	Value			
1.	Click to add...					

Figure 20 - Configuring Accounting Proxy on an example service



Note: Whatever RADIUS accounting data we receive from the NAS we will forward to the Accounting Proxy target. We can also add VSA attributes to the data we forward. However, to add a VSA we must have the Dictionary's for the vendor's product installed/enabled within CPPM, or we may be able to use an IETF VSA. Some vendors have multiple RADIUS Dictionaries across their product ranges, so just because we have one for company X does not mean it will encompass all their products and the VSA's they support.

Configuring RADIUS Accounting on Fortinet (Authenticator & FortiGate)

Utilizing the RADIUS Accounting Proxy in ClearPass allows us to proxy the accounting information to Forti-Authenticator and FortiGate firewalls. Which can use the RADIUS Accounting records to simplify the SSO process for users. Forti-Authenticator can also manipulated the data before it forwards it to the subscribing FortiGate firewalls.

Note: If a customer does not have a Forti-Authenticator then RADIUS Accounting data could be sent directly to the FortiGate firewall, this is explained below in a later section. If a customer has multiple FortiGate firewalls by using the Forti-Authenticator the forwarding of data from ClearPass is simplified as ClearPass now only has to send to a single target. Forti-Authenticator will then forward the data to the subscribing FortiGate firewalls. However, if there is no Forti-Authenticator in the customers network, ClearPass can fulfill the RADIUS accounting 'broadcast' role.

As discussed below in more depth and the reasoning, we will be using the Filter-Id field to pass the 'user-role' from ClearPass to the Forti-Authenticator and FortiGate endpoints.

Here is how you add the RADIUS Accounting attribute Filter-Id [attribute 11] in to the ClearPass Accounting Proxy policy so that when the RADIUS Accounting data is forwarded to the Fortinet product we set the 'user-role' as appropriate. In the below example we are setting the Filter-Id to be 'geek-group', in other ClearPass services we configured for our testing we set a different Filter-Id as appropriate, e.g. **geek-group**, **PLM** or **TME**. This is then parsed and matched on the Forti-Authenticator/FortiGate to tie the user to the relevant User Group to enforce policy.



In the service enable, the Accounting Proxy, add a RADIUS attribute, **Radius:IETF**, under Name, find **Filter-Id** (attribute 11) and set the value as required.

Configuration » Services » Edit - Fortinet-Checkpoint testing

Services - Fortinet-Checkpoint testing

Summary Service Authentication Roles Enforcement **Accounting Proxy**

Accounting Proxy Targets : fortigate

Move Up
Move Down
Remove
View Details
Modify

--Select to Add--

RADIUS attributes to be added for Accounting proxy

Type	Name	=	Value
1. Radius:IETF	Filter-Id	=	geek-group
2. Click to add...			

Figure 21 - Setting RADIUS accounting attribute Filter-Id = 'geek-group'

Note: The **Value** field above can also be a substitutional attribute as shown below.... Just to call this out you could choose from any of the allowable values we support.... Whether they make sense to be used for a 'user-role' will be appropriate to individual deployments..!!

Configuration » Services » Edit - Fortinet-Checkpoint testing

Services - Fortinet-Checkpoint testing

Summary Service Authentication Roles Enforcement **Accounting Proxy**

Accounting Proxy Targets : fortigate [Add new](#)

Move Up
Move Down
Remove
View Details
Modify

--Select to Add--

RADIUS attributes to be added for Accounting proxy

Type	Name	=	Value
1. Radius:IETF	Filter-Id (11)	=	%{Authorization:win28k:}
2. Click to add...			Previous choices %{Authorization:win28k:HostName} %{Authorization:win28k:Name} %{Authorization:win28k:OSServicePack} %{Authorization:win28k:Onboard Groups} %{Authorization:win28k:Onboard memberOf} %{Authorization:win28k:OperatingSystem} %{Authorization:win28k:Phone} %{Authorization:win28k:Title} %{Authorization:win28k:UserDN} %{Authorization:win28k:company} %{Authorization:win28k:memberOf}



Using AD TIPS Role as user-role The above method is a little bit inflexible and maybe not suitable or representative of how you want to identify a users-role. In the below example we are using the AD **memberOf** attribute to assign a Tips ROLE to the user, using the **CONTAINS** calculation.... In our example we look for PLM or TME and assign a similar TIPS role.

Configuration » Services » Edit - Fortinet-Checkpoint (PLM or TME)

Services - Fortinet-Checkpoint (PLM or TME)

Summary Service Authentication **Roles** Enforcement Accounting Proxy

Role Mapping Policy: Group [PLM or TME] [Modify](#) [Add new Role Mapping Policy](#)

Role Mapping Policy Details

Description:

Default Role: SE

Rules Evaluation Algorithm: first-applicable

Conditions	Role
1. (Authorization:win28k:memberOf CONTAINS PLM)	PLM
2. (Authorization:win28k:memberOf CONTAINS TME)	TME

Figure 22 - Calculating the TIPS role from AD memberOf

Then within the Accounting Proxy we use the value **{Tips:Role}** to pass the assigned role to the Fortinet enforcement point.

Note: You have to manually complete and type the text {Tips:Role}, as we do not auto-complete this parameter.

The screenshot shows the 'Configuration » Services » Edit - Fortinet-Checkpoint (PLM or TME)' page. The 'Accounting Proxy' tab is selected. Under 'Accounting Proxy Targets', 'fortiauth-proxy-trg' is listed with buttons for 'Move Up', 'Move Down', 'Remove', 'View Details', and 'Modify'. Below this is a 'RADIUS attributes to be added for Accounting proxy' section containing a table:

Type	Name	=	Value
1. Radius:IETF	Filter-Id	=	%{Tips:Role}
2. Click to add...			

Figure 23 - Using TIPS role as the bases for User-Role in Fortinet

Configure Forti-Authenticator RADIUS Accounting To start, ensure that the Forti-Authenticator is able to receive RADIUS Accounting messages. Check under **System -> Network -> Interfaces [data interface]** and then check the interfaces in use to ensure the Services are enabled as shown below.

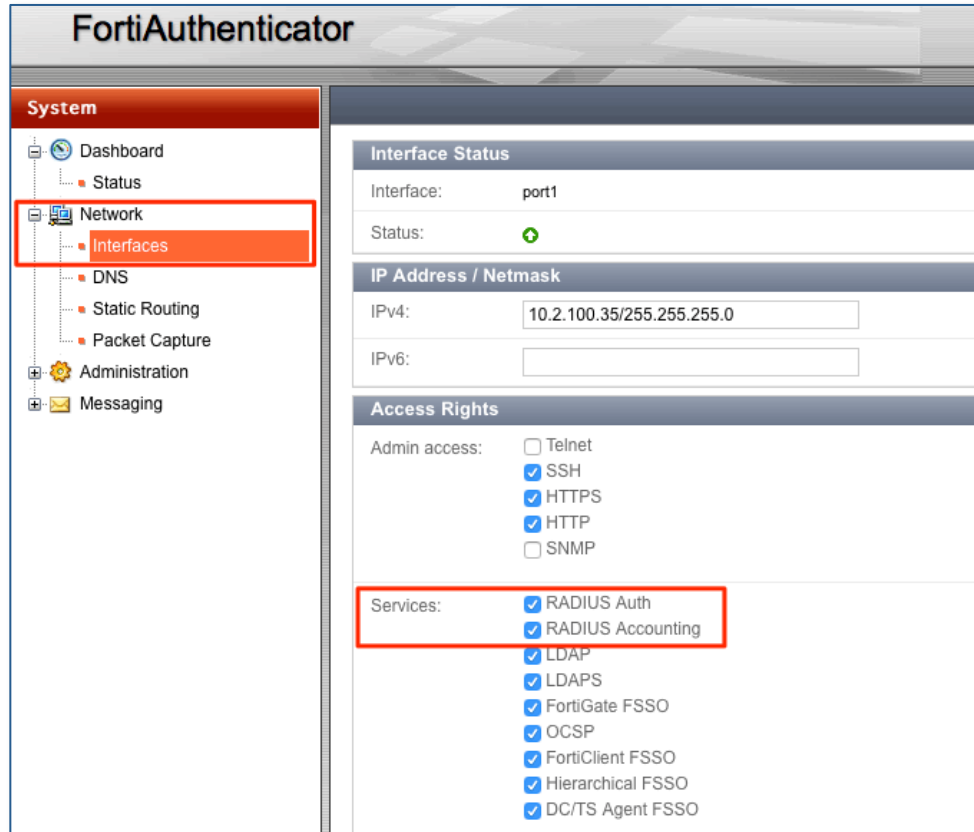


Figure 24 - Checking RADIUS Accounting listen service is enabled on the interface

Next enable RADIUS Accounting SSO clients – **Fortinet SSO Methods -> General**.

FortiAuthenticator

System

Authentication

Fortinet SSO Methods

SSO

General

Portal Services

Fine-grained Controls

SSO Users

SSO Groups

Domain Controllers

RADIUS Accounting

FortiGate Group Filtering

IP Filtering Rules

Tiered Architecture

Accounting Proxy

FortiGate

Listening port: 8000

☒ Enable authentication

Secret key:

Login expiry: 480 minutes

Extend user session beyond logoff by: 0 seconds (0-3600)

☐ Enable NTLM authentication

Fortinet Single Sign-On (FSSO)

Maximum concurrent user sessions: 0 [Configure Per User/Group]

Log level: Warning

☐ Exclude SSO source IP addresses matching these patterns:

☒ Enable Windows Active Directory domain controller polling

☐ Enable polling additional logon events

☒ Enable DNS lookup to get IP from workstation name

☐ Directly use domain DNS suffix in lookup

☒ Enable reverse DNS lookup to get workstation name from IP

☐ Do one more DNS lookup to get full list of IPs after reverse lookup of workstation name

☒ **Enable RADIUS Accounting SSO clients**

☐ Use RADIUS realm as Windows Active Directory domain

Figure 25 - Enable RADIUS SSO client on Forti-Authenticator



Next we need to configure the RADIUS Accounting and define the accounting source, **Fortinet SSO Methods -> SSO -> RADIUS Accounting**. Pay special attention to the RADIUS attributes below. We have mapped **Username** to **User-Name**, **Client IP** to **Framed-IP-Address** and **User group** attribute to **Filter-ID**.

FortiAuthenticator

System

Authentication

Fortinet SSO Methods

SSO

General

Portal Services

Fine-grained Controls

SSO Users

SSO Groups

Domain Controllers

RADIUS Accounting

Syslog

FortiGate Group Filtering

IP Filtering Rules

Tiered Architecture

Accounting Proxy

Name: 10.2.100.162

Client name/IP: 10.2.100.162

Secret:

Description:

SSO user type: External

Local users

Remote users

RADIUS Attributes

Username attribute: User-Name [Browse] [Default]

Client IP attribute: Framed-IP-Address [Browse] [Default]

User group attribute: Filter-Id [Browse] [Default]

Figure 26 - Setting RADIUS Accounting source and remapping attributes

Now we need to navigate to **Fortinet SSO -> Methods- > Accounting Proxy -> Sources** and click 'Create New' to add ClearPass as the source for the RADIUS Accounting messages.

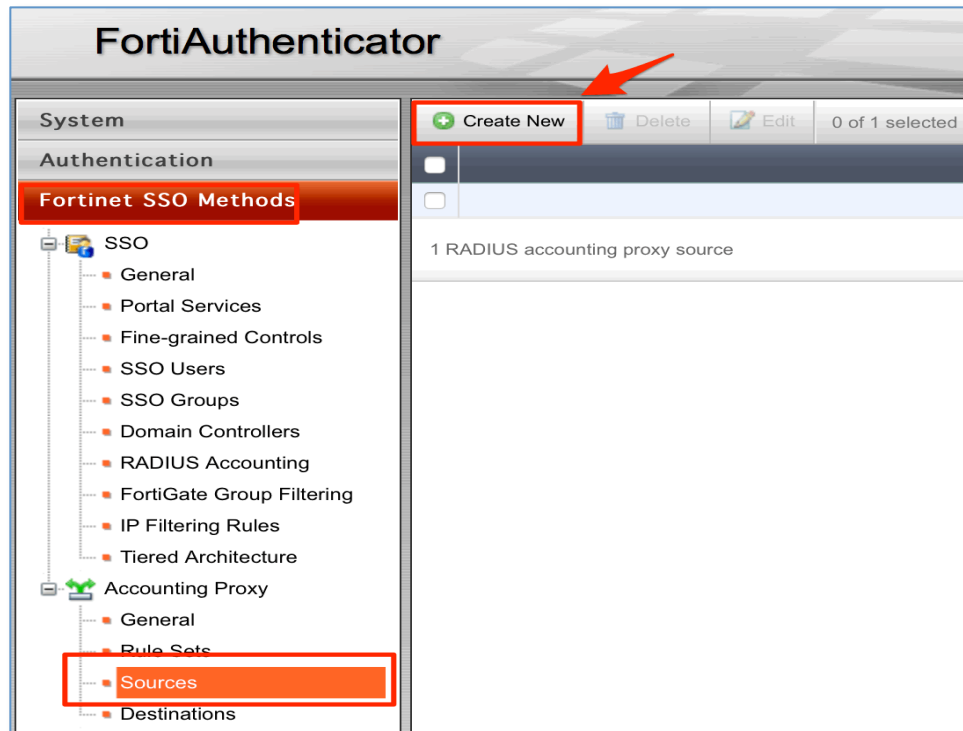


Figure 27 - Adding a RADIUS Accounting source [ClearPass]

Ensure that the PSK password matches the proxy-target you configured above in the ClearPass section.

The screenshot shows a dialog box titled 'Create New RADIUS Accounting Proxy Source'. It contains the following fields: 'Name:' with the value 'ClearPass-RADIUS-ACC_Src'; 'Source name/IP:' with the value '10.2.100.162'; 'Secret:' with a masked password '.....'; and 'Description:' which is empty. The 'Source name/IP:' and 'Secret:' fields are highlighted with a red box. At the bottom right, there are 'OK' and 'Cancel' buttons.

Figure 28 - Adding ClearPass as a RADIUS Accounting source

Next, you'll have to configure the Accounting Proxy Targets, were not going to cover this in detail but this is effectively the FortiGate firewalls.

The screenshot shows the FortiAuthenticator web interface. On the left, the 'System' menu is expanded, and 'Destinations' is selected under 'Accounting Proxy'. The main panel is titled 'Create New RADIUS Accounting Proxy Destination'. It contains the following fields:

- Name:** A text input field.
- Destination name/IP:** A text input field.
- Secret:** A text input field.
- Source:** A dropdown menu with '[Please Select]' as the current selection.
- Rule set:** A dropdown menu with '[Please Select]' as the current selection.

At the bottom right of the form are 'OK' and 'Cancel' buttons.

Figure 29 - Configuring the Forti-Authenticator Accounting Target/Destinations

Also not covered in this document is Forti-Authenticator ability to add or modify RADIUS IETF standard or VSA Accounting attributes to the Accounting data before it forwards to the FortiGate firewalls.

But once the above configuration is complete, you can check on and monitor the SSO session that are know in Forti-Authenticator under **Monitor -> SSO Sessions**

The screenshot shows the FortiAuthenticator web interface with the 'Monitor' tab selected. The 'SSO Sessions' sub-tab is active, displaying a table of active sessions. The table has the following columns: Logon Time, Update Time, Workstation, IP address, Username, and Source. There are 5 sessions listed, with the first three highlighted in red.

	Logon Time	Update Time	Workstation	IP address	Username	Source
<input type="checkbox"/>	Thu Mar 12 12:38:47 2015	Thu Mar 12 12:38:47 2015	\\10.2.100.30	255.255.255.255	ADMINISTRATOR	DC Polling
<input type="checkbox"/>	Thu Mar 12 13:49:48 2015	Thu Mar 12 13:49:48 2015	10.2.100.171	10.2.100.171	CARLOS	Radius Accounting
<input type="checkbox"/>	Thu Mar 12 13:50:45 2015	Thu Mar 12 13:50:45 2015	10.2.100.169	10.2.100.169	DANNY	Radius Accounting
<input type="checkbox"/>	Thu Mar 12 11:02:31 2015	Thu Mar 12 13:49:17 2015	10.2.100.167	10.2.100.167	DJUMP	Radius Accounting
<input type="checkbox"/>	Thu Mar 12 13:51:10 2015	Thu Mar 12 13:51:10 2015	WIN28K-TME.NS-TME.COM	10.2.100.120	F5-AD	DC Polling

5 SSO sessions

Figure 30 - Monitor RADIUS SSO Sessions in Forti-Authenticator

Configure FortiGate RADIUS Accounting

As discussed previously for customers that do not have Forti-Authenticator ClearPass can send RADIUS Accounting data directly to the FortiGate firewalls, this is discussed below.

To start, ensure that the FortiGate is able to receive RADIUS Accounting messages. Check on the FortiGate firewall to allow the interfaces to listen for RADIUS Accounting Messages under **System -> Network -> Interfaces [data interface]** ensure that the *Listen for RADIUS Accounting Messages* is enabled.

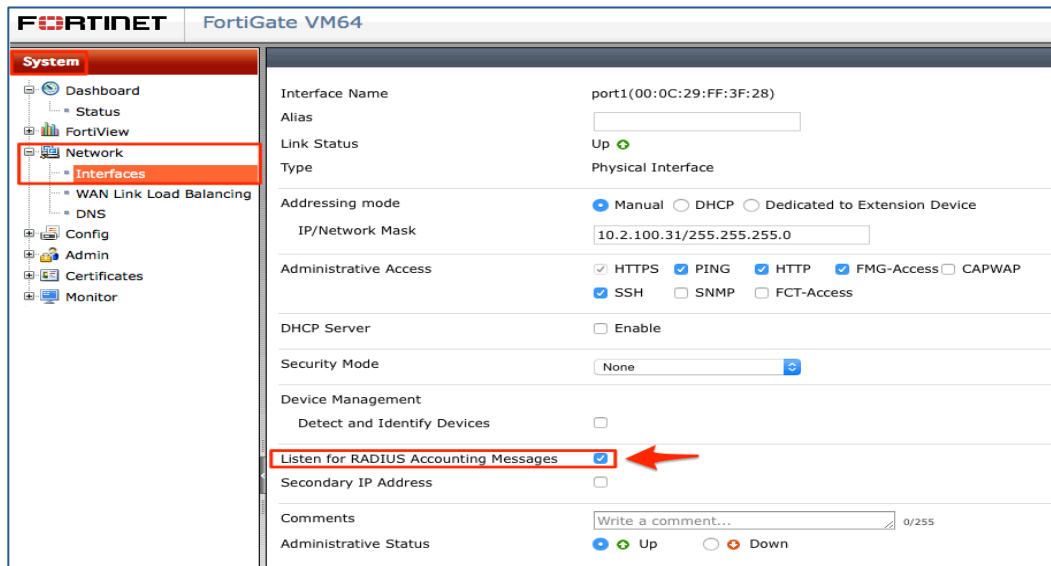


Figure 31 - Enabling RADIUS Accounting listener on FortiGate

Next enable the RADIUS SSO agent (RSSO), **Users & Devices -> Authentication -> Single Sign-On** and set the shared secret to match CPPM.

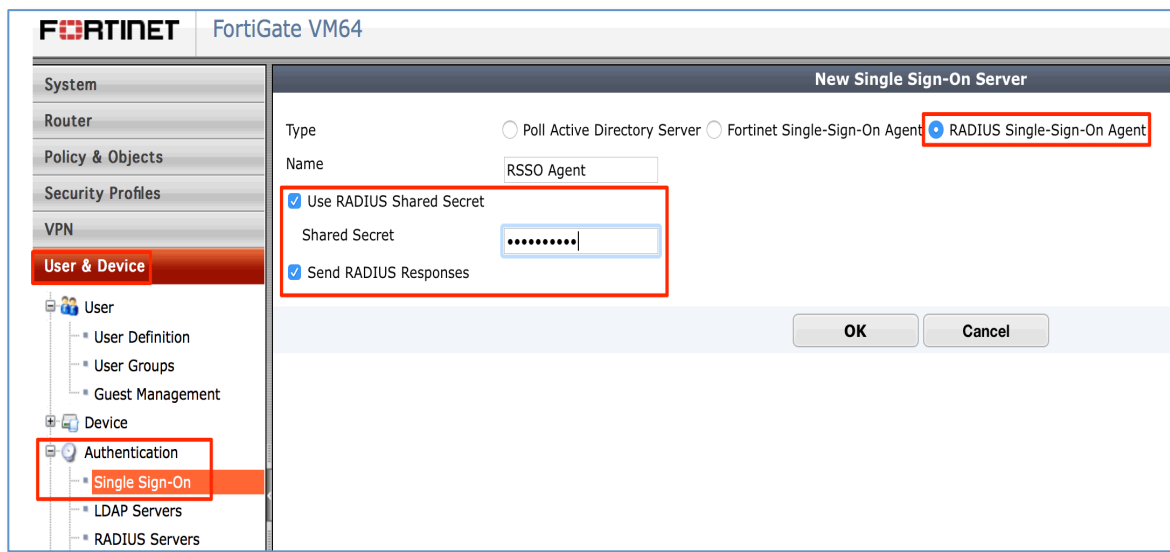


Figure 32 - Configuring RADIUS SSO on FortiGate

Now, the FortiGate will be receiving and consuming the RADIUS Accounting messages being sent from ClearPass. By default the FortiGate firewall will use the MAC address to authenticate the user. We need to modify the mapping so the FortiGate uses the username.

We do this from the CLI.... SSH to the firewall with the appropriate credentials.

Below is the configuration for the user 'radius' before we modify it.

```
fortigate_1 # show user radius
config user radius
  edit "RSSO Agent"
    set rso enable
    set rso-radius-response enable
    set rso-validate-request-secret enable
    set rso-secret ENC MVDPR2MuJzb4Bz0Uy2CrE6BpNTKQPm71wC8xapuEzMaq9HzV0r1GJUBJLQuL9aUHLuABypmovkCKmPLJTvPsaFVrk0QR0mTjdwQs
PXjYJyRmfSgrhHTDhyx+zga9YFma3B5RLhPBghmzdKib5nSyw==
    set rso-log-flags protocol-error profile-missing accounting-stop-missed accounting-event endpoint-block radiusd-other
  next
end
```

Figure 33 - FortiGate RADIUS default configuration

Change the radius configuration attribute **rso-endpoint-attribute** to use 'User-Name' as the authenticator. **Note:** Other attributes could be used.

```
fortigate_1 # config user radius
fortigate_1 (radius) # edit CPPM_650
fortigate_1 (CPPM_650) # set rso-endpoint-attribute User-Name
fortigate_1 (CPPM_650) # end
```

Figure 34 - Setting the FortiGate to use User-Name as the authenticator

Below is the configuration following the change, notice the new line in the configuration **set rso-endpoint-attribute User-Name**.

```
fortigate_1 # show user radius
config user radius
  edit "RSSO Agent"
    set rso enable
    set rso-radius-response enable
    set rso-validate-request-secret enable
    set rso-secret ENC MVDPR2MuJzb4Bz0Uy2CrE6BpNTKQPm71wC8xapuEzMaq9HzV0r1GJUBJLQuL9aUHLuABypmovkCKmPLJTvPsaFVrk0QR0mTjdwQs
PXjYJyRmfSgrhHTDhyx+zga9YFma3B5RLhPBghmzdKib5nSyw==
    set rso-endpoint-attribute User-Name
    set rso-log-flags protocol-error profile-missing accounting-stop-missed accounting-event endpoint-block radiusd-other
  next
end
```

Figure 35 - FortiGate RADIUS configuration after changes



Finally for this section we need to get the FortiGate RSSO User Group to match the Role set within ClearPass. This section requires several changes from the default.

By default the Fortigate firewall expects to parse the 'user-role' from the *RADIUS Attribute* 'Class' sent by ClearPass in the RADIUS Accounting-start messages. However this attribute [Class] is typically present in the RADIUS accounting messages ClearPass receives from some NAD's and would forward this to the FortiGate with an incorrect value. When ClearPass adds the [Class] AVP it adds it as a second index of [Class] but the Fortigate firewall only reads the first index value thus missing the AVP we have added used to set the 'user-role'. To overcome this issue we suggest using an RADIUS accounting attribute that is not being used. For our testing we have used Filer-ID.


Configuring this requires several. Initially when setting up the FortiGate User-Groups and when we add the 'user-role' tag if you float your cursor over the  as below you see the default that it will look to match on in the Accounting-Start messages is 'Class'.



Figure 36 - FortiGate using RADIUS accounting 'class' to parse 'user-role'

So we need to tell ClearPass to send the user-role in a different attribute and have FortiGate look for this AVP in the attribute we define.

Firstly we need to modify FortiGate to look elsewhere in the accounting messages. This is accomplished from within the CLI. Log into the CLI and follow the below commands.

Remember we opted to use the RADIUS attribute 'Filter-Id', you may select a different attribute as long as the ClearPass and FortiGate systems match.

If you look in the default FortiGate configuration the value 'sso-attribute' is not visible, the default is set to use the RADIUS accounting attribute 'class' though.

```
#config user radius
#edit CPPM_650      [this is the name of my CPPM node in FortiGate]
#set sso-attribute Filter-Id
#end
```

Figure 37 - Changing FortiGate to use a different AVP than class for 'user-role'

After this change my radius configuration on the FortiGate looks like this. Notice towards the end of the configuration the sso-attribute set to Filter-Id.

```

fortigate_1 # show user radius
config user radius
  edit "CPPM_650"
    set rso enable
    set rso-radius-response enable
    set rso-validate-request-secret enable
    set rso-secret ENC
    au6KRSJlpl6RIDJyT4Bp39rDaIokGw1e85zr0xcY5NSqHZQtOR+CQyTRswMcq3UOsQYOIvKH92k7cLL
    IJsz/vMnBKyLGTyhMw5bdem8UfAtHNgM+Ag022hSTvXFDk0MsoM9pKh7lj12liEcOU+H/11L+7Spr0I
    j4KBNCrzn5mXdPBjRG/5J/Db2hFPtYG2AbIPBPA==
    set rso-endpoint-attribute User-Name
    set sso-attribute Filter-Id
  next
end

```

Figure 38 - FortiGate RADIUS configuration

Now we need to create the User Groups on the FortiGate appliance and the appropriate label to associate an incoming username to a Fortinet User Group.

Create the User Groups as required, the Type must be set as RADIUS Single Sign-on (RSSO).

Under **User & Device -> User -> User Groups [Create New]**

The name is what FortiGate will use when you are defining policy.... See below....



Figure 39 - Defining a GROUP within FortiGate to match CPPM 'role' for user

We created as shown below three User Groups, and gave each Group a separate Label, aka the RADIUS Attribute Value. The Groups for our testing are PLM, TME and geek-group. The RADIUS attribute value is the same as the User Groups name, just for simplicity.

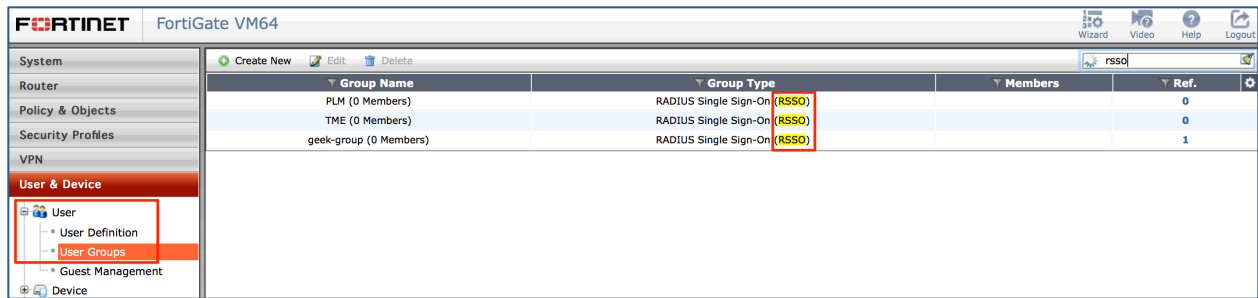


Figure 40 - FortiGate User groups

Now the Groups are created, we can create policy to apply enforcement to users based upon the Fortigate Group membership. This can be thought of as ClearPass is passing the role of the user within the RADIUS Accounting and FortiGate is grouping the users of this role under the User Group for the same level of enforcement.

Finally we defined a simple policy to show how we can reference the User Groups adding a policy rule referencing the group **geek-group**, also notice the other User Groups of **PLM** and **TME** could be selected.

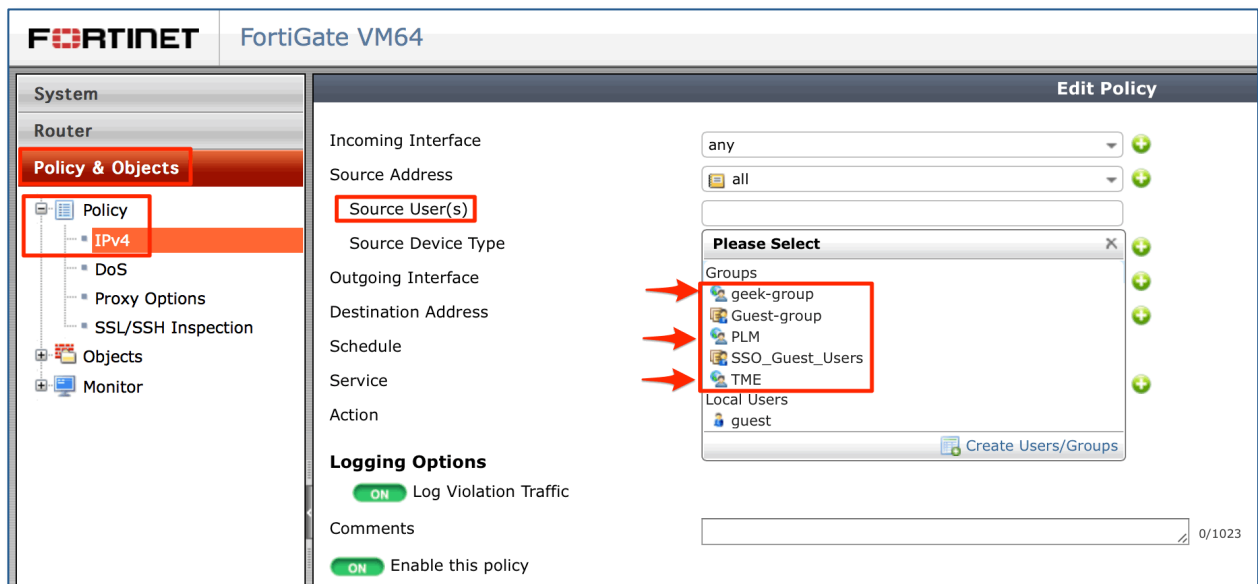
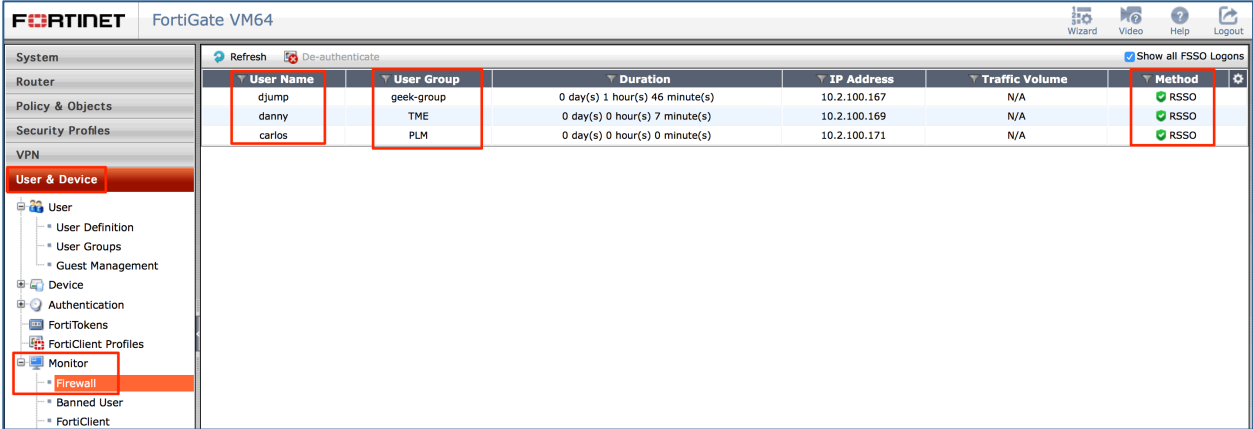


Figure 41 - Adding a rule referencing the group 'geek-group'

Now that ClearPass is passing the username with a 'user-role' we can see below the FortiGate authenticated users are matched to the relevant User-Group.



FortiGate VM64

System Router Policy & Objects Security Profiles VPN

User & Device

- User
 - User Definition
 - User Groups
 - Guest Management
- Device
- Authentication
- FortiTokens
- FortiClient Profiles
- Monitor
 - Firewall
 - Banned User
 - FortiClient

User Name	User Group	Duration	IP Address	Traffic Volume	Method
djump	geek-group	0 day(s) 1 hour(s) 46 minute(s)	10.2.100.167	N/A	RSSO
danny	TME	0 day(s) 0 hour(s) 7 minute(s)	10.2.100.169	N/A	RSSO
carlos	PLM	0 day(s) 0 hour(s) 0 minute(s)	10.2.100.171	N/A	RSSO

Figure 42 - FortiGate showing differentiated users User-Group