FortiAuthenticator - Cookbook

Version 5.5.0

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

August 1, 2019
FortiAuthenticator 5.5.0 Cookbook
23-550-570173-20190801

TABLE OF CONTENTS

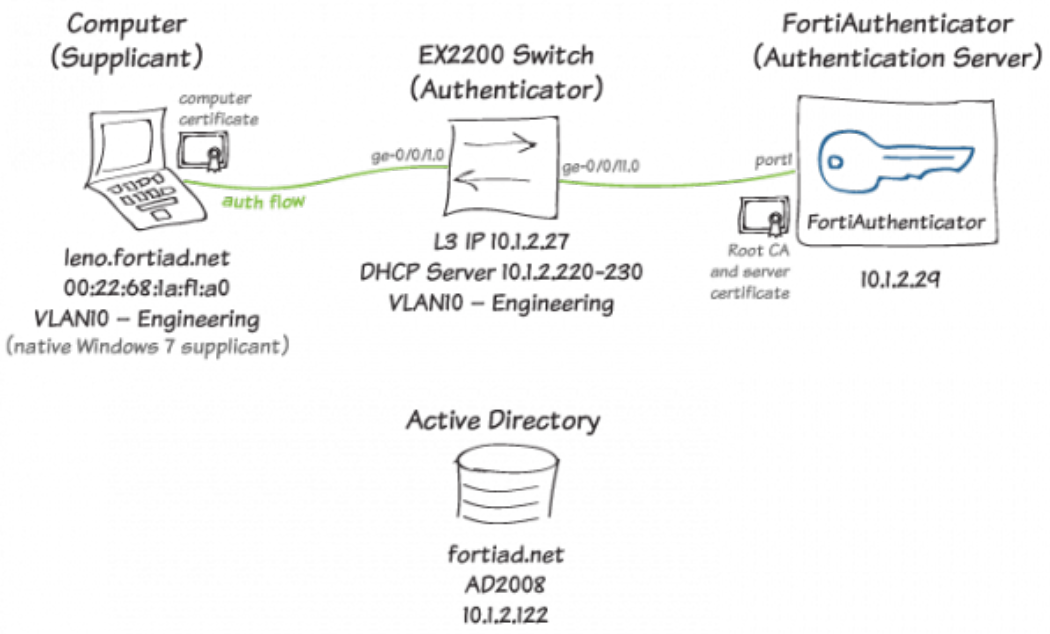
Change log

Date	Change Description
2019-08-01	Initial release.

EAP-TLS authentication

This section describes configuring EAP-TLS authentication with FortiAuthenticator.

Wired 802.1x EAP-TLS with computer authentication



In this recipe, you will configure and demonstrate wired 802.1x EAP-TLS with computer authentication.

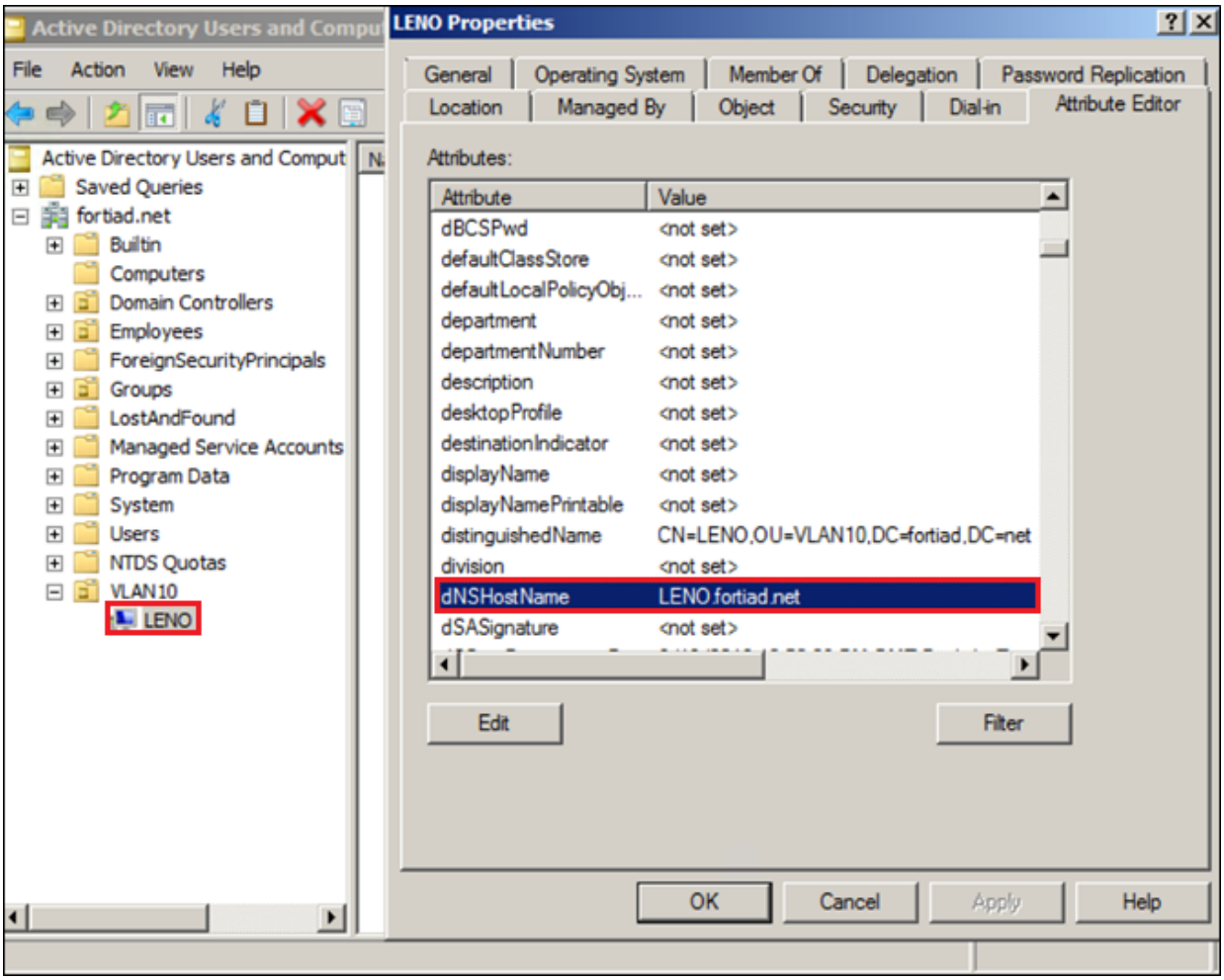
In the example, you will set up FortiAuthenticator as the Root CA and client certificate issuer. The FortiAuthenticator will authenticate user interaction using the domain computer and client certificate (no username or password).

The example includes a native Windows 7 supplicant and a 3rd-party switch (EX2200) to confirm cross-vendor interoperability. It also includes dynamic VLAN assignment on the switch as per the FortiAuthenticator RADIUS attributes.

Active Directory prerequisites

Key considerations:

- Computers must exist in AD Groups that correspond with their VLAN.
- Use the **dNSHostName** attribute for the username.



Configuring the certificates

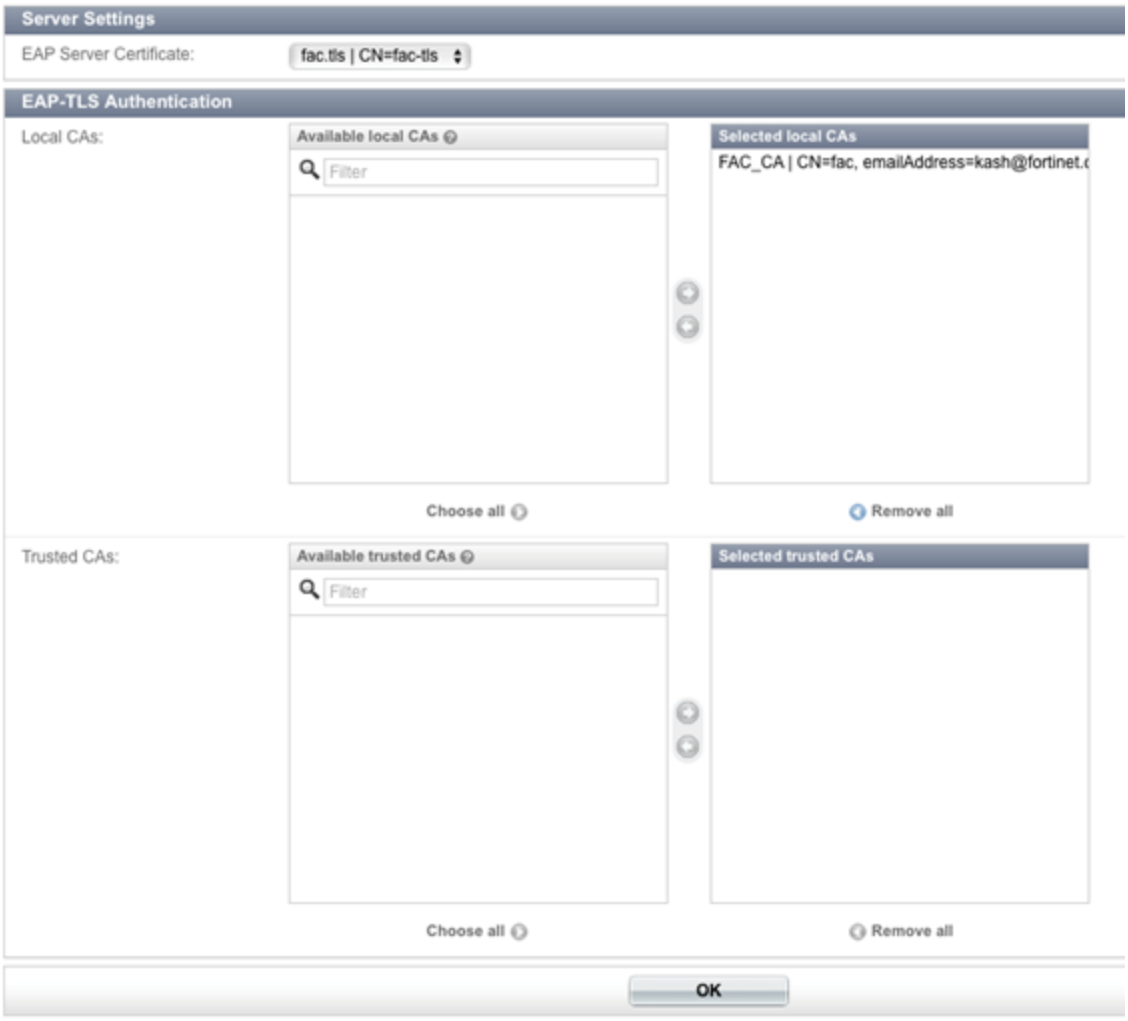
1. On the FortiAuthenticator, go to **Certificate Management > Certificate Authorities > Local CAs** and create a new root CA.

Certificate ID	Subject	Issuer	Status	CA Type
FAC_CA	CN=fac, emailAddress=kash@fortinet.com	CN=fac, emailAddress=kash@fortinet.com	Active	Root CA

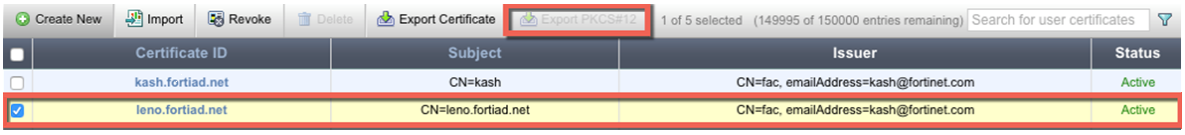
2. Go to **Certificate Management > End Entities > Local Services** and configure a certificate used for EAP-TLS.

Certificate ID	Subject	Issuer	Status
Firmware_Default	C=US, ST=California, L=Sunnyvale, O=Fortinet, OU=FortiAuthent...	Remote CA: C=US, ST=California, L=Sunnyvale, O=Fortinet, OU=C...	Active
fac.tls	CN=fac-tls	CN=fac, emailAddress=kash@fortinet.com	Active

3. Go to **Authentication > RADIUS Service > EAP** and set up the EAP configuration.
   If client certificates were not created by FortiAuthenticator, the 3rd-party server certificate would be uploaded on to FortiAuthenticator as a Trusted CA.
   In this example, FortiAuthenticator creates the client certificates.



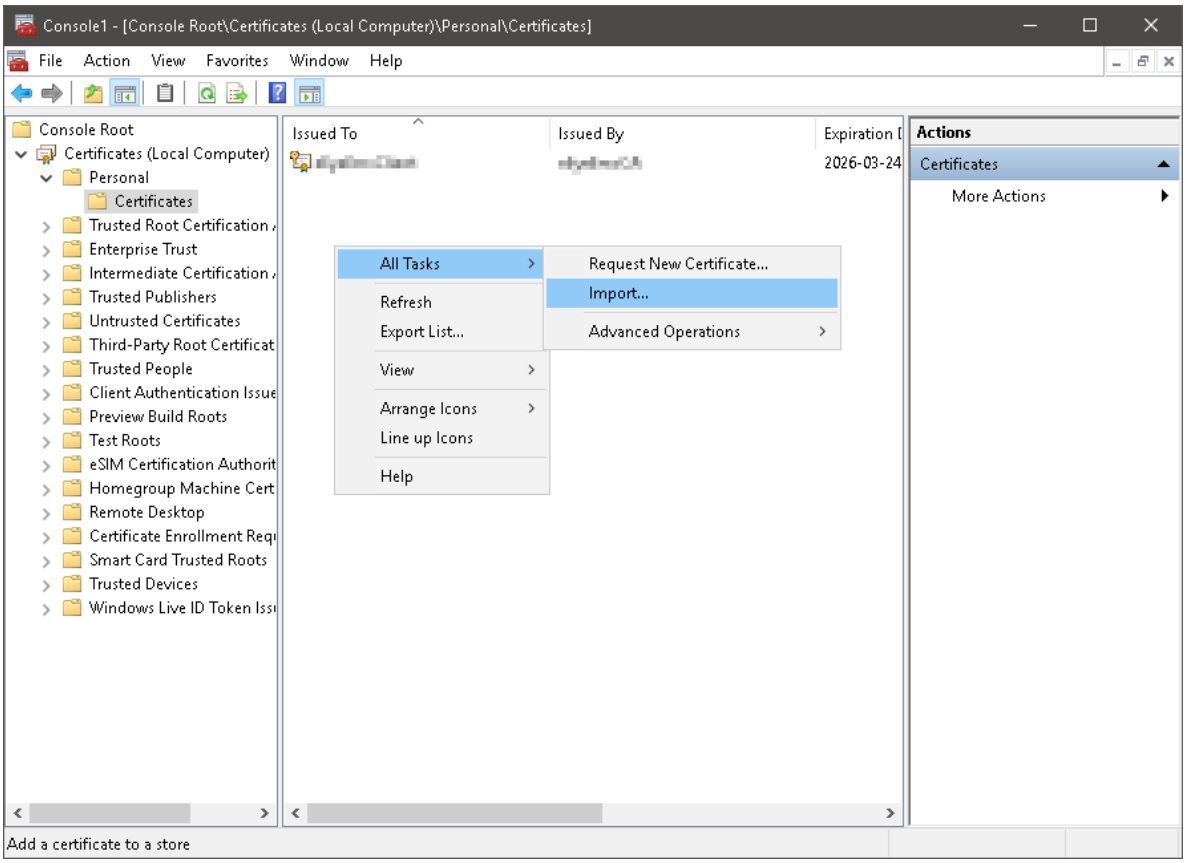
4. Go to **Certificate Management > End Entities > Users** and create a client certificate. The CN must match the full DNS name of the intended computer.
   Select **Export Key and Cert** (with a **Passphrase** to protect it) and download the PKCS#12 file.



   The client certificate can be pushed out using Group Policy Object (GPO). Otherwise, it can be imported manually.

Manually importing the client certificate - Windows 10

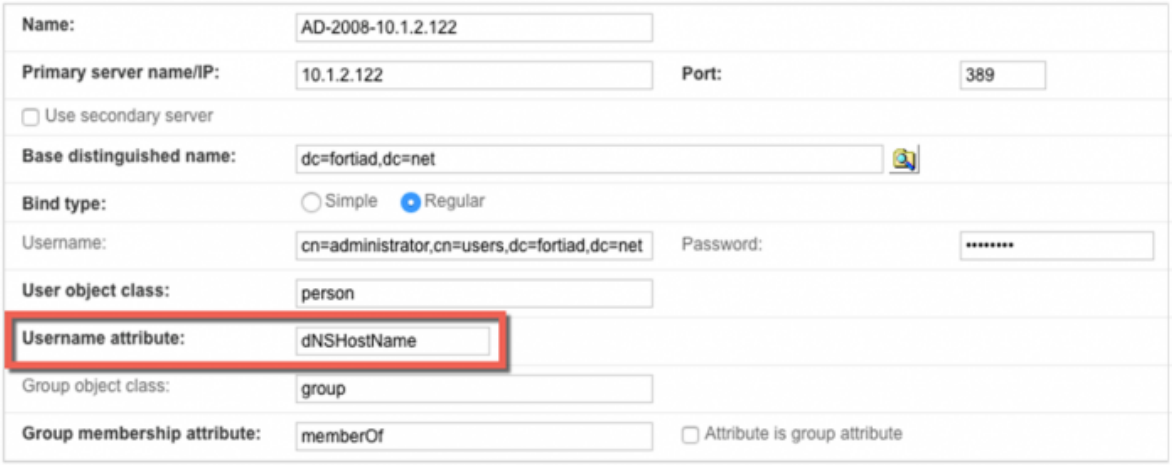
1. The manual import can be completed using Microsoft Management Console (MMC).
   Open Command Prompt and type *mmc* and hit **Enter** to open MMC.
   Go to File menu, click **Add/Remove Snap In**, and add the **Certificates** snap-in for **Local Computer**.
   Once added, right-click in the middle window and select **All Tasks > Import**.



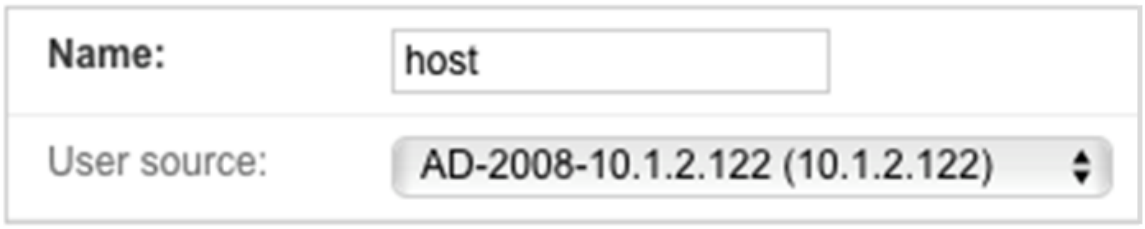
2. Once imported, the certificate should show up under **Local Computer** and not **Current User**.
   Export the FortiAuthenticator certificate and import it under **Trusted Root Certification Authorities**, again under **Certificates (Local Computer)**.

Configuring the FortiAuthenticator AD server

1. Go to **Authentication > Remote Auth. Servers > LDAP** and create a new AD server.
   Ensure that the **Username attribute** matches the entry in the AD configuration from earlier.

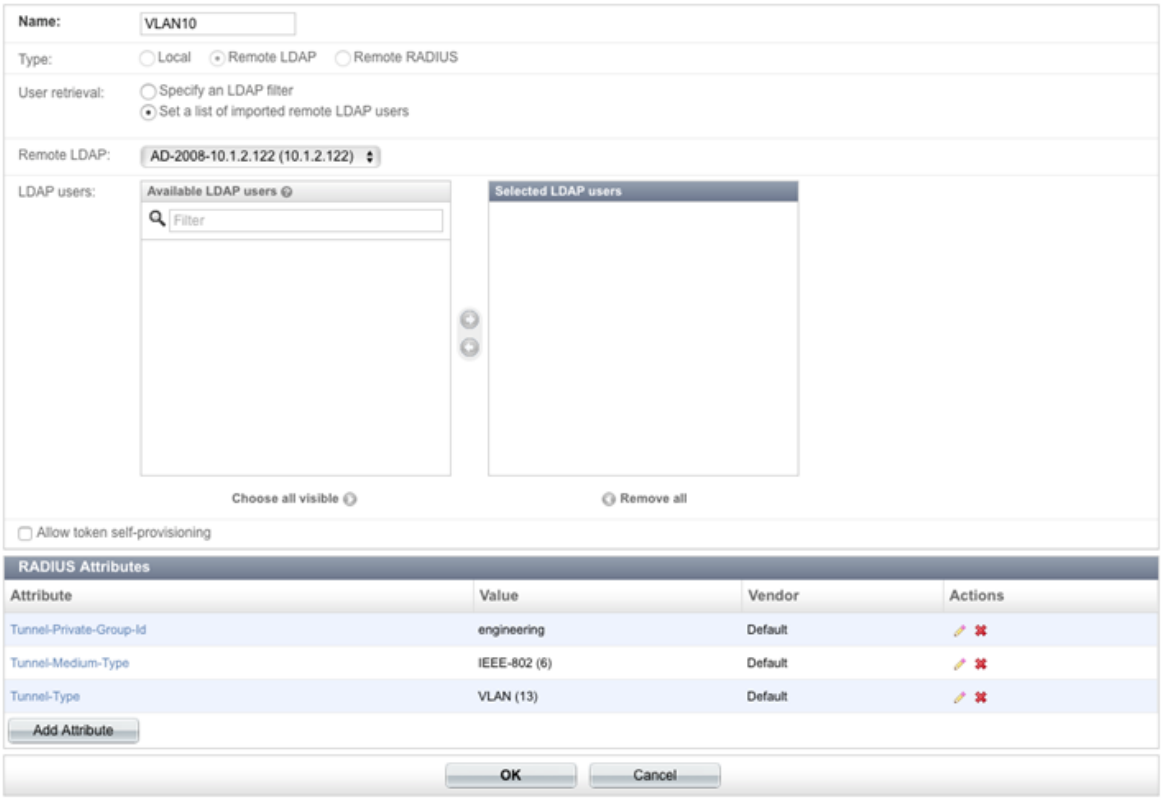


2. Go to **Authentication > User Management > Realms** and create a new realm for these users.



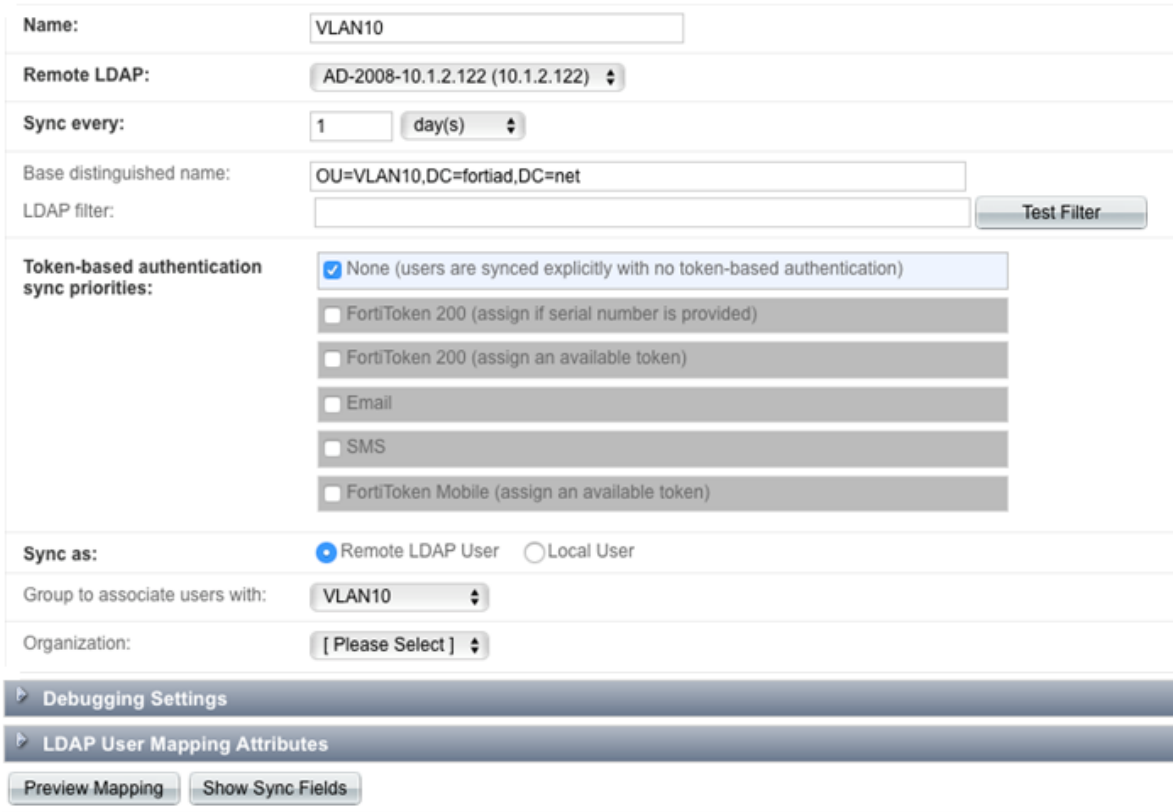
Configuring the user group

1. Go to **Authentication > User Management > User Groups** and create a new user group with the RADIUS attribute shown.
   Note that RADIUS attributes can only be added after the group has been created.



Configuring remote user sync rules

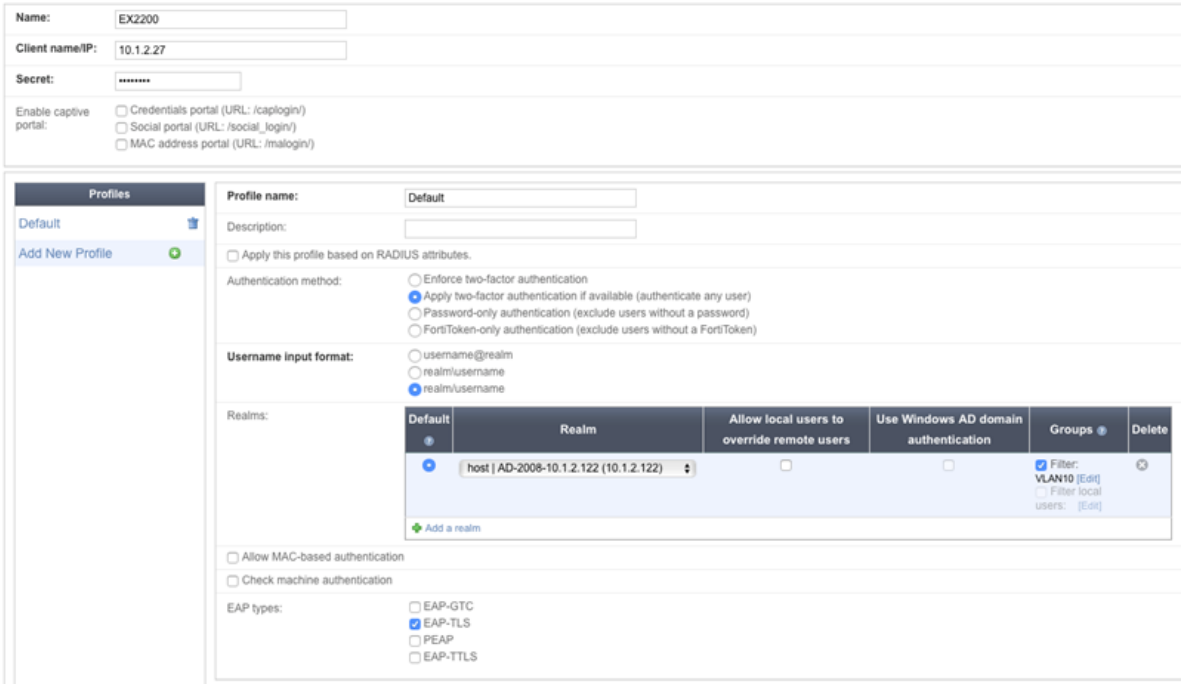
1. Go to **Authentication > User Management > Remote User Sync Rules** and configure a new remote LDAP user synchronization rule.



2. Go to **Authentication > User Management > Remote Users** and check to see if the sync rule worked.

Configuring the FortiAuthenticator RADIUS client

1. Go to **Authentication > RADIUS Service > Clients** and create a RADIUS client to bring the configuration together on the FortiAuthenticator.



Configuring the switch

1. The switch configuration provided below is intended for demonstration only. Your switch configuration is likely to differ significantly.

```
set system services dhcp pool 10.1.2.0/24 address-range low 10.1.2.220
set system services dhcp pool 10.1.2.0/24 address-range high 10.1.2.230
set system services dhcp pool 10.1.2.0/24 domain-name fortiad.net
set system services dhcp pool 10.1.2.0/24 name-server 10.1.2.122
set system services dhcp pool 10.1.2.0/24 router 10.1.2.1
set system services dhcp pool 10.1.2.0/24 server-identifier 10.1.2.27
set interfaces ge-0/0/1 unit 0 family ethernet-switching #windows 7 machine port, no
     VLAN assigned, will be allocated dynamically
set interfaces ge-0/0/11 unit 0 family ethernet-switching vlan members engineering
     #interface used to communicate with FortiAuthenticator
set interfaces me0 unit 0 family inet address 10.1.1.1/24
set interfaces vlan unit 10 family inet address 10.1.2.27/24
set protocols dot1x authenticator authentication-profile-name profile1
set protocols dot1x authenticator interface ge-0/0/1.0 supplicant single #802.1x
     configuration requiring supplicant
set access radius-server 10.1.2.29 secret "$9$kmfzIRSlvLhSLNVYZGk.Pf39"
set access profile profile1 authentication-order radius
set access profile profile1 radius authentication-server 10.1.2.29
set vlans engineering vlan-id 10
set vlans engineering l3-interface vlan.10
```

Results

The authentication flow should initiate as soon as the wired computer starts up (while connected to the domain).

1. Using `tcpdump`, FortiAuthenticator shows receipt of an Incoming Authentication Request (`tcpdump host 10.1.2.27 -nnvvXs`):

```
02:18:48.572998 IP (tos 0x0, ttl 64, id 32483, offset 0, flags [none], proto UDP
      (17), length 203)
   10.1.2.27.60114 > 10.1.2.29.1812: [udp sum ok] RADIUS. length: 175
      Access-Request (1), id: 0x4d, Authenticator: 27e45f0edbfa7026318d583ccf915776
         User-Name Attribute (11. length: 23. Value: host/leno.fortiad.net
            0x0000: 686f 7374 2f6c 656e 6f2e 666f 7274 6961
            0x0010: 642e 6e65 74
         NAS-Port Attribute (5), length: 6, Value: 71
            0x0000: 0000 0047
         EAP-Message Attribute (79), length: 28, Value: .
            0x0000: 0200 001a 0168 6f73 742f 6c65 6e6f 2e66
            0x0010: 6f72 7469 6164 2e6e 6574
         Message-Authenticator Attribute (80), length: 18, Value: ...0S2 ....... .M
            0x0000: b60f 874f 5332 c9a7 e2f5 d90e 8c20 e64d
         Acct-Session-Id Attribute (44), length: 24, Value: 802.1x81fa00370003dd64
            0x0000: 384f 322e 3178 3831 6661 3030 3337 3030
            0x0010: 3033 6464 3634
         NAS-Port-Id Attribute (87), length: 12, Value: ge-0/0/1.0
            0x0000: 6765 2d30 2f30 2f31 2e30
         Calling-Station-Id Attribute (31), length: 19, Value: 00-22-68-1a-ft-a0
            0x0000: 3030 2d32 322d 3638 2d31 612d 6631 2d61
            0x0010: 30
         Called-Station-Id Attribute (30), length: 19, Value: a8-d0-e5-b0-21-80
            0x0000: 6138 2d64 302d 6535 2d62 302d 3231 2d38
            0x0010: 30
         NAS-Port-Type Attribute (61), length: 6, Value: Ethernet
            0x0000: 0000 000f
```

2. Continuing with `tcpdump`, Access-Challenge is issued from FortiAuthenticator to the Switch:

```
02:18:48.578465 IP (tos 0x0, ttl 64, id 29725, offset 0, flags [none], proto UDP
      (17), length 108)
   10.1.2.29.1812 > 10.1.2.27.60114: [bad udp cksum 0x18a3 -> 0x7f96!] RADIUS,
         length: 80
      Access-Challenge (11), id: 0x4d, Authenticator:
            8140836b0192a5ef12630d4d049d05e6
         EAP-Message Attribute (79), length: 24, Value: ..
            0x0000: 0101 0016 0410 bc6b 992d bbfc 141f 3bbl
            0x0010: 1908 2978 2030
         Message-Authenticator Attribute (80), length: 18, Value: .#...:&%N.z.7...
            0x0000: dc23 d299 Of3a 2625 4eed 7a9c 37d9 ef97
         State Attribute (24), length: 18, Value: ........ ...m.q.
            0x0000: c2lb 819c c2la 85b8 20c3 b2b7 6dla 71d6
```

3. Access-Accept message with RADIUS attributes are returned to the Switch:

```
02:18:48.919099 IP (tos Ox0, ttl 64, id 29732, offset 0, flags [none], proto UDP
      (17), length 236)
   10.1.2.29.1812 > 10.1.2.27.60114: [bad udp cksum 0x1923 -> Oxae5a!] RADIUS,
         length: 208
      Access-Accept (2), id: 0x54, Authenticator: 668c7cbb00d96161c278906918ce2291
         Vendor-Specific Attribute (26), length: 58, Value: Vendor: Microsoft (311)
            Vendor Attribute: 17, Length: 50, Value: .p<.6..A [y)..E).....Y..
                  (..P...Xd@..aB.k.
            0x0000: 0000 0137 1134 f270 3cbf 360b 1d41 f5e5
            0x0010: c87f e8eb b9e9 955b 7929 0915 4529 fa92
            0x0020: 8c02 Ofec 59a0 e528 889e 50b9 f506 5864
            0x0030: 4018 ff61 429a 6bb8
```

```
Vendor-Specific Attribute (26), length: 58, Value: Vendor: Microsoft (311)
   Vendor Attribute: 16, Length: 50, Value:
        ..G......Q..............x.=xA/......i.r..a.%R.^..
   0x0000: 0000 0137 1034 ff86 47fc 00f1 99d9 cc51
   0x0010: fc1f 1ae2 b9e3 00a7 1ec9 baf4 031d fa78
   0x0020: 8d3d 7841 2114 0313 a2e8 9e69 dc72 efed
   0x0030: 61b2 2552 995e fbf4
EAP-Message Attribute (79), length: 6, Value: ..
   0x0000: 0307 0004
Message-Authenticator Attribute (80), length: 18, Value: .8............30
   0x0000: 0438 c613 8719 caa2 eaf0 a106 ffb4 3330
User-Name Attribute (1), length: 23, Value: host/leno.fortiad.net
   0x0000: 686f 7374 2f6c 656e 6f2e 666f 7274 6961
   0x0010: 642e 6e65 74
Tunnel-Type Attribute (64), length: 6, Value: Tag[Unused] #13
   0x0000: 0000 000d
Tunnel-Medium-Type Attribute (65), length: 6, Value: Tag[Unused] 802
   0x0000: 0000 0006
Tunnel-Private-Group-ID Attribute (81), length: 13, Value: engineering
   0x0000: 656e 6769 6e65 6572 696e 67
```

4. Post-authentication DHCP transaction is picked up by FortiAuthenticator (tcpdump continued):

```
02:18:52.384838 IP (tos Ox0, ttl 1, id 32640, offset 0, flags [none], proto UDP
     (17), length 328)
   10.1.2.27.67 > 255.255.255.255.68: [udp sum ok] BOOTP/DHCP, Reply, length 300,
      xid Oxf79d54fa, Flags [Broadcast] (0x8000)
     Your-IP 10.1.2.224
     Client-Ethernet-Address 00:22:68:1a:fl:a0
     Vendor-rfc1048 Extensions
        Magic Cookie 0x63825363
        DHCP-Message Option 53, length 1: ACK
        Server-ID Option 54, length 4: 10.1.2.27
        Lease-Time Option 51, length 4: 86400
        Subnet-Mask Option 1, length 4: 255.255.255.0
        Default-Gateway Option 3, length 4: 10.1.2.1
        Domain-Name-Server Option 6, length 4: 10.1.2.122
        Domain-Name Option 15, length 11: "fortiad.net"
```

5. On the FortiAuthenticator, go to Logging > Log Access > Logs to verify the device authentication. The Debug Log (at `https://<fac-ip>/debug/radius`) should also confirm successful authentication.

Log Details	
Log Record Detail	
ID	1557
Timestamp	Mon Sep 26 02:18:48 2016
Level	information
Action	Authentication
Status	Success
NAS Name/IP	10.1.2.27
Message	802.1x authentication successful
User	host/leno.fortiad.net
Log Type	
Type Id	20420
Name	802.1x Authentication OK
Sub Category	Authentication
Category	Event
Description	802.1x authentication successful

The Switch CLI shows a successful dot1x session:

```
root# run show dotlx interface ge-0/0/1.0
802.1X Information:
Interface Role State MAC address User
ge-0/0/1.0 Authenticator Authenticated 00:22:68:1A:F1:A0 host/leno.fortiad.net
```

The Domain Computer interface is dynamically placed into the correct VLAN:

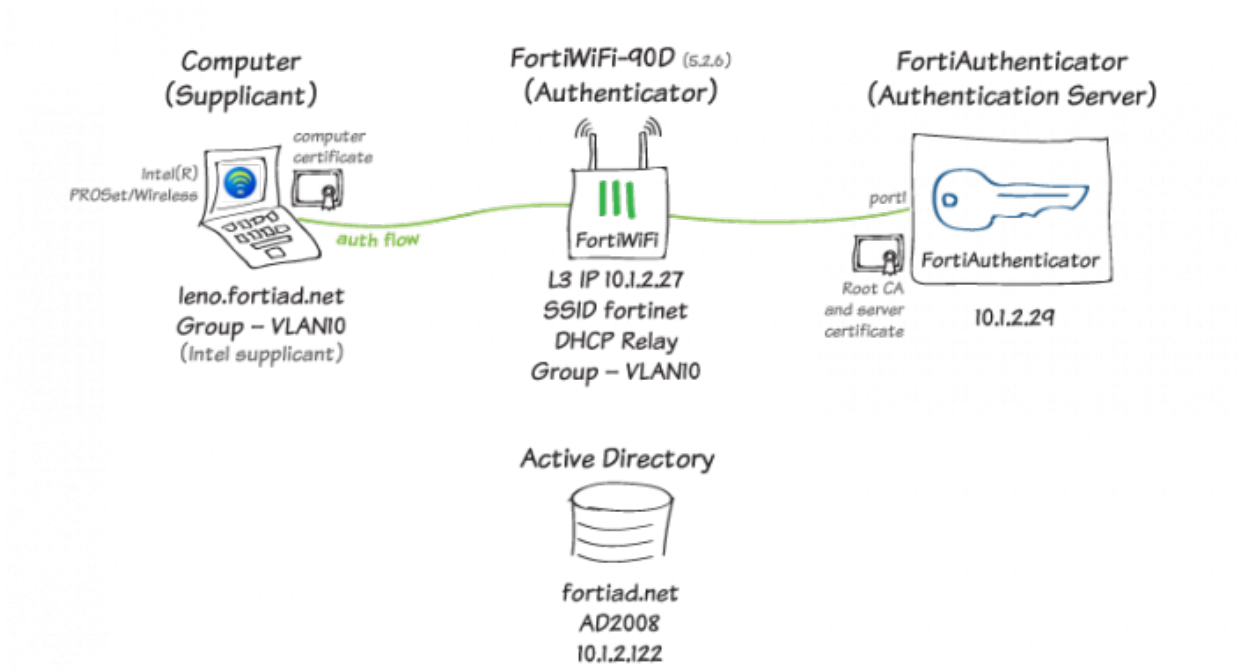
```
root# run show vlans
Name Tag Interfaces
default
     ge-0/0/0.0, ge-0/0/2.0, ge-0/0/3.0, ge-0/0/4.0, ge-0/0/5.0, ge-0/0/6.0, ge-
          0/0/7.0, ge-0/0/8.0, ge-0/0/9.0, ge-0/0/10.0,
engineering 10
     ge-0/0/1.0*, ge-0/0/11.0*
```

Additionally, the domain computer shows as available on the network:

```
root# run show arp interface vlan.10
MAC Address Address Name Interface Flags
00:0c:29:5b:90:68 10.1.2.29 10.1.2.29 vlan.10 none
98:b8:e3:a0:c6:1b 10.1.2.220 10.1.2.220 vlan.10 none
b8:78:2e:38:3e:28 10.1.2.222 10.1.2.222 vlan.10 none
00:22:68:1a:f1:a0 10.1.2.224 10.1.2.224 vlan.10 none
54:e4:3a:d5:16:a0 10.1.2.226 10.1.2.226 vian.10 none
Total entries: 5

{master:0}[edit]
root# run ping 10.1.2.224
```

```
PING 10.1.2.224 (10.1.2.224): 56 data bytes
54 bytes from 10.1.2.224: icmp_seq=0 ttl=128 time=4.651 ms
54 bytes from 10.1.2.224: icmp_seq-1 ttl-128 time-2.385 ms

--- 10.1.2.224 ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max/stddev = 2.385/3.518/4.651/1.133 ms
```

Wireless 802.1x EAP-TLS with computer authentication



In this recipe, you will configure and demonstrate wireless 802.1x EAP-TLS with computer authentication.

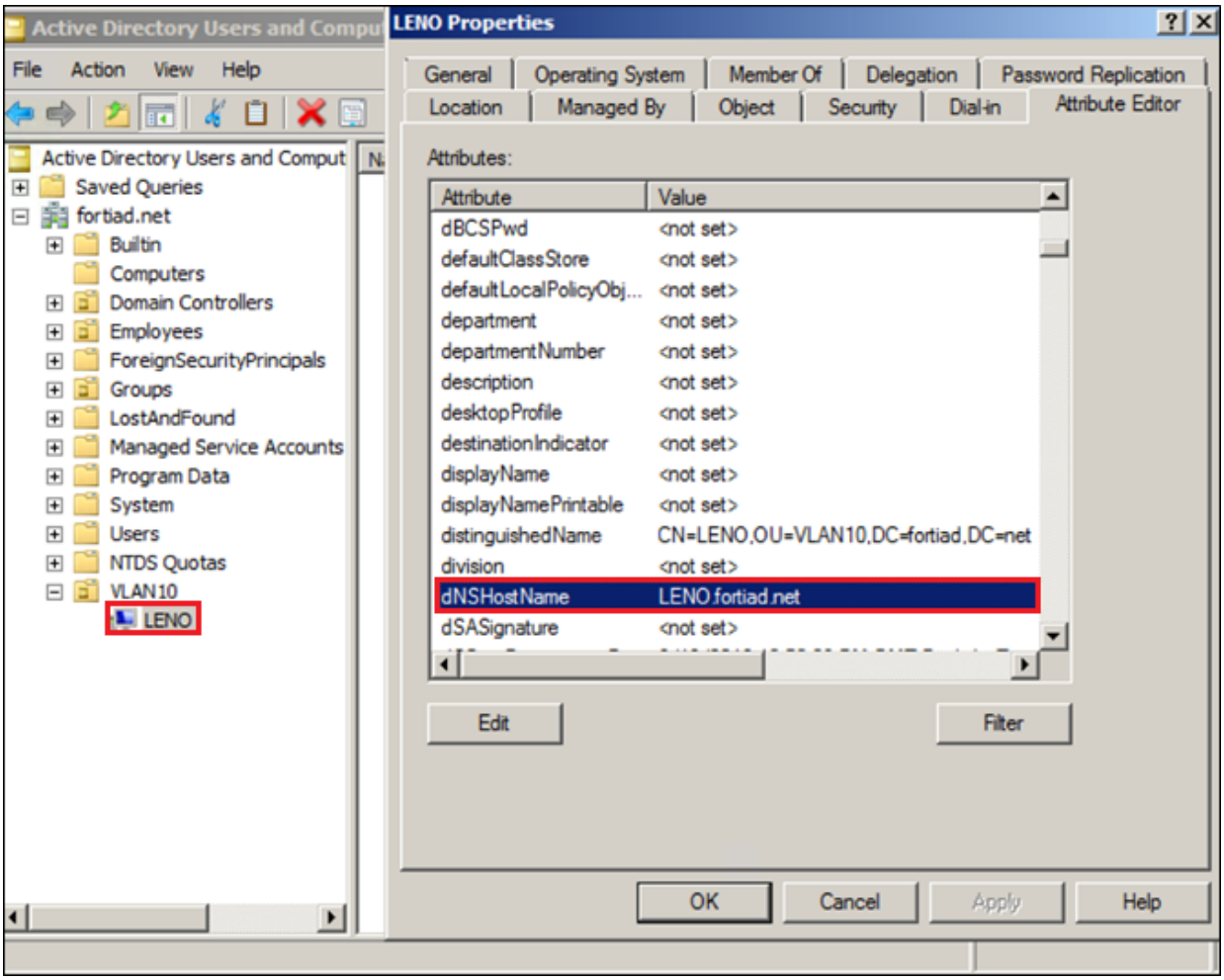
In the example, you will set up FortiAuthenticator as the Root CA and client certificate issuer. The FortiAuthenticator will authenticate without user interaction using the domain computer and client certificate (no username or password).

The example includes an Intel PROSet supplicant as well as a dynamically assigned group on a FortiWiFi using RADIUS attributes.

Active Directory prerequisites

Key considerations:

- Computers must exist in AD Groups that correspond with their VLAN.
- Use the **dNSHostName** attribute for the username.



Configuring the certificates

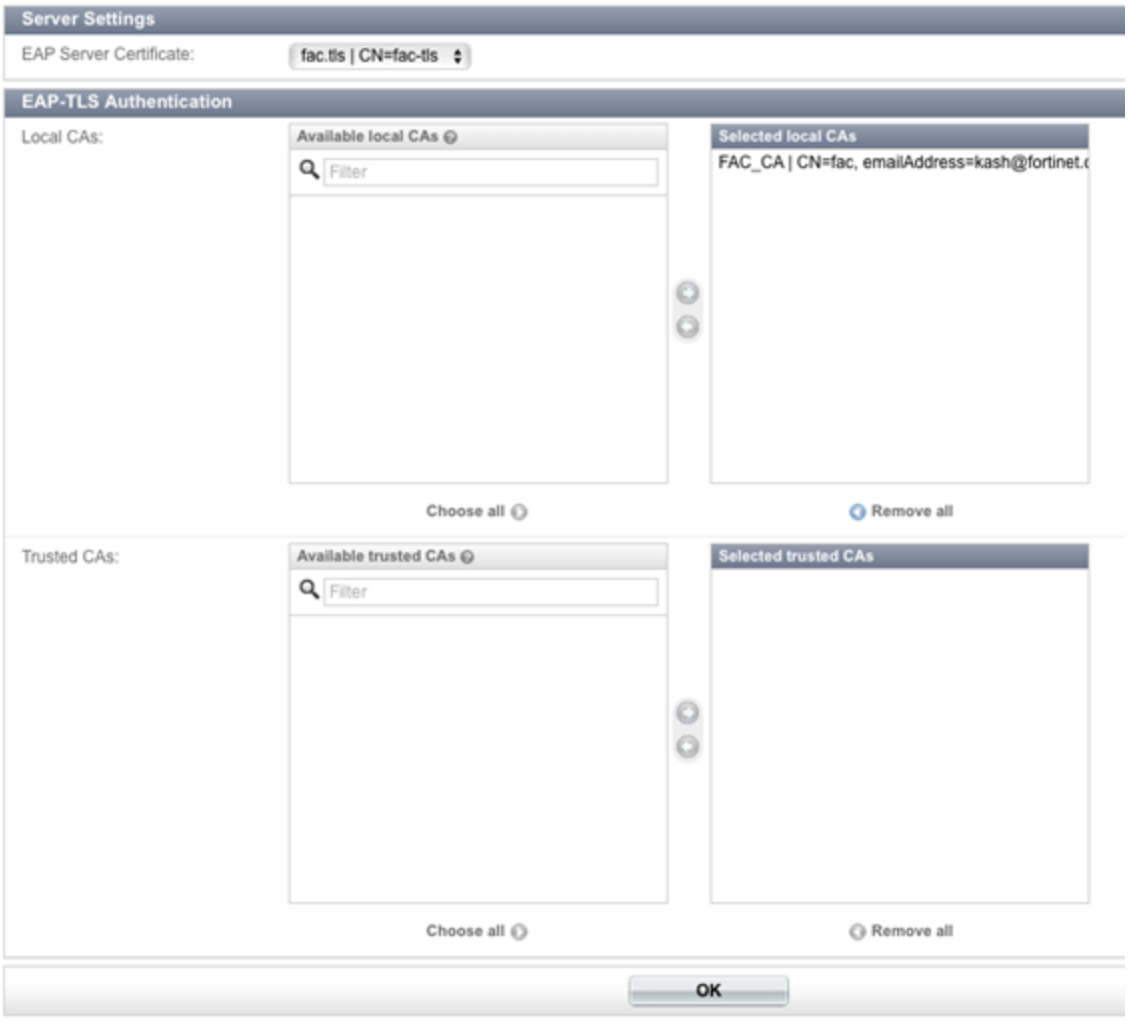
1. On the FortiAuthenticator, go to **Certificate Management > Certificate Authorities > Local CAs** and create a new root CA.

Certificate ID	Subject	Issuer	Status	CA Type
FAC_CA	CN=fac, emailAddress=kash@fortinet.com	CN=fac, emailAddress=kash@fortinet.com	Active	Root CA

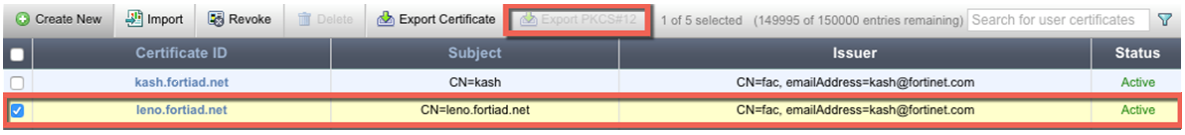
2. Go to **Certificate Management > End Entities > Local Services** and configure a certificate used for EAP-TLS.

Certificate ID	Subject	Issuer	Status
Firmware_Default	C=US, ST=California, L=Sunnyvale, O=Fortinet, OU=FortiAuthent...	Remote CA: C=US, ST=California, L=Sunnyvale, O=Fortinet, OU=C...	Active
fac.tls	CN=fac-tls	CN=fac, emailAddress=kash@fortinet.com	Active

3. Go to **Authentication > RADIUS Service > EAP** and set up the EAP configuration.
   If client certificates were not created by FortiAuthenticator, the 3rd-party server certificate would be uploaded on to FortiAuthenticator as a Trusted CA.
   In this example, FortiAuthenticator creates the client certificates.



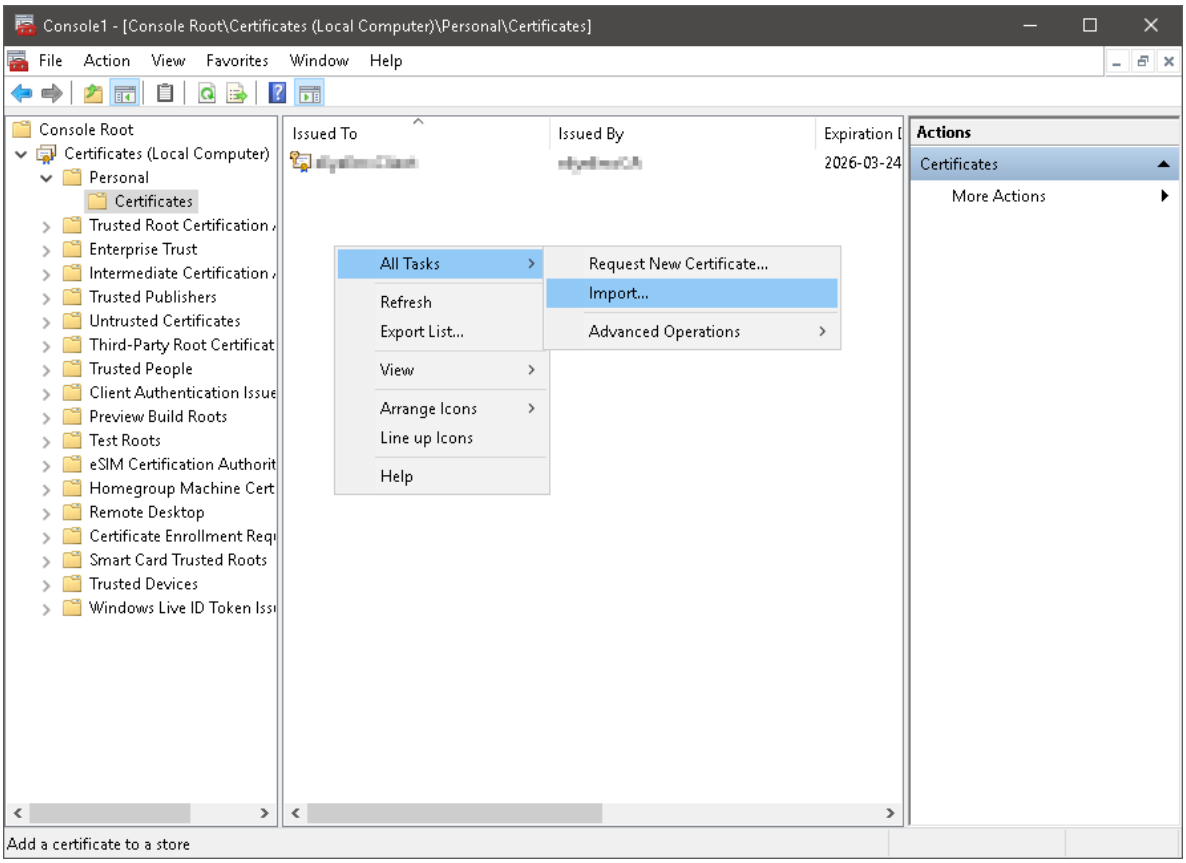
4. Go to **Certificate Management > End Entities > Users** and create a client certificate. The CN must match the full DNS name of the intended computer.
   Select **Export Key and Cert** (with a **Passphrase** to protect it) and download the PKCS#12 file.



   The client certificate can be pushed out using Group Policy Object (GPO). Otherwise, it can be imported manually.

Manually importing the client certificate - Windows 10

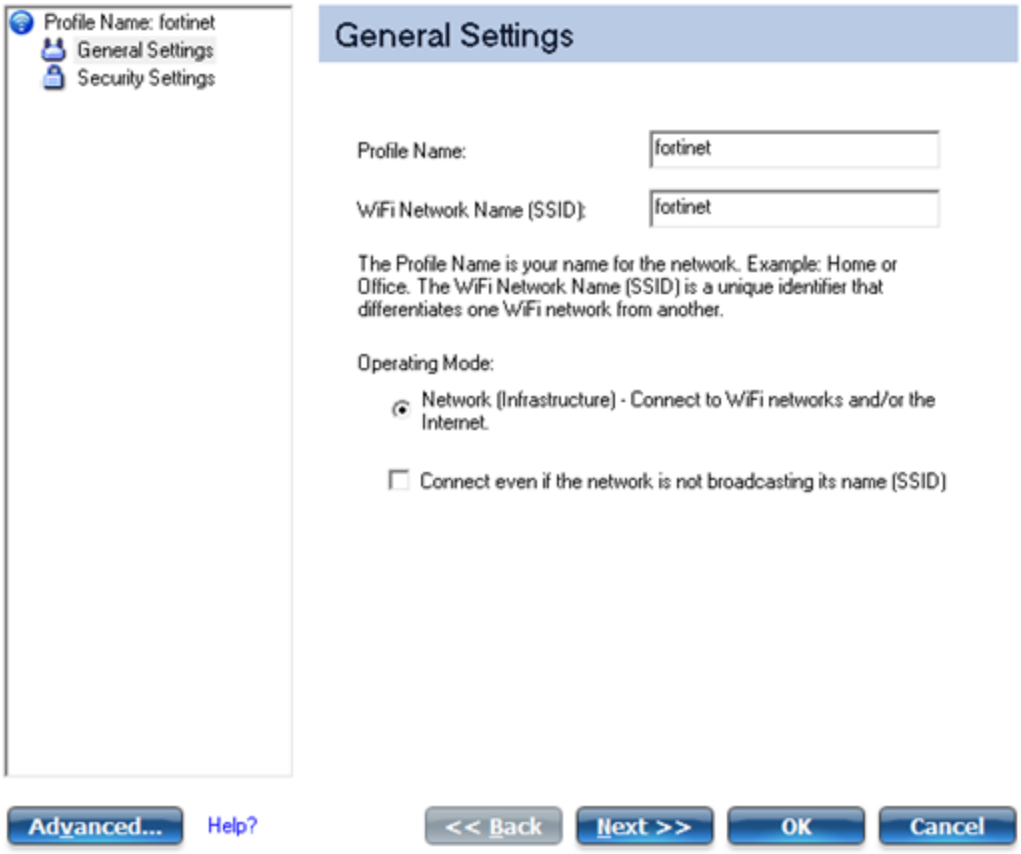
1. The manual import can be completed using Microsoft Management Console (MMC).
   Open Command Prompt and type *mmc* and hit **Enter** to open MMC.
   Go to File menu, click **Add/Remove Snap In**, and add the **Certificates** snap-in for **Local Computer**.
   Once added, right-click in the middle window and select **All Tasks > Import**.



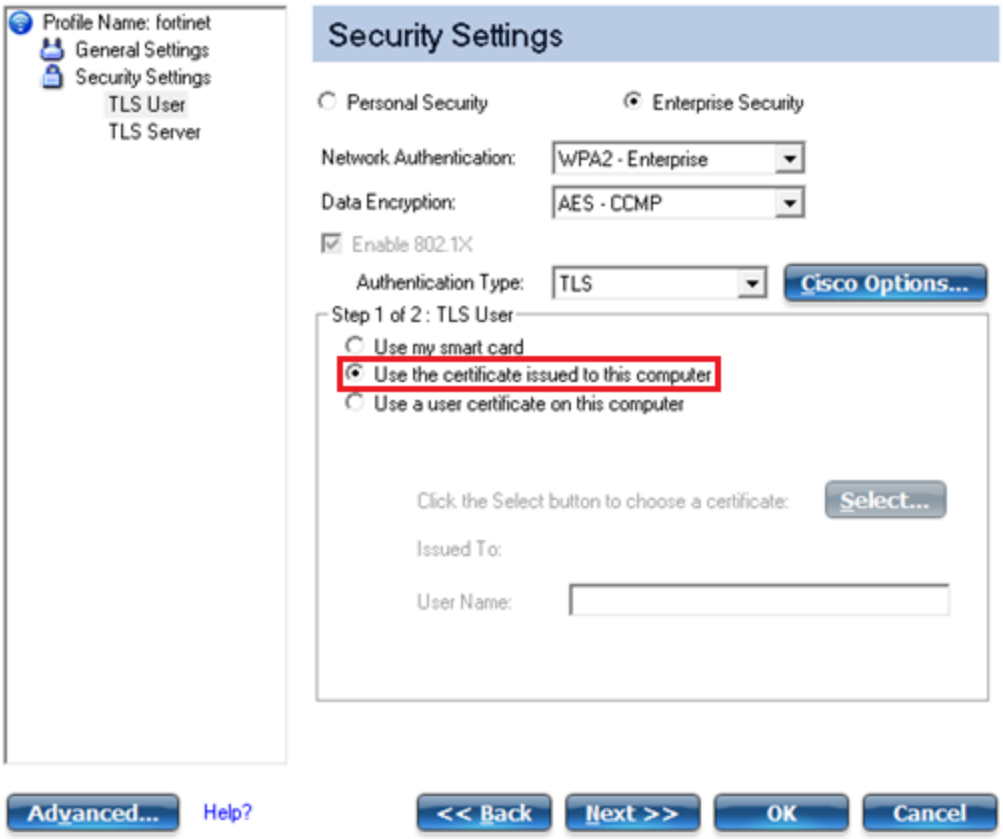
2. Once imported, the certificate should show up under **Local Computer** and not **Current User**.
   Export the FortiAuthenticator certificate and import it under **Trusted Root Certification Authorities**, again under **Certificates (Local Computer)**.

Configuring the Intel PROSet Supplicant - Windows 10

1. The supplicant will automatically select the certificate associated with the computer, based on the configuration shown.
   Under **General Settings**, set **Operating Mode** to **Network [Infrastructure] – Connect to WiFi networks and/or the Internet**.

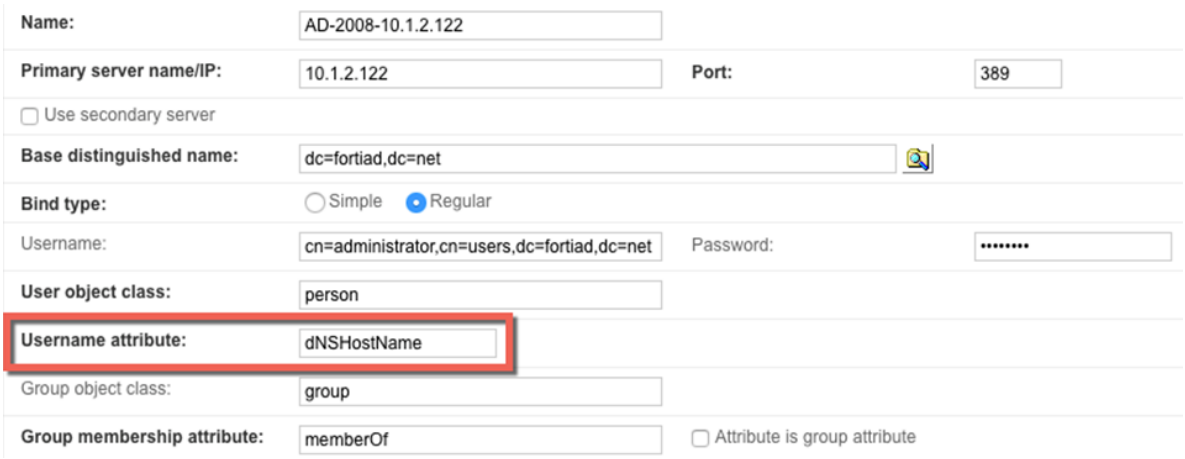


2. Under **Security Settings**, be sure to enable **Use the certificate issued to this computer**.
With this configuration, no user interaction is required for 802.1x EAP-TLS, on startup or attempting to connect to the WiFi, the authentication and authorization process will be transparent to the user.

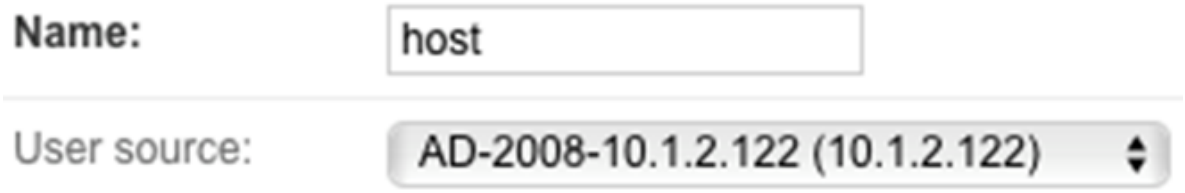


Configuring the FortiAuthenticator AD server

1. Go to **Authentication > Remote Auth. Servers > LDAP** and create a new AD server. Ensure that the **Username attribute** matches the entry in the AD configuration from earlier.

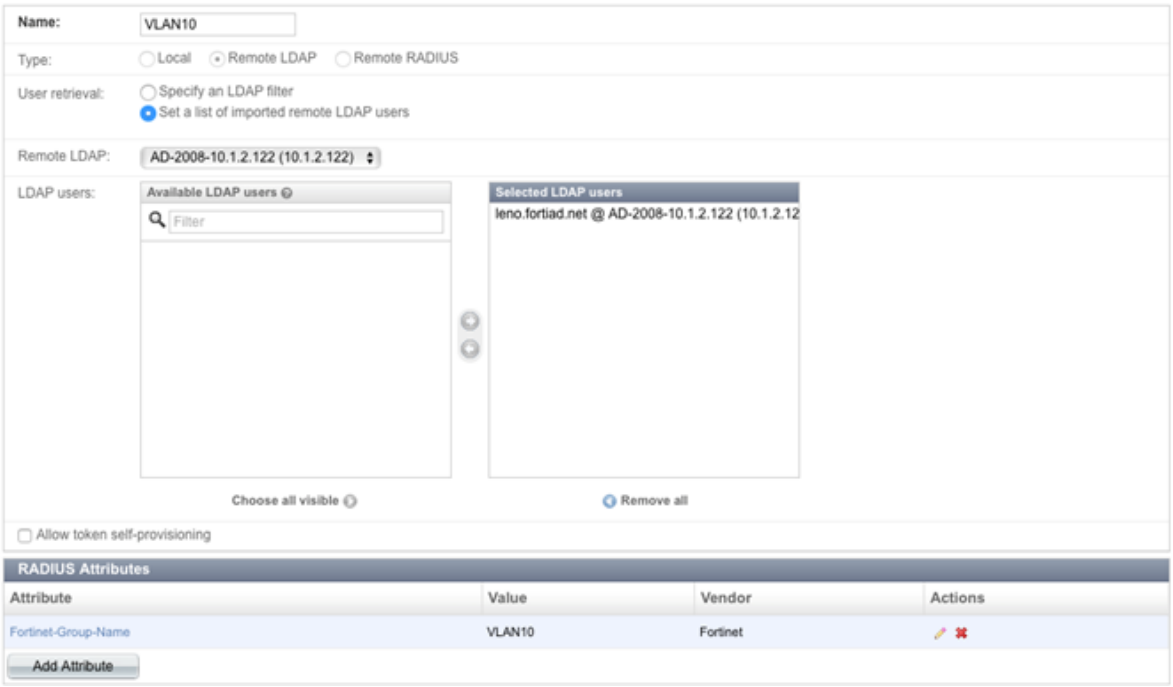


2. Go to **Authentication > User Management > Realms** and create a new realm for these users.



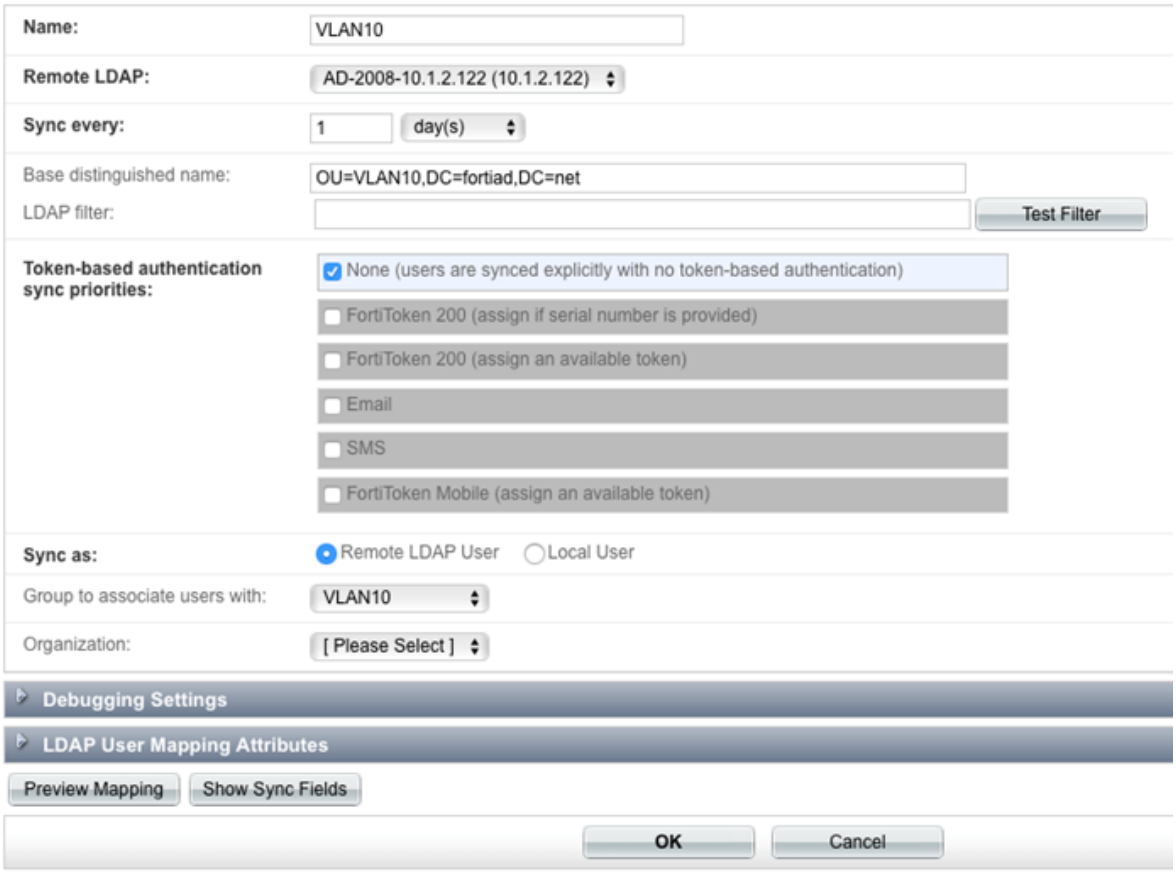
Configuring the user group

1. Go to **Authentication > User Management > User Groups** and create a new user group with the RADIUS attribute shown.
   Note that RADIUS attributes can only be added after the group has been created.

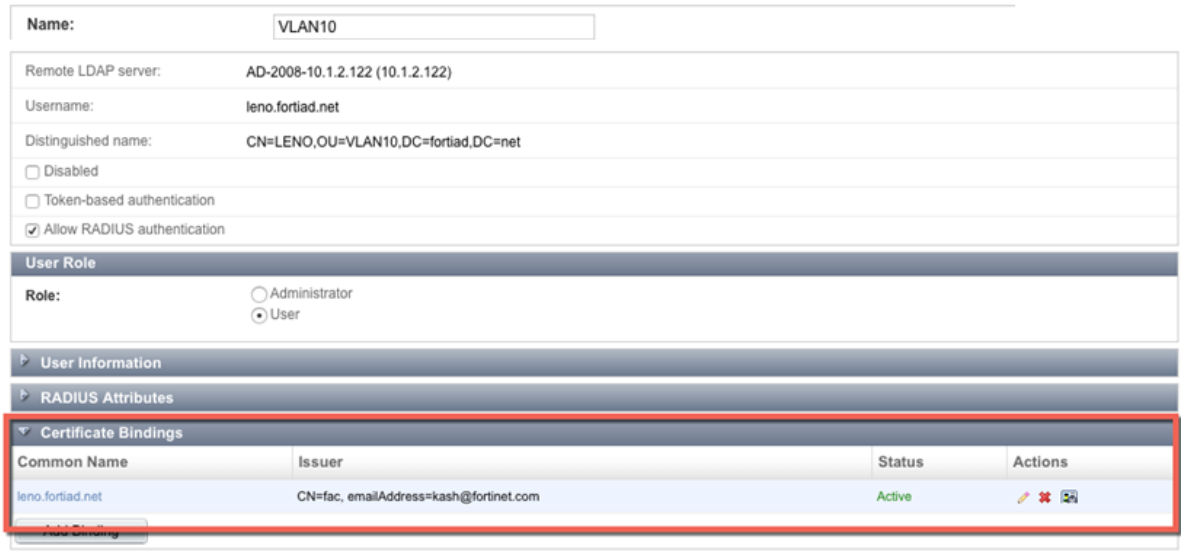


Configuring remote user sync rules

1. Go to **Authentication > User Management > Remote User Sync Rules** and configure a new remote LDAP user synchronization rule.

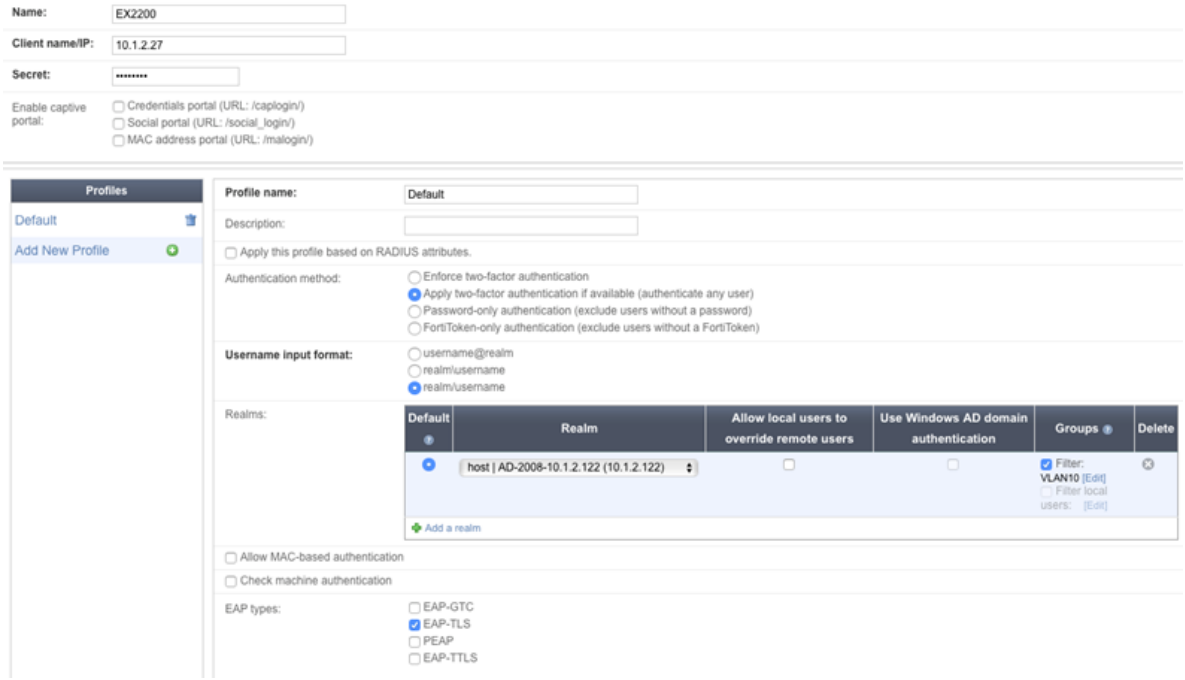


2. Then go to **Authentication > User Management > Remote Users** and check to see if the sync rule worked.



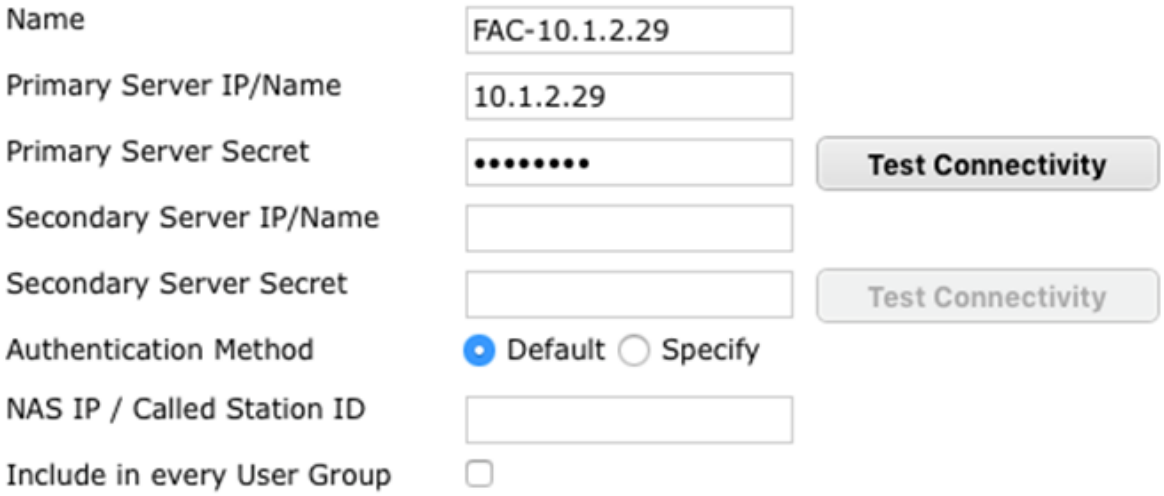
Configuring the FortiAuthenticator RADIUS client

1. Go to **Authentication > RADIUS Service > Clients** and create a RADIUS client to bring the configuration together on the FortiAuthenticator.

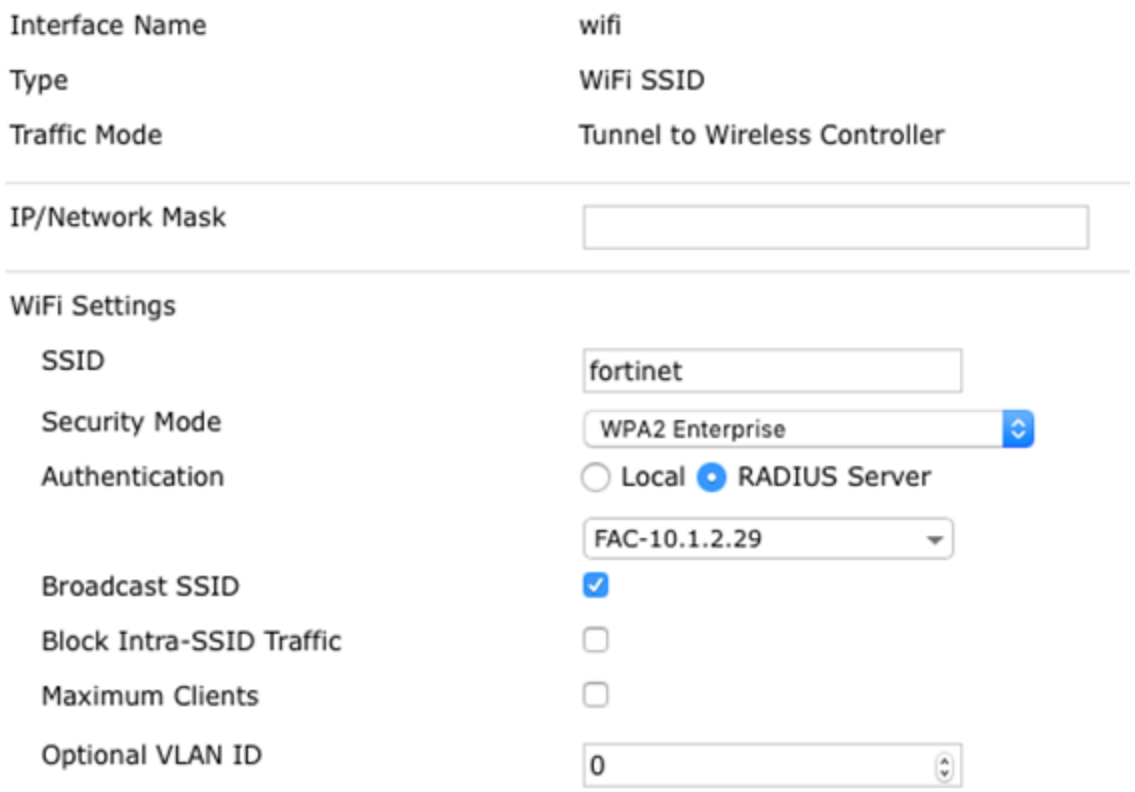


Configuring the FortiWiFi

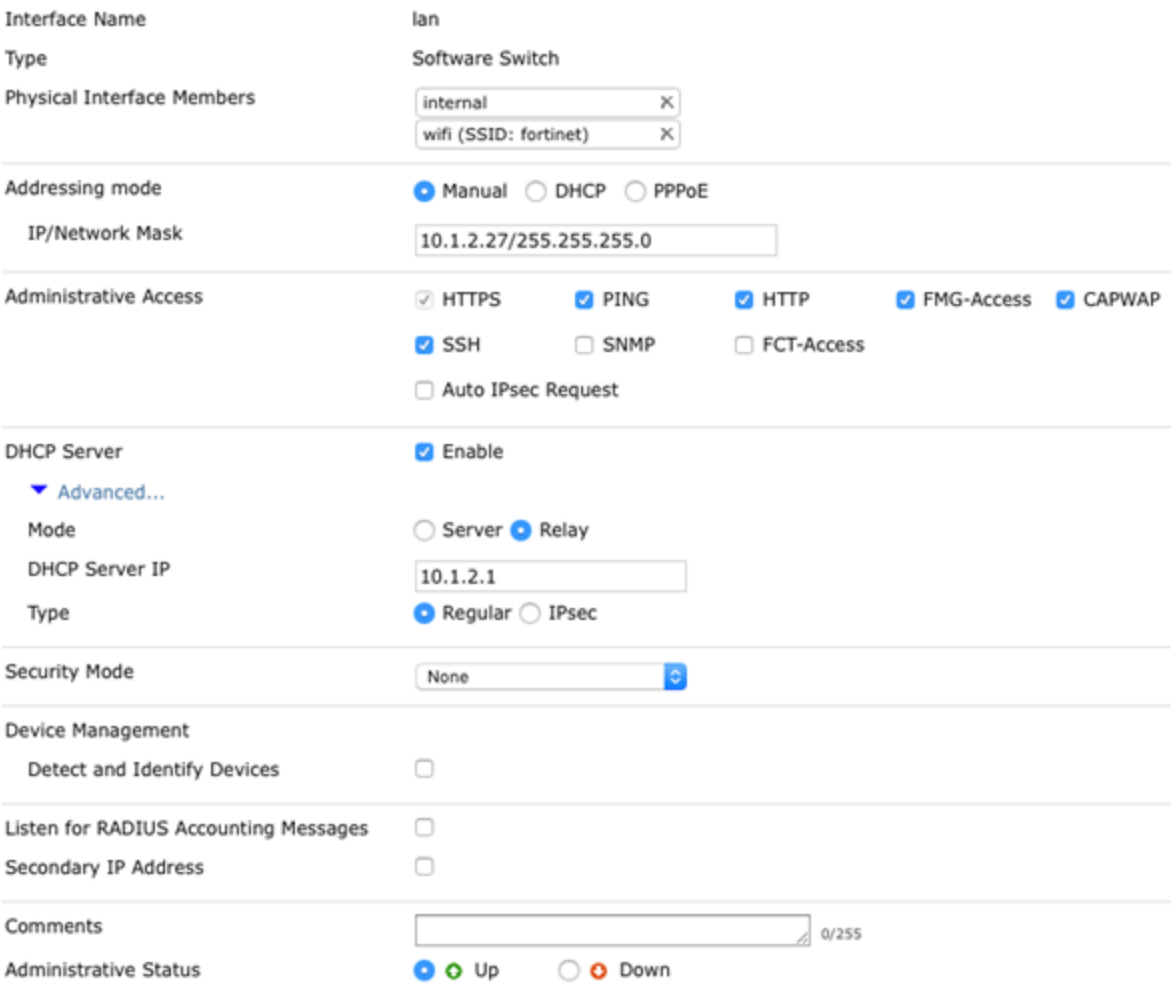
1. On the FortiWiFi, go to **User & Device > RADIUS Servers** and set the FortiAuthenticator as the RADIUS server for the FortiWiFi.



2. Go to **WiFi & Switch Controller > SSID** and configure the WiFi SSID interface.



3. Then go to **Network > Interfaces** and configure a software switch combining the physical and WiFi interfaces.



Results

The authentication flow should initiate as soon as the wired computer starts up (while connected to the domain).

1. Using `tcpdump`, FortiAuthenticator shows receipt of an Incoming Authentication Request (`tcpdump host 10.1.2.27 -nnvvXs`):

```
01:09:34.674298 IP (tos 0x0, ttl 64, id 40954, offset 0, flags [none], proto UDP
      (17), length 212)
   10.1.2.27.1025 > 10.1.2.29.1812: [udp sum ok] RADIUS, length: 184
      Access-Request (1), id: 0x76, Authenticator: 4b859401ddb6c0fb95261e99fc8ef66a
         User-Name Attribute (1), length: 23, Value: host/leno.fortiad.net
            0x0000: 686f 7374 2f6c 656e 6f2e 666f 7274 6961
            0x0010: 642e 6e65 74
         NAS-IP-Address Attribute (4), length: 6, Value: 0.0.0.0
            0x0000: 0000 0000
         NAS-Port Attribute (5), length: 6, Value: 0
            0x0000: 0000 0000
         Called-Station-Id Attribute (30), length: 28, Value: 88-DC-96-27-72-
               68:fortinet
```

```
            0x0000: 3838 2d44 432d 3936 2d32 372d 3732 2d36
            0x0010: 423a 666f 7274 696e 6574
         Calling-Station-Id Attribute (31), length: 19, Value: 6C-88-14-C6-3D-58
            0x0000: 3643 2d38 382d 3134 2d43 362d 3344 2d35
            0x0010: 38
         Framed-MTU Attribute (12), length: 6, Value: 1400
            0x0000: 0000 0578
         NAS-Port-Type Attribute (61), length: 6, Value: Wireless - IEEE 802.11
            0x0000: 0000 0013
         Connect-Info Attribute (77), length: 24, Value: CONNECT 11Mbps 802.11b
            0x0000: 434f 4e4e 4543 5420 3131 4d62 7073 2038
            0x0010: 3032 2e31 3162
```

2. Continuing with `tcpdump`, Access-Challenge is issued from FortiAuthenticator to the FortiWiFi:

```
01:09:34.679881 IP (tos Ox0, ttl 64, id 58896, offset 0, flags [none], proto UDP
      (17), length 108)
   10.1.2.29.1812 > 10.1.2.27.1025: [bad udp cksum 0xl8a3 -> 0xbe6al) RADIUS,
         length: 80
      Access-Challenge (11), id: 0x76, Authenticator:
            a4c016a41e6a0f46c17da49ff813bd6e
         EAP-Message Attribute (79), length: 24, Value: ..
            0x0000: 0101 0016 0410 f23e 13dd 795e 18fa SddS
            0x0010: 3e83 cb34 a99c
         Message-Authenticator Attribute (80), length: 18, Value:
            0x0000: eac9 2509 cbec 6895 804a deac 5de7 d6f8
         State Attribute (24), length: 18, value: *...* .......
            0x0000: 2af7 lbfd 2af6 lfb9 8db9 f1f8 20ad 9cd4
```

The next 14 messages are Challenge->Request EAP transactions between the FortiAuthenticator and the FortiWiFi.

3. Access-Accept message with RADIUS attributes are returned to the FortiWiFi:

```
01:09:36.517763 IP (tos Ox0, ttl 64, id 58903, offset 0, flags (none), proto UDP
      (17), length 225)
   10.1.2.29.1812 > 10.1.2.27.1025: (bad udp cksum 0x1918 0x1f60!) RADIUS, length:
         197
      Access-Accept (2), id: Ox7d, Authenticator: 989626b68773ac50c060d8306287984a
         Vendor-Specific Attribute (26), length: 58, Value: Vendor: Microsoft (311)
            Vendor Attribute: 17, Length: 50, Value: ?...e....NA=E.5.9..y........Q
                  ^R=i..!j .........
            0x0000: 0000 0137 1134 80e3 aefl 65e0 1383 c34e
            0x0010: 413d 4Sbd 350d 39be ac79 04b8 90fa 1551
            0x0020: a4b7 10d3 09b6 f902 5e52 3d69 b3b4 216a
            0x0030: b48f 0ef2 0c08 9cd0
         Vendor-Specific Attribute (26), length: 58, Value: Vendor: Microsoft (311)
            Vendor Attribute: 16, Length: 50, Value: z
            0x0000: 0000 0137 1034 8883 7a9b bllb 9488 f181
            0x0010: d179 29ba 7538 lleb 8311 3c22 1b62 9176
            0x0020: d0be f763 4617 670c d8ca 8659 7a14 dl2c
            0x0030: 8064 5955 942b ccla
         EAP-Message Attribute (79), length: 6, Value: ..
            0x0000: 0307 0004
         Message-Authenticator Attribute (80), length: 18, Value: ....>k....? ...(
            0x0000: 9aec 02c0 3e6b af8e defb 8020 e50b 0728
         User-Name Attribute (1), length: 23, Value: host/leno.fortiad.net
            0x0000: 686f 7374 2f6c 656e 6f2e 666f 7274 6961
            0x0010: 642e 6e65 74 Vendor-Specific Attribute (26), length: 14, Value:
                  Vendor: Fortinet (12356)
         Vendor Attribute: 1, Length: 6, Value: VLAN10
            0x0000: 0000 3044 0108 564c 414e 3130
```

4. Post-authentication DHCP transaction is picked up by FortiAuthenticator (`tcpdump` continued):

```
01:09:39.765661 IP (tos 0x0, ttl 64, id 15537, offset 0, flags [none], proto UDP
    (17), length 300)
  10.1.2.27.67 > 255.255.255.255.68: [udp sum ok] BOOTP/DHCP, Reply, length 272,
      hops 2, xid 0x5a6b3f9e, Flags [none] (0x0000)
    Client-IP 10.1.2.9
    Gateway-IP 10.1.2.27
    Client-Ethernet-Address 6c:88:14:c6:3d:58
    Vendor-rfc1048 Extensions
      Magic Cookie 0x63825363
      DHCP-Message Option 53, length 1: ACK
      Server-ID Option 54, length 4: 10.1.2.1
      Default-Gateway Option 3, length 4: 10.1.2.1
      Domain-Name-Server Option 6, length 8: 212.159.6.9,212.159.6.10
      Time-Zone Option 2, length 4: 3600
```

5. On the FortiAuthenticator, go to Logging > Log Access > Logs to verify the device authentication. The Debug Log (at `https://<fac-ip>/debug/radius`) should also confirm successful authentication.

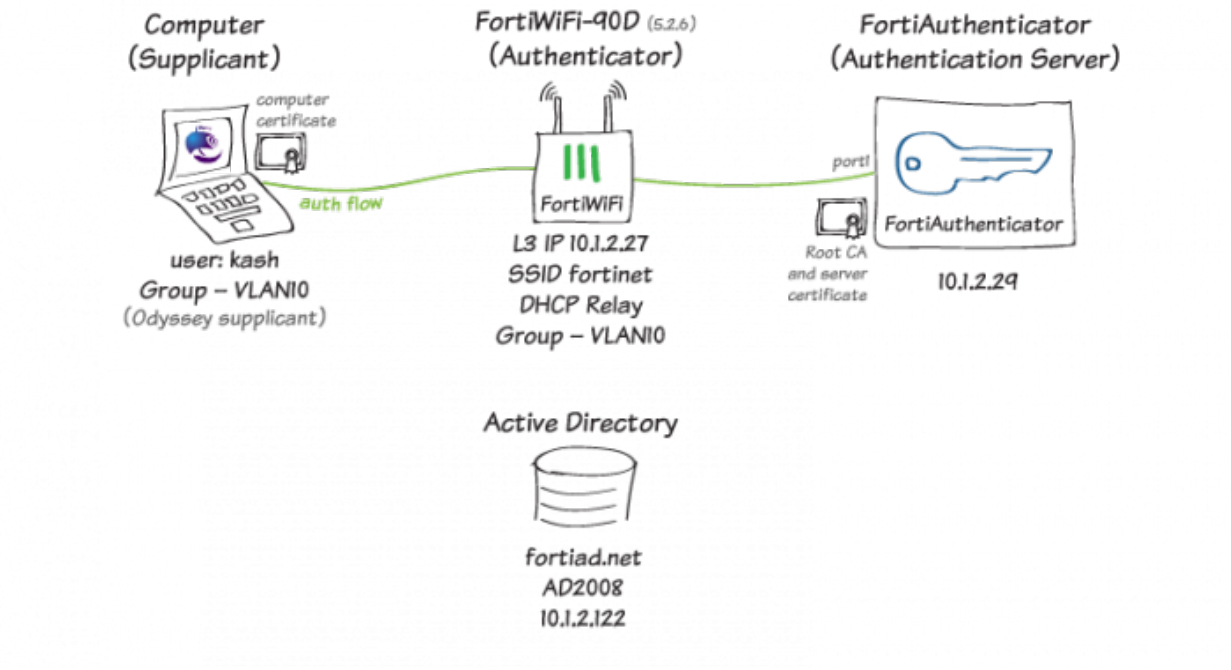
Log Details

Log Record Detail	
ID	1848
Timestamp	Tue Sep 27 01:09:36 2016
Level	information
Action	Authentication
Status	Success
NAS Name/IP	10.1.2.27
Message	802.1x authentication successful
User	host/leno.fortiad.net
Log Type	
Type Id	20420
Name	802.1x Authentication OK
Sub Category	Authentication
Category	Event
Description	802.1x authentication successful

6. On the FortiWifi, go to **WiFi & Switch Controller > Monitor > Client Monitor** and note that the Group is the RADIUS attribute sent from FortiAuthenticator. Any Firewall policy using that Group will now be enabled for the user.

SSID	FortiAP	User	Group	IP	Device	Channel	Bandwidth Tx/Rx	Signal Strength/Noise	Signal Strength
fortinet	Local WiFi Radio (1)	host/leno.fortiad.net	VLAN10	10.1.2.9	6c:88:14:c6:3d:58	11	0 bps	64 dB	

Wireless 802.1x EAP-TLS with user authentication



In this recipe, you will configure and demonstrate wireless 802.1x EAP-TLS with user authentication.

In the example, you will set up FortiAuthenticator as the Root CA and client certificate issuer.

The example includes an Odyssey supplicant as well as a dynamically assigned group on a FortiWiFi using RADIUS attributes.

Configuring the certificates

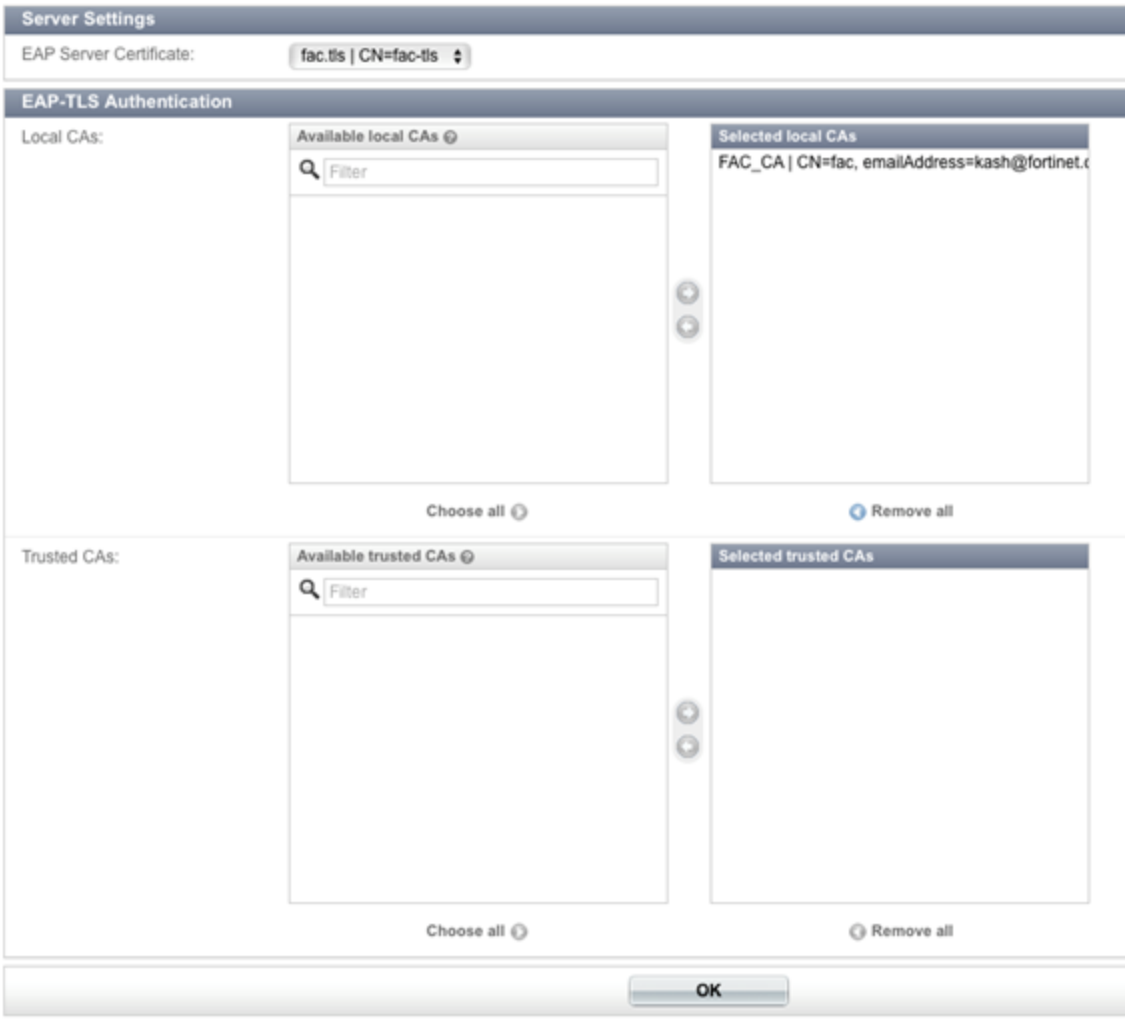
1. On the FortiAuthenticator, go to **Certificate Management > Certificate Authorities > Local CAs** and create a new root CA.

Certificate ID	Subject	Issuer	Status	CA Type
FAC_CA	CN=fac, emailAddress=kash@fortinet.com	CN=fac, emailAddress=kash@fortinet.com	Active	Root CA

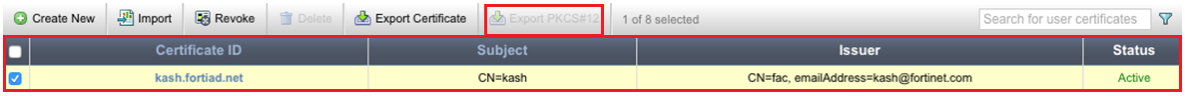
2. Go to **Certificate Management > End Entities > Local Services** and configure a certificate used for EAP-TLS.

Certificate ID	Subject	Issuer	Status
Firmware_Default	C=US, ST=California, L=Sunnyvale, O=Fortinet, OU=FortiAuthent...	Remote CA: C=US, ST=California, L=Sunnyvale, O=Fortinet, OU=C...	Active
fac.tls	CN=fac-tls	CN=fac, emailAddress=kash@fortinet.com	Active

3. Go to **Authentication > RADIUS Service > EAP** and set up the EAP configuration.
   If client certificates were not created by FortiAuthenticator, the 3rd-party server certificate would be uploaded on to FortiAuthenticator as a Trusted CA.
   In this example, FortiAuthenticator creates the client certificates.



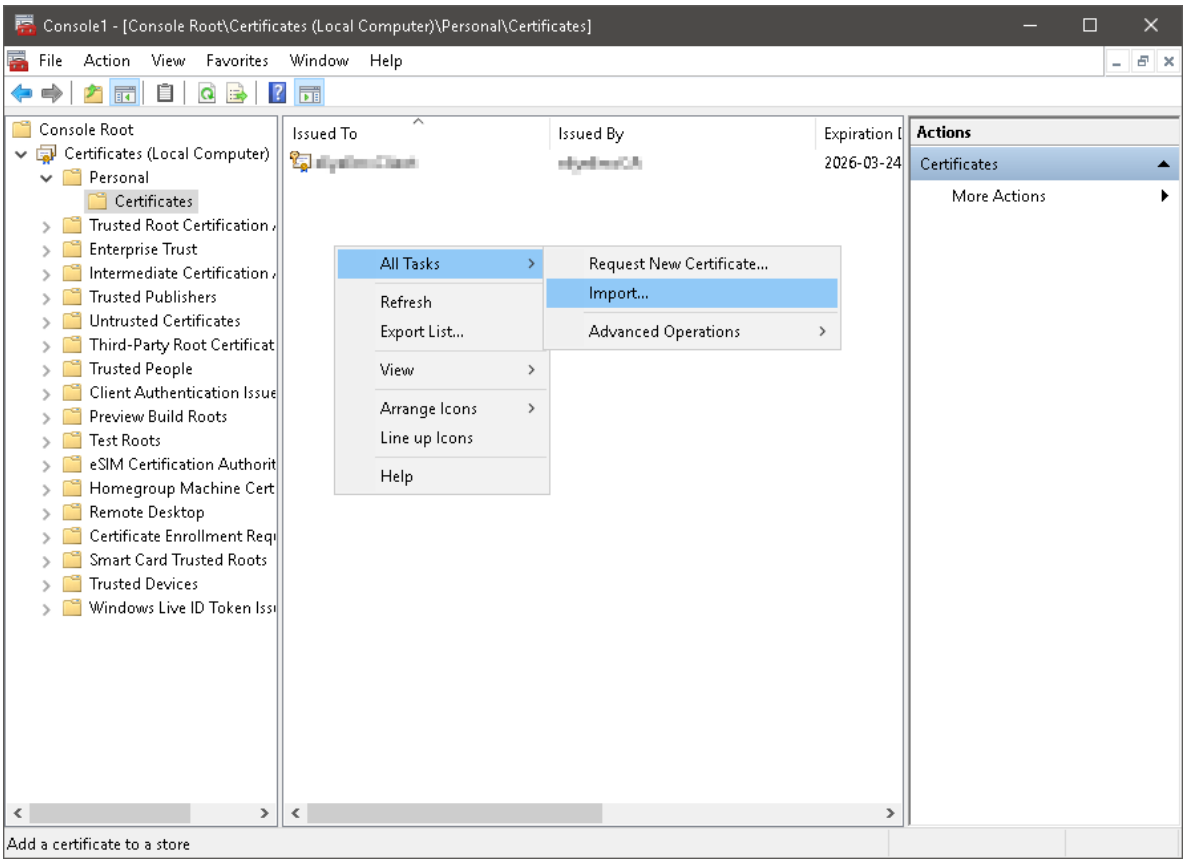
4. Go to **Certificate Management > End Entities > Users** and create a client certificate. The CN must match the AD user name.
   Select **Export Key and Cert** (with a **Passphrase** to protect it) and download the PKCS#12 file.



   The client certificate can be pushed out using Group Policy Object (GPO). Otherwise, it can be imported manually.

Manually importing the client certificate - Windows 10

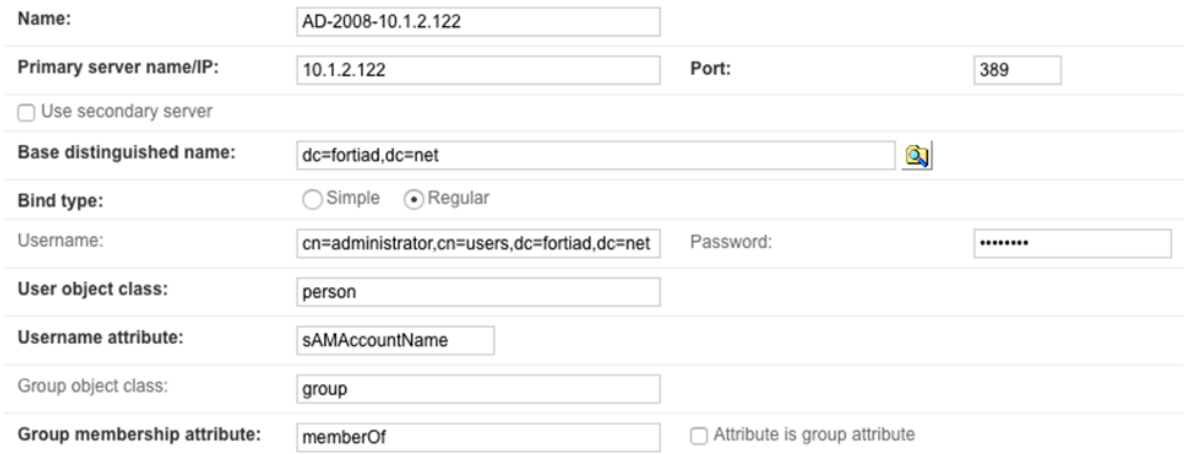
1. The manual import can be completed using Microsoft Management Console (MMC).
   Open Command Prompt and type *mmc* and hit **Enter** to open MMC.
   Go to File menu, click **Add/Remove Snap In**, and add the **Certificates** snap-in for **Local Computer**.
   Once added, right-click in the middle window and select **All Tasks > Import**.



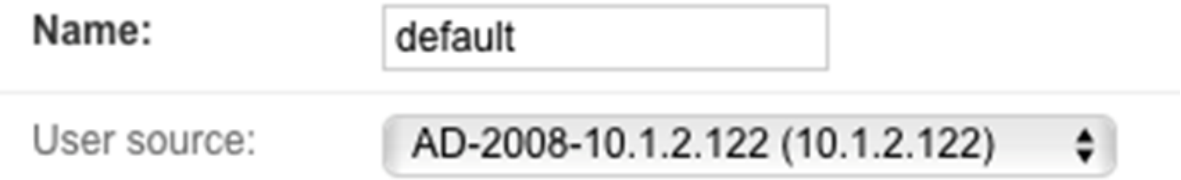
2. Once imported, the certificate should show up under **Local Computer** and not **Current User**.
   Export the FortiAuthenticator certificate and import it under **Trusted Root Certification Authorities**, again under **Certificates (Local Computer)**.

Configuring the FortiAuthenticator AD server

1. Go to **Authentication > Remote Auth. Servers > LDAP** and create a new AD server.
   Ensure that the **Username attribute** matches the entry in the AD configuration from earlier.

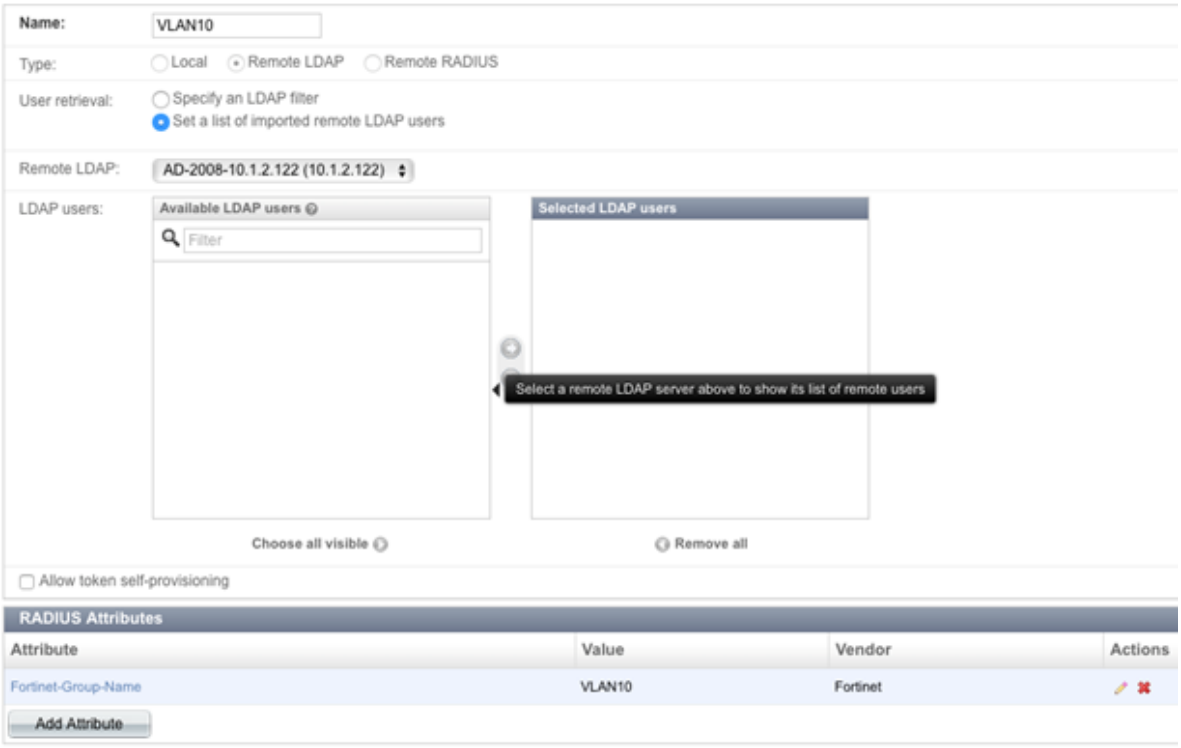


2. Go to **Authentication > User Management > Realms** and create a new realm for these users.



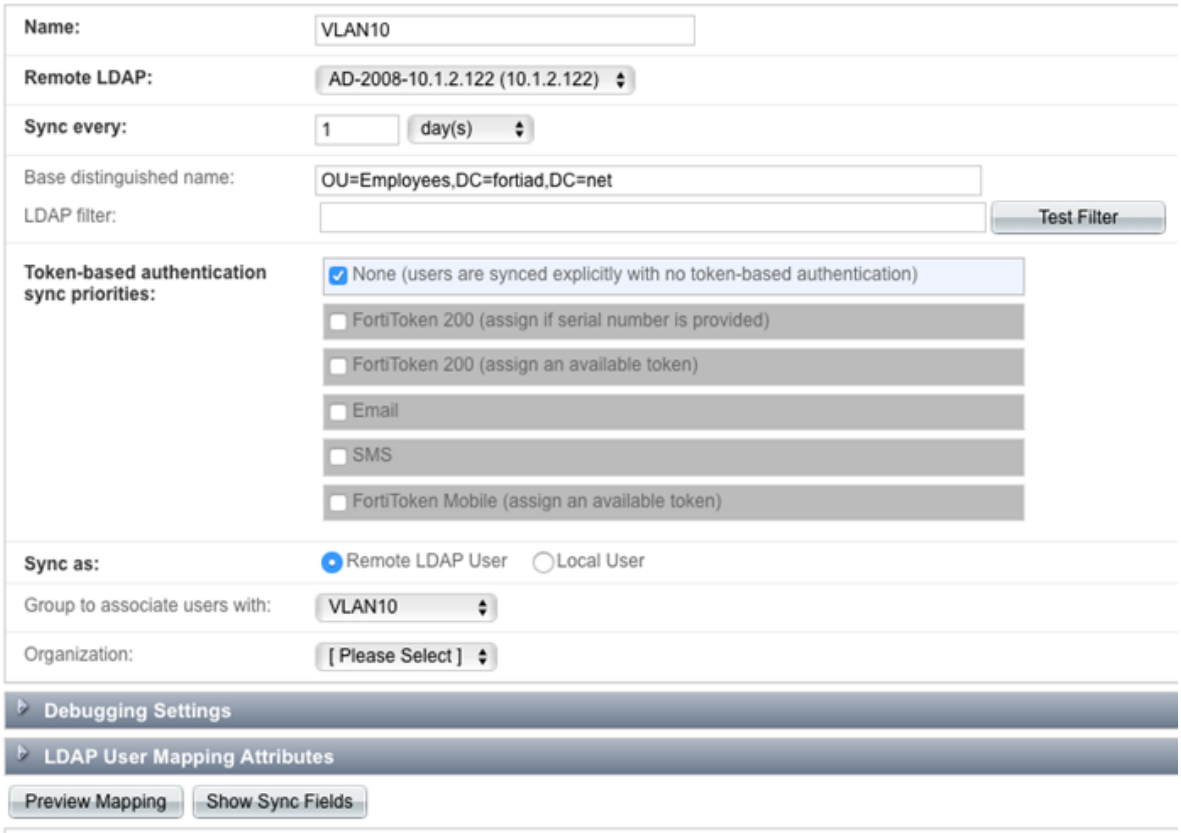
Configuring the user group

1. Go to **Authentication > User Management > User Groups** and create a new user group with the RADIUS attribute shown.
   Note that RADIUS attributes can only be added after the group has been created.



Configuring remote user sync rules

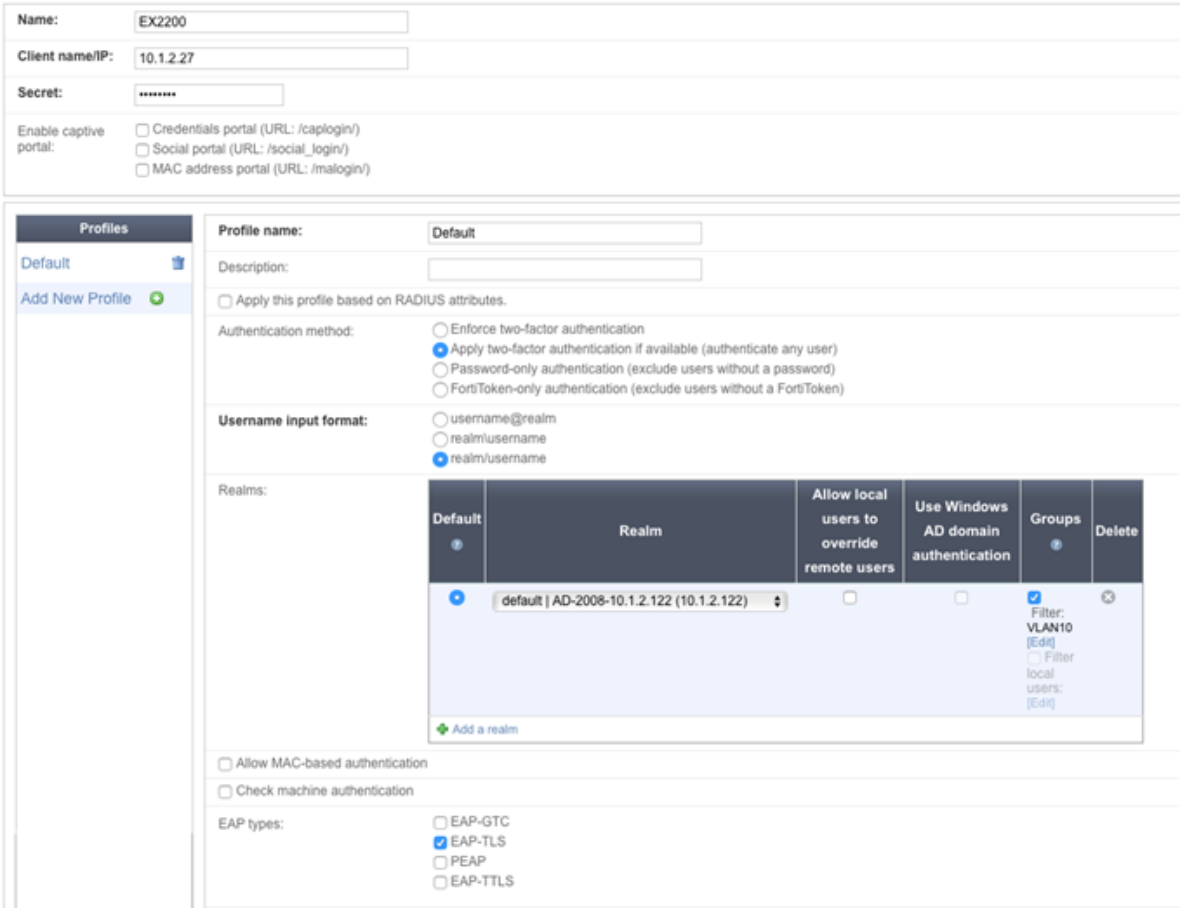
1. Go to **Authentication > User Management > Remote User Sync Rules** and configure a new remote LDAP user synchronization rule.



2. Then go to **Authentication > User Management > Remote Users** and check to see if the sync rule worked.

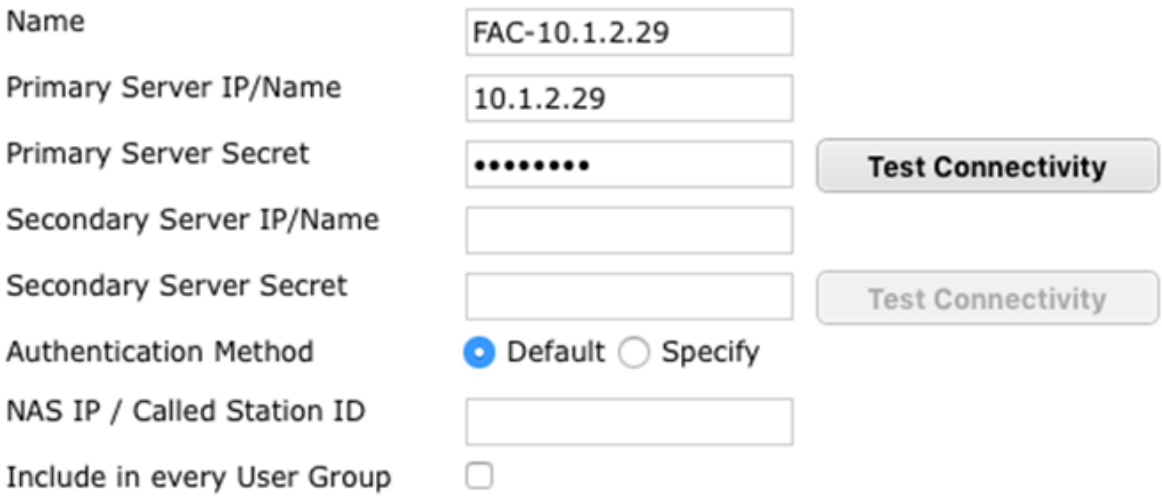
Configuring the FortiAuthenticator RADIUS client

1. Go to **Authentication > RADIUS Service > Clients** and create a RADIUS client to bring the configuration together on the FortiAuthenticator.

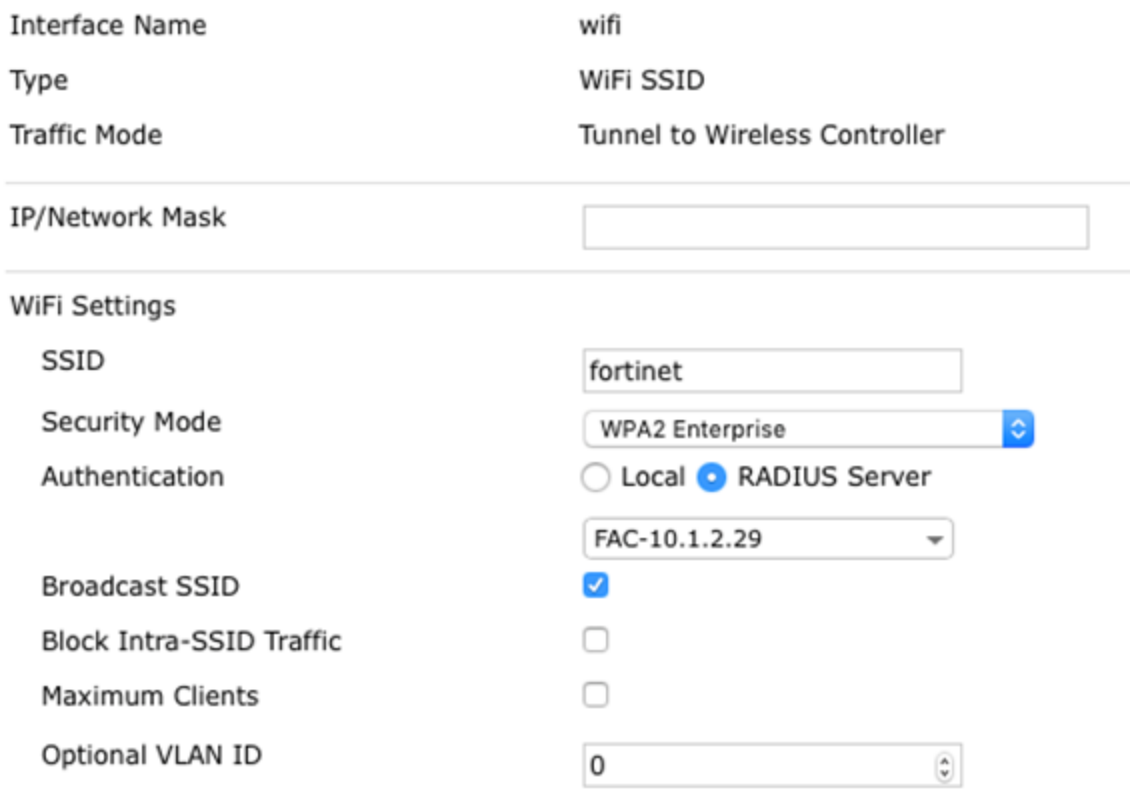


Configuring the FortiWiFi

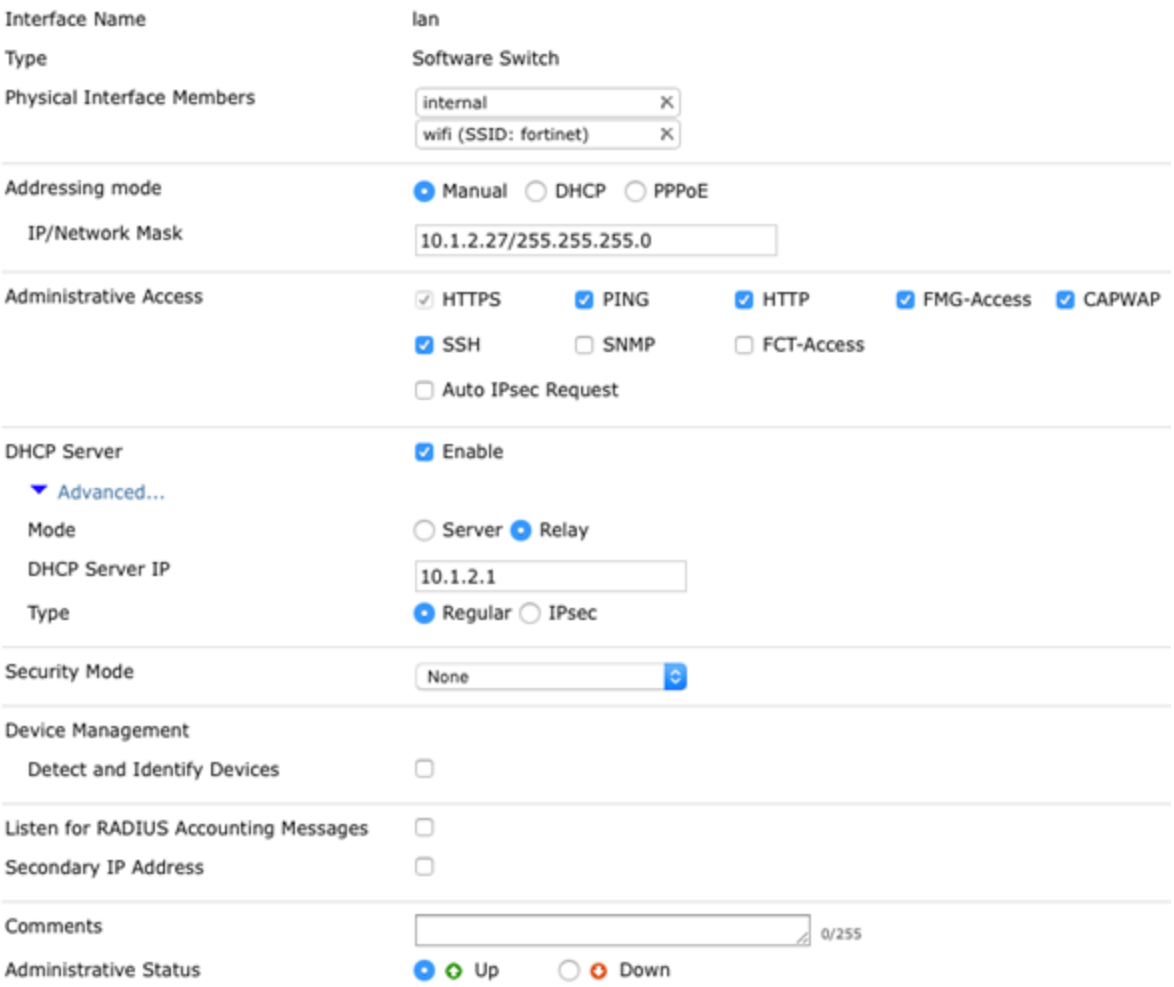
1. On the FortiWiFi, go to **User & Device > RADIUS Servers** and set the FortiAuthenticator as the RADIUS server for the FortiWiFi.



2. Go to **WiFi & Switch Controller > SSID** and configure the WiFi SSID interface.

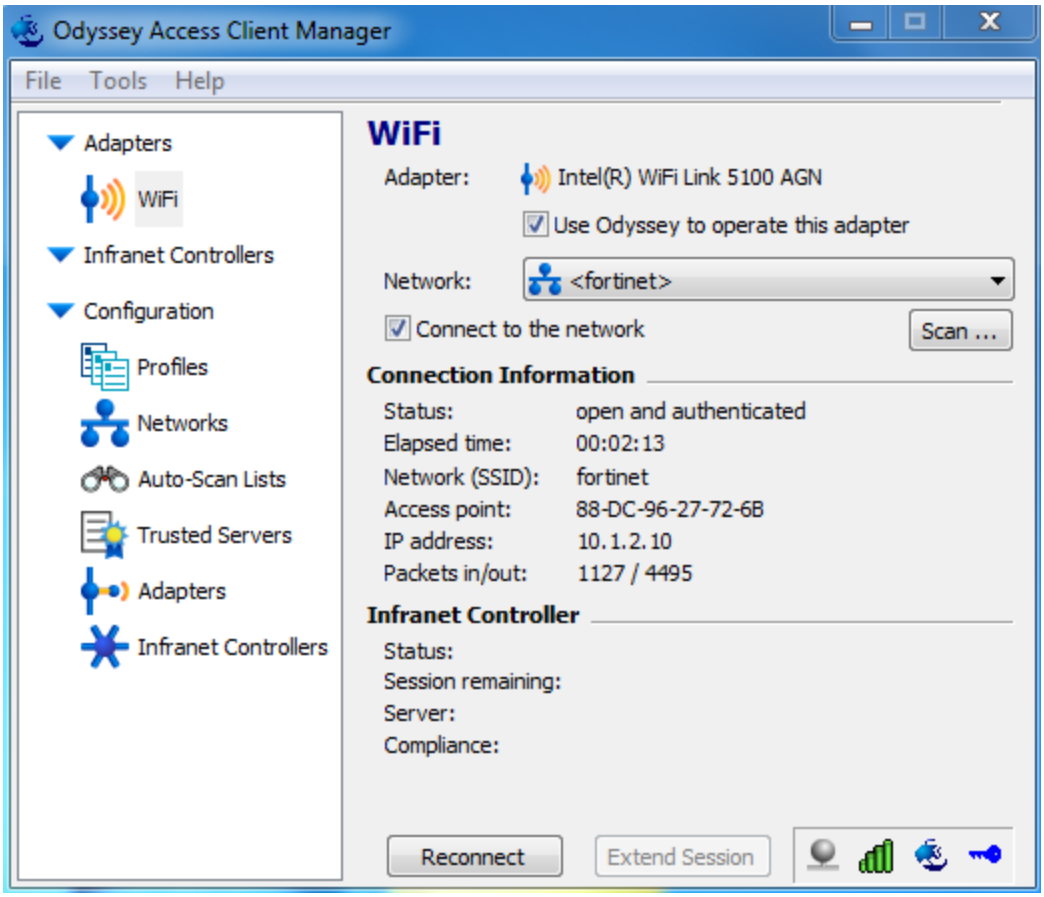


3. Then go to **Network > Interfaces** and configure a software switch combining the physical and WiFi interfaces.



Results

1. In the **Odyssey Access Client Manager**, select **Connect to the network**. Once connected, the **Status** should show as **open and authenticated**.
   The authentication flow should initiate as soon as the supplicant makes a connection request.



2. Using `tcpdump`, FortiAuthenticator shows receipt of an incoming authentication request (`tcpdump host 10.1.2.27 -nnvvXs`):

```
02:04:09.790423 IP (tos 0x0, ttl 64, id 9792, offset 0, flags [none], proto UDP
      (17), length 178)
   10.1.2.27.1025 > 10.1.2.29.1812: [udp sum ok] RADIUS, length: 150
      Access-Request (1), id: 0x9c, Authenticator: 874c50b16efbb87e593a5851e8361f10
         User-Name Attribute (1), length: 6, Value: kash
            0x0000: 6b61 7368
         NAS-IP-Address Attribute (4), length: 6, Value: 0.0.0.0
            0x0000: 0000 0000
         NAS-Port Attribute (5), length: 6, Value: 0
            0x0000: 0000 0000
         Called-Station-Id Attribute (30), length: 28, Value: 88-DC-96-27-72-
               6B:fortinet
            0x0000: 3838 2d44 432d 3936 2d32 372d 3732 2d36
            0x0010: 423a 666f 7274 696e 6574
         Calling-Station-Id Attribute (31), length: 19, Value: 00-26-C6-6A-E6-B2
            0x0000: 3030 2d32 362d 4336 2d36 412d 4536 2d42
            0x0010: 32
         Framed-MTU Attribute (12), length: 6, Value: 1400
            0x0000: 0000 0578
         NAS-Port-Type Attribute (61), length: 6, Value: Wireless - IEEE 802.11
            0x0000: 0000 0013
         Connect-Info Attribute (77), length: 24, Value: CONNECT 11Mbps 802.11b
            0x0000: 434f 4e4e 4543 5420 3131 4d62 7073 2038
            0x0010: 3032 2e31 3162
```

3. Continuing with `tcpdump`, Access-Challenge is issued from FortiAuthenticator to the FortiWiFi:

```
01:09:34.679881 IP (tos Ox0, ttl 64, id 58896, offset 0, flags [none], proto UDP
      (17), length 108)
   10.1.2.29.1812 > 10.1.2.27.1025: [bad udp cksum 0xl8a3 -> 0xbd921] RADIUS,
         length: 80
      Access-Challenge (11), id: 0x9c, Authenticator:
            c67b8d0f8805db68e57e9757deda20d0
         EAP-Message Attribute (79), length: 24, Value: ..
            0x0000: 0101 0016 0410 8b8c ae75 4696 0a47 96fd
            0x0010: 7c26 528a 097e
         Message-Authenticator Attribute (80), length: 18, Value: ..... 1.!.q._.*[.
            0x0000: @ad flfd e931 1321 f571 f85f dl2a Sbd3
         State Attribute (24), length: 18, Value: .!&.. "..9[~....
            0x0000: ad21 2611 ad20 22e2 e539 5b7e 94e2 9a87
```

The next 14 messages are Challenge->Request EAP transactions between the FortiAuthenticator and the FortiWiFi.

4. Access-Accept message with RADIUS attributes are returned to the FortiWiFi:

```
2:04:10.000998 IP (tos Ox0, ttl 64, id 44468, offset 0, flags (none), proto UDP
      (17), length 208)
   10.1.2.29.1812 > 10.1.2.27.1025: (bad udp cksum 0x1918 0x77e9I) RADIUS, length:
         180
      Access-Accept (2), id: Ox7d, Authenticator: 144538f6ifd7f4b12d768e76f05709ae2
         Vendor-Specific Attribute (26), length: 58, Value: Vendor: Microsoft (311)
            Vendor Attribute: 17, Length: 50, Value: ..S.|..W...^.. ..h0p.U..~..{.
                  P..|b7".............s..
            0x0000: 0000 0137 1134 80e3 aefl 65e0 1383 c34e
            0x0010: 413d 4Sbd 350d 39be ac79 04b8 90fa 1551
            0x0020: a4b7 10d3 09b6 f902 5e52 3d69 b3b4 216a
            0x0030: b48f 0ef2 0c08 9cd0
         Vendor-Specific Attribute (26), length: 58, Value: Vendor: Microsoft (311)
            Vendor Attribute: 16, Length: 50, Value: .t._
                  M.,...a...a.JhFz5.....2.;"..."...D.y.=..{./..?.
            0x0000: 0000 0137 1034 8883 7a9b bllb 9488 f181
            0x0010: d179 29ba 7538 lleb 8311 3c22 1b62 9176
            0x0020: d0be f763 4617 670c d8ca 8659 7a14 dl2c
            0x0030: 8064 5955 942b ccla
         EAP-Message Attribute (79), length: 6, Value: ..
            0x0000: 0307 0004
         Message-Authenticator Attribute (80), length: 18, Value: .c.b..m.G.ZH.'.6
            0x0000: 9aec 02c0 3e6b af8e defb 8020 e50b 0728
         User-Name Attribute (1), length: 6, Value: kash
            0x0000: 6b61 7368
         Vendor-Specific Attribute (26), length: 14, Value: Vendor: Fortinet (12356)
            Vendor Attribute: 1, Length: 6, Value: VLAN10
            0x0000: 0000 3044 0108 564c 414e 3130
```

5. On the FortiAuthenticator, go to **Logging > Log Access > Logs** to verify the device authentication. The Debug Log (at `https://<fac-ip>/debug/radius`) should also confirm successful authentication.

Log Details

Log Record Detail	
ID	1848
Timestamp	Tue Sep 27 01:09:36 2016
Level	information
Action	Authentication
Status	Success
NAS Name/IP	10.1.2.27
Message	802.1x authentication successful
User	host/leno.fortiad.net
Log Type	
Type Id	20420
Name	802.1x Authentication OK
Sub Category	Authentication
Category	Event
Description	802.1x authentication successful

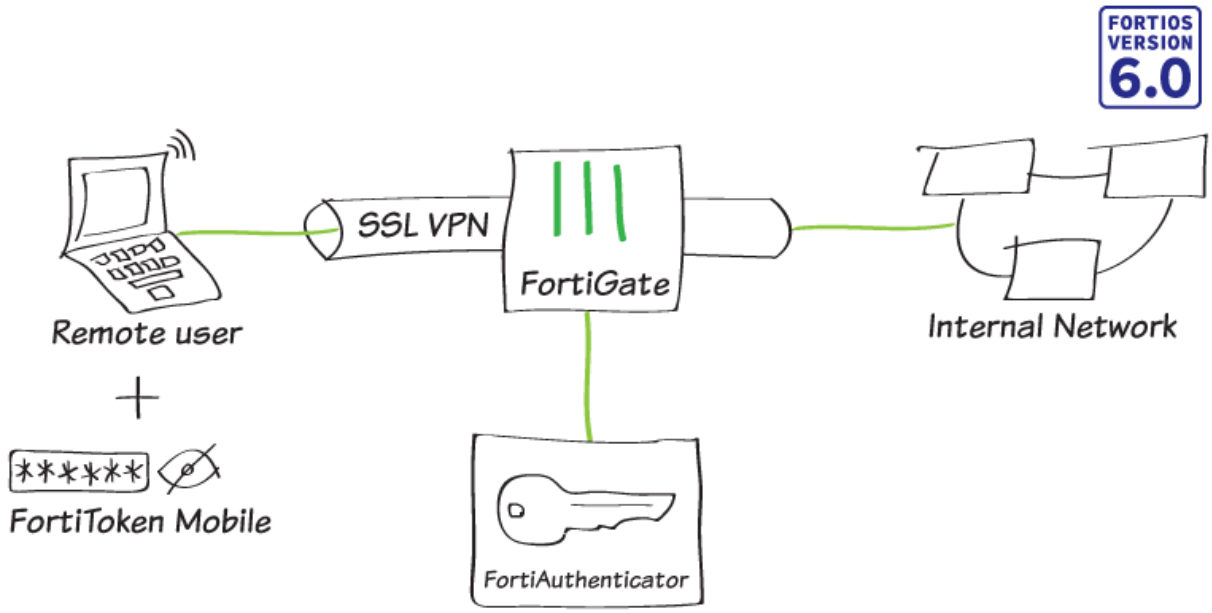
6. On the FortiWifi, go to **WiFi & Switch Controller > Monitor > Client Monitor** and note that the group is the RADIUS attribute sent from FortiAuthenticator. Any firewall policy using that group will now be enabled for the user.

FortiToken and FortiToken Mobile

This section describes various authentication scenarios involving FortiToken, a disconnected one-time password (OTP) generator that's either a physical device or a mobile token. Time-based token passcodes require that the FortiAuthenticator clock is accurate. If possible, configure the system time to be synchronized with a network time protocol (NTP) server.

To perform token-based authentication, the user must enter the token passcode. If the user's username and password are also required, this is called two-factor authentication.

FortiToken Mobile Push for SSL VPN



In this recipe, you set up FortiAuthenticator to function as a RADIUS server to authenticate SSL VPN users using FortiToken Mobile Push two-factor authentication. With Push notifications enabled, the user can easily accept or deny the authentication request.

For this configuration, you:

- Create a user on the FortiAuthenticator.
- Assign a FortiToken Mobile license to the user.
- Create the RADIUS client (FortiGate) on the FortiAuthenticator, and enable FortiToken Mobile Push notifications.
- Connect the FortiGate to the RADIUS server (FortiAuthenticator).
- Create an SSL VPN on the FortiGate, allowing internal access for remote users.

The following names and IP addresses are used:

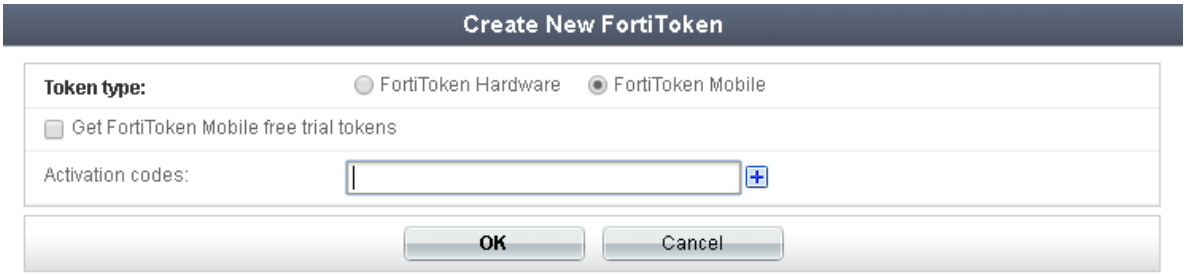
- Username: gthreepwood
- User group: RemoteFTMGroup
- RADIUS server: OfficeRADIUS
- RADIUS client: OfficeServer
- SSL VPN user group: SSLVPNGroup
- FortiAuthenticator: 172.25.176.141
- FortiGate: 172.25.176.92

For the purposes of this recipe, a FortiToken Mobile free trial token is used. This recipe also assumes that the user has already installed the FortiToken Mobile application on their smartphone. You can install the application for Android and iOS. For details, see:

- FortiToken Mobile for Android
- FortiToken Mobile for iOS

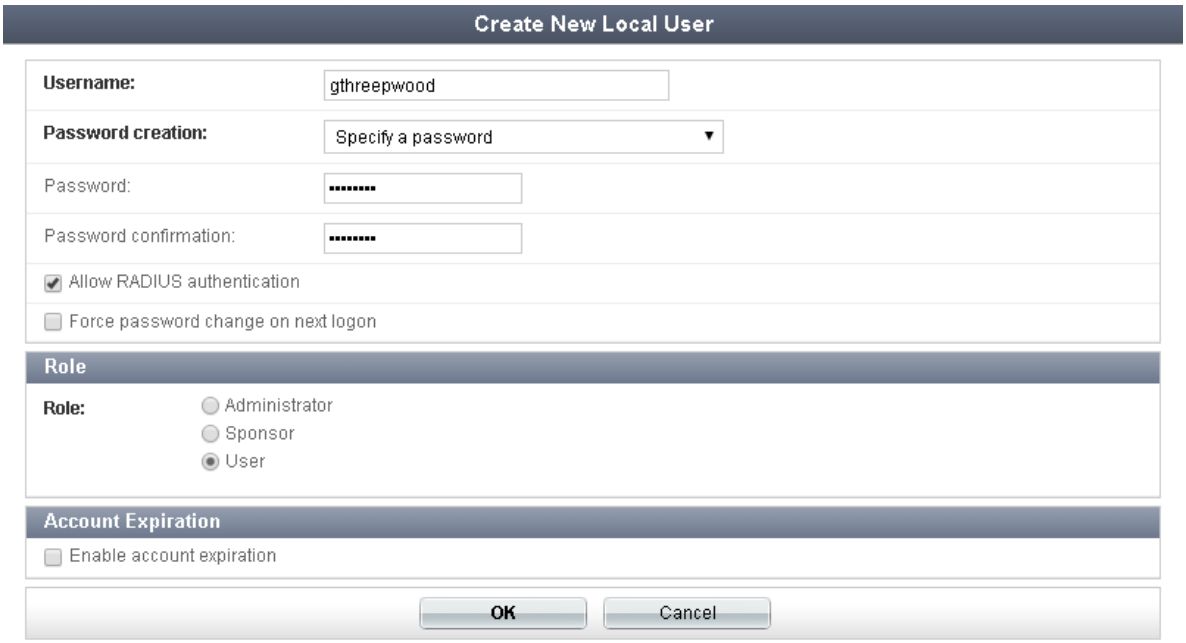
Adding a FortiToken to the FortiAuthenticator

1. On the FortiAuthenticator, go to **Authentication > User Management > FortiTokens**, and select **Create New**.
2. Set **Token type** to **FortiToken Mobile**, and enter the FortiToken **Activation codes** in the field provided.

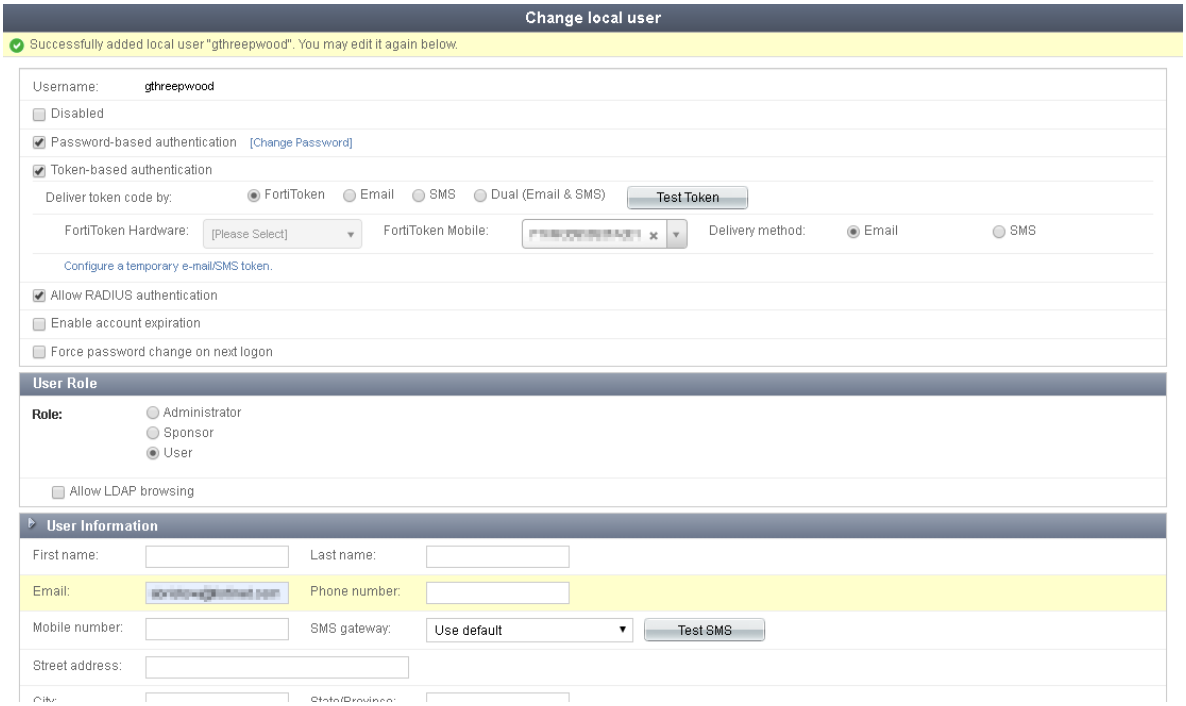


Adding the user to the FortiAuthenticator

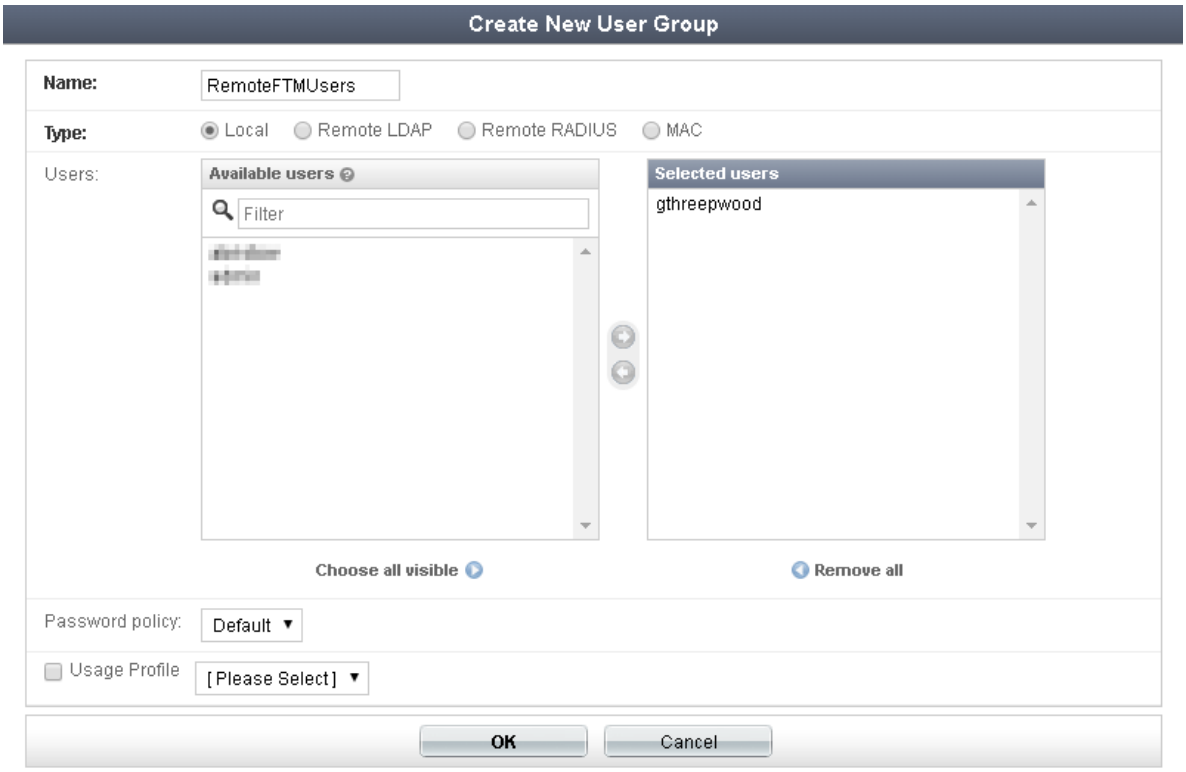
1. On the FortiAuthenticator, go to **Authentication > User Management > Local Users**, and select **Create New**.
   Enter a **Username** (*gthreepwood*) and enter and confirm the user password.
   Enable **Allow RADIUS authentication**, and select **OK** to access additional settings.



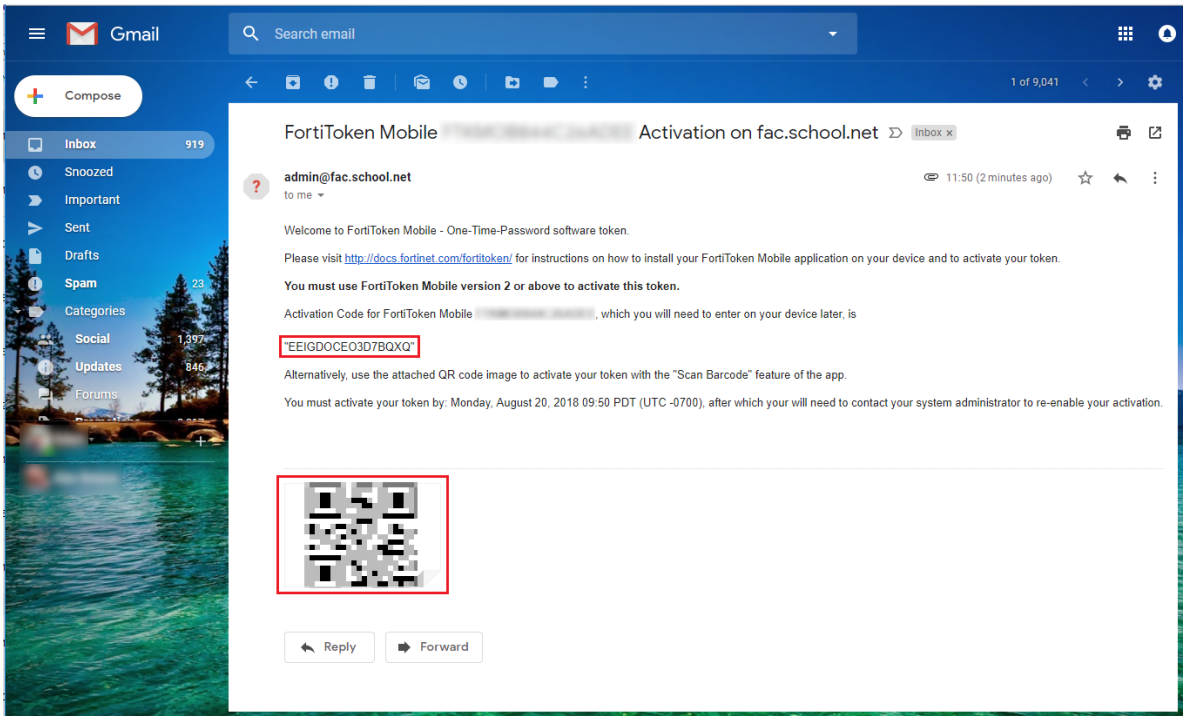
2. Enable **Token-based authentication** and select to deliver the token code by **FortiToken**. Select the FortiToken added earlier from the **FortiToken Mobile** drop-down menu.
   Set **Delivery method** to **Email**. This will automatically open the **User Information** section where you can enter the user email address in the field provided.



3. Next, go to **Authentication > User Management > User Groups**, and select **Create New**.
   Enter a **Name** (*RemoteFTMUsers*) and add **gthreepwood** to the group by moving the user from **Available users** to **Selected users**.



4. The FortiAuthenticator sends the FortiToken Mobile activation to the user's email address. If the email does not appear in the inbox, check the spam folder.
   The user activates their FortiToken Mobile through the FortiToken Mobile application by either entering the activation code provided or by scanning the QR code attached.

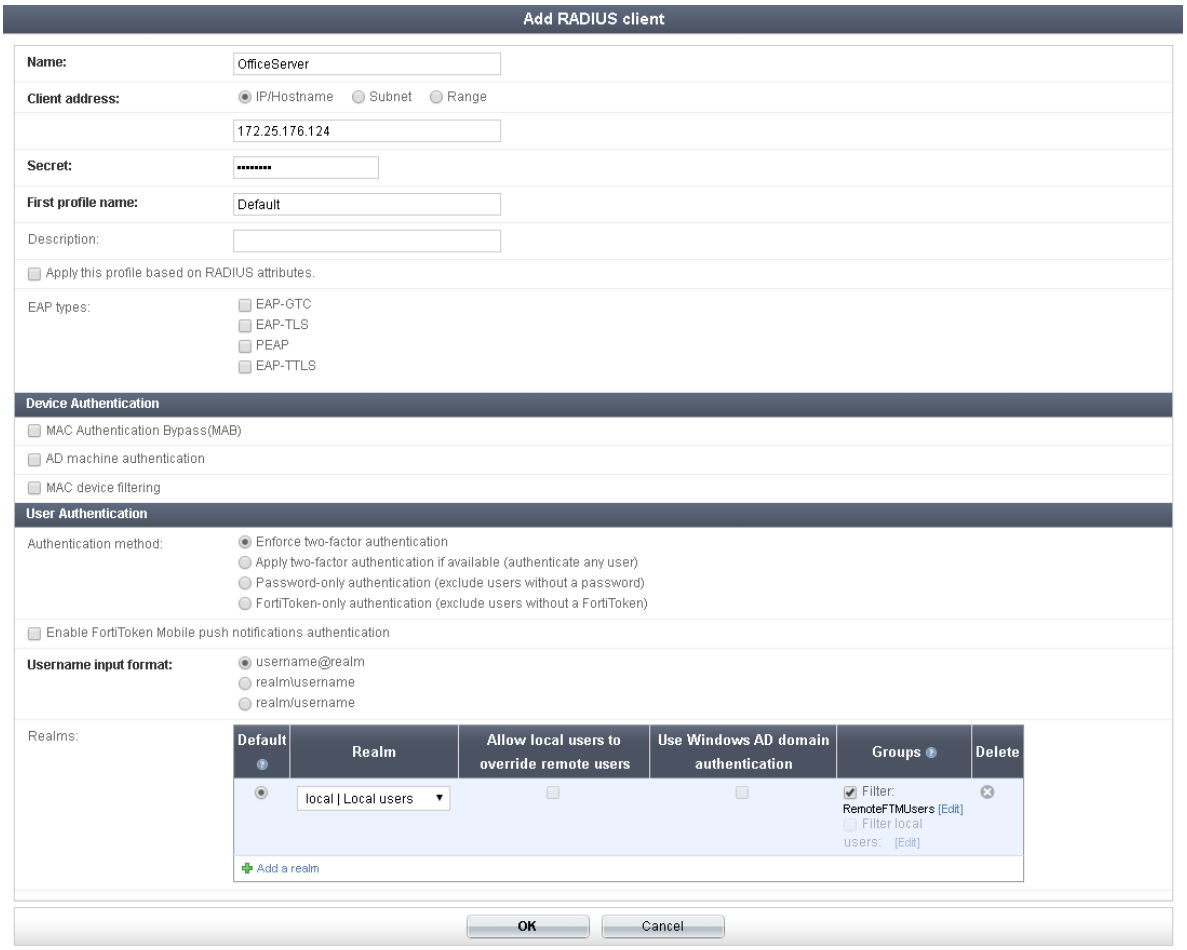


For more information, see the FortiToken Mobile user instructions.

Creating the RADIUS client on the FortiAuthenticator

1. On the FortiAuthenticator, go to **Authentication > RADIUS Service > Clients**, and select **Create New** to add the FortiGate as a RADIUS client.
2. Enter a **Name** (*OfficeServer*), the IP address of the FortiGate, and set a **Secret**. The secret is a pre-shared secure password that the FortiGate will use to authenticate to the FortiAuthenticator.
3. Set **Authentication method** to **Enforce two-factor authentication** and check the **Enable FortiToken Mobile push notifications authentication** checkbox.
4. Set **Realms** to **local | Local users**, and add **RemoteFTMUsers** to the **Groups** filter.

Note the **Username input format**. This is the format that the user must use to enter their username in the web portal, made up of their username and realm. In this example, the full username for gthreepwood is "**gthreepwood@local**".

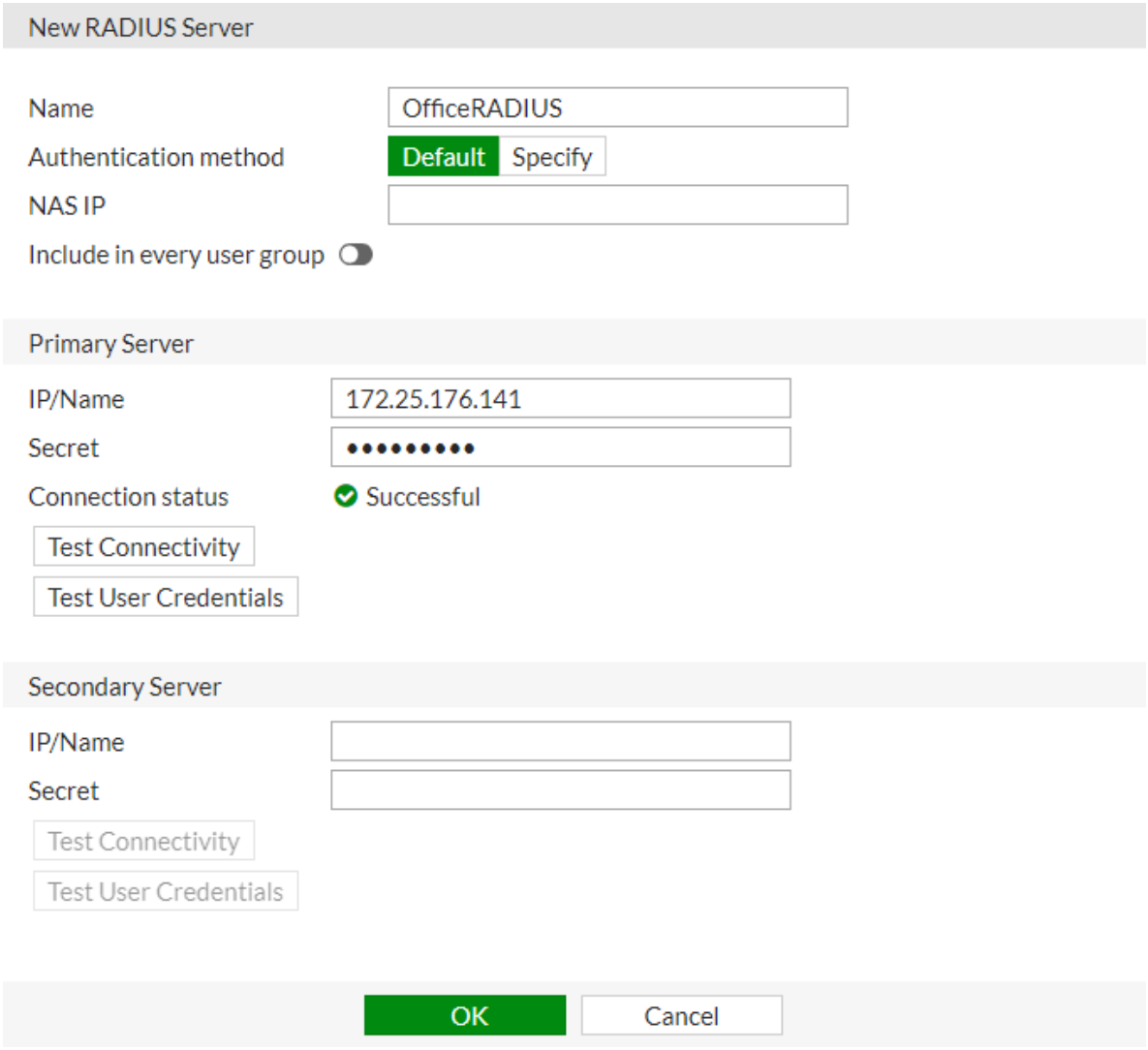


Connecting the FortiGate to the RADIUS server

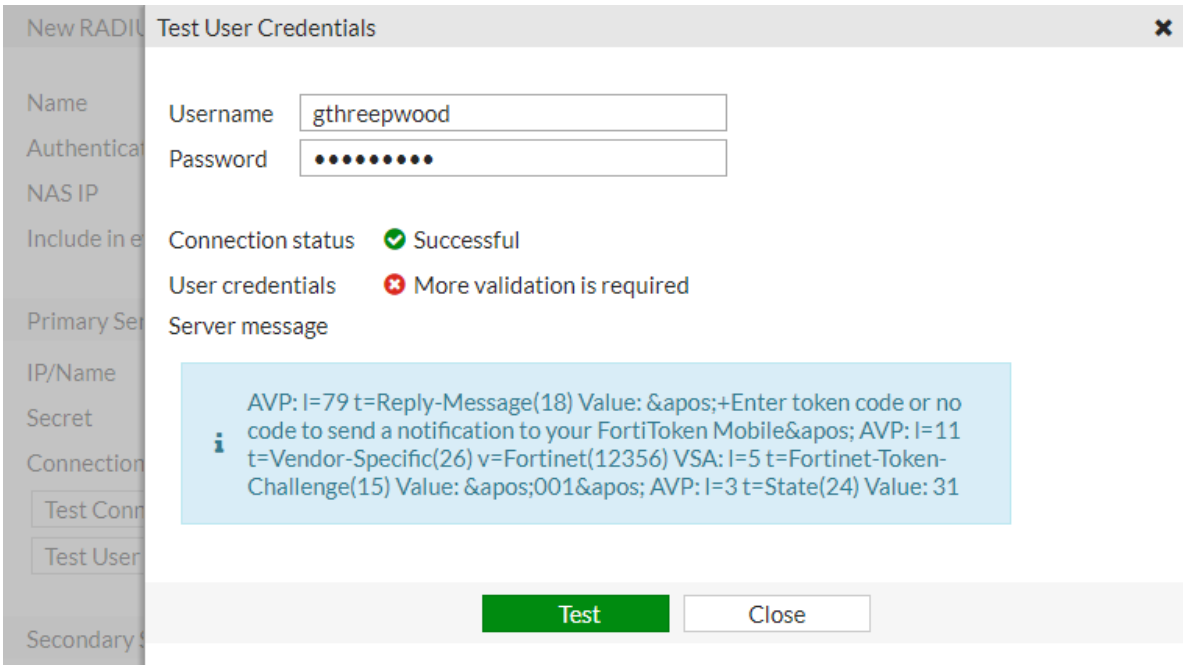
1. On the FortiGate, go to **User & Device > RADIUS Servers**, and select **Create New** to connect to the RADIUS server (FortiAuthenticator).

Enter a **Name** (*OfficeRADIUS*), the IP address of the FortiAuthenticator, and enter the **Secret** created before.

Select **Test Connectivity** to be sure you can connect to the RADIUS server. Then select **Test User Credentials** and enter the credentials for **gthreepwood**.

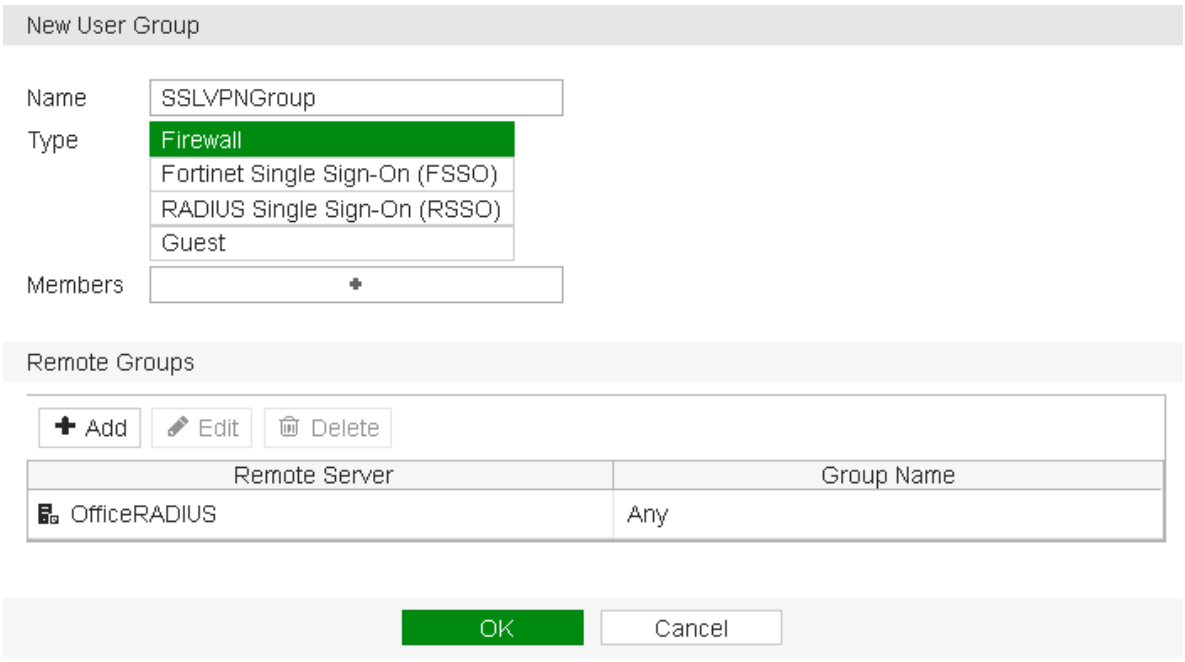


Because the user has been assigned a FortiToken, the test should return stating that **More validation is required**.



The FortiGate can now connect to the FortiAuthenticator as the RADIUS client configured earlier.

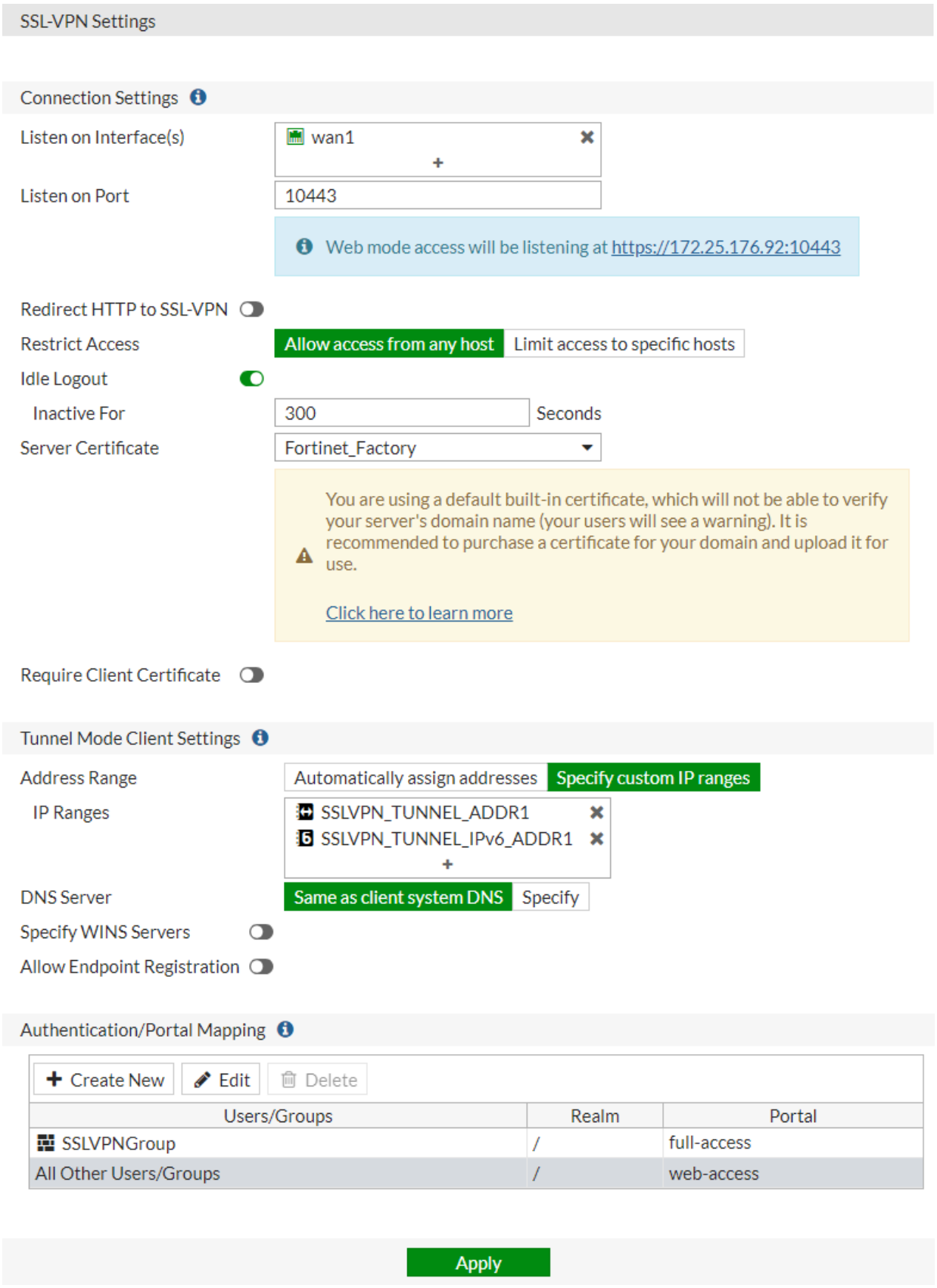
2. Then go to **User & Device > User Groups**, and select **Create New** to map authenticated remote users to a user group on the FortiGate.
   Enter a **Name** (*SSLVPNGroup*) and select **Add** under **Remote Groups**.
   Select **OfficeRADIUS** under the **Remote Server** drop-down menu, and leave the **Groups** field blank.



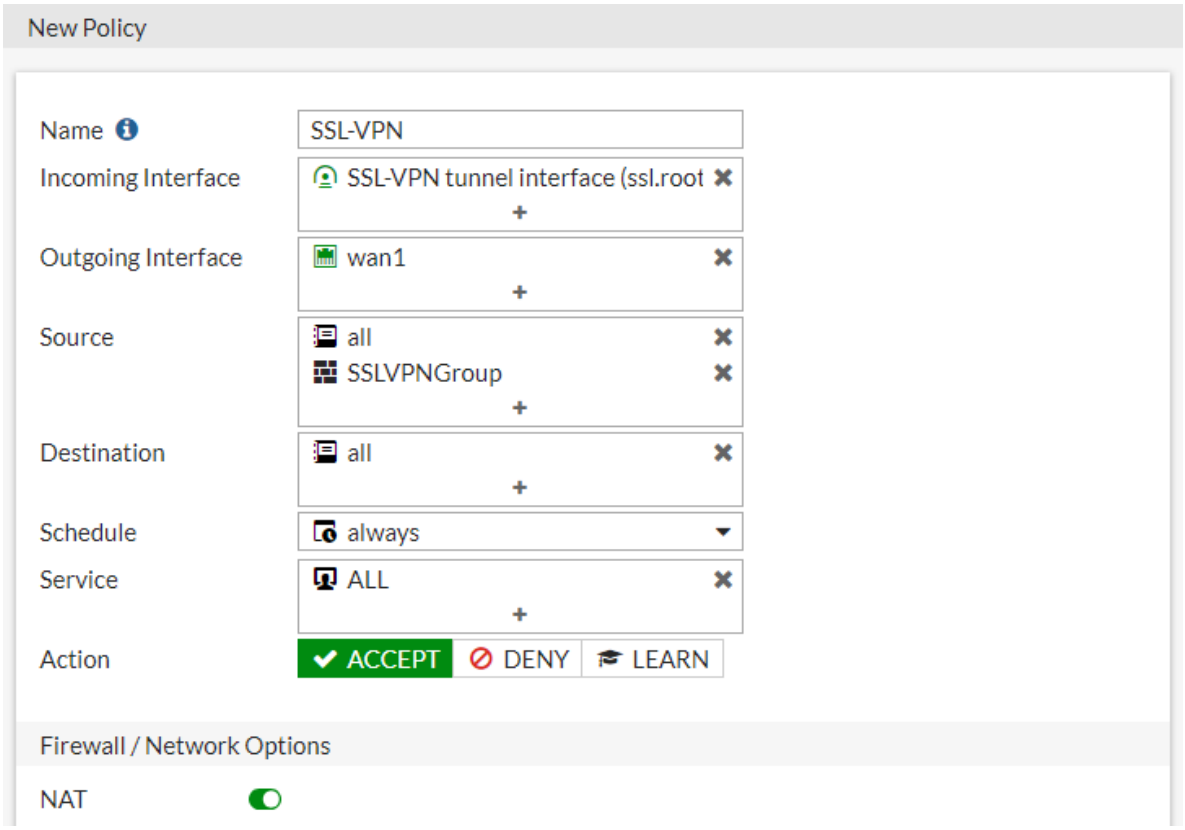
Configuring the SSL VPN

1. On the FortiGate, go to **VPN > SSL-VPN Portals**, and edit the **full-access** portal.
   Toggle **Enable Split Tunneling** so that it is disabled.

2. Go to **VPN > SSL-VPN Settings**.
   Under **Connection Settings** set **Listen on Interface(s)** to **wan1** and **Listen on Port** to **10443**.
   Under **Tunnel Mode Client Settings**, select **Specify custom IP ranges**. The **IP Ranges** should be set to **SSLVPN_TUNNEL_ADDR1** and the IPv6 version by default.
   Under **Authentication/Portal Mapping**, select **Create New**.
   Set the **SSLVPNGroup** user group to the **full-access** portal, and assign **All Other Users/Groups** to **web-access** — this will grant all other users access to the web portal *only*.

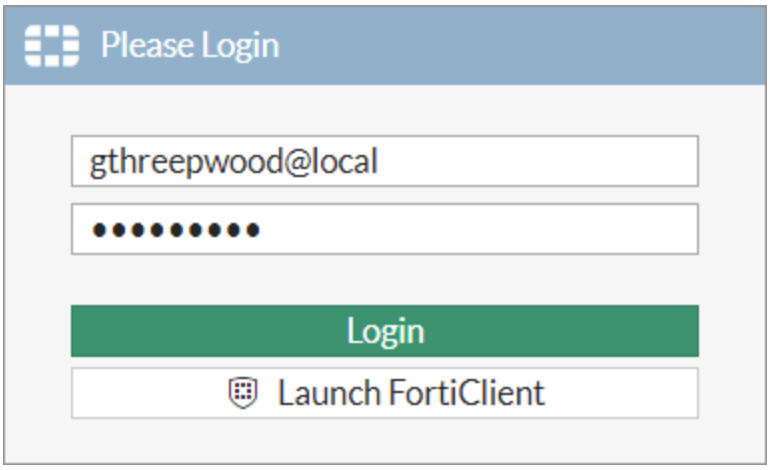

SSL-VPN Settings
Connection Settings
Listen on Interface(s)
wan1
Listen on Port
10443
Web mode access will be listening at https://172.25.176.92:10443
Redirect HTTP to SSL-VPN
Restrict Access
Allow access from any host
Limit access to specific hosts
Idle Logout
Inactive For
300
Seconds
Server Certificate
Fortinet_Factory
You are using a default built-in certificate, which will not be able to verify your server's domain name (your users will see a warning). It is recommended to purchase a certificate for your domain and upload it for use.
Click here to learn more
Require Client Certificate
Tunnel Mode Client Settings
Address Range
Automatically assign addresses
Specify custom IP ranges
IP Ranges
SSLVPN_TUNNEL_ADDR1
SSLVPN_TUNNEL_IPv6_ADDR1
DNS Server
Same as client system DNS
Specify
Specify WINS Servers
Allow Endpoint Registration
Authentication/Portal Mapping
Create New
Edit
Delete
Users/Groups
Realm
Portal
SSLVPNGroup
/
full-access
All Other Users/Groups
/
web-access
Apply

3. Then go to **Policy & Objects > IPv4 Policy** and create a new SSL VPN policy.
   Set **Incoming Interface** to the **SSL-VPN tunnel interface** and set **Outgoing Interface** to the Internet-facing interface (in this case, **wan1**).
   Set **Source** to the **SSLVPNGroup** user group and the **all** address.
   Set **Destination** to **all**, **Schedule** to **always**, **Service** to **ALL**, and enable **NAT**.

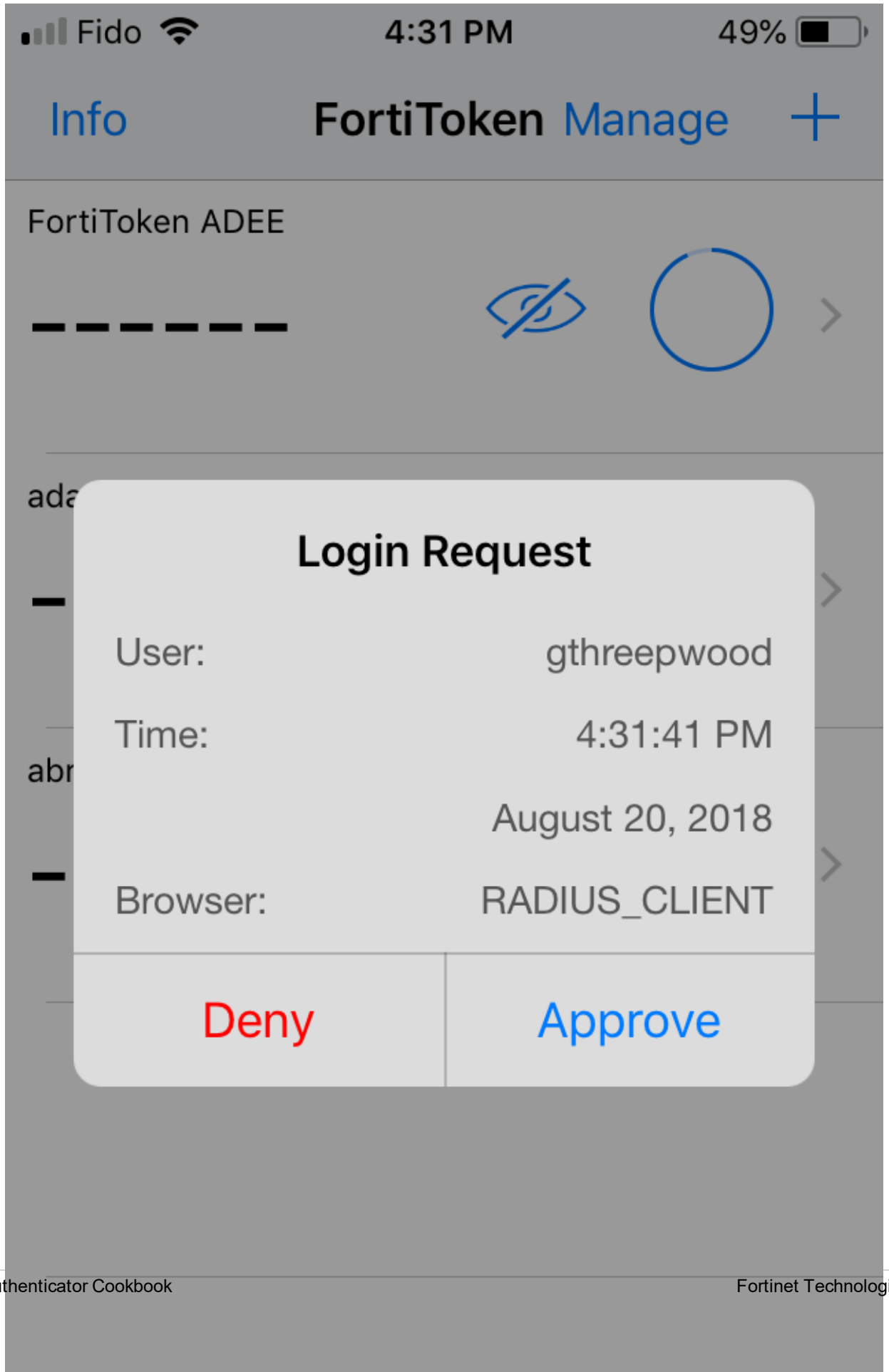


Results

1. From a remote device, open a web browser and navigate to the SSL VPN web portal *(https://<fortigate-ip>:10443*).
2. Enter **gthreepwood**'s credentials and select **Login**. Use the correct format (in this case, username@realm), as per the client configuration on the FortiAuthenticator.

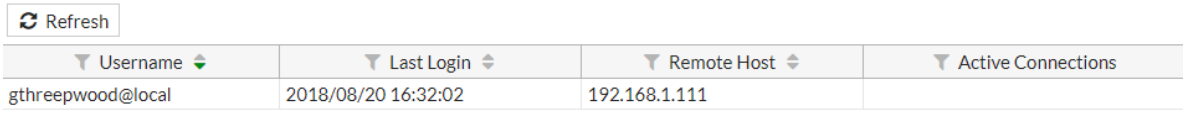


3. The FortiAuthenticator will then push a login request notification through the FortiToken Mobile application. Select **Approve**.


Fido
4:31 PM
49%
Info
FortiToken
Manage
FortiToken ADEE
Login Request
User:
gthreepwood
Time:
4:31:41 PM
August 20, 2018
Browser:
RADIUS_CLIENT
Deny
Approve

Upon approving the authentication, **gthreepwood** is successfully logged into the SSL VPN portal.

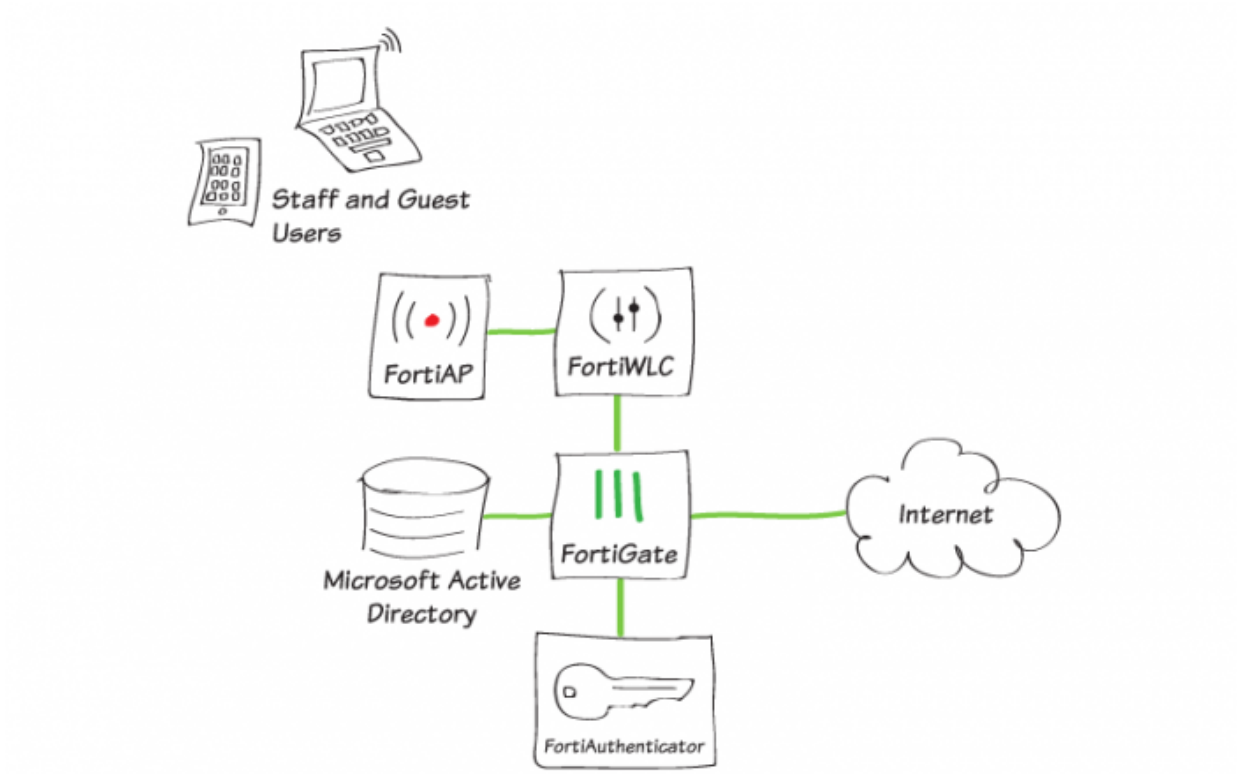
3. On the FortiGate, go to **Monitor > SSL-VPN Monitor** to confirm the user's connection.



Guest Portals

This section contains information about creating and using guest portals.

FortiAuthenticator as Guest Portal for FortiWLC

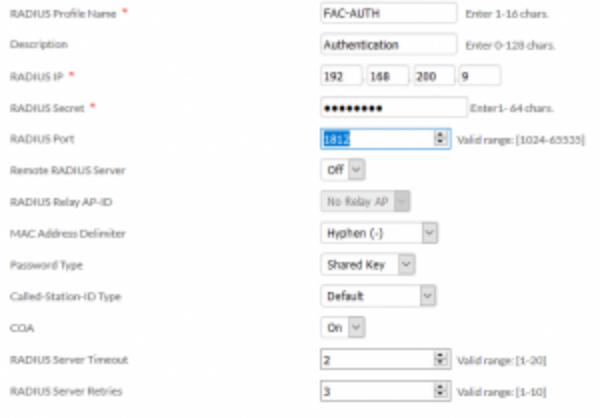


In this recipe we will use FortiAuthenticator as Guest Portal for users getting wireless connection provided by FortiWLC.

Creating the FortiAuthenticator as RADIUS server on the FortiWLC

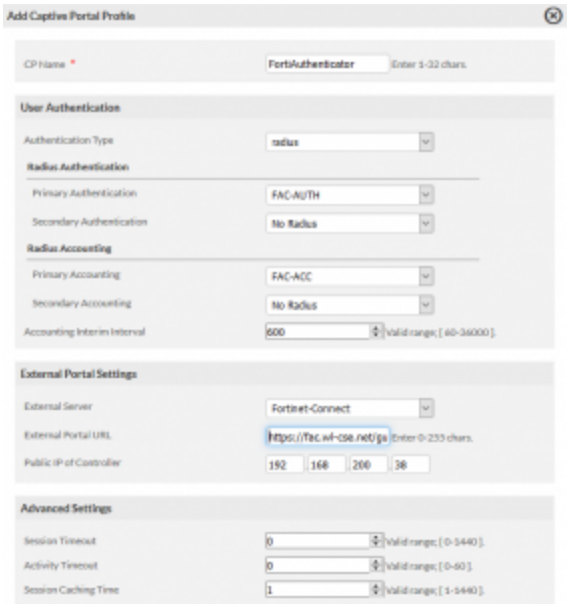
1. On the FortiWLC, go to **Configuration > Security > RADIUS** and select **ADD** and create two profiles. One to be used for **Authentication** and one to be used for **Accounting**.
   - **RADIUS Profile name**: Enter a name for the profile. Use a name that will indicate if the profile is used for **Authentication** or **Accounting**.
   - **RADIUS IP**: IP address of the FortiAuthenticator.
   - **RADIUS Secret**: Shared secret between WLC and FortiAuthenticator.

- **RADIUS Port**: Use **1812** for **Authentication** profile and **1813** when creating an **Accounting** profile.



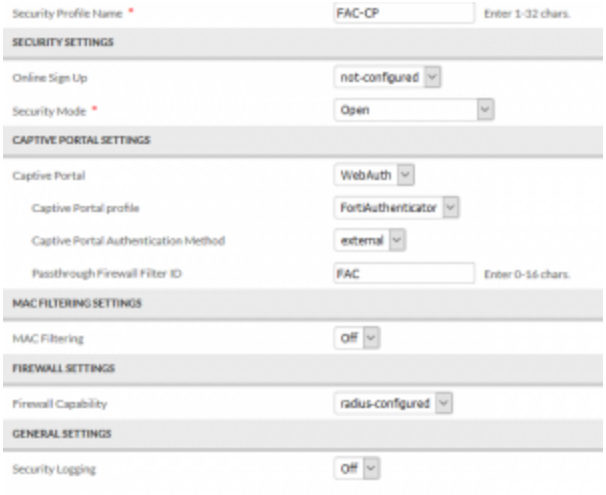
Creating the Captive Portal profile on the FortiWLC

1. On the FortiWLC, go to **Configuration > Security > Captive Portal**, select the **Captive Portal Profiles** tab, and **ADD** a new profile.
   - **CP Name**: Enter a name for the profile.
   - **Authentication Type**: **RADIUS**
   - **Primary Authentication**:Your Authentication profile.
   - **Primary Accounting**: Your Accounting profile.
   - **External Server**: Fortinet-Connect
   - **External Portal**: https://<fortiauthenticator-ip>/guests
   - **Public IP of Controller**: IP address of the FortiWLC.



Creating the security profile on the FortiWLC

1. On the FortiWLC, go to **Configuration > Security > Profile** and **ADD** a new profile.
   - **Profile Name**: Enter a name for the profile.
   - **Security Mode**: **Open**
   - **Captive Portal**: **WebAuth**
   - **Captive Portal Profile**: Select the profile created earlier.
   - **Captive Portal Authentication Method**: **external**
   - **Passthrough Firewall Filter ID**: An ID used to allow access to the portal before authentication using QoS rules.



Creating the QoS rule on the FortiWLC

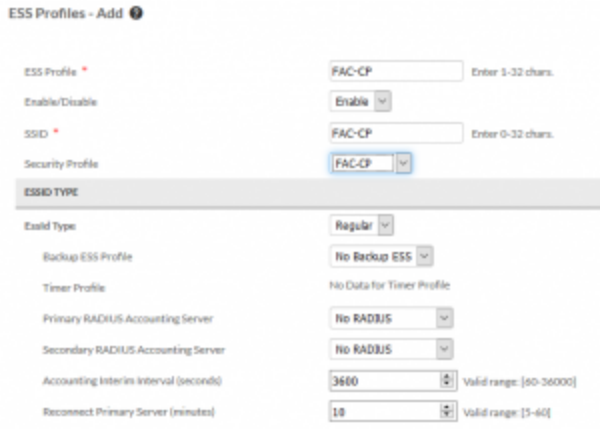
1. On the FortiWLC, go to **Configuration > Policies > QoS** and select the **QoS and Firewall Rules** tab. Select **ADD** to create two profiles.
   For the first rule, allow the wireless client to access the FortiAuthenticator guest portal.
   - **ID**: Rule number (in the example, *20*).
   - **Destination IP**: IP address of the FortiAuthenticator, and enable **Match**.
   - **Destination Netmask**: *255.255.255.255*
   - **Destination Port**: *443*, and enable **Match**.
   - **Network Protocol**: *6*, and enable **Match**.
   - **Firewall Filter ID**: String from the security profile, and enable **Match**.
   - **QoS Protocol**: Other.

2. For the second rule, allow FortiAuthenticator to reach the clients.
   - **ID**: Rule number (in the example, *21*).
   - **Source IP**: IP address of the FortiAuthenticator, and enable **Match**.
   - **Source Netmask**: *255.255.255.255*
   - **Source Port**: *443*, and enable **Match**.
   - **Network Protocol**: *6*, and enable **Match**.
   - **Firewall Filter ID**: Use the **Passthrough Firewall Filter ID** string from the security profile, and enable **Match**.
   - **QoS Protocol**: Other.

Creating the ESS Profile on the FortiWLC

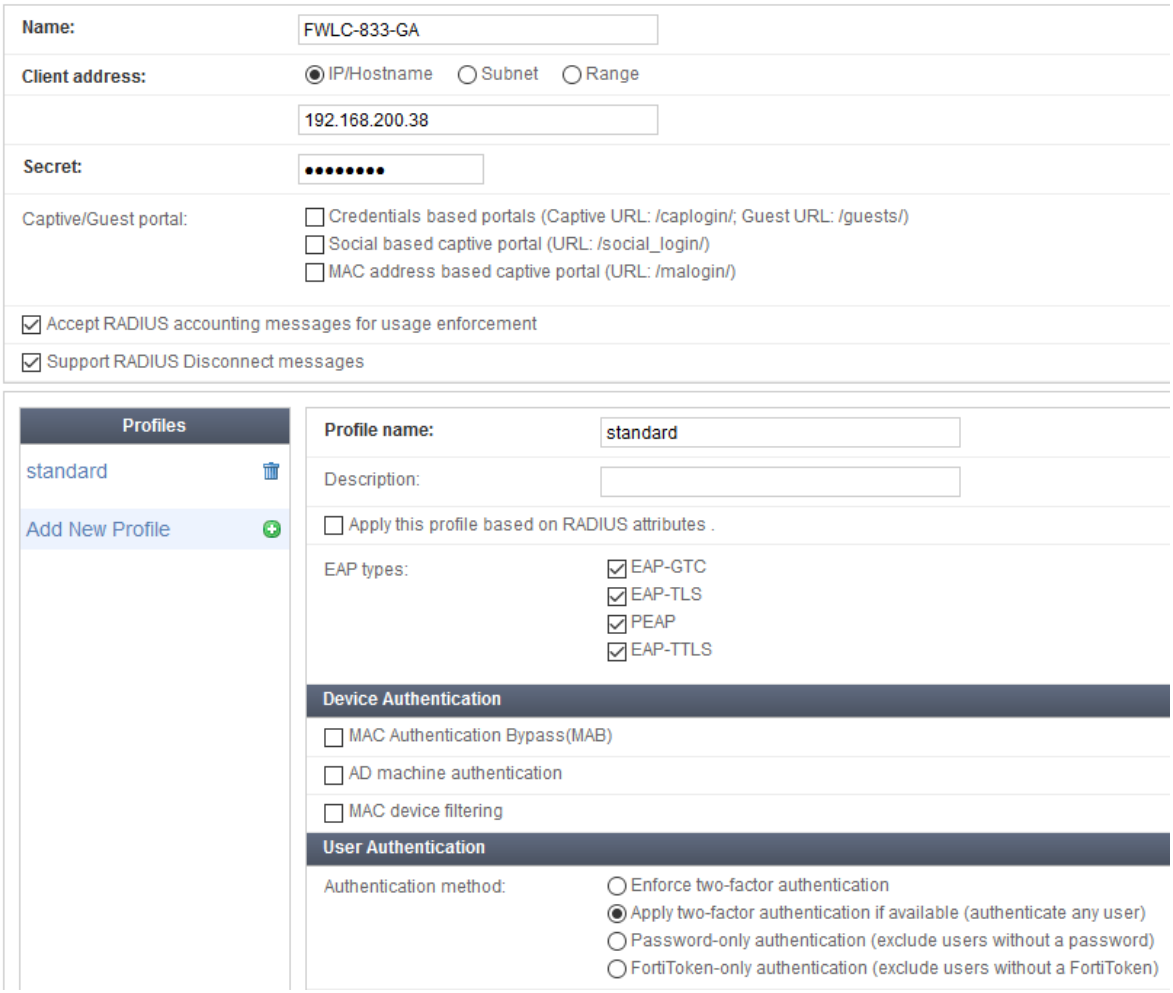
1. On the FortiWLC, go to **Configuration > Wireless > ESS** and **ADD** an ESS profile.
   Configure the profile with an appropriate **ESS Profile** and **SSID**. Then select the **Security Profile** that

contains the Captive Portal settings.



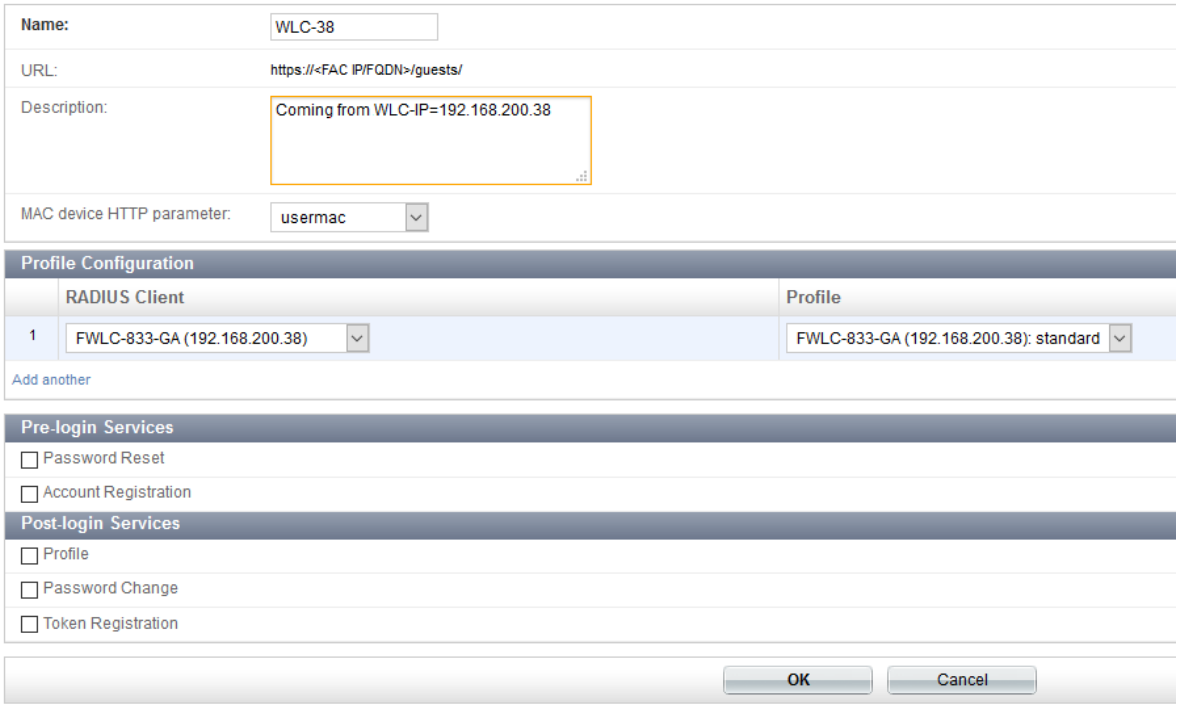
Creating FortiWLC as RADIUS Client on the FortiAuthenticator

1. On the FortiAuthenticator, go to **Authentication > RADIUS Service > Clients** and create a new client.
   Set **Client address** to **IP/Hostname** and enter the FortiWLC management IP as the IP address.
   Set the same **Secret** that was entered during the RADIUS configuration on the FortiWLC.
   Set a new **First profile name** and enable the **EAP types**.
   Under **Realms**, select the realms that are allowed.



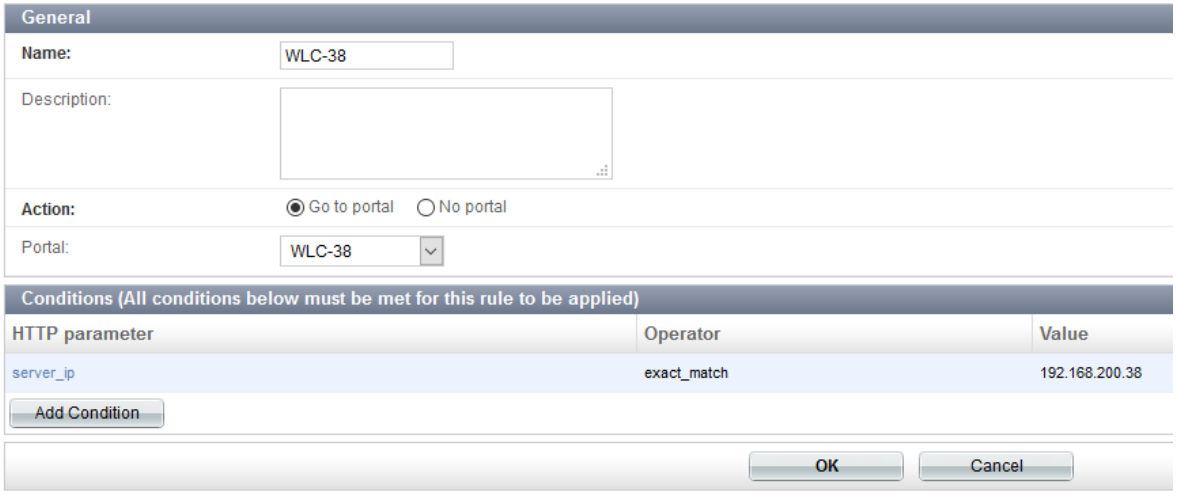
Creating the Guest Portal on the FortiAuthenticator

1. On the FortiAuthenticator, go to **Authentication > Guest Portals > Portals** and create a new portal. Under **Profile Configuration** select the RADIUS profile created earlier.



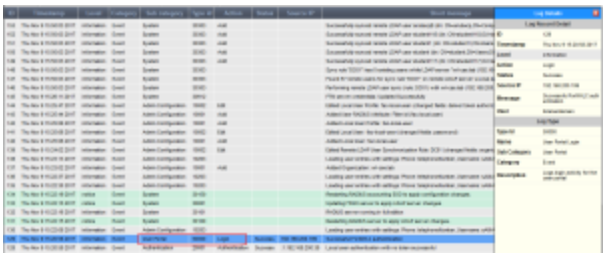
Creating the Portal Rule on the FortiAuthenticator

1. On the FortiAuthenticator, go to **Authentication > Guest Portals > Rules** and create a new rule. Set **Action** to **Go to portal** and select the portal created earlier. Select **OK**.
   Once the rule is created, select **Add Condition** and create the following HTTP parameter. This will be used to determine which portal to show (used for instances with multiple portals from different FortiWLC's and or Client IP subnets).



Results

1. Connect a client to the SSID created on the FortiWLC, then log in to the portal with the correct username and password.
   On the FortiAuthenticator, you can go to **Authentication > User Management > Local Users** to create local user accounts.
2. To confirm the successful log in, on FortiAuthenticator, go to **Logging > Log Access > Logs**.
   Find the line showing **User Portal** at **Sub Category**.

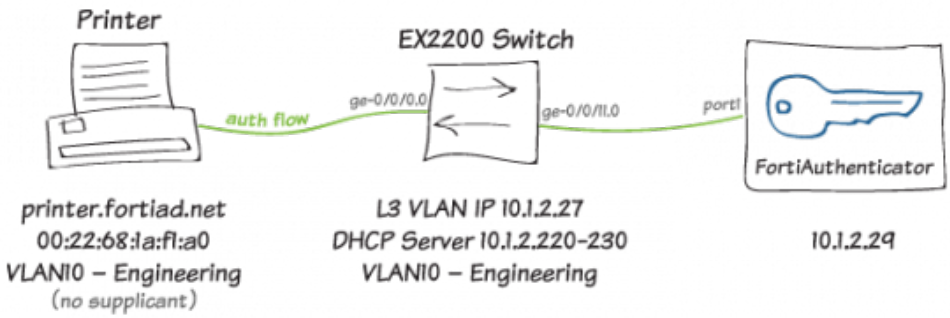


3. To confirm the successful log in, on FortiWLC, go to **Monitor > Devices > All Stations** and find the device showing the authenticated user.

MAC authentication bypass

This section describes configuring MAC address bypass with FortiAuthenticator.

MAC authentication bypass with dynamic VLAN assignment

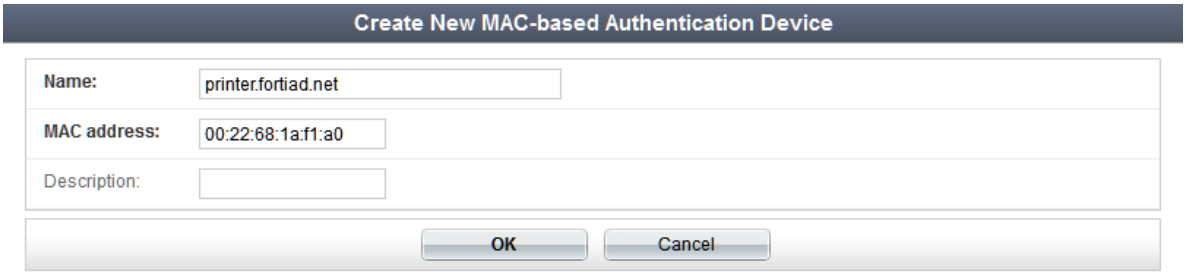


In this recipe, you will configure MAC authentication bypass in a wired network with dynamic VLAN assignment.

The purpose of this recipe is to configure and demonstrate MAC address bypass with FortiAuthenticator, using a 3rd-party switch (EX2200) to confirm cross-vendor interoperability. The recipe also demonstrates dynamic VLAN allocation without a supplicant.

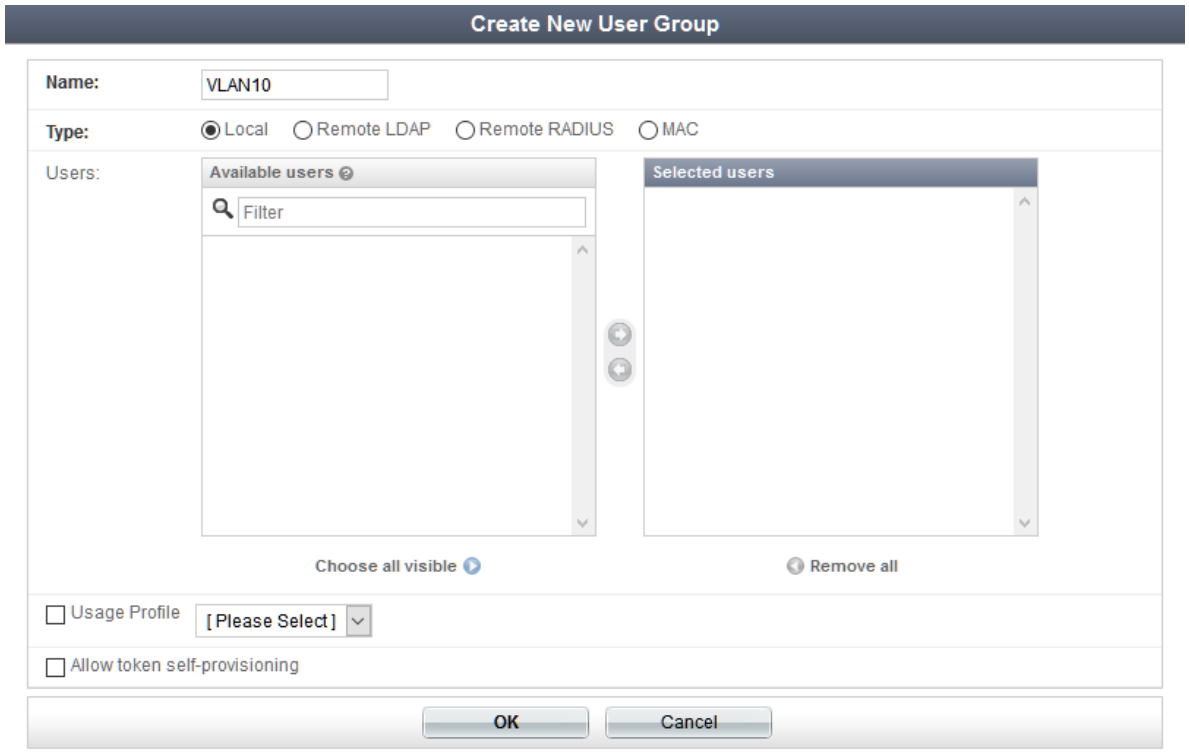
Configuring MAC authentication bypass on the FortiAuthenticator

1. Go to **Authentication > User Management > MAC Devices** and create a new MAC-based device. Alternatively, you can use the **Import** option to import from a CSV file.

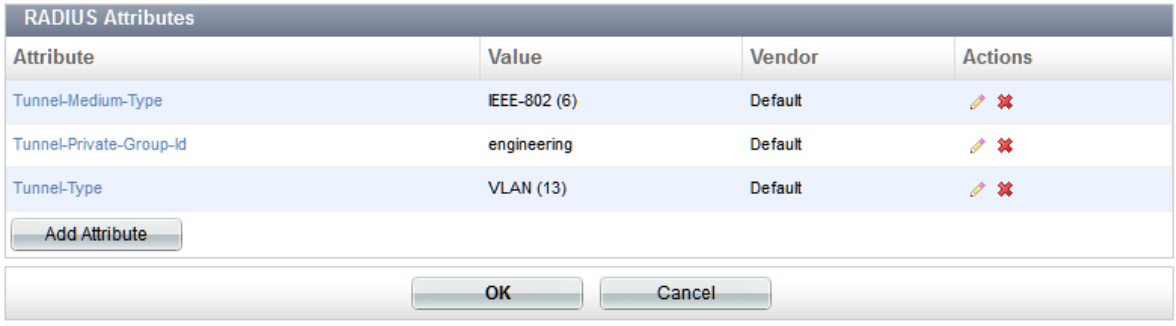


Configuring the user group

1. Go to **Authentication > User Management > User Groups** and create a new user group.
   No members are required; MAC-based authentication devices are automatically linked with this group.



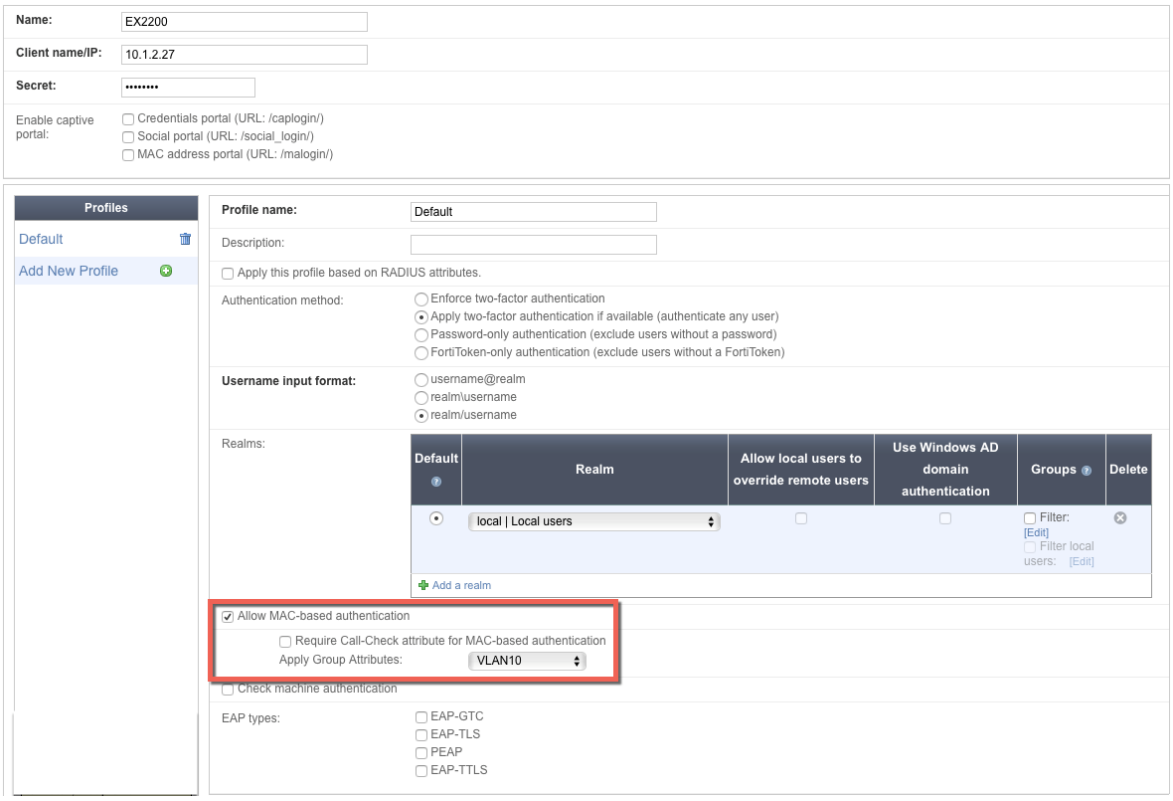
Add the **RADIUS Attributes** shown. Note that RADIUS attributes can only be added after the group has been created.



Configuring the RADIUS client

1. Go to **Authentication > RADIUS Service > Clients** and create a new RADIUS client. Configure the switch IP and shared secret.
   Use the **Local** realm.

Allow **MAC-based authentication** and link the group created earlier.



Configuring the 3rd-party switch

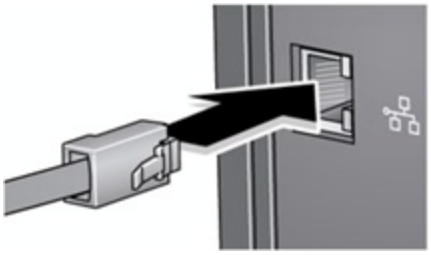
The switch configuration provided below is intended for demonstration only. Your switch configuration is likely to differ significantly.

```
set system services dhcp pool 10.1.2.0/24 address-range low 10.1.2.220
set system services dhcp pool 10.1.2.0/24 address-range high 10.1.2.230
set system services dhcp pool 10.1.2.0/24 domain-name fortiad.net
set system services dhcp pool 10.1.2.0/24 name-server 10.1.2.122
set system services dhcp pool 10.1.2.0/24 router 10.1.2.1
set system services dhcp pool 10.1.2.0/24 server-identifier 10.1.2.27
set interfaces ge-0/0/0 unit 0 family ethernet-switching #no vlan assigned to printer
     port, this will be allocated based on Group attributes
set interfaces ge-0/0/11 unit 0 family ethernet-switching vlan members engineering
     #interface used to communicate with FortiAuthenticator
set interfaces vlan unit 10 family inet address 10.1.2.27/24
set protocols dot1x authenticator authentication-profile-name profile1
set protocols dot1x authenticator interface ge-0/0/0.0 mac-radius restrict #forces mac
     address as username over RADIUS
set access radius-server 10.1.2.29 secret "$9$kmfzIRSlvLhSLNVYZGk.Pf39"
set access profile profile1 authentication-order radius
set access profile profile1 radius authentication-server 10.1.2.29
set vlans engineering vlan-id 10
set vlans engineering l3-interface vlan.10
```

No configuration is required on the endpoint.

Results

1. Connect the wired device (in this case, the printer).



2. Using `tcpdump`, FortiAuthenticator shows receipt of an Incoming Authentication Request (`tcpdump host 10.1.2.27 -nnvvXs`):

```
tcpdump: listening on port1, link-type EN10MB (Ethernet), capture size 262144 bytes
17:36:19.110399 IP (tos 0x0, ttl 64, id 18417, offset 0, flags [none], proto UDP
      (17), length 185)
   10.1.2.27.60114 > 10.1.2.29.1812: [udp sum ok] RADIUS, length: 157
      Access-Request (1), id: 0x08, Authenticator: b77fe0657747891fc8d53ae0ad2b0e7a
         User-Name Attribute (1), length: 14, Value: 0022681af1a0 #Switch forces
               username to be endpoint MAC address, no configuration needed on
               endpoint
            0x0000: 3030 3232 3638 3161 6631 6130
         NAS-Port Attribute (5), length: 6, Value: 70
            0x0000: 0000 0046
         EAP-Message Attribute (79), length: 19, Value: .
            0x0000: 0200 0011 0130 3032 3236 3831 6166 3161
            0x0010: 30
         Message-Authenticator Attribute (80), length: 18, Value: .y{.j.%..9|es.'x
            0x0000: a679 7b82 6344 2593 f639 7c65 73eb 2778
         Acct-Session-Id Attribute (44), length: 24, value: 802.1x81fa002500078442
            0x0000: 384f 322e 3178 3831 6661 3030 3235 3030
            0x0010: 3037 3834 3432
         NAS-Port-rd Attribute (87), length: 12, Value: ge-0/0/0.0
            0x0000: 6765 2430 2f30 2f30 2e30
         Calling-Station-Id Attribute (31), length: 19, value: 00-22-68-1a-fl-a0
            0x0000: 3030 2032 3220 3638 2031 6120 6631 2461
            0x0010: 30
         Called-Station-Id Attribute (30), length: 19, Value: a8-40-e5-b0-21-80
            0x0000: 6138 2464 3024 6535 2d62 302d 3231 2d38
            0x0010: 30
         NAS-Port-Type Attribute (61), length: 6, value: Ethernet
            0x0000: 0000 000f
```

3. On the FortiAuthenticator, go to **Logging > Log Access > Logs** to verify the device authentication. The Debug Log (at `https://<fac-ip>/debug/radius`) should also confirm successful authentication.

Log Details	
Log Record Detail	
ID	1479
Timestamp	Sun Sep 25 17:36:19 2016
Level	information
Action	Authentication
Status	Success
NAS Name/IP	10.1.2.27
Message	MAC-based authentication successful
User	printer.fortiad.net
Log Type	
Type Id	20400
Name	MAC Authentication OK
Sub Category	Authentication
Category	Event
Description	MAC-based authentication successful

4. Continuing with `tcpdump`, authentication is accepted from FortiAuthenticator and authorization attributes returned to the switch:

```
17:36:19.115264 IP (tos 0x0, ttl 64, id 49111, offset 0, flags [none], proto UDP
      (17), length 73)
   10.1.2.29.1812 > 10.1.2.27.60114: (bad udp cksum 0x1880 -> 0x5ccel] RADIUS,
         length: 45
      Access-Accept (2), id: 0x08, Authenticator: b5c7b1bb5a316fb483a622eaae58ccc2
         Tunnel-Type Attribute (64), length: 6, Value: Tag[Unused] #13
            0x0000: 0000 000d
         Tunnel-Medium-Type Attribute (65), length: 6, Value: Tag[Unused] 802
            0x0000: 0000 0006
         Tunnel-Private-Group-ID Attribute (81), length: 13, Value: engineering
            0x0000: 656e 6769 6e65 6572 696e 67
      0x0000: 4500 0049 bfd7 0000 4011 a293 0a01 021d E..I....@ .......
      0x0010: 0a01 021b 0714 ead2 0035 1880 0208 002d 5
      0x0020: b5c7 blbb 5a31 6fb4 83a6 22ea ae58 ccc2 ....21o..."..X..
      0x0030: 4006 0000 0000 4106 0000 0006 510d 656e @ A Q en
      0x0040: 6769 6e65 6572 696e 67 gineering
```

5. Post-authentication DHCP transaction is picked up by FortiAuthenticator (tcpdump continued):

```
17:36:22.955537 IP (tos 0x0, ttl 1, id 18546, offset 0, flags [none], proto UDP
      (17), length 328)
   10.1.2.27.67 > 255.255.255.255.68: judo sum ok] BOOTP/DHCP, Reply, length 300,
         xid 0x9fc8f40c, Flags (Broadcast] (0x8000)
      Your-IP 10.1.2.224
      Client-Ethernet-Address 00:22:68:1a:fl:a0
      Vendor-rfc1048 Extensions
            Magic Cookie 0x63825363
   DHCP-Message Option 53, length 1: ACK
   Server-ID Option 54, length 4: 10.1.2.27
   Lease-Time Option 51, length 4: 86400
   Subnet-Mask Option 1, length 4: 255.255.255.0
   Default-Gateway Option 3, length 4: 10.1.2.1
   Domain-Name-Server Option 6, length 4: 10.1.2.122
   Domain-Name Option 15, length 11: "fortiad.net"
```

The Switch CLI shows a successful dot1x session:

```
root# run show dotlx interface ge-0/0/0.0
```

```
802.1X Information:
Interface Role State MAC address User
ge-0/0/0.0 Authenticator Authenticated 00:22:68:1A:F1:A0 0022681af1a0
```

The MAC address interface has been dynamically placed into correct VLAN:

```
root# run show vlans engineering
Name Tag Interfaces
engineering 10
     ge-0/0/0.0*, ge-0/0/11.0*
```

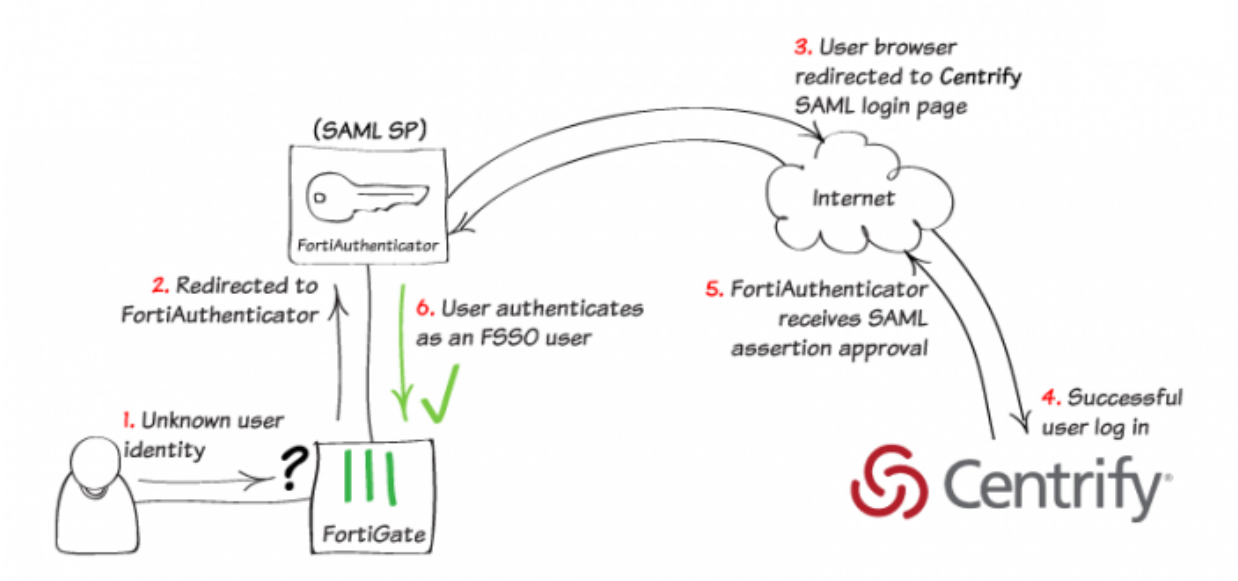
Additionally, the printer shows as available on the network:

```
root# run show arp interface vlan.10
MAC Address Address Name Interface Flags
00:0c:29:5b:90:68 10.1.2.29 10.1.2.29 vlan.10 none
6c:70:9f:d6:ae:al 10.1.2.220 10.1.2.220 vlan.10 none
b8:53:ac:4a:d5:f5 10.1.2.221 10.1.2.221 vlan.10 none
00:22:68:1a:fl:a0 10.1.2.224 10.1.2.224 vlan.10 none
a4:c3:61:24:b9:07 10.1.2.228 10.1.2.228 vlan.10 none
Total entries: 5

{master:0}[edit]
root* run ping 10.1.2.224
PING 10.1.2.224 (10.1.2.224): 56 data bytes
64 bytes from 10.1.2.224: icmp_seq=0 tt1=128 time=2.068 ms
64 bytes from 10.1.2.224: icmp_seq=1 tt1=128 time=2.236 ms
64 bytes from 10.1.2.224: icmp_seq=2 tt1=128 time=2.699 ms

--- 10.1.2.224 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max/stddev = 2.068/2.334/2.699/0.267 ms
```

SAML authentication

Security Assertion Markup Language (SAML) is used for exchanging authentication and authorization data between an identity provider (IdP) and a service provider (SP), such as Google Apps, Office 365, and Salesforce. The FortiAuthenticator can be configured as an IdP, providing trust relationship authentication for unauthenticated users trying to access an SP.

SAML 2.0 FSSO with FortiAuthenticator and Centrify



In this example, you will provide a Security Assertion Markup Language (SAML) FSSO cloud authentication solution using FortiAuthenticator with Centrify Identity Service, a cloud-based or on-premises service. This solution can help mitigate one of the leading points of attack in data breaches: compromised credentials. The FortiAuthenticator will act as the service p[rovider (SP) and Centrify as the identity provider (IdP).

Centrify Identity Service improves end-user productivity and secures access to cloud, mobile, and on-premises apps via SSO, user provisioning, and multi-factor authentication.

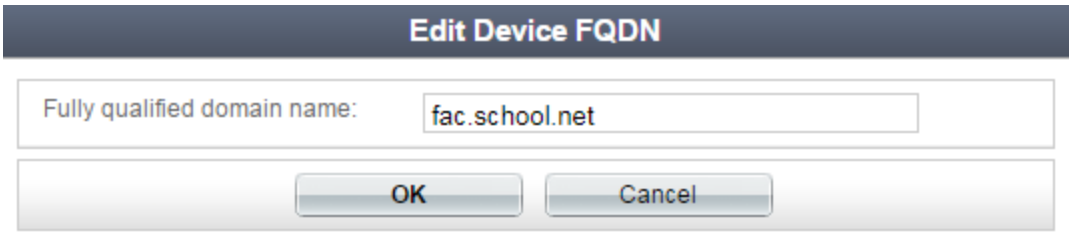
This configuration assumes that you have already created a Centrify tenant admin account, and added a local and an SSO user group to FortiAuthenticator both called **saml_users**.

.

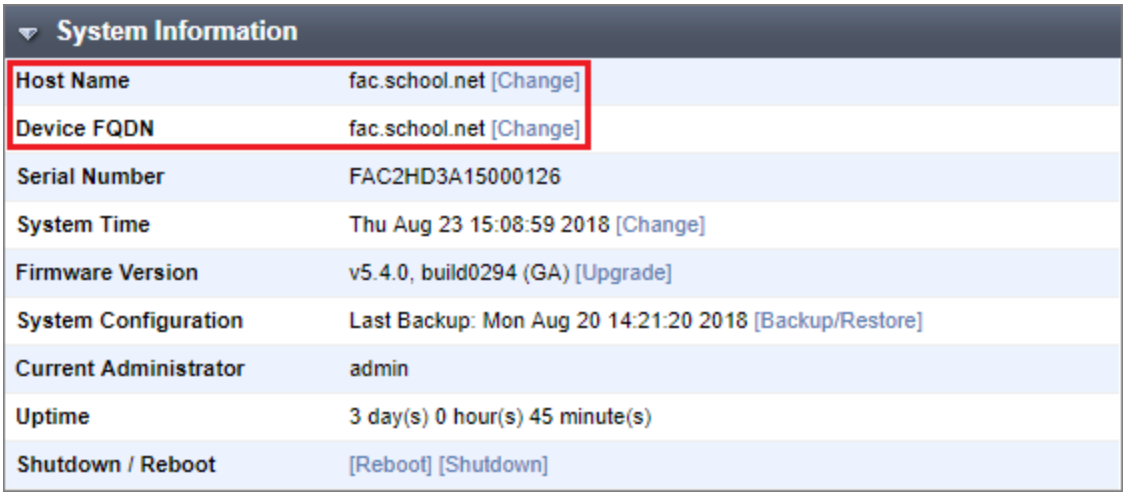
Configuring DNS and FortiAuthenticator's FQDN

1. On the FortiAuthenticator, go to **System > Dashboard > Status**. In the **System Information** widget, select **Change** next to **Device FQDN**.

Enter a domain name (in this example, *fac.school.net*). This will help identify where the FortiAuthenticator is located in the DNS hierarchy.



2. Enter the same name for the **Host Name**. This is so you can add the unit to the FortiGate's DNS list, so that the local DNS lookup of this FQDN can be resolved.

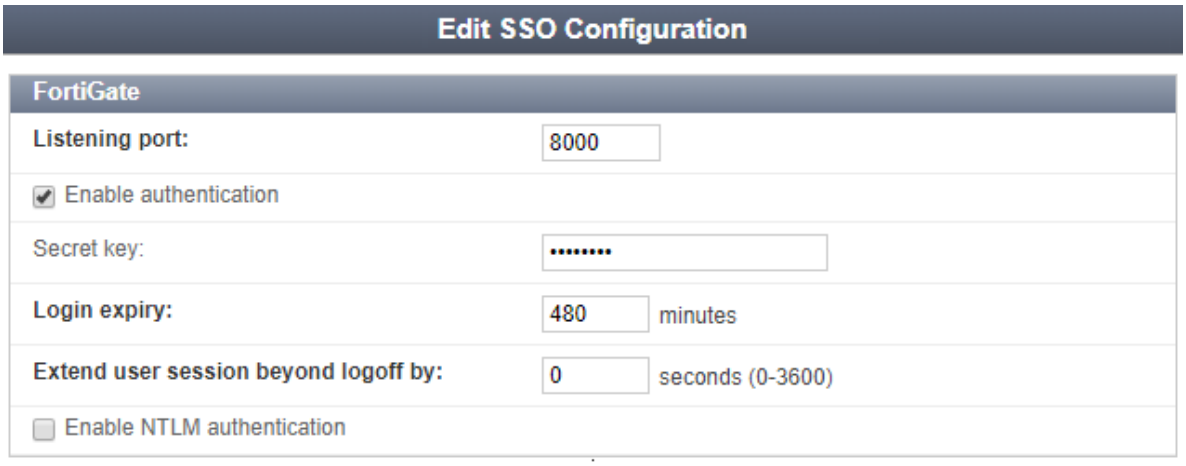


3. On the FortiGate, open the **CLI Console** and enter the following command, entering the FortiAuthenticator's host name and Internet-facing IP address:

```
config system dns-database
   edit school.net
      config dns-entry
         edit 1
            set hostname fac.school.net
            set ip 172.25.176.141
         next
      end
      set domain school.net
   next
end
```

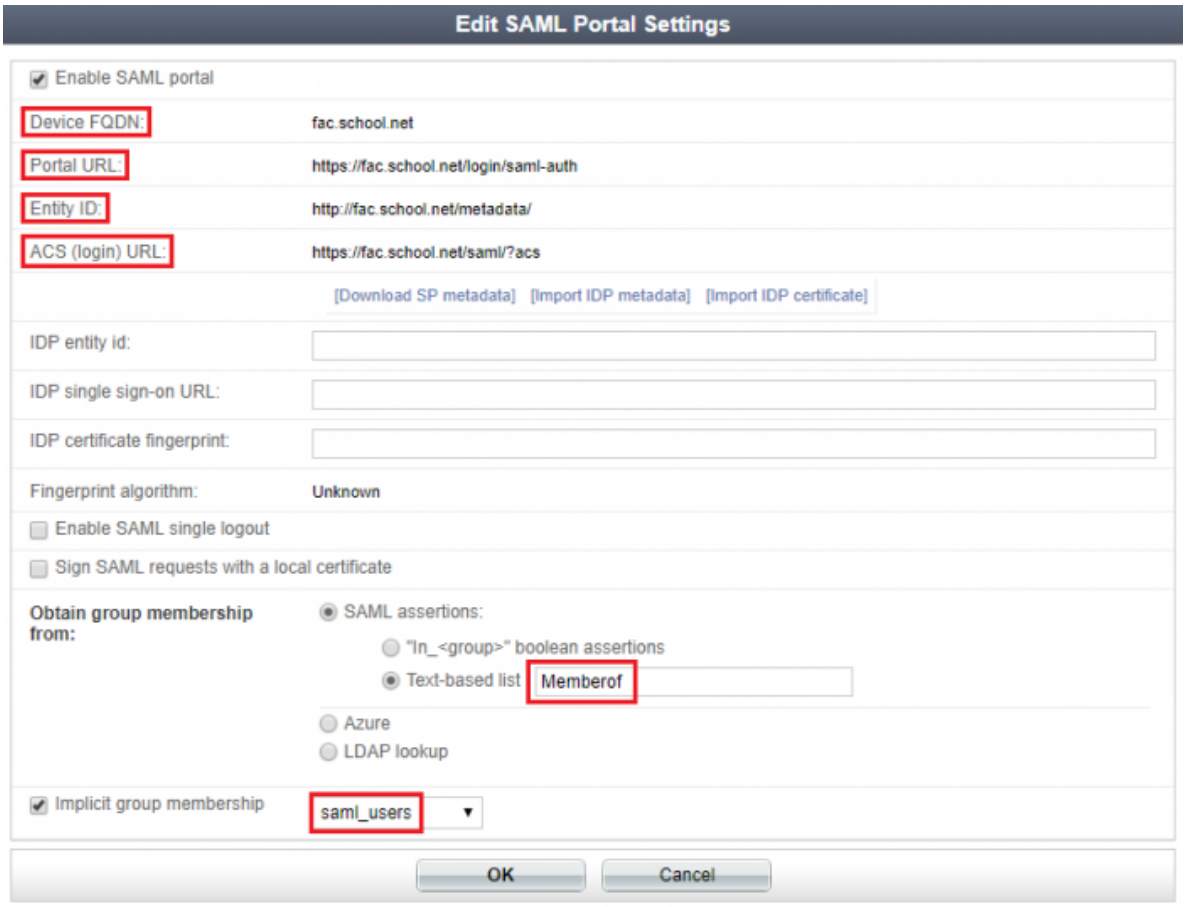
Enabling FSSO and SAML on the FortiAuthenticator

1. On the FortiAuthenticator, go to **Fortinet SSO Methods > SSO > General** and set FortiGate SSO options. Make sure to **Enable authentication**.
   Enter a **Secret key** and select **OK** to apply your changes. This key will be used on the FortiGate to add the FortiAuthenticator as the FSSO server.



2. Then go to **Fortinet SSO Methods > SSO > SAML Authentication** and select **Enable SAML portal**. All necessary URLs are automatically generated:
   - **Portal URL** - Captive Portal URL for the FortiGate and user.
   - **Entity ID** - Used in the Centrify SAML IdP application setup.
   - **ACS (login) URL** - Assertion POST URL used by the SAML IdP.

   Enable **Text-based list** under **SAML assertions** and enter **Memberof** in the field provided. This attribute will be configured later on the Centrify tenant to be included in the SAML response to the FortiAuthenticator.
3. Enable **Implicit group membership** and assign the **saml_users** group from the drop-down menu. This will place SAML authenticated users into this group.

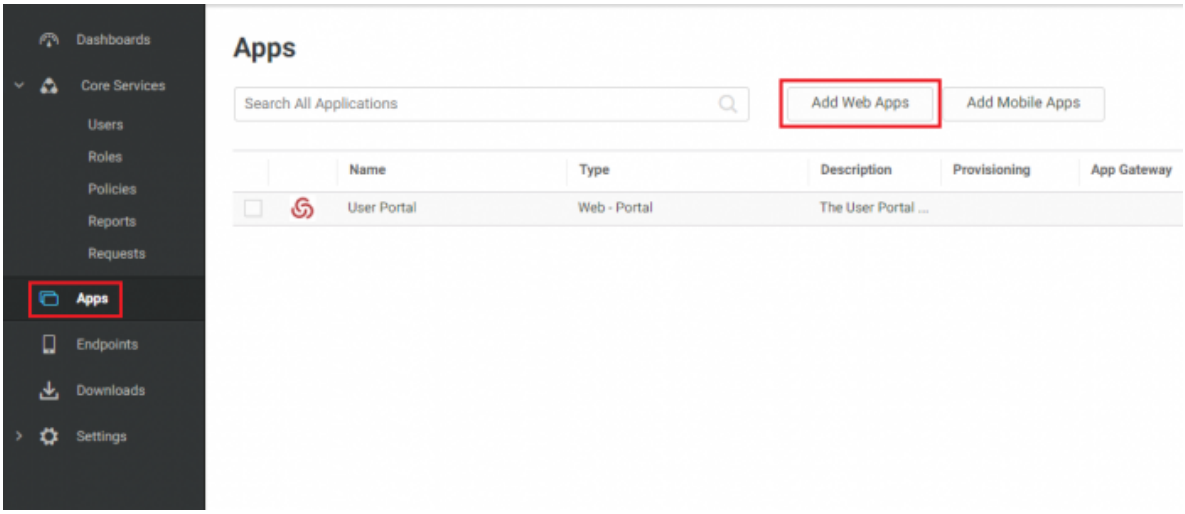


Keep this window open as these URLs will be needed during the IdP application configuration and for testing.

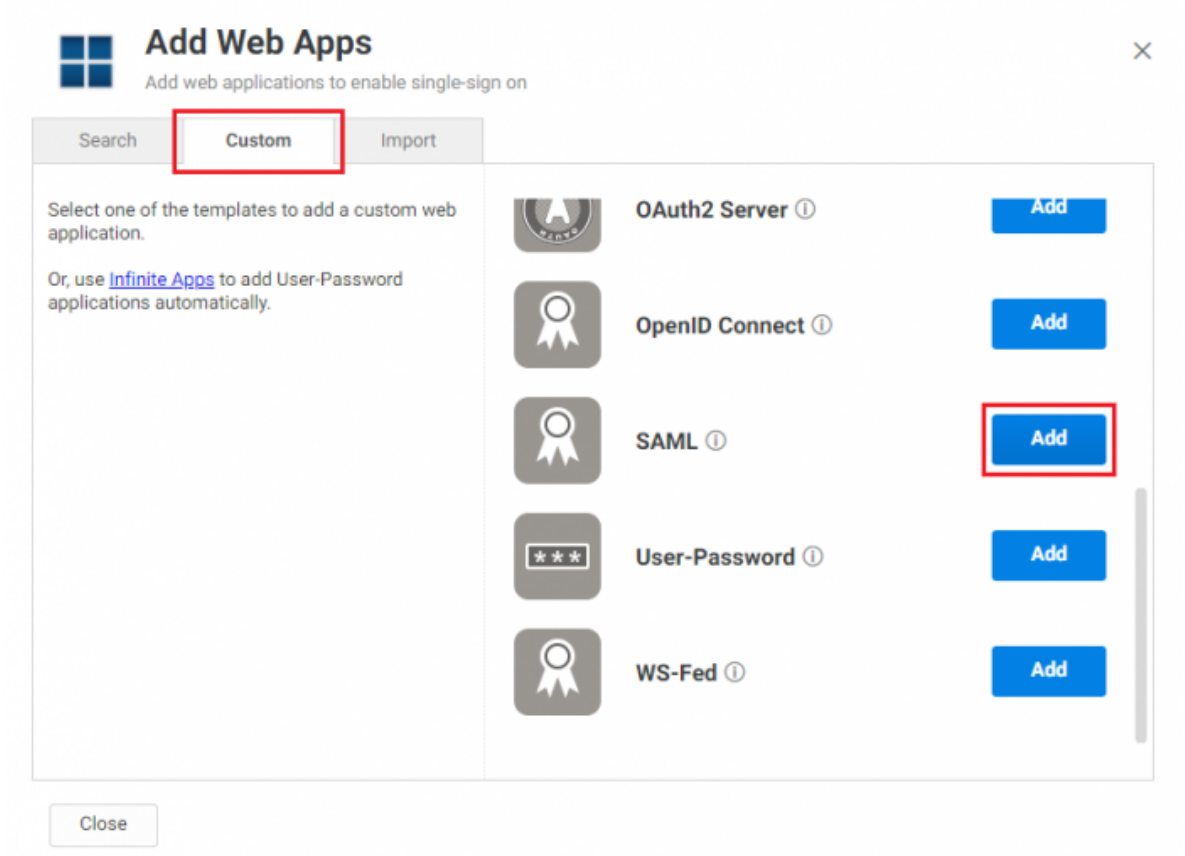
Note that, at this point, you will not be able to save these settings, as the IdP information — **IDP entity id**, **IDP single sign-on URL**, and **IDP certificate fingerprint** — needs to be entered. These fields will be filled once the IdP application configuration is complete.

Adding SAML connector to Centrify for IdP metadata

1. Login to the Centrify tenant as an administrator and go to **Apps > Add Web Apps**.

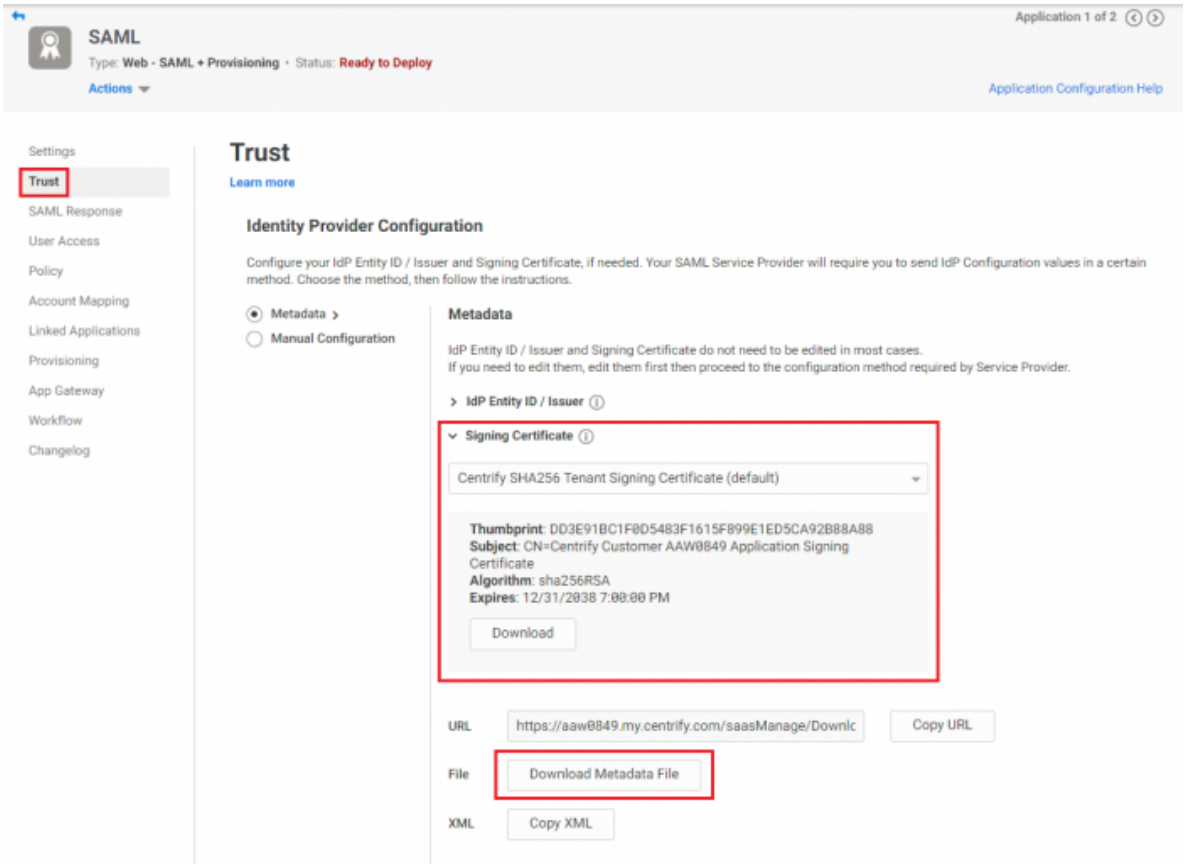


2. Under the **Custom** tab, scroll down to **SAML** and select **Add**. Select **Yes** to agree to add the SAML web app and then select **Close**.

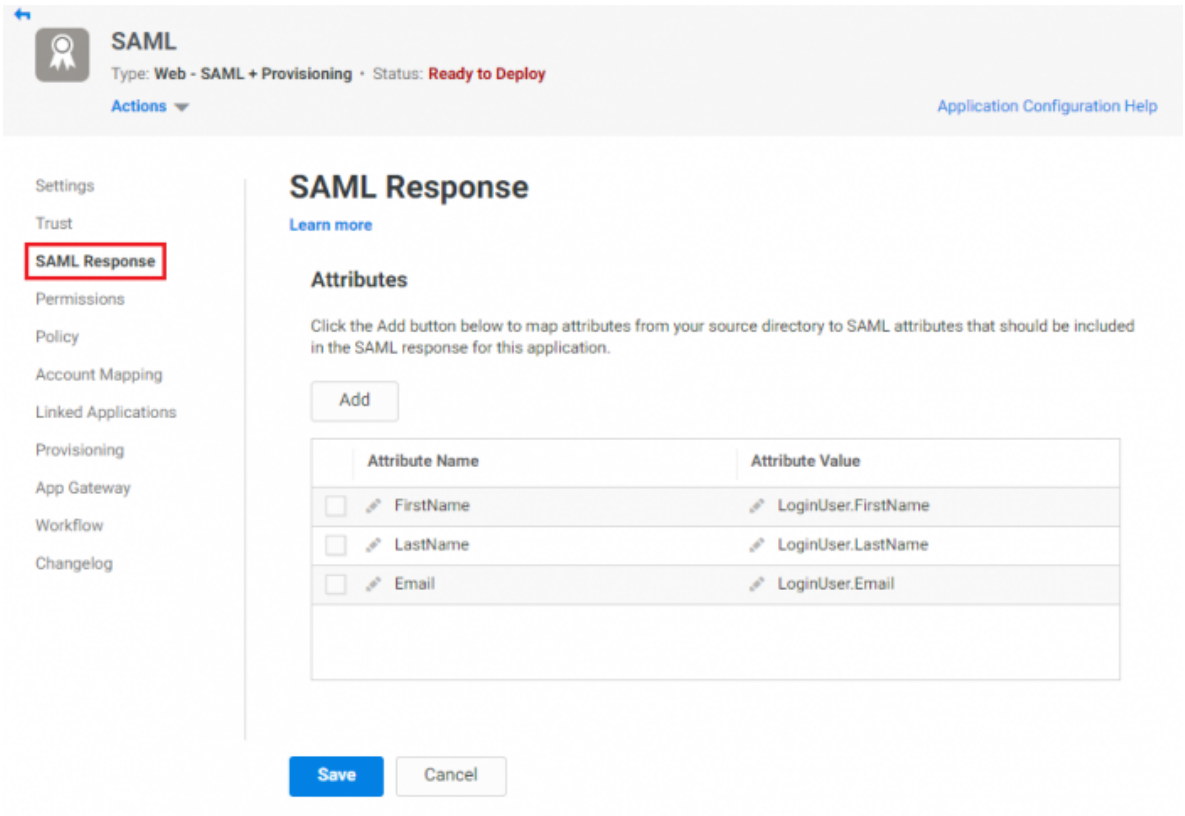


3. The SAML configuration page will open automatically onto the **Settings** tab.
Go to **Trust** to view the **Identity Provider Configuration** section. Select the **Signing Certificate** drop-down and **Download** both the Centrify signing certificate and the metadata file – these will be uploaded to

the FortiAuthenticator.

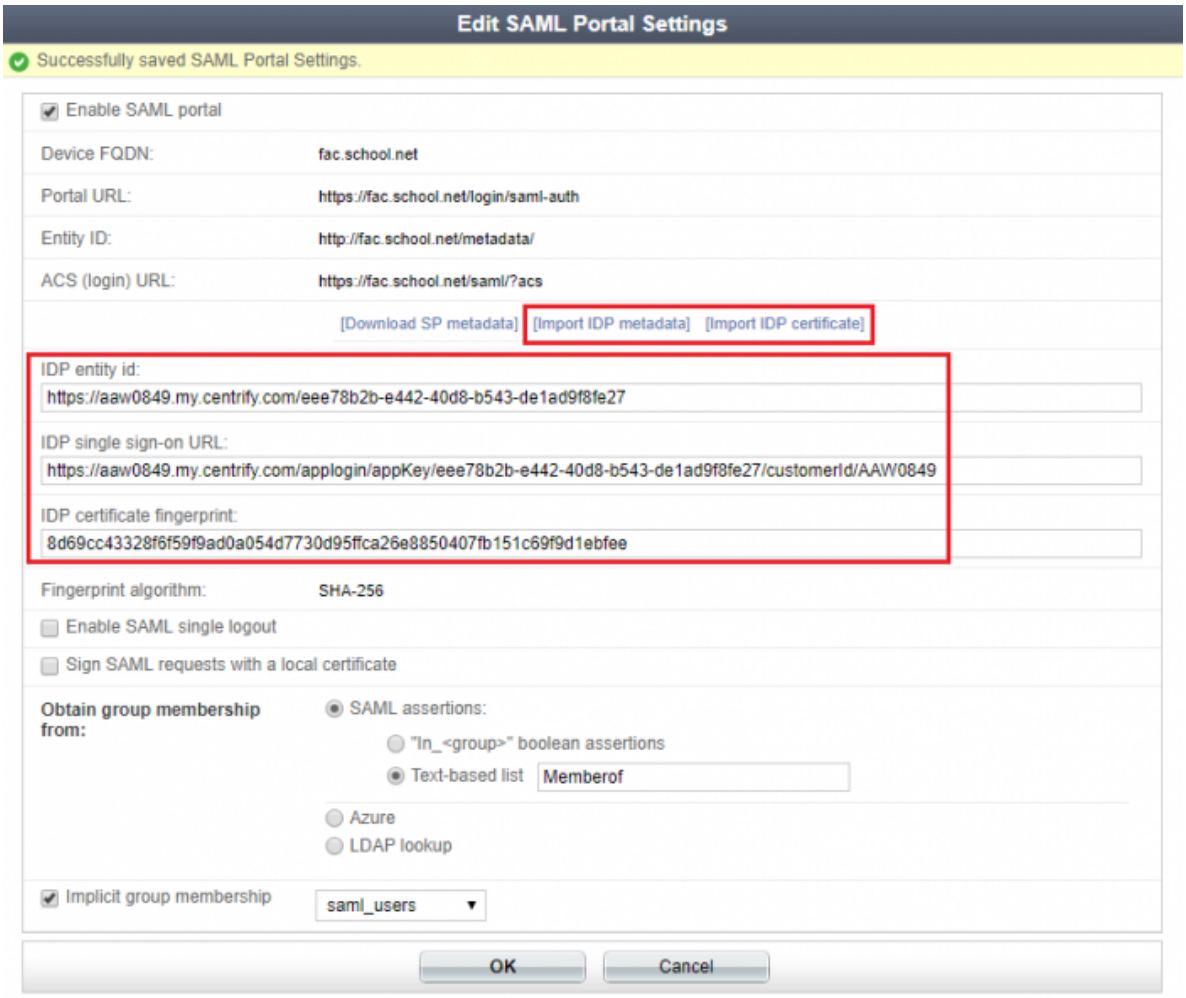


4. Then go to **SAML Response** and select **Add**.
   Add the **FirstName**, **LastName**, **Email**, and **Memberof** user attributes. Then select **Save**.

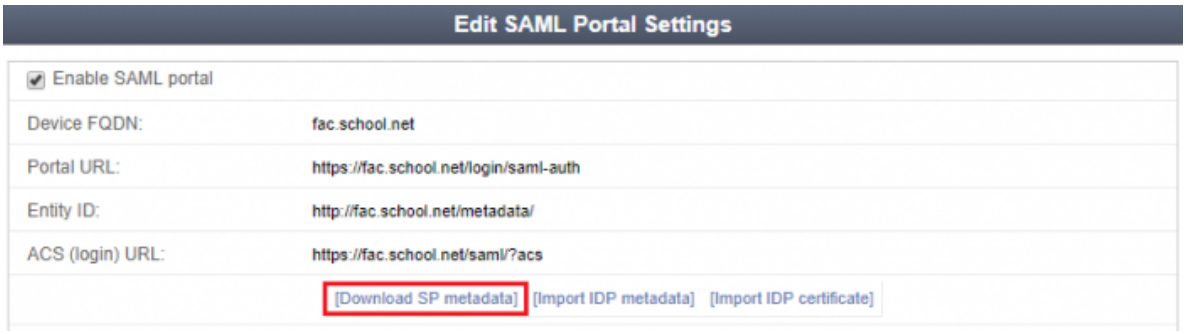


Importing the IdP certificate and metadata on the FortiAuthenticator

1. On the FortiAuthenticator, go to **Fortinet SSO Methods > SSO > SAML Authentication** and import the IdP metadata and certificate downloaded earlier.
   This will automatically fill the IdP fields (as shown in the example). Make sure to select **OK** to save these changes.

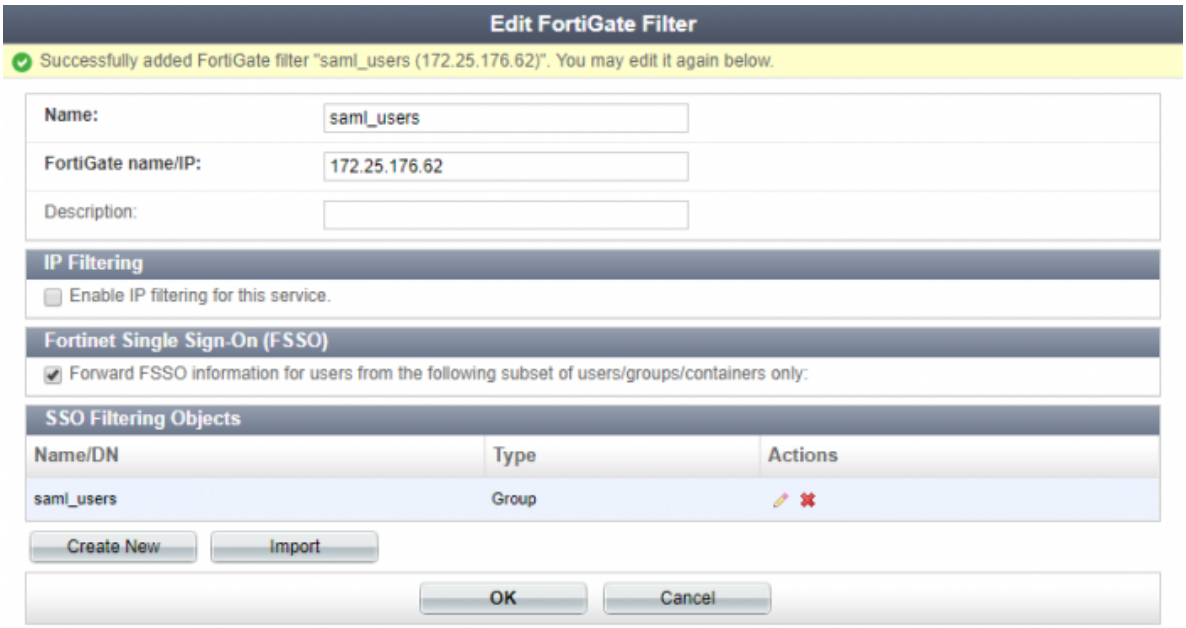


2. Select **Download SP metadata** – this will be uploaded to the Centrify tenant.



3. Then go to **Fortinet SSO Methods > SSO > FortiGate Filtering** and create a new FortiGate filter. Enter a name and the FortiGate's wan-interface IP address, and select **OK**.

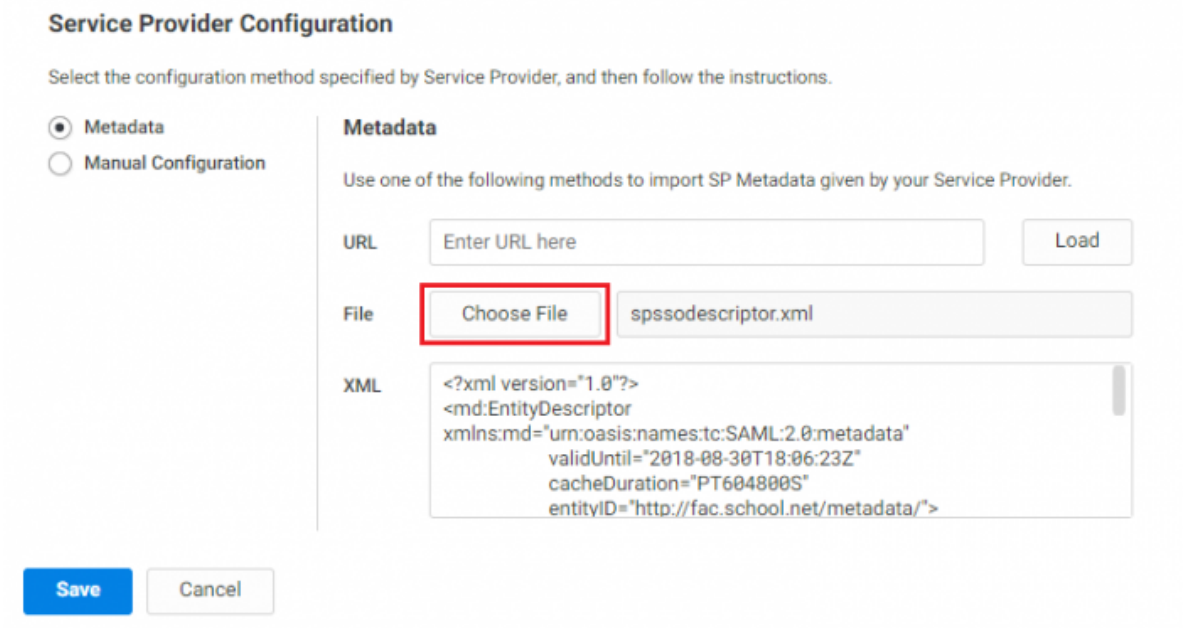
   Once created, enable **Fortinet Single Sign-On (FSSO)**. Select **Create New** to create an SSO group filtering object (as shown already created in the example), and select **OK** to apply all changes.



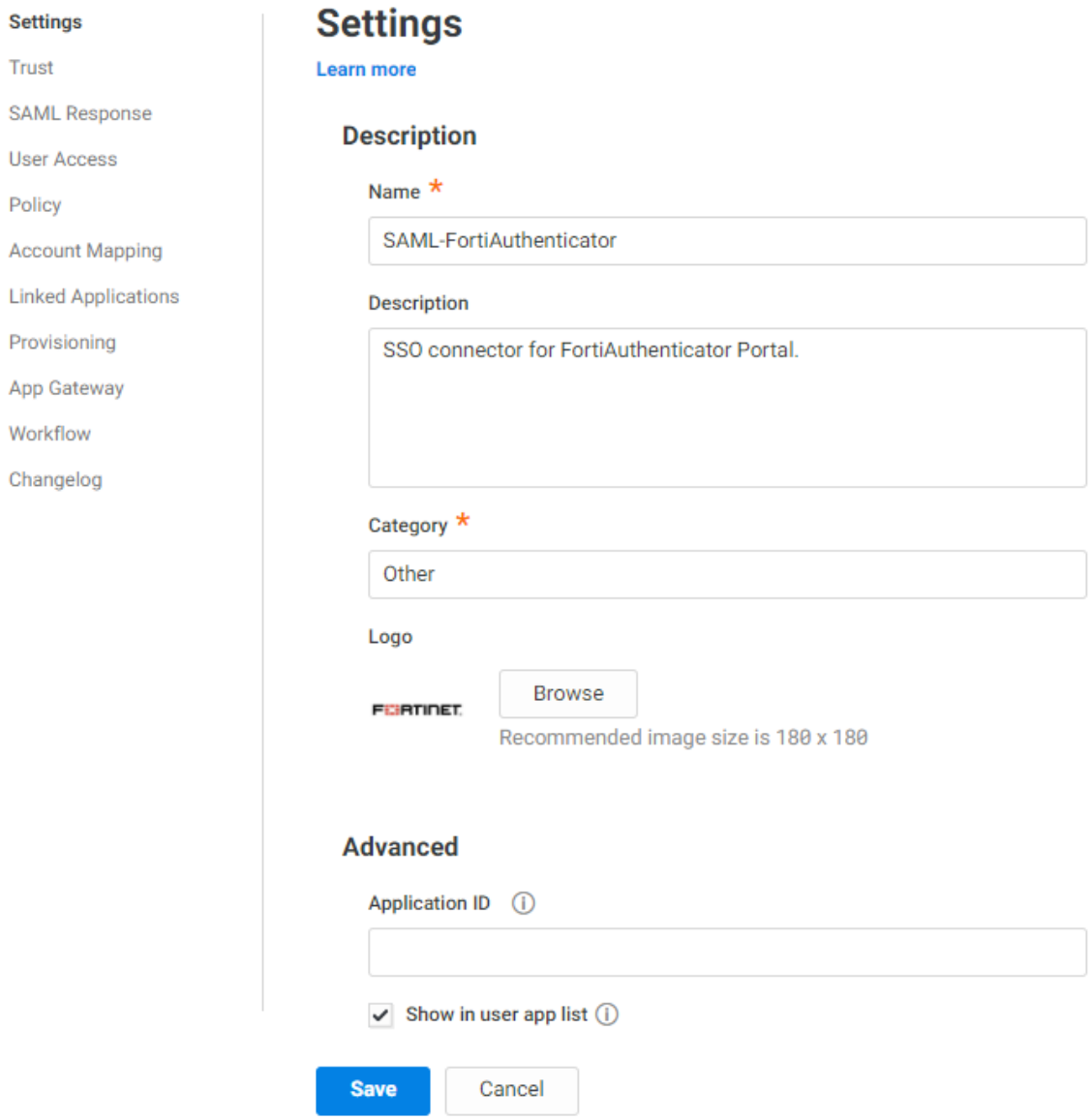
Note that the name entered for the filter must be the same as the group name created for SAML users (**saml_users**). The two user groups must have the exact same name or SSO information will not be pushed to the FortiGate.

Uploading the SP metadata to the Centrify tenant

1. On the Centrify tenant, back on the **Trust** tab, scroll down to the **Service Provider Configuration** section. Select **Choose File** to upload the SP metadata from the FortiAuthenticator.
Once uploaded, the XML box will automatically populate. Make sure to select **Save**.

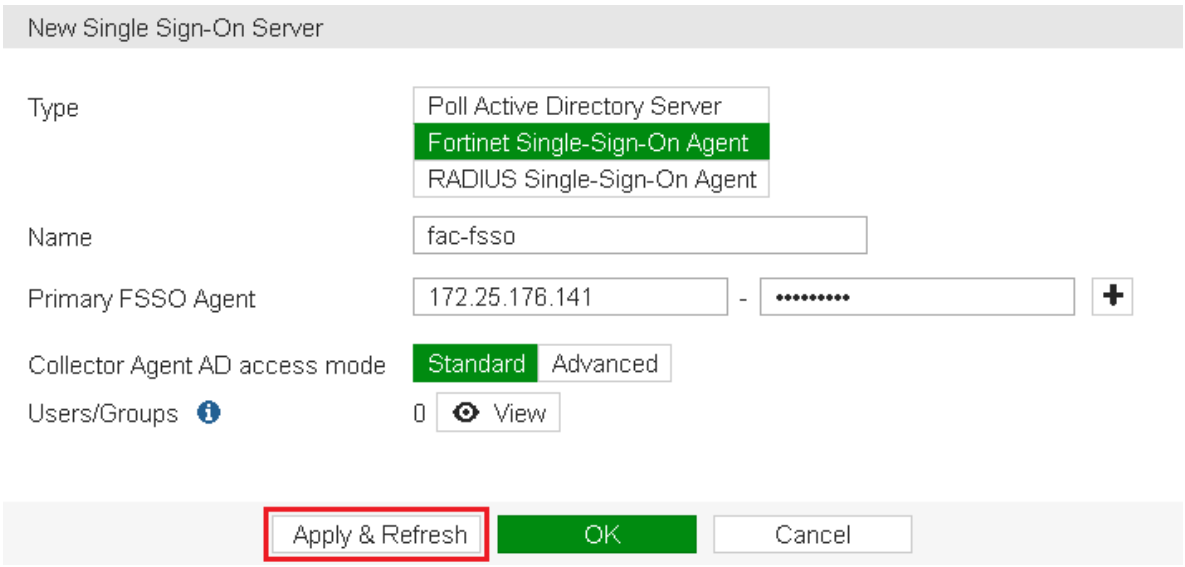


2. Optionally, you can go to **Settings** and enter a **Name** and **Description**. Then upload a custom **Logo** as required (as shown in the example). Again, be sure to select **Save**.

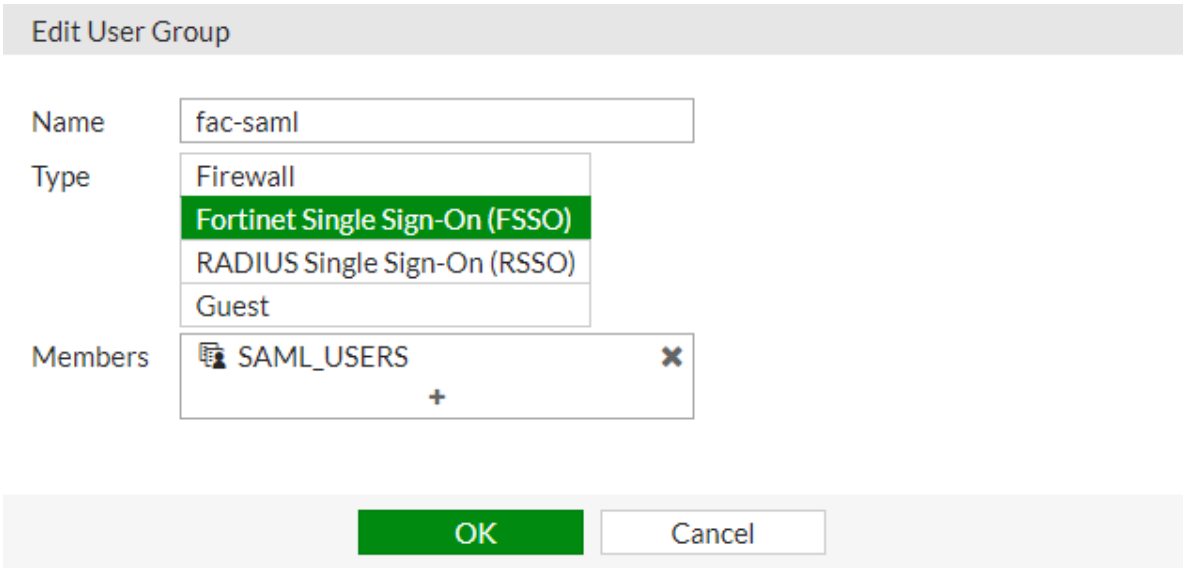


Configuring FSSO on the FortiGate

1. On the FortiGate, go to **User & Device > Single Sign-On** and select **Create New**.
   Set Type to **Fortinet Single-Sign-On Agent**, enter a **Name**, the FortiAuthenticator's Internet-interface IP address, and the password, which must match the secret key entered at the beginning of the FortiAuthenticator configuration process.
   Select **Apply & Refresh**.

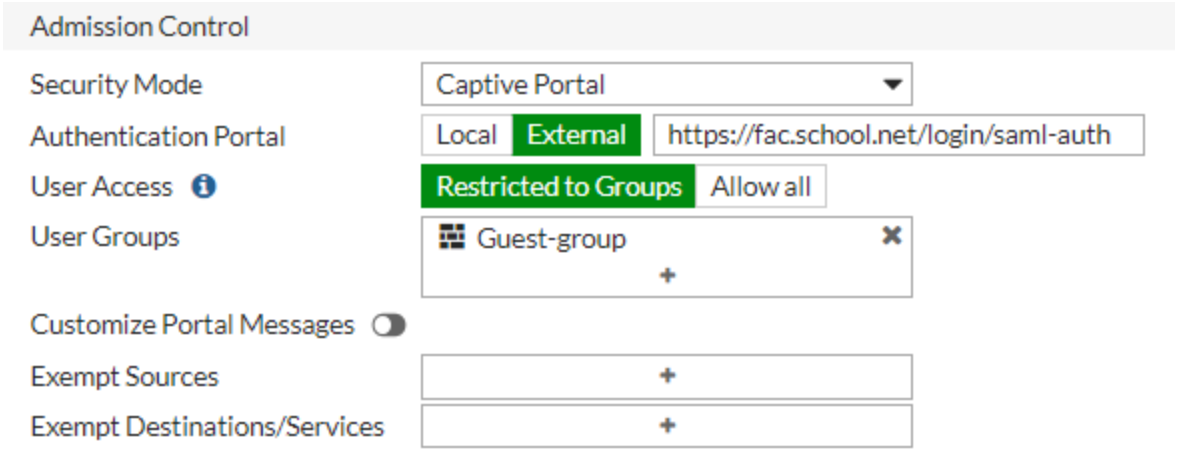


2. The SAML user group name has been successfully pushed to the FortiGate from the FortiAuthenticator, appearing when you select **View**.
   You may have to wait a few minutes before the user group appears.
3. Then go to **User & Device > User Groups** and create a new FSSO user group. Successfully authenticated users via SAML FSSO will be placed in this group.
   Enter a **Name**, set **Type** to **Fortinet Single Sign-On (FSSO)**, and add the FSSO group as a **Member**.

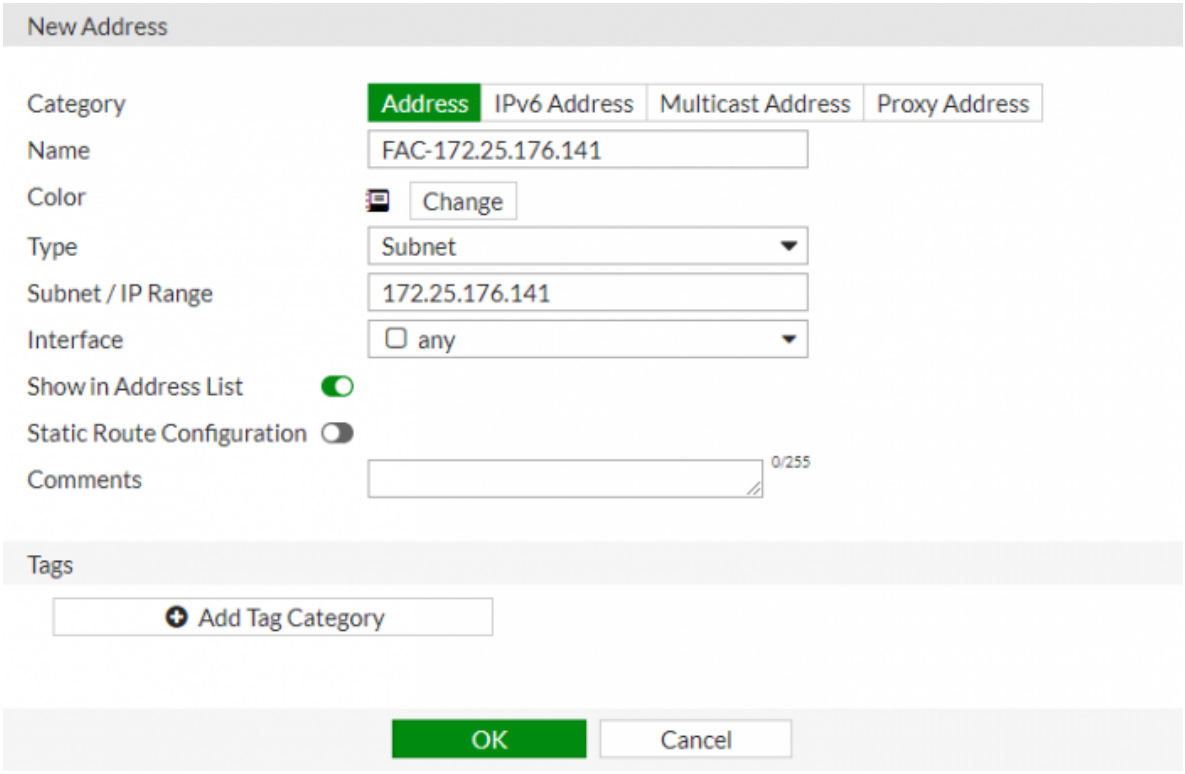


Configuring captive portal and security policies

1. On the FortiGate, go to **Network > Interfaces** and edit the internal interface.
   Under **Admission Control**, set **Security Mode** to **Captive Portal**.
   Set **Authentication Portal** to **External**, and enter the SAML authentication portal URL.
   Set **User Access** to **Restricted to Groups**, and set **User Groups** to any local group, as you'll notice the FSSO group is not available; this local group won't be used for access.



2. Next go to **Policy & Objects > Addresses** and add the FortiAuthenticator as an address object.

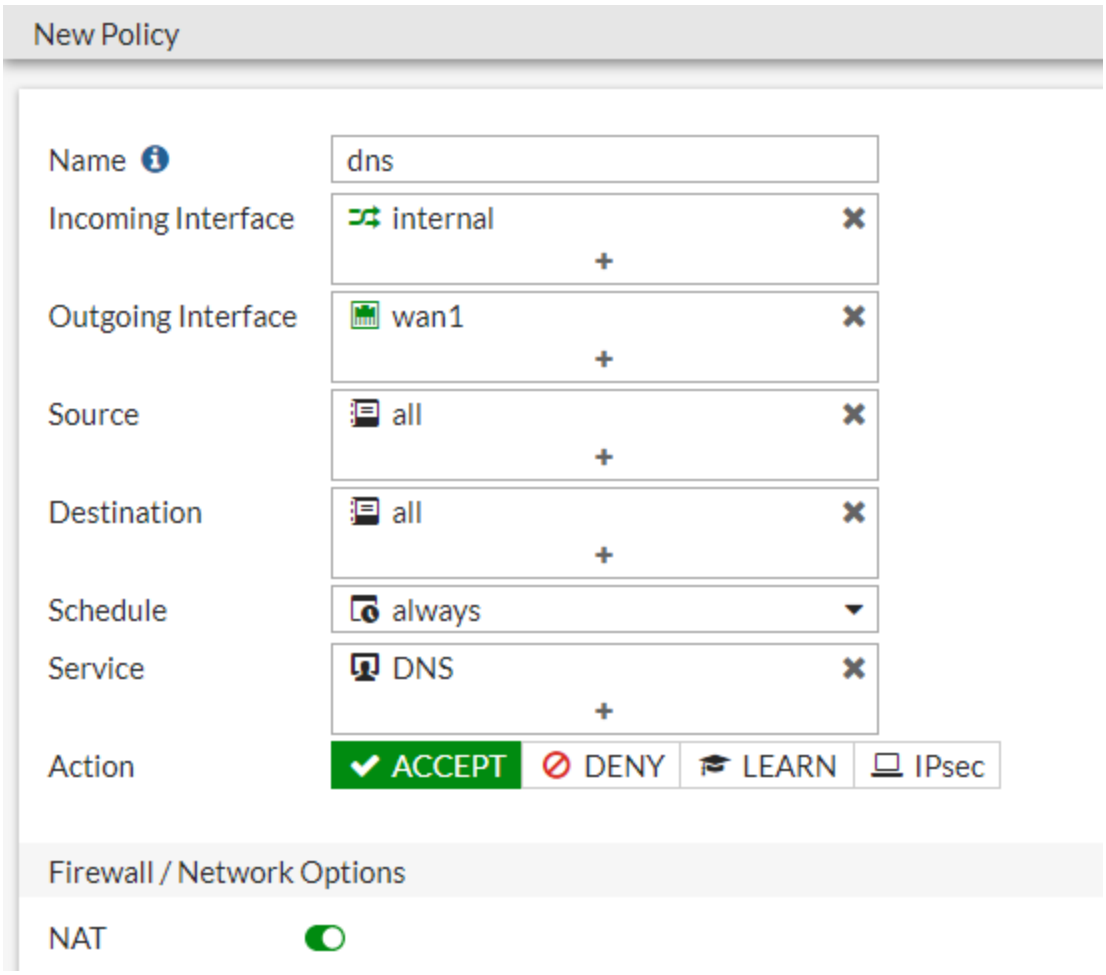


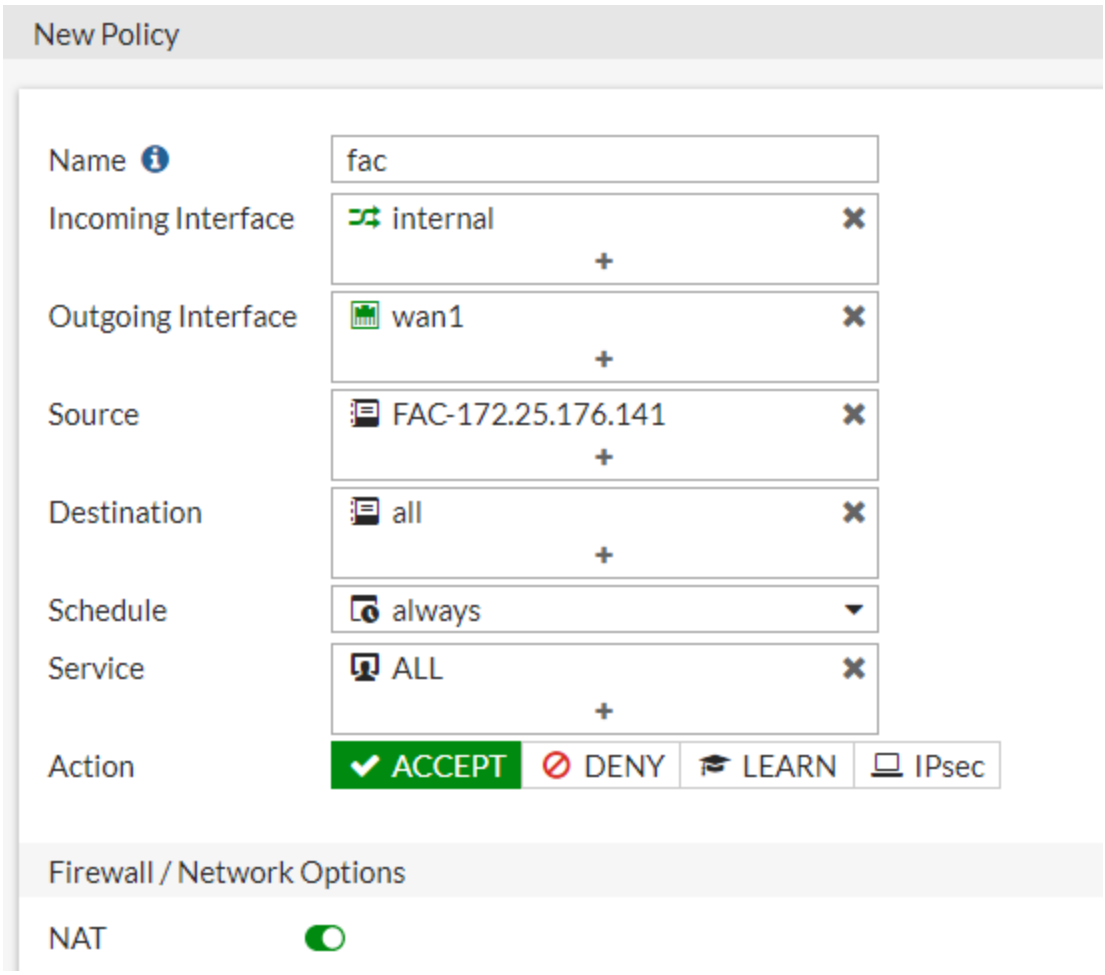
Then create an FQDN object of your Centrify tenant portal:

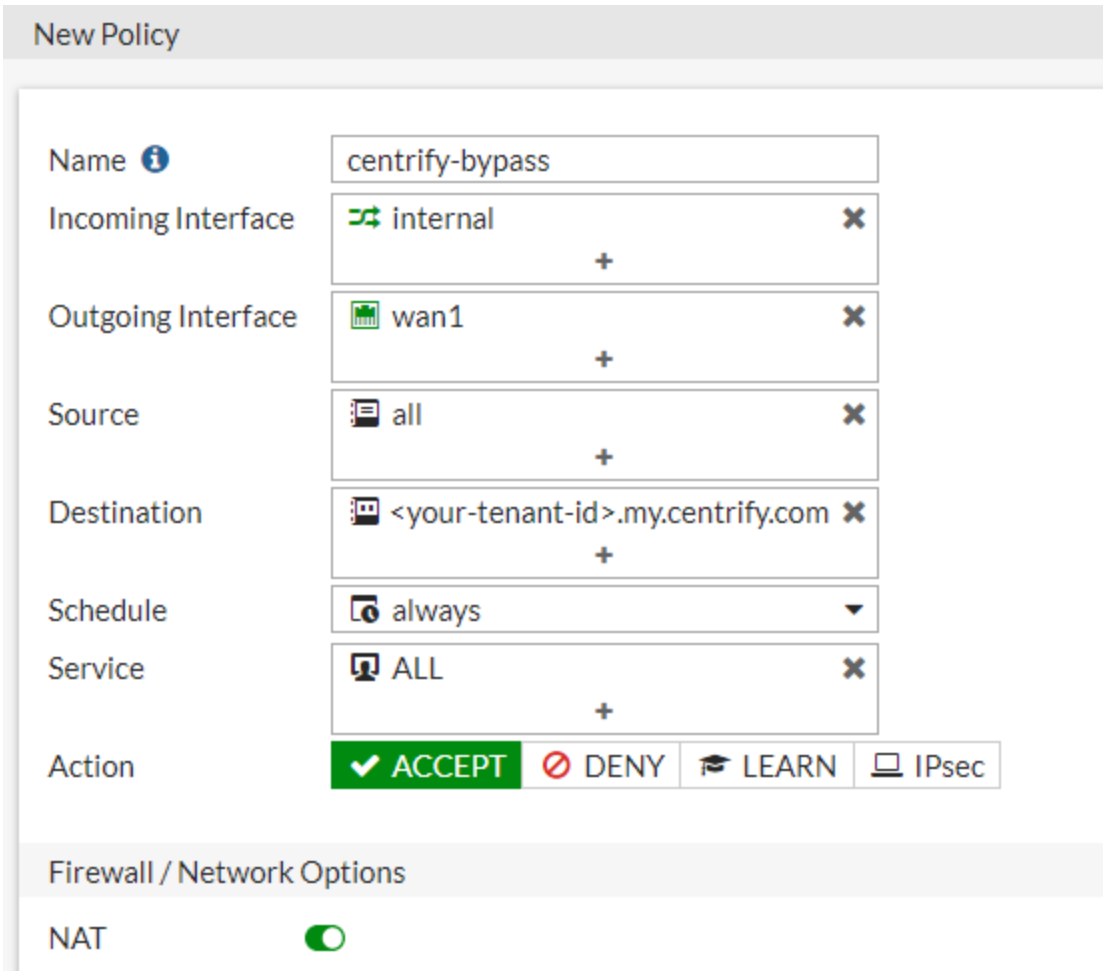
- <your-tenant-id>.my.centrify.com

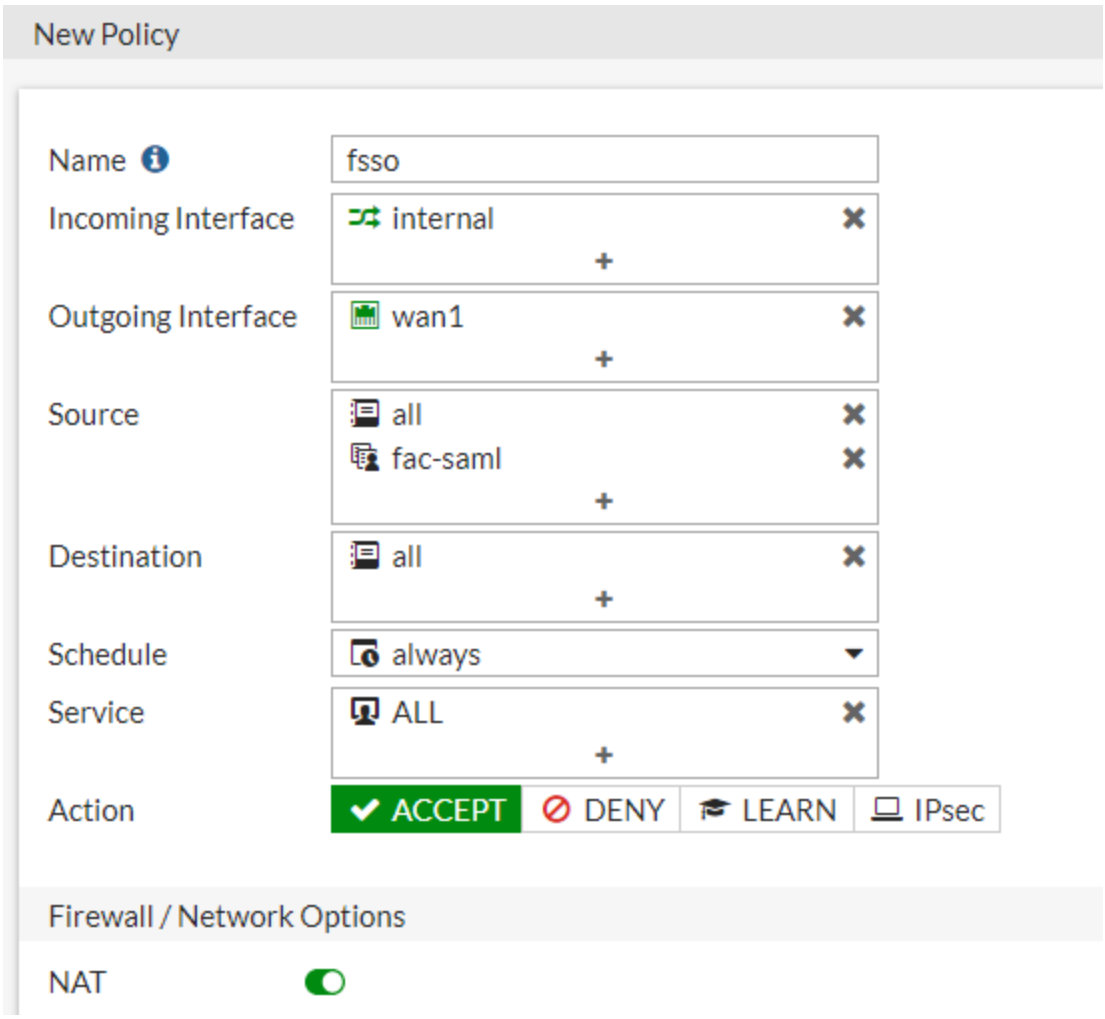
As this is an FQDN, make sure to set **Type** to **FQDN**.

3. Then go to **Policy & Objects > IPv4 Policy** and create all policies shown in the examples:
   - A policy for DNS,
   - for access from the FortiAuthenticator,
   - for Centrify bypass,
   - and the last policy for FSSO, including the SAML user group.


New Policy
Name
dns
Incoming Interface
internal
Outgoing Interface
wan1
Source
all
Destination
all
Schedule
always
Service
DNS
Action
ACCEPT
DENY
LEARN
IPsec
Firewall / Network Options
NAT


New Policy
Name
fac
Incoming Interface
internal
Outgoing Interface
wan1
Source
FAC-172.25.176.141
Destination
all
Schedule
always
Service
ALL
Action
ACCEPT
DENY
LEARN
IPsec
Firewall / Network Options
NAT


New Policy
Name
centrify-bypass
Incoming Interface
internal
Outgoing Interface
wan1
Source
all
Destination
<your-tenant-id>.my.centrify.com
Schedule
always
Service
ALL
Action
ACCEPT
DENY
LEARN
IPsec
Firewall / Network Options
NAT



4. When finished, right-click each policy (*except* the FSSO policy), select **Edit in CLI**, and enter the following command:

```
    set captive-portal-exempt enable
  next
end
```

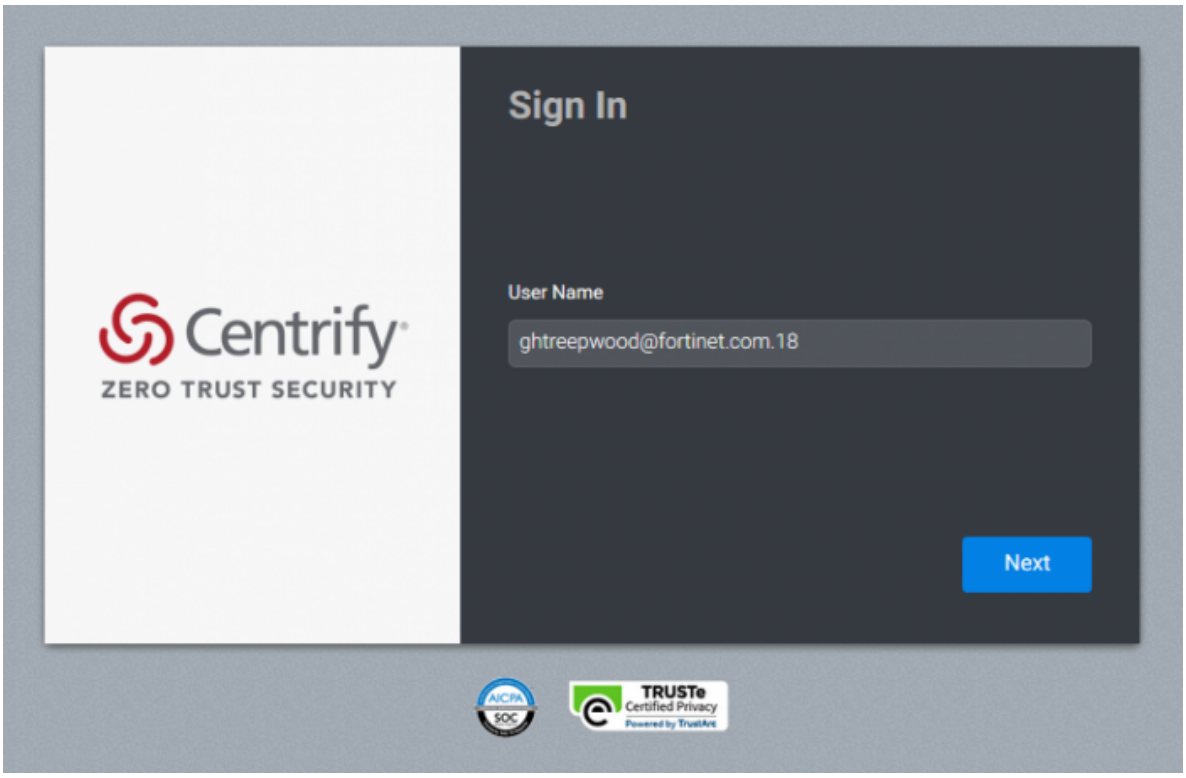
This command exempts users of these policies from the captive portal interface.

Results

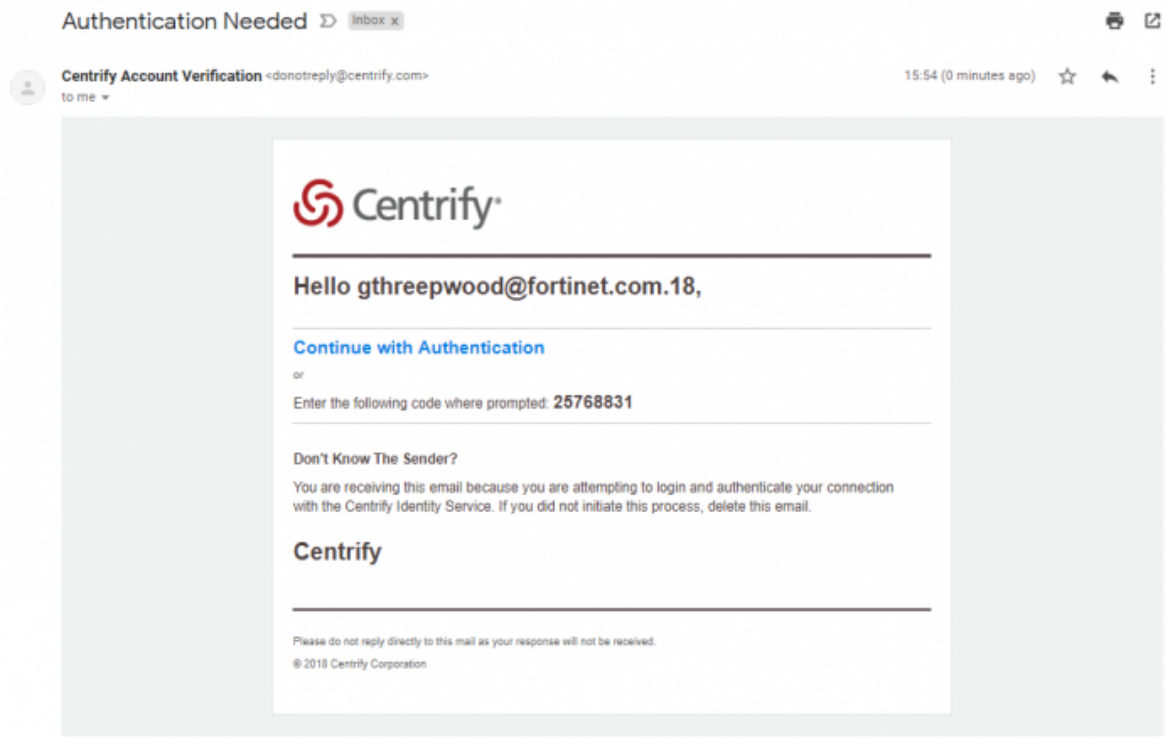
To test the connection, as the user, open a new browser window and attempt to browse the Internet. The browser will redirect to the FortiAuthenticator SAML portal, which pushes the browser to the SAML IdP.

Alternatively, you can directly navigate to the portal URL.

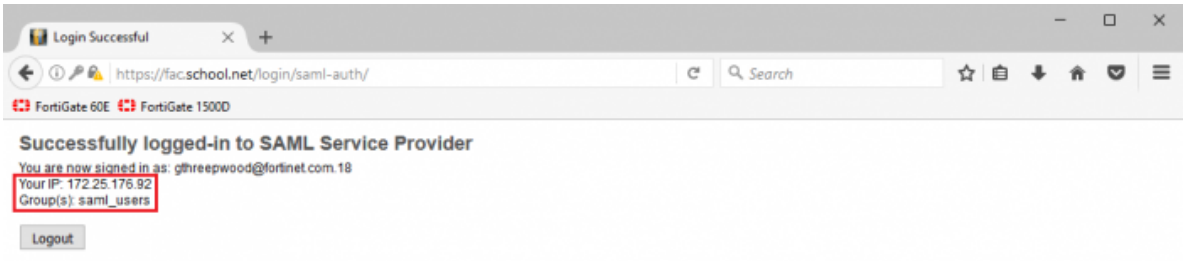
1. Enter valid Centrify account credentials and select **Next**.



2. You will need to verify your account on your first login. An eight-digit code is sent to your email. Use the code to verify your identity and log into the portal.

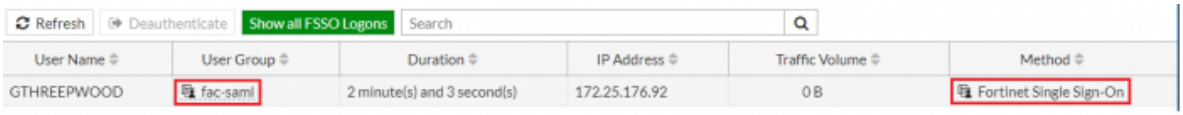


3. The user assertion pushes to the FortiAuthenticator where the user is successfully authenticated. Take note of the user IP and group name.

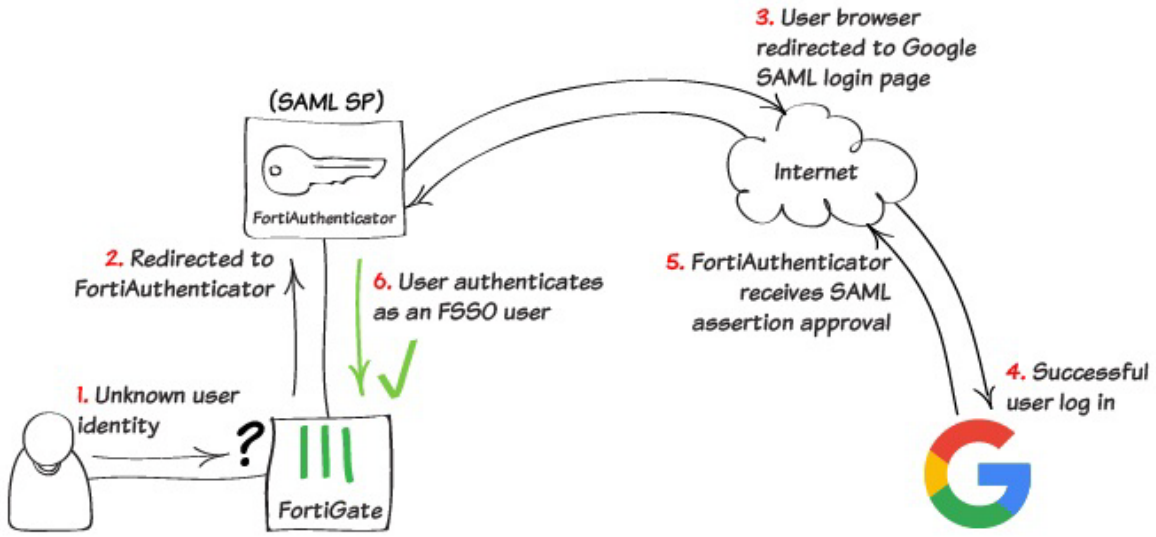


4. View user information including IP address, source, and user group on the FortiAuthenticator under **Monitor > SSO > SSO Sessions**.

5. Confirm that the user has been authenticated via FSSO and place in the correct user group on the FortiGate under **Monitor > Firewall User Monitor**.



SAML 2.0 FSSO with FortiAuthenticator and Google G Suite



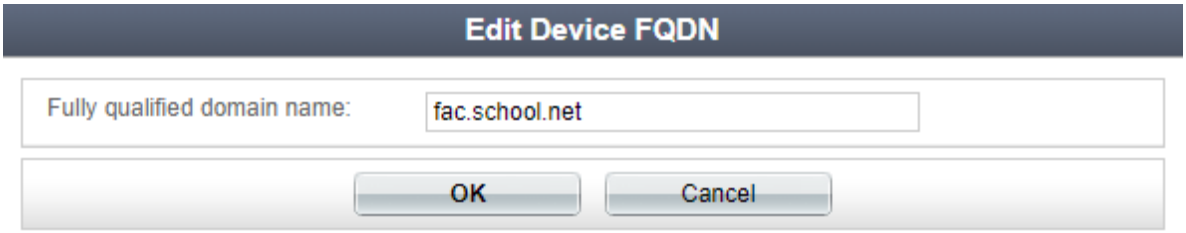
In this example, you provide a Security Assertion Markup Language (SAML) FSSO cloud authentication solution using FortiAuthenticator in conjunction with Google G Suite. The FortiAuthenticator acts as the authentication Service Provider (SP) and Google as the Identity Provider (IdP).

The FortiGate has a WAN IP address of **172.25.176.92**, and the FortiAuthenticator has the WAN IP address of **172.25.176.141**. This recipe uses DNS names and IP addresses that work in our test network. To get this or any authentication setup working for your network you must use IP addresses and host names that work for your network. Also, to avoid problems in the long run, it is a best practice to double check all names and IP addresses as you enter them.

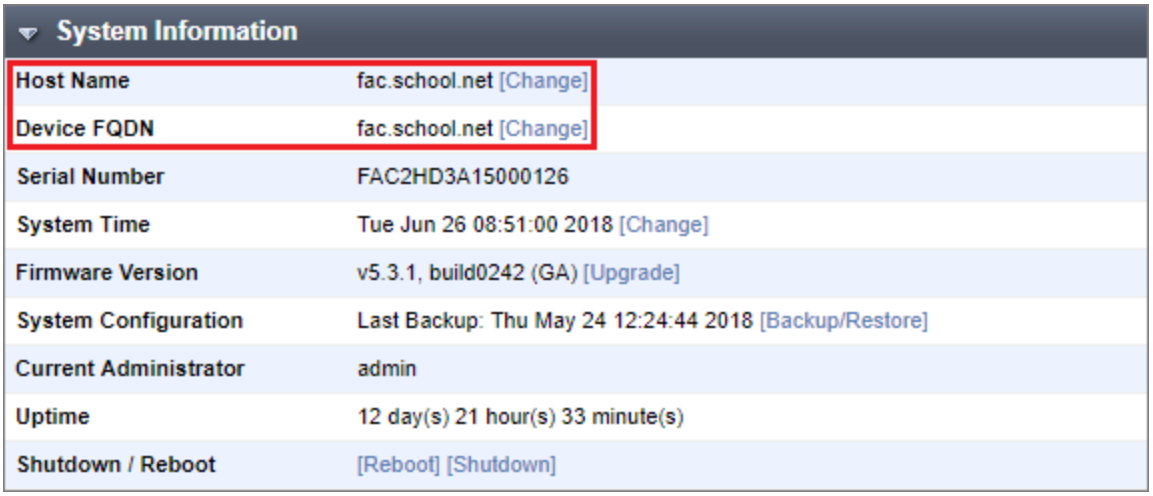
Before you begin, on the FortiAuthenticator create a local user group and an SSO user group. These user groups must have identical names. In this example they are called **saml_users**.

Configuring FSSO and SAML on the FortiAuthenticator

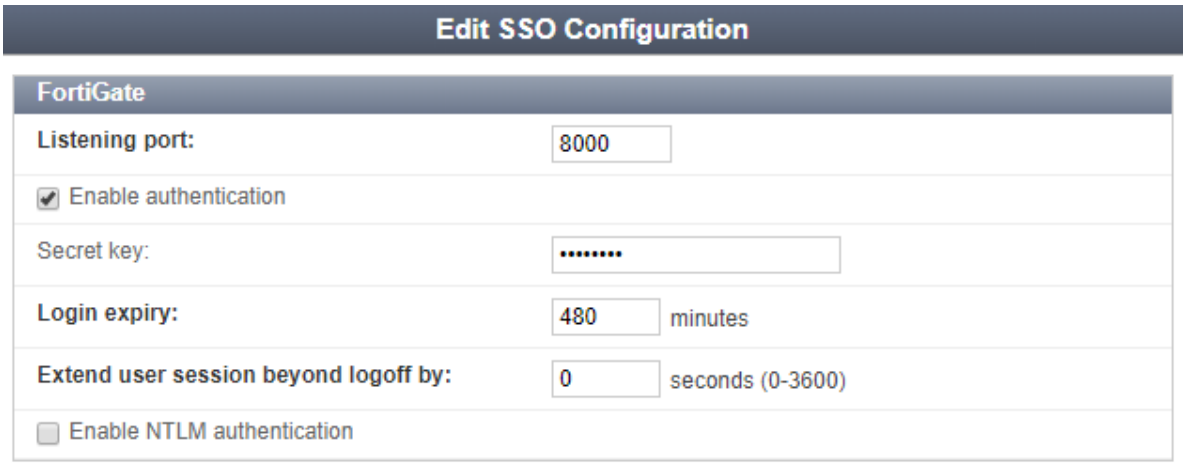
1. Identify where the FortiAuthenticator is in your organization's DNS hierarchy. On the FortiAuthenticator go to **System > Dashboard > Status**. Change the **Device FQDN** to *fac.school.net*.



2. Enter the same name for the **Host Name**.

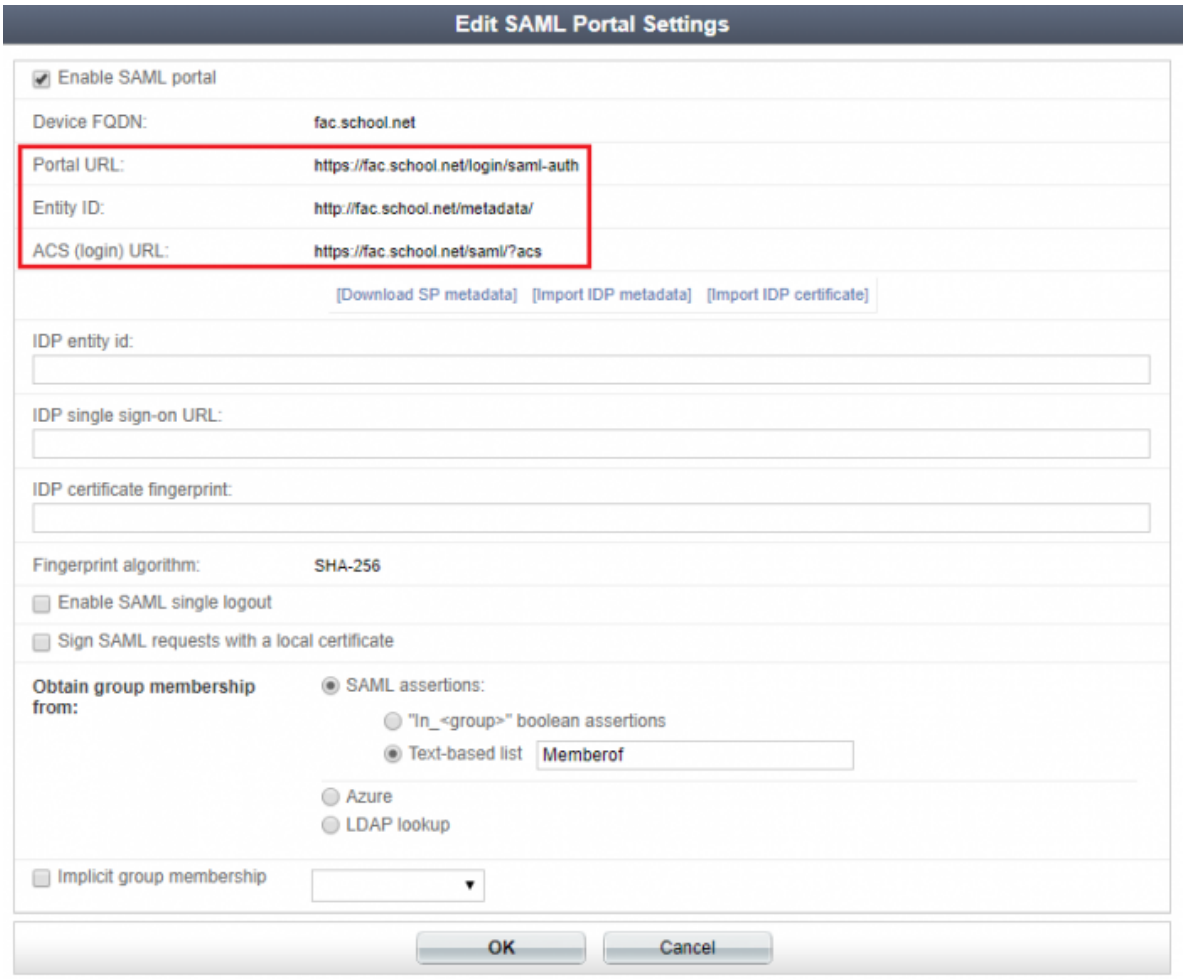


3. Configure the FortiAuthenticator as the FSSO server for the FortiGate. Go to **Fortinet SSO Methods > SSO > General** and set FortiGate SSO options. Make sure to **Enable authentication**.
   Enter a **Secret key** and select **OK** to apply your changes.



4. Then enable the SAML authentication portal. Go to **Fortinet SSO Methods > SSO > SAML Authentication** and select **Enable SAML portal**.
   You will not yet be able to save the settings in this page, as other IdP information — IDP entity id, IDP single sign-on URL, and IDP certificate fingerprint — needs to be entered. These fields can be filled once the IdP application configuration is complete.
   The FortiAuthenticator generates the following SAML portal URLs. You will add them to your IdP application configuration:
   - **Portal url** - Captive Portal URL.
   - **Entity id**
   - **ACS (Login) url** - Assertion POST URL used by the SAML IdP.

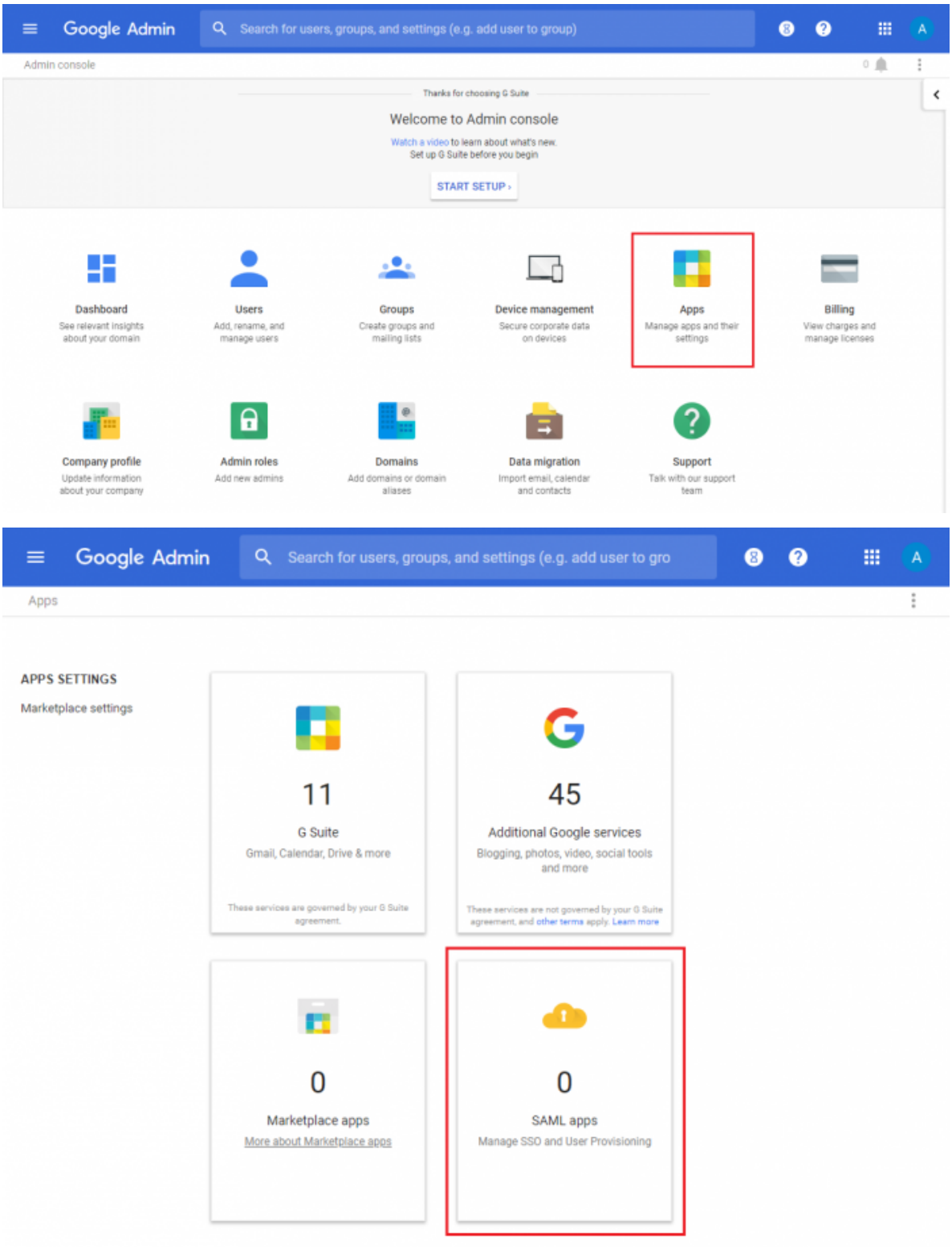
   To determine user group membership, enable Text-based list under SAML assertions and enter Memberof (this field is case-sensitive).

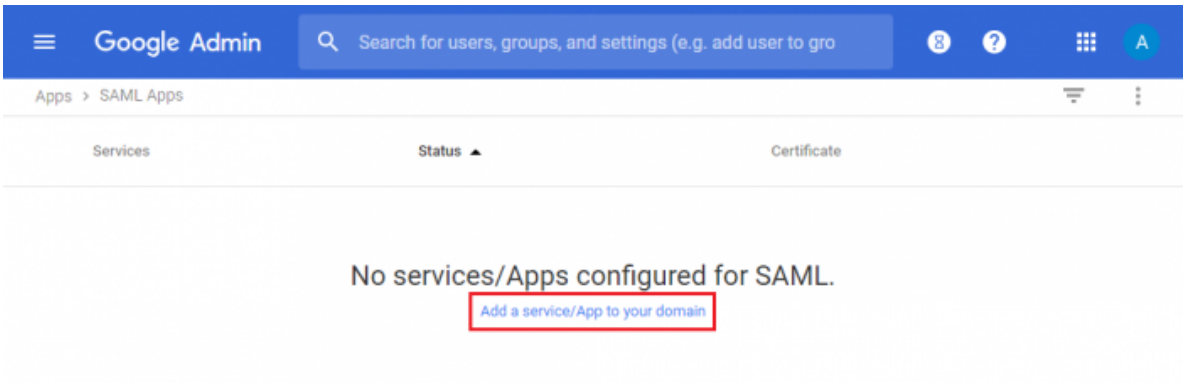


Keep the Edit SAML Portal Settings window open for reference when you are configuring the IdP application and for testing.

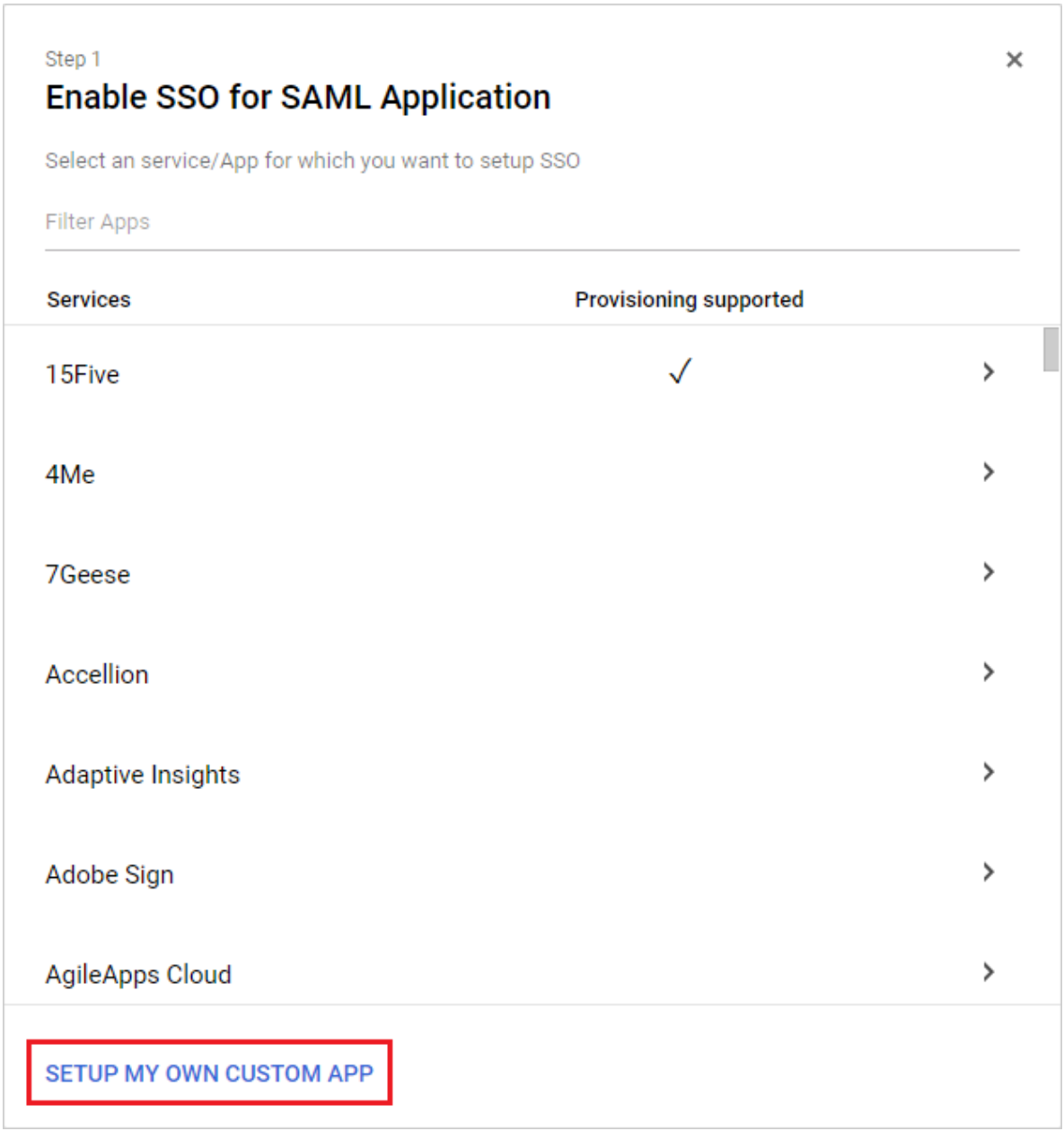
Configuring SAML on G Suite

1. To configure SAML, log in to your G Suite administrator account.
   From the **Admin console**,select **Apps > SAML apps > Add a service/App**.


Google Admin
Search for users, groups, and settings (e.g. add user to group)
Admin console
Thanks for choosing G Suite
Welcome to Admin console
Watch a video to learn about what's new.
Set up G Suite before you begin
START SETUP
Dashboard
See relevant insights about your domain
Users
Add, rename, and manage users
Groups
Create groups and mailing lists
Device management
Secure corporate data on devices
Apps
Manage apps and their settings
Billing
View charges and manage licenses
Company profile
Update information about your company
Admin roles
Add new admins
Domains
Add domains or domain aliases
Data migration
Import email, calendar and contacts
Support
Talk with our support team
Google Admin
Search for users, groups, and settings (e.g. add user to gro
Apps
APPS SETTINGS
Marketplace settings
11
G Suite
Gmail, Calendar, Drive & more
These services are governed by your G Suite agreement.
45
Additional Google services
Blogging, photos, video, social tools and more
These services are not governed by your G Suite agreement, and other terms apply. Learn more
0
Marketplace apps
More about Marketplace apps
0
SAML apps
Manage SSO and User Provisioning

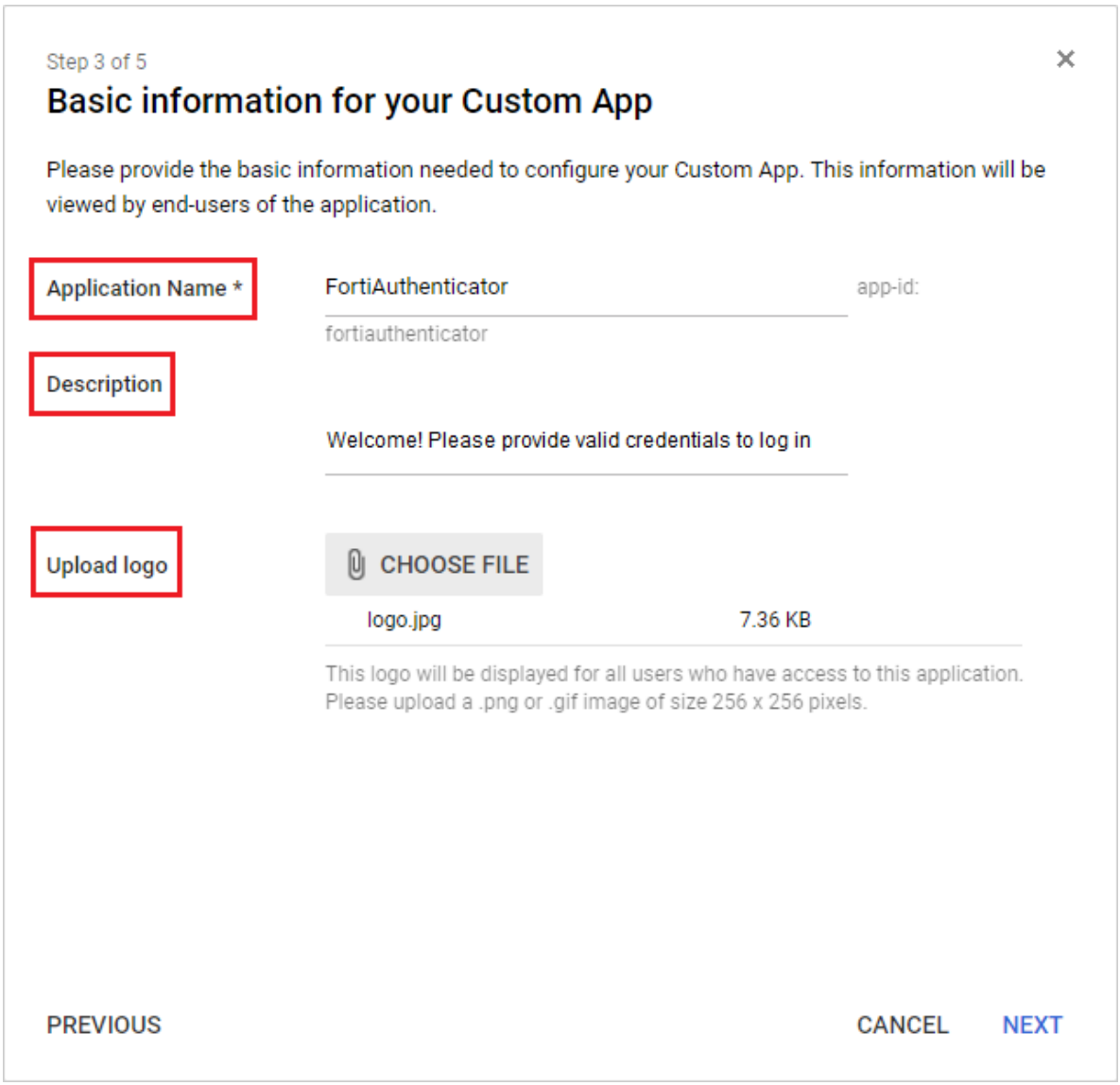


2. In the **Enable SSO for SAML Application** page, select to **SETUP MY OWN CUSTOM APP**.

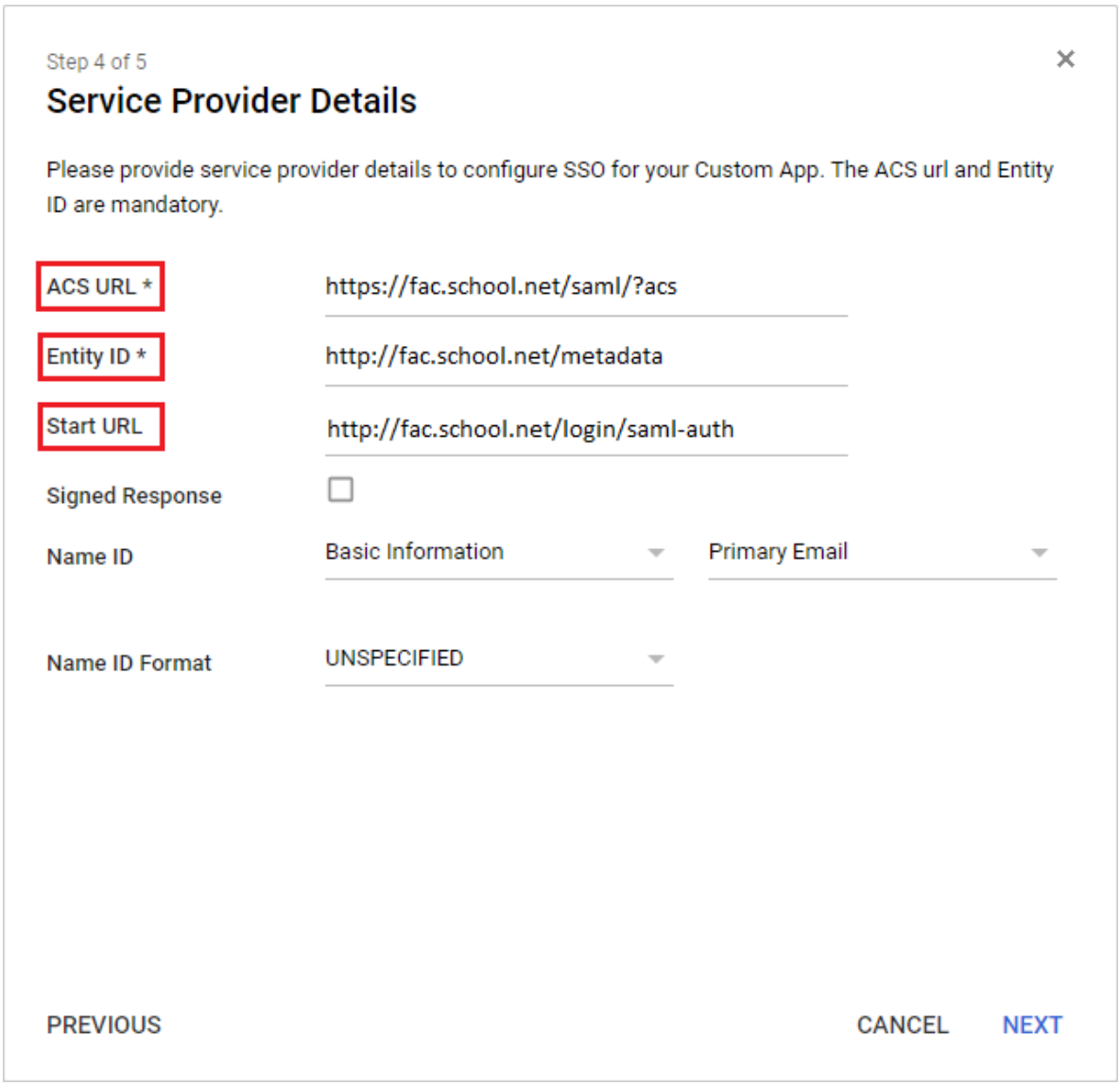


3. In the **Google IdP Information** page, download the **Certificate** and **IDP metadata**. Select **Next**.

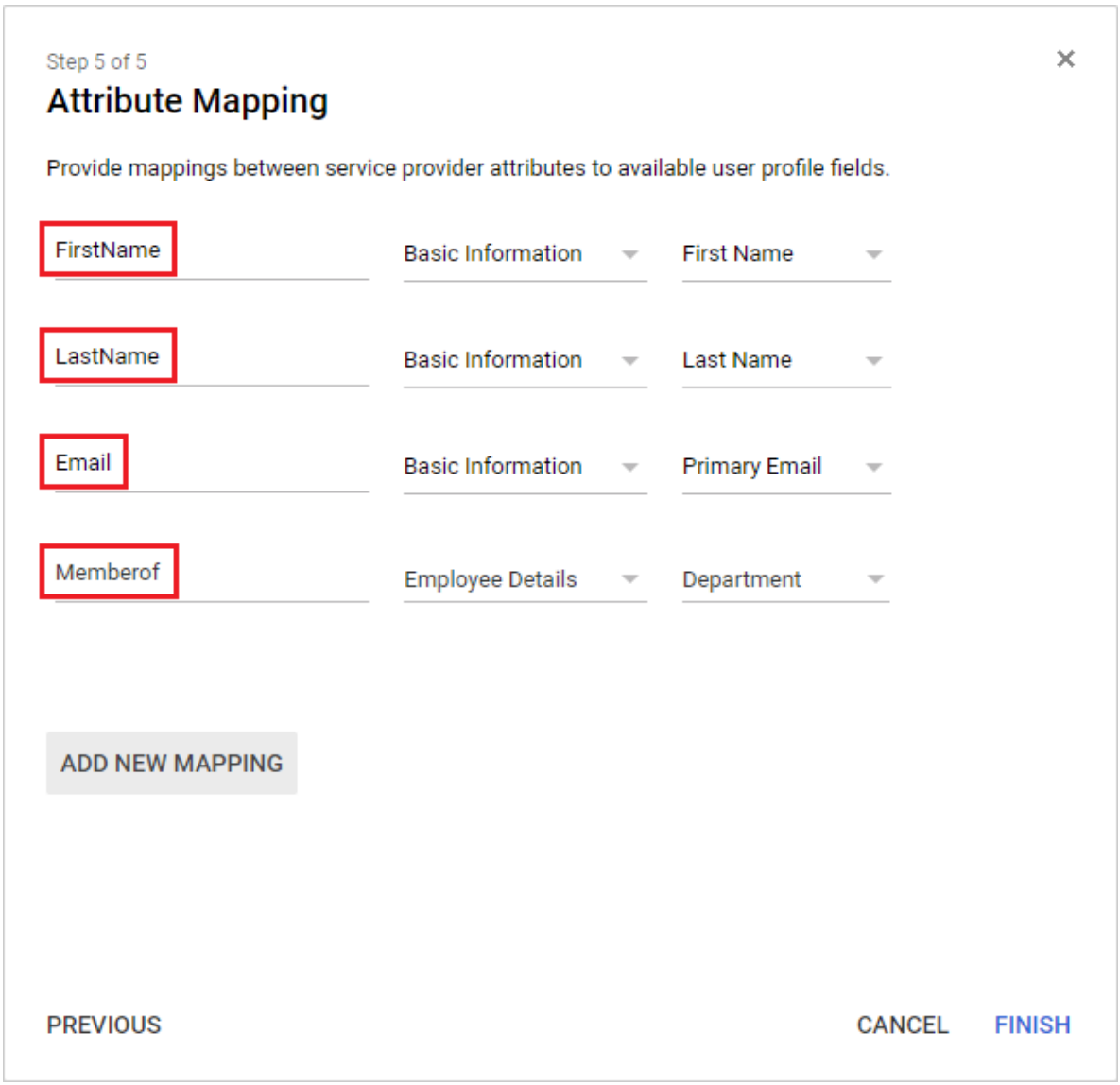
4. In the Basic information for your Custom App page, enter an Application Name, and optionally provide a Description and Upload logo. Select Next.



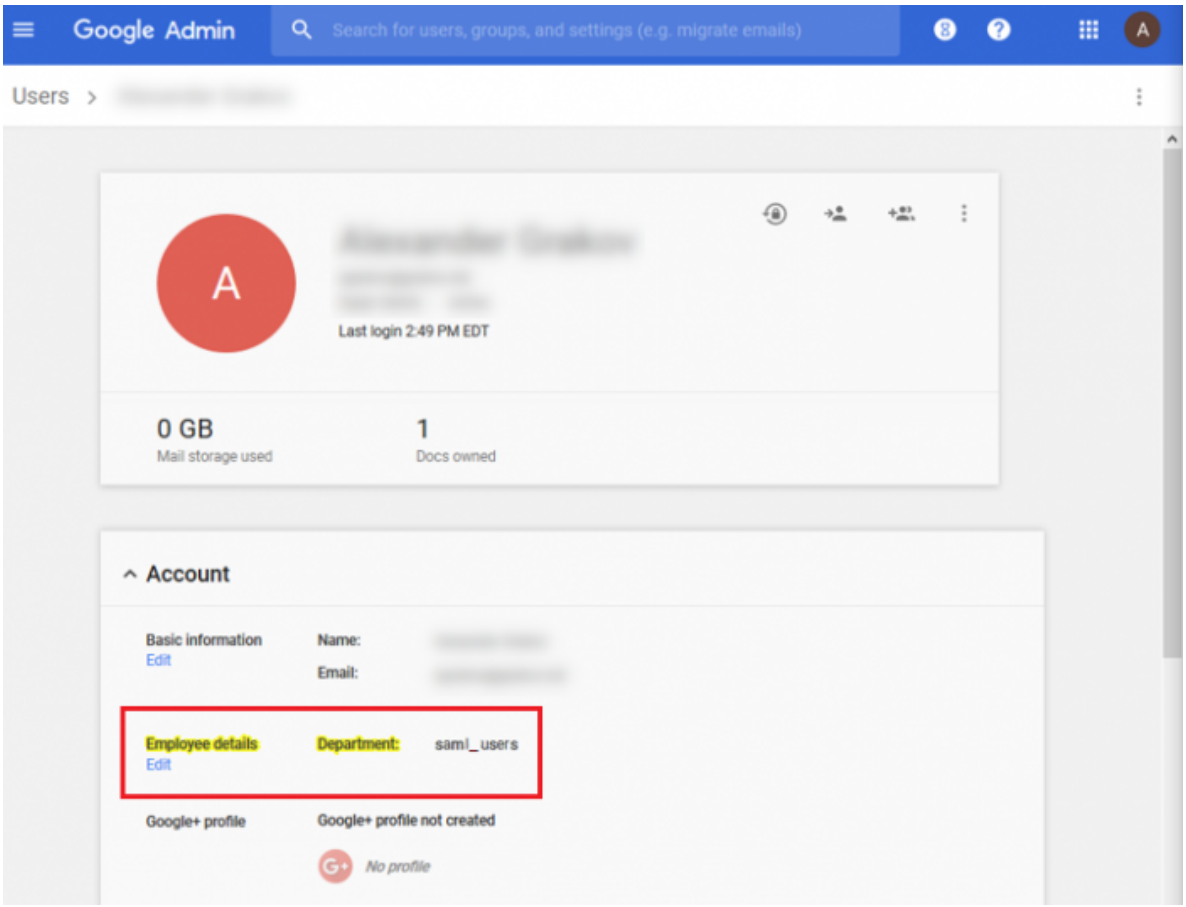
5. In the **Service Provider Details** page, set the **ACS URL**, **Entity ID**, and **Start URL** – these are the **ACS (login) url**, **Entity id**, and **Portal url** (respectively) from the FortiAuthenticator **Edit SAML Portal Settings** window. Select **Next**.



6. In the **Attribute Mapping** page, add the **FirstName**, **LastName**, **Email**, and **Memberof** user attributes. The **Department** setting for **Memberof** must match the FortiAuthenticator **saml_users** group. Select **Finish**.

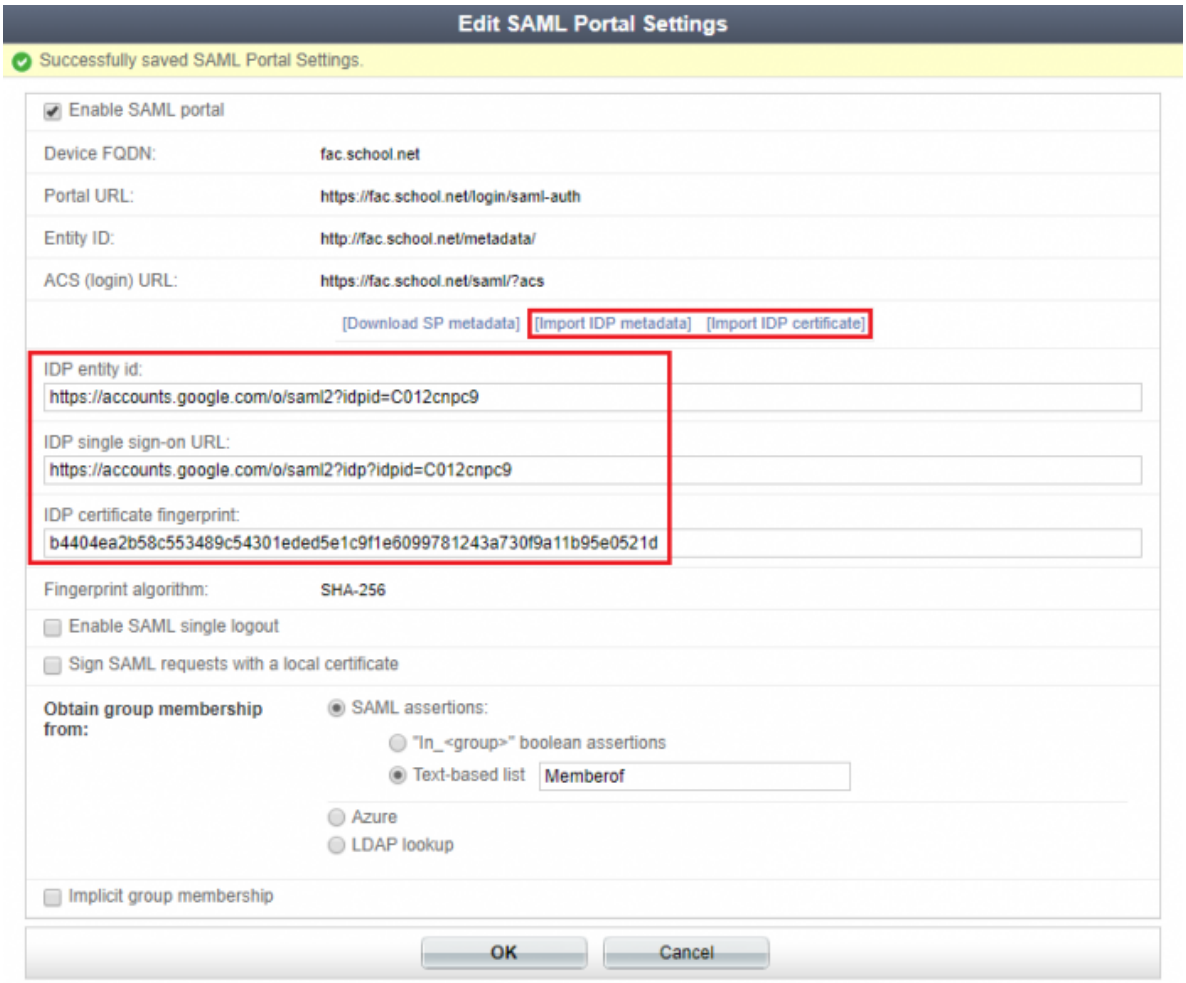


7. Finally, make sure the application is **ON** for everyone, and go to your user's **Account** information and make sure that **Employee details** show as **Department**. Set **Department** to the same FortiAuthenticator **saml_users** user group name.

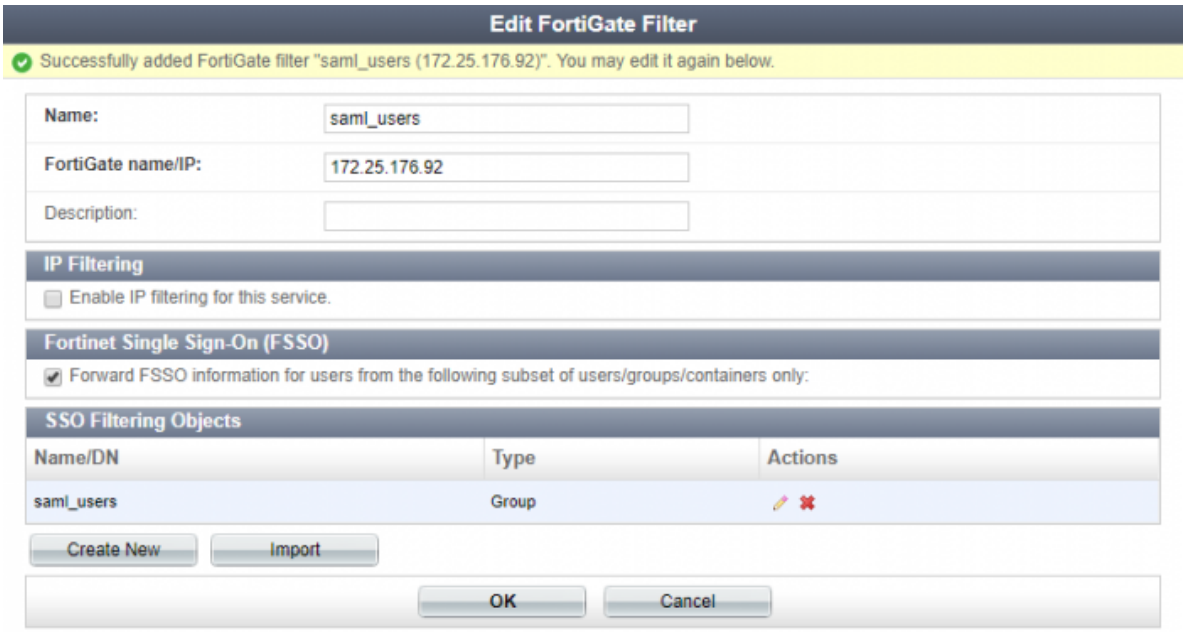


Importing the IdP certificate and metadata on the FortiAuthenticator

1. To import the Google IdP data, on the FortiAuthenticator, go to **Fortinet SSO Methods > SSO > SAML Authentication** and import the IdP metadata and certificate downloaded during the **Google IdP Information** step earlier.
   This automatically fills the IdP fields. Make sure to select **OK** to save these changes.

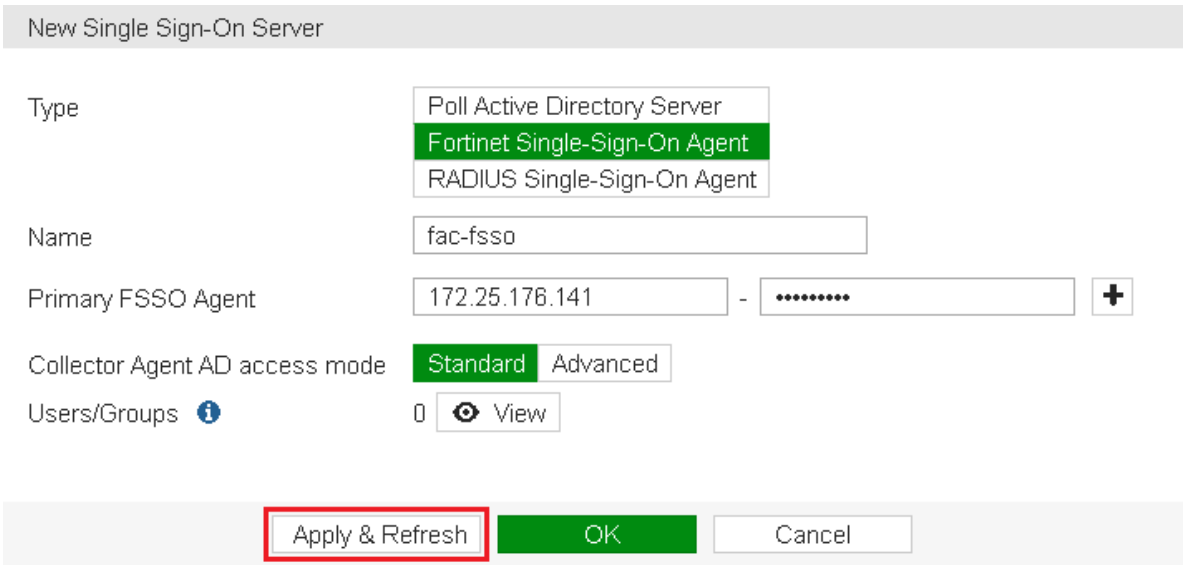


2. Create a new FortiGate filter for FSSO Push. Go to **Fortinet SSO Methods > SSO > FortiGate Filtering** and select **Create New**.
   Enter a name and the FortiGate's wan-interface IP address. Select **OK** and then enable **Fortinet Single Sign-On (FSSO)**.
   Select **Create New** to create an SSO group filtering object. The group filtering object name must once again match the original SAML group user name (**saml_users**).
   Select **OK** to apply all changes.



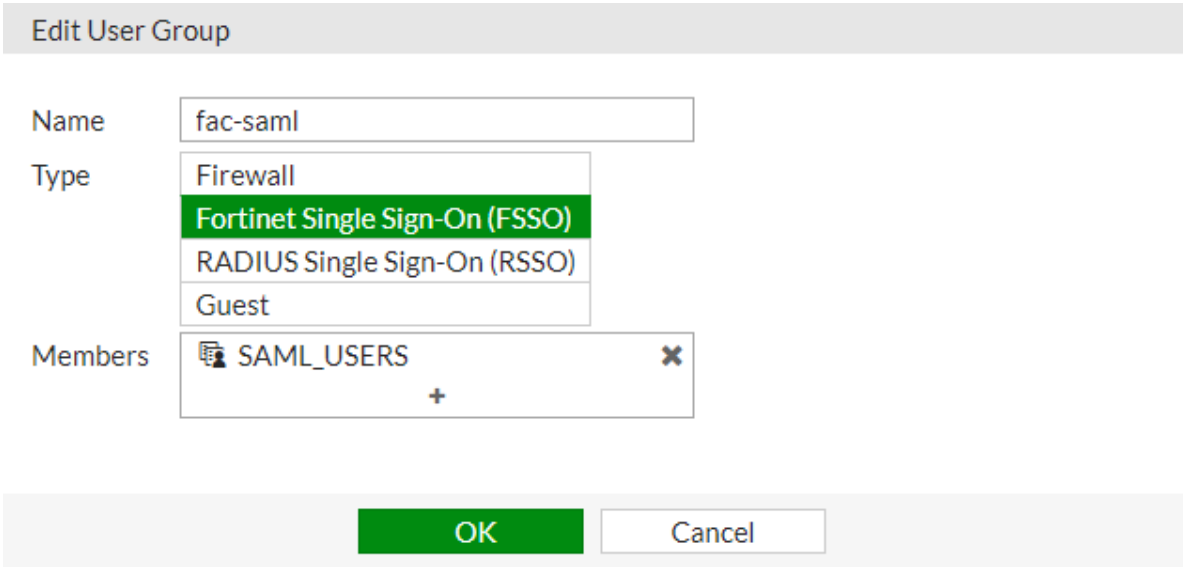
Configuring FSSO on the FortiGate

1. On the FortiGate, go to **User & Device > Single Sign-On** and select **Create New**.
   Set Type to **Fortinet Single-Sign-On Agent**, enter a **Name**, the FortiAuthenticator's Internet-interface IP address, and the password, which must match the secret key entered at the beginning of the FortiAuthenticator configuration process.
   Select **Apply & Refresh**.



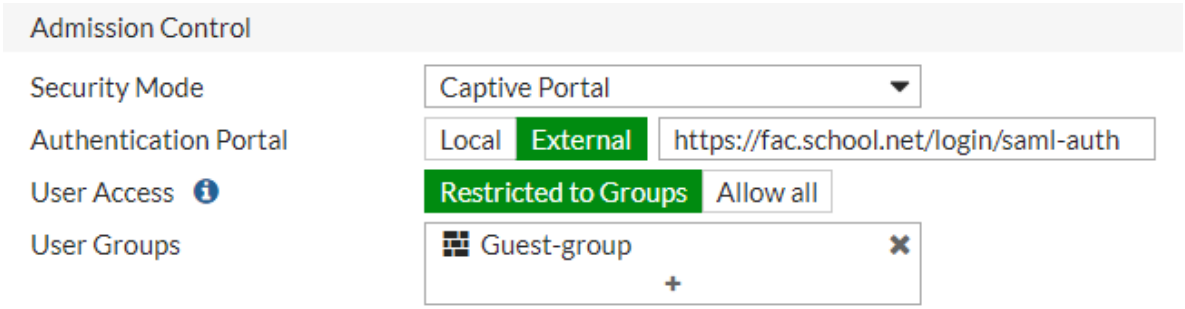
2. The SAML user group name has been successfully pushed to the FortiGate from the FortiAuthenticator, appearing when you select **View**.
   You may have to wait a few minutes before the user group appears.

3. Then go to **User & Device > User Groups** and create a new FSSO user group. Successfully authenticated users via SAML FSSO will be placed in this group.
Enter a **Name**, set **Type** to **Fortinet Single Sign-On (FSSO)**, and add the FSSO group as a **Member**.

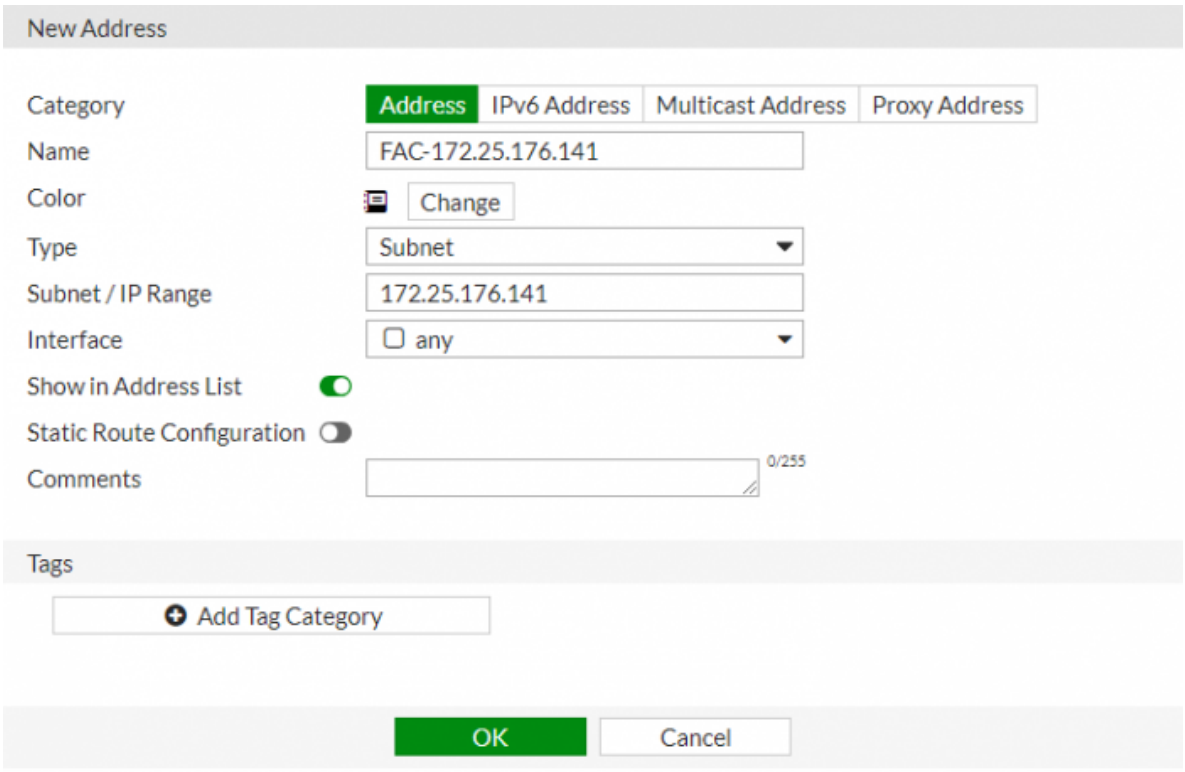


Configuring Captive Portal and security policies

1. On the FortiGate, go to **Network > Interfaces** and edit the internal interface.
Under **Admission Control**, set **Security Mode** to **Captive Portal**.
Set **Authentication Portal** to **External**, and enter the SAML authentication portal URL.
Set **User Access** to **Restricted to Groups**, and set **User Groups** to any local group.



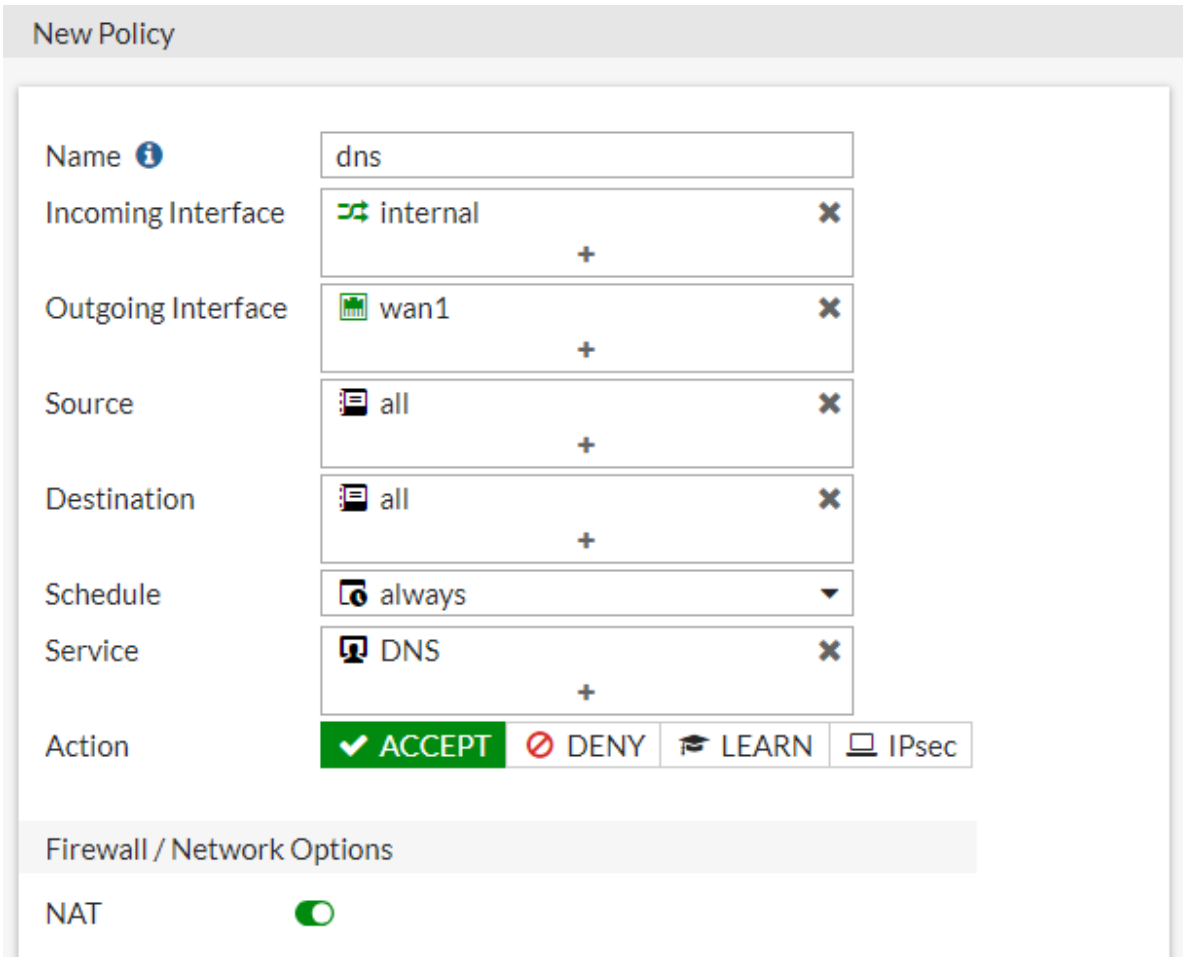
2. Go to **Policy & Objects > Addresses** and add the FortiAuthenticator as an address object.

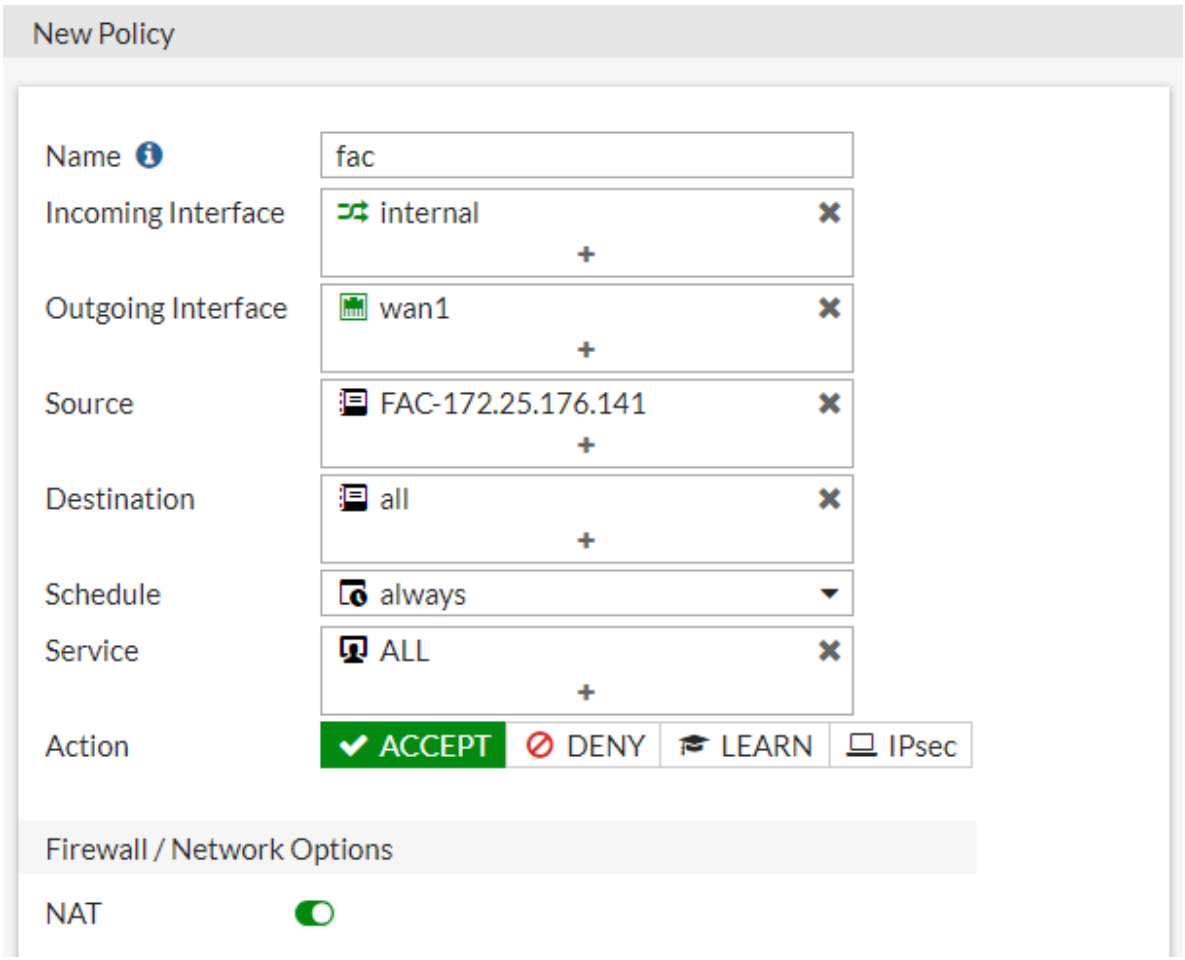


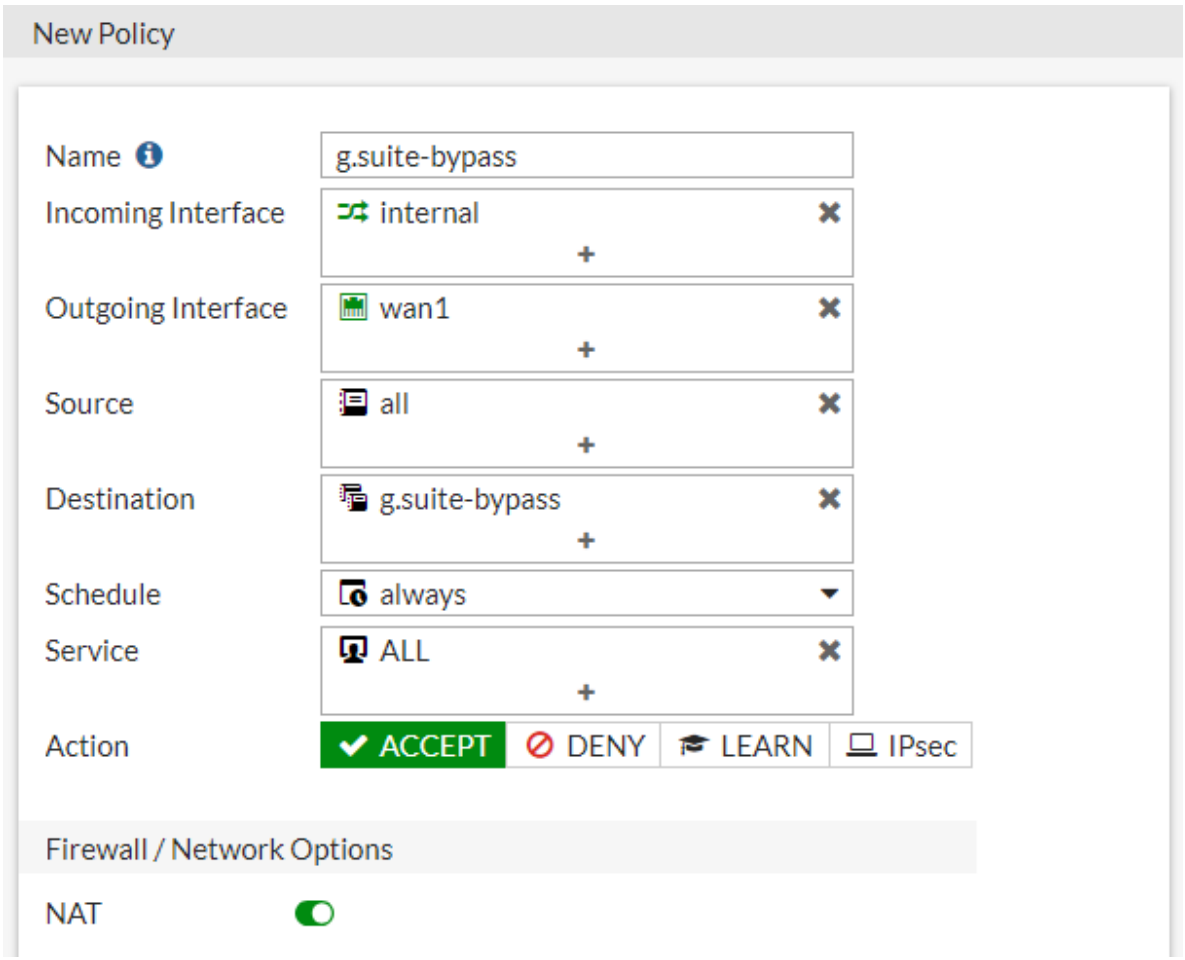
3. Then create the following FQDN objects:
   - www.googleapis.com
   - accounts.google.com
   - ssl-gstatic.com
   - fonts.gstatic.com
   - www.gstatic.com

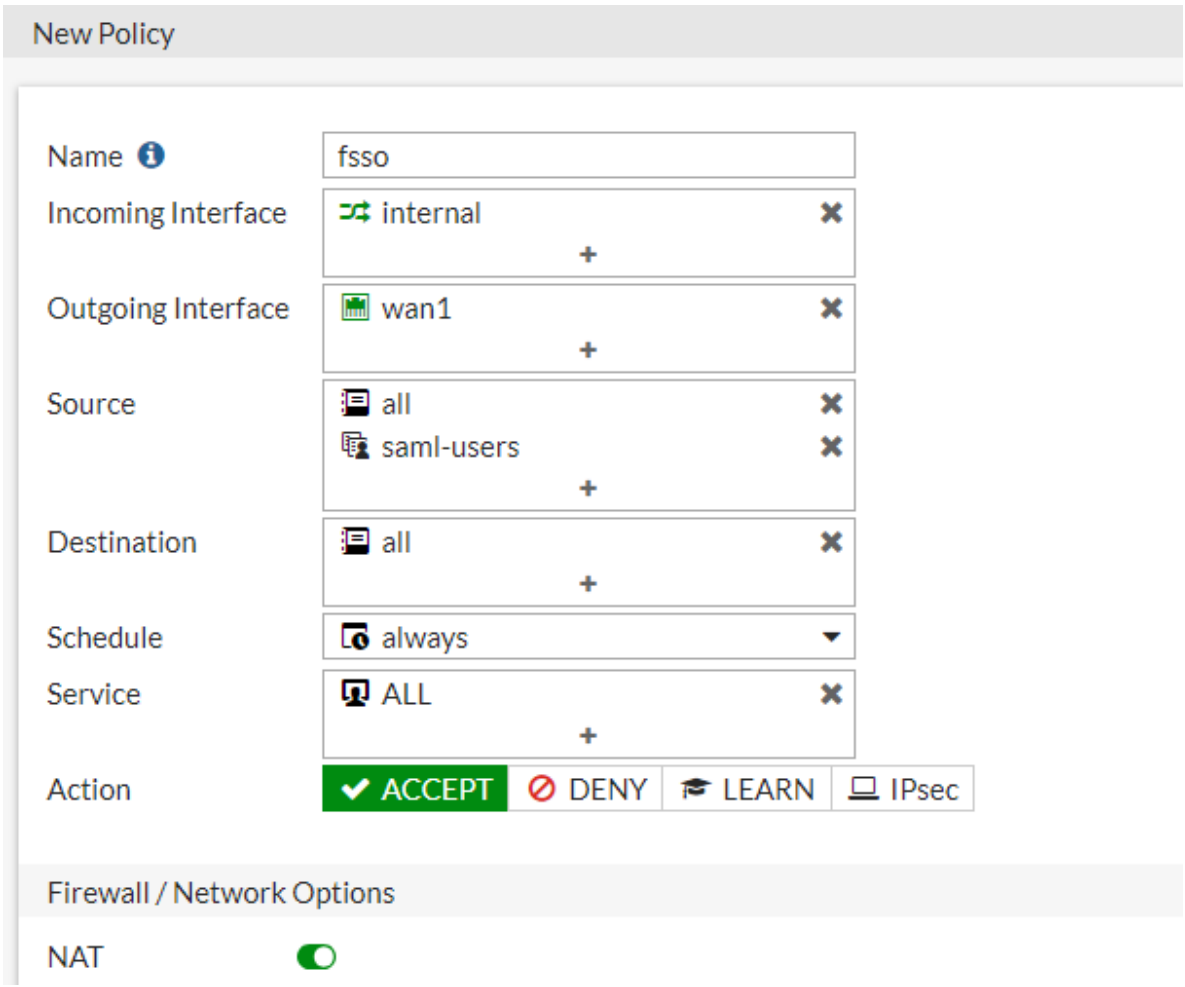
   Then add the following Google subnets:
   - 172.217.9.0/24
   - 216.58.192.0/19

   Then create ad address group, adding all created objects as members (in this example, **g.suite-bypass**).
4. Go to **Policy & Objects > IPv4 Policy** and create the following policies: one for DNS, for access from FortiAuthenticator, for G Suite bypass, and the last policy for FSSO, including the SAML user group.


New Policy
Name
dns
Incoming Interface
internal
Outgoing Interface
wan1
Source
all
Destination
all
Schedule
always
Service
DNS
Action
ACCEPT
DENY
LEARN
IPsec
Firewall / Network Options
NAT


New Policy
Name
fac
Incoming Interface
internal
Outgoing Interface
wan1
Source
FAC-172.25.176.141
Destination
all
Schedule
always
Service
ALL
Action
ACCEPT
DENY
LEARN
IPsec
Firewall / Network Options
NAT


New Policy
Name
g.suite-bypass
Incoming Interface
internal
Outgoing Interface
wan1
Source
all
Destination
g.suite-bypass
Schedule
always
Service
ALL
Action
ACCEPT
DENY
LEARN
IPsec
Firewall / Network Options
NAT



5. When finished, right-click each policy (*except* the FSSO policy), select **Edit in CLI**, and enter the following command for each policy except the FSSO policy:

```
    set captive-portal-exempt enable
  next
end
```

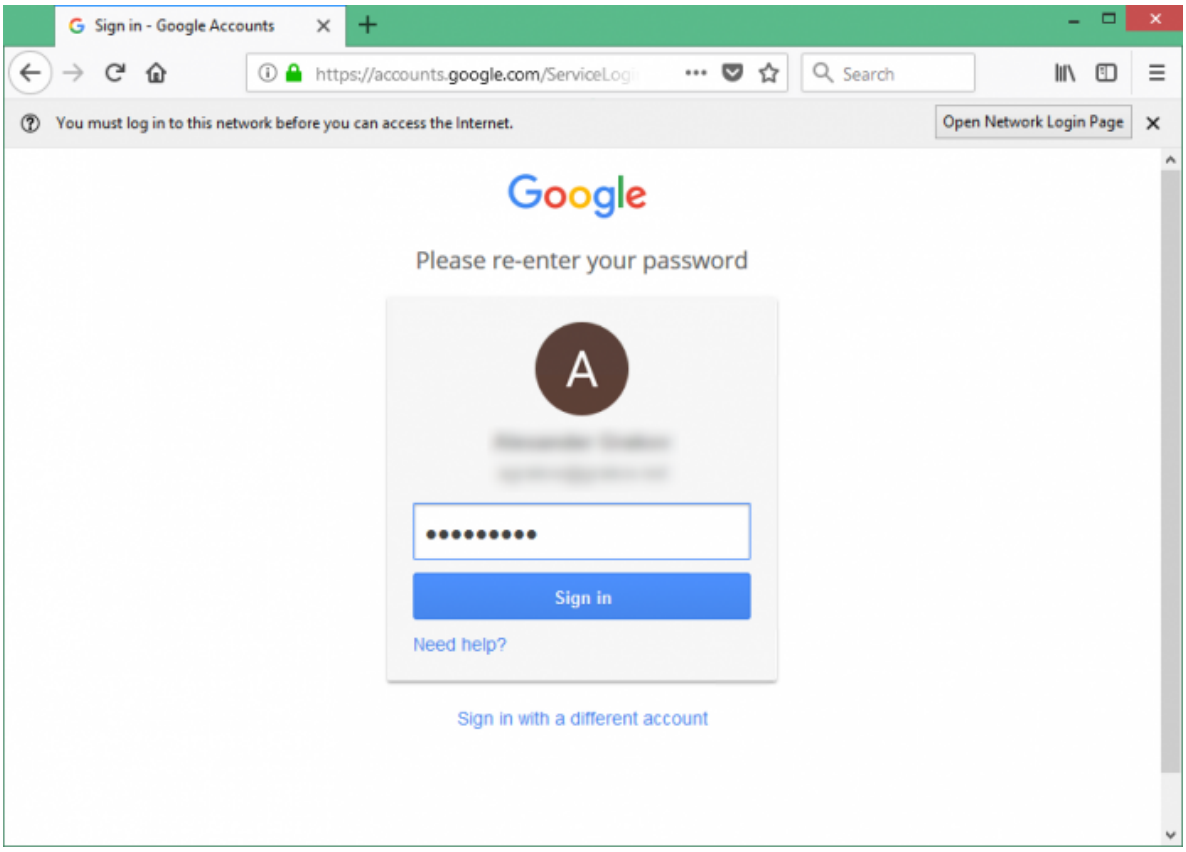
This command exempts users of these policies from the captive portal interface.

Results

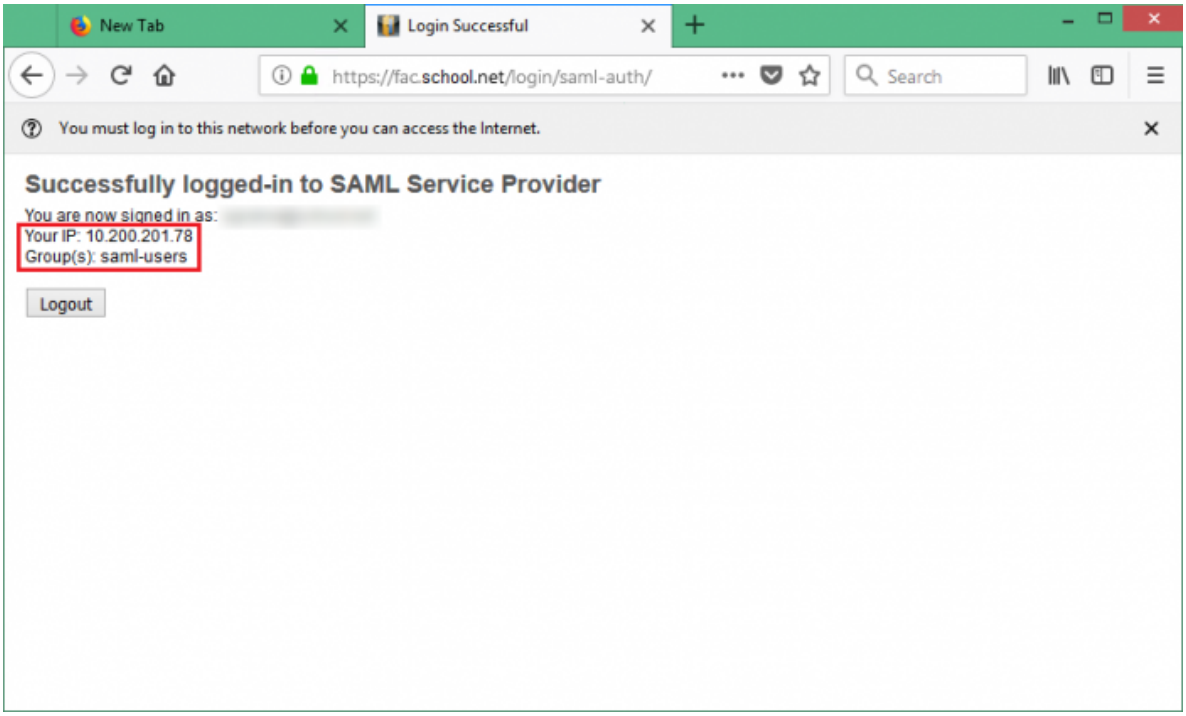
To test the connection, open a new browser window and attempt to browse the Internet. The browser redirects to the FortiAuthenticator SAML portal, which pushes the browser to the SAML IdP.

Alternatively, you can directly navigate to the portal URL.

1. Enter valid Google account credentials and confirm your password.

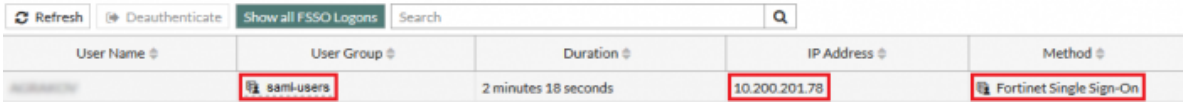


2. The user assertion pushes to the FortiAuthenticator where the user is successfully authenticated. Take note of the user IP and group name.

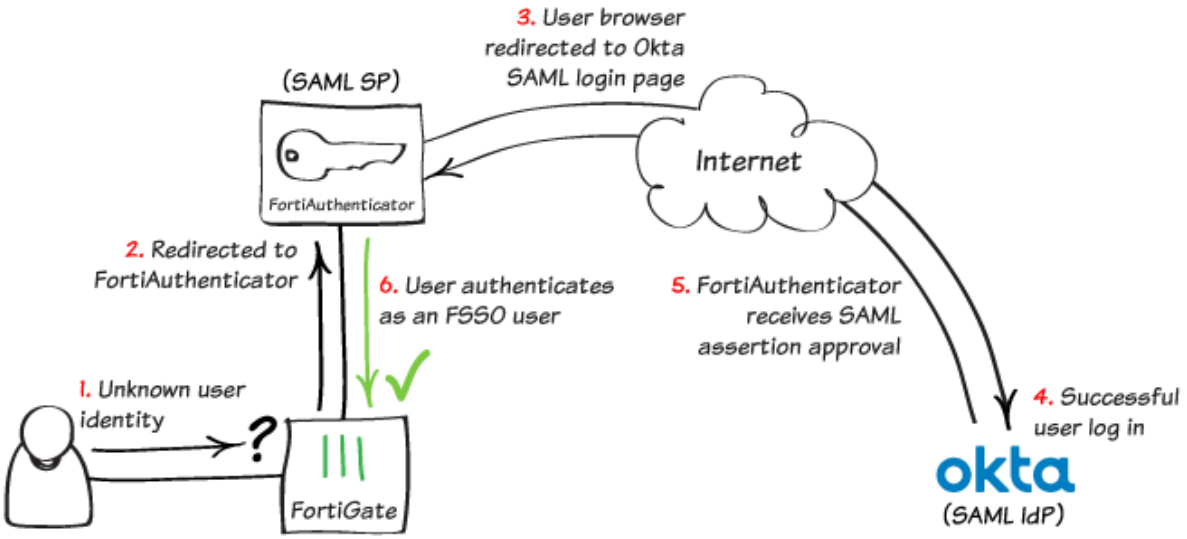


3. View user information including IP address and user group on the FortiAuthenticator under **Monitor > SSO > SSO Sessions**.

4. Confirm that the user has been authenticated via FSSO on the FortiGate under **Monitor > Firewall User Monitor**.



SAML 2.0 FSSO with FortiAuthenticator and Okta



In this example, you will provide a Security Assertion Markup Language (SAML) FSSO cloud authentication solution using FortiAuthenticator as the service provider (SP) and Okta, a cloud-based user directory, as the identity provider (IdP).

Okta is a secure authentication and identity-access management service that offer secure SSO solutions. Okta can be implemented with a variety of technologies and services including Office 365, G Suite, Dropbox, AWS, and more.

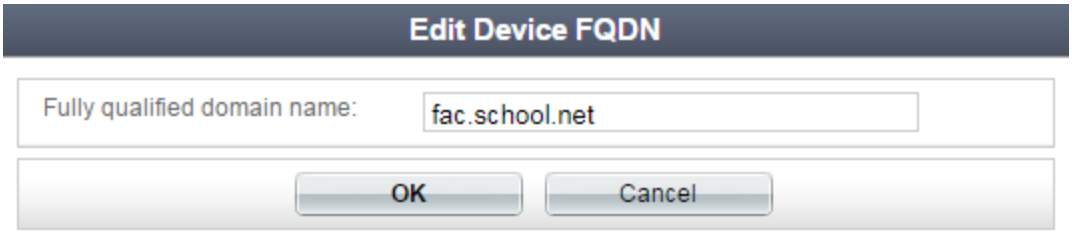
A user will start by attempting to make an unauthenticated web request (1). The FortiGate's captive portal will offload the authentication request to the FortiAuthenticator's SAML SP portal (2), which in turn redirects that client/browser to the SAML IdP login page (3). Assuming the user successfully logs into the portal (4), a positive SAML assertion will be sent back to the FortiAuthenticator (5), converting the user's credentials into those of an FSSO user (6).

The FortiGate has a WAN IP address of **172.25.176.92**, and the FortiAuthenticator has the WAN IP address of **172.25.176.141**. Note that, for testing purposes, the FortiAuthenticator's IP and FQDN have been added to the host's file of trusted host names; this is not necessary for a typical network.

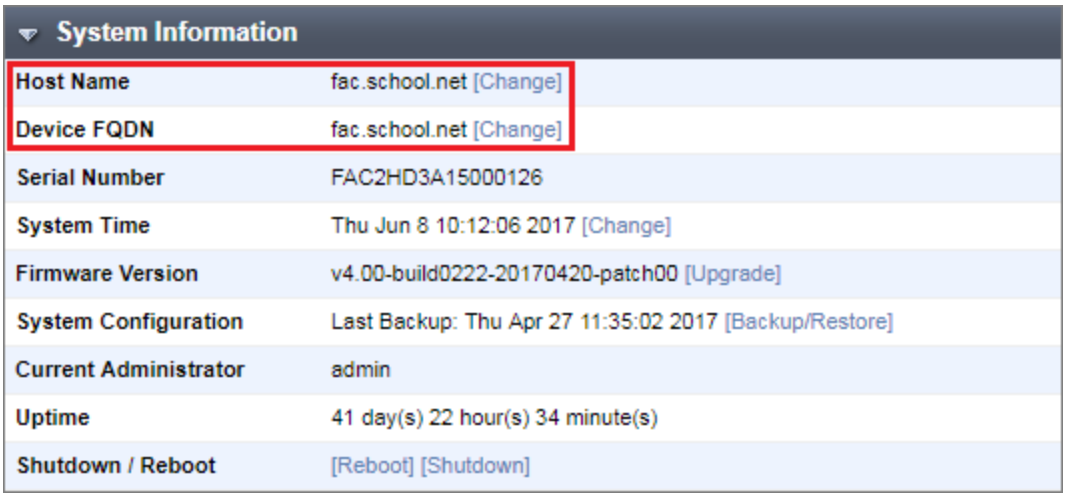
This configuration assumes that you have already created an Okta developer account. It is also assumed that two user groups have been created on the FortiAuthenticator both called **saml_users**: one local user group, and an SSO user group.

Configuring DNS and FortiAuthenticator's FQDN

1. On the FortiAuthenticator, go to **System > Dashboard > Status**. In the **System Information** widget, select **Change** next to **Device FQDN**.
   Enter a domain name (in this example, *fac.school.net*). This will help identify where the FortiAuthenticator is located in the DNS hierarchy.



2. Enter the same name for the **Host Name**. This is so you can add the unit to the FortiGate's DNS list, so that the local DNS lookup of this FQDN can be resolved.

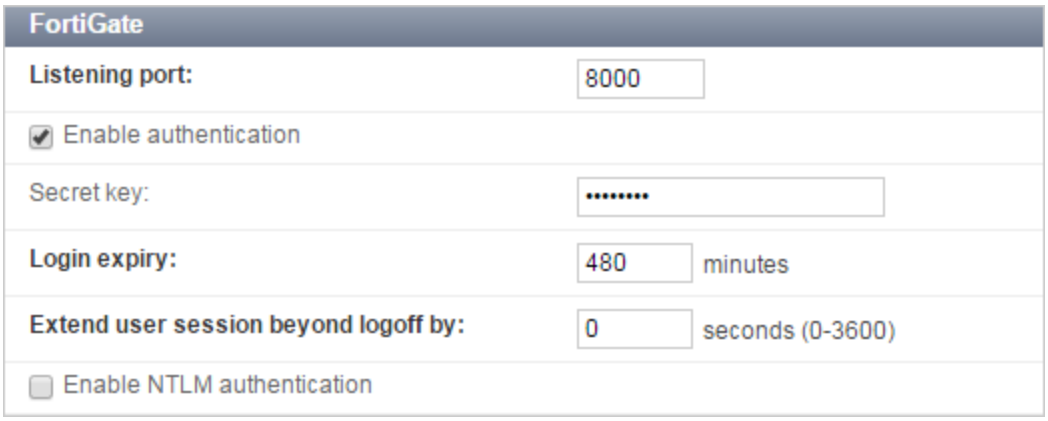


3. On the FortiGate, open the **CLI Console** and enter the following command, entering the FortiAuthenticator's host name and Internet-facing IP address:

```
config system dns-database
   edit school.net
      config dns-entry
         edit 1
            set hostname fac.school.net
            set ip 172.25.176.141
         next
      end
      set domain school.net
   next
end
```

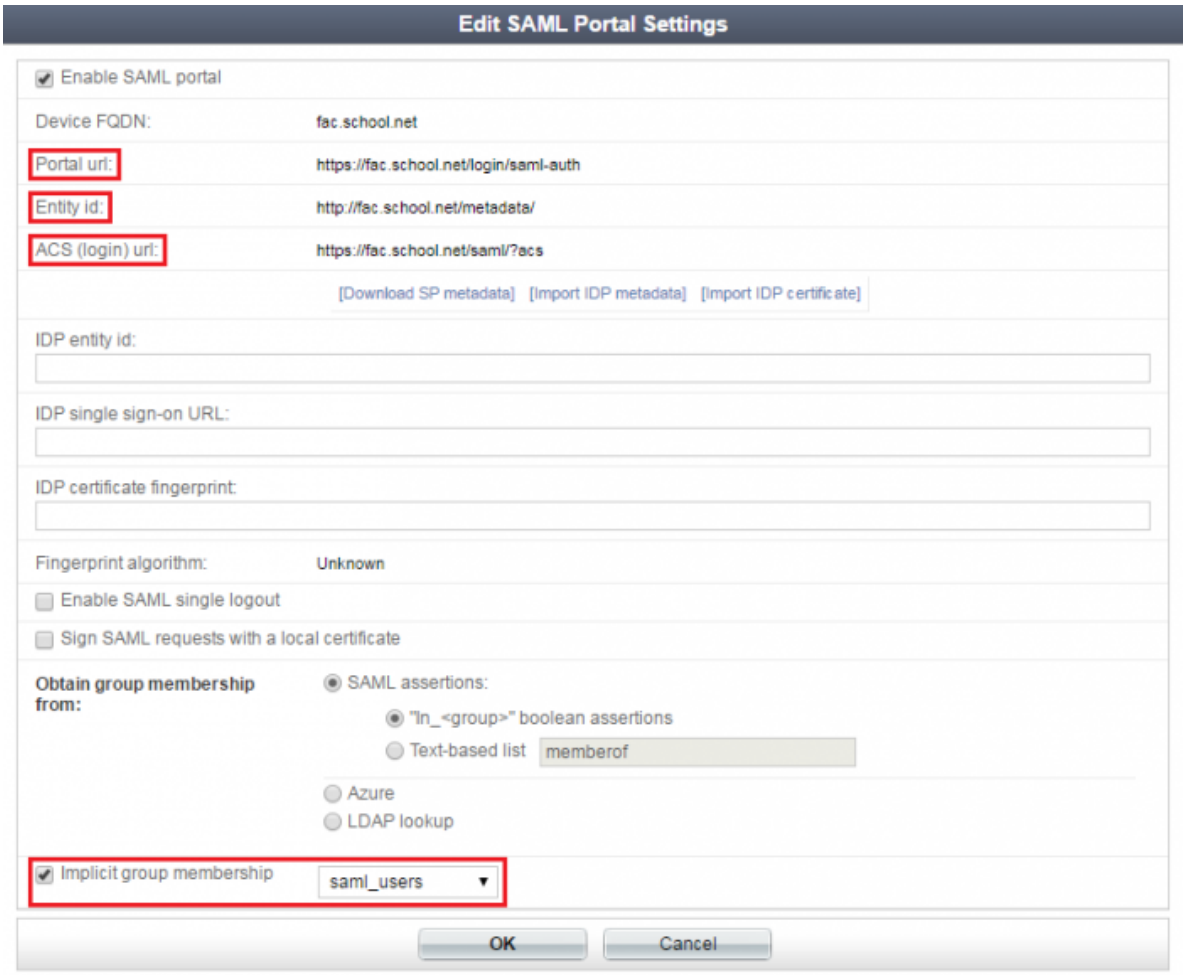
Enabling FSSO and SAML on the FortiAuthenticator

1. On the FortiAuthenticator, go to **Fortinet SSO Methods > SSO > General** and set FortiGate SSO options. Make sure to **Enable authentication**.
   Enter a **Secret key** and select **OK** to apply your changes. This key will be used on the FortiGate to add the FortiAuthenticator as the FSSO server.



2. Then go to **Fortinet SSO Methods > SSO > SAML Authentication** and select **Enable SAML portal**. All necessary URLs are automatically generated:
   - **Portal url** - Captive Portal URL for the FortiGate and user.
   - **Entity id** - Used in the Okta SAML IdP application setup.
   - **ACS (login) url** - Assertion POST URL used by the SAML IdP.

   Enable **Implicit group membership** and assign the **saml_users** group from the drop-down menu. This will place SAML authenticated users into this group.

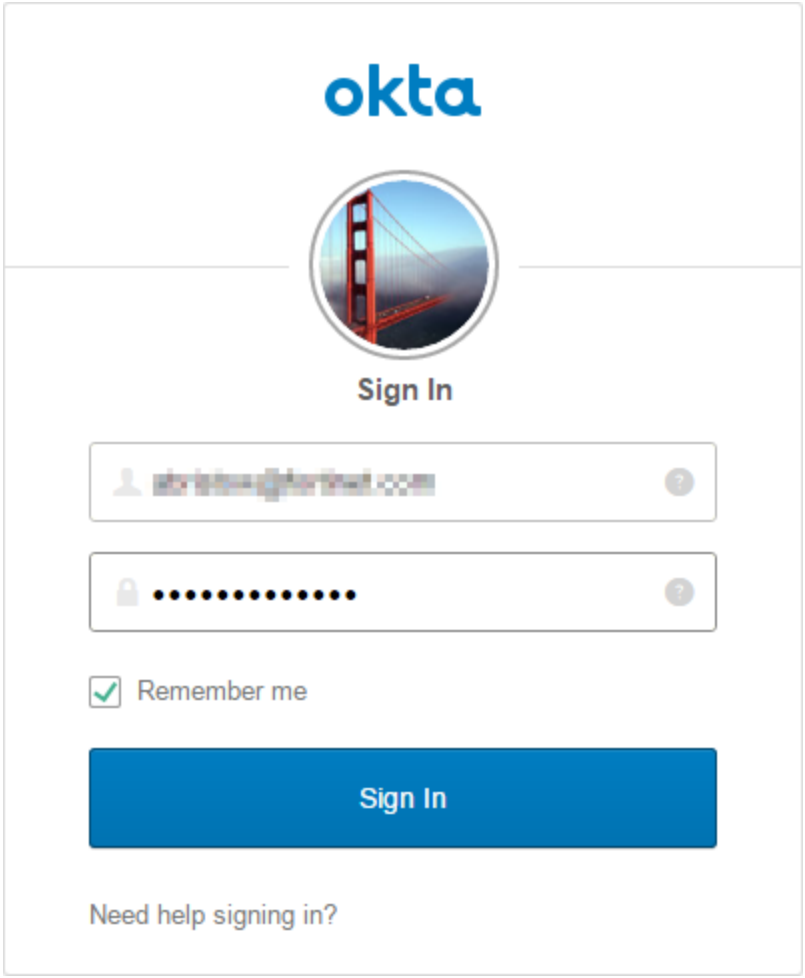


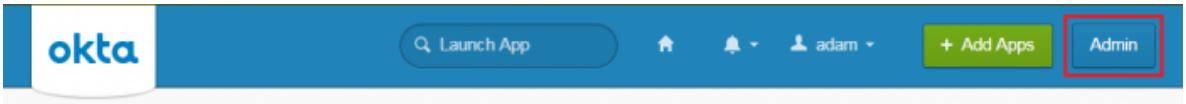
Keep this window open as these URLs will be needed during the IdP application configuration and for testing.

Note that, at this point, you will not be able to save these settings, as the IdP information — **IDP entity id**, **IDP single sign-on URL**, and **IDP certificate fingerprint** — needs to be entered. These fields will be filled once the IdP application configuration is complete.

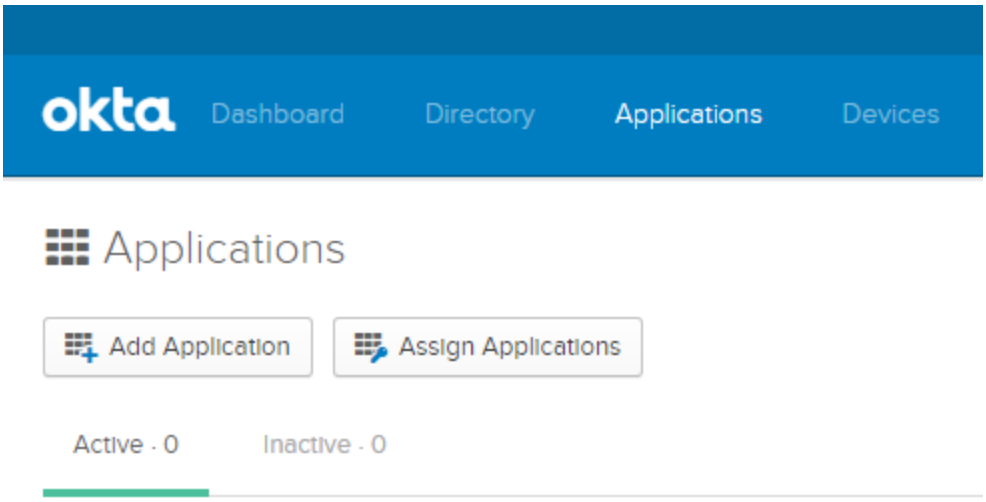
Configuring the Okta developer account IDP application

1. Open a browser, log in to your Okta developer account, and select Admin under your user settings.

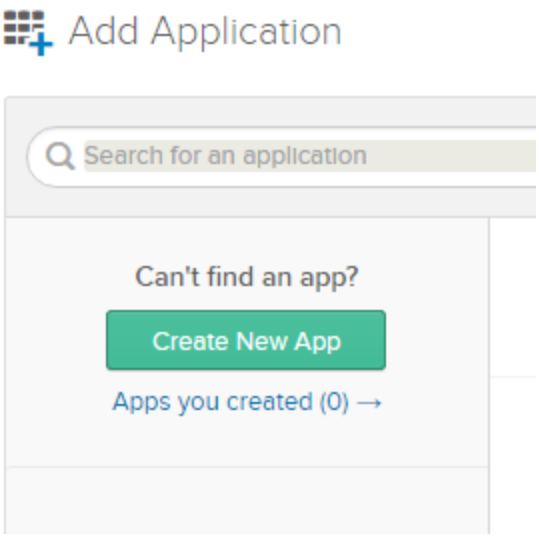


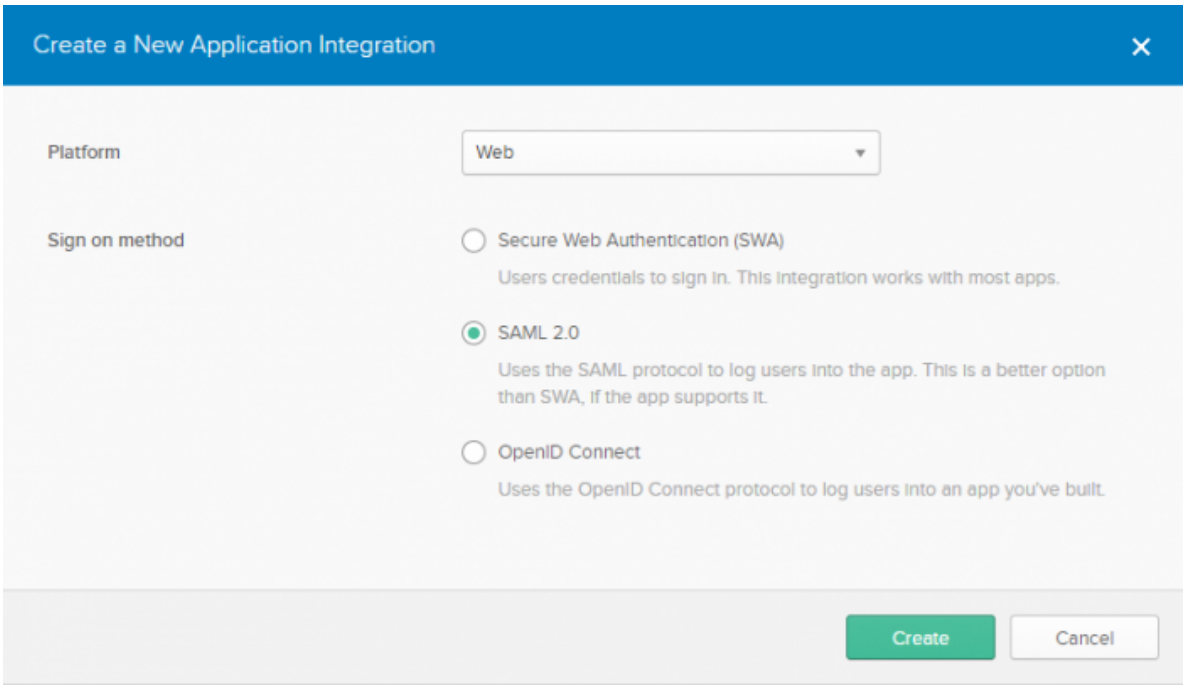


2. Go to the **Applications** tab and select **Add Application**.

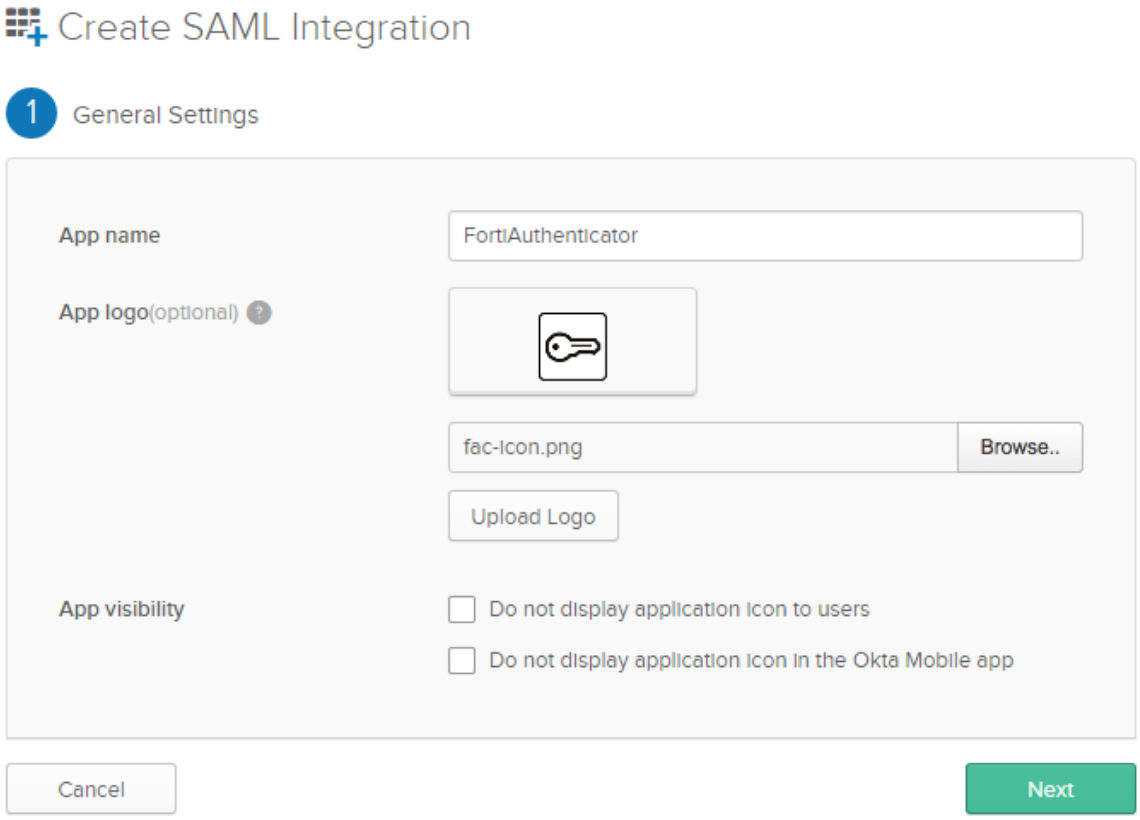


3. Select **Create New App** and create a new application with the SAML 2.0 sign on method.





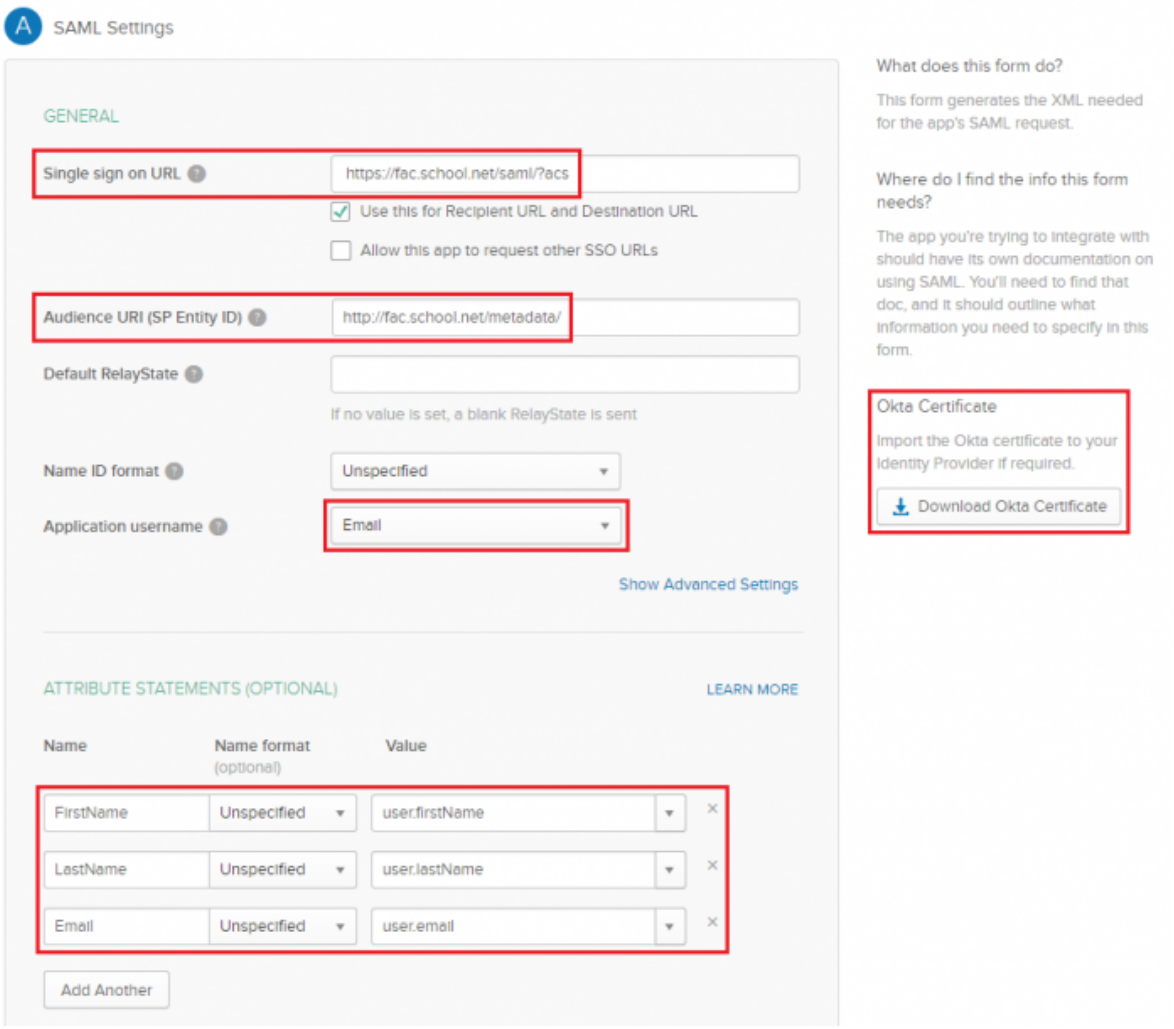
4. Enter a custom App name and select Next (upload an App logo if you wish).
Note that the name entered here is the name of the portal the user will log into.



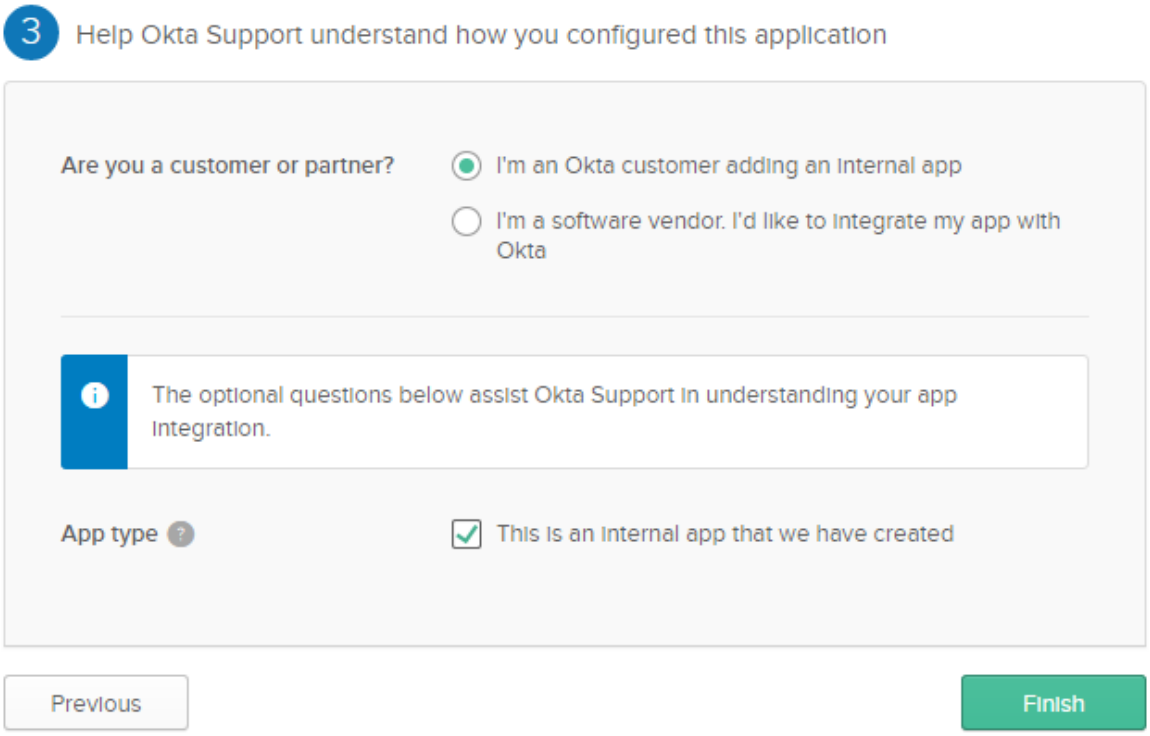
5. Under A – SAML Settings, set Single sign on URL and Audience URI (SP Entity ID) to the ACS and Entity URLs (respectively) from the Edit SAML Portal Settings page on the FortiAuthenticator.

Users will be required to provide their email address as their username, and their first and last names (as seen in the example).

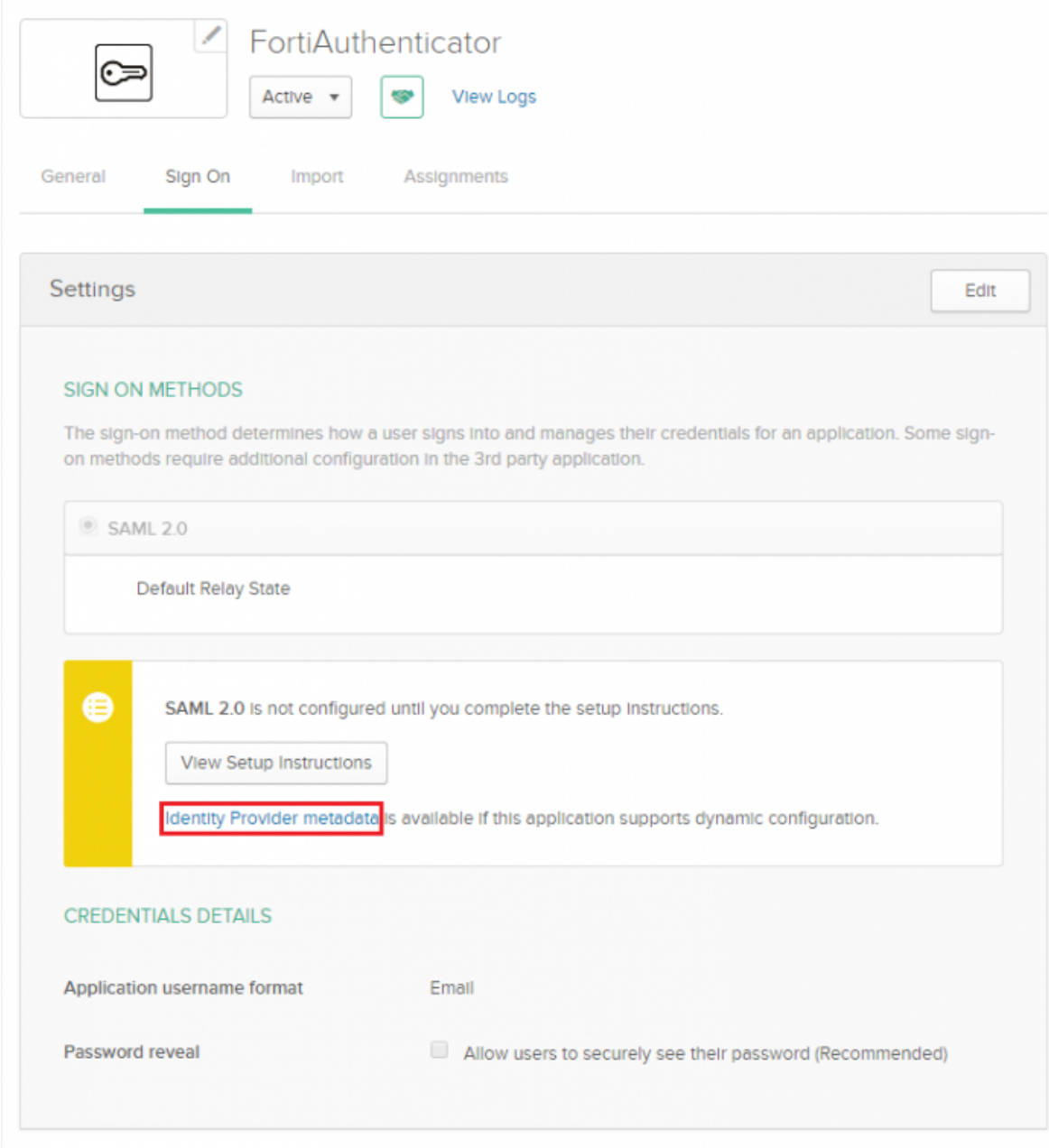
Before continuing, make sure to select **Download Okta Certificate**. This will be imported to the FortiAuthenticator later. You do not need to configure group attributes or section **B** below.



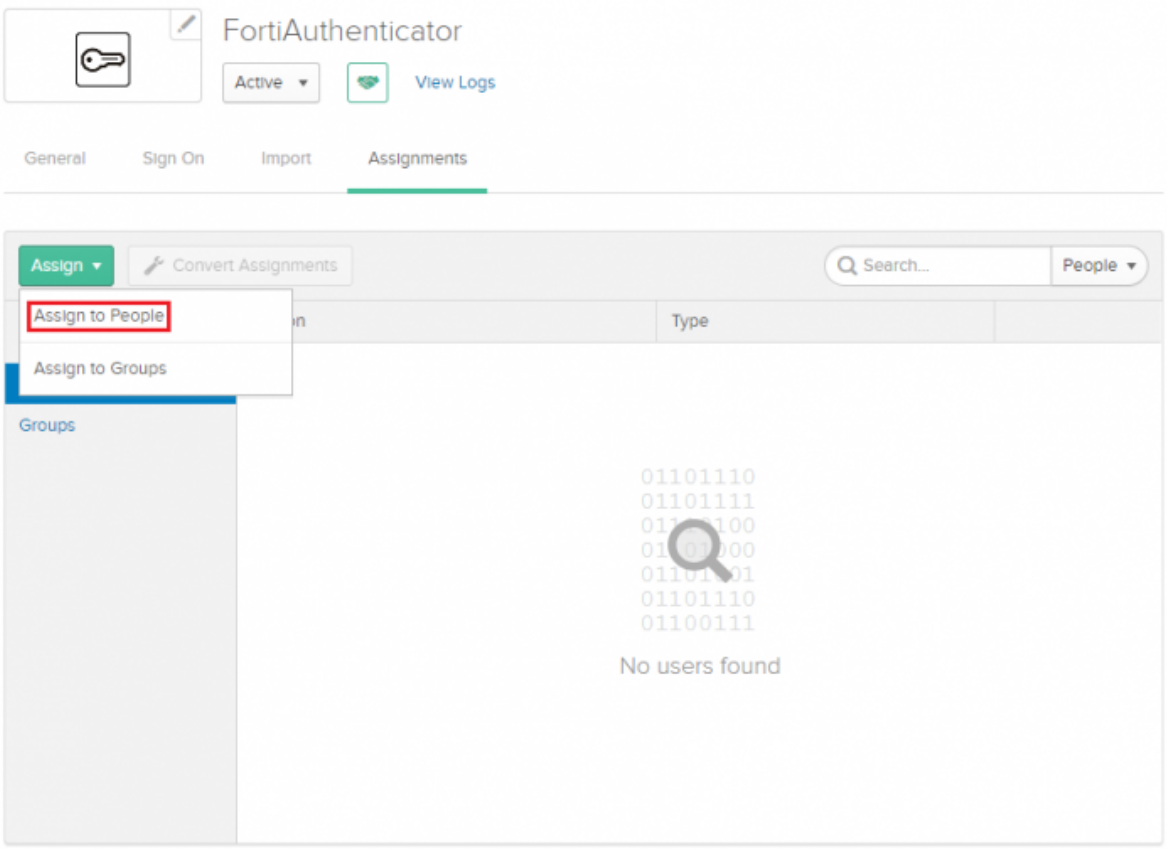
6. In the last step, confirm that you are an Okta customer, and set the **App type** to an internal app. Then select **Finish**.



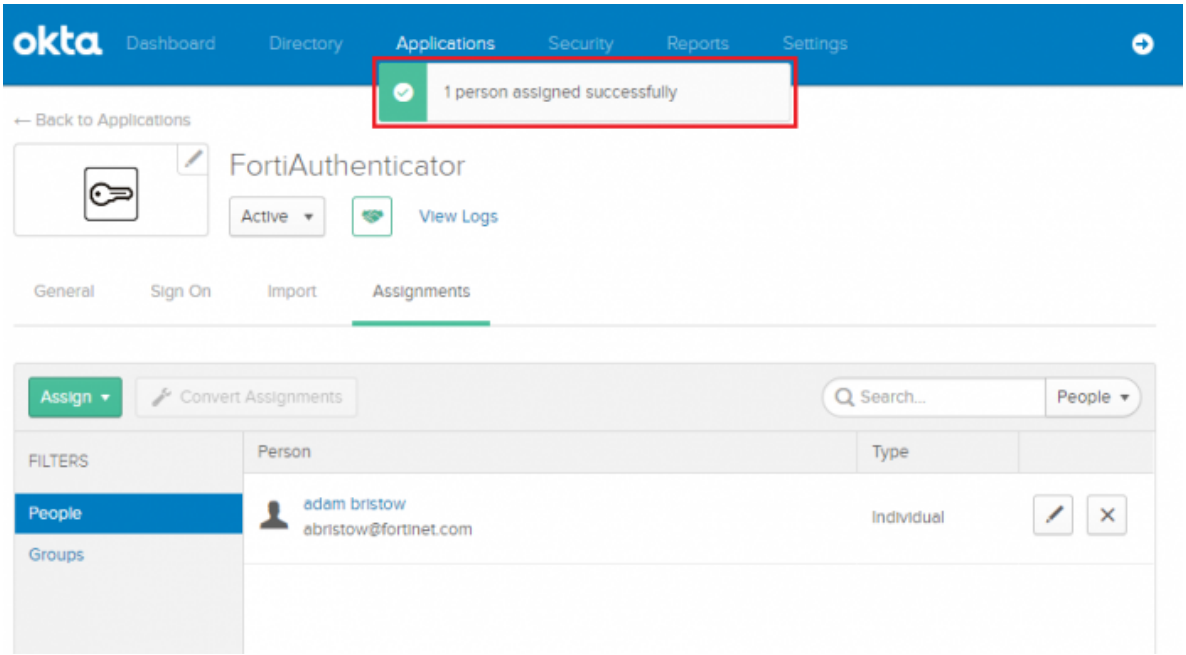
7. Once created, open the **Sign On** tab and download the **Identity Provider metadata**.



8. Finally, open the **Assignments** tab and select **Assign > Assign to People**.
   Assign the users you wish to add to the application. This will permit the user to log in to the application's portal. Save your changes and select **Done**.

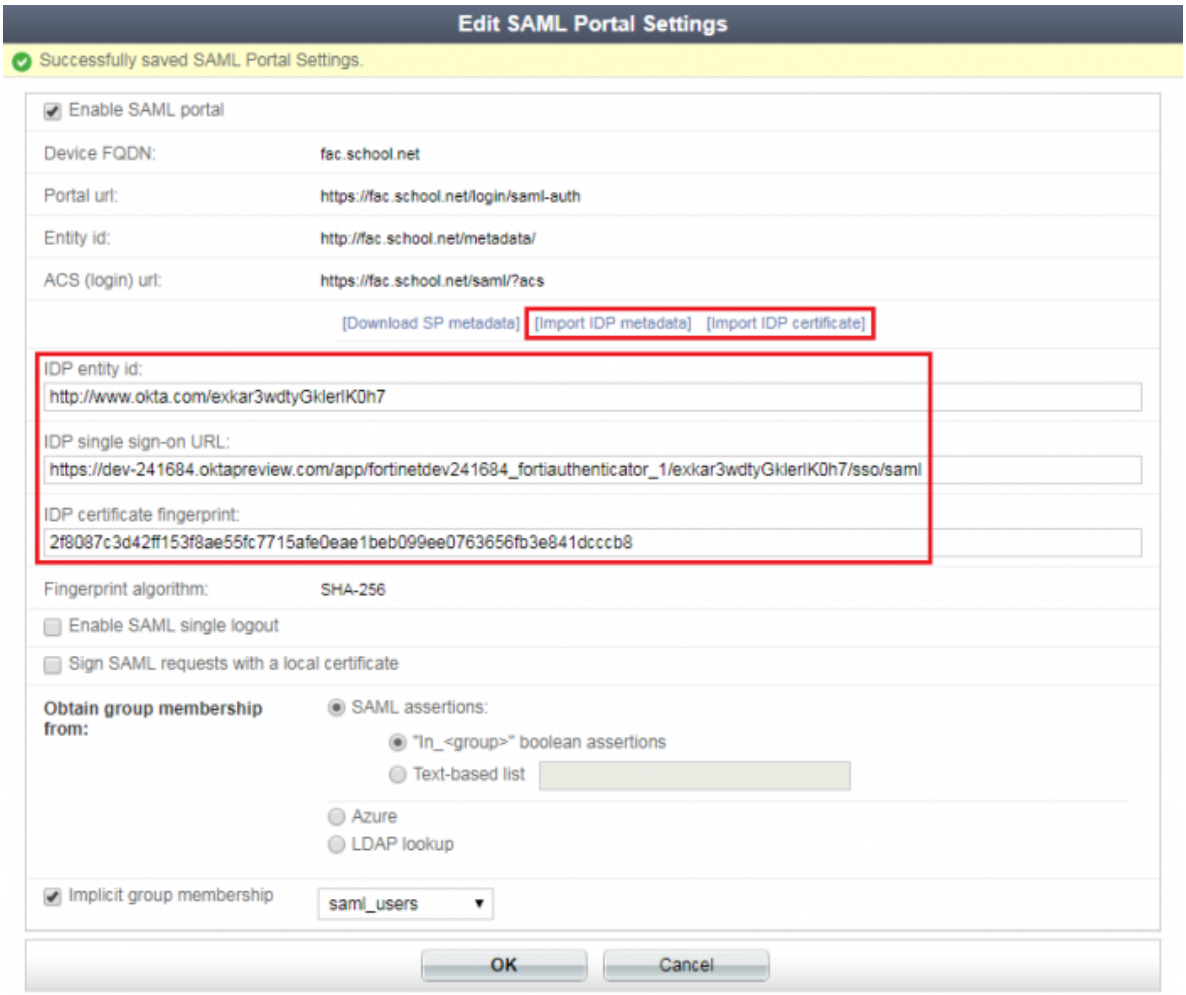


The user is successfully assigned. This concludes the steps necessary in configuring SAML 2.0.



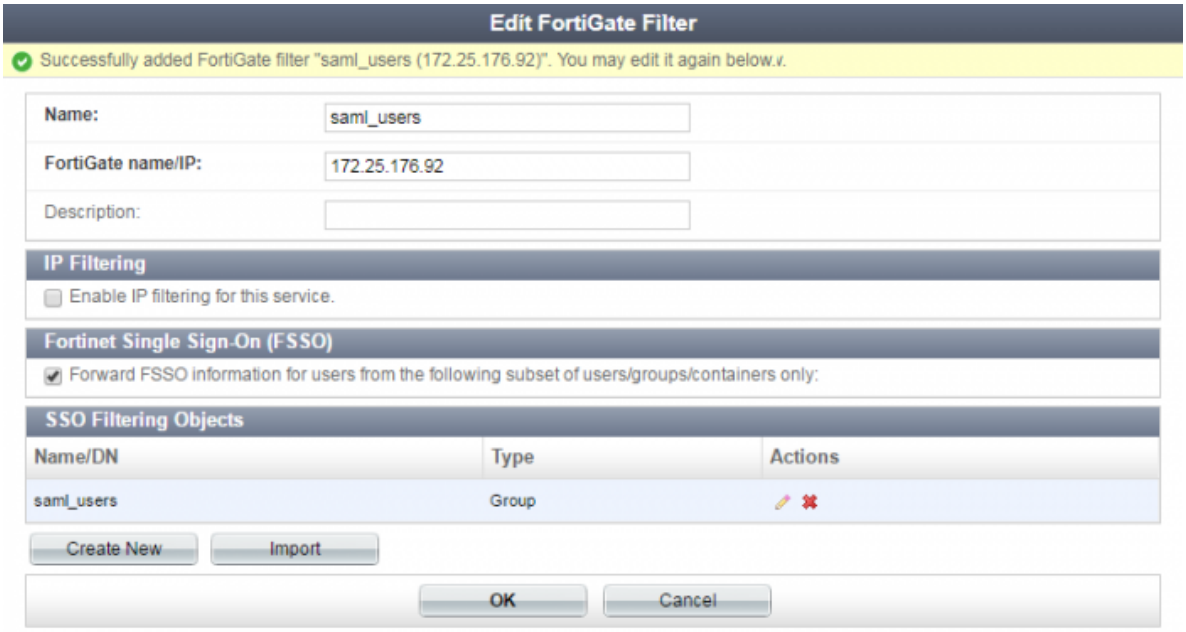
Importing the IDP certificate and metadata on the FortiAuthenticator

1. Back on the FortiAuthenticator, go to **Fortinet SSO Methods > SSO > SAML Authentication** and import the IDP metadata and certificate downloaded earlier.
   This will automatically fill the IDP fields (as shown in the example). Make sure to select **OK** to save these changes.



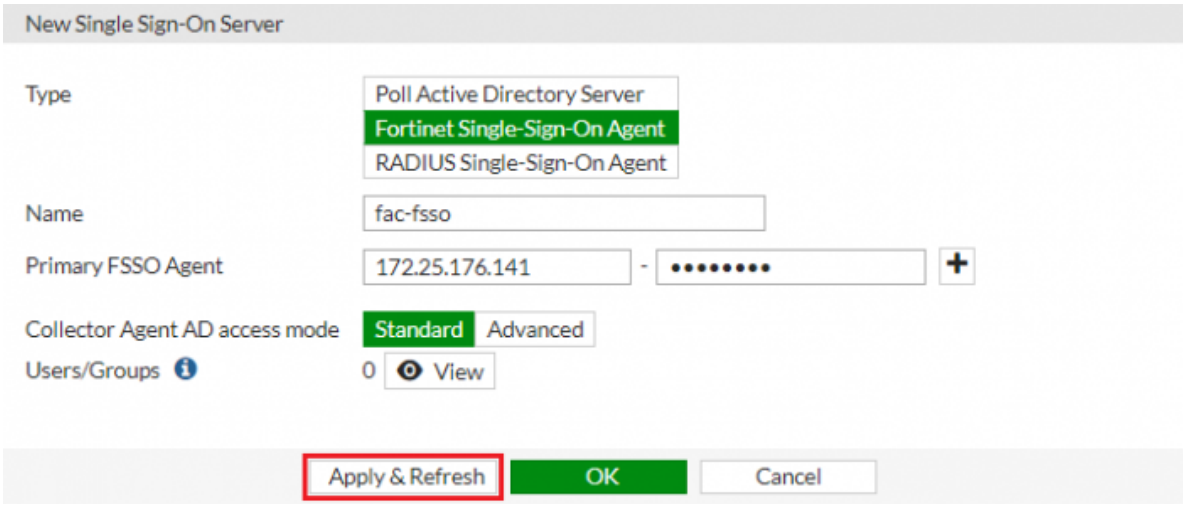
2. Next, go to **Fortinet SSO Methods > SSO > FortiGate Filtering** and create a new FortiGate filter. Enter a name and the FortiGate's wan-interface IP address, and select **OK**.
   Once created, enable **Fortinet Single Sign-On (FSSO)**. Select **Create New** to create an SSO group filtering object (as shown already created in the example), and select **OK** to apply all changes.
   Note that the name entered for the filter must be the same as the group name created for SAML users (**saml_users**). Failing to enter the exact same name will result in the SSO information not being pushed

to the FortiGate.

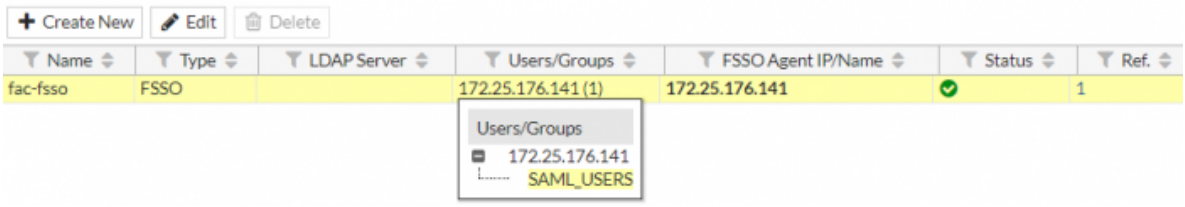


Configuring FSSO on the FortiGate

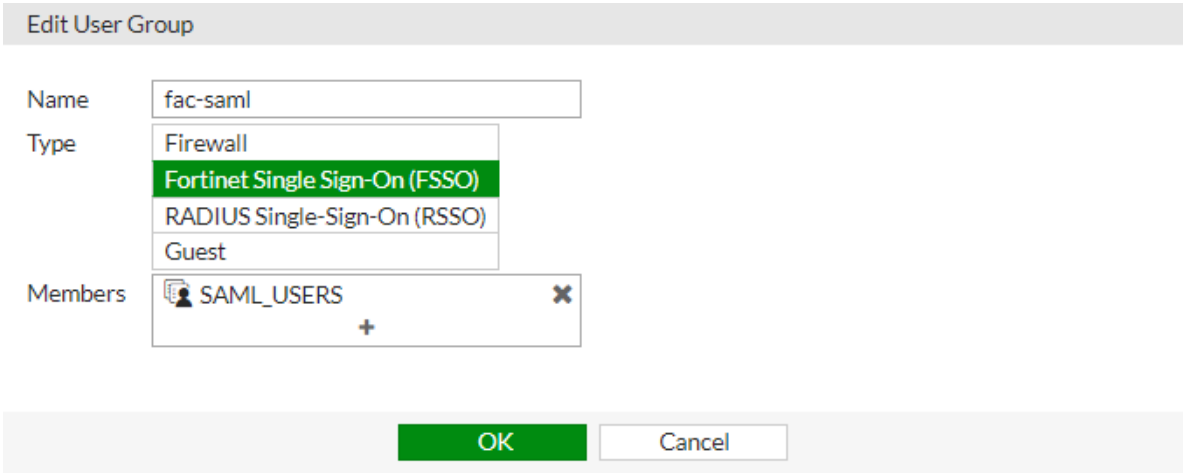
1. On the FortiGate, go to **User & Device > Single Sign-On** and select **Create New**.
   Set **Type** to **Fortinet Single Sign-On Agent**, enter a **Name**, the FortiAuthenticator's wan-interface IP, and the password, using the secret key entered into the FortiAuthenticator earlier.
   Select **Apply & Refresh**. The SAML user group name has been successfully pushed to the FortiGate from the FortiAuthenticator, appearing when you select **View**.
   Note that you may have to wait a few minutes before the user group appears.



2. Once created, the server will be listed. Mouse over the entry under the **Users/Groups** column and make sure that the FSSO group has been pushed down.

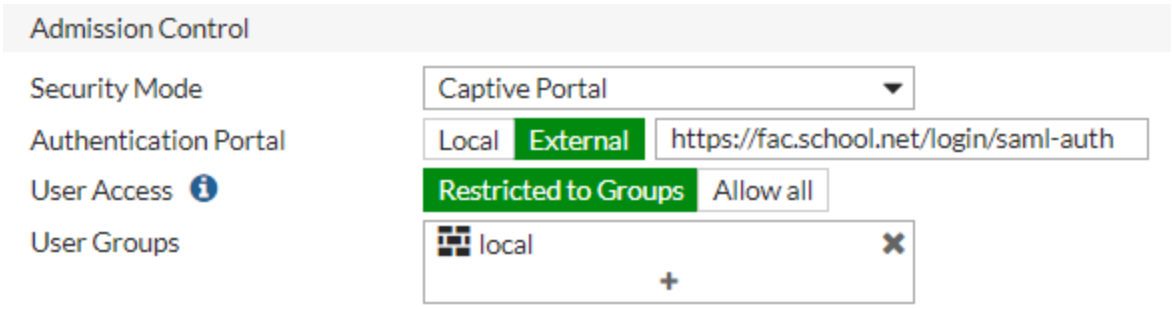


3. Then go to **User & Device > User Groups** and create a new user group.
   Enter a **Name**, set **Type** to **Fortinet Single Sign-On (FSSO)**, and add the FSSO group as a **Member**.

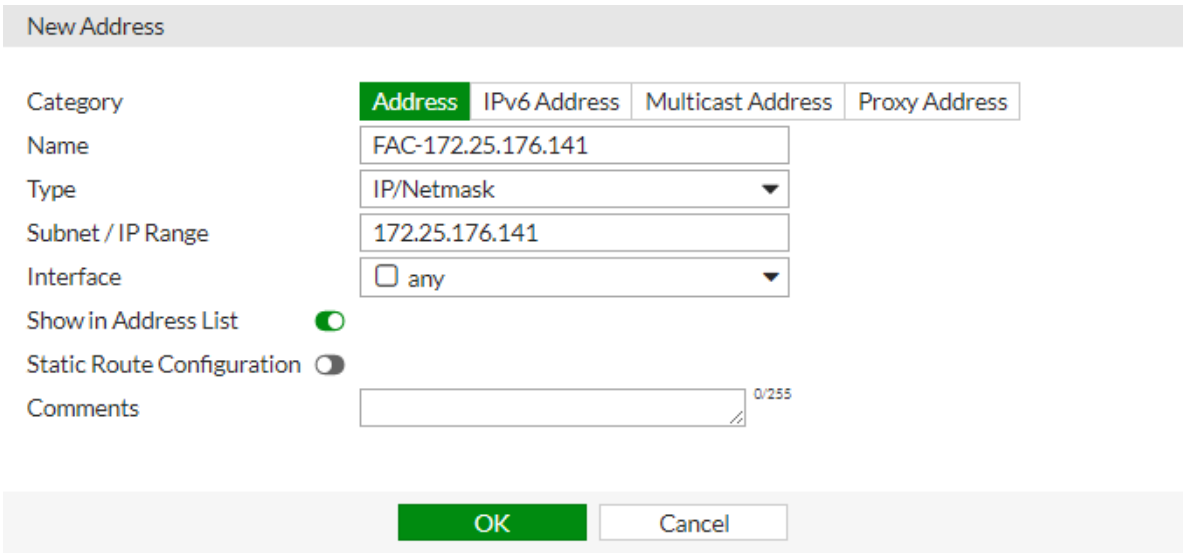


Configuring Captive Portal and security policies

1. On the FortiGate, go to **Network > Interfaces** and edit the internal interface.
   Under **Admission Control**, set **Security Mode** to **Captive Portal**.
   Set **Authentication Portal** to **External**, and enter the SAML authentication portal URL.
   Set **User Access** to **Restricted to Groups**, and set **User Groups** to any local group, as you'll notice the FSSO group is not available; this local group won't be used for access.

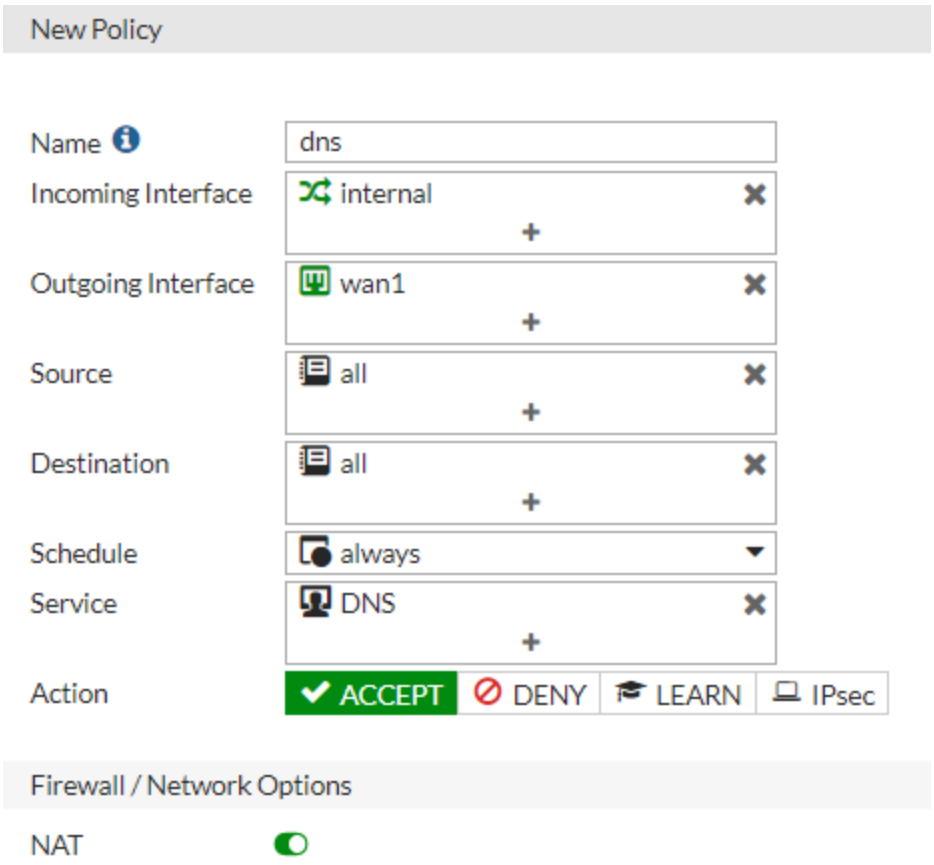


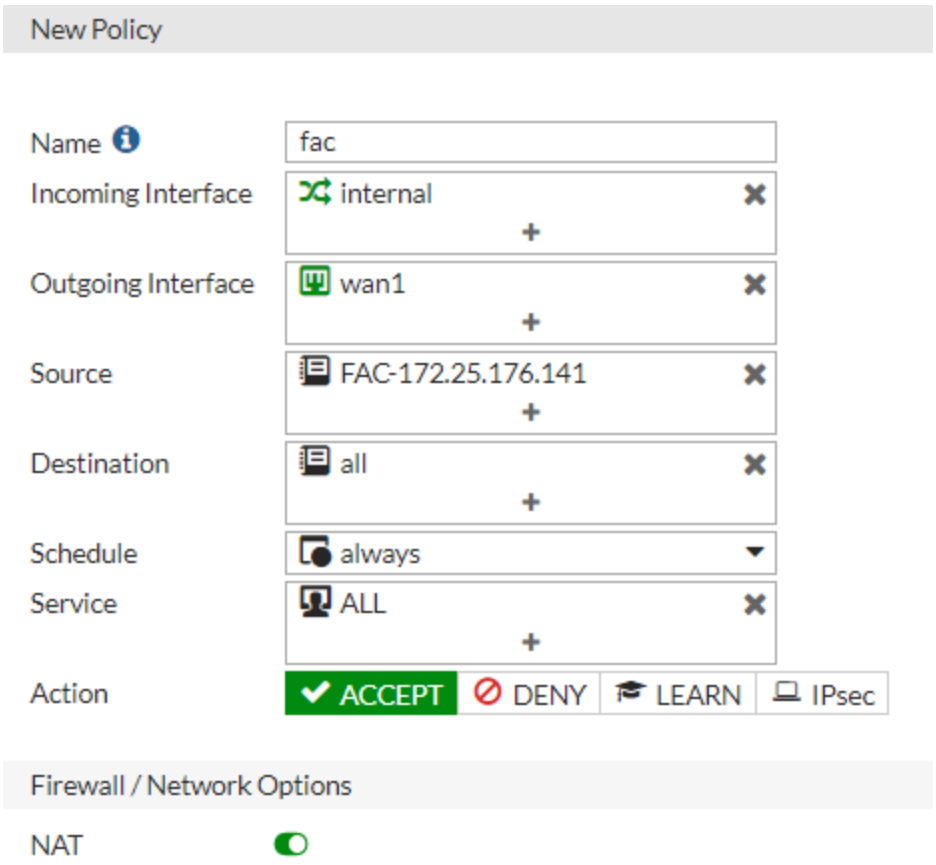
2. Next go to **Policy & Objects > Addresses** and add the FortiAuthenticator as an address object.

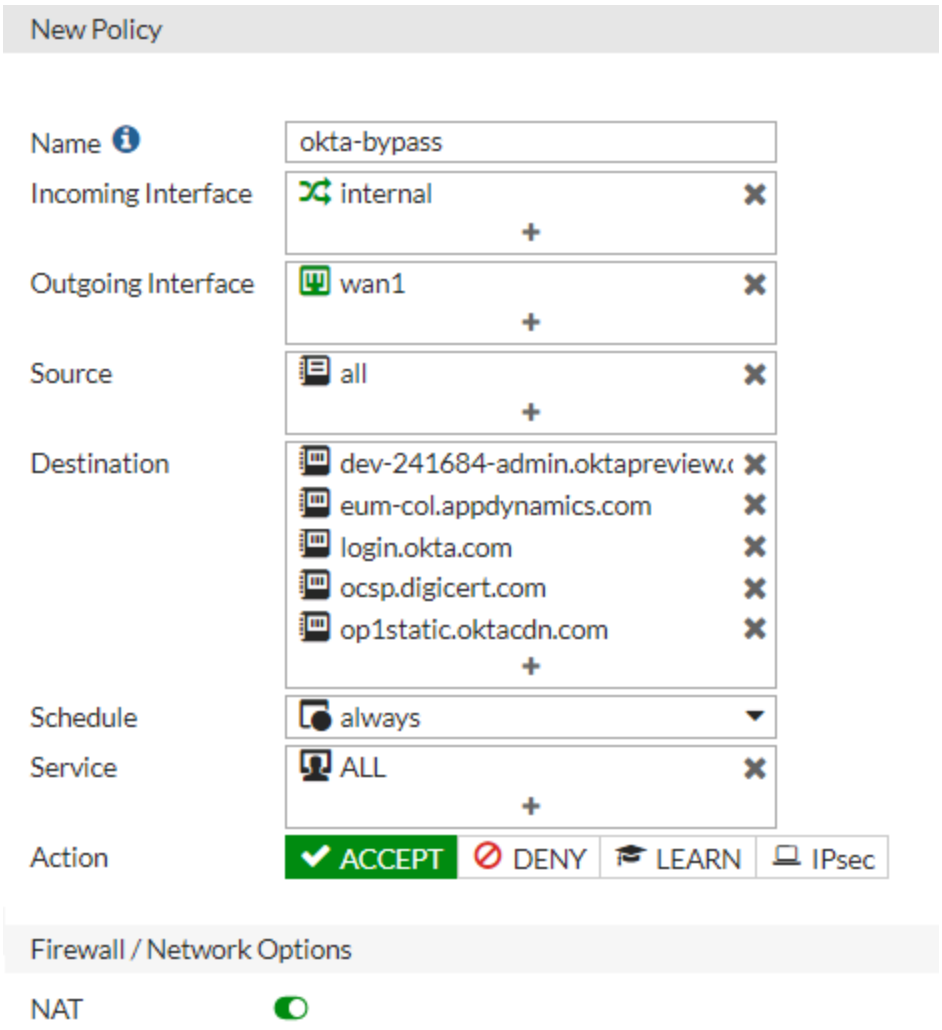


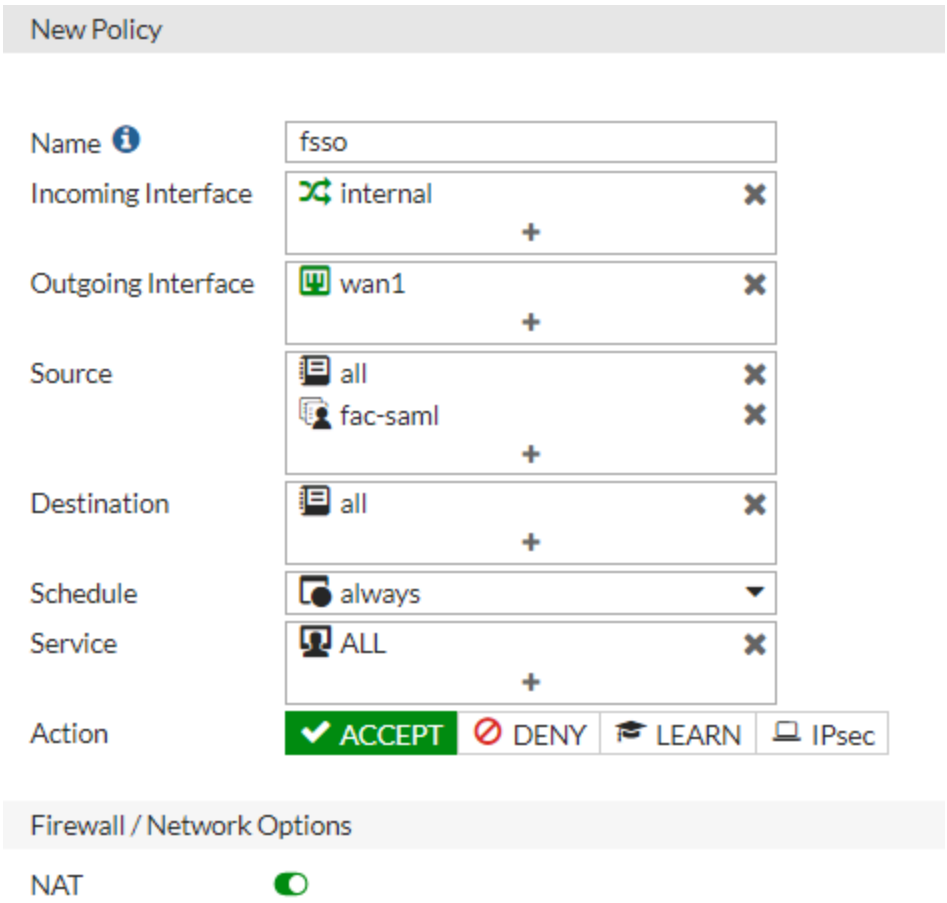
3. Then create five FQDN objects: one of your Okta developer page and the following:
   - eum-col.appdynamics.com
   - login.okta.com
   - ocsp.digicert.com
   - op1static.oktacdn.com

   As these are FQDNs, make sure to set **Type** to **FQDN**.
4. Then go to **Policy & Objects > IPv4 Policy** and create all policies shown in the examples: a policy for DNS, for access from FortiAuthenticator, for Okta bypass, and the last policy for FSSO, including the SAML user group.


New Policy
Name
dns
Incoming Interface
internal
Outgoing Interface
wan1
Source
all
Destination
all
Schedule
always
Service
DNS
Action
ACCEPT
DENY
LEARN
IPsec
Firewall / Network Options
NAT


New Policy
Name
fac
Incoming Interface
internal
Outgoing Interface
wan1
Source
FAC-172.25.176.141
Destination
all
Schedule
always
Service
ALL
Action
ACCEPT
DENY
LEARN
IPsec
Firewall / Network Options
NAT


New Policy
Name
okta-bypass
Incoming Interface
internal
Outgoing Interface
wan1
Source
all
Destination
dev-241684-admin.oktapreview.(
eum-col.appdynamics.com
login.okta.com
ocsp.digicert.com
op1static.oktacdn.com
Schedule
always
Service
ALL
Action
ACCEPT
DENY
LEARN
IPsec
Firewall / Network Options
NAT



5. When finished, right-click each policy (*except* the FSSO policy), select Edit in CLI, and enter the following command:

```
    set captive-portal-exempt enable
  next
end
```

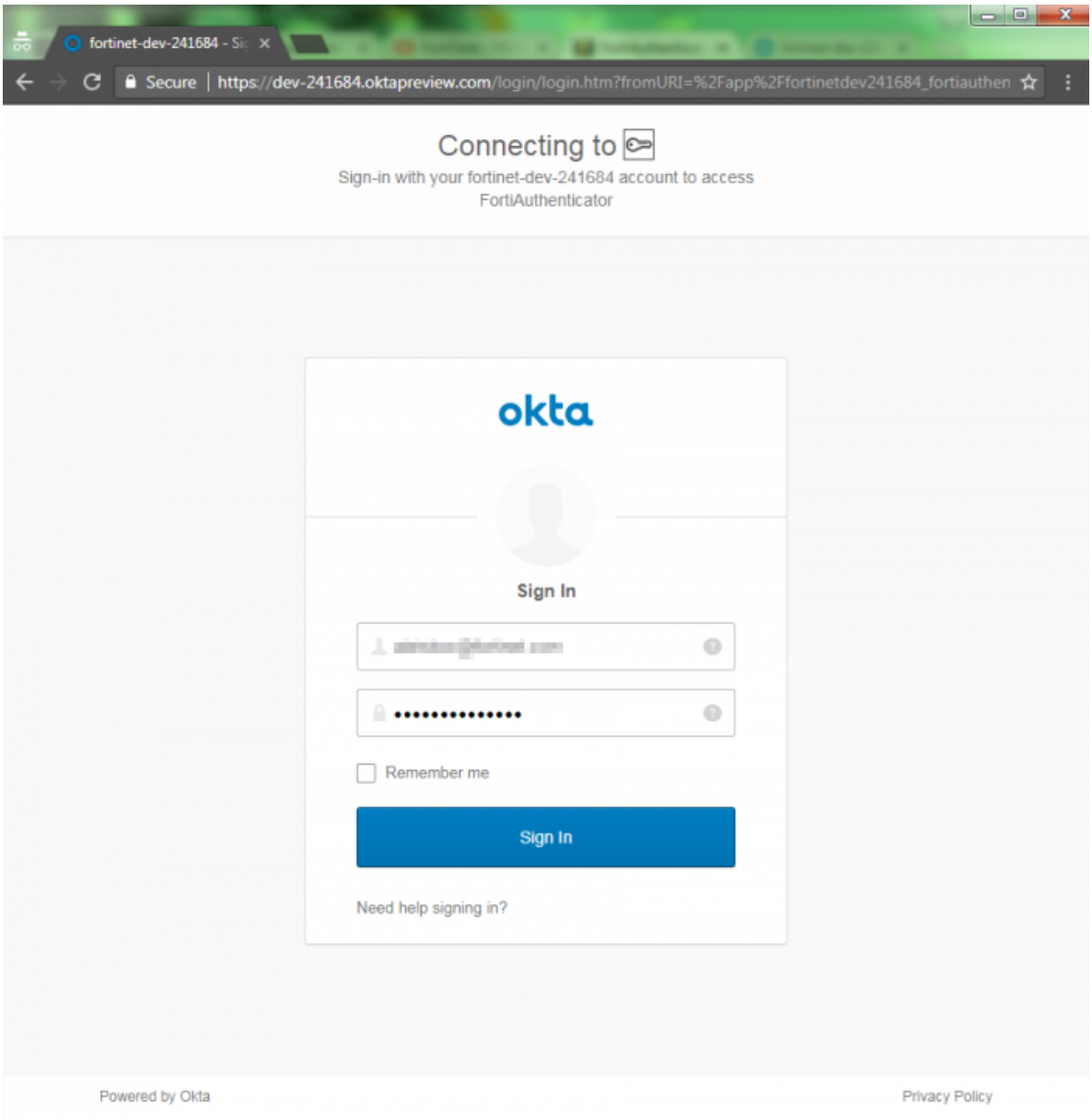
This command will exempt users of this policy from the captive portal interface.

Results

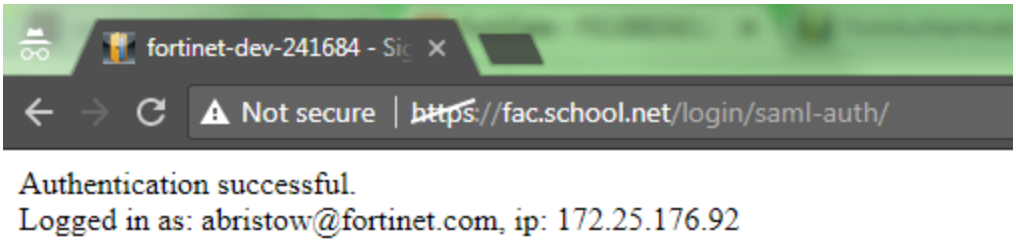
To test the connection, open a new browser window and attempt to browse the Internet. The browser will redirect to the FortiAuthenticator SAML portal, which pushes the browser to the SAML IdP.

Alternatively, you can directly navigate to the portal URL.

1. Enter the user's credentials and select **Sign In**.



The assertion is pushed back to the FortiAuthenticator where the user is authenticated.



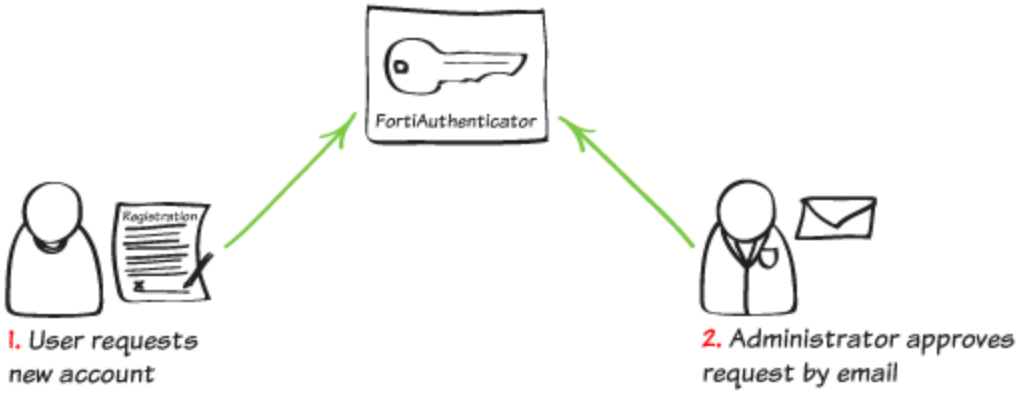
2. On the FortiAuthenticator, go to **Monitor > SSO > SSO Sessions** to view the user and assigned user group.

3. On the FortiGate, go to **Monitor > Firewall User Monitor** to view user information, and confirm that the user has been authenticated via FSSO.

Self-service Portal

Configure general self-service portal options, including access control settings, self-registration options, replacement messages, and device self-enrollment settings.

FortiAuthenticator user self-registration



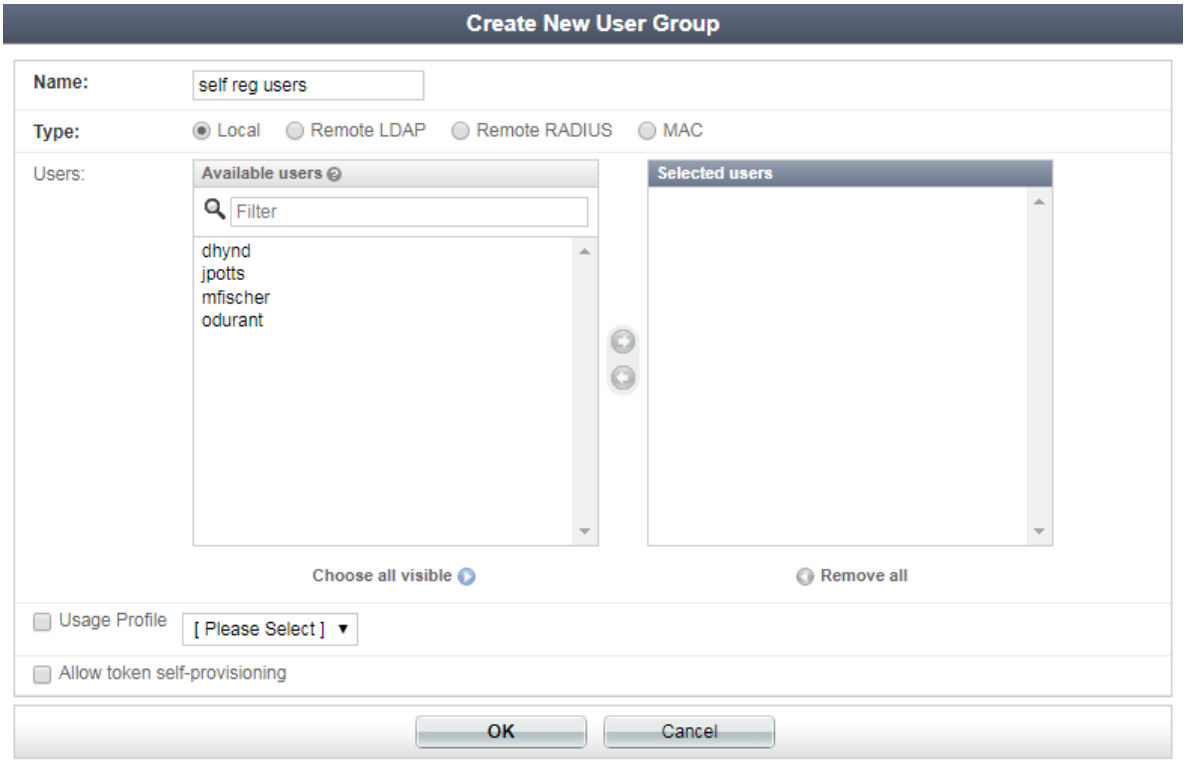
For this recipe, you will configure the FortiAuthenticator self-service portal to allow users to add their own account and create their own passwords.

Note that enabling and using administrator approval requires the use of an email server, or SMTP server. Since administrators will approve requests by email, this recipe describes how to add an email server to your FortiAuthenticator. You will create and use a new server instead of the unit's default server.

Creating a self-registration user group

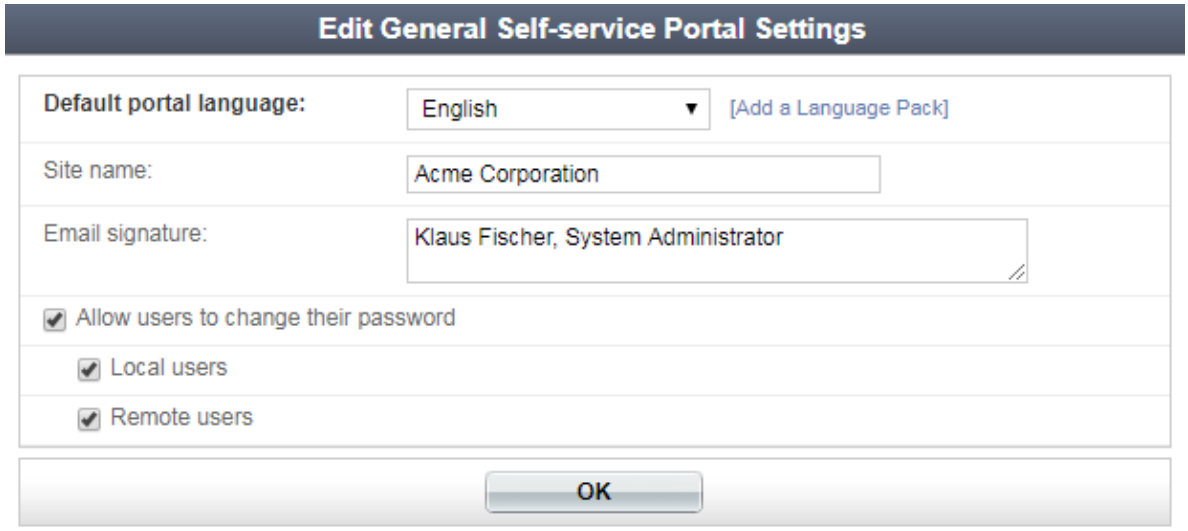
1. Go to **Authentication > User Management > User Groups** and create a new user group for self-registering users.
   Enter a **Name** and select **OK**. Users will be added to this group once they register through the self-

registration portal.



Enabling self-registration

1. Go to **Authentication > Self-service Portal > General**.
   Enter a **Site name**, add an **Email signature** that you would like appended to the end of outgoing emails, and select **OK**.

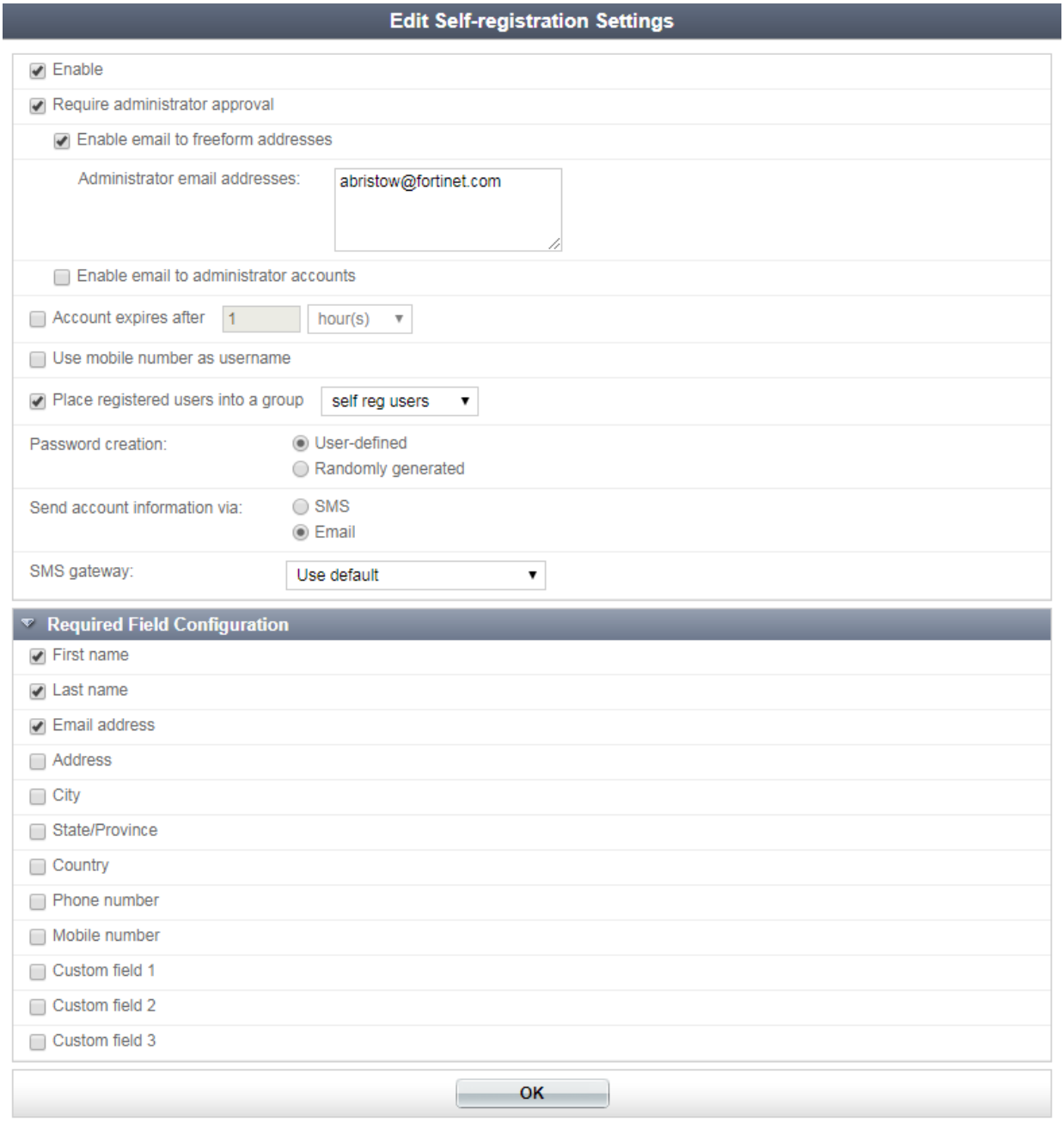


2. Then go to **Authentication > Self-service Portal > Self-registration** and select **Enable**.

Enable **Require administrator approval** and **Enable email to freeform addresses**, and enter the administrator's email address in the field provided.

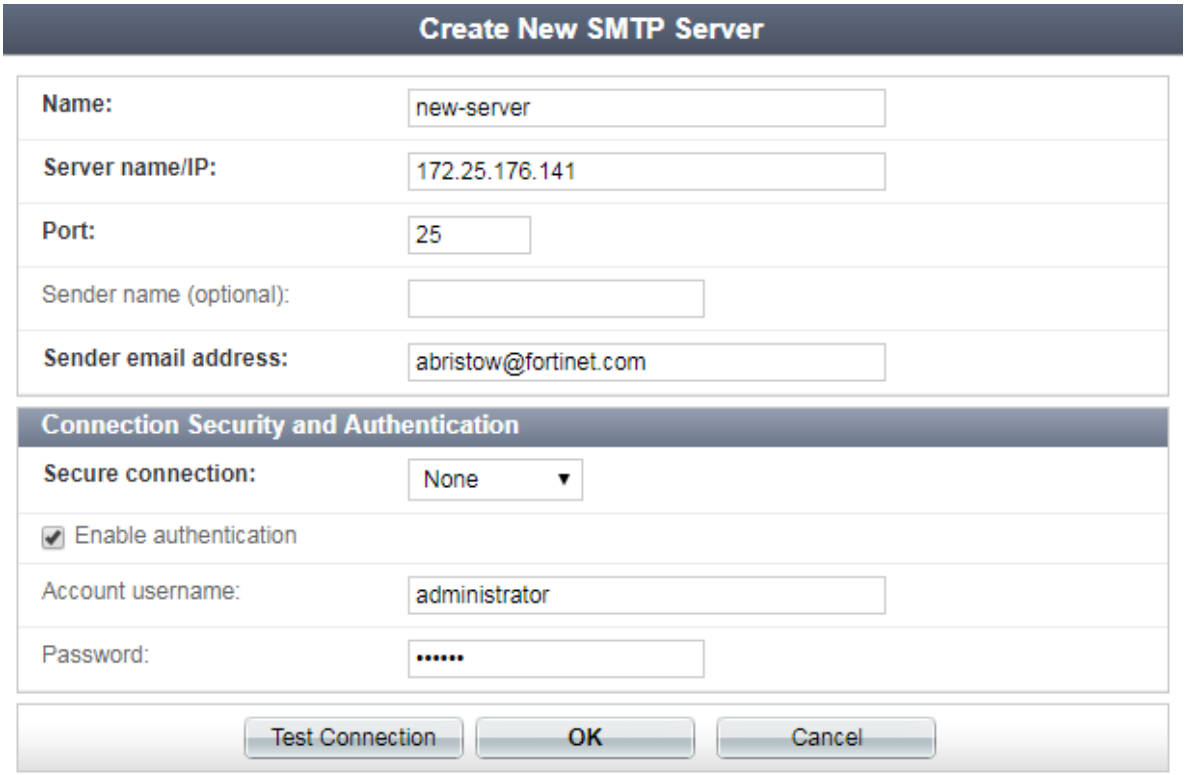
Enable **Place registered users into a group**, select the user group created earlier, and configure basic account information to be sent to the user by **Email**.

Open the **Required Field Configuration** drop-down and enable **First name**, **Last name**, and **Email address**.

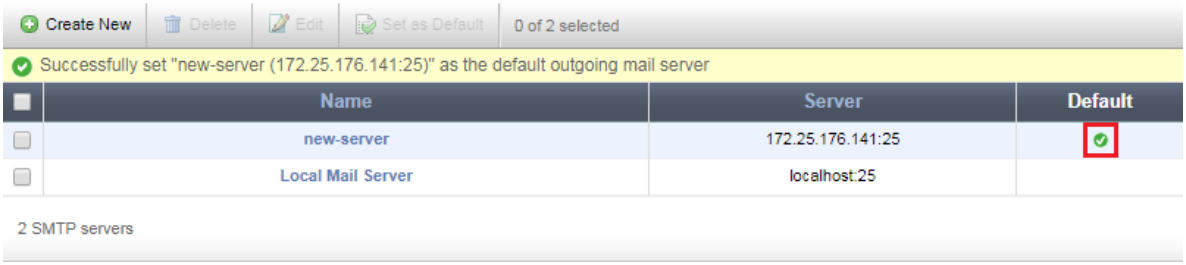


Creating a new SMTP server

1. Go to **System > Messaging > SMTP Servers** and create a new email server for your users.
   Enter a **Name**, the IP address of the FortiAuthenticator, and leave the default port value (25).
   Enter the administrator's email address, **Account username**, and **Password**.
   Note that, for the purpose of this recipe, **Secure connection** will not be set to **STARTTLS** as a signed CA certificate would be required.



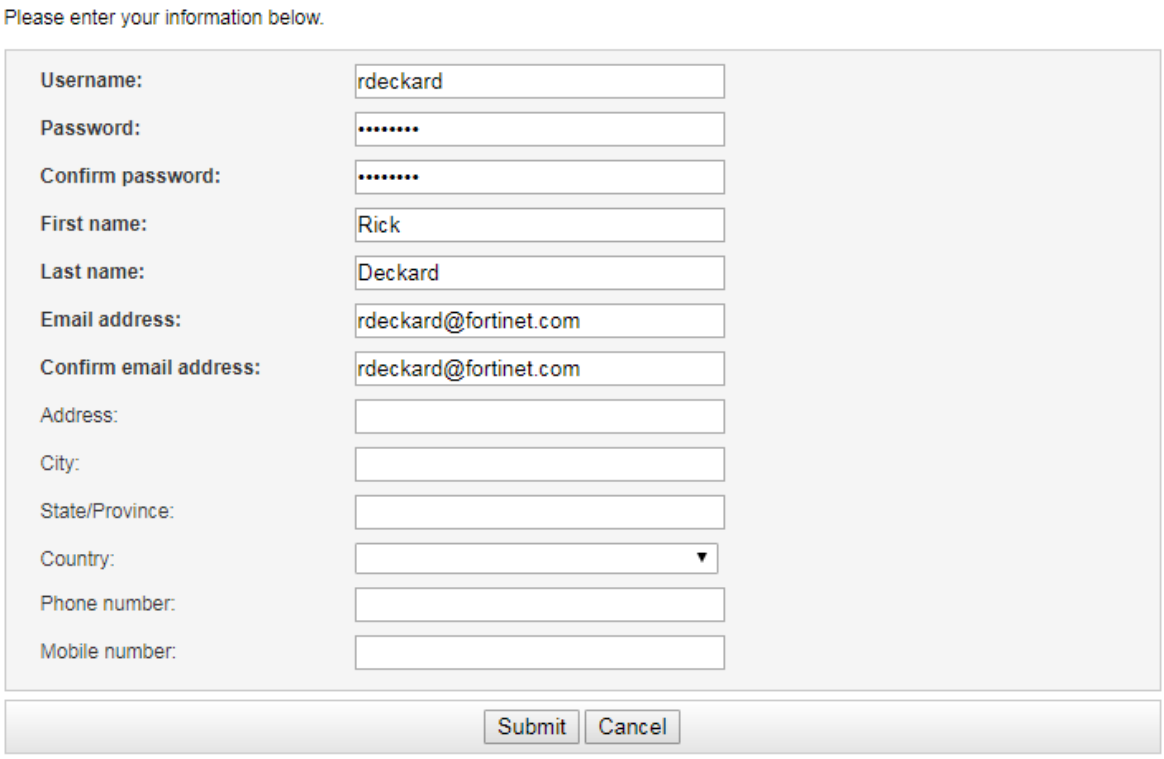
2. Once created, highlight the new server and select **Set as Default**.
   The new SMTP server will now be used for future user registration.



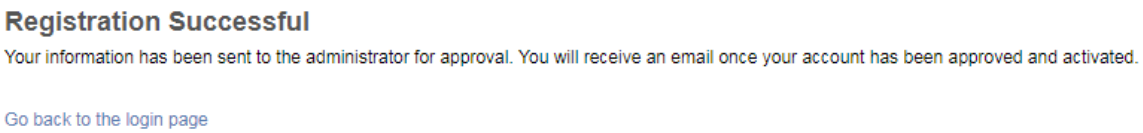
Results - Self-registration

1. When the user visits the login page, *https://<FortiAuthenticator-IP>/auth/register/*, they can click the **Register** button, where they will be prompted to enter their information.
   They will need to enter and confirm a **Username**, **Password**, **First name**, **Last name**, and **Email address**. These are the only required fields, as configured in the FortiAuthenticator earlier.

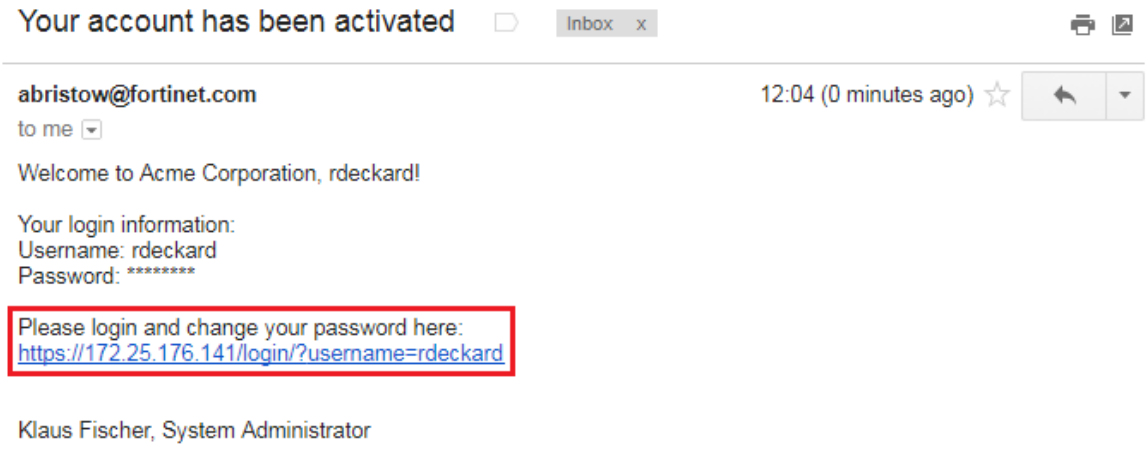
Select **Submit**.



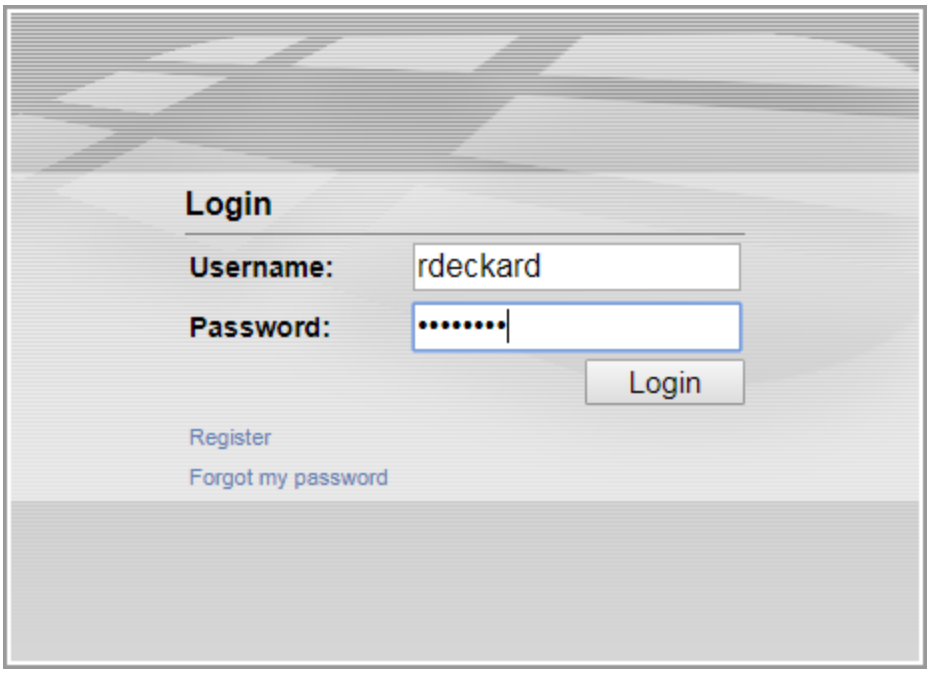
2. The user's registration is successful, and their information has been sent to the administrator for approval.



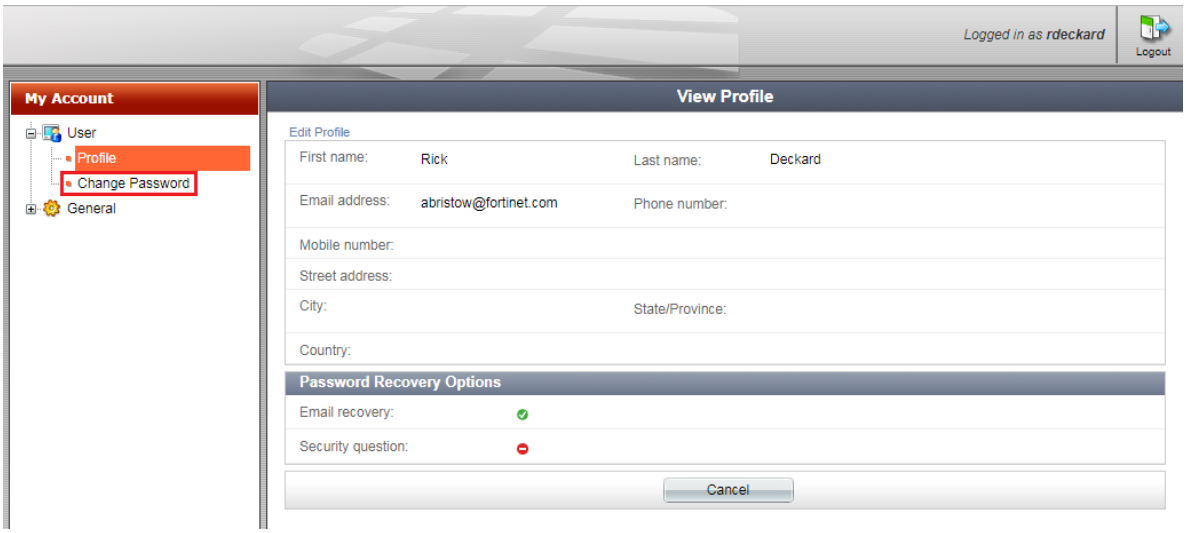
3. When the administrator has enabled the user's account, the user will receive an activation welcome email. The user's login information will be listed.



4. Select the link and log in to the user's portal.

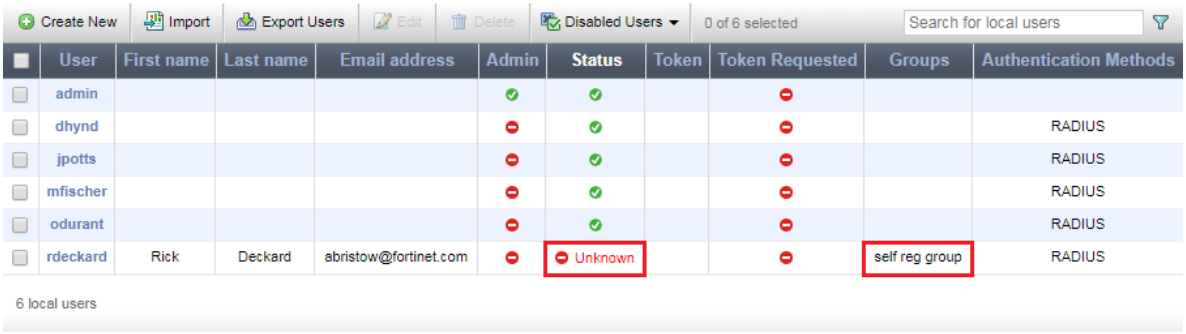


5. The user is now logged into their account where they can review their information.
   As recommended in the user's welcome email, the user may change their password. However, this is optional.

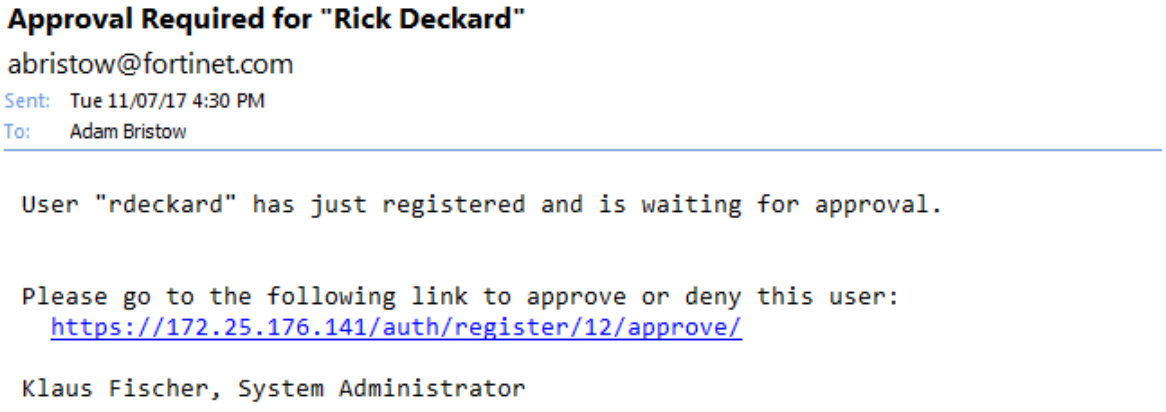


Results - Administrator approval

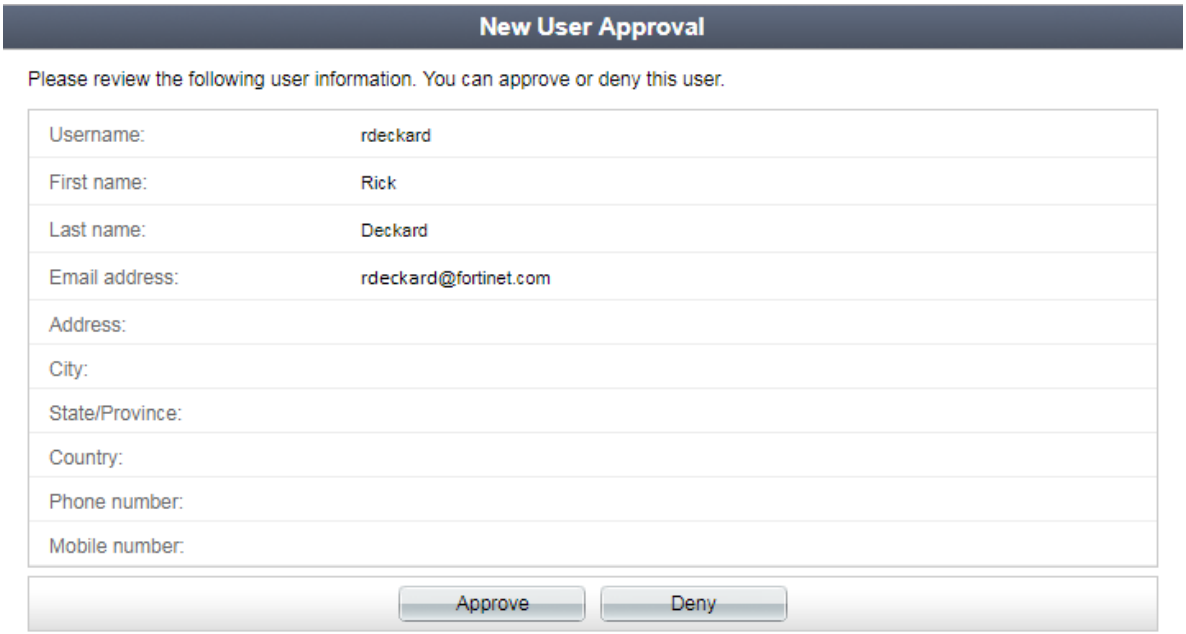
1. After receiving the user's registration request, in the FortiAuthenticator as the administrator, go to **Authentication > User Management > Local Users**. The user has been added, but their **Status** is listed as **Unknown**.



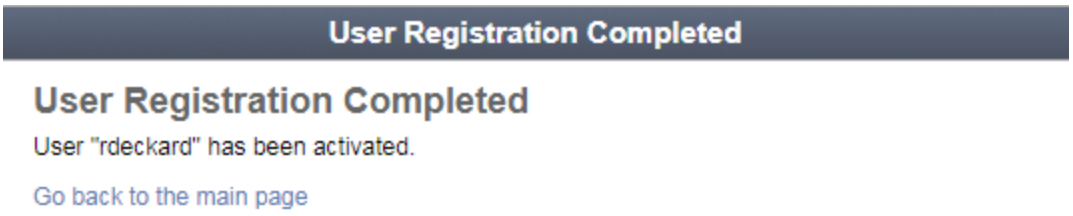
2. In the administrator's email account, open the user's **Approval Required** email. The user's full name will appear in the email's subject, along with their username in the email's body.
Select the link to approve or deny the user.



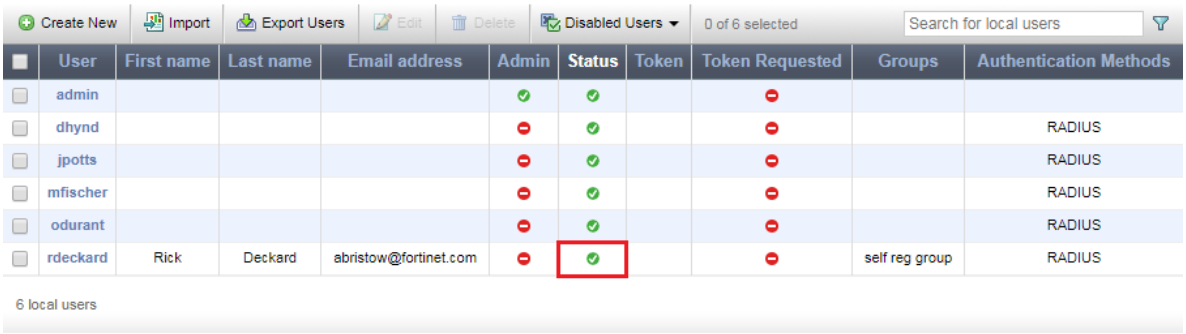
3. The link will take you to the **New User Approval** page, where you can review the user's information and either approve or deny the user's full registration.
Select **Approve**.



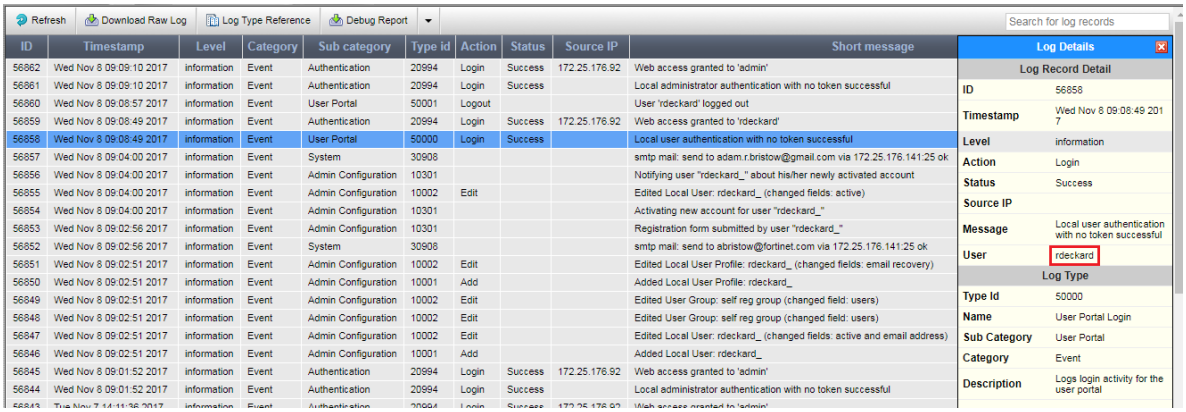
4. The user has now been approved and activated by the administrator.



This can be confirmed by going back to **Authentication > User Management > Local Users**. The user's **Status** has changed to **Enabled**.



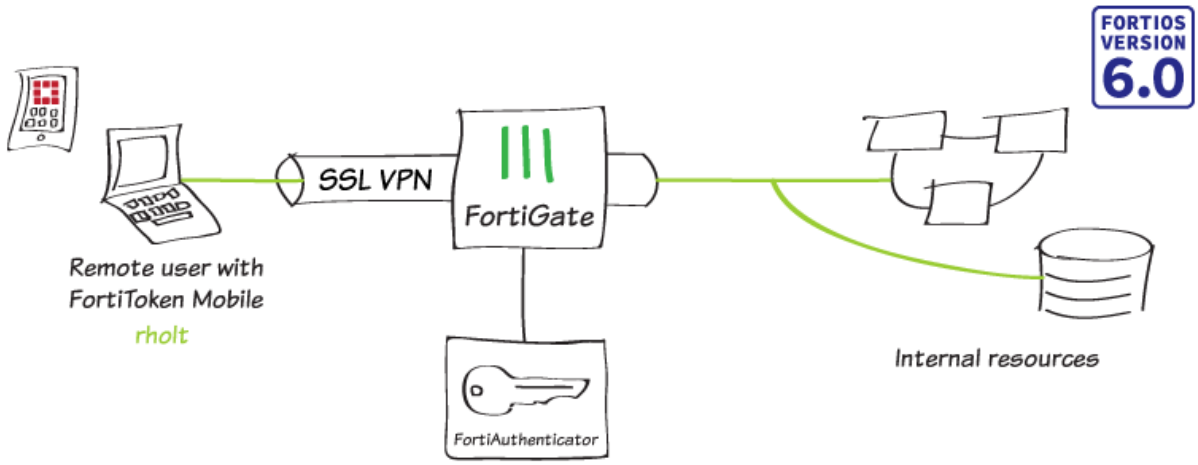
5. You can also go to **Logging > Log Access > Logs** to view the successful login of the user and more information.



VPNs

This section contains information about creating and using a virtual private network (VPN).

SSL VPN with RADIUS and FortiToken

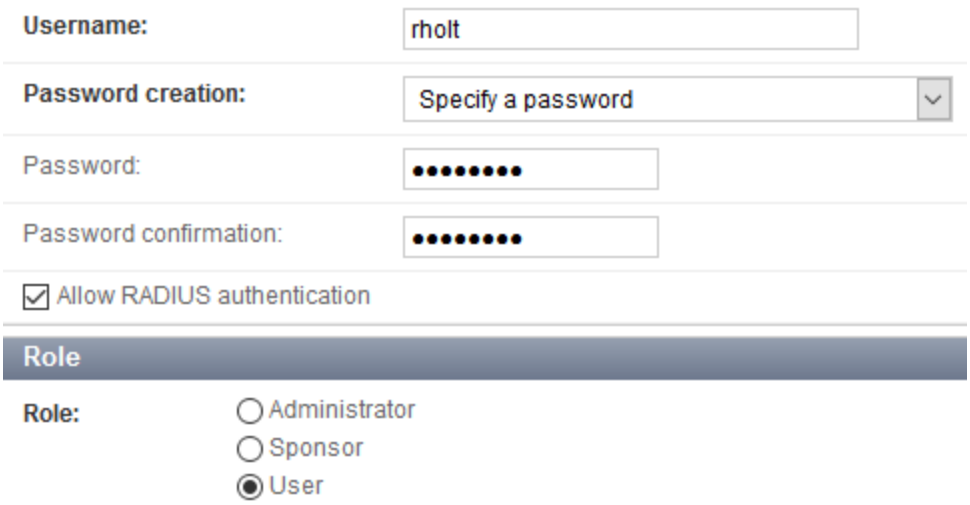


In this recipe, you configure a FortiAuthenticator as a RADIUS server to use with a FortiGate SSL VPN. Remote users connect to the SSL VPN using FortiClient and use FortiToken for two-factor authentication.

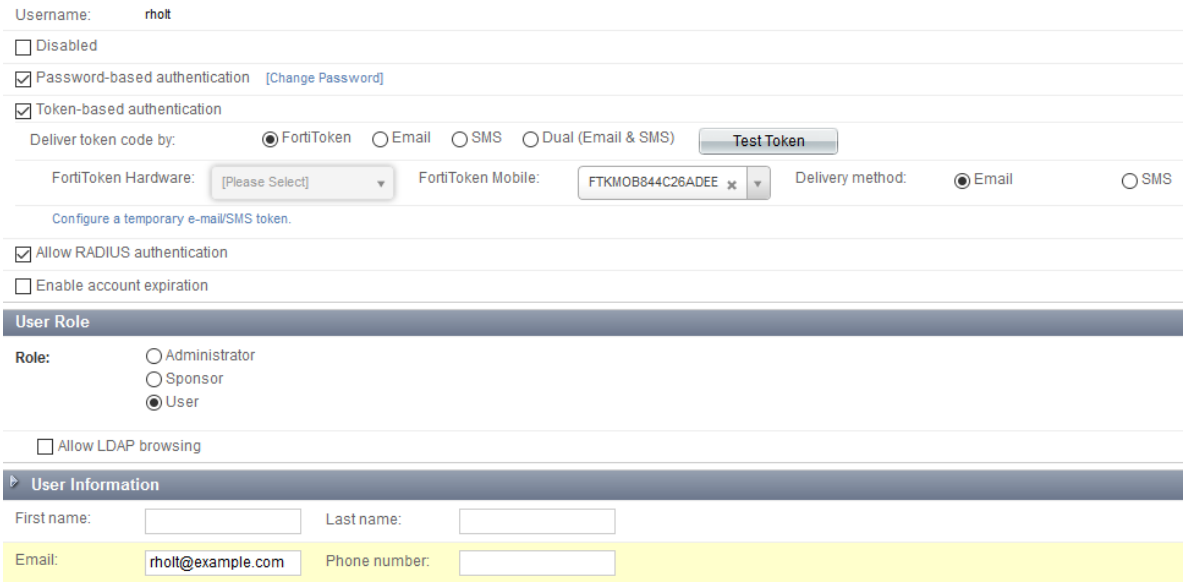
If you do not already have an SSL VPN tunnel configured, see SSL VPN using web and tunnel mode.

Creating a user and a user group

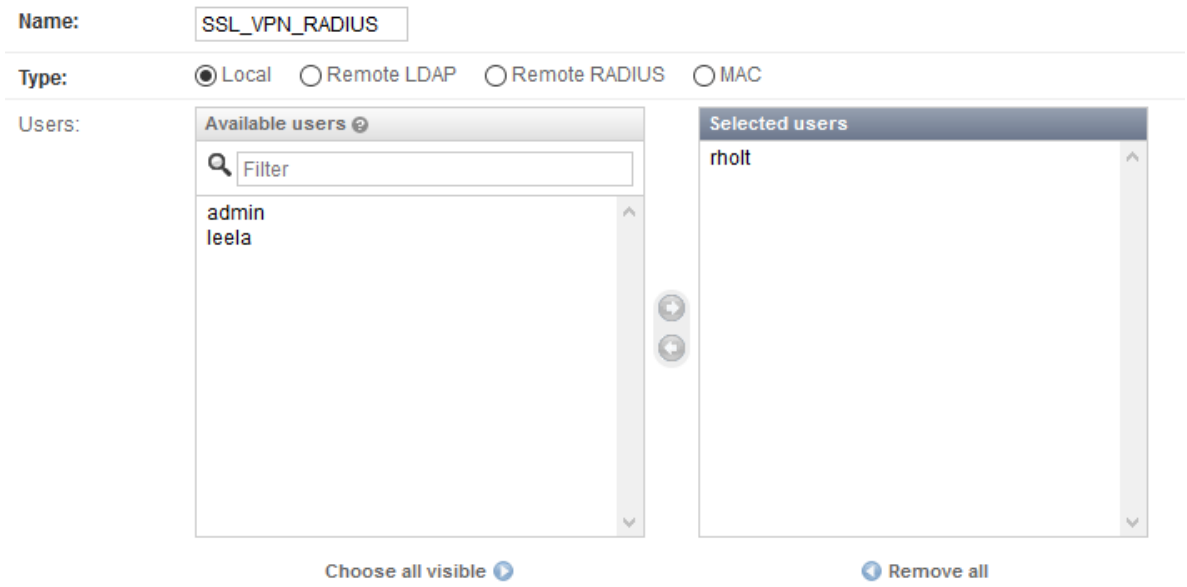
1. On the FortiAuthenticator, go to **Authentication > User Management > Local Users** and select **Create New**.



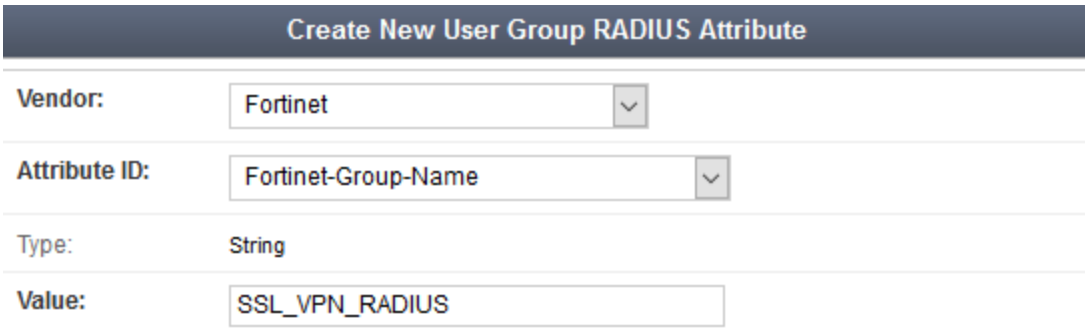
2. Enter a **Username** and set **Password creation** to **Specify a password**. Enter and confirm the password. Enable **Allow RADIUS authentication** and set **Role** to **User**.
3. After you create the user, more options are available. Edit the account and enable **Token-based authentication**.



4. Set **Deliver token code by** to **FortiToken**. Set **FortiToken Mobile** to an available FortiToken. Set **Delievery method** to **Email**.
5. Under **User Information**, set **Email** to the user's email address.
6. To create a user group, go to **Authentication > User Management > User Groups** and select **Create New**. Add the new user to the group.

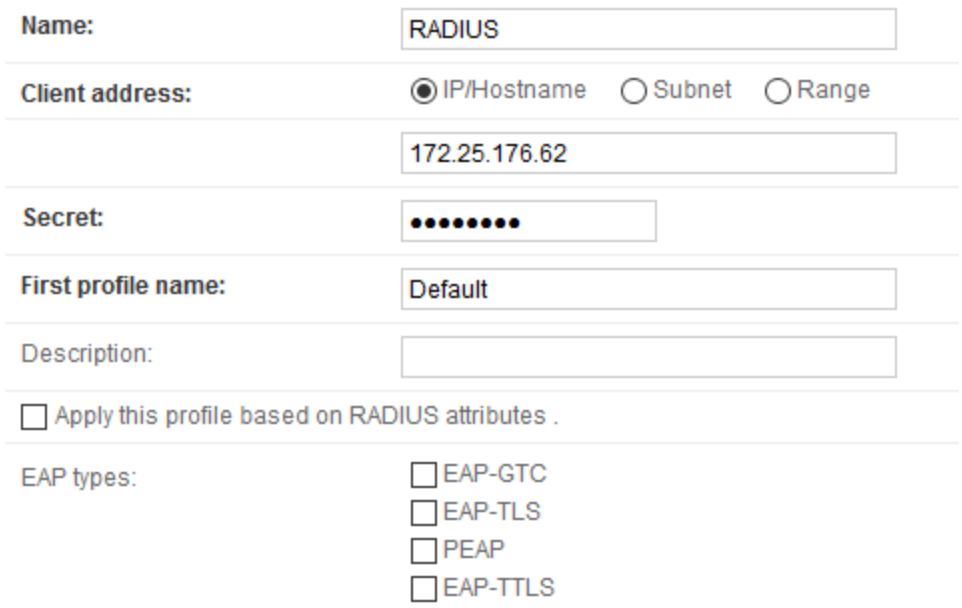


7. After you create the user group, more options are available. Edit the group and create a new RADIUS attribute. Set **Vendor** to **Fortinet**, set **Attribute ID** to **Fortinet-Group-Name**, and set **Value** to the name of the group (in the example, *SSL_VPN_RADIUS*).

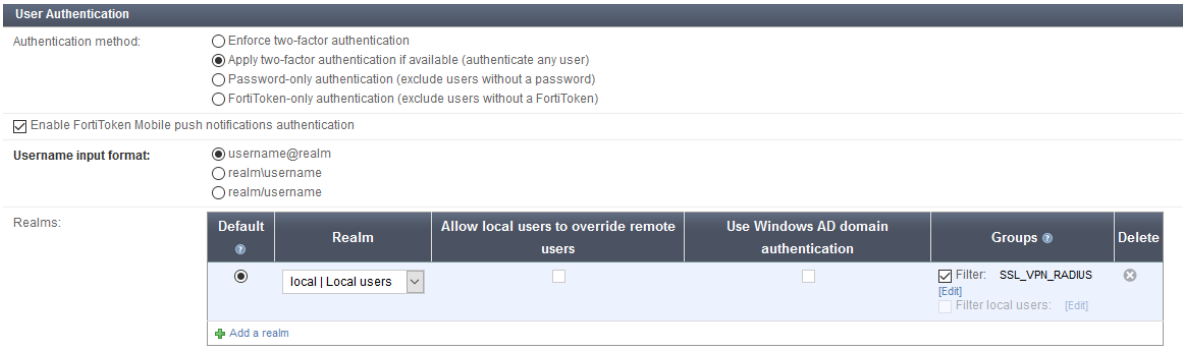


Creating the RADIUS client

1. On the FortiAuthenticator, go to **Authentication > RADIUS Service > Clients** and select **Create New** to create a RADIUS client.
2. Enter a **Name** for the client. Set **Client address** to **IP/Hostname** and enter the IP address of the FortiGate (in the example, *172.25.176.62*). Set a **Secret** for the client.



3. Under **User Authentication**, set **Authentication method** to **Apply two-factor authentication if available**. Select **Enable FortiToken Mobile push notifications authentication**.

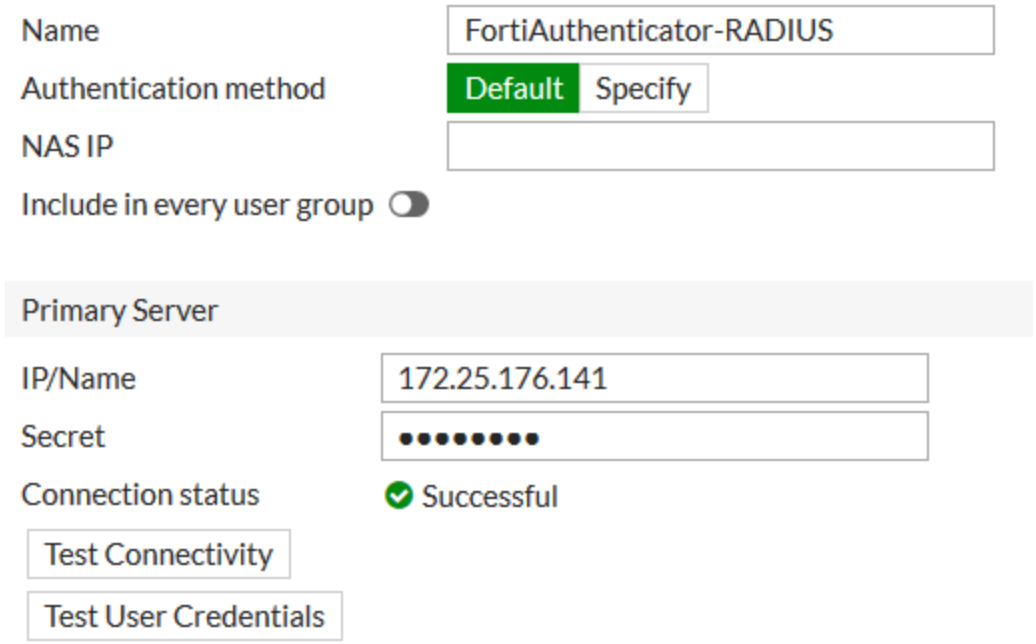


4. For **Realms**, set the default realm to **local | Local users**. Under **Groups**, enable **Filter** and set it to the user group.

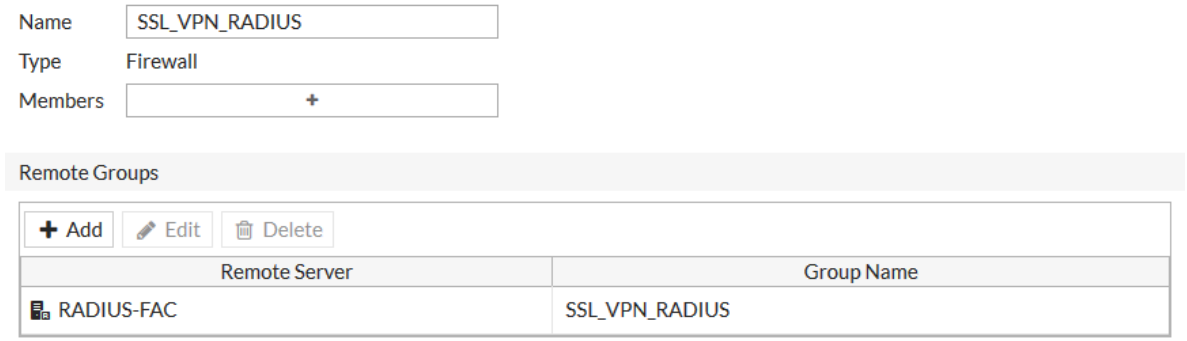
Connecting the FortiGate to FortiAuthenticator

1. To add the FortiAuthenticator as a RADIUS server for FortiGate, on the FortiGate, go to **User & Device > RADIUS Servers** and select **Create New**.

2. Set a **Name** for the server and set **Authentication method** to **Default**.



3. Under **Primary Server,** set **IP/Name** to the IP address of the FortiAuthenticator (in this example, *172.25.176.141*) and set **Secret** to the same secret you configured on the FortiAuthenticator.
4. Select **Test Connectivity** to make sure you used the proper settings.
5. To import the user group, go to **User & Device > User Groups** and create a new group.

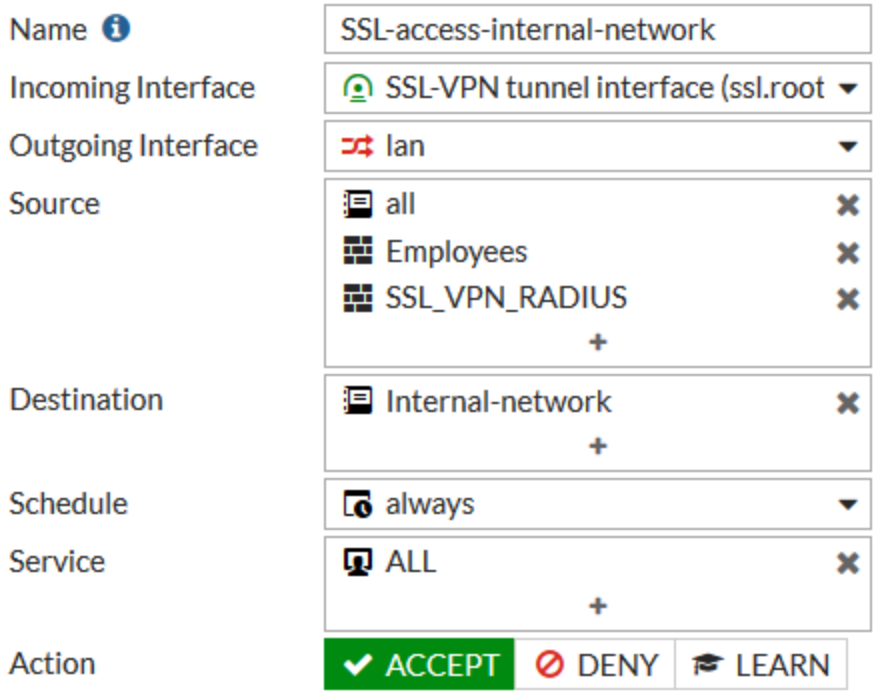


6. Set a **Name** for the group. Under **Remote Groups**, select **+Add** and select the RADIUS server. Set **Groups** to the RADIUS attribute you assigned to the group (in the example, *SSL_VPN_RADIUS*).

Allowing users to connect to the VPN

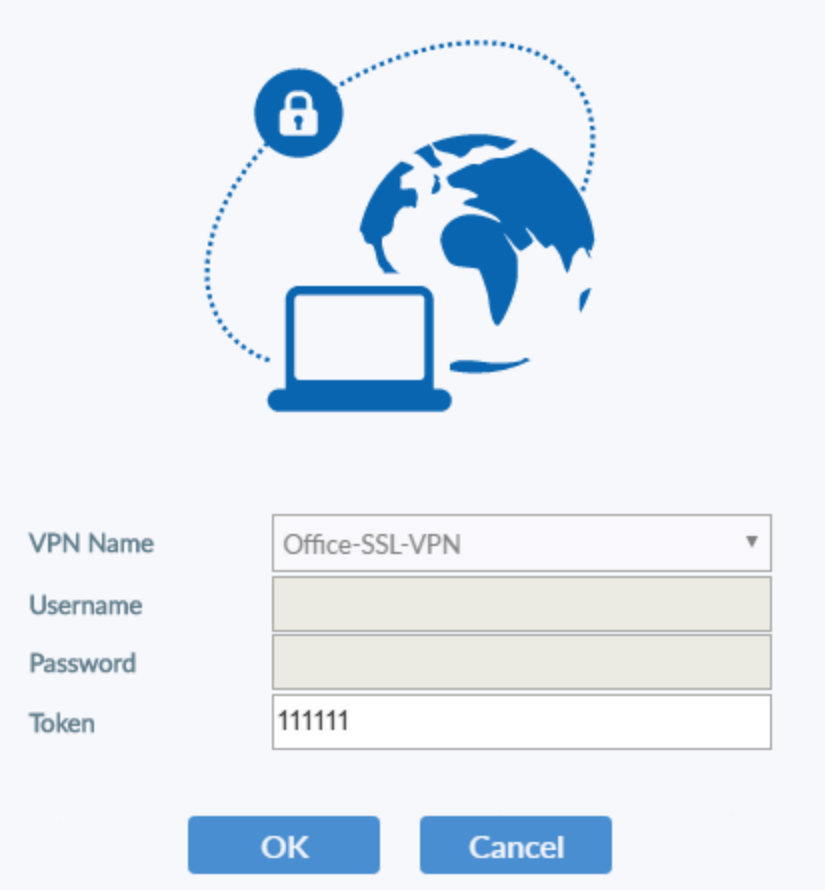
1. On the FortiGate, go to **VPN > SSL-VPN Settings** to configure SSL VPN authentication.

2. Under **Authentication/Portal Mapping**, create a new entry for the RADIUS group. Set **Portal** to **tunnel-access**, which allows users to connect using FortiClient.
3. To allow the new group access to the VPN, go to **Policy & Objects > IPv4 Policy** and edit the policy for the SSL VPN. Select **Source** and set **User** to include the RADIUS group.



Results

1. Log in to the SSL VPN.
2. Enter the FortiToken code when it is requested.



3. You are connected to the VPN tunnel.

Legacy

Please note that the following section contains recipes that were produced with older versions of FortiAuthenticator. These recipes may still prove useful, however they are no longer supported by FortiAuthenticator 5.5 and later.

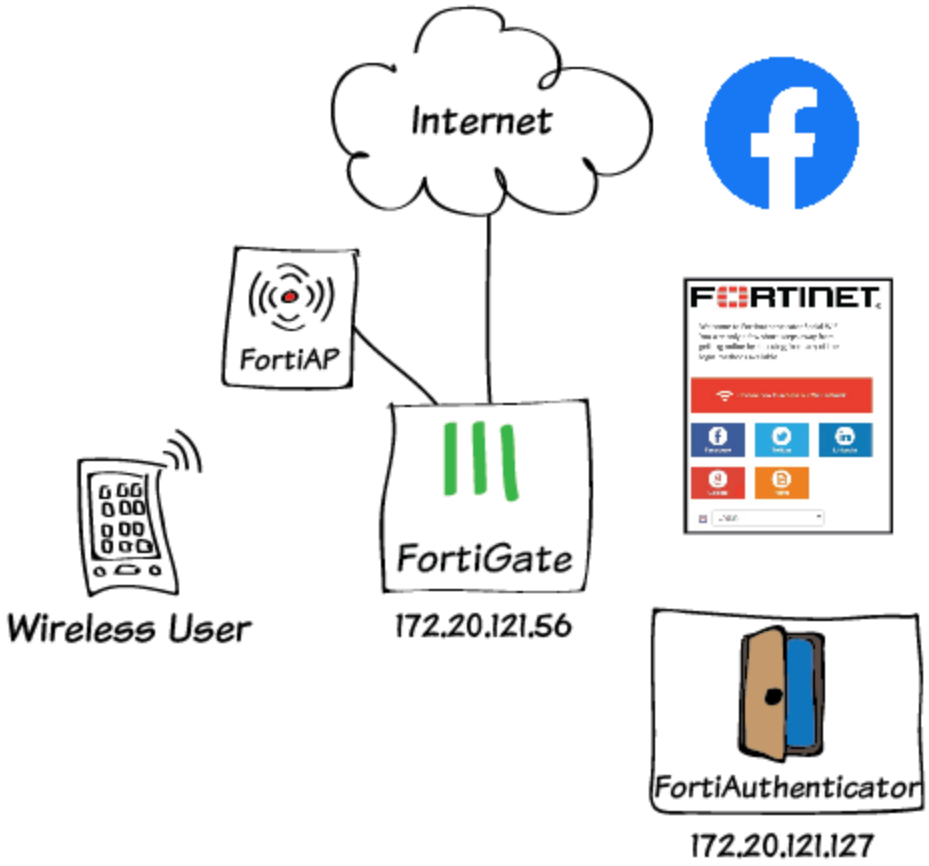
Social WiFi captive portal

Captive portal authentication grants remote users access to certain portions of the network using delegated authentication. Users are required to associate their device with the guest SSID as published by the FortiGate wireless controller.

Social WiFi authentication allows FortiAuthenticator to utilize third-party user identity methods (social sites, valid e-mail address, or phone number) to authenticate users into a wireless guest network. The goal is to provide some traceability of users without requiring the heavy overhead of creating guest accounts.

This section documents the various social WiFi authentication methods, including Facebook, Form-based, Google +, LinkedIn, and Twitter.

Social WiFi captive portal with FortiAuthenticator (Facebook)



This recipe involves configuring an API for Facebook accounts, setting up a social portal RADIUS service on the FortiAuthenticator, and configuring the FortiGate for captive portal access.

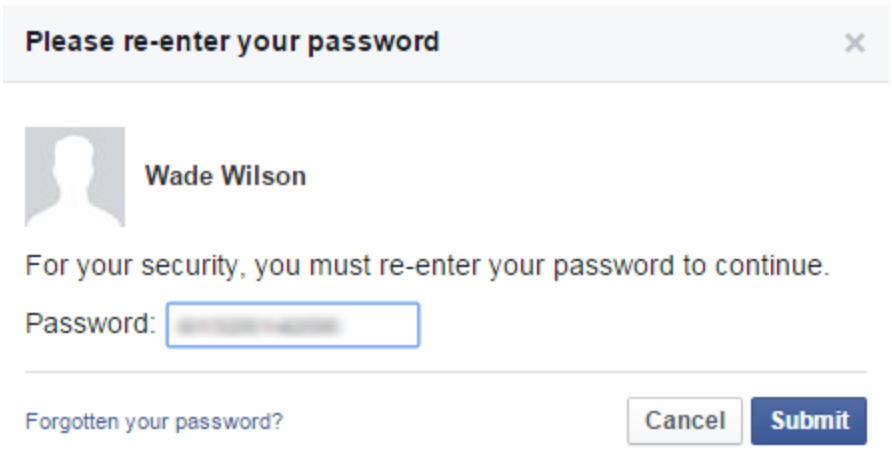
This recipe does not include FortiAP registration instructions.

Note that some CLI usage is required when configuring the FortiGate.

The FortiAuthenticator has been given an example fully qualified domain name (FQDN) - *fortiauthenticator.example.com*.

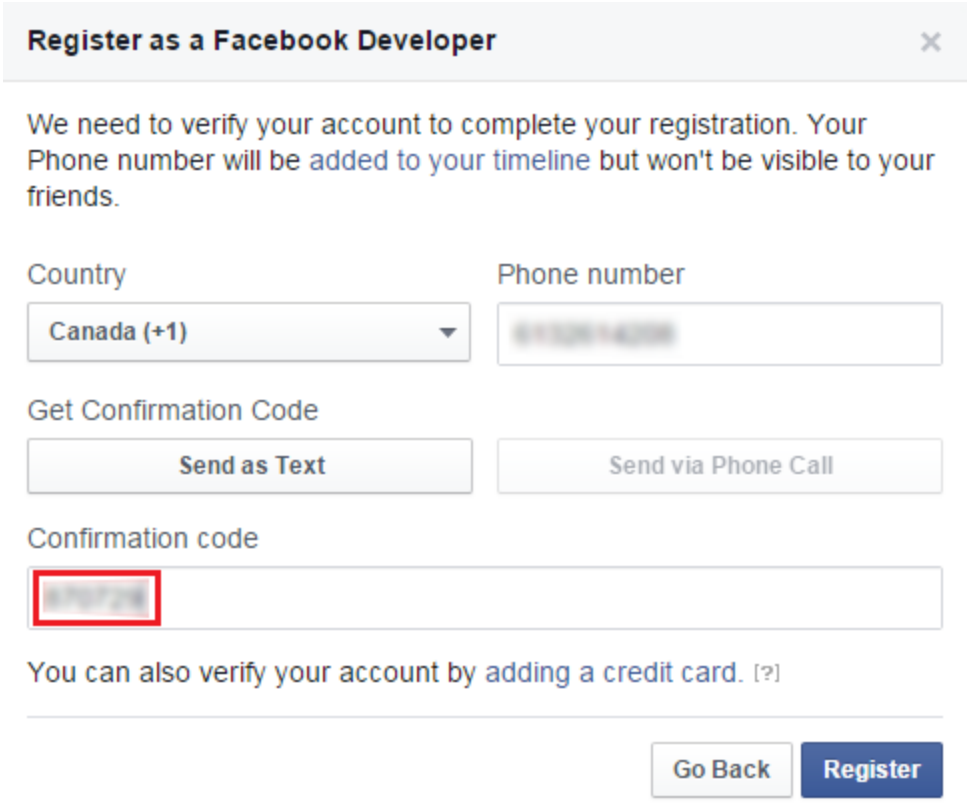
Configuring the Facebook developer account API

1. Open a browser and log in to your Facebook account.
   Browse to the following URL:
   https://developers.facebook.com/products/login/
2. Select **My Apps** and select **Register as Developer**.
3. Confirm your Facebook password to continue.

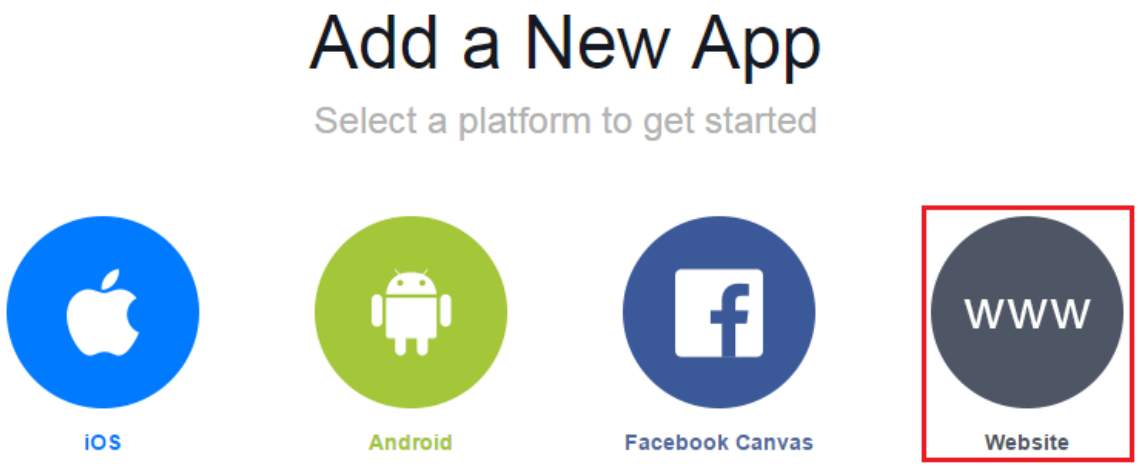


Select that you have read and agree to the Facebook Platform and Facebook Privacy policies, and select **Next** to continue.

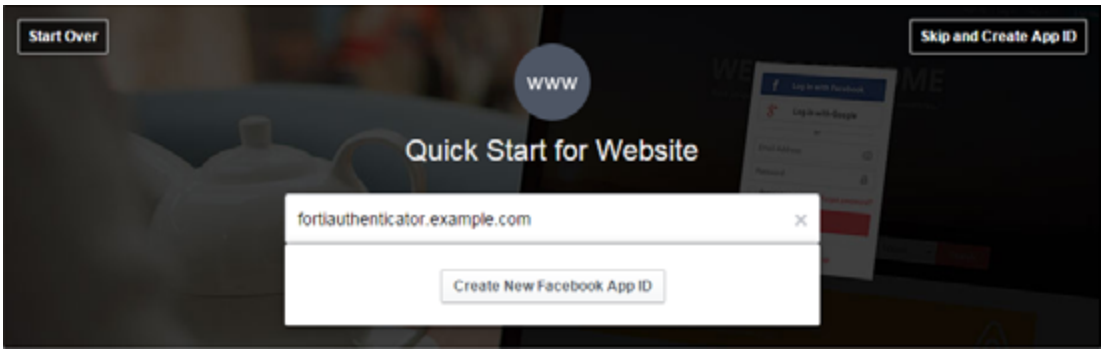
4. Enter your phone number and select to have your confirmation code sent to you via text (you may also choose to verify via phone call).
   Once received, enter the code and select **Register** to continue. You will now be registered as a Facebook developer.



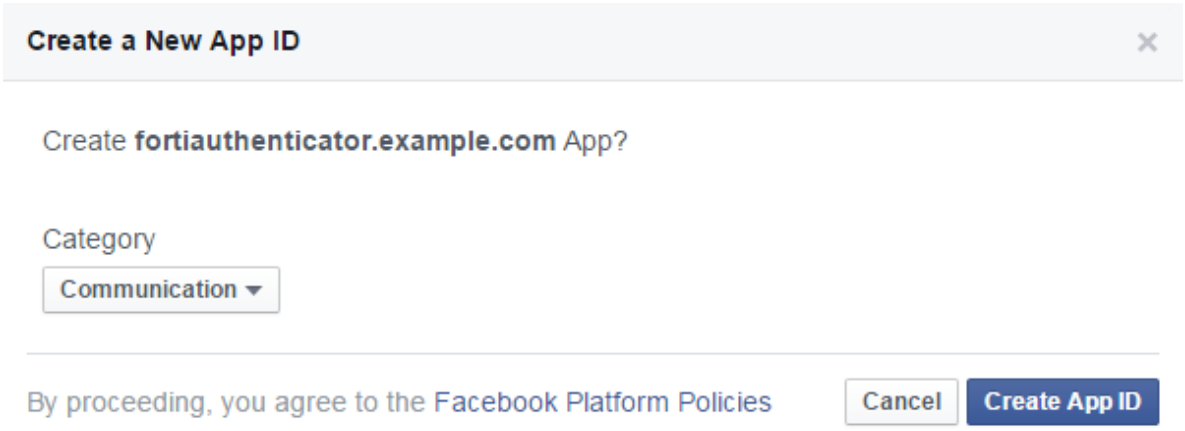
5. Next, select the **Website** platform to add a new application.



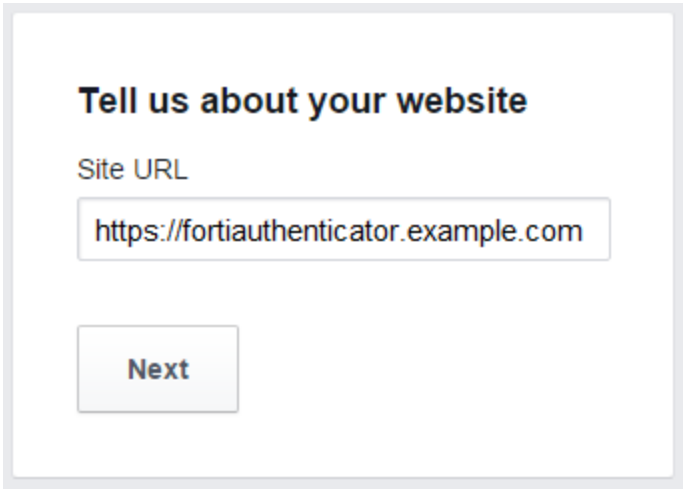
Enter a name for the website and select **Create New Facebook App ID**.



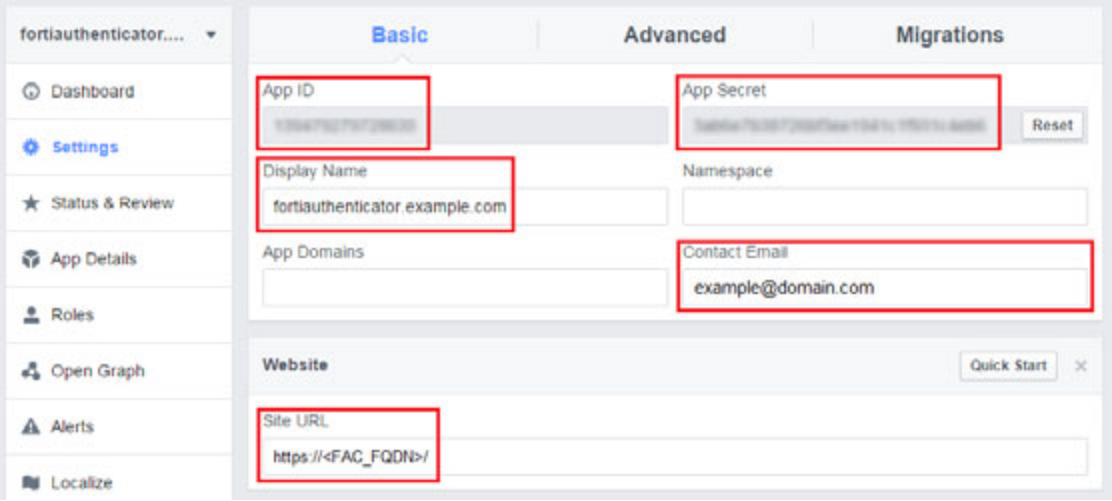
6. Select **Communication** from the drop-down **Category** menu and select **Create App ID**.



Scroll down to the bottom of the page and enter the site's URL, then select **Next**. Scroll back up to the top of the page and select **Skip Quick Start**.

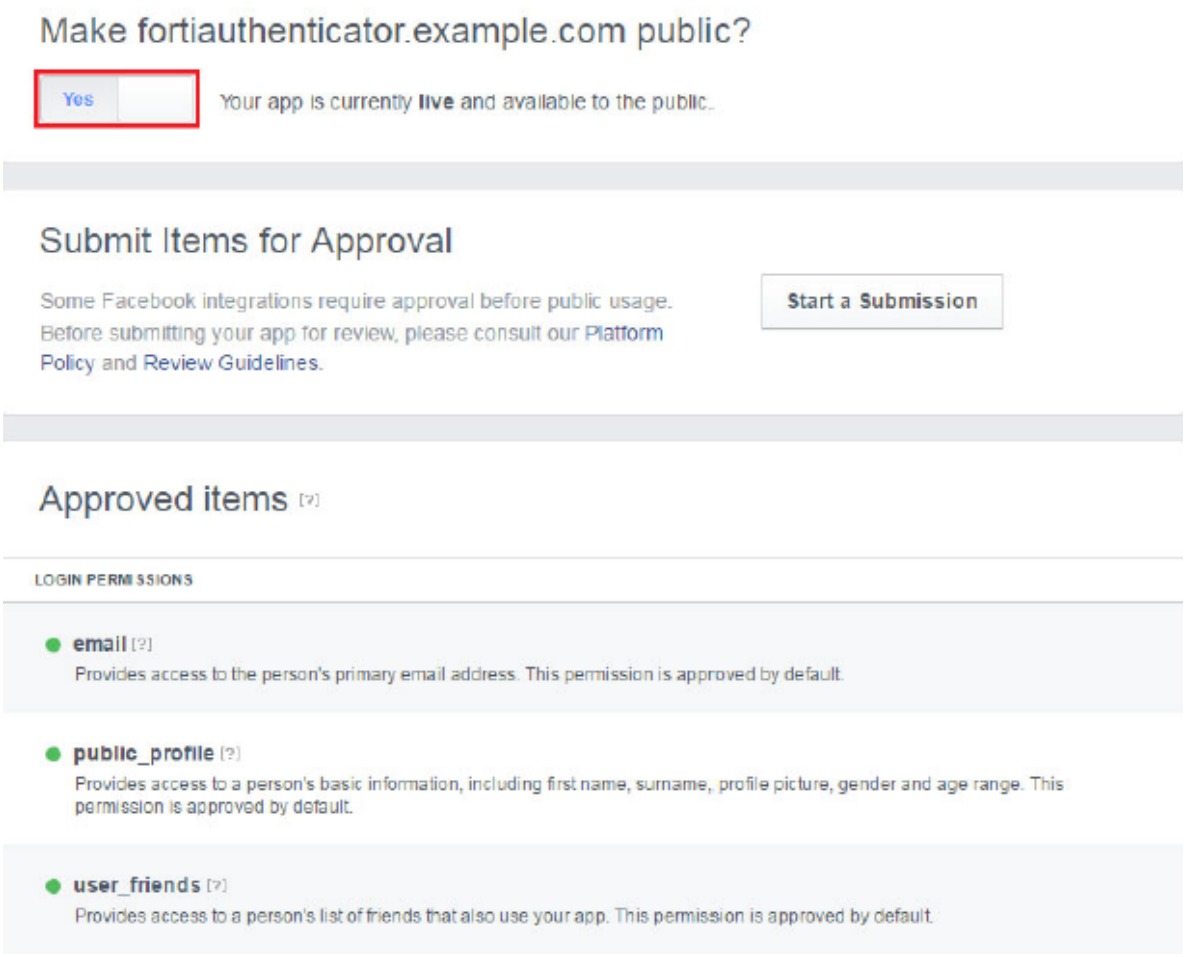


7. To confirm the configuration, go to **Settings > Basic**. From here you can see your **App ID**, **App Secret**, **Display Name**, and **Site URL**.
   Take note of the **App ID** and **App Secret** as they are required when configuring thr captive portal on the FortiAuthenticator.
   Make sure to enter a **Contact Email** as it is required before you can make your application live to the public.



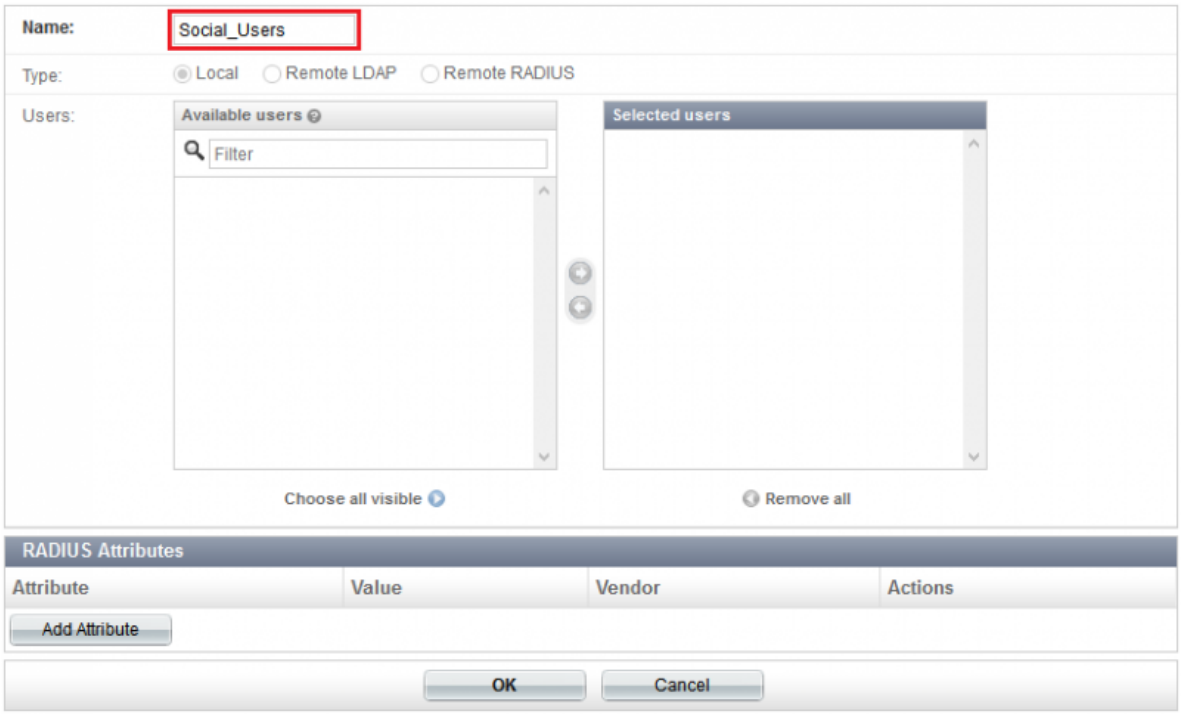
8. Next you must add the FortiAuthenticator as the OAUTH2 client.
   Go to **Settings > Advanced**.
   Under **Security**, enter the **Server IP Whitelist**.
   Note that the server IP whitelist must inclide the public IP addresses of the FortiAuthenticator - this is the NAT IP address of the FortiAuthenticator uses to reach the Internet.

9. Next, go to **App Review** and enable the application - the account needs to be made "live" before WiFi users can successfully authenticate through Facebook.
   The **App ID** and **App Secret** can be accessed at any time on the Facebook developer account, but it may be a good idea to copy them to a secure location.

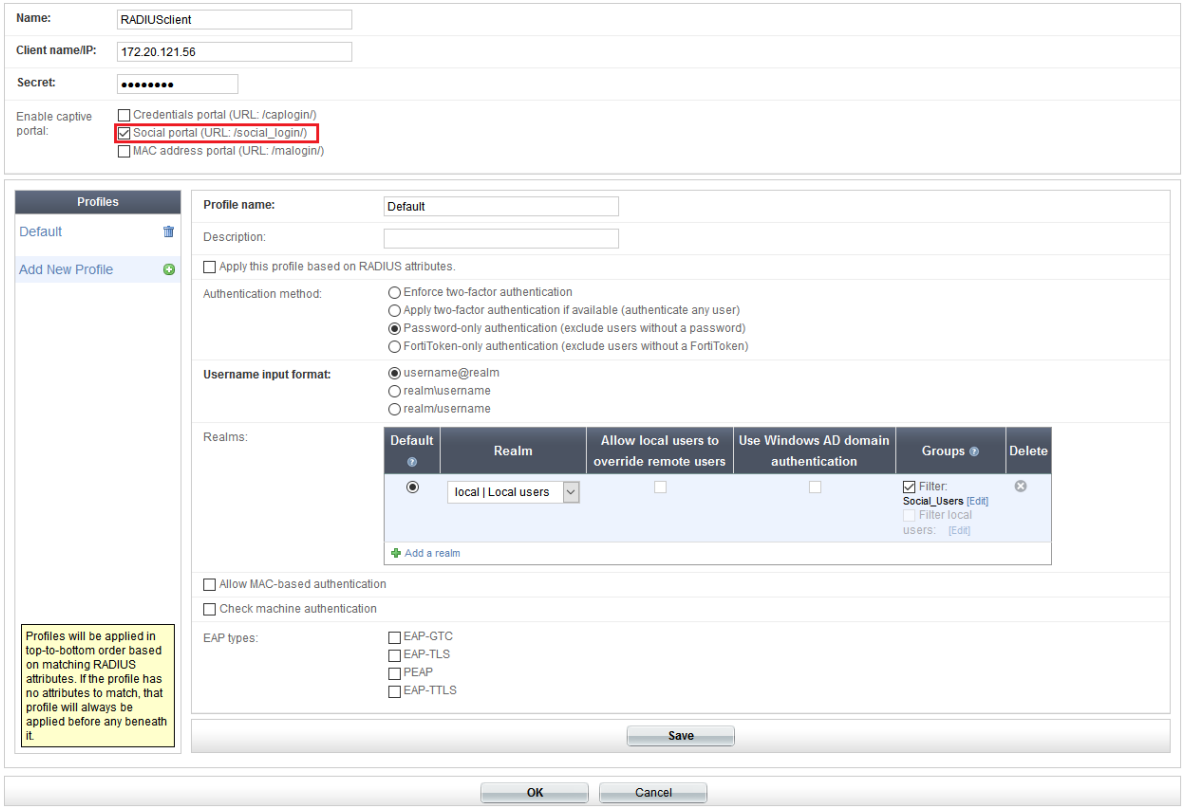


Configuring the social portal RADIUS service on the FortiAuthenticator

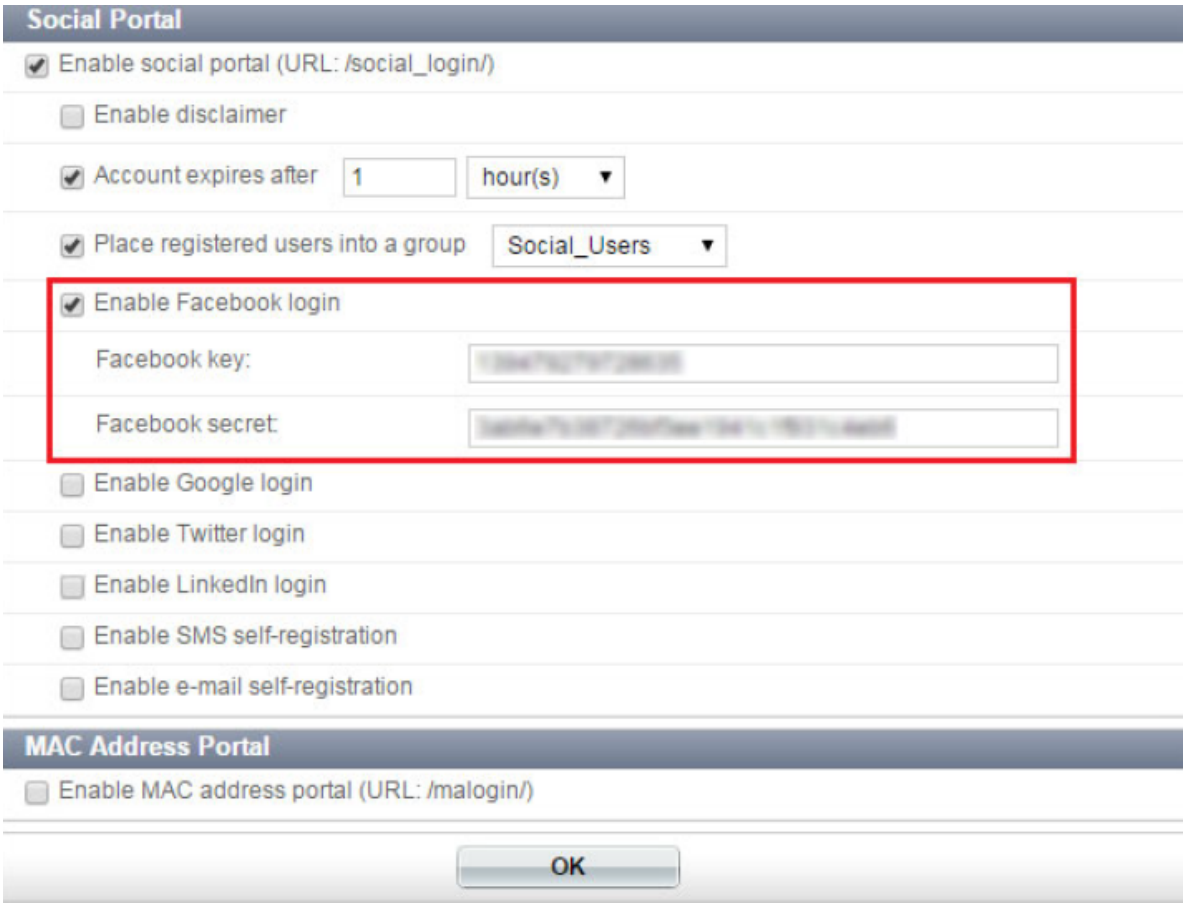
1. Go to **Authentication > User Management > User Groups** and create a **Social_Users** user group. Users that log in through the forms-based authentication method will be placed in this group once it is added to the captive portal general settings.



2. Go to **Authentication > RADIUS Service > Clients** and create a new RADIUS client.
   Enter a **Name** for the RADIUS client (the FortiGate) and enter its IP address (in the example, *172.20.121.56*).
   Enable the **Social portal** captive portal.
   Enter the pre-shared **Secret** and set the **Authentication method**. The FortiGate will use this secret key in its RADIUS configuration.
   Add the **Social_Users** user group to the **Realms** group filter as shown.
   Select **Save** and then **OK**.

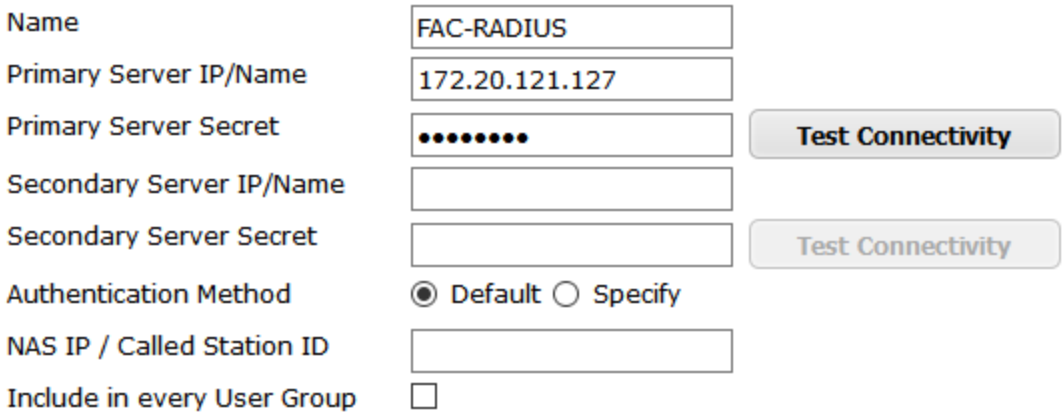


3. Next go to **Authentication > Captive Portal > General** and enable **Social Portal**.
   Configure the account expiry time (in the example, **1 hour**).
   Set **Place registered users into a group** to **Social_Users**.
   Enable the **Facebook** login option and add your **Facebook key** and **Facebook secret**.



Configuring the FortiGate authentication settings

1. On the FortiGate, go to **User & Device > RADIUS Servers** and create the connection to the FortiAuthenticator RADIUS server, using its IP and pre-shared secret.
   Use the **Test Connectivity** option with valid credentials to test the connection.

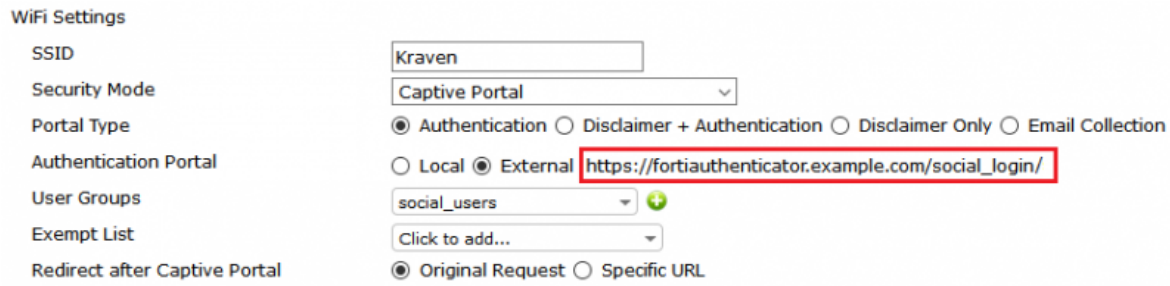


2. Next go to **User & Device > User Groups** and create a RADIUS user group.

Set **Type** to **Firewall** and add the RADIUS server to the **Remote groups** table.

Configuring the FortiGate WiFi settings

1. Go to **WiFi & Switch Controller > SSID** and select the SSID interface.
   Under **WiFi Settings**, set the **Security Mode** to **Captive Portal**.



2. For the **Authentication Portal**, select **External**, and enter the FQDN of the FortiAuthenticator, followed by **/social_login/**.
   For this recipe, it is set to `https://fortiauthenticator.example.com/social_login/`
   Set **User Groups** to the **social_users** group.

Configuring the FortiGate to allow access to Facebook

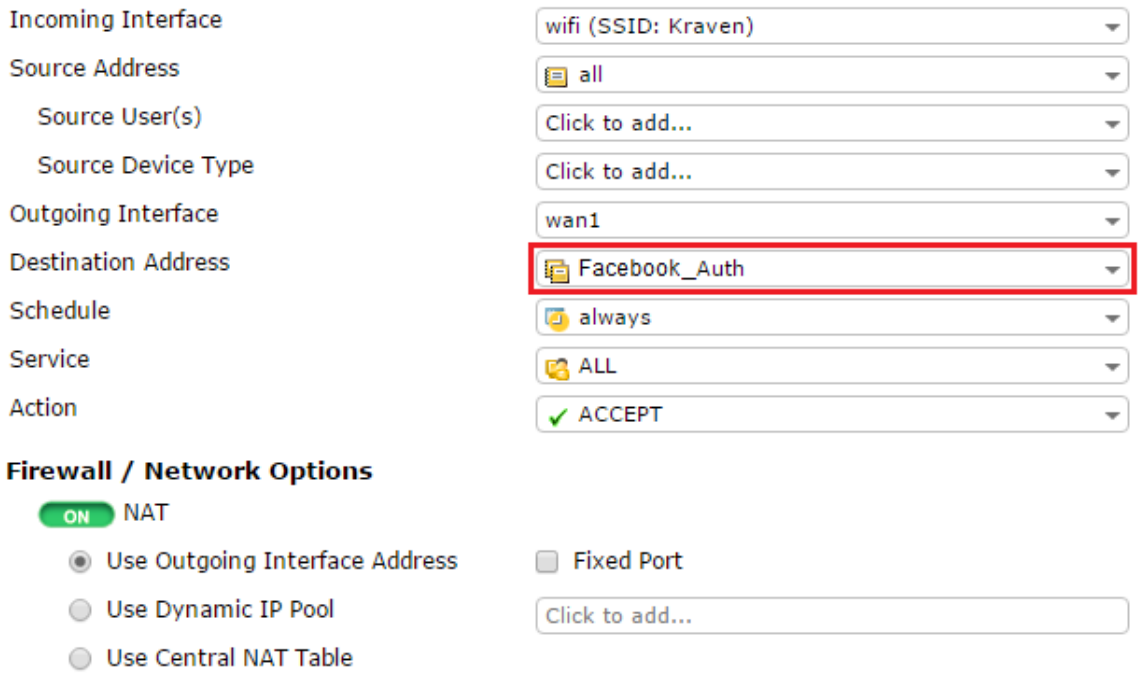
1. On the FortiGate, configure firewall addresses to allow users to access the Facebook login page.
   The following step can be performed in the GUI, but may take considerably longer than using the CLI. You can copy and paste the commands below.
   Open the **CLI Console** and enter the following, which creates the firewall addresses and adds them to a firewall address group called **Facebook_Auth**.

```
config firewall address
   edit "FB0"
      set subnet 5.178.32.0 255.255.240.0
   next
   edit "FB1"
      set subnet 195.27.154.0 255.255.255.0
   next
   edit "FB2"
      set subnet 80.150.154.0 255.255.255.0
   next
   edit "FB3"
      set subnet 77.67.96.0 255.255.252.0
   next
   edit "FB4"
      set subnet 212.119.27.0 255.255.255.128
```

```
next
edit "FB5"
   set subnet 2.16.0.0 255.248.0.0
next
edit "FB6"
   set subnet 66.171.231.0 255.255.255.0
next
edit "FB7"
   set subnet 31.13.24.0 255.255.248.0
next
edit "FB8"
   set subnet 31.13.64.0 255.255.192.0
next
edit "FB9"
   set subnet 23.67.246.0 255.255.255.0
next
edit "akamai-subnet-23.74.8"
   set subnet 23.74.8.0 255.255.255.0
next
edit "akamai-subnet-23.74.9"
   set subnet 23.74.9.0 255.255.255.0
next
edit "external.fcgrl-1.fna.fbcdn.net"
   set type fqdn
   set fqdn "external.fcgrl-1.fna.fbcdn.net"
next
edit "scontent.xx.fbcdn.net"
   set type fqdn
   set fqdn "scontent.xx.fbcdn.net
next
edit "akamaihd.net"
   set type fqdn
   set fqdn "akamaihd.net
next
edit "channel-proxy-06-frcl.facebook.com"
   set type fqdn
   set fqdn channel-proxy-06-frcl.facebook.com
next
edit "code.jquery.com"
   set type fqdn
   set fqdn "code.jquery.com"
next
edit "connect.facebook.com"
   set type fqdn
   set fqdn "connect.facebook.com"
next
edit "fbcdn-photos-c-a.akamaihd.net"
   set type fqdn
   set fqdn "fbcdn-photos-c-a.akamaihd.net"
next
edit "fbcdn-profile-a.akamaihd.net"
   set type fqdn
   set fqdn "fbcdn-profile-a.akamaihd.net"
next
edit "fbexternal-a.akamaihd.net"
   set type fqdn
   set fqdn "fbexternal-a.akamaihd.net"
```

```
    next
    edit "fbstatic-a.akamaihd.net"
      set type fqdn
      set fqdn "fbstatic-a.akamaihd.net"
    next
    edit "m.facebook.com"
      set type fqdn
      set fqdn "m.facebook.com"
    next
    edit "ogp.me"
      set type fqdn
      set fqdn "ogp.me"
    next
    edit "s-static.ak.facebook.com"
      set type fqdn
      set fqdn "s-static.ak.facebook.com"
    next
    edit "static.ak.facebook.com"
      set type fqdn
      set fqdn "static.ak.facebook.com"
    next
    edit "static.ak.fbcdn.com"
      set type fqdn
      set fqdn "static.ak.fbcdn.com"
    next
    edit "web_ext_addr_SocialWiFi"
      set type fqdn
      set fqdn "web_ext_addr_SocialWiFi"
    next
    edit "www.facebook.com"
      set type fqdn
      set fqdn "www.facebook.com"
    next
  end
  config firewall addgrp
    edit "Facebook_Auth"
      set member set member "FB0" "FBl" "FB2" "FB3" "FB4" "FBS" "FB6" "FB7" "FB8"
           "FB9" "akamaisubnet-23.74.8" "akamai-subnet-23.74.9" "external.fcgrl-
           1.fna.fbcdn.net" "scontent.xx.fbcdn.net" "akamaihd.net" "channel-proxy-
           06-rcl.facebook.com" "code.jquery.com" "connect.facebook.com" "fbcdn-
           photos-a-akaihd.net" "fbcdn-profile-a.akamaihd.net" "fbexternal-
           a.akamaihd.net" "fbstatic-a.akamaihd.net" "m.facebook.com" "ogp.me" "s-
           static.ak.facebook.com" "static.ak.facebook.com" "static.ak.fbcdn.com"
           "web_ext_addr_SocialWiFi" "www.facebook.com" "FortiAuthenticator"
    next
  end
```

2. Then go to **Policy & Objects > IPv4 Policy** and create a policy for Facebook authentication traffic.
   Set **Incoming Interface** to the WiFi SSID interface and set **Source Address** to **all**.
   Set **Outgoing Interface** to the Internet-facing interface and set **Destination Address** to **Facebook_Auth**.
   Set **Service** to **ALL** and enable **NAT**. Configure **Security Profiles** accordingly.
   Once created, note the policy's ID using the **ID** column.



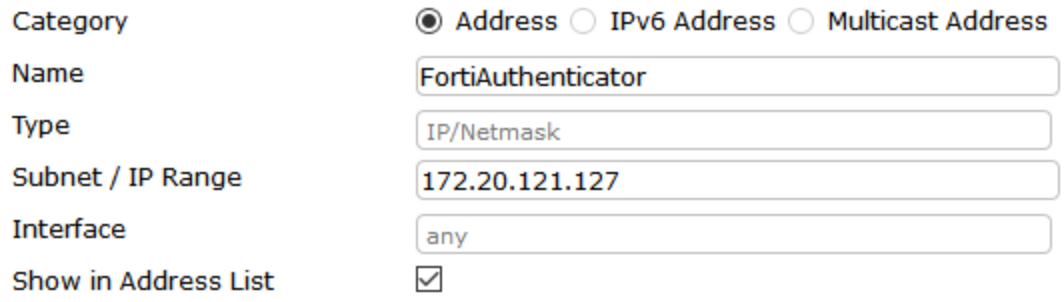
3. Then open the **CLI Console**. Using the policy's ID, enter the following command to exempt the Facebook authentication traffic policy from the captive portal:

```
config firewall policy
   edit <policy_id>
      set captive-portal-exempt enable
   next
end
```

This command allows access to the external captive portal.

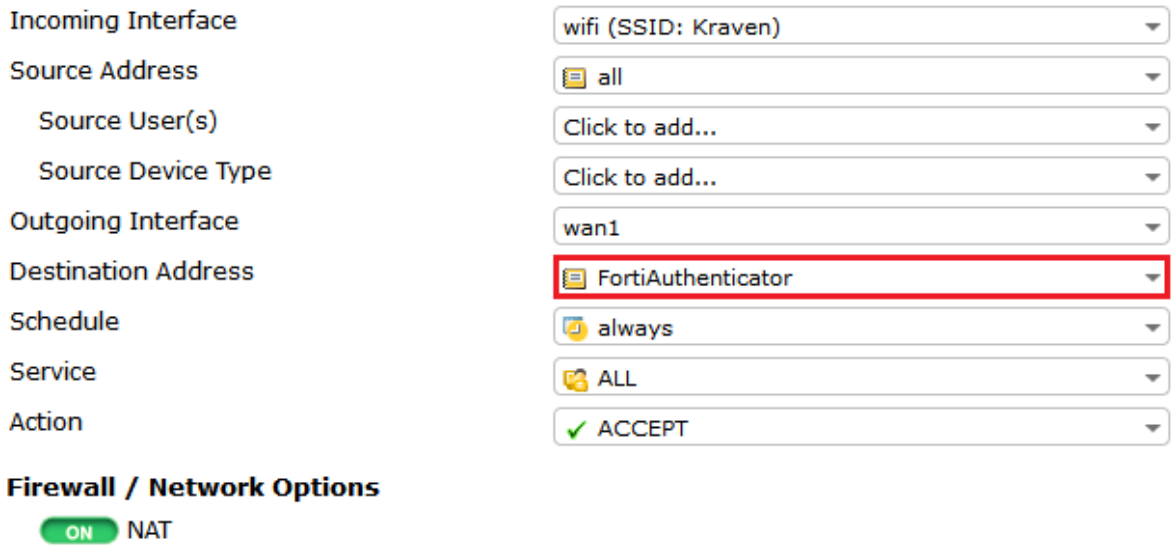
Configuring the FortiGate to allow access to the FortiAuthenticator

1. On the FortiGate, go to **Policy & Objects > Addresses** and add the FortiAuthenticator firewall object. For **Subnet/IP Range** enter the IP address of the FortiAuthenticator.



2. Go to **Policy & Objects > IPv4 Policy** and create the FortiAuthenticator access policy.
   Set **Incoming Interface** to the WiFi SSID interface and set **Source Address** to **all**.
   Set **Outgoing Interface** to the Internet-facing interface and set **Destination Address** to the **FortiAuthenticator** address object.
   Set **Service** to **ALL** and enable **NAT**.

Once created, note the policy's ID using the **ID** column.



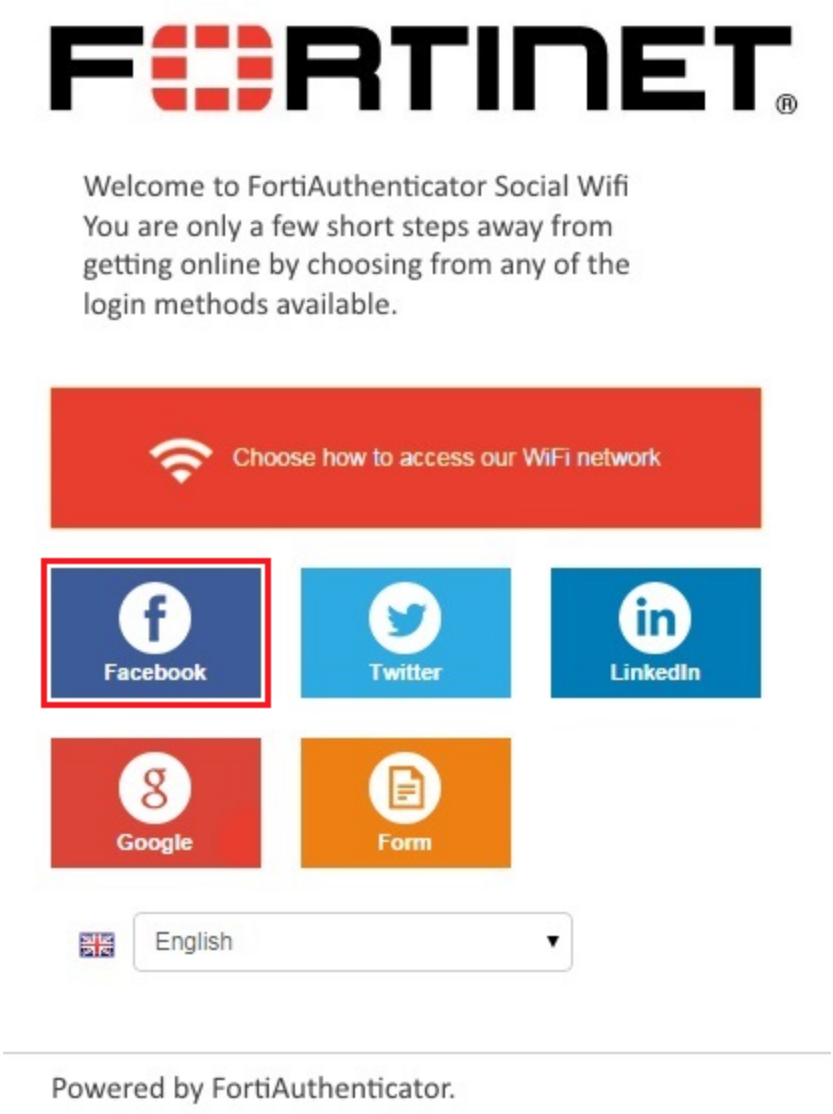
3. Open the **CLI Console** and enter the following command to exempt the FortiAuthenticator access policy from the captive portal:

```
config firewall policy
   edit <policy_id>
      set captive-portal-exempt enable
   next
end
```

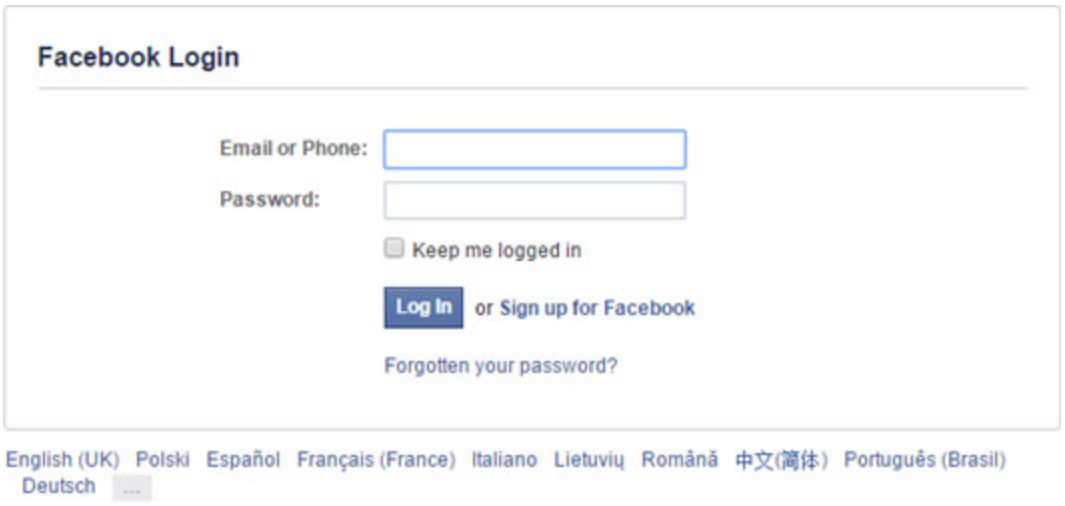
This command allows access to the external captive portal.

Results

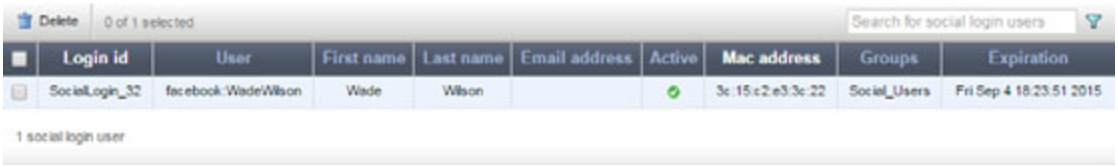
1. Connect to the WiFi and attempt to browse the Internet. You will be redirected to the captive portal splash page.
   Select **Facebook** and you should be redirected to the Facebook login page.



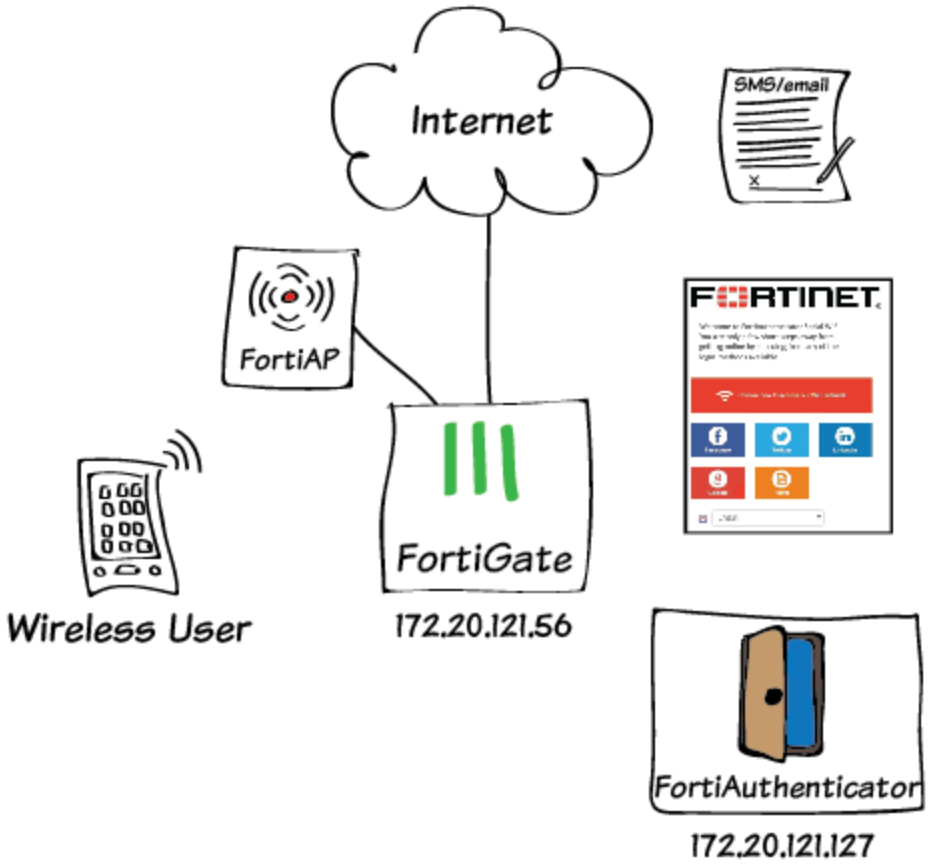
2. Enter valid Facebook credentials and you will be redirected to the URL initially requested.
You can now browse freely until the social login account expires, as configured on the FortiAuthenticator under **Authentication > Captive Portal > General**.



3. To view the authenticated user added on FortiAuthenticator, go to **Authentication > User Management > Social Login Users**.



Social WiFi captive portal with FortiAuthenticator (Form-based)

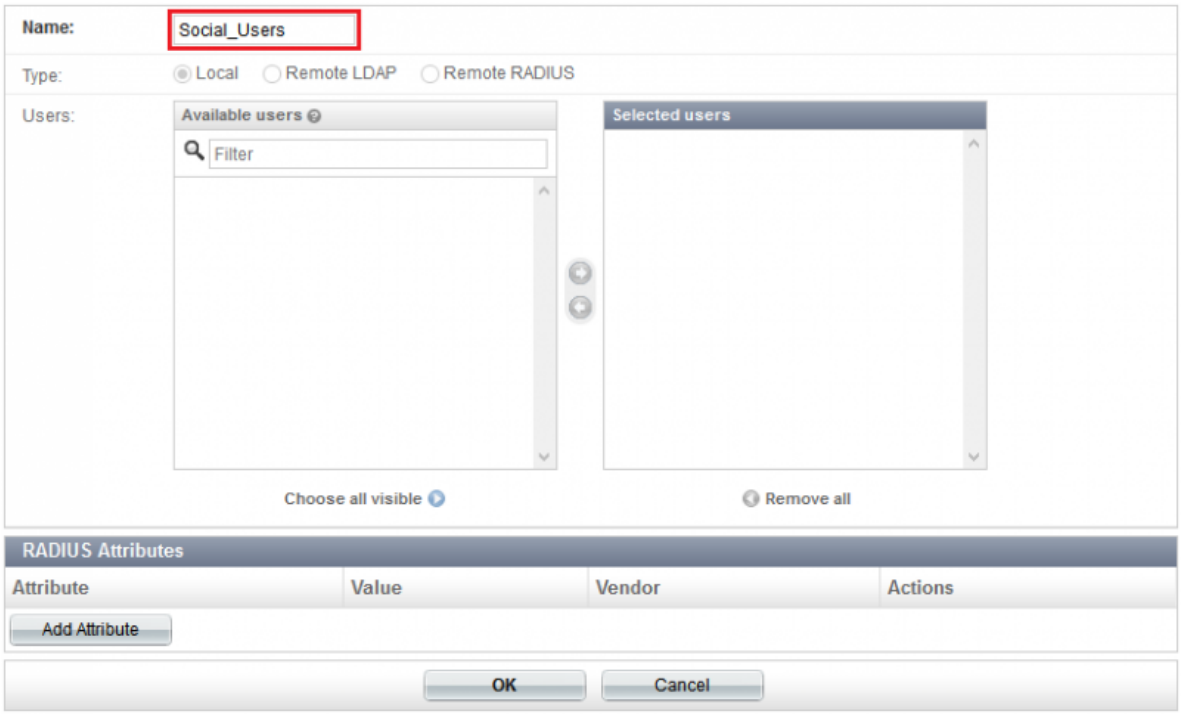


This recipe involves setting up a social portal RADIUS service on the FortiAuthenticator, and configuring the FortiGate for captive portal access, allowing users to log in to the WiFi network using either SMS or email self-registration.

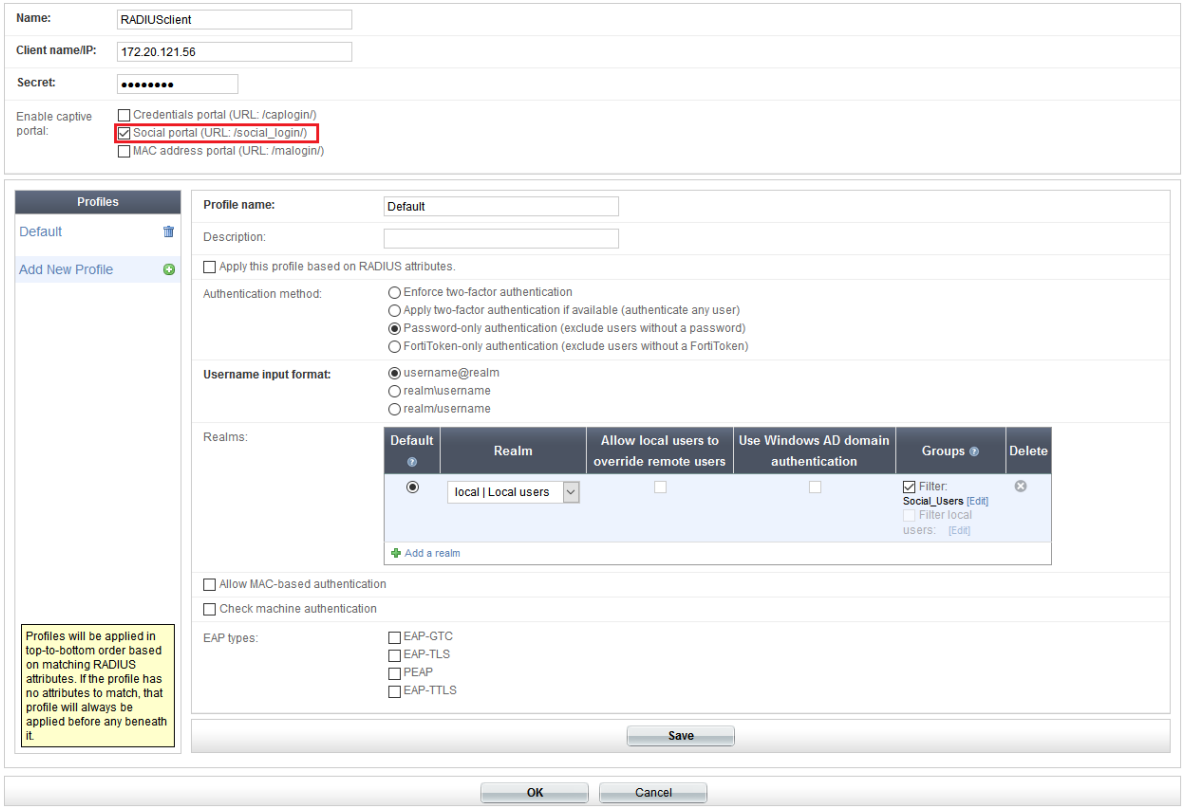
This recipe does not include FortiAP registration instructions.

Configuring the social portal RADIUS service on the FortiAuthenticator

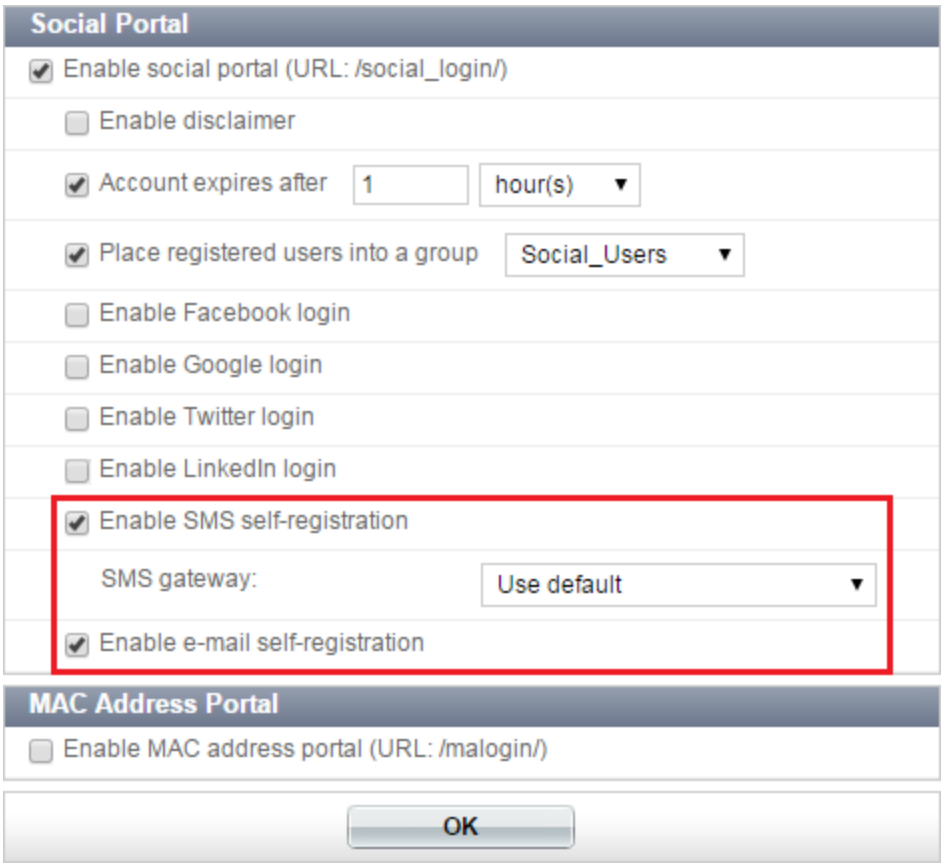
1. Go to **Authentication > User Management > User Groups** and create a **Social_Users** user group. Users that log in through the forms-based authentication method will be placed in this group once it is added to the captive portal general settings.



2. Go to **Authentication > RADIUS Service > Clients** and create a new RADIUS client.
   Enter a **Name** for the RADIUS client (the FortiGate) and enter its IP address (in the example, *172.20.121.56*).
   Enable the **Social portal** captive portal.
   Enter the pre-shared **Secret** and set the **Authentication method**. The FortiGate will use this secret key in its RADIUS configuration.
   Add the **Social_Users** user group to the **Realms** group filter as shown.
   Select **Save** and then **OK**.

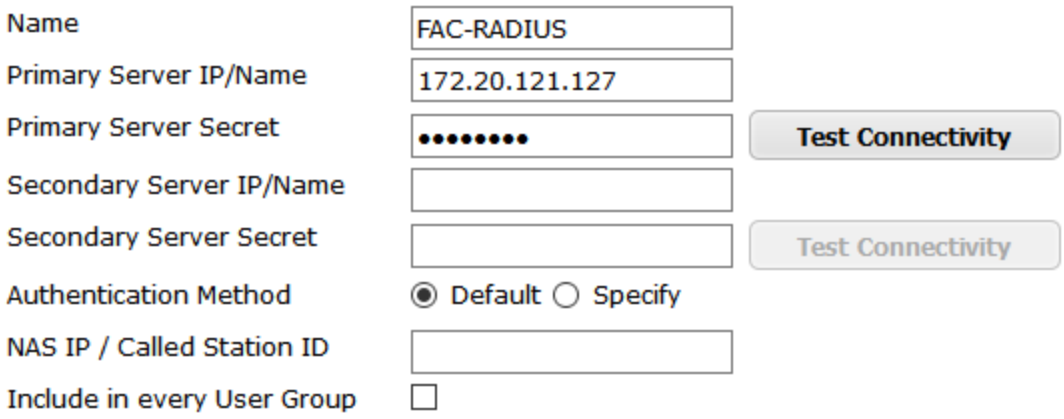


3. Next go to **Authentication > Captive Portal > General** and enable **Social Portal**.
   Configure the account expiry time (in the example, **1 hour**).
   Set **Place registered users into a group** to **Social_Users**.
   Enable the **SMS self-registration** and **e-mail self-registration** login options. Be sure SMS gateway is set to **Use default**.



Configuring the FortiGate authentication settings

1. On the FortiGate, go to **User & Device > RADIUS Servers** and create the connection to the FortiAuthenticator RADIUS server, using its IP and pre-shared secret.
   Use the **Test Connectivity** option with valid credentials to test the connection.

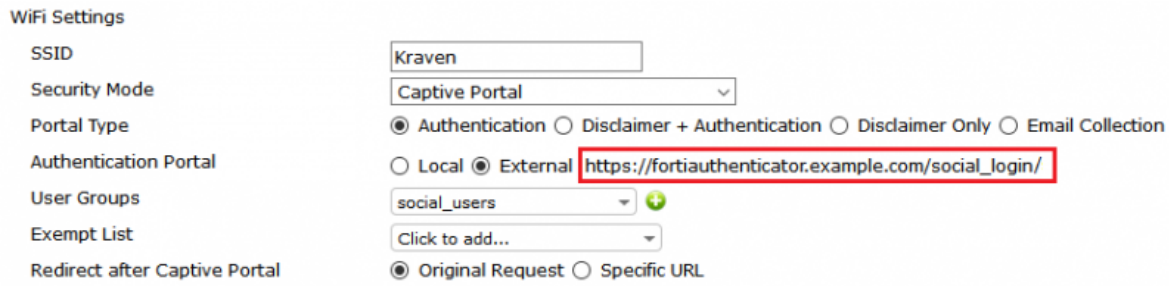


2. Next go to **User & Device > User Groups** and create a RADIUS user group.

Set **Type** to **Firewall** and add the RADIUS server to the **Remote groups** table.

Configuring the FortiGate WiFi settings

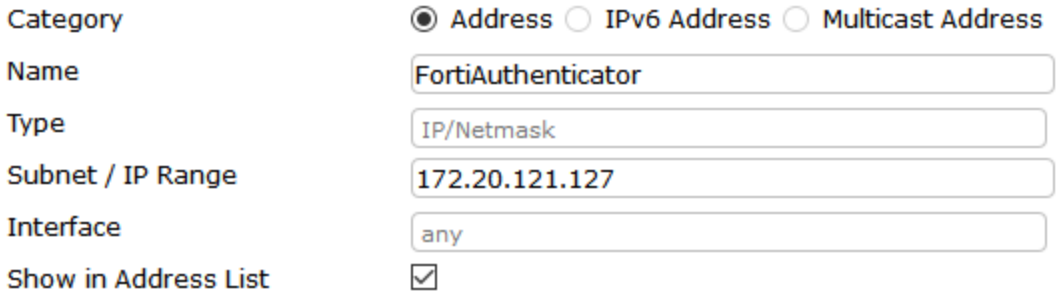
1. Go to **WiFi & Switch Controller > SSID** and select the SSID interface.
   Under **WiFi Settings**, set the **Security Mode** to **Captive Portal**.



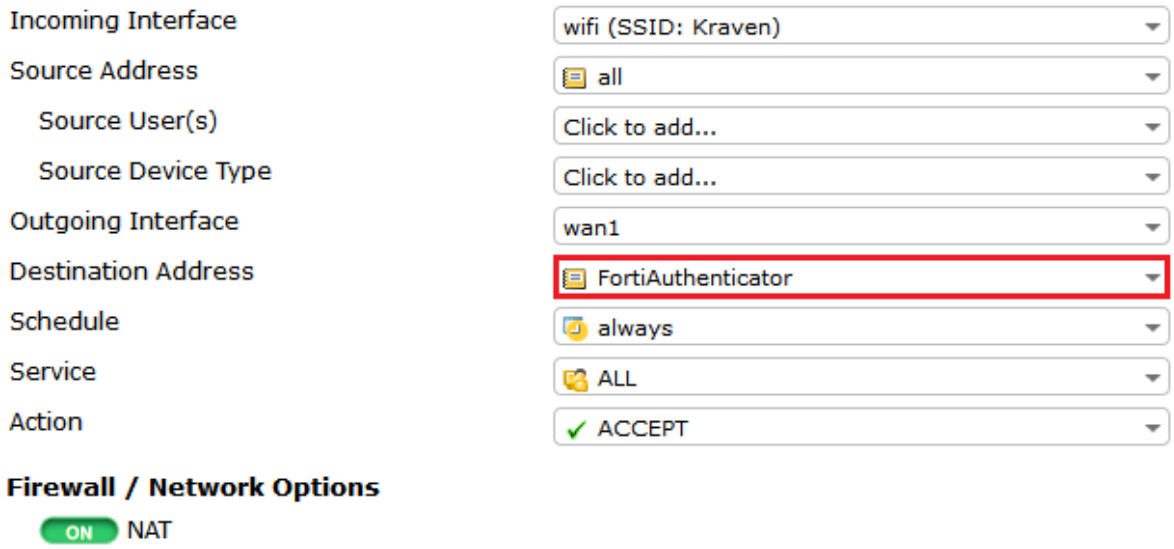
2. For the **Authentication Portal**, select **External**, and enter the FQDN of the FortiAuthenticator, followed by **/social_login/**.
   For this recipe, it is set to `https://fortiauthenticator.example.com/social_login/`
   Set **User Groups** to the **social_users** group.

Configuring the FortiGate to allow access to the FortiAuthenticator

1. On the FortiGate, go to **Policy & Objects > Addresses** and add the FortiAuthenticator firewall object.
   For **Subnet/IP Range** enter the IP address of the FortiAuthenticator.



2. Go to **Policy & Objects > IPv4 Policy** and create the FortiAuthenticator access policy.
   Set **Incoming Interface** to the WiFi SSID interface and set **Source Address** to **all**.
   Set **Outgoing Interface** to the Internet-facing interface and set **Destination Address** to the **FortiAuthenticator** address object.
   Set **Service** to **ALL** and enable **NAT**.
   Once created, note the policy's ID using the **ID** column.



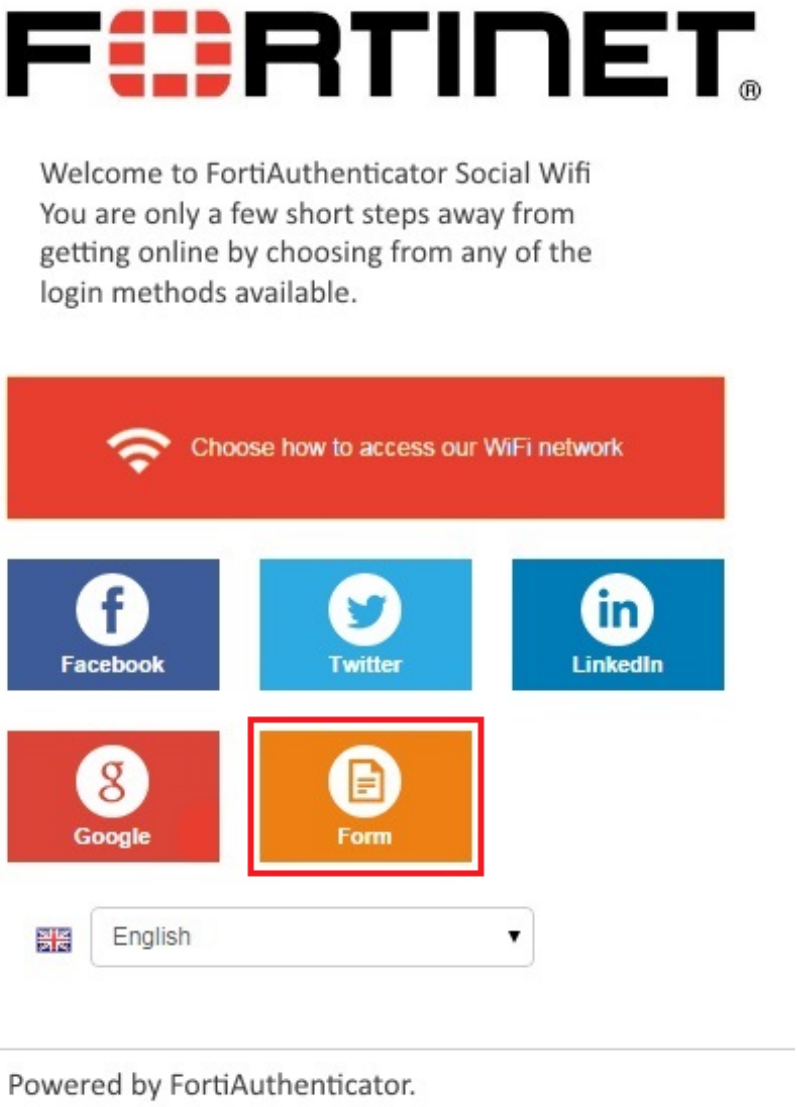
3. Open the **CLI Console** and enter the following command to exempt the FortiAuthenticator access policy from the captive portal:

```
config firewall policy
   edit <policy_id>
      set captive-portal-exempt enable
   next
end
```

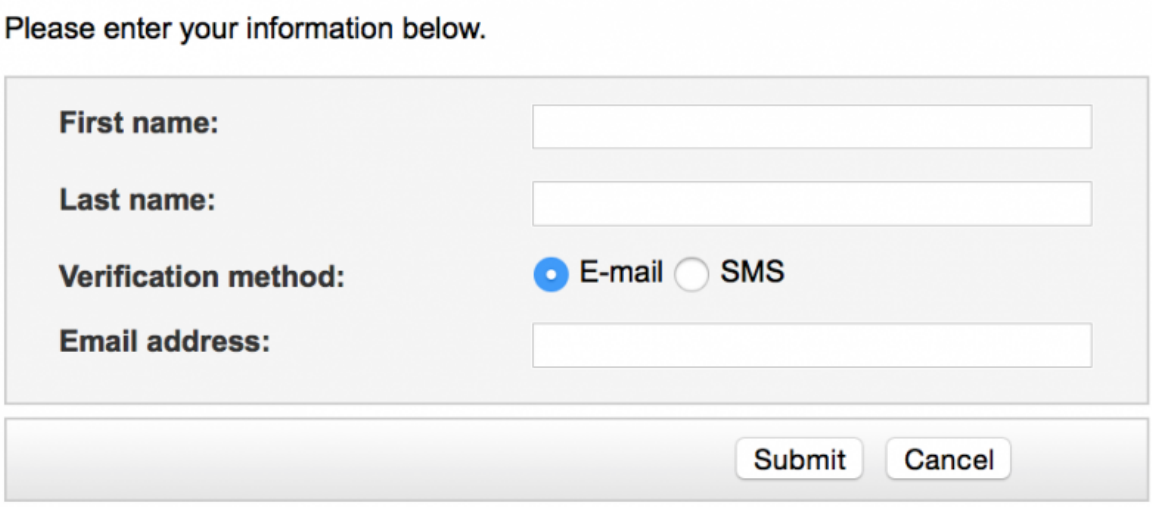
This command allows access to the external captive portal.

Results

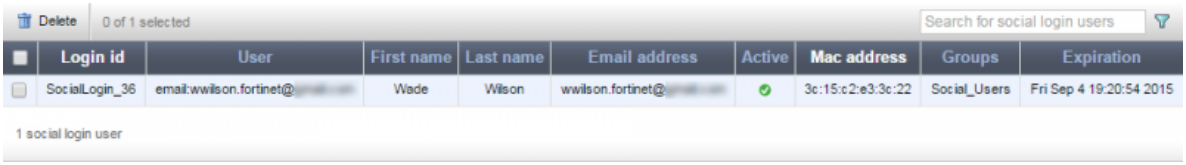
1. Connect to the WiFi and attempt to browse the Internet. You will be redirected to the captive portal splash page.
   Select **Form** and you should be redirected to the form-based authentication login page.



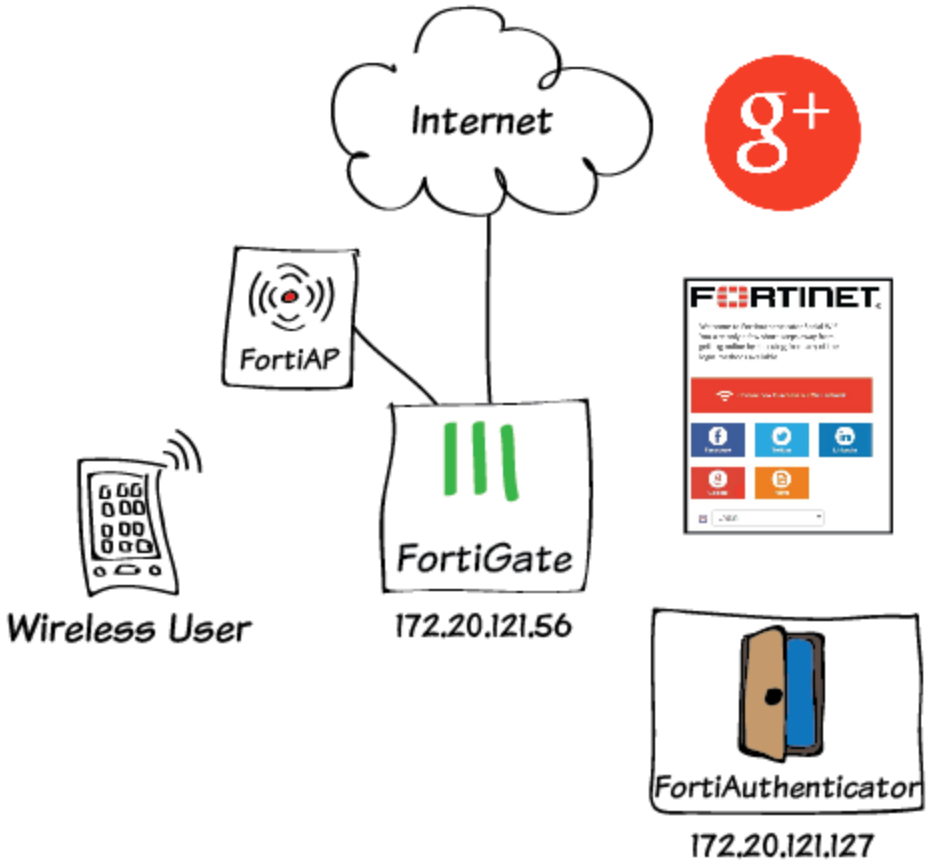
2. Select your preferred **Verification method**, enter valid credentials, and select **Submit**. You will be redirected to the URL initially requested.
   You can now browse freely until the social login account expires, as configured on the FortiAuthenticator under **Authentication > Captive Portal > General**.



3. To view the authenticated user added on FortiAuthenticator, go to **Authentication > User Management > Social Login Users**.



Social WiFi captive portal with FortiAuthenticator (Google+)



This recipe involves configuring an API for Google+ accounts, setting up a social portal RADIUS service on the FortiAuthenticator, and configuring the FortiGate for captive portal access.

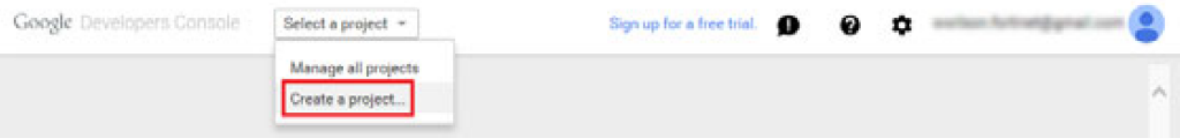
This recipe does not include FortiAP registration instructions.

Note that some CLI usage is required when configuring the FortiGate.

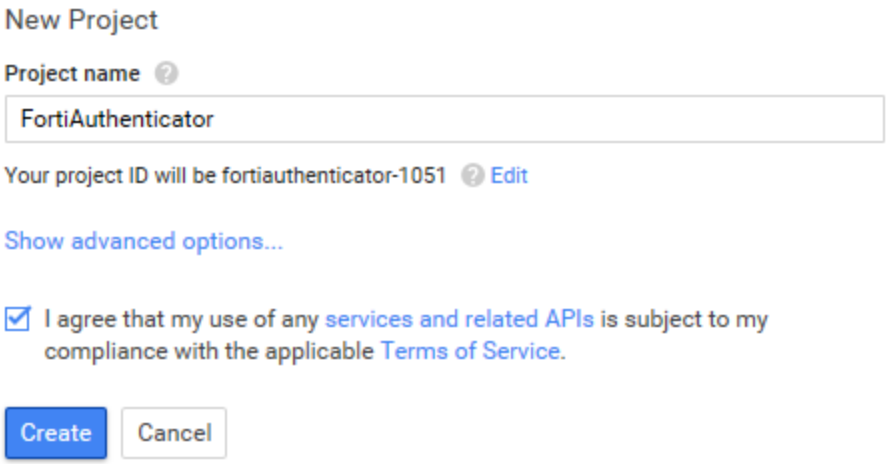
The FortiAuthenticator has been given an example fully qualified domain name (FQDN) -- *fortiauthenticator.example.com*.

Configuring the Google+ developer account API

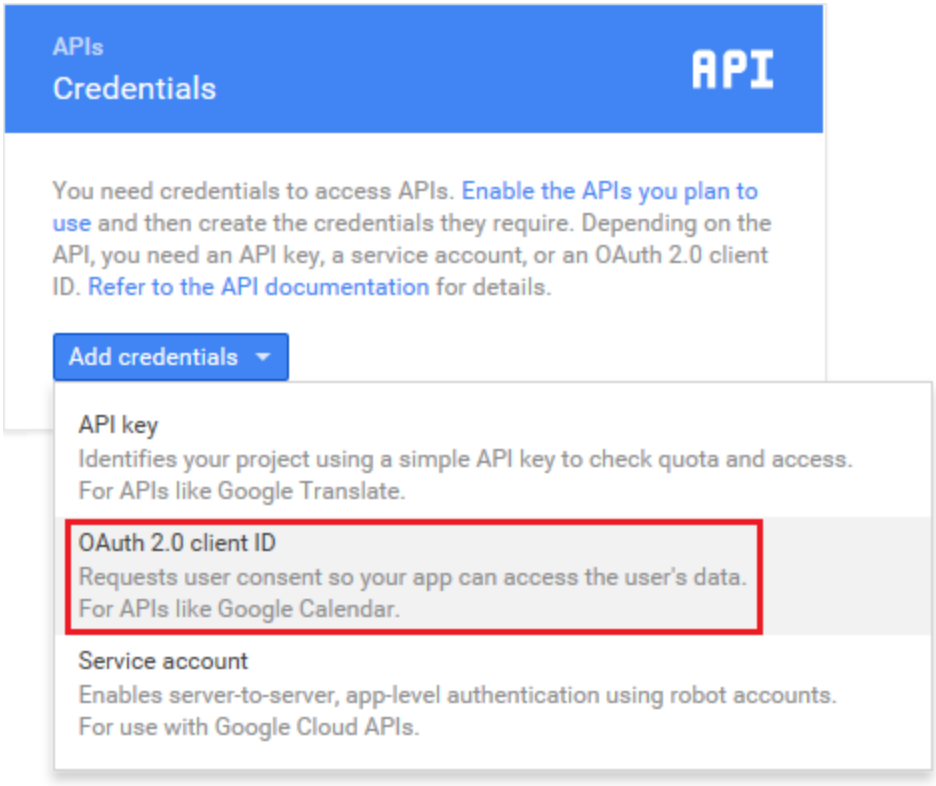
1. Open a browser and log in to your Google account.
   Browse to the following URL:
   https://console.developers.google.com
   Under **Select a project**, select **Create a project**.



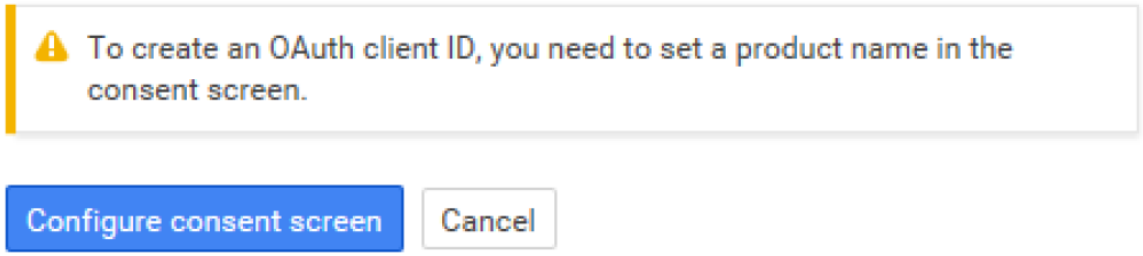
2. Enter a **Project name**, and accept the Terms of Service before continuing.



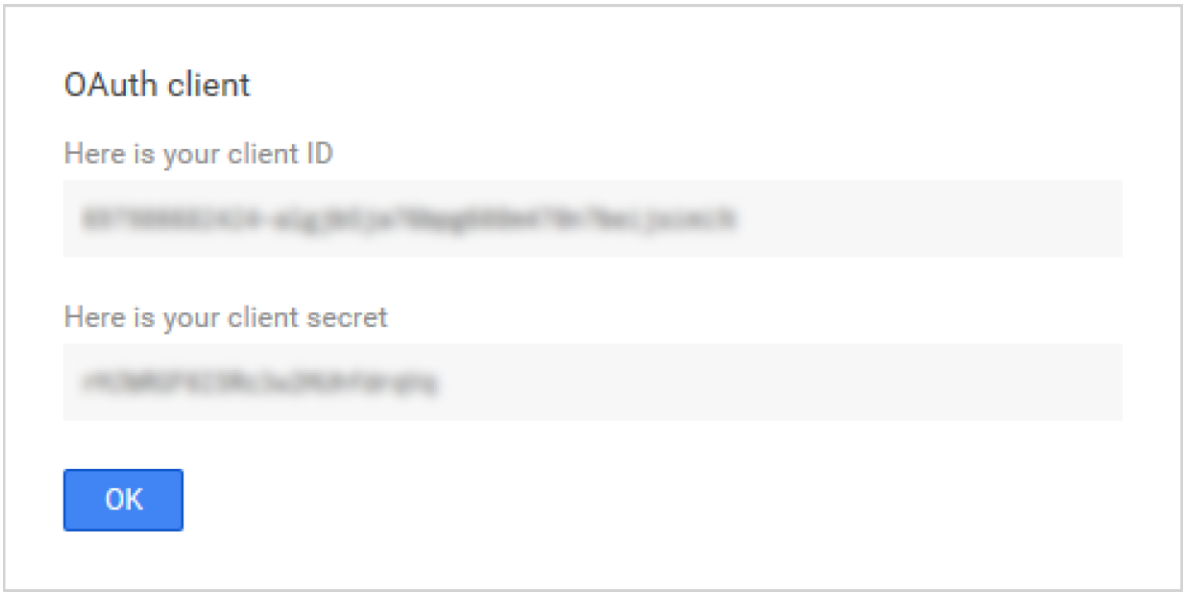
3. Go to **APIs & auth > Credentials** and select **OAuth 2.0 client ID** from the **Add credentials** drop-down.



4. When prompted, select **Configure consent screen**. Enter an **Email address** and **Product name**. You must now create the client ID.

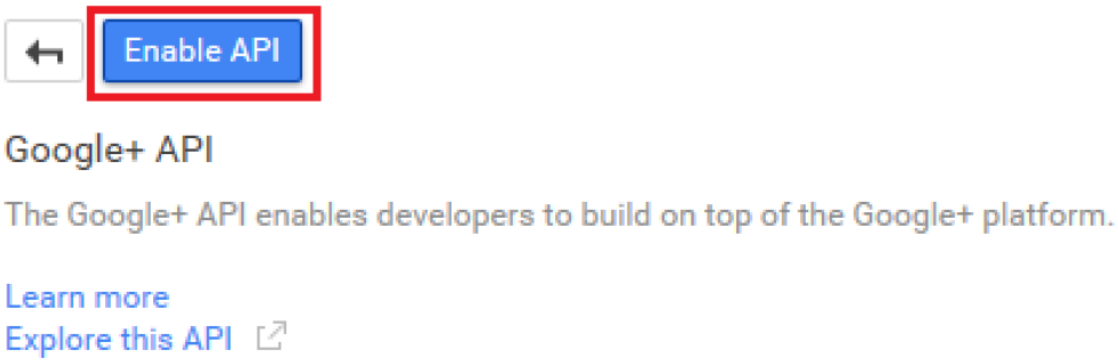


5. Set **Application type** to **Web application**. Under **Authorized JavaScript origins**, enter the FortiAuthenticator FQDN.
   Under **Authorized redirect URIs**, enter the following:
   https://fortiauthenticator.example.com/social/complete/google-oauth2/
   Note that the FortiAuthenticator needs to be able to access the Internet.
6. Upon creating the client ID, a window will appear with your **client ID** and **client secret**.
   Take note of the **client ID** and **client secret** as they are required when configuring the captive portal on the FortiAuthenticator.



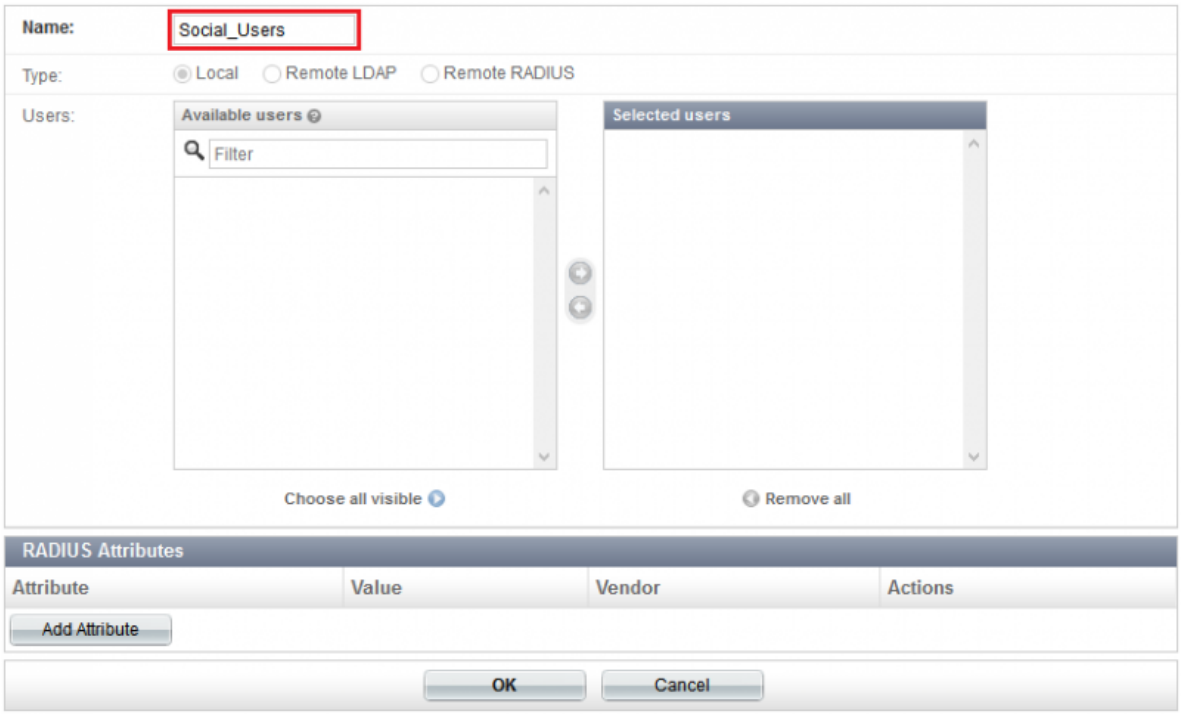
   The **client ID** and **client secret** can be accessed at any time on the Google developer account, but it may be a good idea to copy them to a secure location.
7. Go to **APIs & auth > APIs > Social APIs**, and select **Google+ API**.

8. Enable the API.

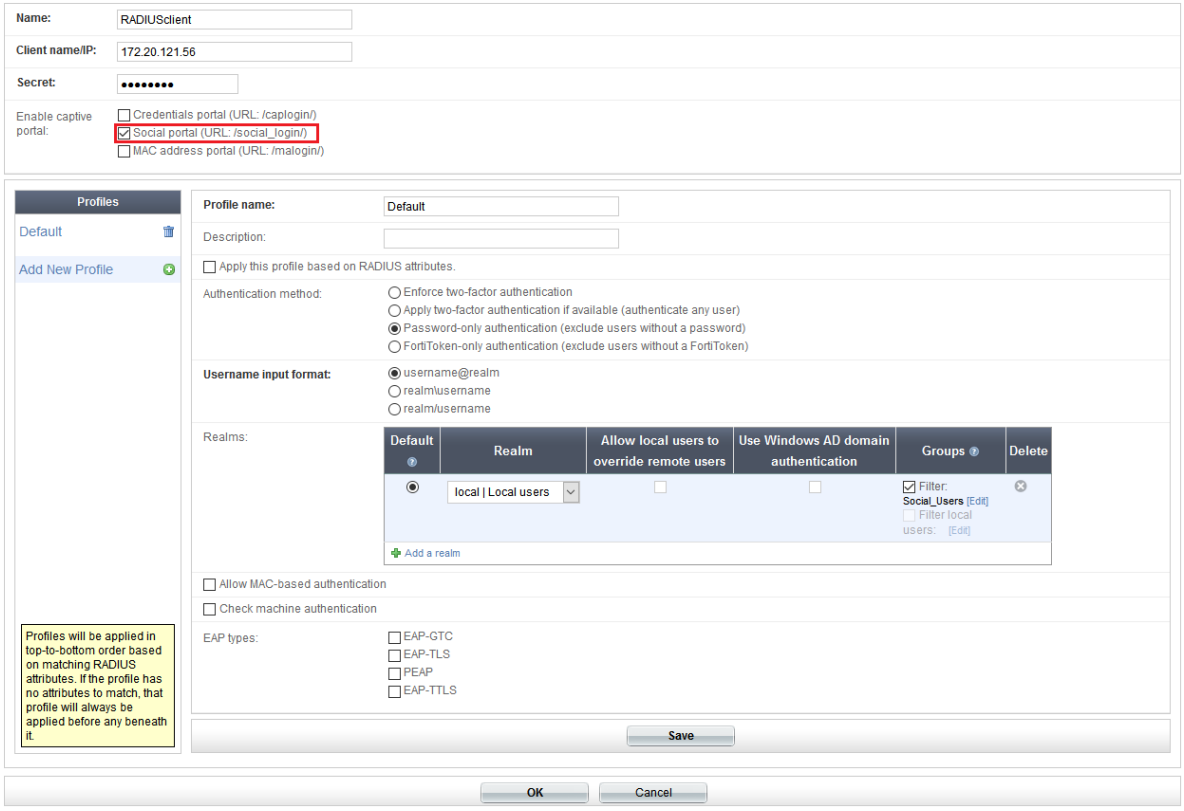


Configuring the social portal RADIUS service on the FortiAuthenticator

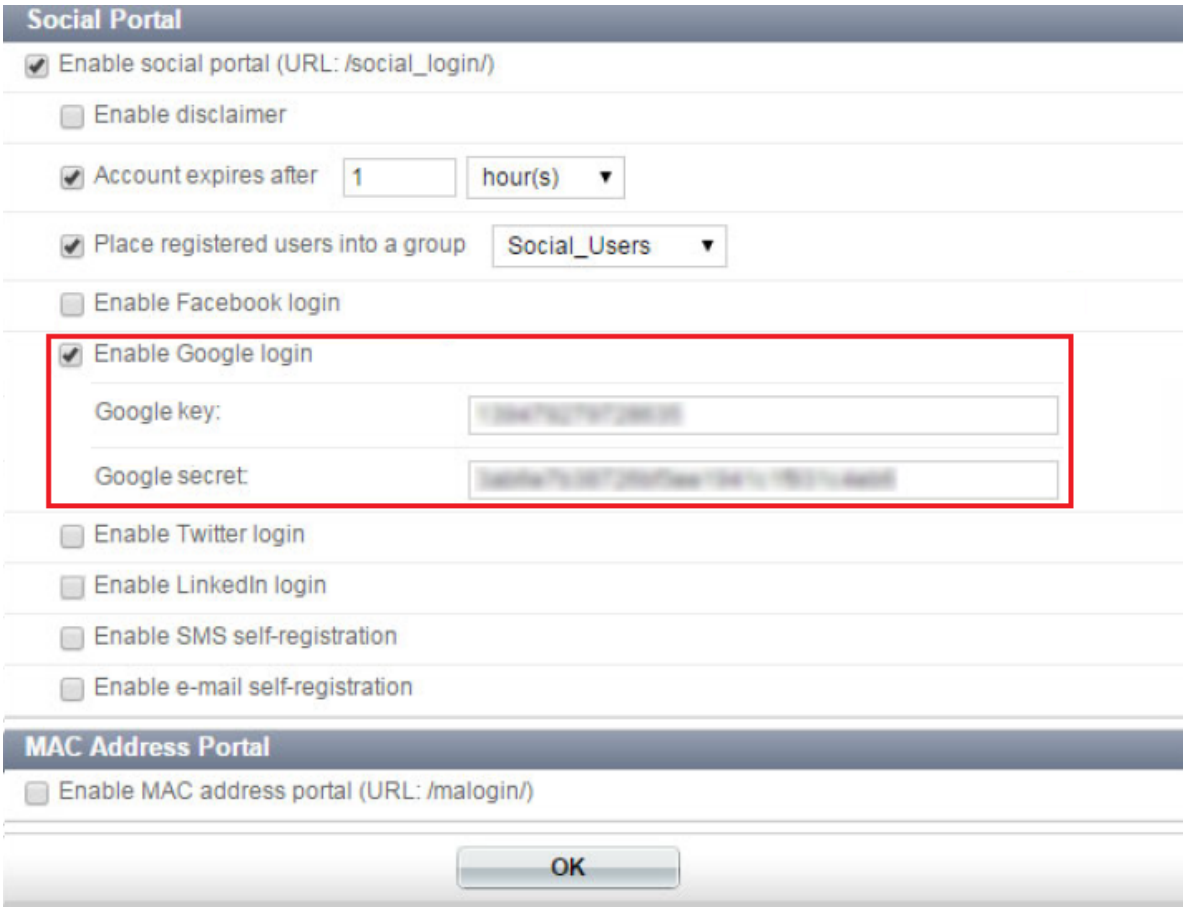
1. Go to **Authentication > User Management > User Groups** and create a **Social_Users** user group. Users that log in through the forms-based authentication method will be placed in this group once it is added to the captive portal general settings.



2. Go to **Authentication > RADIUS Service > Clients** and create a new RADIUS client.
   Enter a **Name** for the RADIUS client (the FortiGate) and enter its IP address (in the example, *172.20.121.56*).
   Enable the **Social portal** captive portal.
   Enter the pre-shared **Secret** and set the **Authentication method**. The FortiGate will use this secret key in its RADIUS configuration.
   Add the **Social_Users** user group to the **Realms** group filter as shown.
   Select **Save** and then **OK**.

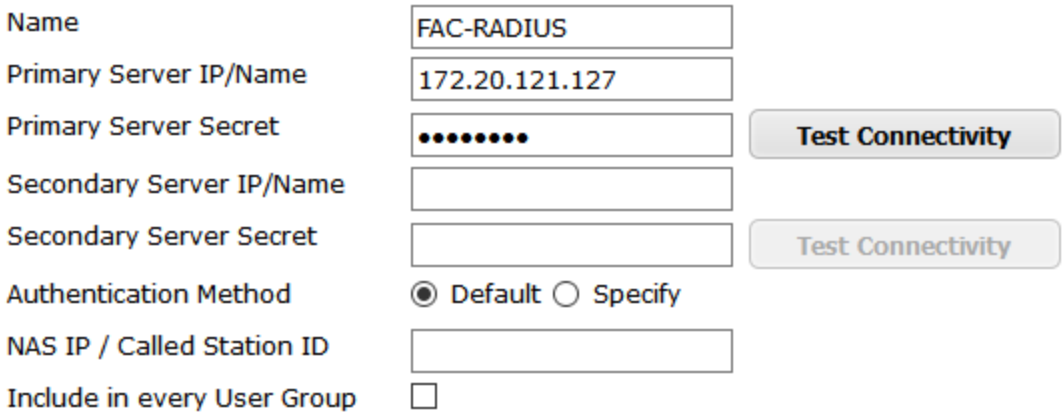


3. Next go to **Authentication > Captive Portal > General** and enable **Social Portal**.
   Configure the account expiry time (in the example, **1 hour**).
   Set **Place registered users into a group** to **Social_Users**.
   Enable the **Google** login option and add your **Google key** and **Google secret**.



Configuring the FortiGate authentication settings

1. On the FortiGate, go to **User & Device > RADIUS Servers** and create the connection to the FortiAuthenticator RADIUS server, using its IP and pre-shared secret.
   Use the **Test Connectivity** option with valid credentials to test the connection.

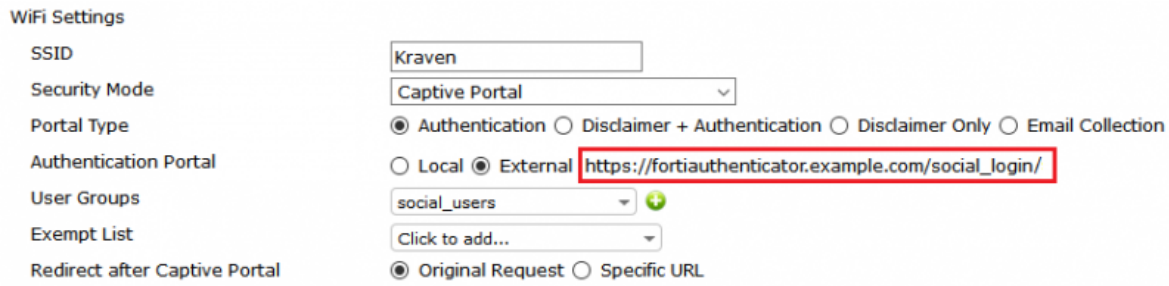


2. Next go to **User & Device > User Groups** and create a RADIUS user group.

Set **Type** to **Firewall** and add the RADIUS server to the **Remote groups** table.

Configuring the FortiGate WiFi settings

1. Go to **WiFi & Switch Controller > SSID** and select the SSID interface.
   Under **WiFi Settings**, set the **Security Mode** to **Captive Portal**.



2. For the **Authentication Portal**, select **External**, and enter the FQDN of the FortiAuthenticator, followed by **/social_login/**.
   For this recipe, it is set to `https://fortiauthenticator.example.com/social_login/`
   Set **User Groups** to the **social_users** group.

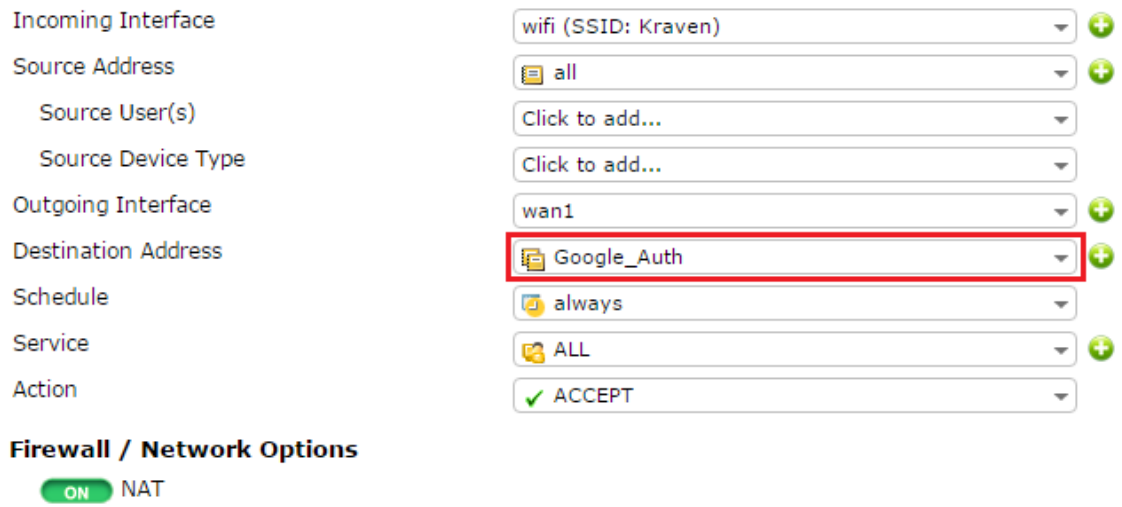
Configuring the FortiGate to allow access to Google

1. On the FortiGate, configure firewall addresses to allow users to access the Google login page.
   The following step can be performed in the GUI, but may take considerably longer than using the CLI. You can copy and paste the commands below.
   Open the **CLI Console** and enter the following, which creates the firewall addresses and adds them to a firewall address group called **Google_Auth**.

```
config firewall address
   edit "www.googleapis.com"
      set type fqdn
      set fqdn "www.googleapis.com"
   next
   edit "accounts.google.com"
      set type fqdn
      set fqdn "accounts.google.com"
   next
   edit "ssl.gstatic.com"
      set type fqdn
      set fqdn "ssl.gstatic.com"
   next
   edit "fonts.gstatic.com"
      set type fqdn
```

```
      set fqdn "fonts.gstatic.com"
   next
   edit "www.gstatic.com"
      set type fqdn
      set fqdn "www.gstatic.com"
   next
   edit "Google_13"
      set subnet 216.58.192.0 255.255.224.0
   next
end
config firewall addrgrp
   edit "Google_Auth"
      set member "ssl.gstatic.com" "accounts.google.com" "www.googleapis.com"
           "fonts.gstatic.com" "www.gstatic.com" "Google_13"
   next
end
```

2. Go to **Policy & Objects > IPv4 Policy** and create a policy for Google authentication traffic.
   Set **Incoming Interface** to the WiFi SSID interface and set **Source Address** to **all**.
   Set **Outgoing Interface** to the Internet-facing interface and set **Destination Address** to **Google_Auth**.
   Set **Service** to **ALL** and enable **NAT**. Configure **Security Profiles** accordingly.



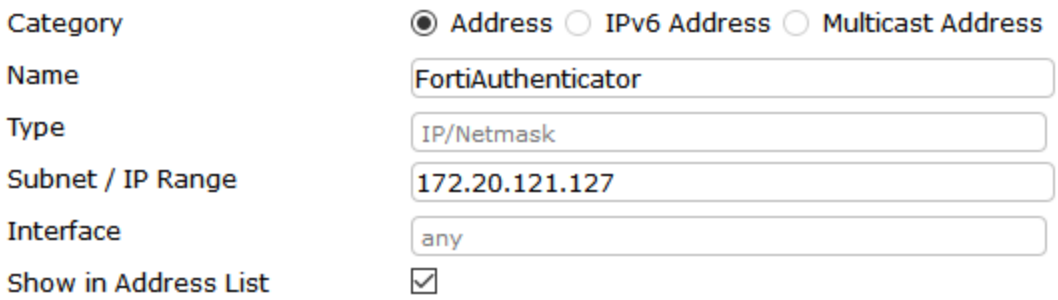
3. Then open the **CLI Console**. Using the policy's ID, enter the following command to exempt the Google authentication traffic policy from the captive portal:

```
config firewall policy
   edit <policy_id>
      set captive-portal-exempt enable
   next
end
```

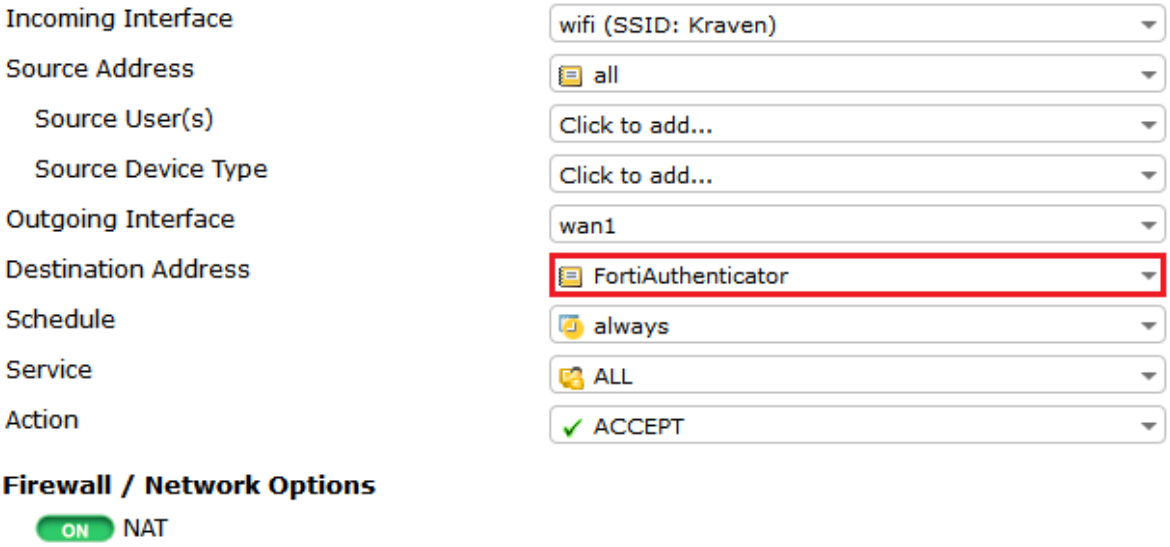
   This command allows access to the external captive portal.

Configuring the FortiGate to allow access to the FortiAuthenticator

1. On the FortiGate, go to **Policy & Objects > Addresses** and add the FortiAuthenticator firewall object.
   For **Subnet/IP Range** enter the IP address of the FortiAuthenticator.



2. Go to **Policy & Objects > IPv4 Policy** and create the FortiAuthenticator access policy.
   Set **Incoming Interface** to the WiFi SSID interface and set **Source Address** to **all**.
   Set **Outgoing Interface** to the Internet-facing interface and set **Destination Address** to the **FortiAuthenticator** address object.
   Set **Service** to **ALL** and enable **NAT**.
   Once created, note the policy's ID using the **ID** column.



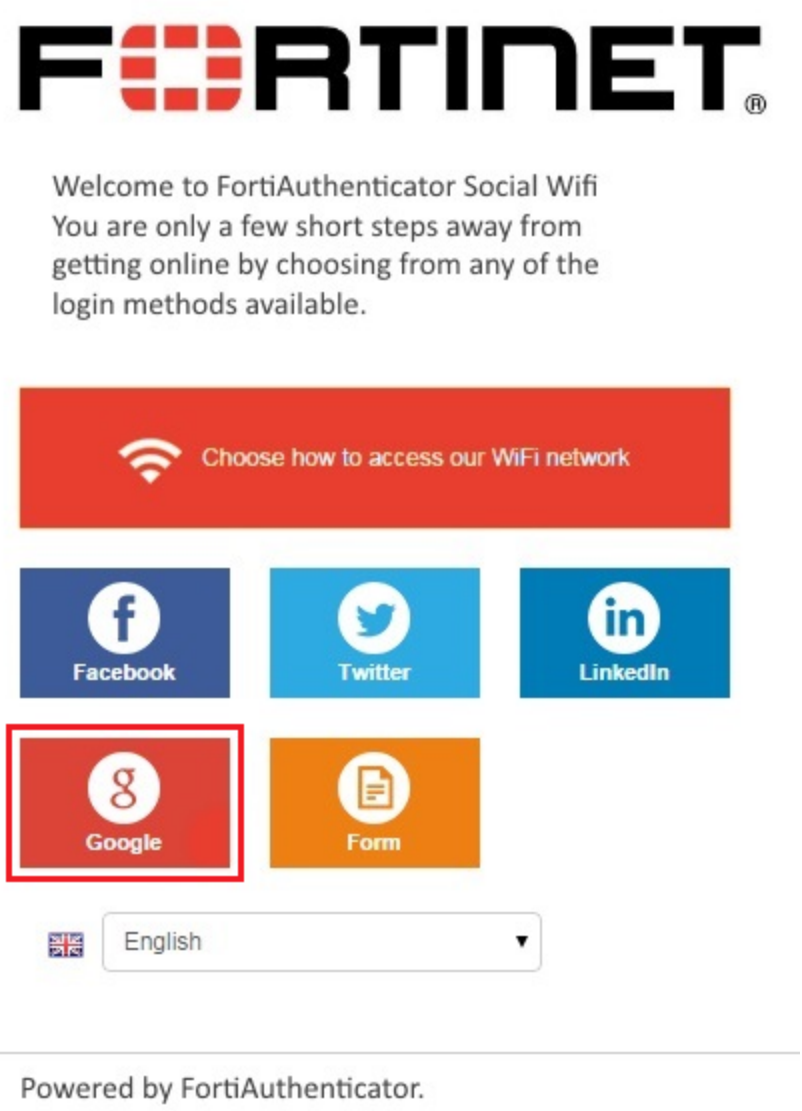
3. Open the **CLI Console** and enter the following command to exempt the FortiAuthenticator access policy from the captive portal:

```
config firewall policy
   edit <policy_id>
      set captive-portal-exempt enable
   next
end
```

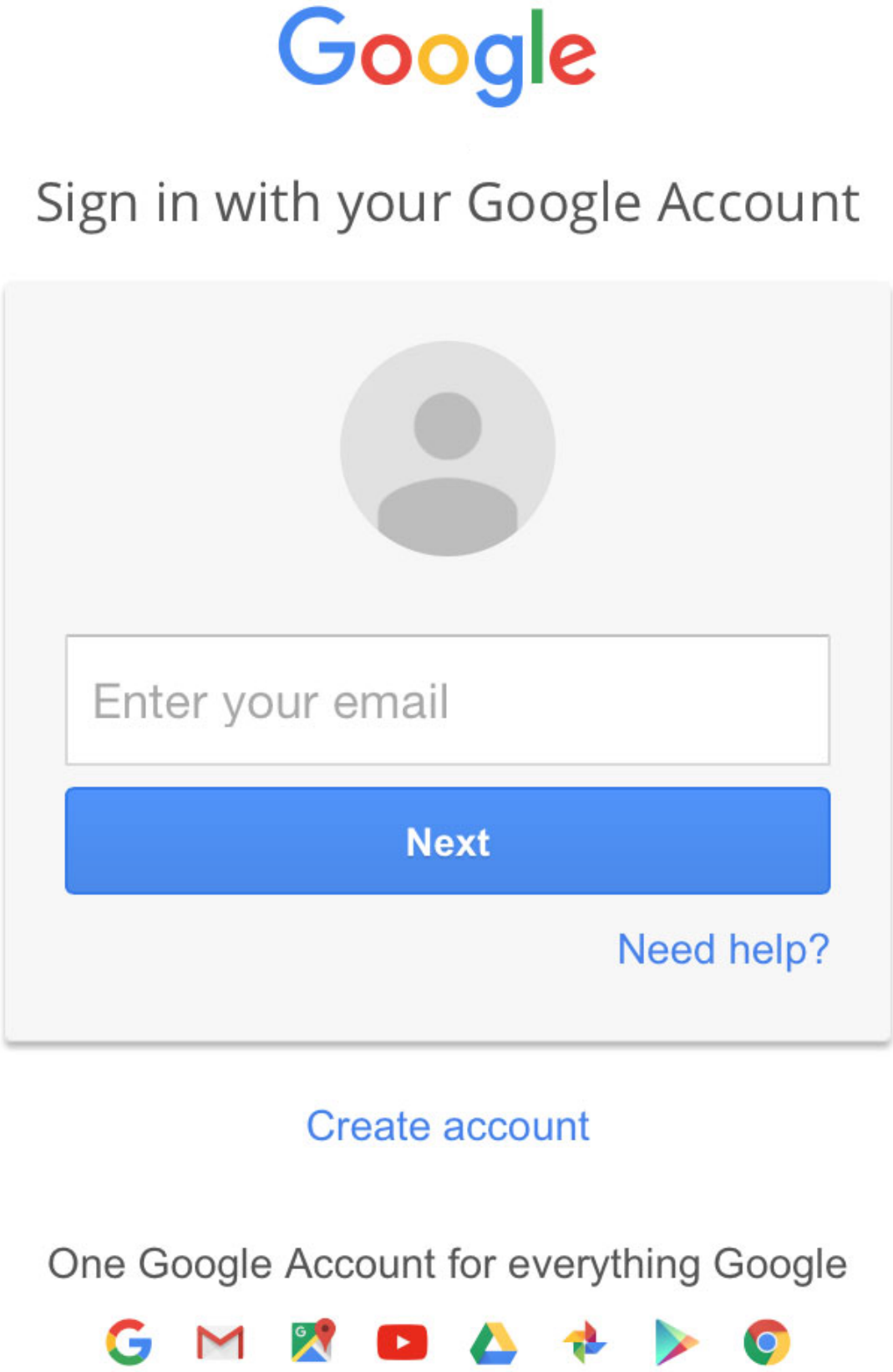
   This command allows access to the external captive portal.

Results

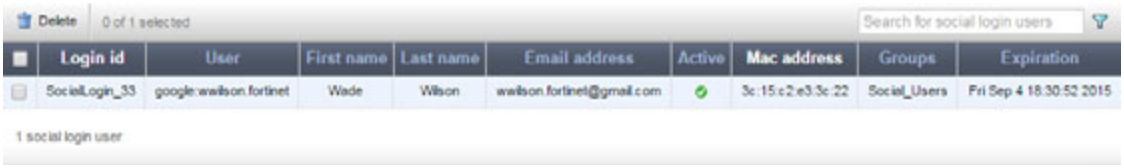
1. Connect to the WiFi and attempt to browse the Internet. You will be redirected to the captive portal splash page.
   Select **Google** and you should be redirected to the Google login page.



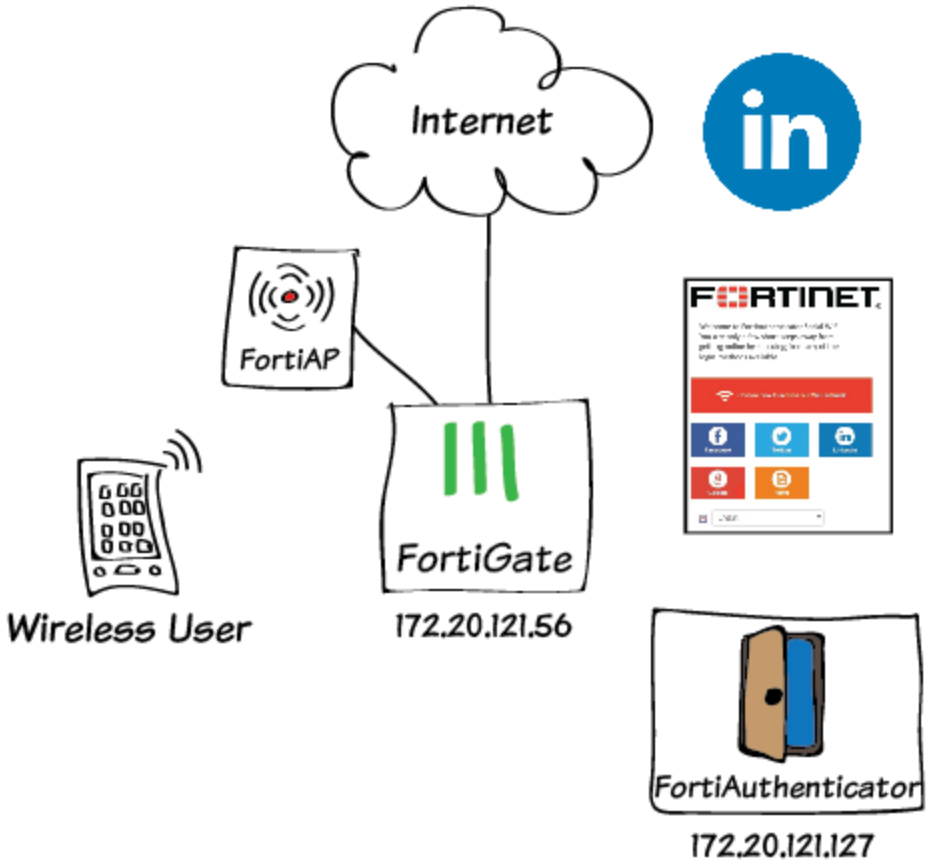
2. Enter valid Google credentials and you will be redirected to the URL initially requested.
   You can now browse freely until the social login account expires, as configured on the FortiAuthenticator under **Authentication > Captive Portal > General**.


Google
Sign in with your Google Account
Enter your email
Next
Need help?
Create account
One Google Account for everything Google

3. To view the authenticated user added on FortiAuthenticator, go to **Authentication > User Management > Social Login Users**.



Social WiFi captive portal with FortiAuthenticator (LinkedIn)



This recipe involves configuring an API for LinkedIn accounts, setting up a social portal RADIUS service on the FortiAuthenticator, and configuring the FortiGate for captive portal access.

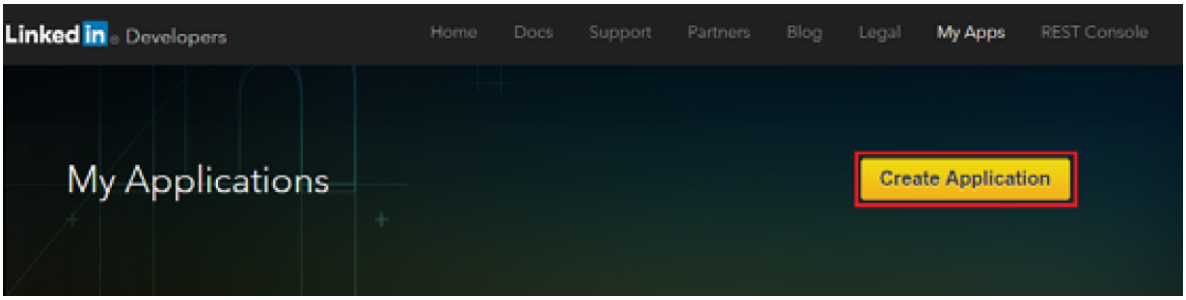
This recipe does not include FortiAP registration instructions.

Note that some CLI usage is required when configuring the FortiGate.

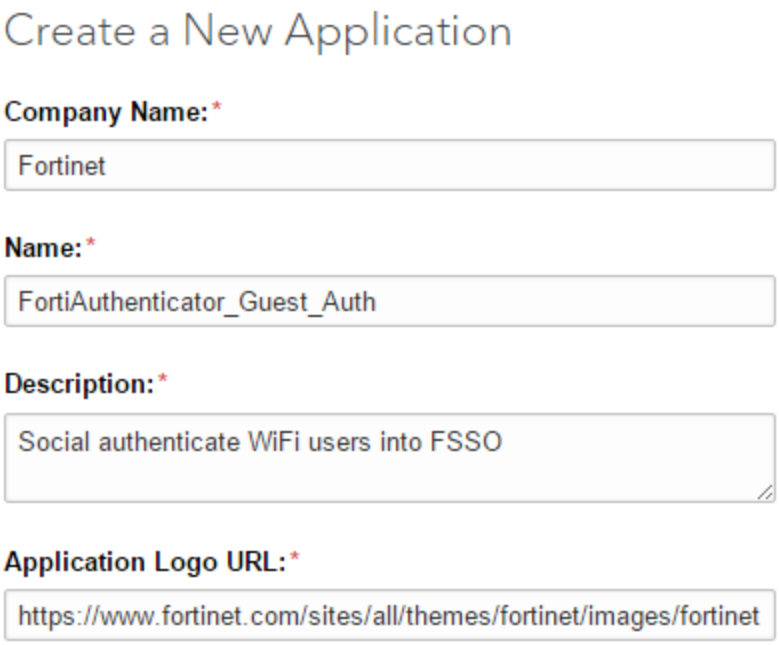
The FortiAuthenticator has been given an example fully qualified domain name (FQDN) -- *fortiauthenticator.example.com*.

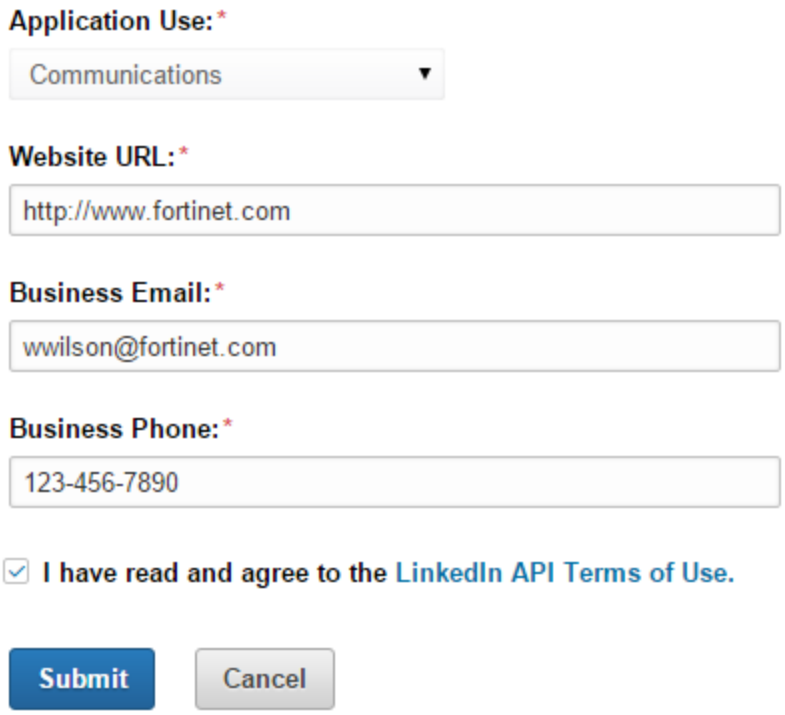
Configuring the LinkedIn developer account API

1. Open a browser and log in to your LinkedIn account.
   Navigate to the following URL:
   https://developer.linkedin.com/documents/authentication
   Select **Create Application**.

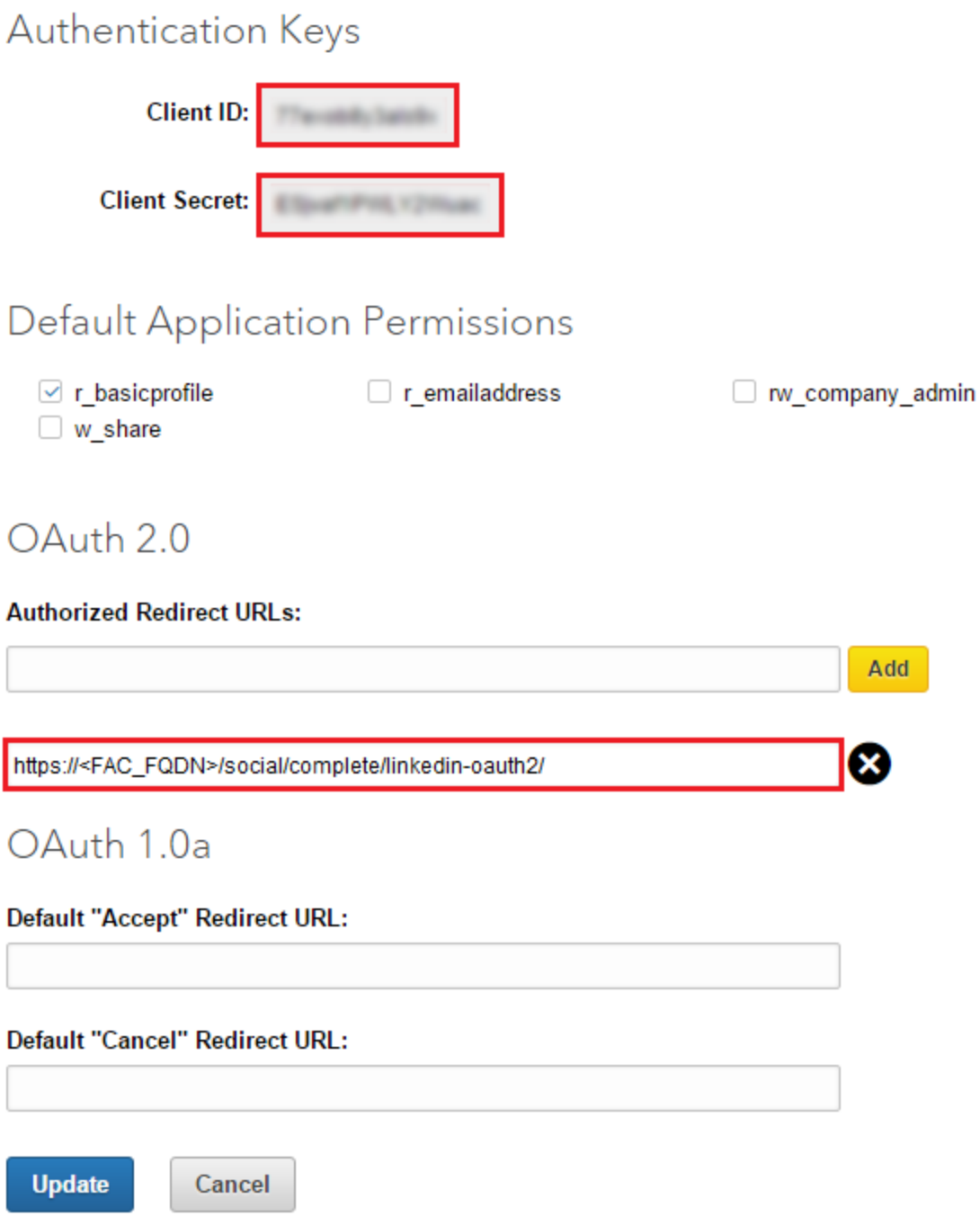


2. Enter information in the required fields. Unlike the other social applications, LinkedIn requires an Application Logo URL.
   Select that you have read and agree to the LinkedIn API Terms of Use and select **Submit**.





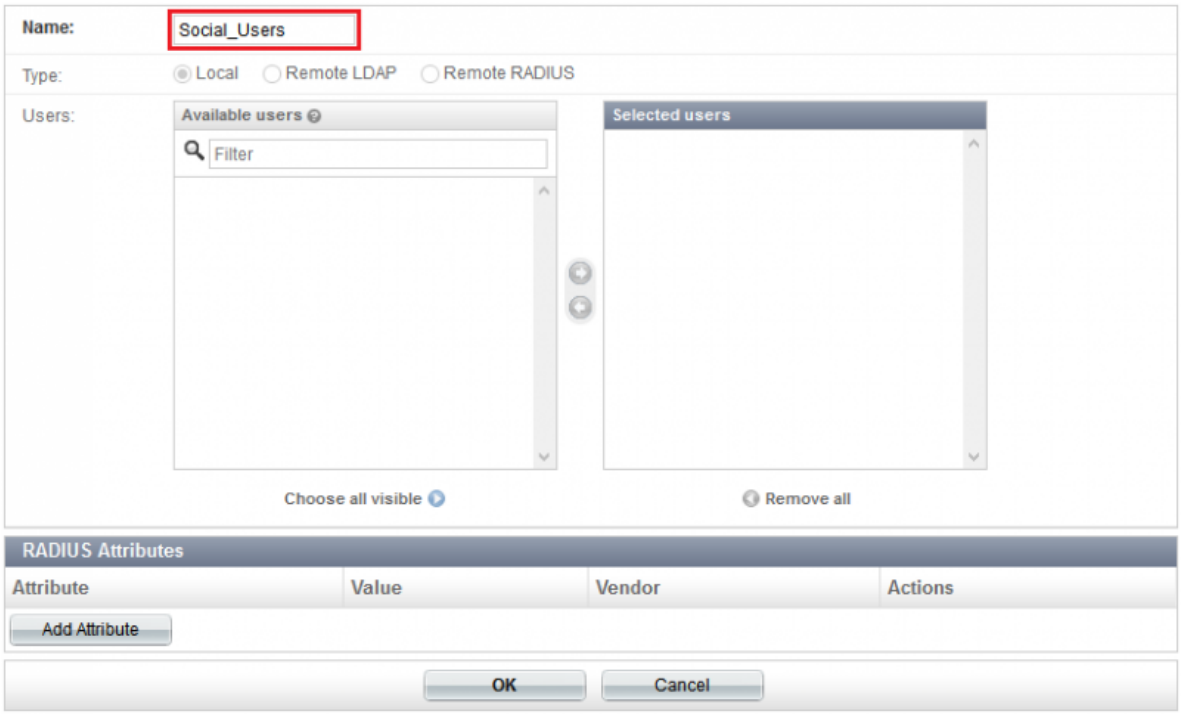
3. The next screen shows your **Client ID** and **Client secret**.
   Take note of the **Client ID** and **Client secret** as they are required when configuring the captive portal on the FortiAuthenticator.



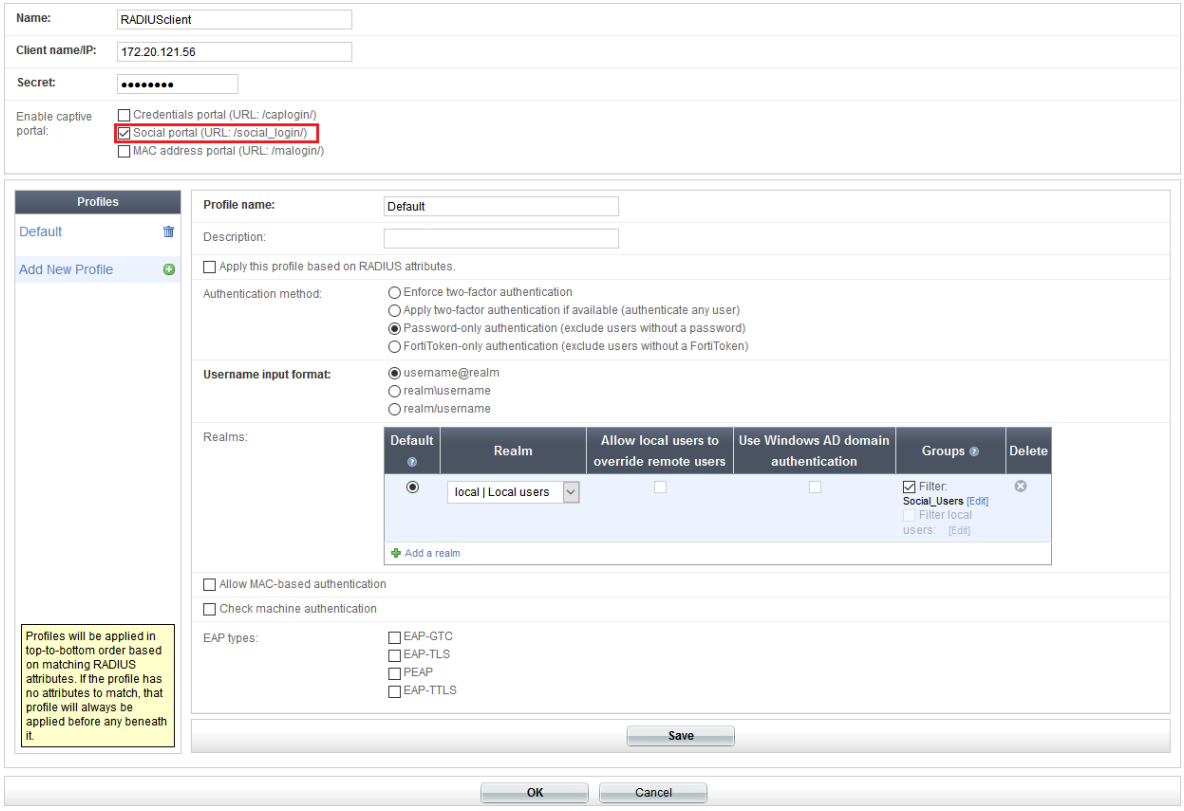
4. Under Authorized Redirect URLs, enter the following:
   https://fortiauthenticator.example.com/social/complete/linkedin-oauth2/
   Note that the FortiAuthenticator needs to be able to access the Internet.
   The **client ID** and **client secret** can be accessed at any time on the LinkedIn developer account, but it may be a good idea to copy them to a secure location.

Configuring the social portal RADIUS service on the FortiAuthenticator

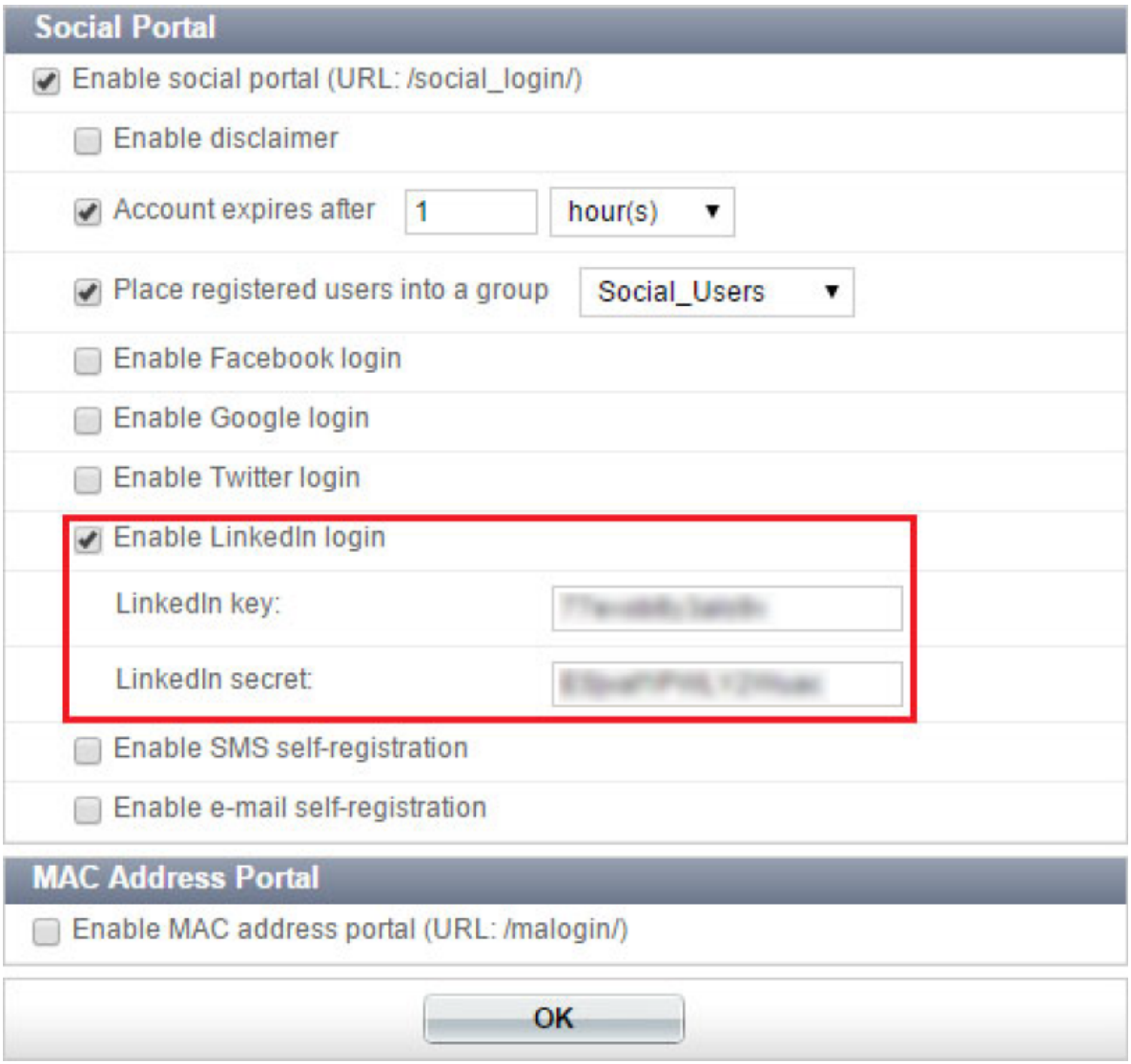
1. Go to **Authentication > User Management > User Groups** and create a **Social_Users** user group. Users that log in through the forms-based authentication method will be placed in this group once it is added to the captive portal general settings.



2. Go to **Authentication > RADIUS Service > Clients** and create a new RADIUS client.
   Enter a **Name** for the RADIUS client (the FortiGate) and enter its IP address (in the example, *172.20.121.56*).
   Enable the **Social portal** captive portal.
   Enter the pre-shared **Secret** and set the **Authentication method**. The FortiGate will use this secret key in its RADIUS configuration.
   Add the **Social_Users** user group to the **Realms** group filter as shown.
   Select **Save** and then **OK**.

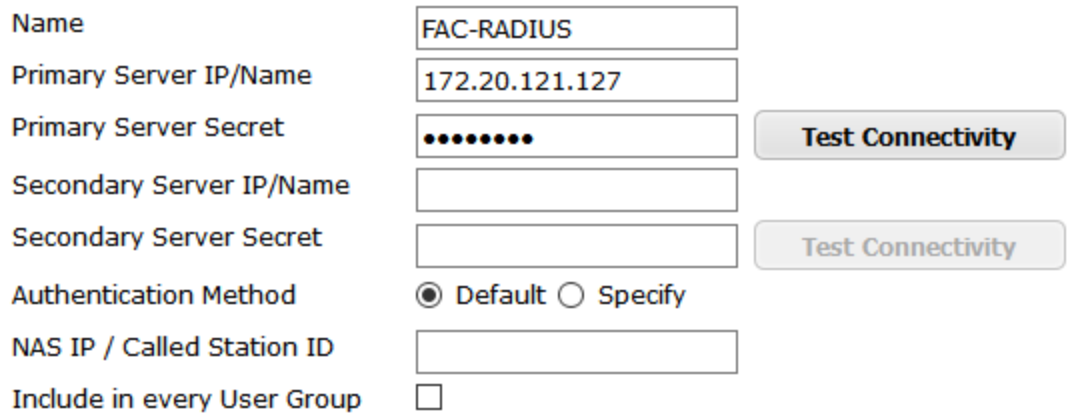


3. Next go to **Authentication > Captive Portal > General** and enable **Social Portal**.
   Configure the account expiry time (in the example, **1 hour**).
   Set **Place registered users into a group** to **Social_Users**.
   Enable the **LinkedIn** login option and add your **LinkedIn key** and **LinkedIn secret**.



Configuring the FortiGate authentication settings

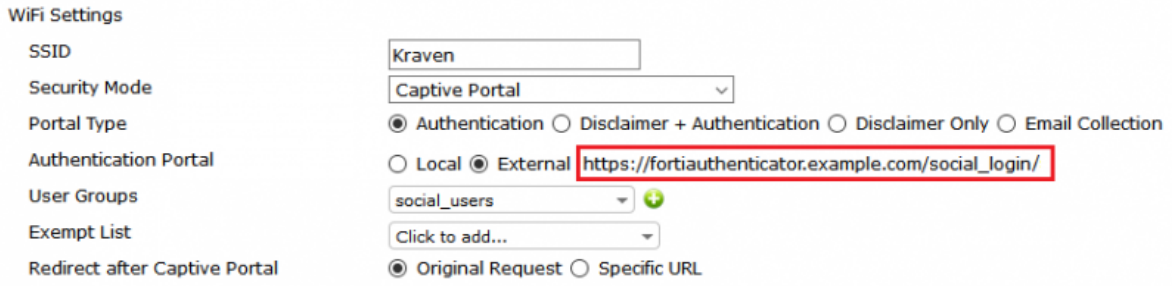
1. On the FortiGate, go to **User & Device > RADIUS Servers** and create the connection to the FortiAuthenticator RADIUS server, using its IP and pre-shared secret.
   Use the **Test Connectivity** option with valid credentials to test the connection.



2. Next go to **User & Device > User Groups** and create a RADIUS user group.
   Set **Type** to **Firewall** and add the RADIUS server to the **Remote groups** table.

Configuring the FortiGate WiFi settings

1. Go to **WiFi & Switch Controller > SSID** and select the SSID interface.
   Under **WiFi Settings**, set the **Security Mode** to **Captive Portal**.



2. For the **Authentication Portal**, select **External**, and enter the FQDN of the FortiAuthenticator, followed by **/social_login/**.
   For this recipe, it is set to `https://fortiauthenticator.example.com/social_login/`
   Set **User Groups** to the **social_users** group.

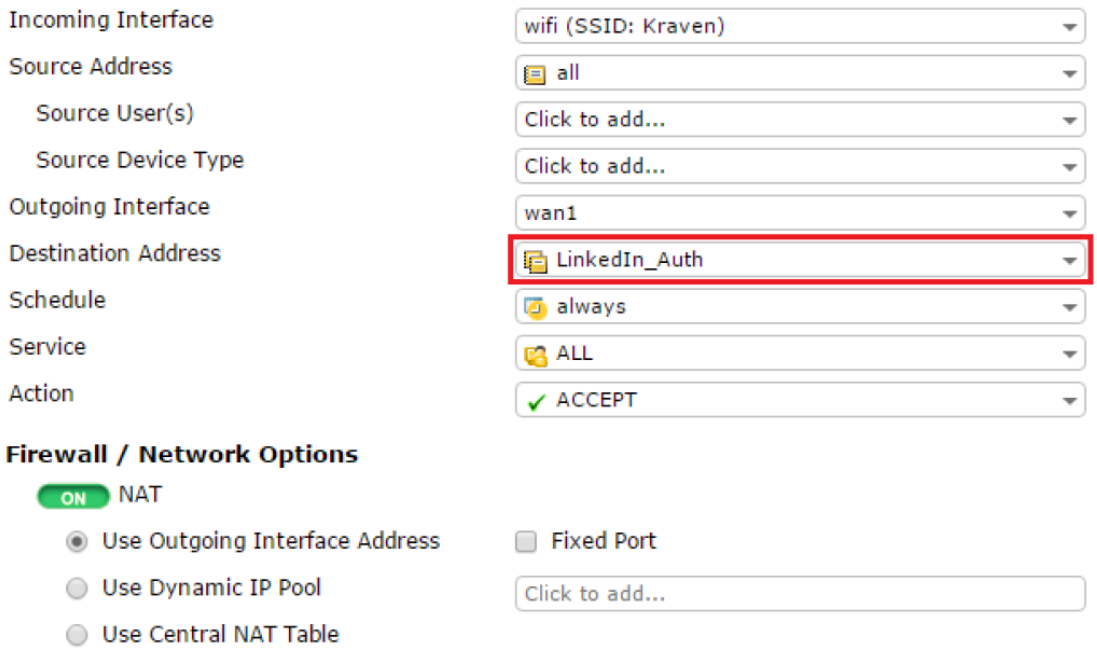
Configuring the FortiGate to allow access to LinkedIn

1. On the FortiGate, configure firewall addresses to allow users to access the LinkedIn login page.
   The following step can be performed in the GUI, but may take considerably longer than using the CLI. You can copy and paste the commands below.

Open the **CLI Console** and enter the following, which creates the firewall addresses and adds them to a firewall address group called **LinkedIn_Auth**.

```
config firewall address
   edit "www.linkedin.com"
      set type fqdn
      set fqdn "www.linkedin.com"
   next
   edit "api.linkedin.com"
      set type fqdn
      set fqdn "api.linkedin.com"
   next
   edit "static.licdn.com"
      set type fqdn
      set fqdn "static.licdn.com"
   next
   edit "help.linkedin.com"
      set type fqdn
      set fqdn "help.linkedin.com"
   next
   edit "www.fortinet.com"
      set type fqdn
      set fqdn "www.fortinet.com"
   next
end
config firewall addrgrp
   edit "LinkedIn_Auth"
      set member "api.linkedin.com" "www.linkedin.com" "help.linkedin.com"
           "www.fortinet.com" "static.licdn.com"
   next
end
```

2. Go to **Policy & Objects > IPv4 Policy** and create a policy for LinkedIn authentication traffic.
   Set **Incoming Interface** to the WiFi SSID interface and set **Source Address** to **all**.
   Set **Outgoing Interface** to the Internet-facing interface and set **Destination Address** to **LinkedIn_Auth**.
   Set **Service** to **ALL** and enable **NAT**. Configure **Security Profiles** accordingly.



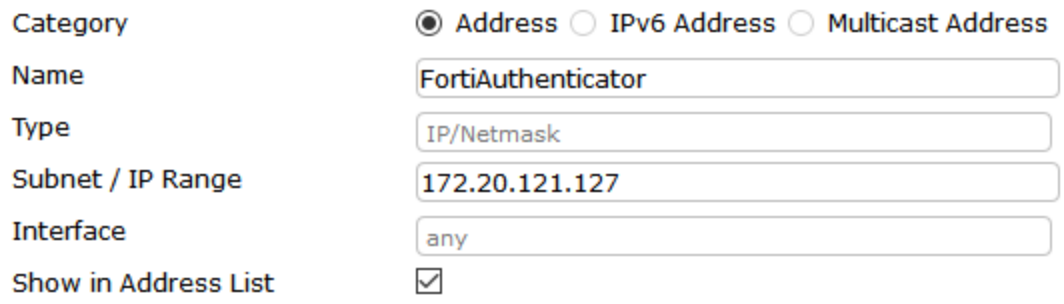
3. Then open the **CLI Console**. Using the policy's ID, enter the following command to exempt the LinkedIn authentication traffic policy from the captive portal:

```
config firewall policy
   edit <policy_id>
      set captive-portal-exempt enable
   next
end
```

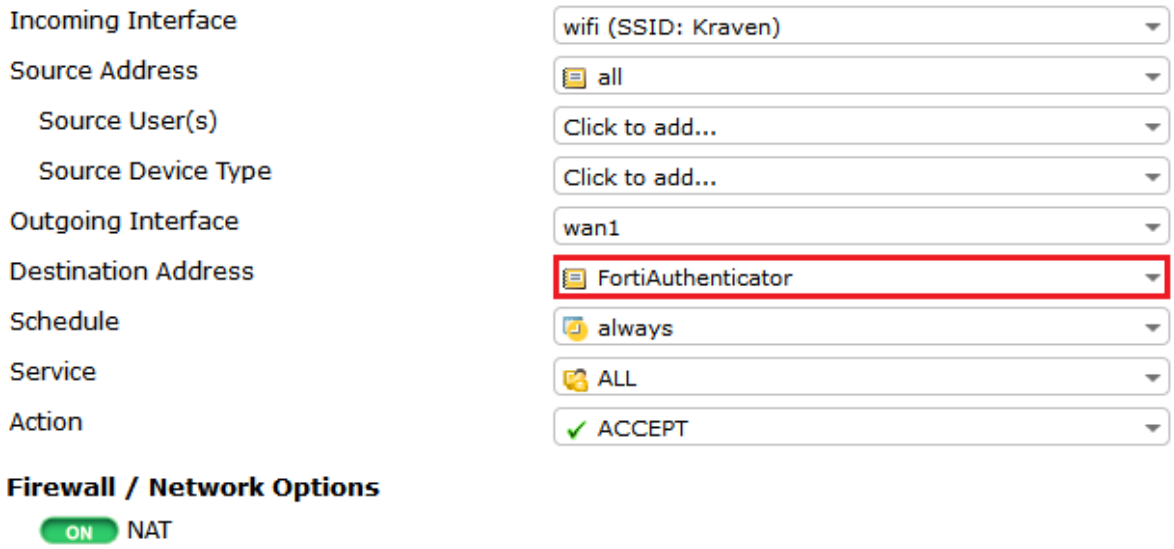
This command allows access to the external captive portal.

Configuring the FortiGate to allow access to the FortiAuthenticator

1. On the FortiGate, go to **Policy & Objects > Addresses** and add the FortiAuthenticator firewall object. For **Subnet/IP Range** enter the IP address of the FortiAuthenticator.



2. Go to **Policy & Objects > IPv4 Policy** and create the FortiAuthenticator access policy.
   Set **Incoming Interface** to the WiFi SSID interface and set **Source Address** to **all**.
   Set **Outgoing Interface** to the Internet-facing interface and set **Destination Address** to the **FortiAuthenticator** address object.
   Set **Service** to **ALL** and enable **NAT**.
   Once created, note the policy's ID using the **ID** column.



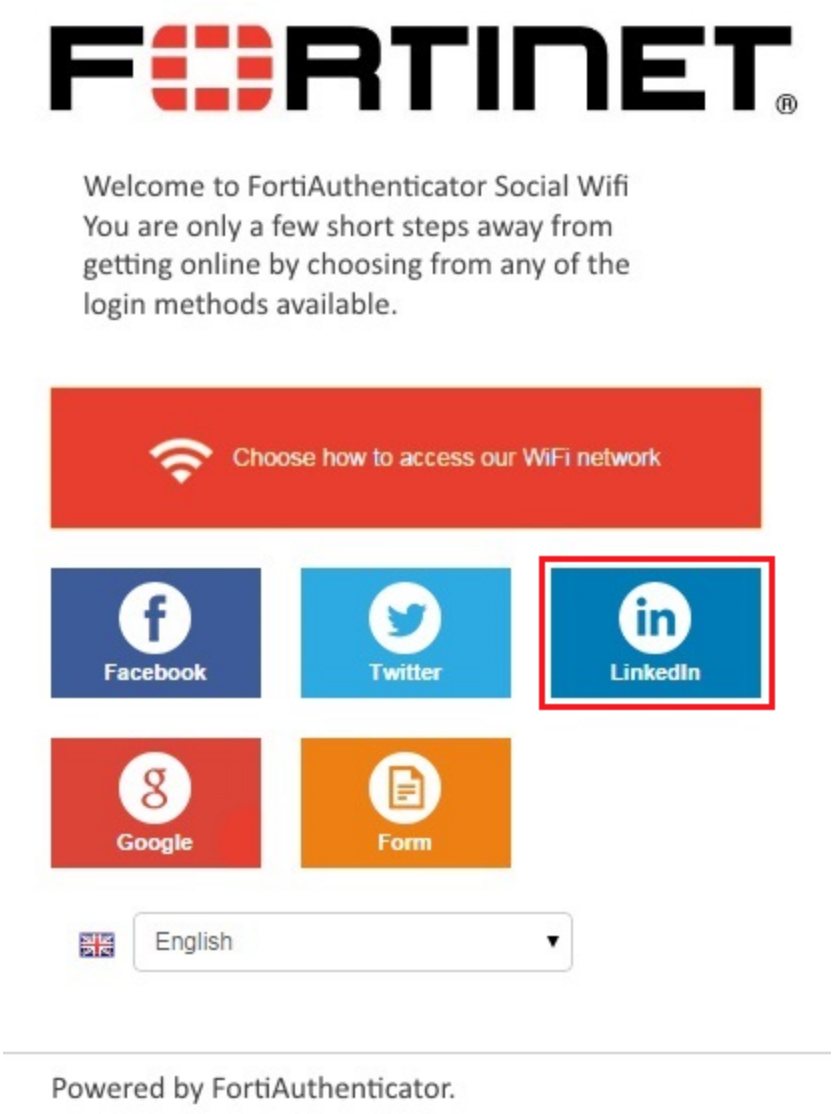
3. Open the **CLI Console** and enter the following command to exempt the FortiAuthenticator access policy from the captive portal:

```
config firewall policy
   edit <policy_id>
      set captive-portal-exempt enable
   next
end
```

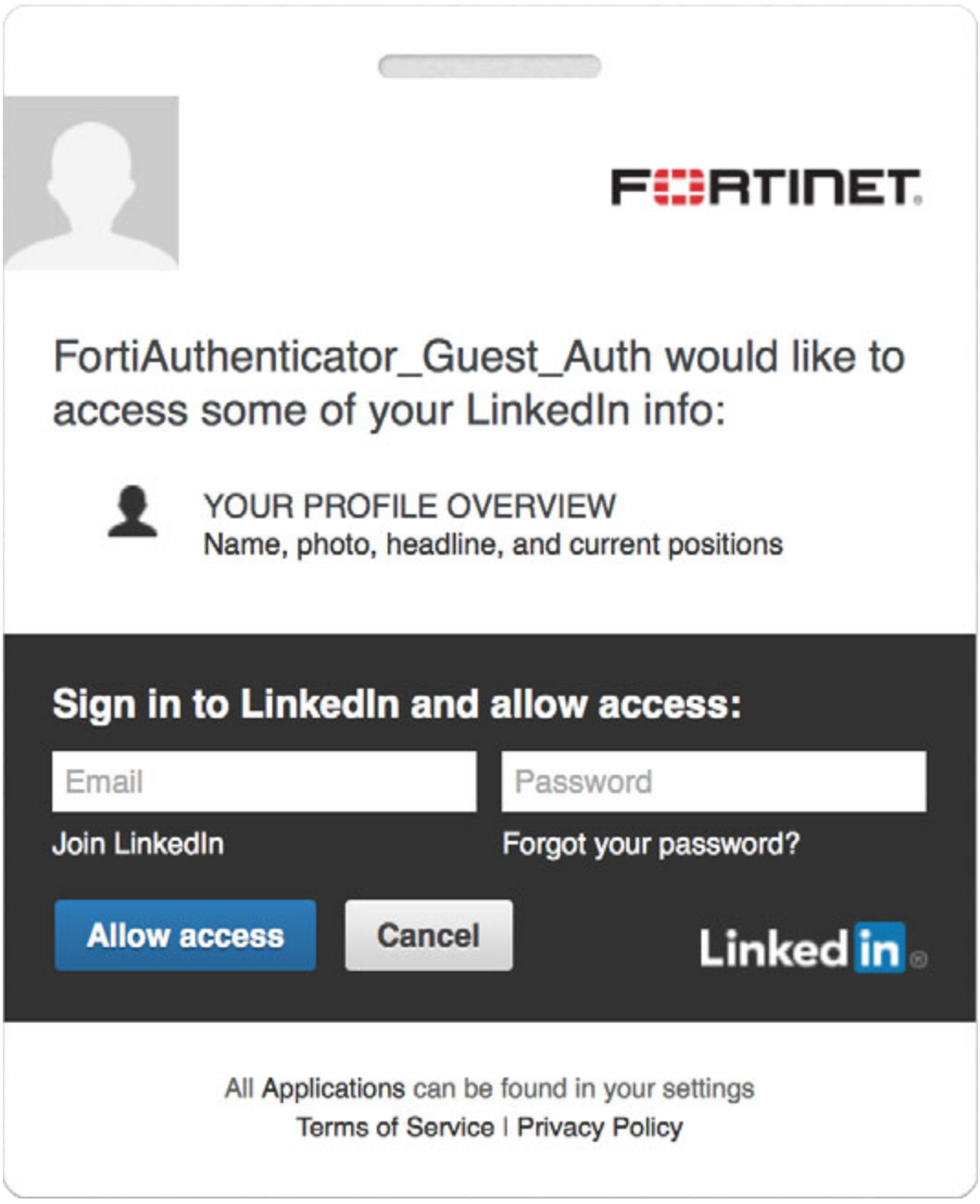
This command allows access to the external captive portal.

Results

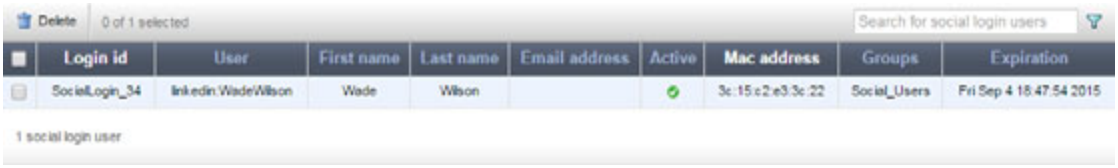
1. Connect to the WiFi and attempt to browse the Internet. You will be redirected to the captive portal splash page.
   Select **LinkedIn** and you should be redirected to the LinkedIn login page.



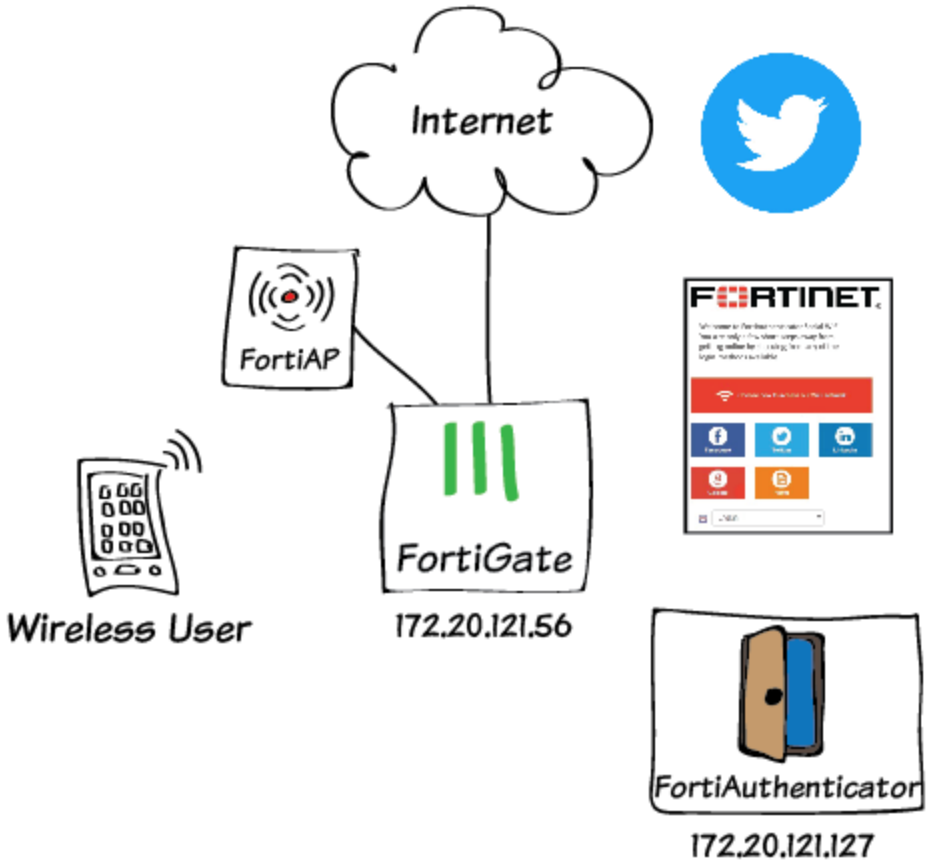
2. Enter valid LinkedIn credentials and you will be redirected to the URL initially requested.
You can now browse freely until the social login account expires, as configured on the FortiAuthenticator under **Authentication > Captive Portal > General**.



3. To view the authenticated user added on FortiAuthenticator, go to **Authentication > User Management > Social Login Users**.



Social WiFi captive portal with FortiAuthenticator (Twitter)



This recipe involves configuring an API for Twitter accounts, setting up a social portal RADIUS service on the FortiAuthenticator, and configuring the FortiGate for captive portal access.

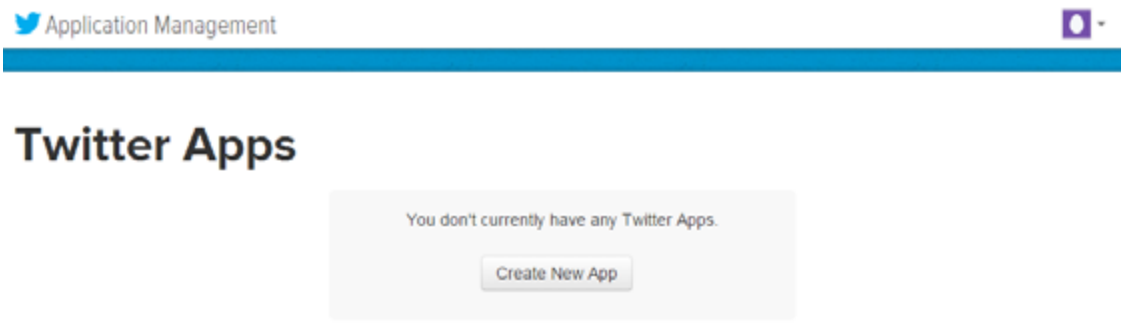
This recipe does not include FortiAP registration instructions.

Note that some CLI usage is required when configuring the FortiGate.

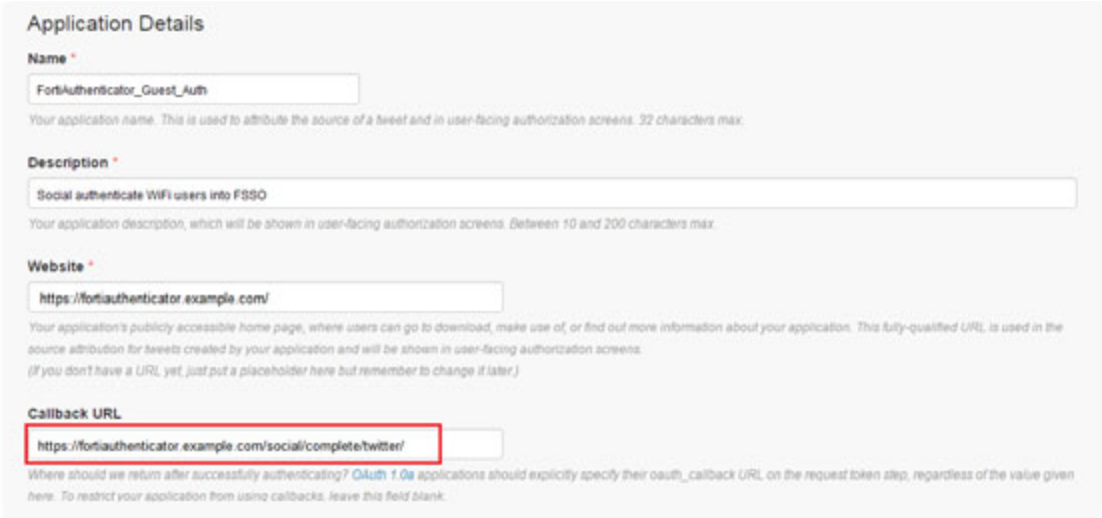
The FortiAuthenticator has been given an example fully qualified domain name (FQDN) -- *fortiauthenticator.example.com*.

Configuring the Twitter developer account API

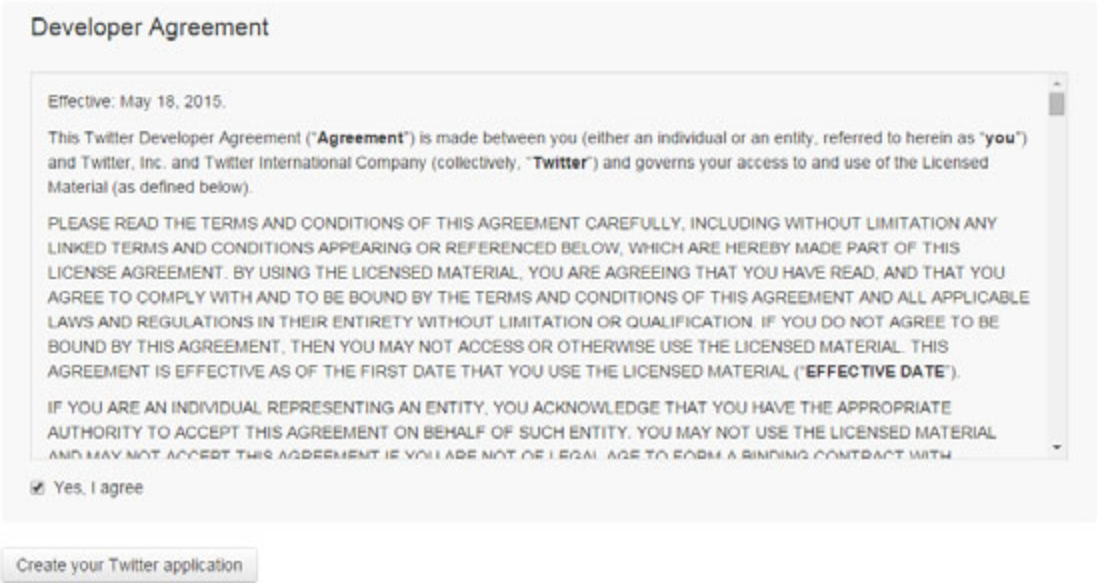
1. Open a browser and log in to your Twitter account.
   Navigate to the following URL:
   https://apps.twitter.com
   Select **Create New App**.



2. Enter a **Name**, **Description**, and **Website** for the application.
   In the Callback URL field, enter the following:
   https://fortiauthenticator.example.com/social/complete/twitter/
   Note that the FortiAuthenticator needs to be able to access the Internet.



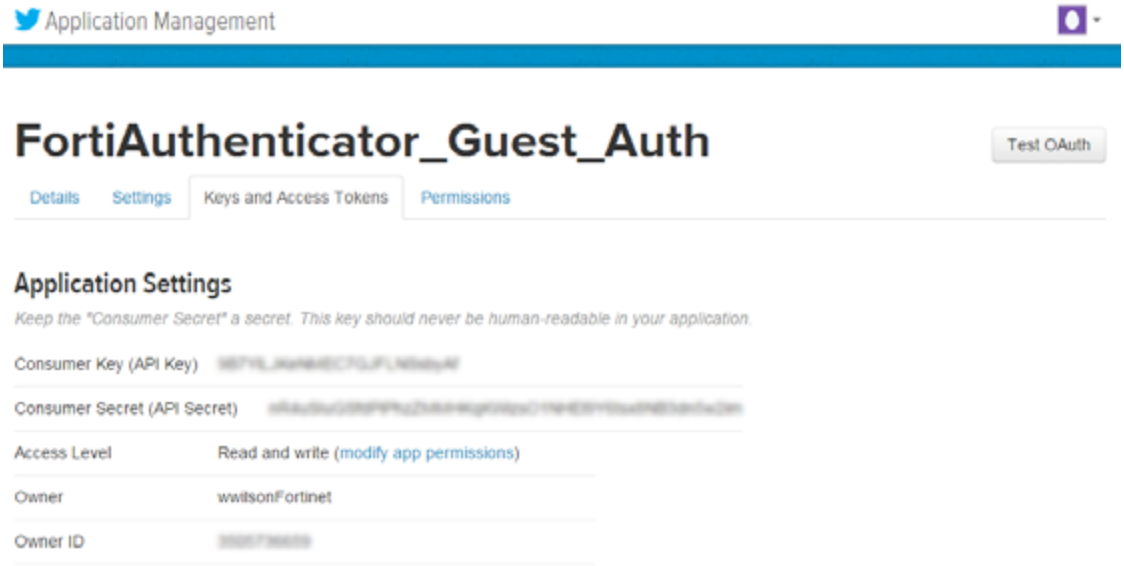
3. Accept the **Developer Agreement** and select **Create Twitter application**.



4. Go to **Keys and Access Tokens** to view your **Consumer Key** and **Consumer Secret**.

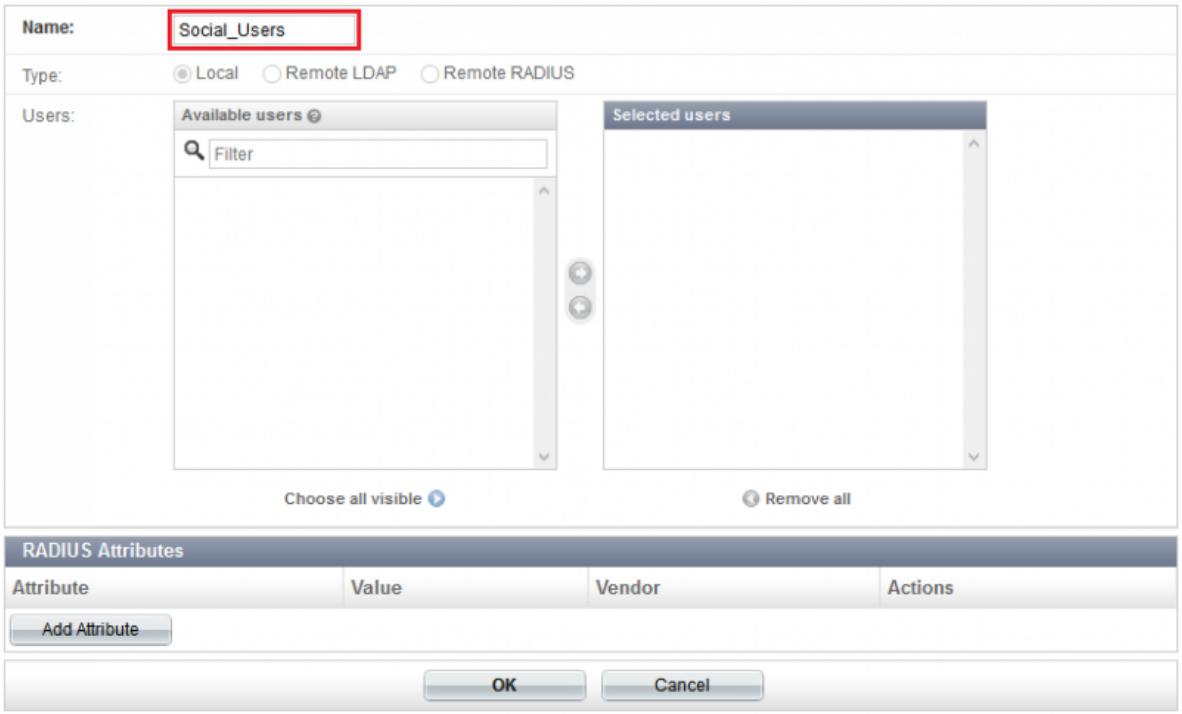
Take note of the **Consumer Key** and **Consumer Secret** as they are required when configuring the captive portal on the FortiAuthenticator.

The **Consumer Key** and **Consumer Secret** can be accessed at any time on the Twitter developer account, but it may be a good idea to copy them to a secure location.

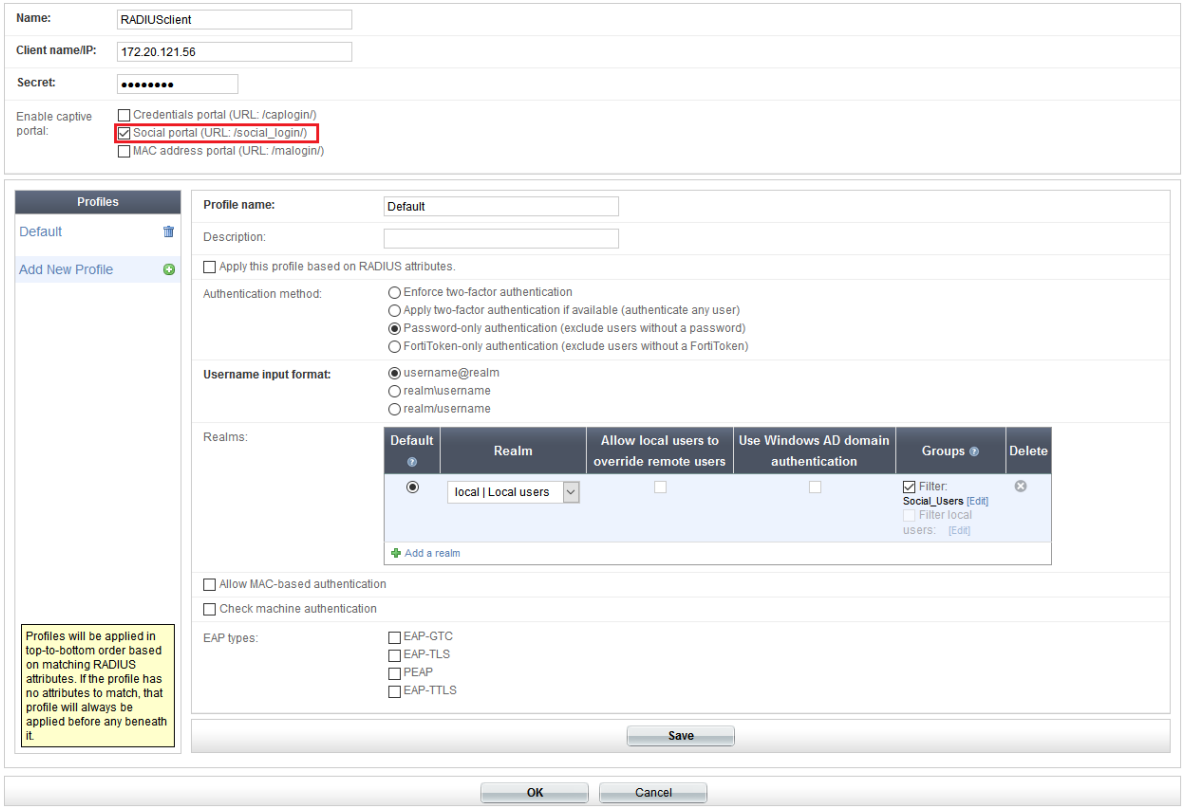


Configuring the social portal RADIUS service on the FortiAuthenticator

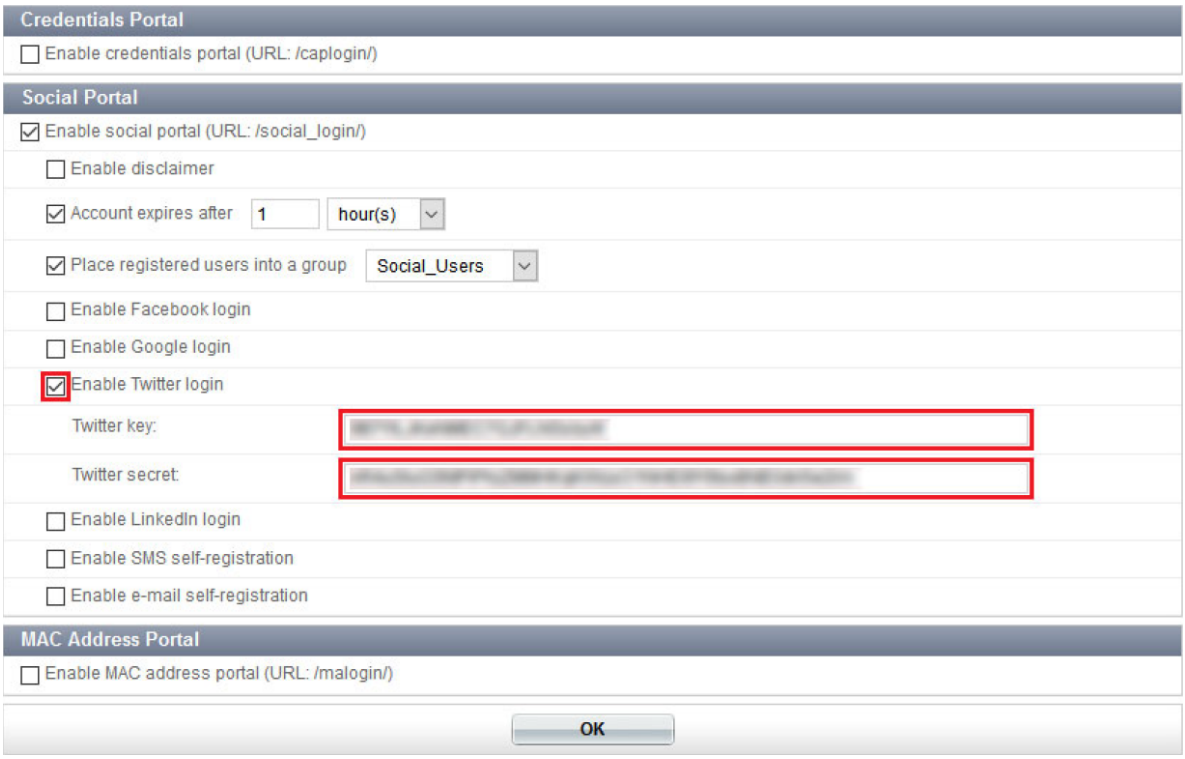
1. Go to **Authentication > User Management > User Groups** and create a **Social_Users** user group. Users that log in through the forms-based authentication method will be placed in this group once it is added to the captive portal general settings.



2. Go to **Authentication > RADIUS Service > Clients** and create a new RADIUS client.
   Enter a **Name** for the RADIUS client (the FortiGate) and enter its IP address (in the example, *172.20.121.56*).
   Enable the **Social portal** captive portal.
   Enter the pre-shared **Secret** and set the **Authentication method**. The FortiGate will use this secret key in its RADIUS configuration.
   Add the **Social_Users** user group to the **Realms** group filter as shown.
   Select **Save** and then **OK**.

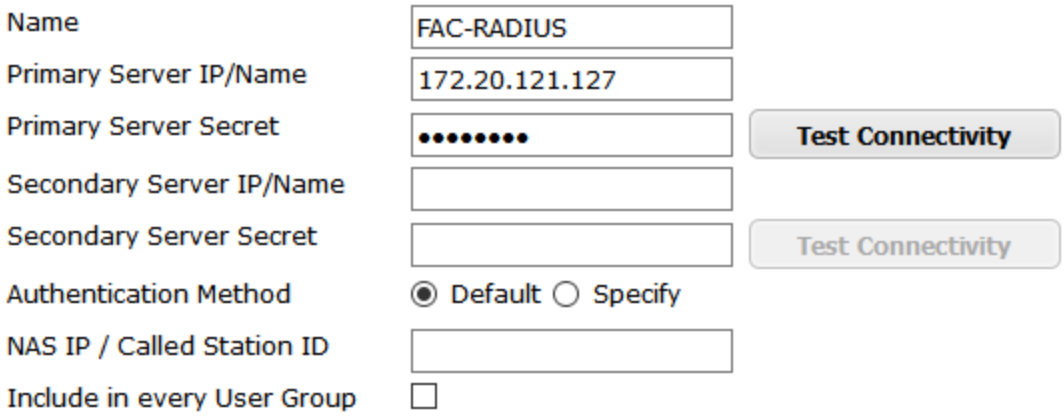


3. Next go to **Authentication > Captive Portal > General** and enable **Social Portal**.
   Configure the account expiry time (in the example, **1 hour**).
   Set **Place registered users into a group** to **Social_Users**.
   Enable the **Twitter** login option and add your **Twitter key** and **Twitter secret**.



Configuring the FortiGate authentication settings

1. On the FortiGate, go to **User & Device > RADIUS Servers** and create the connection to the FortiAuthenticator RADIUS server, using its IP and pre-shared secret.
   Use the **Test Connectivity** option with valid credentials to test the connection.

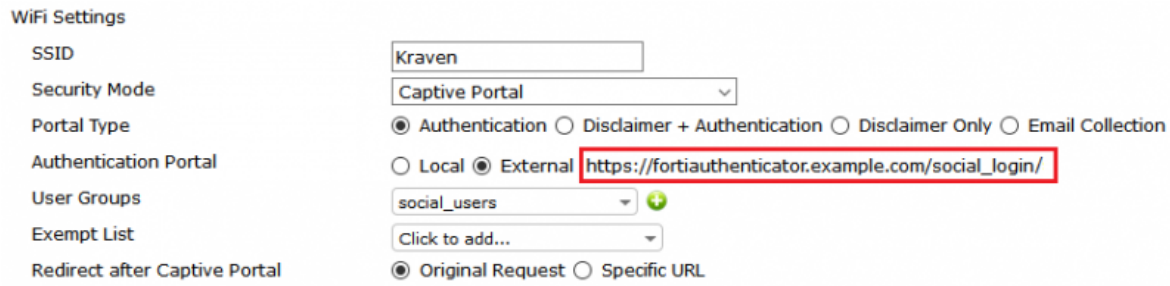


2. Next go to **User & Device > User Groups** and create a RADIUS user group.

Set **Type** to **Firewall** and add the RADIUS server to the **Remote groups** table.

Configuring the FortiGate WiFi settings

1. Go to **WiFi & Switch Controller > SSID** and select the SSID interface.
   Under **WiFi Settings**, set the **Security Mode** to **Captive Portal**.



2. For the **Authentication Portal**, select **External**, and enter the FQDN of the FortiAuthenticator, followed by **/social_login/**.
   For this recipe, it is set to `https://fortiauthenticator.example.com/social_login/`
   Set **User Groups** to the **social_users** group.

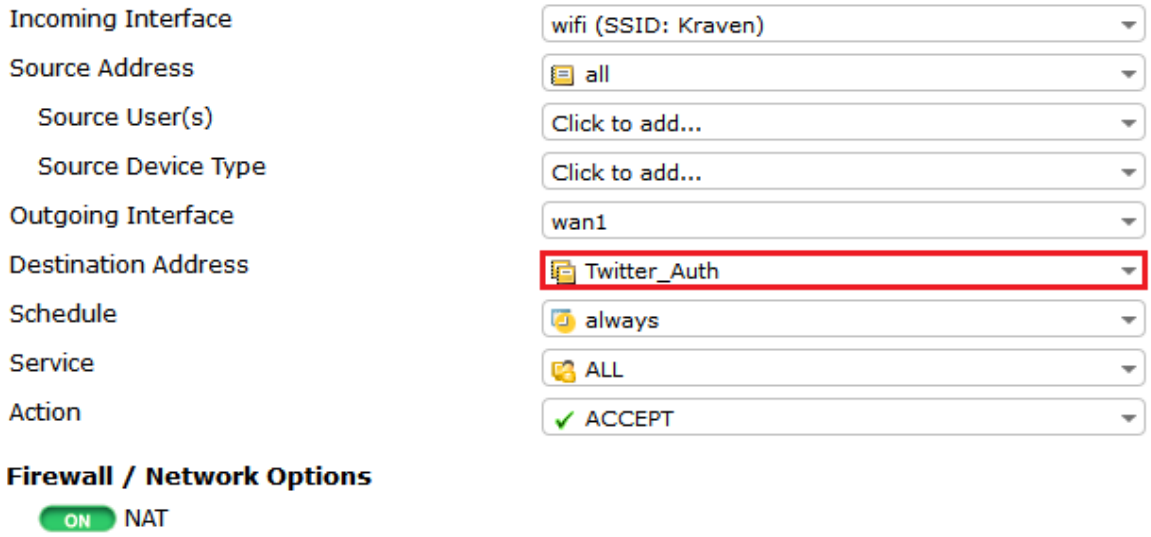
Configuring the FortiGate to allow access to Twitter

1. On the FortiGate, configure firewall addresses to allow users to access the Twitter login page.
   The following step can be performed in the GUI, but may take considerably longer than using the CLI. You can copy and paste the commands below.
   Open the **CLI Console** and enter the following, which creates the firewall addresses and adds them to a firewall address group called **Twitter_Auth**.

```
config firewall address
   edit "api.twitter.com"
      set type fqdn
      set fqdn "api.twitter.com"
   next
   edit "abs.twimg.com"
      set type fqdn
      set fqdn "abs.twimg.com"
   next
   edit "abs-0.twimg.com"
      set type fqdn
      set fqdn "abs-0.twimg.com"
   next
end
config firewall addrgrp
```

```
    edit "LinkedIn_Auth"
       set member "api.twitter.com" "abs.twimg.com" "abs-0.twimg.com"
    next
end
```

2. Go to **Policy & Objects > IPv4 Policy** and create a policy for Twitter authentication traffic.
   Set **Incoming Interface** to the WiFi SSID interface and set **Source Address** to **all**.
   Set **Outgoing Interface** to the Internet-facing interface and set **Destination Address** to **Twitter_Auth**.
   Set **Service** to **ALL** and enable **NAT**. Configure **Security Profiles** accordingly.



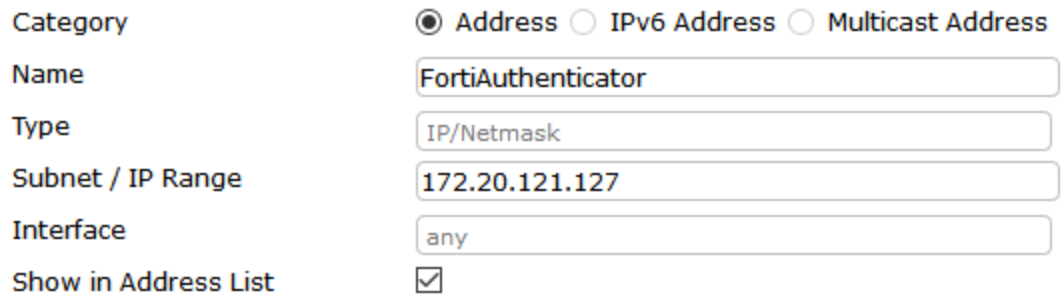
3. Then open the **CLI Console**. Using the policy's ID, enter the following command to exempt the Twitter authentication traffic policy from the captive portal:

```
config firewall policy
   edit <policy_id>
      set captive-portal-exempt enable
   next
end
```

   This command allows access to the external captive portal.

Configuring the FortiGate to allow access to the FortiAuthenticator

1. On the FortiGate, go to **Policy & Objects > Addresses** and add the FortiAuthenticator firewall object.
   For **Subnet/IP Range** enter the IP address of the FortiAuthenticator.

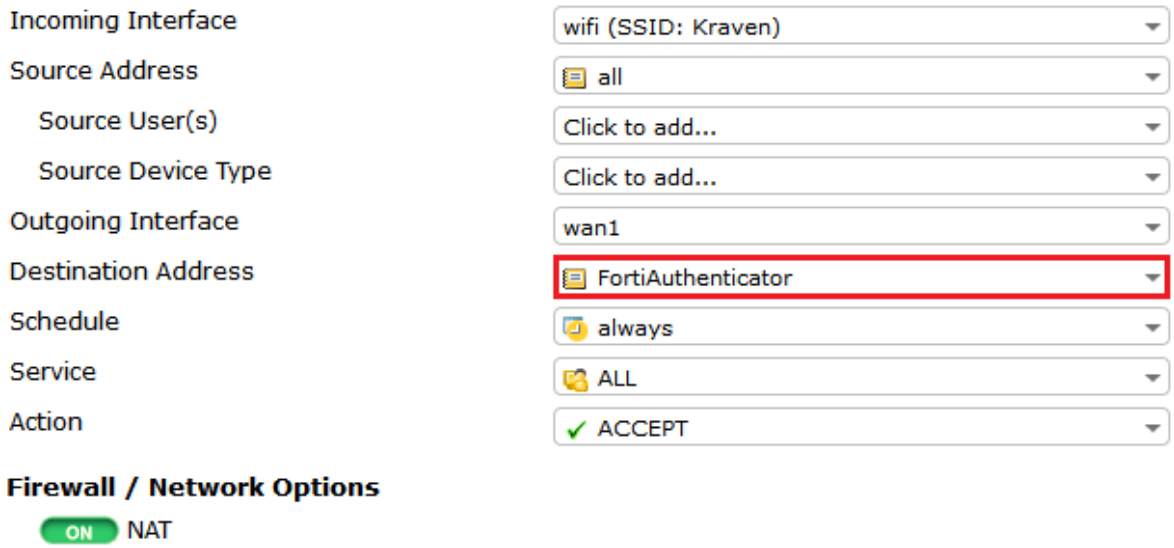


2. Go to **Policy & Objects > IPv4 Policy** and create the FortiAuthenticator access policy.
   Set **Incoming Interface** to the WiFi SSID interface and set **Source Address** to **all**.

Set **Outgoing Interface** to the Internet-facing interface and set **Destination Address** to the **FortiAuthenticator** address object.

Set **Service** to **ALL** and enable **NAT**.

Once created, note the policy's ID using the **ID** column.



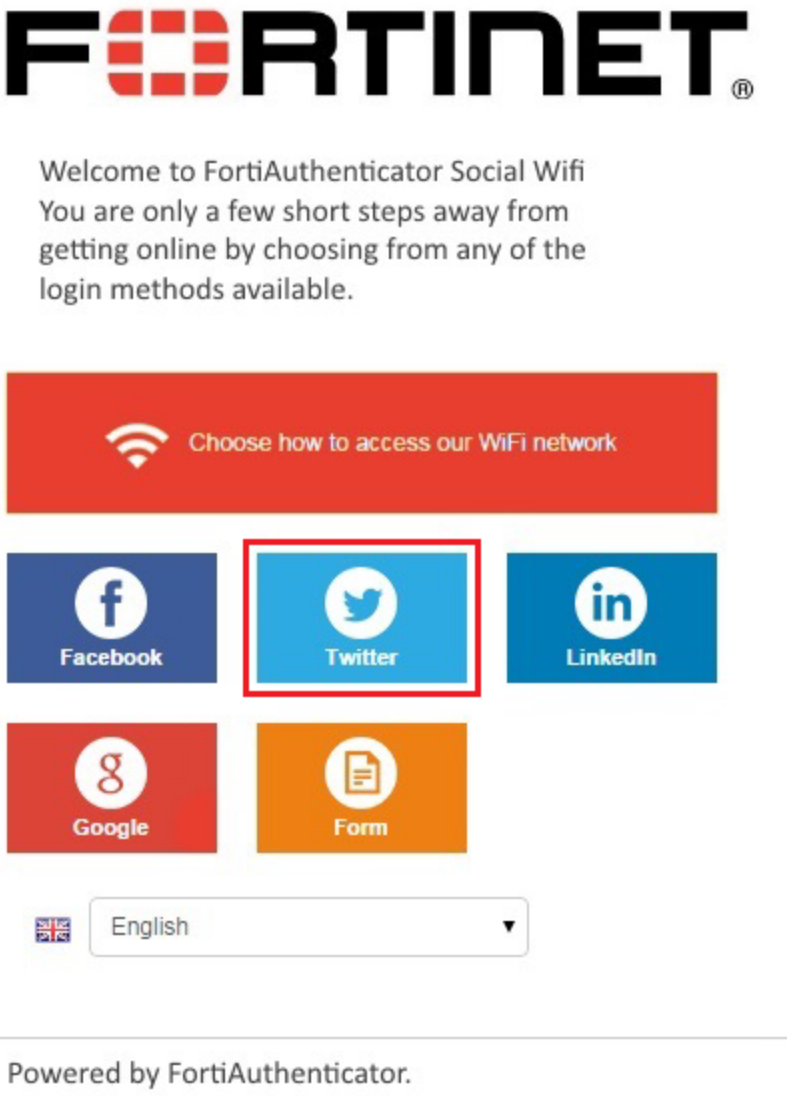
3. Open the **CLI Console** and enter the following command to exempt the FortiAuthenticator access policy from the captive portal:

```
config firewall policy
   edit <policy_id>
      set captive-portal-exempt enable
   next
end
```

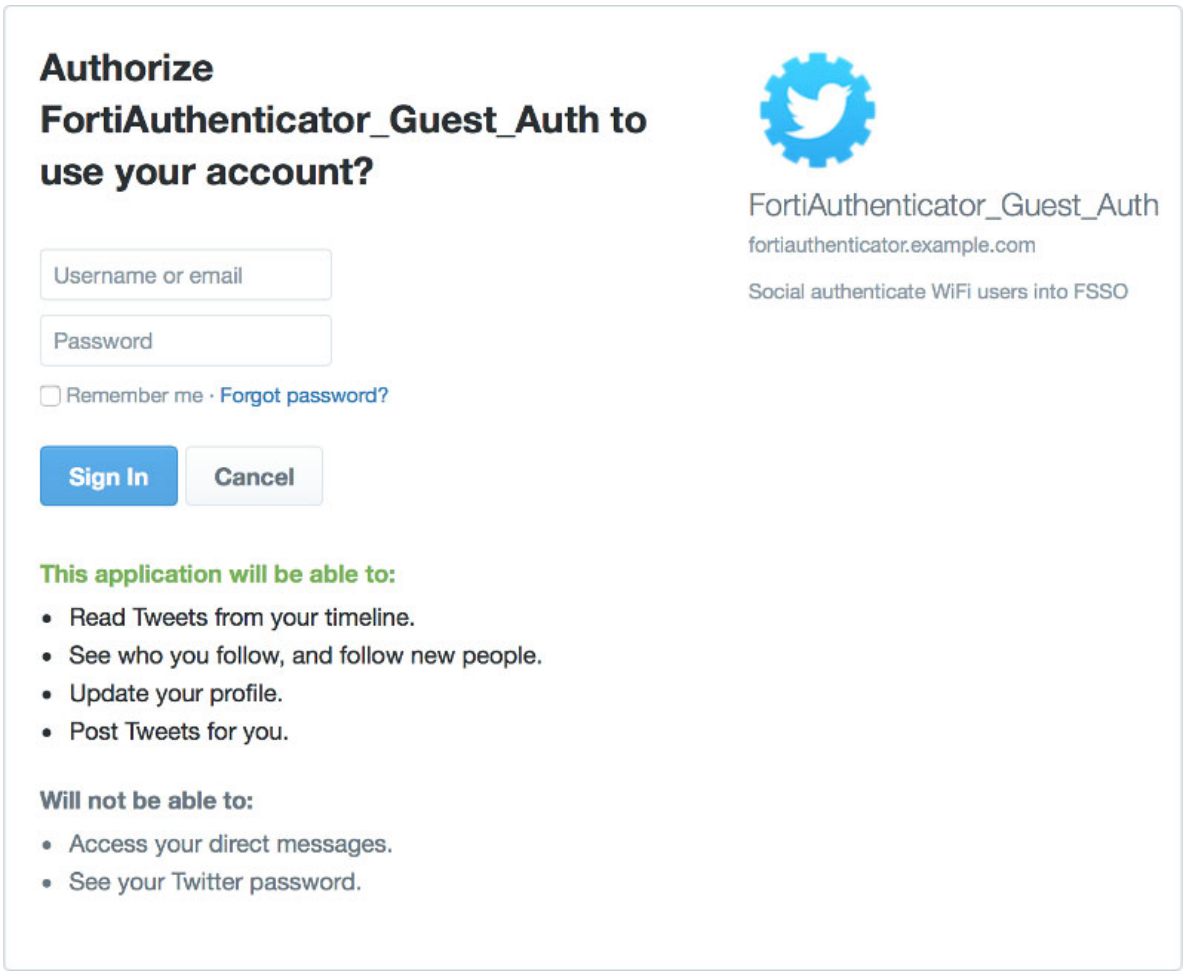
This command allows access to the external captive portal.

Results

1. Connect to the WiFi and attempt to browse the Internet. You will be redirected to the captive portal splash page.
   Select **Twitter** and you should be redirected to the LinkedIn login page.



2. Enter valid Twitter credentials and you will be redirected to the URL initially requested.
   You can now browse freely until the social login account expires, as configured on the FortiAuthenticator under **Authentication > Captive Portal > General**.



3. To view the authenticated user added on FortiAuthenticator, go to **Authentication > User Management > Social Login Users**.