FortiAuthenticator RADIUS Accounting with SSO for FortiOS 5.2.4 Design Guide

VERSION 3.0
# Contents

Introduction ........................................................................................................................................... 3
Audience .................................................................................................................................................. 3
RADIUS Overview ................................................................................................................................. 3
  Clarification of Terms ........................................................................................................................... 3
FAC RADIUS Accounting Overview ...................................................................................................... 4
Protected EAP with MS-CHAPv2 Overview ........................................................................................... 5
FortiAuthenticator Configuration ........................................................................................................ 6
  Enable FAC to LDAP Integration ........................................................................................................ 7
  Enable FAC as a source of Single Sign-On ........................................................................................... 8
  Import Groups From LDAP .................................................................................................................. 9
  Enable FAC RADIUS Accounting ...................................................................................................... 10
FortiGate Configuration ......................................................................................................................... 11
  FGT to FAC Integration ...................................................................................................................... 11
  FGT Group Selection ........................................................................................................................... 11
  FGT Identity-Based Policy Using Group Imported From FAC ............................................................ 12
  FGT to NPS Integration ...................................................................................................................... 12
Microsoft Network Policy Server (NPS) ................................................................................................. 13
  RADIUS Clients and Remote RADIUS Server Groups .................................................................... 13
  RADIUS Connection and Network Policies ..................................................................................... 15
Client Configuration ............................................................................................................................. 18
  FAC RADIUS Accounting to SSO Verification and Troubleshooting .............................................. 21
Introduction
The purpose of this design guide is to provide a validated working configuration of FortiAuthenticator RADIUS Accounting to SSO. FortiAuthenticator supports the ability to receive RADIUS Accounting Packets and use the RADIUS Attribute Value Pairs as a source of authentication information and then push these events into FSSO. The components used are:

- FortiGate (FortiOS 5.2.4)
- Windows Server 2012 R2 with Network Policy Server
- FortiAP (v5.2-build0245)
- FortiAuthenticator v3.00-build0182-20150717-patch00
- Windows 7 SP1 laptop supporting 802.1X wireless authentication

This guide assumes that Virtual Domains are not enabled on the FortiGate and that Certificate Services are installed on the Network Policy Server. A Root CA is required because the CA public key is an integral part of 802.1x and will not work without it. This guide is also intended for medium to enterprise-sized environments that have a FortiAuthenticator (FAC). The FAC has better group management scalability and other features versus just a FortiGate (FGT) with RSSO, see the Clarification of Terms section for a further explanation.

Audience
This guide is written for network and security administrators who have a solid understanding for following areas:

- Microsoft Server 2012 and Network Policy (NPS) Server administration
- Configuring Protected EAP with MS-CHAPv2
- Windows 7 administration
- FortiOS administration with FAC integration
- Wireless Access Points (AP) configuration

RADIUS Overview

Clarification of Terms
‘RADIUS Single Sign-On’ or RSSO – A FortiOS feature which uses RADIUS accounting start/stop messages to extract information including username and IP Address. The group parameter (Class attribute) is used to match a local Fortigate RSSO Group containing the string we expect to receive from the RADIUS peer. RSSO does not lookup incoming user accounts against LDAP or any other authorization backend information, and does not therefore know what groups a given AD user is a member of. Hence an admin will need to manage totally separate identity groups versus FSSO even if the users are the same.

‘RADIUS Accounting’ – A FortiAuthenticator feature which also uses RADIUS accounting start/stop messages to extract information including username and IP Address. The FortiAuthenticator then queries an LDAP backend for a given username and retrieves all group memberships for that user. The FortiAuthenticator can then create standard FSSO Groups with that information allowing a FortiOS policy to remain identical to the Active Directory group naming structure. The main benefit, is it provides one set of unified FSSO Groups for identity based rules.

In summary of the above, RSSO does not equate to RADIUS Accounting as most environments ideally want to be using RADIUS Accounting, and thus a FAC, to avoid the complexity surrounding the management of two separate types of group identity.
FAC RADIUS Accounting Overview

Summary:
WPA2 Enterprise via 802.1x, PEAP/MSCHAPv2 sends User Login to NPS.
NPS validates Username and password.
NPS sends Start/Stop/Interim RADIUS packets details to the FAC.
FAC queries LDAP for user group information.
FAC sends updates to FGT via SSO.
Protected EAP with MS-CHAPv2 Overview

PEAP with MS-CHAP v2 is an EAP type that this design guide uses which is more easily deployed than Extensible Authentication Protocol with Transport Level Security (EAP-TLS) or PEAP-TLS because user authentication is accomplished by using password-based credentials (an Active Directory username and password) instead of digital certificates or smart cards. Only servers running Network Policy Server (NPS) and providing PEAP-MS-CHAPv2 authentication are required to have a certificate.

This next part is optional, the administrator can design to the solution to not use ‘Server Validation’ but involves more design consideration. When using Server Validation successful PEAP-MS-CHAP v2 authentication requires that the client trust the NPS server after examining the server certificate. For the client to trust the NPS server, the certification authority (CA) that issued the server certificate must have its own certificate in the Trusted Root Certification Authorities certificate store on the client computer. The server certificate used by NPS can be issued by your organization’s private trusted root CA deployed on your network, or by a public CA, such as VeriSign or Thawte, that is already trusted by the client computer.

The diagram below shows a generic 802.1x authentication exchange. The WLC in our case is the FortiGate. The FortiAuthenticator is not shown, but it would communicate with NPS server for RADIUS Accounting packets which would be step 2 in Figure 1.

![Diagram of 802.1x authentication exchange](image-url)
FortiAuthenticator Configuration

Excluding the FortiAP profile which is outside the scope of this guide, but briefly described in the previous section, there are three main components required to support FAC RSSO Accounting functionality. Those components are specific to the FAC, FGT, and NPS. This guide also includes an optional step of Server Validation that the client performs against the NPS server as described in the PEAP section above.

The main configuration components we will be working with in the following sections are shown below:

1. FAC RSSO Accounting configuration
2. FGT to the FAC for SSO connectivity
3. NPS and FAC integration

At the conclusion of the steps listed above, the FAC will receive RADIUS Accounting details from NPS and the FGT will receive SSO details from the FAC. The FGT will also inherit SSO Groups directly from the FAC which will allow the replication of the actual LDAP group structure and can then be used to create identity based policies on the FortiGate.

A couple of notes to consider:

- FAC RADIUS Accounting is different to FAC RADIUS Accounting Proxy. The Accounting Proxy is not used or covered in this design guide, see the online RADIUS Accounting Proxy Guide for more information.
- If the FGT is providing DHCP services for the SSID instead of a DHCP Relay to a backend DHCP server, then the FGT will update NPS with RADIUS Accounting packets relating to the IP Address provided to wireless clients.
Enable FAC to LDAP Integration

1. On the FAC, navigate to Authentication -> Remote Auth. Servers -> LDAP
2. Enter a Name, the ‘Primary server name/IP’ will be an Active Directory Global Catalog server. This relates to step 3 in Figure 1.

3. Test the LDAP lookup functionality by clicking the folder search icon next to the ‘Base distinguished name’ in order to select a starting point in the LDAP tree for group and user queries.
Enable FAC as a source of Single Sign-On

1. On the FAC browse Fortinet SSO Methods -> SSO -> General
2. Select ‘Enable authentication’ and enter a ‘Secret key’. The key must match similar configuration on the FGT which will be done in a later step. This relates to step 4 in Figure 1.
3. Select ‘Enable RADIUS Accounting SSO clients’, and ‘Use RADIUS realm as Windows Active Directory domain’. This relates to step 4 in Figure 1.
4. Select ‘Restrict user groups to SSO groups list’ and ‘Active’. This relates to step 4 in Figure 1. With this setting, the only groups that the FGT sees are the ones the FAC imports from LDAP and adds under FAC ‘SSO Groups’.

Figure 5
Import Groups From LDAP

1. On the FAC, browse to Fortinet SSO Methods -> SSO -> SSO Groups and click ‘Import’
2. Expand the LDAP tree (See ‘Enable FAC to LDAP Integration’ on page 7 for reference)
3. Whatever groups are selected here will be passed on to the FGT

![FortiAuthenticator](image)

Figure 6
Enable FAC RADIUS Accounting

1. On the FAC browse Fortinet SSO Methods -> SSO -> RADIUS Accounting

2. Enter a Name, the ‘Client name/IP’ will be the NPS, select ‘SSO user type’ ‘Remote Users’, and select ‘Remote LDAP server’ which was configured in the previous section. This relates to step 2 in Figure 1.

3. It is then necessary to configure NPS to forward RADIUS Accounting packets to the FAC which will be done in a later step. In order for FAC RADIUS Accounting to work, it is mandatory that the accounting packets contain the required Attribute Value Pairs (AVPs) which trigger an authentication event. The mandatory AVPs are:
   - Username = <User-Name>
   - Client IP = <Framed-IP-Address>

Figure 7
FortiGate Configuration

FGT to FAC Integration

1. On the FGT navigate to User&Device->Authentication->SingleSign-On and click ‘Create New’
2. Enter a Name, and under ‘Primary Agent IP/Name’ enter the FAC details
3. Click ‘Users/Groups’ and the groups available should match exactly what was imported into the FAC see page 9 for reference. Any time the FAC groups sent to the FGT are changed, you need to click ‘Apply&Refresh’ shown below in order for the new groups to appear
4. Note, there is no need to select an LDAP server because the FGT is not doing any LDAP queries – the group information received is based on what the FAC is configured to send

![FGT Group Selection](image8)

Figure 8

FGT Group Selection

1. On the FGT navigate to User&Device->UserGroups, click ‘Create New’, select ‘Fortinet Single Sign-On (FSSO), click the ‘+’ sign to add ‘Members’ – the group displayed will match what the FAC has selected from LDAP. The ones selected by the FAC are the only groups that will be made available to the FGT, see page 9 for reference

![FGT Group Selection](image9)

Figure 9
FGT Identity-Based Policy Using Group Imported From FAC

1. Create an Identity-Based Policy as usual

![FGT Identity-Based Policy Using Group Imported From FAC](image1)

Figure 10

FGT to NPS Integration

1. On the FGT navigate to User&Device -> Authentication -> RADIUS Servers, click ‘Create New’, and enter the NPS details. The 'Primary Server Secret' must match the NPS configuration for that setting. This related to step 1 of figure 1 and is what allows the WPA2 Enterprise wireless authentication to work.

![FGT to NPS Integration](image2)

Figure 11
Microsoft Network Policy Server (NPS)
The Microsoft NPS provides the authentication and accounting functionality in this environment. When a user provides login details to via the AP, the FGT will send those details via 802.1x to the NPS to verify the username and password against Active Directory. The NPS will then send RADIUS Accounting Packets to the FAC.

At the end of this section, the NPS will be configured to:

1. Authenticate users
2. Receive RADIUS Accounting packets from the FGT about the IP Address per wireless client
3. Send RADIUS Accounting packets to the FAC (see step 2 in Figure 1 for reference)

RADIUS Clients and Remote RADIUS Server Groups

1. In the “Network Policy Server” click “NPS (Local) | RADIUS Clients and Servers”
2. Right-Click “RADIUS Clients” | Select “New” and enter “Friendly name” “IP Address” and “Shared Secret” which must match the FortiGate ‘Primary Server Secret’ entered in a previous section.

![Figure 12](image-url)
3. Right-Click ‘Remote RADIUS Server Groups’, select ‘New’ and enter the Group name and click ‘Add’
4. Enter the FAC details accordingly.

![Figure 13](image-url)
RADIUS Connection and Network Policies

1. Right click ‘Connect Request Policies’ and create a new policy like what is shown below.
2. The ‘Called Station ID’ is the SSID from the FortiGate. Use the Called Station ID in this format ‘SSID$’ in order to further control the policy selection
3. The ‘Client IP Address’ is the FortiGate interface that sends the 802.1x details on behalf of the wireless client.
4. It advisable to link the Connect Request and Network Policies with the Called Station ID and Client IP Address, because it helps ensure that the Connection and Network Policies are ‘linked’ which helps with scalability in large environments
5. The ‘Accounting Provider Name’ references the FAC configuration for ‘Remote RADIUS Server Groups’ from the previous page

![Network Policy Server](image)

Figure 14
6. Right click ‘Network Policies’ and enter a policy similar to what is shown below for ‘Conditions’ and ‘Settings’.

   The ‘Condition’ settings relate to:
   - User Groups = the LDAP group that contains users authenticating for wireless services
   - Client IPv4 Address = the FGT interface that sends the 802.1x on behalf of the wireless client
   - Called Station ID = is the SSID from the FortiGate. Use the SSID with a dollar-sign as the value
   - Authentication Method = EAP needs to link to the NPS server certificate for 802.1x to work properly. See Figure 15 for an example, select ‘Microsoft: Protected EAP (PEAP)’, highlight then click ‘Edit’ to select the certificate

![Network Policy Server]

**Figure 15**
Figure 16
Client Configuration

This section assumes that your 802.1x client is configured correctly in order to connect to an SSID using “WPA2 Enterprise” authentication. A Root CA is also required, but Server Validation is optional.

Below is an example of how the Windows 7 wireless network connection should look on a windows laptop running Window 7 SP1. Add a new wireless connection as shown in the following two images.

![Figure 17]
1. Click “Advanced settings”, select “Specify authentication mode” and select “User authorization”. Click ‘Save credentials’ to automate a wireless re-authentication anytime the user is in range. Be aware, that when the user changes passwords this will have to be updated.

![Advanced settings](image)

Figure 18

2. The following is an example of Server Validation where the wireless client verifies the certificate it’s presented by the NPS server. This step is optional and is one of the most common errors/difficulties when using 802.1x. If “Validate server certificate” is selected then the Root CA certificate from the NPS must to be added to the Trusted Root Certificate Store of the client. This can be done manually, via Group Policy in Active Directory, or by adding Certificate Services Web Enrollment to the NPS server along with an open SSID to allow clients to reach [https://192.168.0.1/certsrv](https://192.168.0.1/certsrv) to download/install the certificate to the Trusted Root store.

3. Click “Configure...” and make sure that “Automatically use my Windows logon name and password” is not selected. This is also a main source of failure for clients as EAP will try to use the logon name/password of the local machine which is not the same as the users Active Directory credentials.
Figure 19
FAC RADIUS Accounting to SSO Verification and Troubleshooting

1. This is an example of an Android mobile connecting to an WPA2 Enterprise SSID. The first task is to confirm with a packet sniffer that the FGT is connecting to NPS, and that NPS is connecting to FAC.

   FGTvm-home # diag sniffer packet any 'port 1812 or port 1813' 4 50
   interfaces=[any]
   filters=[port 1812 or port 1813]
   4.133392 port1 out 192.168.0.1.1029 -> 192.168.10.4.1813: udp 257 <--- FGT to NPS
   4.134308 port1 in 192.168.10.4.61096 -> 10.0.20.2.1813: udp 267 <--- NPS to FAC
   4.134326 port4 out 192.168.10.4.61096 -> 10.0.20.2.1813: udp 267
   4.135517 port4 in 10.0.20.2.1813 -> 192.168.10.4.61096: udp 20
   4.135524 port1 out 10.0.20.2.1813 -> 192.168.10.4.61096: udp 20
   20.807236 port1 out 192.168.0.1.1031 -> 192.168.10.4.1812: udp 245
   21.020201 port1 in 192.168.10.4.1812 -> 192.168.0.1.1031: udp 44
   25.001154 port1 out 192.168.0.1.1030 -> 192.168.10.4.1812: udp 175
   25.508790 port1 in 192.168.10.4.1812 -> 192.168.0.1.1030: udp 90

2. Wireshark conversion of step 1 showing successful MS-CHAPv2 via EAP tunnel from FGT to NPS. The NPS in this example is confirming a successful authentication.

   Figure 20
3. Wireshark conversion of step 1 showing RADIUS Accounting from FGT to NPS. The FGT is not only forwarding port 1812 to NPS, but it’s also initiating traffic on port 1813 to inform NPS of the Framed-IP-Address. If there are problems at this stage, ensure your FGT source-ip matches what the NPS expects, see to page 13 for reference. Notice the last line under ‘Attribute Value Pairs --> ‘Called-Station-Id’, that is the SSID and MAC address from the FGT which is used in NPS Connection and Network Policies.

![Wireshark screenshot](image)

Figure 21
4. Wireshark conversion of step 1 showing RADIUS Accounting from NPS to FAC. It includes the mandatory AVPs as described on page 10. When the FGT is providing DHCP services for wireless clients it will send Framed-IP-Address. If the FGT is a relay for DHCP, then the other DHCP server needs to provide this or the Framed-IP-Address will be missing and the FAC will discard the RADIUS Accounting packets.

![Wireshark capture showing RADIUS Accounting](image)

Figure 22
5. The same information from step 1 can also be confirmed in the NPS Security Log. The most common error at this point is Connection Policy or Network Policy ‘not matched’. If that happens, there is conflicting or missing information being received by NPS from the FGT. Adjust or correct the NPS policies as required.

![Event Viewer](image)

**Figure 23**

<table>
<thead>
<tr>
<th>Security</th>
<th>Number of events: 1,677</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keywords</td>
<td>Date and Time</td>
</tr>
<tr>
<td>Audit Success</td>
<td>10/12/2015 7:40:47 PM</td>
</tr>
<tr>
<td>Audit Success</td>
<td>10/12/2015 7:40:47 PM</td>
</tr>
<tr>
<td>Audit Success</td>
<td>10/12/2015 7:40:47 PM</td>
</tr>
<tr>
<td>Audit Success</td>
<td>10/12/2015 7:40:47 PM</td>
</tr>
</tbody>
</table>

**Event Viewer (Local)**

<table>
<thead>
<tr>
<th>Event View</th>
<th>XML View</th>
</tr>
</thead>
<tbody>
<tr>
<td>NASPortType</td>
<td>Wireless - IEEE 802.11</td>
</tr>
<tr>
<td>NASPort</td>
<td>0</td>
</tr>
<tr>
<td>ClientName</td>
<td>FGTvm5.2</td>
</tr>
<tr>
<td>ClientIPAddress</td>
<td>192.168.0.1</td>
</tr>
<tr>
<td>ProxyPolicyName</td>
<td>FGT Connection Policy (ssid ftnt_byod_fac)</td>
</tr>
<tr>
<td>NetworkPolicyName</td>
<td>FGTvm5.2 Network Policy [ssid ftnt_byod_fac]</td>
</tr>
<tr>
<td>AuthenticationProvider</td>
<td>Windows</td>
</tr>
<tr>
<td>AuthenticationServer</td>
<td>server-nps.fortinetlab.dyndns.org</td>
</tr>
<tr>
<td>AuthenticationType</td>
<td>PEAP</td>
</tr>
<tr>
<td>EAPType</td>
<td>Microsoft: Secured password (EAP-MSCHAP v2)</td>
</tr>
</tbody>
</table>
6. Run a 'tcpdump' on the FAC to confirm what it’s seeing. Any FAC RADIUS Accounting problems can also be viewed via gui by pointing a browser to https://10.0.20.2/debug and selecting RADIUS Accounting from the pull-down menu. An authentication may be successful, but if the user is not found in LDAP (or LDAP is not configured correctly), the login will be received but the record will be dropped due to a lack of group information.

> tcpdump port 1813 -vv

tcpdump: listening on port1, link-type EN10MB (Ethernet), capture size 262144 bytes

19:40:35.784818 IP (tos 0x0, ttl 125, id 21174, offset 0, flags [DF], proto UDP (17), length 301)
192.168.10.4.61096 > 10.0.20.2.radius-acct: [udp sum ok] RADIUS, length: 273

Accounting-Request (4), id: 0x33, Authenticator: 78d24a0730b85c2eb8ab841046ec85e
Acct-Session-Id Attribute (44), length: 19, Value: 5619045A-00000438
Acct-Status-Type Attribute (40), length: 6, Value: Start
Acct-Authentic Attribute (45), length: 6, Value: RADIUS
User-Name Attribute (1), length: 16, Value: mobile-android
  0x0000: 6d6f62696c652d616e64726f6964
NAS-IP-Address Attribute (4), length: 6, Value: 0.0.0.0
Framed-IP-Address Attribute (8), length: 6, Value: 10.0.202.6
NAS-Port Attribute (5), length: 6, Value: 0
Framed-IP-Address Attribute (8), length: 6, Value: 10.0.202.6

Connect-Info Attribute (77), length: 24, Value: CONNECT 11Mbps 802.11
Class Attribute (25), length: 46, Value: Z0...
Vendor-Specific Attribute (26), length: 14, Value: Vendor: Fortinet (12356)
Vendor Attribute: 23, Length: 6, Value: .fK.=x
Vendor-Specific Attribute (26), length: 24, Value: Vendor: Fortinet (12356)
Vendor Attribute: 24, Length: 16, Value: FAP21B3U13000175
Vendor-Specific Attribute (26), length: 12, Value: Vendor: Fortinet (12356)
Vendor Attribute: 25, Length: 4, Value: V.r.
Proxy-State Attribute (33), length: 10, Value: ....

7. Successful WPA2 Enterprise logons should ultimately appear in the FAC log as ‘RADIUS Accounting’ events under Monitor -> SSO -> SSO Sessions and display under ‘Source’ as ‘Radius Accounting’. Notice also, that the FAC has done an LDAP lookup for that use and all the groups will also display to the right of the ‘Source’ column.

![FortiAuthenticator](image1)

**Figure 24**

8. Those same events seen on the FAC as ‘RADIUS Accounting’ will appear on the FGT as ‘FSSO’ under User&Device -> Monitor -> Firewall but will display as ‘Method’ ‘FSSO’.

![FortiGate](image2)

**Figure 25**

9. Some additional FGT cli commands to help with troubleshooting are shown below:

```
FGTvm-home # diag firewall auth list
10.0.202.6, MOBILE-ANDROID
  type: fss0, id: 0, duration: 12, idled: 12
  server: FAC
  group_id: 3
  group_name: byod

FGTvm-home # diag debug app authd 8256
_FGTVm-home # _event_read[FAC]: received heartbeat 0
_event_read[ControllerAgent]: received heartbeat 125628
_process logon[FAC]: MOBILE-ANDROID(10.0.202.6) logged on with session id(0), port_range_sz=0
```

---

End of Document

Page 26 of 26