



# 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](mailto:techdoc@fortinet.com)



August 1, 2019

FortiAuthenticator 5.5.0 Cookbook

23-550-570173-20190801

# TABLE OF CONTENTS

<b>Change log</b>	<b>6</b>
<b>EAP-TLS authentication</b>	<b>7</b>
Wired 802.1x EAP-TLS with computer authentication	7
Active Directory prerequisites	7
Configuring the certificates	8
Manually importing the client certificate - Windows 10	9
Configuring the FortiAuthenticator AD server	10
Configuring the user group	11
Configuring remote user sync rules	11
Configuring the FortiAuthenticator RADIUS client	12
Configuring the switch	13
Results	13
Wireless 802.1x EAP-TLS with computer authentication	17
Active Directory prerequisites	17
Configuring the certificates	18
Manually importing the client certificate - Windows 10	19
Configuring the Intel PROSet Supplicant - Windows 10	20
Configuring the FortiAuthenticator AD server	22
Configuring the user group	23
Configuring remote user sync rules	23
Configuring the FortiAuthenticator RADIUS client	25
Configuring the FortiWiFi	25
Results	27
Wireless 802.1x EAP-TLS with user authentication	30
Configuring the certificates	30
Manually importing the client certificate - Windows 10	31
Configuring the FortiAuthenticator AD server	32
Configuring the user group	33
Configuring remote user sync rules	33
Configuring the FortiAuthenticator RADIUS client	34
Configuring the FortiWiFi	35
Results	37
<b>FortiToken and FortiToken Mobile</b>	<b>41</b>
FortiToken Mobile Push for SSL VPN	41
Adding a FortiToken to the FortiAuthenticator	42
Adding the user to the FortiAuthenticator	42
Creating the RADIUS client on the FortiAuthenticator	45
Connecting the FortiGate to the RADIUS server	45
Configuring the SSL VPN	48
Results	50
<b>Guest Portals</b>	<b>54</b>
FortiAuthenticator as Guest Portal for FortiWLC	54
Creating the FortiAuthenticator as RADIUS server on the FortiWLC	54
Creating the Captive Portal profile on the FortiWLC	55
Creating the security profile on the FortiWLC	56

Creating the QoS rule on the FortiWLC .....	56
Creating the ESS Profile on the FortiWLC .....	57
Creating FortiWLC as RADIUS Client on the FortiAuthenticator .....	58
Creating the Guest Portal on the FortiAuthenticator .....	59
Creating the Portal Rule on the FortiAuthenticator .....	60
Results .....	61
<b>MAC authentication bypass .....</b>	<b>62</b>
MAC authentication bypass with dynamic VLAN assignment .....	62
Configuring MAC authentication bypass on the FortiAuthenticator .....	62
Configuring the user group .....	62
Configuring the RADIUS client .....	63
Configuring the 3rd-party switch .....	64
Results .....	65
<b>SAML authentication .....</b>	<b>68</b>
SAML 2.0 FSSO with FortiAuthenticator and Centrify .....	68
Configuring DNS and FortiAuthenticator's FQDN .....	68
Enabling FSSO and SAML on the FortiAuthenticator .....	69
Adding SAML connector to Centrify for IdP metadata .....	72
Importing the IdP certificate and metadata on the FortiAuthenticator .....	74
Uploading the SP metadata to the Centrify tenant .....	76
Configuring FSSO on the FortiGate .....	77
Configuring captive portal and security policies .....	78
Results .....	83
SAML 2.0 FSSO with FortiAuthenticator and Google G Suite .....	85
Configuring FSSO and SAML on the FortiAuthenticator .....	86
Configuring SAML on G Suite .....	88
Importing the IdP certificate and metadata on the FortiAuthenticator .....	95
Configuring FSSO on the FortiGate .....	97
Configuring Captive Portal and security policies .....	98
Results .....	103
SAML 2.0 FSSO with FortiAuthenticator and Okta .....	105
Configuring DNS and FortiAuthenticator's FQDN .....	106
Enabling FSSO and SAML on the FortiAuthenticator .....	107
Configuring the Okta developer account IDP application .....	109
Importing the IDP certificate and metadata on the FortiAuthenticator .....	116
Configuring FSSO on the FortiGate .....	117
Configuring Captive Portal and security policies .....	118
Results .....	123
<b>Self-service Portal .....</b>	<b>126</b>
FortiAuthenticator user self-registration .....	126
Creating a self-registration user group .....	126
Enabling self-registration .....	127
Creating a new SMTP server .....	129
Results - Self-registration .....	129
Results - Administrator approval .....	131
<b>VPNs .....</b>	<b>134</b>
SSL VPN with RADIUS and FortiToken .....	134



---

Creating a user and a user group .....	134
Creating the RADIUS client .....	136
Connecting the FortiGate to FortiAuthenticator .....	137
Allowing users to connect to the VPN .....	139
Results .....	140
<b>Legacy .....</b>	<b>142</b>
Social WiFi captive portal .....	142
Social WiFi captive portal with FortiAuthenticator (Facebook) .....	143
Social WiFi captive portal with FortiAuthenticator (Form-based) .....	159
Social WiFi captive portal with FortiAuthenticator (Google+) .....	167
Social WiFi captive portal with FortiAuthenticator (LinkedIn) .....	178
Social WiFi captive portal with FortiAuthenticator (Twitter) .....	191

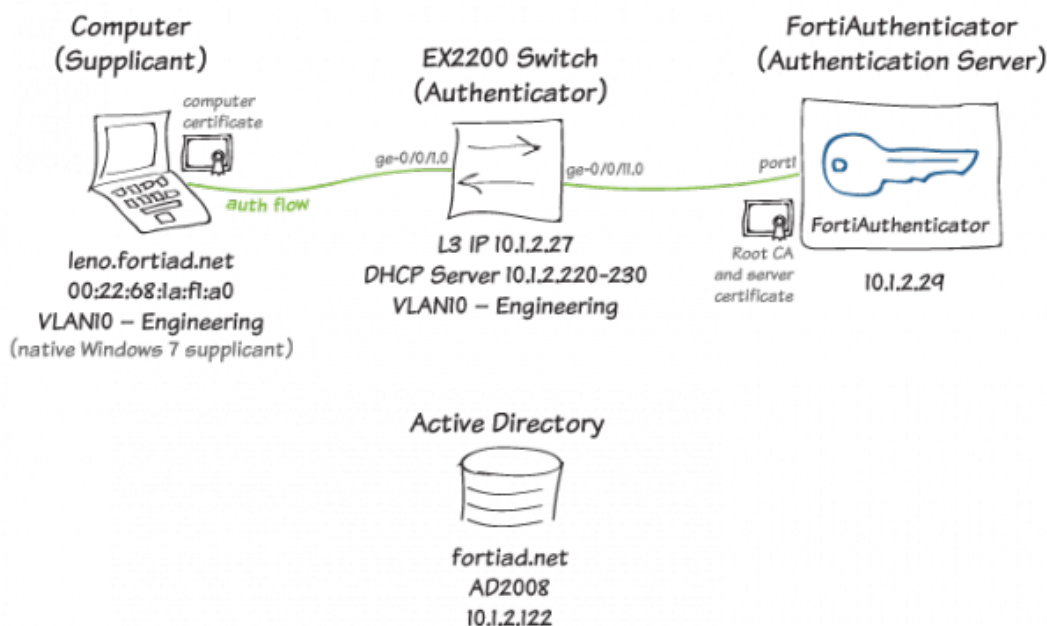
## Change log

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.

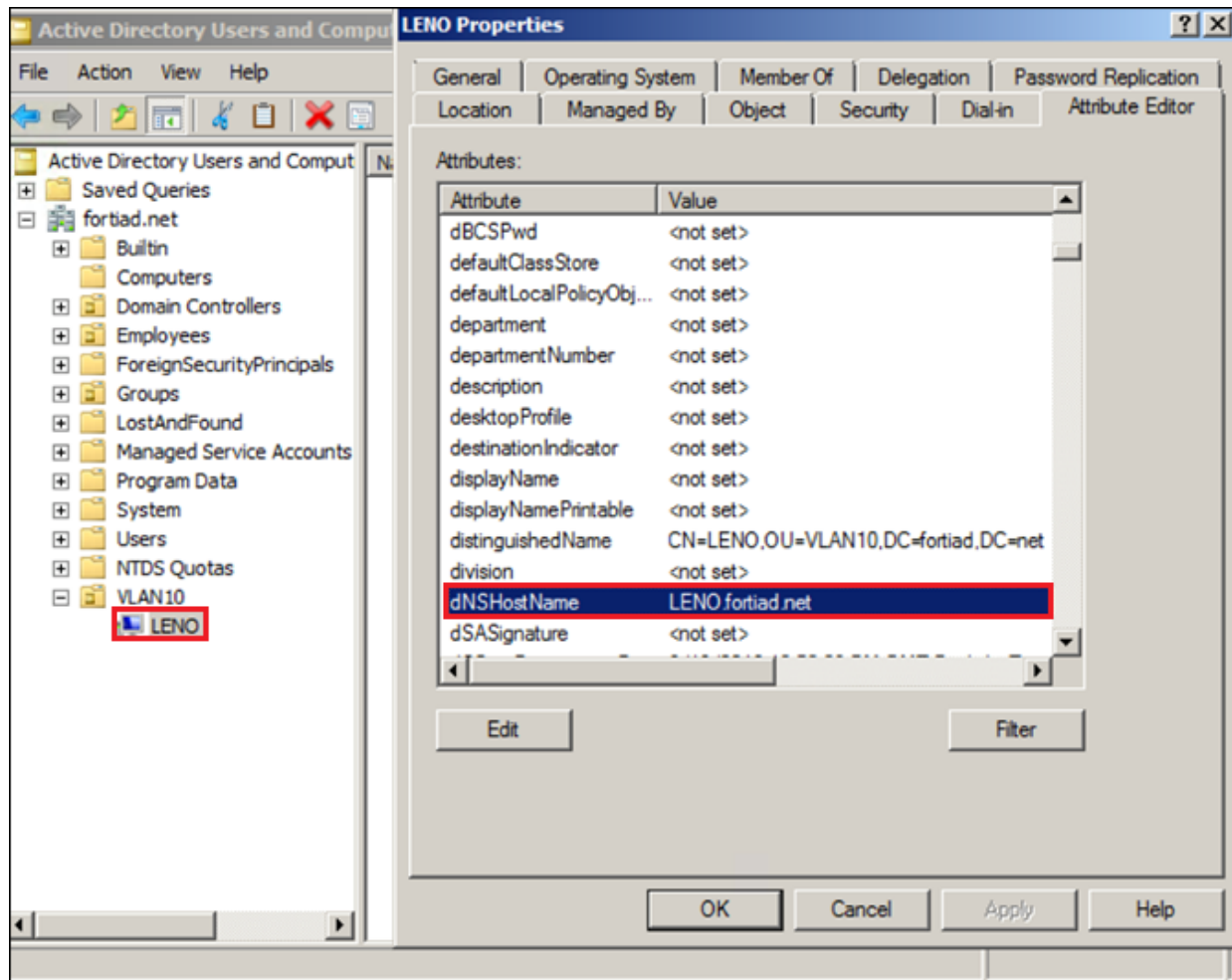
In the example, you will set up FortiAuthenticator as the Root CA and client certificate issuer. The FortiAuthenticator will authenticate user interaction using the domain computer and client certificate (no username or password).

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

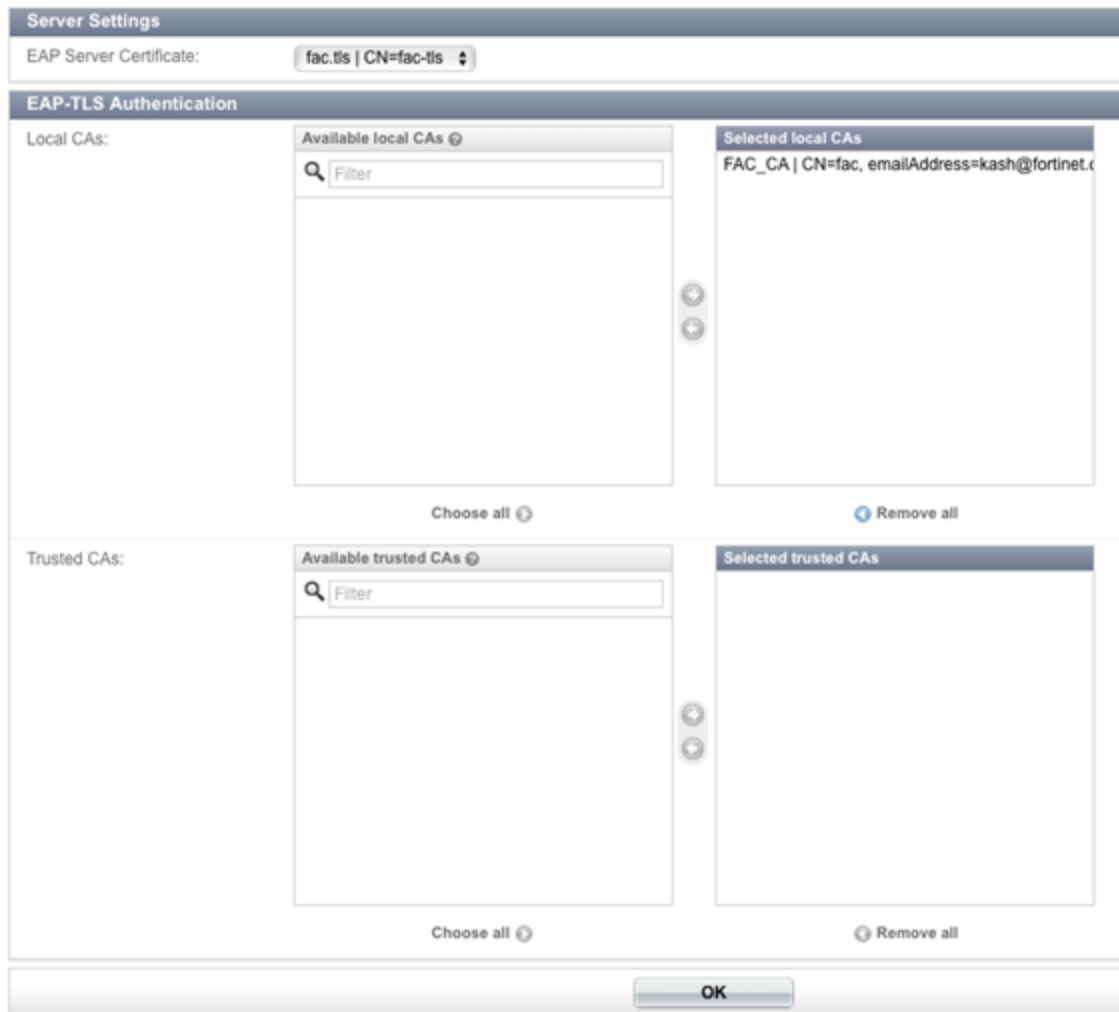
1. On the FortiAuthenticator, go to **Certificate Management > Certificate Authorities > Local CAs** and create a new root CA.

<input type="checkbox"/>	Certificate ID	Subject	Issuer	Status	CA Type
<input type="checkbox"/>	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.

<input type="checkbox"/>	Certificate ID	Subject	Issuer	Status
<input type="checkbox"/>	Firmware_Default	C=US, ST=California, L=Sunnyvale, O=Fortinet, OU=FortiAuth...	Remote CA: C=US, ST=California, L=Sunnyvale, O=Fortinet, OU=C...	Active
<input type="checkbox"/>	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.



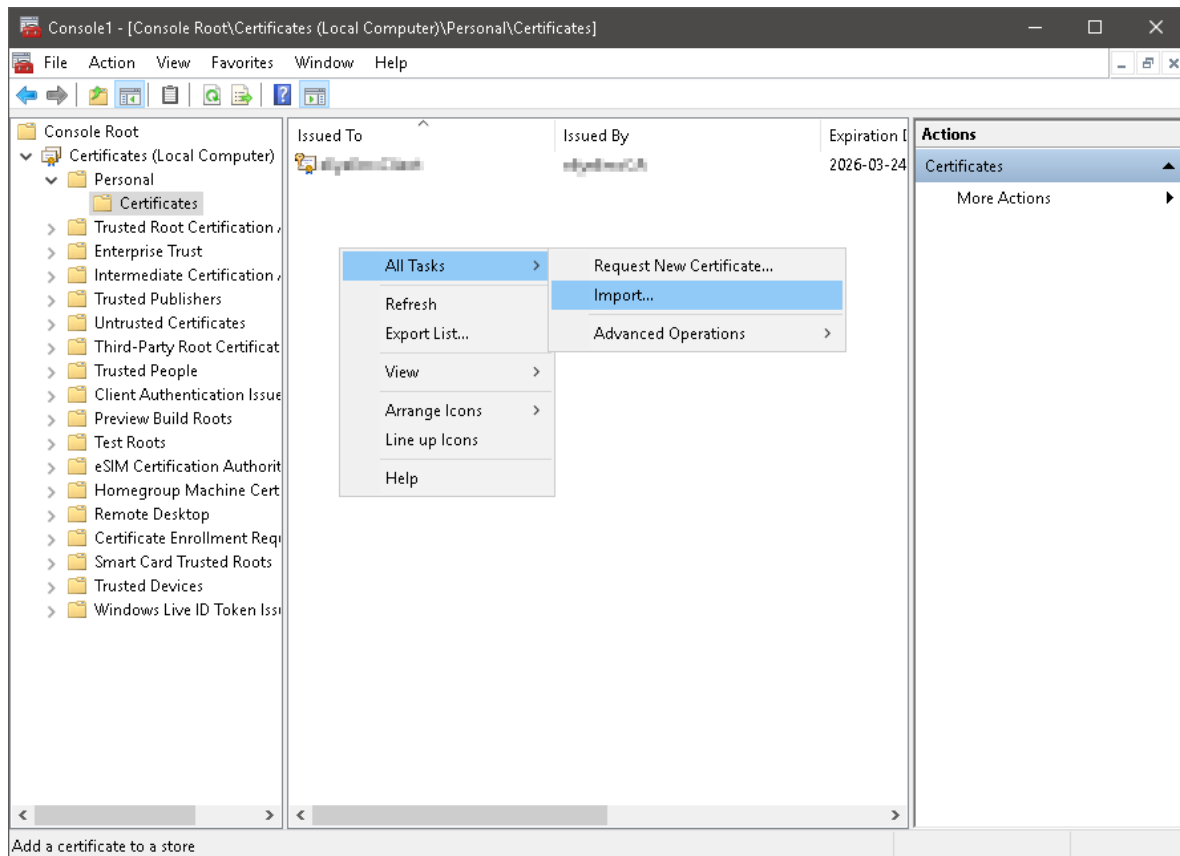
- Go to **Certificate Management > End Entities > Users** and create a client certificate. The CN must match the full DNS name of the intended computer. Select **Export Key and Cert** (with a **Passphrase** to protect it) and download the PKCS#12 file.

<a href="#">Create New</a> <a href="#">Import</a> <a href="#">Revoke</a> <a href="#">Delete</a> <a href="#">Export Certificate</a> <a href="#">Export PKCS#12</a> <span>1 of 5 selected (149995 of 150000 entries remaining)</span> <input type="text" value="Search for user certificates"/>				
<input type="checkbox"/>	Certificate ID	Subject	Issuer	Status
<input type="checkbox"/>	kash.fortiad.net	CN=kash	CN=fac, emailAddress=kash@fortinet.com	Active
<input checked="" type="checkbox"/>	leno.fortiad.net	CN=leno.fortiad.net	CN=fac, emailAddress=kash@fortinet.com	Active

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

- 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.

Name:	AD-2008-10.1.2.122		
Primary server name/IP:	10.1.2.122	Port:	389
<input type="checkbox"/> Use secondary server			
Base distinguished name:	dc=fortiad,dc=net		
Bind type:	<input type="radio"/> Simple <input checked="" type="radio"/> Regular		
Username:	cn=administrator,cn=users,dc=fortiad,dc=net	Password:	*****
User object class:	person		
Username attribute:	dNSHostName		
Group object class:	group		
Group membership attribute:	memberOf	<input type="checkbox"/> Attribute is group attribute	

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

**Name:**

**User source:** AD-2008-10.1.2.122 (10.1.2.122) ▾

## 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.

**Name:**

**Type:** ☐ Local ☒ Remote LDAP ☐ Remote RADIUS

**User retrieval:** ☐ Specify an LDAP filter ☒ Set a list of imported remote LDAP users

**Remote LDAP:** AD-2008-10.1.2.122 (10.1.2.122) ▾

**LDAP users:**

**Available LDAP users**

**Selected LDAP users**

☐ Allow token self-provisioning

RADIUS Attributes			
Attribute	Value	Vendor	Actions
Tunnel-Private-Group-Id	engineering	Default	
Tunnel-Medium-Type	IEEE-802 (6)	Default	
Tunnel-Type	VLAN (13)	Default	

## Configuring remote user sync rules

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

**Name:**

**Remote LDAP:**

**Sync every:**

**Base distinguished name:**

**LDAP filter:**

**Token-based authentication sync priorities:**

- ☒ None (users are synced explicitly with no token-based authentication)
- ☐ FortiToken 200 (assign if serial number is provided)
- ☐ FortiToken 200 (assign an available token)
- ☐ Email
- ☐ SMS
- ☐ FortiToken Mobile (assign an available token)

**Sync as:** ☒ Remote LDAP User ☐ Local User

**Group to associate users with:**

**Organization:**

**Debugging Settings**

**LDAP User Mapping Attributes**

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

**Remote LDAP server:** AD-2008-10.1.2.122 (10.1.2.122)

**Username:** leno.fortiad.net

**Distinguished name:** CN=LENO,OU=VLAN10,DC=fortiad,DC=net

☐ Disabled

☐ Token-based authentication

☒ Allow RADIUS authentication

**User Role**

**Role:** ☐ Administrator ☒ User

**User Information**

**RADIUS Attributes**

**Certificate Bindings**

Common Name	Issuer	Status	Actions
leno.fortiad.net	CN=fac, emailAddress=kash@fortinet.com	Active	

## Configuring the FortiAuthenticator RADIUS client

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



Name:


Client name/IP:


Secret:

Enable captive portal: ☐ Credentials portal (URL: /caplogin/)  
☐ Social portal (URL: /social\_login/)  
☐ MAC address portal (URL: /maclogin/)

---

**Profiles**

Default 

[Add New Profile](#) 

**Profile name:**

**Description:**

☐ Apply this profile based on RADIUS attributes.

**Authentication method:**

☐ Enforce two-factor authentication

☒ Apply two-factor authentication if available (authenticate any user)

☐ Password-only authentication (exclude users without a password)

☐ FortiToken-only authentication (exclude users without a FortiToken)





**Username input format:**

☐ username@realm

☐ realm/username

☒ realm/username

**Realms:**

Default	Realm	Allow local users to override remote users	Use Windows AD domain authentication	Groups	Delete
	host   AD-2008-10.1.2.122 (10.1.2.122)	<input type="checkbox"/>	<input type="checkbox"/>	 Filter: VLAN10 <a href="#">[Edit]</a> Filter local users: <a href="#">[Edit]</a>	
<a href="#">Add a realm</a> 					

☐ Allow MAC-based authentication

☐ Check machine authentication

**EAP types:**

☐ EAP-GTC

☒ EAP-TLS

☐ PEAP

☐ EAP-TTLS

## 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 13-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 3bb1
    0x0010: 1908 2978 2030
Message-Authenticator Attribute (80), length: 18, Value: .#....:&%N.z.7...
    0x0000: dc23 d299 0f3a 2625 4eed 7a9c 37d9 ef97
State Attribute (24), length: 18, Value: ..... ..m.q.
    0x0000: c21b 819c c21a 85b8 20c3 b2b7 6d1a 71d6
```

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

```
02:18:48.919099 IP (tos 0x0, 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 -> 0xae5a!] 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: fclf 1ae2 b9e3 00a7 lec9 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 0x0, 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 0xf79d54fa, Flags [Broadcast] (0x8000)
  Your-IP 10.1.2.224
  Client-Ethernet-Address 00:22:68:1a:f1: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 dot1x 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
```

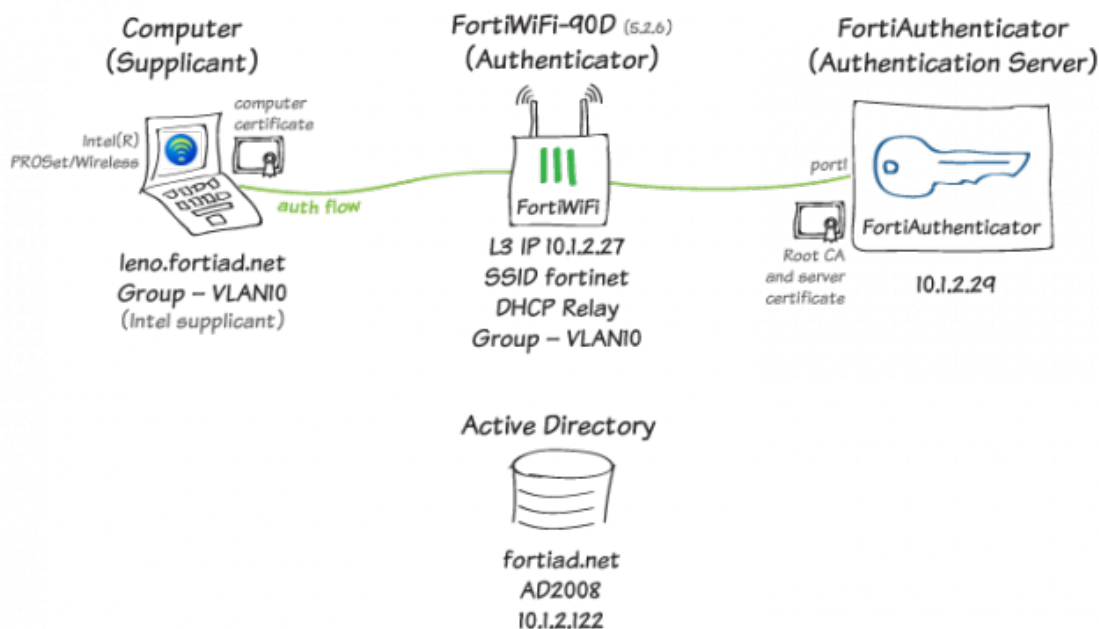
```

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.

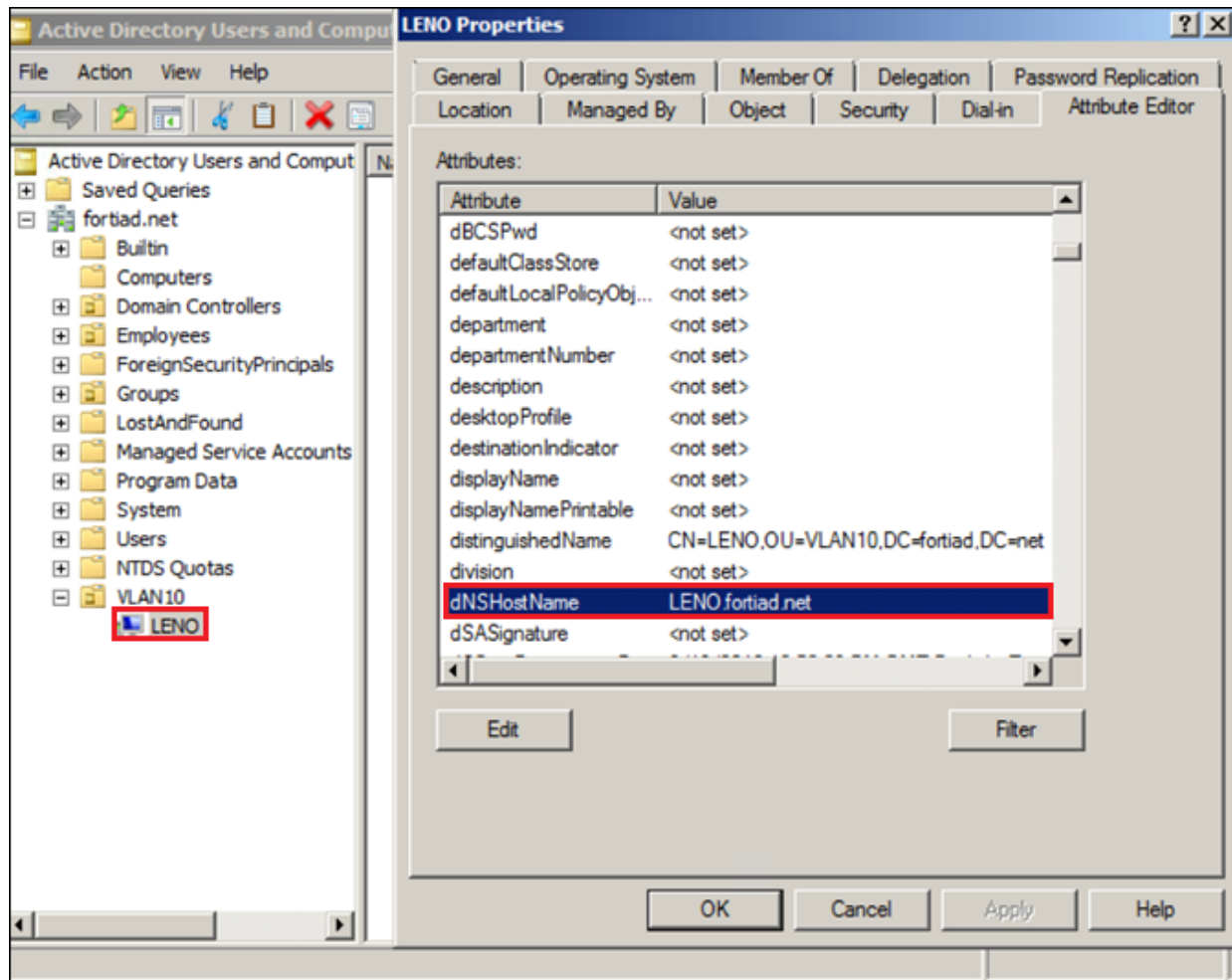
In the example, you will set up FortiAuthenticator as the Root CA and client certificate issuer. The FortiAuthenticator will authenticate without user interaction using the domain computer and client certificate (no username or password).

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

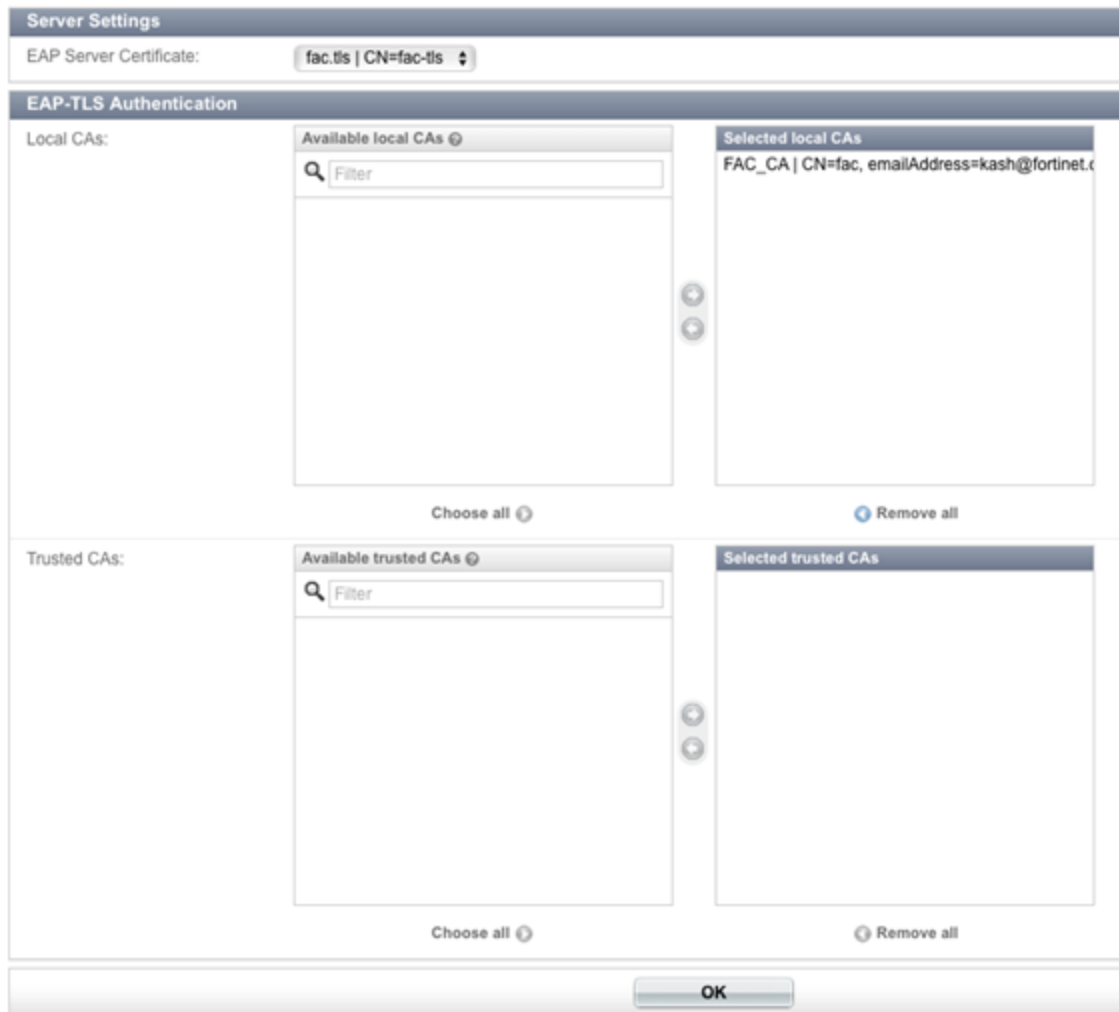
1. On the FortiAuthenticator, go to **Certificate Management > Certificate Authorities > Local CAs** and create a new root CA.

Certificate ID	Subject	Issuer	Status	CA Type
<input type="checkbox"/> 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
<input type="checkbox"/> Firmware_Default	C=US, ST=California, L=Sunnyvale, O=Fortinet, OU=FortiAuth...	Remote CA: C=US, ST=California, L=Sunnyvale, O=Fortinet, OU=C...	Active
<input type="checkbox"/> 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.



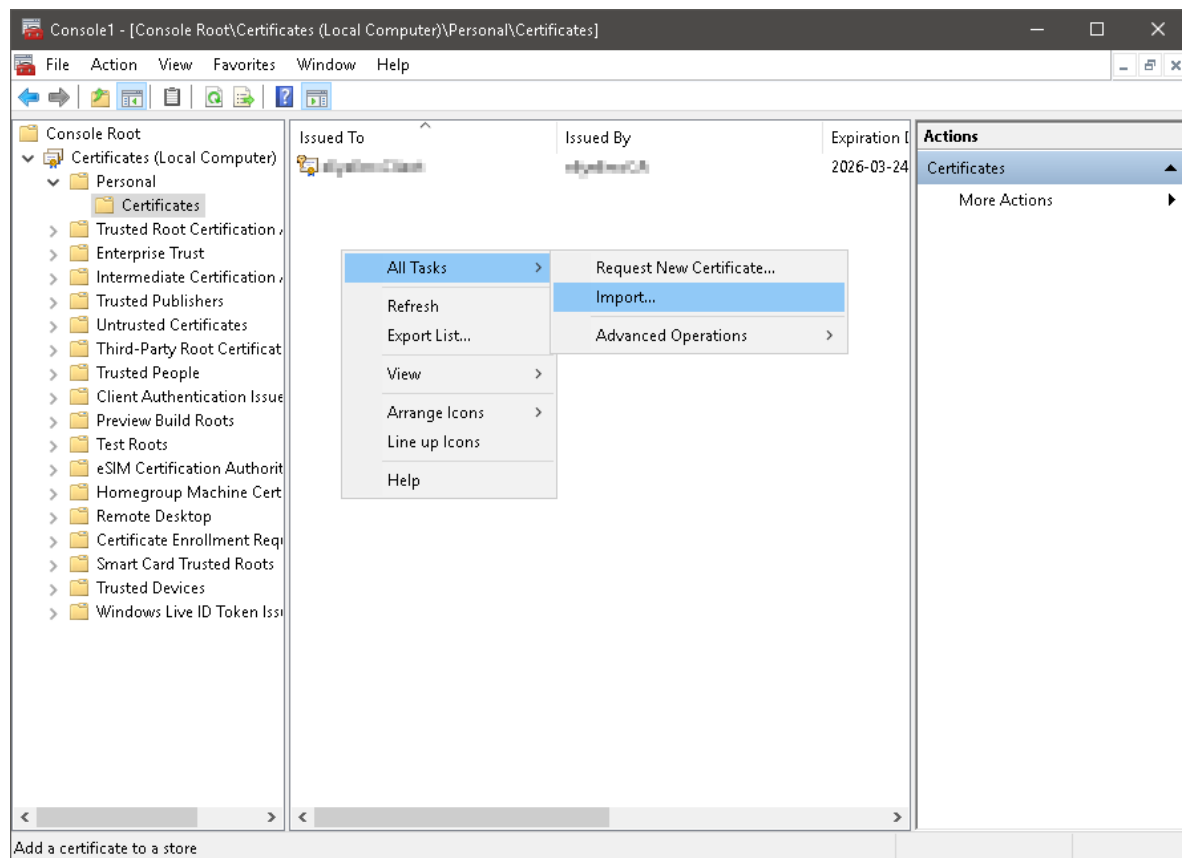
- Go to **Certificate Management > End Entities > Users** and create a client certificate. The CN must match the full DNS name of the intended computer. Select **Export Key and Cert** (with a **Passphrase** to protect it) and download the PKCS#12 file.

<a href="#">Create New</a> <a href="#">Import</a> <a href="#">Revoke</a> <a href="#">Delete</a> <a href="#">Export Certificate</a> <a href="#">Export PKCS#12</a> <span>1 of 5 selected (149995 of 150000 entries remaining)</span> <input type="text" value="Search for user certificates"/>				
<input type="checkbox"/>	Certificate ID	Subject	Issuer	Status
<input type="checkbox"/>	kash.fortiad.net	CN=kash	CN=fac, emailAddress=kash@fortinet.com	Active
<input checked="" type="checkbox"/>	leno.fortiad.net	CN=leno.fortiad.net	CN=fac, emailAddress=kash@fortinet.com	Active

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

- 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**.



The screenshot shows a 'General Settings' dialog box. On the left is a sidebar with a tree view containing 'Profile Name: fortinet', 'General Settings' (selected), and 'Security Settings'. The main area has a title bar 'General Settings'. Below it, 'Profile Name:' is set to 'fortinet' and 'WiFi Network Name (SSID):' is also set to 'fortinet'. A text block explains: 'The Profile Name is your name for the network. Example: Home or Office. The WiFi Network Name (SSID) is a unique identifier that differentiates one WiFi network from another.' Under 'Operating Mode:', the 'Network (Infrastructure) - Connect to WiFi networks and/or the Internet.' option is selected with a radio button. There is an unchecked checkbox for 'Connect even if the network is not broadcasting its name (SSID)'. At the bottom are buttons for 'Advanced...', 'Help?', '<< Back', 'Next >>', 'OK', and 'Cancel'.

Profile Name: fortinet

General Settings

Security Settings

General Settings

Profile Name: fortinet

WiFi Network Name (SSID): fortinet

The Profile Name is your name for the network. Example: Home or Office. The WiFi Network Name (SSID) is a unique identifier that differentiates one WiFi network from another.

Operating Mode:

☒ Network (Infrastructure) - Connect to WiFi networks and/or the Internet.

☐ Connect even if the network is not broadcasting its name (SSID)

Advanced... Help? << Back Next >> OK Cancel

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.

The screenshot shows the 'Security Settings' window for a profile named 'fortinet'. The 'Enterprise Security' radio button is selected. Under 'Network Authentication', 'WPA2 - Enterprise' is chosen. Under 'Data Encryption', 'AES - CCMP' is chosen. The 'Enable 802.1X' checkbox is checked. The 'Authentication Type' is set to 'TLS', with a 'Cisco Options...' button next to it. A sub-dialog titled 'Step 1 of 2: TLS User' is open, showing three radio button options: 'Use my smart card', 'Use the certificate issued to this computer' (which is selected and highlighted with a red box), and 'Use a user certificate on this computer'. Below these options, there is a 'Select...' button and a 'User Name' text field. At the bottom of the main window are buttons for 'Advanced...', 'Help?', '<< Back', 'Next >>', 'OK', and 'Cancel'.

## 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.

The screenshot shows the LDAP server configuration form. The 'Name' field contains 'AD-2008-10.1.2.122'. The 'Primary server name/IP' is '10.1.2.122' and the 'Port' is '389'. The 'Use secondary server' checkbox is unchecked. The 'Base distinguished name' is 'dc=fortiad,dc=net'. The 'Bind type' is set to 'Regular'. The 'Username' is 'cn=administrator,cn=users,dc=fortiad,dc=net' and the 'Password' is masked with dots. The 'User object class' is 'person'. The 'Username attribute' field, which is highlighted with a red box, contains 'dNSHostName'. The 'Group object class' is 'group'. The 'Group membership attribute' is 'memberOf'. There is an unchecked checkbox for 'Attribute is group attribute'.

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

**Name:**

---

**User source:** AD-2008-10.1.2.122 (10.1.2.122) 

## 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.


**Name:**

**Type:** ☐ Local ☒ Remote LDAP ☐ Remote RADIUS



**User retrieval:** ☐ Specify an LDAP filter ☒ Set a list of imported remote LDAP users

**Remote LDAP:** AD-2008-10.1.2.122 (10.1.2.122) 



**LDAP users:**

**Available LDAP users** 

**Selected LDAP users**  
lens.fortiad.net @ AD-2008-10.1.2.122 (10.1.2.122)

Choose all visible   Remove all

☐ Allow token self-provisioning

RADIUS Attributes			
Attribute	Value	Vendor	Actions
Fortinet-Group-Name	VLAN10	Fortinet	 

## Configuring remote user sync rules

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

**Name:** VLAN10

**Remote LDAP:** AD-2008-10.1.2.122 (10.1.2.122) ▾

**Sync every:** 1 day(s) ▾

**Base distinguished name:** OU=VLAN10,DC=fortiad,DC=net

**LDAP filter:**  **Test Filter**

**Token-based authentication sync priorities:**

- ☒ None (users are synced explicitly with no token-based authentication)
- ☐ FortiToken 200 (assign if serial number is provided)
- ☐ FortiToken 200 (assign an available token)
- ☐ Email
- ☐ SMS
- ☐ FortiToken Mobile (assign an available token)

**Sync as:** ☒ Remote LDAP User ☐ Local User

**Group to associate users with:** VLAN10 ▾

**Organization:** [ Please Select ] ▾

**Debugging Settings**

**LDAP User Mapping Attributes**

**Preview Mapping** **Show Sync Fields**

**OK** **Cancel**

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

**Name:** VLAN10

**Remote LDAP server:** AD-2008-10.1.2.122 (10.1.2.122)

**Username:** leno.fortiad.net

**Distinguished name:** CN=LENO,OU=VLAN10,DC=fortiad,DC=net

☐ Disabled

☐ Token-based authentication

☒ Allow RADIUS authentication

**User Role**

**Role:** ☐ Administrator ☒ User

**User Information**

**RADIUS Attributes**

**Certificate Bindings**

Common Name	Issuer	Status	Actions
leno.fortiad.net	CN=fac, emailAddress=kash@fortinet.com	Active	

**Add Binding**

## 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.

Name:

Client name/IP:

Secret:

Enable captive portal: ☐ Credentials portal (URL: /caplogin/)  
☐ Social portal (URL: /social\_login/)  
☐ MAC address portal (URL: /malogin/)

---

**Profiles**

Default

[Add New Profile](#)

---

Profile name:

Description:

☐ Apply this profile based on RADIUS attributes.

Authentication method:

☐ Enforce two-factor authentication  
☒ Apply two-factor authentication if available (authenticate any user)  
☐ Password-only authentication (exclude users without a password)  
☐ FortiToken-only authentication (exclude users without a FortiToken)

Username input format:

☐ username@realm  
☐ realm/username  
☒ realm/username

Realms:

Default	Realm	Allow local users to override remote users	Use Windows AD domain authentication	Groups	Delete
	host   AD-2008-10.1.2.122 (10.1.2.122)	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/> Filter: VLAN10 <a href="#">[Edit]</a> Filter local users: <a href="#">[Edit]</a>	

[Add a realm](#)

☐ Allow MAC-based authentication  
☐ Check machine authentication

EAP types:

☐ EAP-GTC  
☒ EAP-TLS  
☐ PEAP  
☐ EAP-TTLS

## Configuring the FortiWiFi

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

Name

Primary Server IP/Name

Primary Server Secret  [Test Connectivity](#)

Secondary Server IP/Name

Secondary Server Secret

Authentication Method ☒ Default ☐ Specify

NAS IP / Called Station ID

Include in every User Group ☐

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




Interface Name	wifi
Type	WiFi SSID
Traffic Mode	Tunnel to Wireless Controller

---

IP/Network Mask	<input type="text"/>
-----------------	----------------------

---

WiFi Settings

SSID	<input type="text" value="fortinet"/>
Security Mode	<input type="text" value="WPA2 Enterprise"/> 
Authentication	<input type="radio"/> Local <input checked="" type="radio"/> RADIUS Server
	<input type="text" value="FAC-10.1.2.29"/> 
Broadcast SSID	<input checked="" type="checkbox"/>
Block Intra-SSID Traffic	<input type="checkbox"/>
Maximum Clients	<input type="checkbox"/>
Optional VLAN ID	<input type="text" value="0"/> 

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

Interface Name	lan				
Type	Software Switch				
Physical Interface Members	<input type="text" value="internal"/> X <input type="text" value="wifi (SSID: fortinet)"/> X				
Addressing mode	<input checked="" type="radio"/> Manual <input type="radio"/> DHCP <input type="radio"/> PPPoE				
IP/Network Mask	<input type="text" value="10.1.2.27/255.255.255.0"/>				
Administrative Access	<input checked="" type="checkbox"/> HTTPS <input checked="" type="checkbox"/> PING <input checked="" type="checkbox"/> HTTP <input checked="" type="checkbox"/> FMG-Access <input checked="" type="checkbox"/> CAPWAP <input checked="" type="checkbox"/> SSH <input type="checkbox"/> SNMP <input type="checkbox"/> FCT-Access <input type="checkbox"/> Auto IPsec Request				
DHCP Server	<input checked="" type="checkbox"/> Enable				
▼ Advanced...					
Mode	<input type="radio"/> Server <input checked="" type="radio"/> Relay				
DHCP Server IP	<input type="text" value="10.1.2.1"/>				
Type	<input checked="" type="radio"/> Regular <input type="radio"/> IPsec				
Security Mode	<input type="text" value="None"/>				
Device Management					
Detect and Identify Devices	<input type="checkbox"/>				
Listen for RADIUS Accounting Messages	<input type="checkbox"/>				
Secondary IP Address	<input type="checkbox"/>				
Comments	<input type="text" value=""/> 0/255				
Administrative Status	<input checked="" type="radio"/> Up <input type="radio"/> Down				

## Results

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

- 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 0x0, 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 0x18a3 -> 0xbe6a1] 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 1bfd 2af6 1fb9 8db9 1f18 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 0x0, 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: 0x7d, 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 aef1 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 b11b 9488 f181
0x0010: d179 29ba 7538 11eb 8311 3c22 1b62 9176
0x0020: d0be f763 4617 670c d8ca 8659 7a14 d12c
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
```

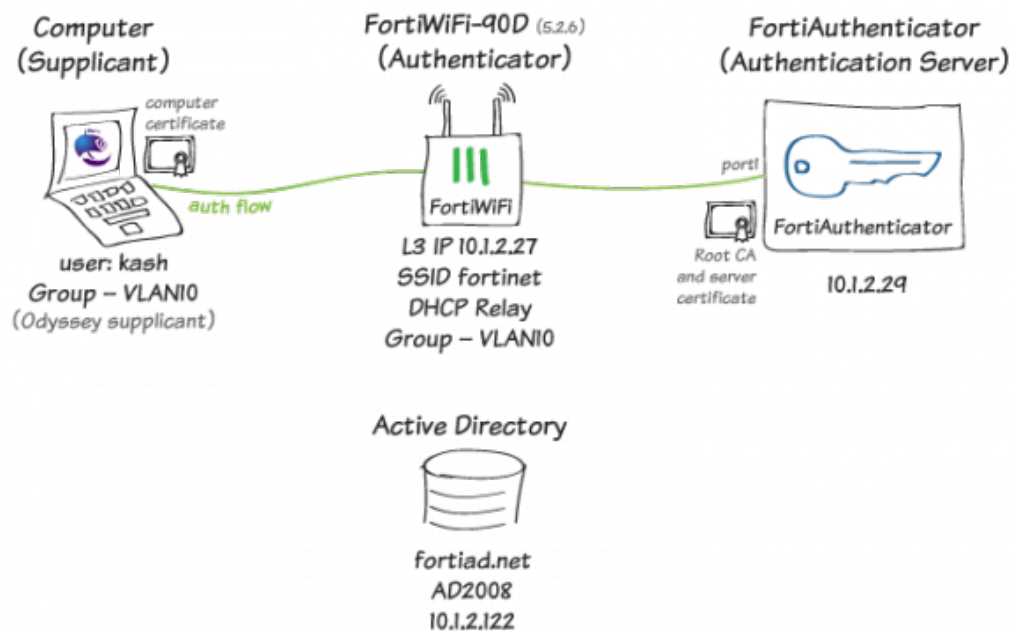
5. On the FortiAuthenticator, go to Logging > Log Access > Logs to verify the device authentication. The Debug Log (at <https://<fac-ip>/debug/radius>) should also confirm successful authentication.

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

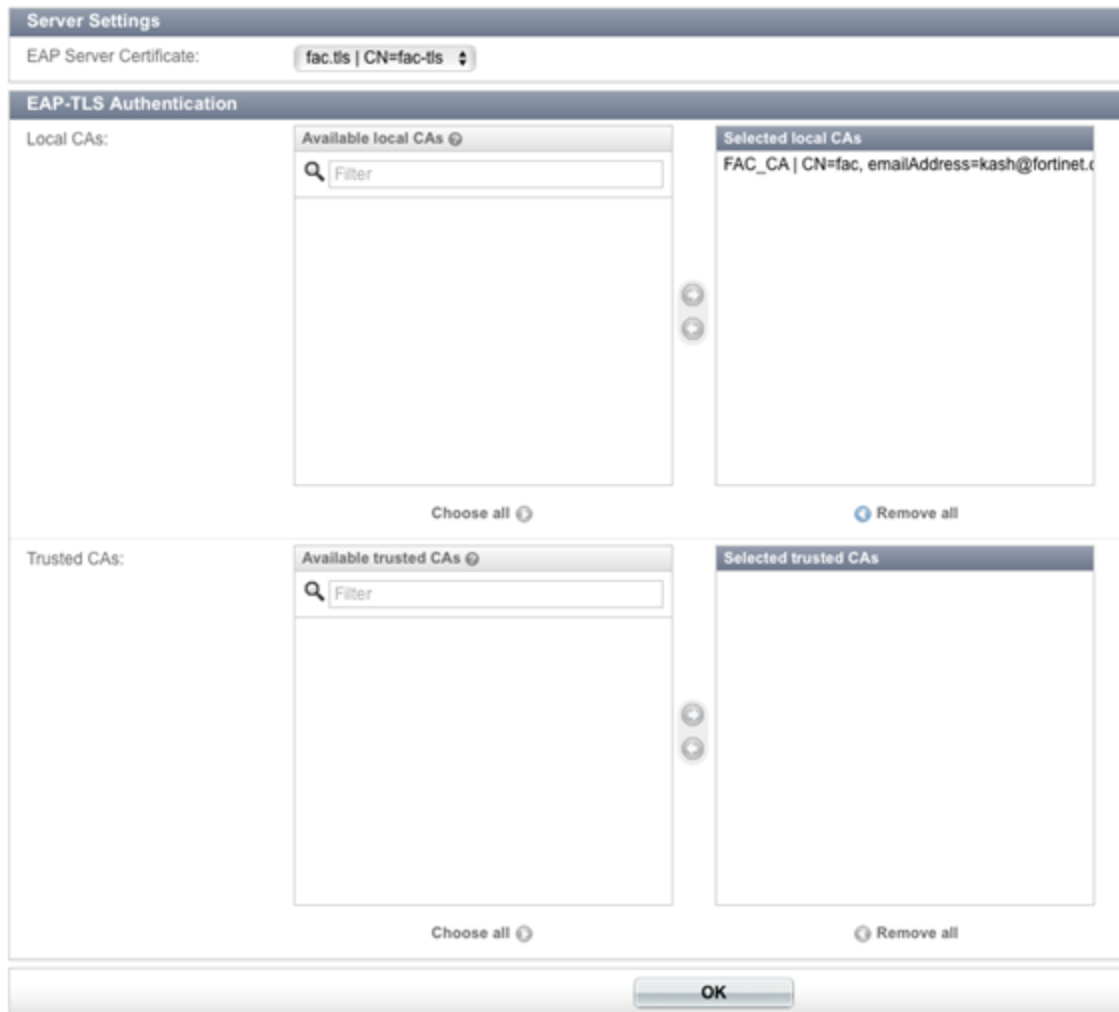
1. On the FortiAuthenticator, go to **Certificate Management > Certificate Authorities > Local CAs** and create a new root CA.

Certificate ID	Subject	Issuer	Status	CA Type
<input type="checkbox"/> 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
<input type="checkbox"/> 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
<input type="checkbox"/> 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.



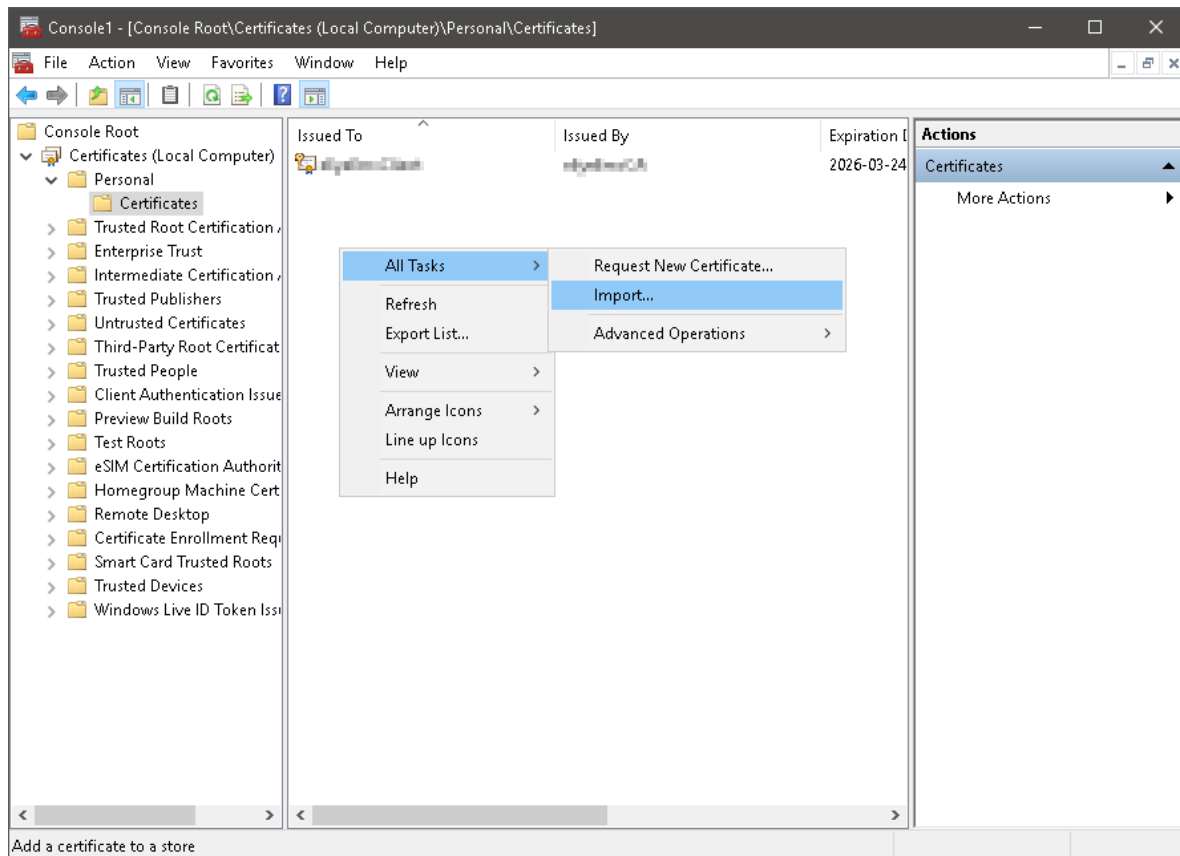
- Go to **Certificate Management > End Entities > Users** and create a client certificate. The CN must match the AD user name. Select **Export Key and Cert** (with a **Passphrase** to protect it) and download the PKCS#12 file.

<a href="#">Create New</a> <a href="#">Import</a> <a href="#">Revoke</a> <a href="#">Delete</a> <a href="#">Export Certificate</a> <a href="#">Export PKCS#12</a> <span>1 of 8 selected</span> <span>Search for user certificates</span>			
	Certificate ID	Subject	Status
<input checked="" type="checkbox"/>	kash.fortiad.net	CN=kash	Active

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

- 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.

Name:	AD-2008-10.1.2.122		
Primary server name/IP:	10.1.2.122	Port:	389
<input type="checkbox"/> Use secondary server			
Base distinguished name:	dc=fortiad,dc=net		
Bind type:	<input type="radio"/> Simple <input checked="" type="radio"/> Regular		
Username:	cn=administrator,cn=users,dc=fortiad,dc=net	Password:	*****
User object class:	person		
Username attribute:	sAMAccountName		
Group object class:	group		
Group membership attribute:	memberOf	<input type="checkbox"/> Attribute is group attribute	

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

**Name:**

---

**User source:** AD-2008-10.1.2.122 (10.1.2.122) 

## 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.


**Name:**


**Type:** ☐ Local ☒ Remote LDAP ☐ Remote RADIUS



**User retrieval:** ☐ Specify an LDAP filter ☒ Set a list of imported remote LDAP users


**Remote LDAP:** AD-2008-10.1.2.122 (10.1.2.122) 

**LDAP users:**


Available LDAP users 





 Choose all visible

Selected LDAP users

 Remove all

Select a remote LDAP server above to show its list of remote users

☐ Allow token self-provisioning

RADIUS Attributes			
Attribute	Value	Vendor	Actions
Fortinet-Group-Name	VLAN10	Fortinet	 

## Configuring remote user sync rules

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

**Name:**

**Remote LDAP:**

**Sync every:**

**Base distinguished name:**

**LDAP filter:**

**Token-based authentication sync priorities:**

- ☒ None (users are synced explicitly with no token-based authentication)
- ☐ FortiToken 200 (assign if serial number is provided)
- ☐ FortiToken 200 (assign an available token)
- ☐ Email
- ☐ SMS
- ☐ FortiToken Mobile (assign an available token)

**Sync as:** ☒ Remote LDAP User ☐ Local User

**Group to associate users with:**

**Organization:**

**Debugging Settings**

**LDAP User Mapping Attributes**

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

**Remote LDAP server:** AD-2008-10.1.2.122 (10.1.2.122)

**Username:** kash

**Distinguished name:** CN=kash valji,OU=Employees,DC=fortiad,DC=net

☐ Disabled

☐ Token-based authentication

☒ Allow RADIUS authentication

**User Role**

**Role:** ☐ Administrator ☒ User

**User Information**

**RADIUS Attributes**

**Certificate Bindings**

Common Name	Issuer	Status	Actions
kash	CN=fac, emailAddress=kash@fortinet.com	N/A	

## Configuring the FortiAuthenticator RADIUS client

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

Name:

Client name/IP:

Secret:

Enable captive portal: ☐ Credentials portal (URL: /caplogin/)  
☐ Social portal (URL: /social\_login/)  
☐ MAC address portal (URL: /malogin/)

---

**Profiles**

Default

[Add New Profile](#)

Profile name:

Description:

☐ Apply this profile based on RADIUS attributes.

Authentication method: ☐ Enforce two-factor authentication  
☒ Apply two-factor authentication if available (authenticate any user)  
☐ Password-only authentication (exclude users without a password)  
☐ FortiToken-only authentication (exclude users without a FortiToken)

Username input format: ☐ username@realm  
☐ realm/username  
☒ realm/username

Realms:

Default	Realm	Allow local users to override remote users	Use Windows AD domain authentication	Groups	Delete
	default   AD-2008-10.1.2.122 (10.1.2.122)	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/> Filter: VLAN10 [Edit] <input type="checkbox"/> Filter local users: [Edit]	

[Add a realm](#)

☐ Allow MAC-based authentication

☐ Check machine authentication

EAP types: ☐ EAP-GTC  
☒ EAP-TLS  
☐ PEAP  
☐ EAP-TTLS

## Configuring the FortiWiFi

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

Name

Primary Server IP/Name

Primary Server Secret  [Test Connectivity](#)

Secondary Server IP/Name

Secondary Server Secret

Authentication Method ☒ Default ☐ Specify

NAS IP / Called Station ID

Include in every User Group ☐

[Test Connectivity](#)

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




Interface Name	wifi
Type	WiFi SSID
Traffic Mode	Tunnel to Wireless Controller

---

IP/Network Mask	<input type="text"/>
-----------------	----------------------

---

WiFi Settings

SSID	<input type="text" value="fortinet"/>
Security Mode	<input type="text" value="WPA2 Enterprise"/> 
Authentication	<input type="radio"/> Local <input checked="" type="radio"/> RADIUS Server
	<input type="text" value="FAC-10.1.2.29"/> 
Broadcast SSID	<input checked="" type="checkbox"/>
Block Intra-SSID Traffic	<input type="checkbox"/>
Maximum Clients	<input type="checkbox"/>
Optional VLAN ID	<input type="text" value="0"/> 

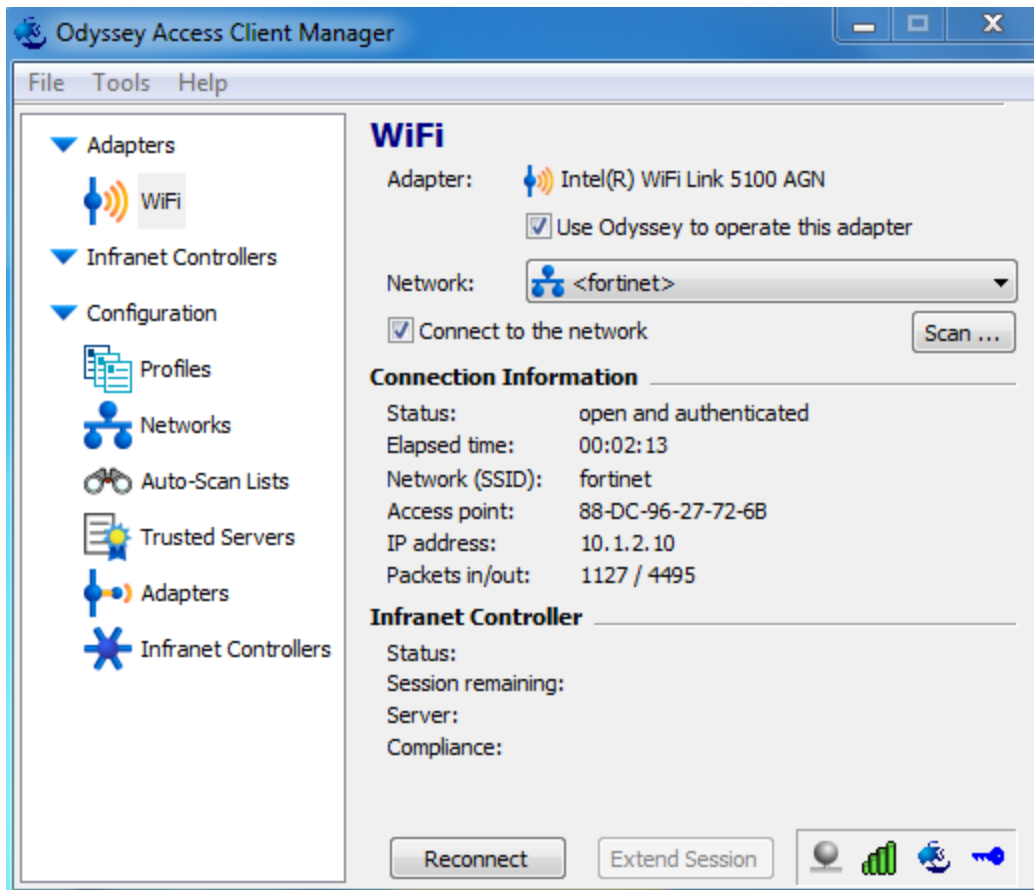
3. Then go to **Network > Interfaces** and configure a software switch combining the physical and WiFi interfaces.



Interface Name	lan
Type	Software Switch
Physical Interface Members	<div>internal X</div> <div>wifi (SSID: fortinet) X</div>
Addressing mode	<input checked="" type="radio"/> Manual <input type="radio"/> DHCP <input type="radio"/> PPPoE
IP/Network Mask	<div>10.1.2.27/255.255.255.0</div>
Administrative Access	<div><input checked="" type="checkbox"/> HTTPS <input checked="" type="checkbox"/> PING <input checked="" type="checkbox"/> HTTP <input checked="" type="checkbox"/> FMG-Access <input checked="" type="checkbox"/> CAPWAP</div> <div><input checked="" type="checkbox"/> SSH <input type="checkbox"/> SNMP <input type="checkbox"/> FCT-Access</div> <div><input type="checkbox"/> Auto IPsec Request</div>
DHCP Server	<input checked="" type="checkbox"/> Enable
▼ Advanced...	
Mode	<input type="radio"/> Server <input checked="" type="radio"/> Relay
DHCP Server IP	<div>10.1.2.1</div>
Type	<input checked="" type="radio"/> Regular <input type="radio"/> IPsec
Security Mode	<div>None</div>
Device Management	
Detect and Identify Devices	<input type="checkbox"/>
Listen for RADIUS Accounting Messages	<input type="checkbox"/>
Secondary IP Address	<input type="checkbox"/>
Comments	<div></div> 0/255
Administrative Status	<div><input checked="" type="radio"/> Up <input type="radio"/> Down</div>

## 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.



- 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 0x0, 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 0x18a3 -> 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 0x0, 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: 0x7d, 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 aef1 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 b11b 9488 f181
0x0010: d179 29ba 7538 11eb 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
```

- 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.

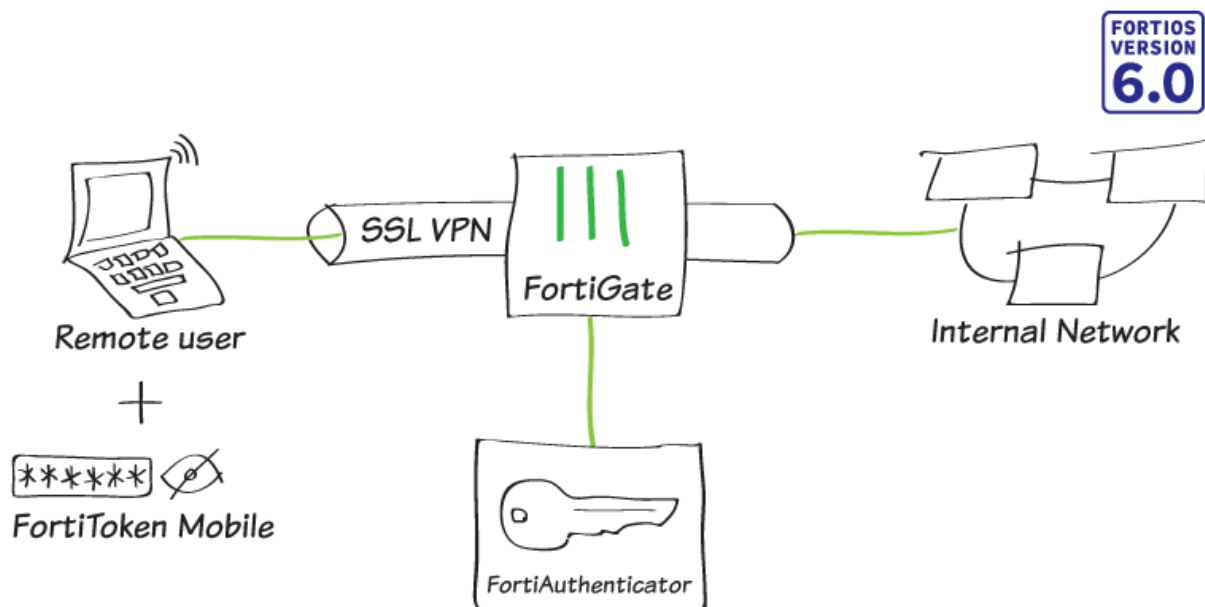
SSID	FortiAP	User	Group	IP	Device	Channel	Bandwidth Tx/Rx	Signal Strength/Noise	Signal Strength	Association Time
fortinet	Local WiFi Radio (1)	kash	VLAN10	10.1.2.10	00:26:c6:6a:e6:b2	11	0 bps	65 dB		02:07:19

## 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:

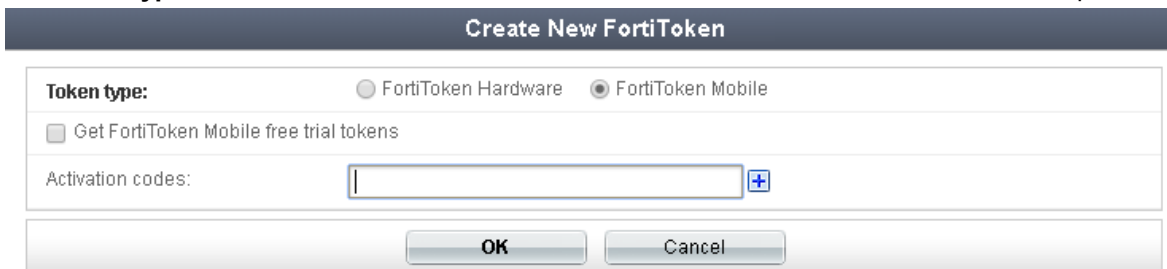
- Username: gthreepwood
- User group: RemoteFTMGroup
- RADIUS server: OfficeRADIUS
- RADIUS client: OfficeServer
- SSL VPN user group: SSLVPNGroup
- FortiAuthenticator: 172.25.176.141
- FortiGate: 172.25.176.92

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.



**Create New FortiToken**

**Token type:** ☐ FortiToken Hardware ☒ FortiToken Mobile

☐ Get FortiToken Mobile free trial tokens

Activation codes:

## 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.

**Create New Local User**

<b>Username:</b>	<input type="text" value="gthreepwood"/>
<b>Password creation:</b>	<div style="border: 1px solid #ccc; padding: 2px; display: flex; align-items: center;">Specify a password ▼</div>
Password:	<input type="password" value="*****"/>
Password confirmation:	<input type="password" value="*****"/>
<input checked="" type="checkbox"/> Allow RADIUS authentication	
<input type="checkbox"/> Force password change on next logon	

**Role**

<b>Role:</b>	<input type="radio"/> Administrator <input type="radio"/> Sponsor <input checked="" type="radio"/> User
--------------	---

**Account Expiration**

<input type="checkbox"/> Enable account expiration
--

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.

**Change local user**

✓ Successfully added local user "gthreepwood". You may edit it again below.

Username:	<input type="text" value="gthreepwood"/>		
<input type="checkbox"/> Disabled			
<input checked="" type="checkbox"/> Password-based authentication	<a href="#">[Change Password]</a>		
<input checked="" type="checkbox"/> Token-based authentication			
Deliver token code by:	<input checked="" type="radio"/> FortiToken <input type="radio"/> Email <input type="radio"/> SMS <input type="radio"/> Dual (Email & SMS) <input type="button" value="Test Token"/>		
FortiToken Hardware:	<div style="border: 1px solid #ccc; padding: 2px;">[Please Select] ▼</div>	FortiToken Mobile:	<div style="border: 1px solid #ccc; padding: 2px;">XXXXXXXXXX x ▼</div>
		Delivery method:	<input checked="" type="radio"/> Email <input type="radio"/> SMS
<a href="#">Configure a temporary e-mail/SMS token.</a>			
<input checked="" type="checkbox"/> Allow RADIUS authentication			
<input type="checkbox"/> Enable account expiration			
<input type="checkbox"/> Force password change on next logon			

**User Role**

<b>Role:</b>	<input type="radio"/> Administrator <input type="radio"/> Sponsor <input checked="" type="radio"/> User
<input type="checkbox"/> Allow LDAP browsing	

**User Information**

First name:	<input type="text"/>	Last name:	<input type="text"/>
Email:	<input type="text" value="gthreepwood@fortinet.com"/>		
Mobile number:	<input type="text"/>	SMS gateway:	<div style="border: 1px solid #ccc; padding: 2px;">Use default ▼</div>
<input type="button" value="Test SMS"/>			
Street address:	<input type="text"/>		

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**.

**Create New User Group**

**Name:** RemoteFTMUsers

**Type:** ☒ Local ☐ Remote LDAP ☐ Remote RADIUS ☐ MAC

**Users:**

**Available users**

Filter

**Selected users**

gthreepwood

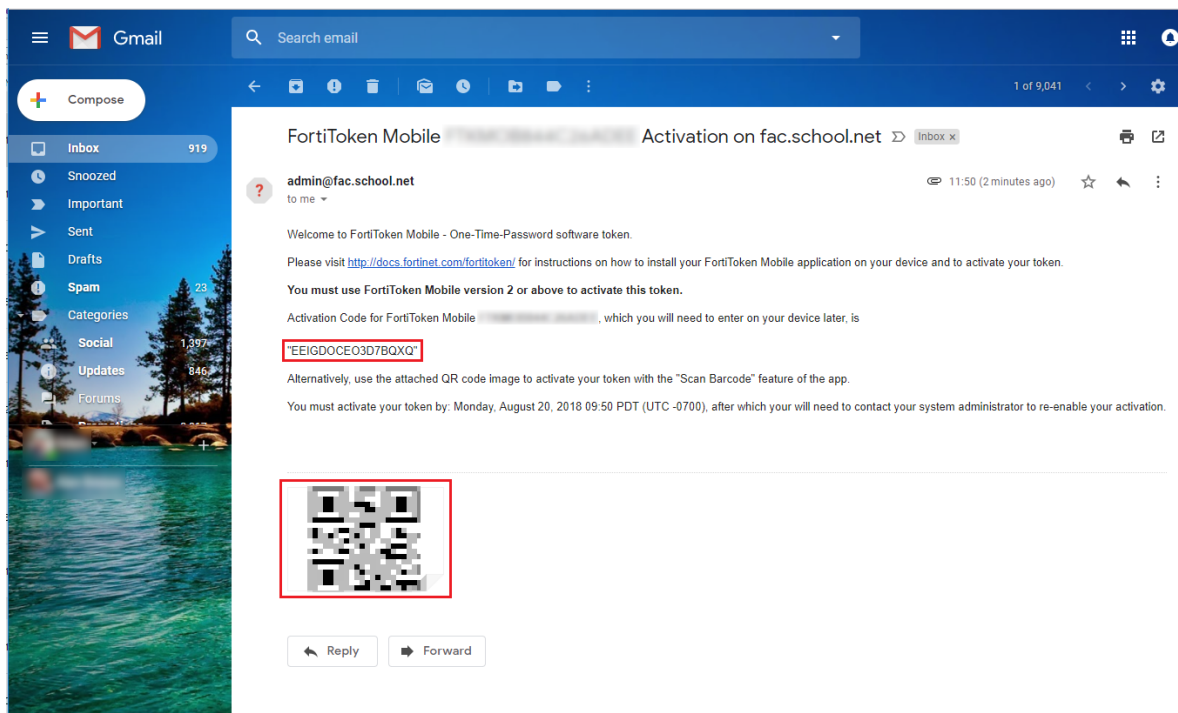
Choose all visible Remove all

**Password policy:** Default

☐ Usage Profile [Please Select]

OK Cancel

- 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".

Add RADIUS client

Name:	<input type="text" value="OfficeServer"/>																						
Client address:	<input checked="" type="radio"/> IP/Hostname <input type="radio"/> Subnet <input type="radio"/> Range																						
	<input type="text" value="172.25.176.124"/>																						
Secret:	<input type="password" value="*****"/>																						
First profile name:	<input type="text" value="Default"/>																						
Description:	<input type="text"/>																						
<input type="checkbox"/> Apply this profile based on RADIUS attributes.																							
EAP types:	<input type="checkbox"/> EAP-GTC <input type="checkbox"/> EAP-TLS <input type="checkbox"/> PEAP <input type="checkbox"/> EAP-TTLS																						
Device Authentication																							
<input type="checkbox"/> MAC Authentication Bypass(MAB)																							
<input type="checkbox"/> AD machine authentication																							
<input type="checkbox"/> MAC device filtering																							
User Authentication																							
Authentication method:	<input checked="" type="radio"/> Enforce two-factor authentication <input type="radio"/> Apply two-factor authentication if available (authenticate any user) <input type="radio"/> Password-only authentication (exclude users without a password) <input type="radio"/> FortiToken-only authentication (exclude users without a FortiToken)																						
<input type="checkbox"/> Enable FortiToken Mobile push notifications authentication																							
Username input format:	<input checked="" type="radio"/> username@realm <input type="radio"/> realm/username <input type="radio"/> realm/username																						
Realms:	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 5%;">Default</th> <th style="width: 35%;">Realm</th> <th style="width: 20%;">Allow local users to override remote users</th> <th style="width: 20%;">Use Windows AD domain authentication</th> <th style="width: 15%;">Groups</th> <th style="width: 15%;">Delete</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="radio"/></td> <td>local   Local users</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td> <input checked="" type="checkbox"/> Filter: RemoteFTMUsers [Edit]  <input type="checkbox"/> Filter local users: [Edit]               </td> <td><input type="button" value="X"/></td> </tr> <tr> <td colspan="6" style="text-align: center;"> <a href="#">+ Add a realm</a> </td> </tr> </tbody> </table>					Default	Realm	Allow local users to override remote users	Use Windows AD domain authentication	Groups	Delete	<input checked="" type="radio"/>	local   Local users	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/> Filter: RemoteFTMUsers [Edit] <input type="checkbox"/> Filter local users: [Edit]	<input type="button" value="X"/>	<a href="#">+ Add a realm</a>					
Default	Realm	Allow local users to override remote users	Use Windows AD domain authentication	Groups	Delete																		
<input checked="" type="radio"/>	local   Local users	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/> Filter: RemoteFTMUsers [Edit] <input type="checkbox"/> Filter local users: [Edit]	<input type="button" value="X"/>																		
<a href="#">+ Add a realm</a>																							

## 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**.

New RADIUS Server

Name

OfficeRADIUS

Authentication method

Default

Specify

NAS IP

Include in every user group

☐

Primary Server

IP/Name

172.25.176.141

Secret

••••••••

Connection status

☒ Successful

Test Connectivity

Test User Credentials

Secondary Server

IP/Name

Secret

Test Connectivity

Test User Credentials

OK

Cancel

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

New RADIUS Test User Credentials ✕

Name Username

Authentication Password

NAS IP

Include in e Connection status ✓ Successful

Primary Set User credentials ✗ More validation is required

IP/Name Server message

Secret

Connection

Test Conn

Test User

Secondary

i AVP: l=79 t=Reply-Message(18) Value: &apos;+Enter token code or no code to send a notification to your FortiToken Mobile&apos;; AVP: l=11 t=Vendor-Specific(26) v=Fortinet(12356) VSA: l=5 t=Fortinet-Token-Challenge(15) Value: &apos;001&apos;; AVP: l=3 t=State(24) Value: 31

Test Close

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.

New User Group

Name

Type Firewall  
Fortinet Single Sign-On (FSSO)  
RADIUS Single Sign-On (RSSO)  
Guest

Members

Remote Groups

✚ Add ✎ Edit 🗑 Delete

Remote Server	Group Name
OfficeRADIUS	Any

OK Cancel

## 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.

The screenshot shows the 'Edit SSL-VPN Portal' configuration page for the 'full-access' portal. The 'Name' field is set to 'full-access'. The 'Limit Users to One SSL-VPN Connection at a Time' toggle is turned off. Under the 'Tunnel Mode' section, the 'Enable Split Tunneling' toggle is turned off and is highlighted with a red rectangle. Below this, the 'Source IP Pools' section shows a list with one entry, 'SSLVPN\_TUNNEL\_ADDR1', which is also highlighted with a red rectangle. A plus sign is visible below the list, indicating the option to add more IP pools.

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

- 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**.

New Policy

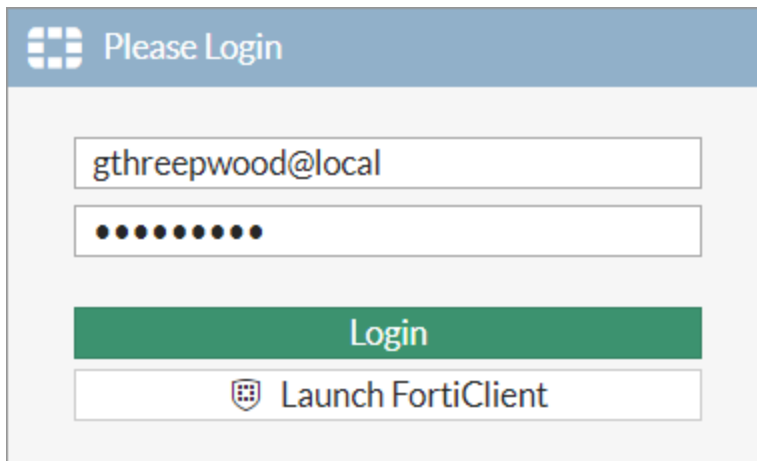
Name	SSL-VPN
Incoming Interface	SSL-VPN tunnel interface (ssl.root)
Outgoing Interface	wan1
Source	all, SSLVPNGroup
Destination	all
Schedule	always
Service	ALL
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY <input type="checkbox"/> LEARN

Firewall / Network Options

NAT ☒

## Results

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

The image shows a login interface for FortiAuthenticator. At the top, there is a blue header bar with a grid icon and the text "Please Login". Below this, there are two input fields: the first contains the email address "gthreepwood@local", and the second contains ten black dots representing a password. Below the password field is a green button labeled "Login". At the bottom, there is a white button with a shield icon and the text "Launch FortiClient".

Please Login

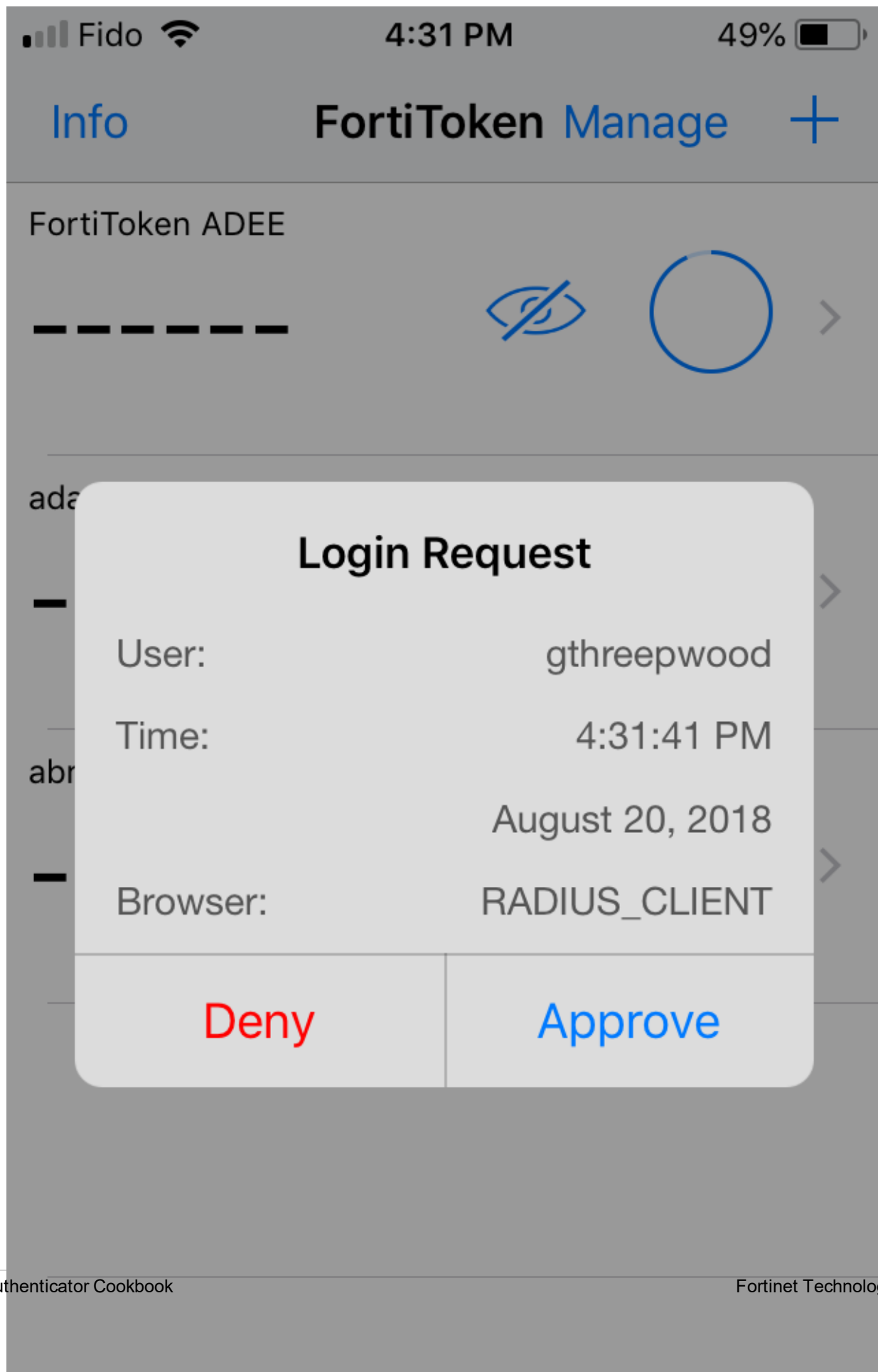
gthreepwood@local

●●●●●●●●●●

Login

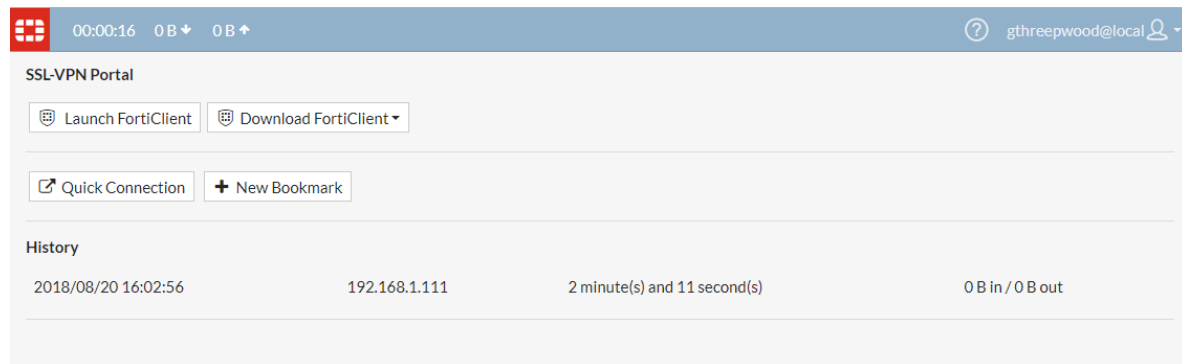
Launch FortiClient

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





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



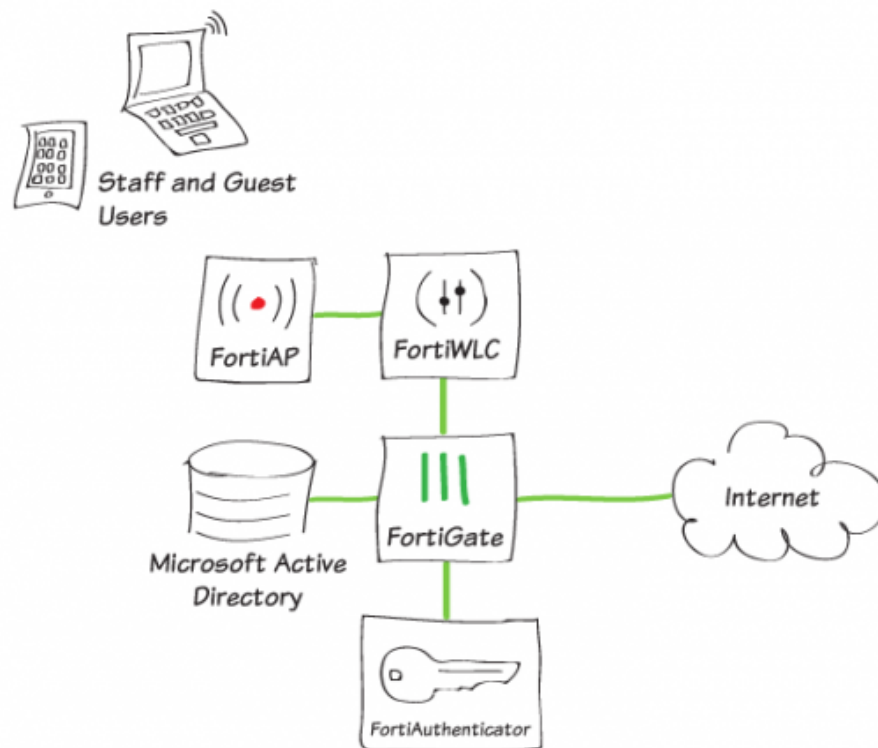
3. On the FortiGate, go to **Monitor > SSL-VPN Monitor** to confirm the user's connection.

Refresh			
▼ Username ↕	▼ Last Login ↕	▼ Remote Host ↕	▼ Active Connections
gthreepwood@local	2018/08/20 16:32:02	192.168.1.111	

## 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.

RADIUS Profile Name: FAC-AUTH (Enter 1-16 chars.)

Description: Authentication (Enter 0-128 chars.)

RADIUS IP: 192.168.200.9

RADIUS Secret: \*\*\*\*\* (Enter 1-64 chars.)

RADIUS Port: 1812 (Valid range: [1024-65535])

Remote RADIUS Server: Off

RADIUS Relay AP-ID: No Relay AP

MAC Address Delimiter: Hyphen (-)

Password Type: Shared Key

Called-Station-ID Type: Default

COA: On

RADIUS Server Timeout: 2 (Valid range: [1-20])

RADIUS Server Retries: 3 (Valid range: [1-10])

## 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.

Add Captive Portal Profile

CP Name: FortiAuthenticator (Enter 1-32 chars.)

User Authentication

Authentication Type: radius

Radius Authentication

Primary Authentication: FAC-AUTH

Secondary Authentication: No Radius

Radius Accounting

Primary Accounting: FAC-ACC

Secondary Accounting: No Radius

Accounting Interim Interval: 600 (Valid range: [40-36000])

External Portal Settings

External Server: Fortinet-Connect

External Portal URL: https://fac-wlc98.net/ga (Enter 0-255 chars.)

Public IP of Controller: 192.168.200.38

Advanced Settings

Session Timeout: 0 (Valid range: [0-3440])

Activity Timeout: 0 (Valid range: [0-60])

Session Caching Time: 1 (Valid range: [1-3440])

## Creating the security profile on the FortiWLC

- 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.

Security Profile Name: FAC-CP (Enter 1-32 chars.)

**SECURITY SETTINGS**

Online Sign Up: not-configured

Security Mode: Open

**CAPTIVE PORTAL SETTINGS**

Captive Portal: WebAuth

Captive Portal profile: FortiAuthenticator

Captive Portal Authentication Method: external

Passthrough Firewall Filter ID: FAC (Enter 0-56 chars.)

**MAC FILTERING SETTINGS**

MAC Filtering: OFF

**FIREWALL SETTINGS**

Firewall Capability: radius-configured

**GENERAL SETTINGS**

Security Logging: OFF

## Creating the QoS rule on the FortiWLC

- 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.

		Match	Excl. Class
ID *	28 <small>Valid range: [0-42534]</small>		
Destination IP	182 168 280 9	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Destination Netmask	255 255 255 255		
Destination Port	443 <small>Valid range: [0-65535]</small>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Source IP	0 0 0 0	<input type="checkbox"/>	<input type="checkbox"/>
Source Netmask	0 0 0 0		
Source Port	0 <small>Valid range: [0-65535]</small>	<input type="checkbox"/>	<input type="checkbox"/>
Network Protocol	6 <small>Valid range: [0-255]</small>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Firewall Filter ID	PAC <small>Enter 0-35 chars.</small>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Packet minimum length	0 <small>Valid range: [0-1500]</small>	<input type="checkbox"/>	<input type="checkbox"/>
Packet maximum length	0 <small>Valid range: [0-1500]</small>		
QoS Protocol *	other <small>or</small>		

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.

		Match	Excl. Class
ID *	21 <small>Valid range: [0-42534]</small>		
Destination IP	0 0 0 0	<input type="checkbox"/>	<input type="checkbox"/>
Destination Netmask	0 0 0 0		
Destination Port	0 <small>Valid range: [0-65535]</small>	<input type="checkbox"/>	<input type="checkbox"/>
Source IP	192 168 200 9	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Source Netmask	255 255 255 255		
Source Port	443 <small>Valid range: [0-65535]</small>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Network Protocol	6 <small>Valid range: [0-255]</small>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Firewall Filter ID	PAC <small>Enter 0-35 chars.</small>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Packet minimum length	0 <small>Valid range: [0-1500]</small>	<input type="checkbox"/>	<input type="checkbox"/>
Packet maximum length	0 <small>Valid range: [0-1500]</small>		
QoS Protocol *	other <small>or</small>		

## 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.

ESS Profiles - Add ⓘ

ESS Profile *	FAC-CP	Enter 1-32 chars.
Enable/Disable	Enable	
SSID *	FAC-CP	Enter 0-32 chars.
Security Profile	FAC-CP	

**ESSID TYPE**

ESSID type	Regular	
Backup ESS Profile	No Backup ESS	
Timer Profile	No Data for Timer Profile	
Primary RADIUS Accounting Server	No RADIUS	
Secondary RADIUS Accounting Server	No RADIUS	
Accounting Interim Interval (seconds)	3600	Valid range: [60-36000]
Reconnect Primary Server (minutes)	10	Valid range: [5-60]

## 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.

<b>Name:</b>	FWLC-833-GA
<b>Client address:</b>	<input checked="" type="radio"/> IP/Hostname <input type="radio"/> Subnet <input type="radio"/> Range
	192.168.200.38
<b>Secret:</b>	••••••••
<b>Captive/Guest portal:</b>	<input type="checkbox"/> Credentials based portals (Captive URL: /caplogin/; Guest URL: /guests/) <input type="checkbox"/> Social based captive portal (URL: /social_login/) <input type="checkbox"/> MAC address based captive portal (URL: /malogin/)
<input checked="" type="checkbox"/> Accept RADIUS accounting messages for usage enforcement	
<input checked="" type="checkbox"/> Support RADIUS Disconnect messages	

Profiles	
standard	
Add New Profile	

<b>Profile name:</b>	standard
<b>Description:</b>	
<input type="checkbox"/> Apply this profile based on RADIUS attributes .	
<b>EAP types:</b>	<input checked="" type="checkbox"/> EAP-GTC <input checked="" type="checkbox"/> EAP-TLS <input checked="" type="checkbox"/> PEAP <input checked="" type="checkbox"/> EAP-TTLS
<b>Device Authentication</b>	
<input type="checkbox"/> MAC Authentication Bypass(MAB)	
<input type="checkbox"/> AD machine authentication	
<input type="checkbox"/> MAC device filtering	
<b>User Authentication</b>	
<b>Authentication method:</b>	<input type="radio"/> Enforce two-factor authentication <input checked="" type="radio"/> Apply two-factor authentication if available (authenticate any user) <input type="radio"/> Password-only authentication (exclude users without a password) <input type="radio"/> FortiToken-only authentication (exclude users without a FortiToken)

## 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.

Name:	WLC-38	
URL:	https://<FAC IP/FQDN>/guests/	
Description:	Coming from WLC-IP=192.168.200.38	
MAC device HTTP parameter:	usermac	
<b>Profile Configuration</b>		
	<b>RADIUS Client</b>	<b>Profile</b>
1	FWLC-833-GA (192.168.200.38)	FWLC-833-GA (192.168.200.38): standard
<a href="#">Add another</a>		
<b>Pre-login Services</b>		
<input type="checkbox"/> Password Reset		
<input type="checkbox"/> Account Registration		
<b>Post-login Services</b>		
<input type="checkbox"/> Profile		
<input type="checkbox"/> Password Change		
<input type="checkbox"/> Token Registration		
		OK Cancel

## Creating the Portal Rule on the FortiAuthenticator

- 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).

<b>General</b>		
Name:	WLC-38	
Description:		
Action:	<input checked="" type="radio"/> Go to portal <input type="radio"/> No portal	
Portal:	WLC-38	
<b>Conditions (All conditions below must be met for this rule to be applied)</b>		
HTTP parameter	Operator	Value
server_ip	exact_match	192.168.200.38
<a href="#">Add Condition</a>		
		OK Cancel



## 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**.

The screenshot shows the 'Log Access' interface on FortiAuthenticator. The table lists various log entries. The entry at the bottom, with a blue header, is highlighted. It shows a successful login for a user named 'test' on the 'test' device, with the 'Sub Category' set to 'User Portal'.

Time	Device	User	Auth Method	Result	Sub Category	Details
2023-09-14 10:00:00	test	test	Local User	Success	User Portal	Successful login for user test on device test.

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

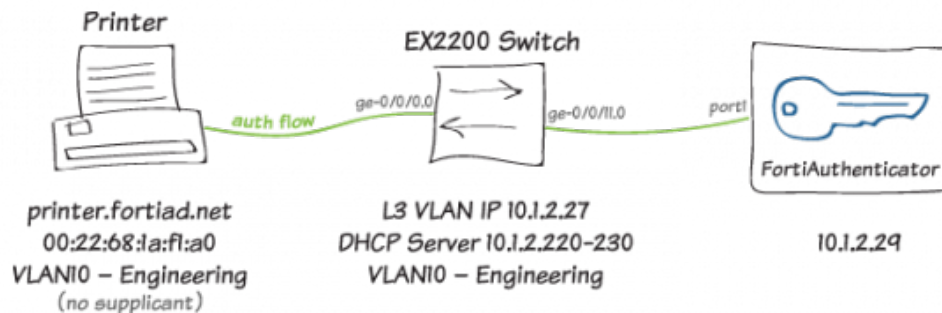
The screenshot shows the 'All Stations' interface on FortiWLC. The table lists various stations. The entry at the bottom, with a blue header, is highlighted. It shows a station named 'test' with the 'Auth Method' set to 'Local User'.

Station Name	IP Address	MAC Address	Auth Method	Result	Sub Category	Details
test	10.10.10.10	00:00:00:00:00:00	Local User	Success	User Portal	Successful login for user test on device test.

## 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.

Create New MAC-based Authentication Device	
Name:	<input type="text" value="printer.fortiad.net"/>
MAC address:	<input type="text" value="00:22:68:1a:f1:a0"/>
Description:	<input type="text"/>
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

### 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.

**Create New User Group**

**Name:**

**Type:** ☒ Local ☐ Remote LDAP ☐ Remote RADIUS ☐ MAC

**Users:**

**Available users**

**Selected users**

Choose all visible
Remove all

☐ Usage Profile [Please Select]

☐ Allow token self-provisioning

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

RADIUS Attributes			
Attribute	Value	Vendor	Actions
Tunnel-Medium-Type	IEEE-802 (6)	Default	
Tunnel-Private-Group-Id	engineering	Default	
Tunnel-Type	VLAN (13)	Default	
<input type="button" value="Add Attribute"/>			
<input type="button" value="OK"/> <input type="button" value="Cancel"/>			

## 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.

FortiAuthenticator Cookbook

Fortinet Technologies Inc.

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

Name: EX2200

Client name/IP: 10.1.2.27

Secret: \*\*\*\*\*

Enable captive portal: ☐ Credentials portal (URL: /caplogin/)  
☐ Social portal (URL: /social\_login/)  
☐ MAC address portal (URL: /malogin/)

**Profiles**

Default

Add New Profile

Profile name: Default

Description:

☐ Apply this profile based on RADIUS attributes.

Authentication method: ☐ Enforce two-factor authentication  
☒ Apply two-factor authentication if available (authenticate any user)  
☐ Password-only authentication (exclude users without a password)  
☐ FortiToken-only authentication (exclude users without a FortiToken)

Username input format: ☐ username@realm  
☐ realm/username  
☒ realm/username

Realms:

Default	Realm	Allow local users to override remote users	Use Windows AD domain authentication	Groups	Delete
	local   Local users	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> Filter: [Edit] <input type="checkbox"/> Filter local users: [Edit]	

Add a realm

☒ Allow MAC-based authentication

☐ Require Call-Check attribute for MAC-based authentication

Apply Group Attributes: VLAN10

☐ Check machine authentication

EAP types: ☐ EAP-GTC  
☐ EAP-TLS  
☐ PEAP  
☐ EAP-TTLS

## Configuring the 3rd-party switch

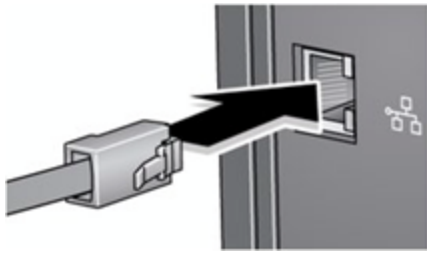
The switch configuration provided below is intended for demonstration only. Your switch configuration is likely to differ significantly.

```
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 13-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-f1-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 -> 0x5cccl) 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 ...2lo..."..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:f1: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 dot1x 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:a1 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:f1: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
```

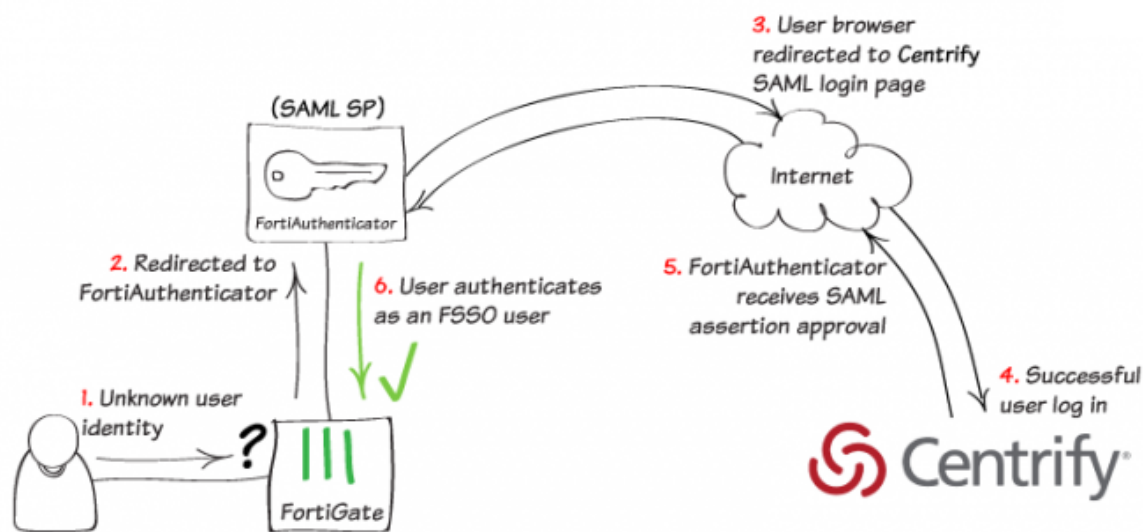
```
{master:0}[edit]
root* run ping 10.1.2.224
PING 10.1.2.224 (10.1.2.224): 56 data bytes
64 bytes from 10.1.2.224: icmp_seq=0 ttl=128 time=2.068 ms
64 bytes from 10.1.2.224: icmp_seq=1 ttl=128 time=2.236 ms
64 bytes from 10.1.2.224: icmp_seq=2 ttl=128 time=2.699 ms

--- 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.

System Information	
Host Name	fac.school.net [Change]
Device FQDN	fac.school.net [Change]
Serial Number	FAC2HD3A15000126
System Time	Thu Aug 23 15:08:59 2018 [Change]
Firmware Version	v5.4.0, build0294 (GA) [Upgrade]
System Configuration	Last Backup: Mon Aug 20 14:21:20 2018 [Backup/Restore]
Current Administrator	admin
Uptime	3 day(s) 0 hour(s) 45 minute(s)
Shutdown / Reboot	[Reboot] [Shutdown]

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.

Edit SSO Configuration	
FortiGate	
Listening port:	<input type="text" value="8000"/>
<input checked="" type="checkbox"/> Enable authentication	
Secret key:	<input type="text" value="....."/>
Login expiry:	<input type="text" value="480"/> minutes
Extend user session beyond logoff by:	<input type="text" value="0"/> seconds (0-3600)
<input type="checkbox"/> Enable NTLM authentication	

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.

### Edit SAML Portal Settings

☒ Enable SAML portal

Device FQDN:	fac.school.net
Portal URL:	https://fac.school.net/login/saml-auth
Entity ID:	http://fac.school.net/metadata/
ACS (login) URL:	https://fac.school.net/saml/?acs

[\[Download SP metadata\]](#) [\[Import IDP metadata\]](#) [\[Import IDP certificate\]](#)

IDP entity id:

IDP single sign-on URL:

IDP certificate fingerprint:

Fingerprint algorithm:

Unknown

☐ Enable SAML single logout

☐ Sign SAML requests with a local certificate

Obtain group membership from:

☒ SAML assertions:

☐ "In\_<group>" boolean assertions

☒ Text-based list 

Memberof

☐ Azure

☐ LDAP lookup

☒ Implicit group membership

saml\_users

OK

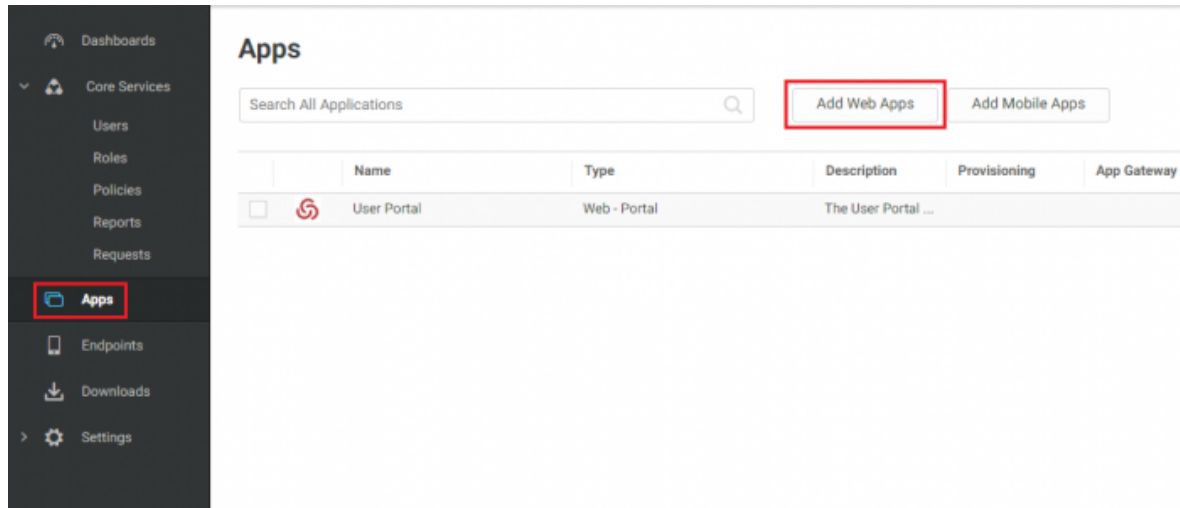
Cancel

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

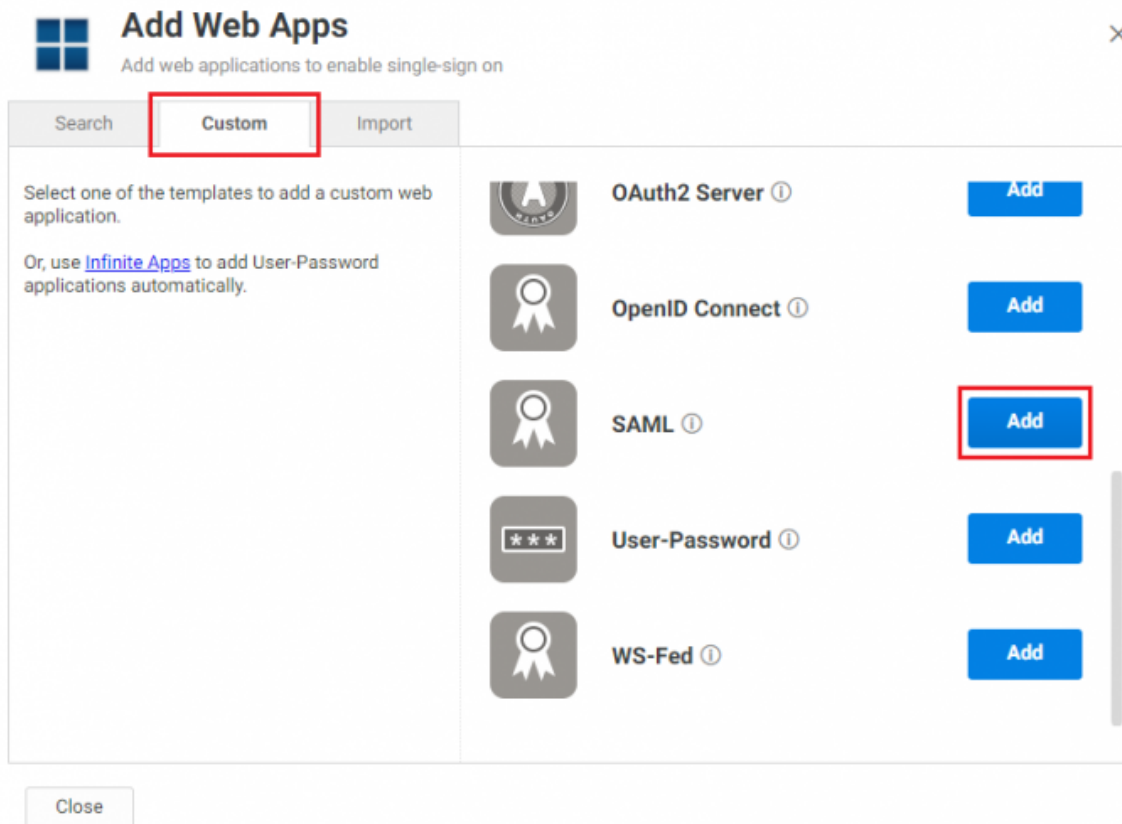
Note that, at this point, you will not be able to save these settings, as the IdP information — **IDP entity id**, **IDP single sign-on URL**, and **IDP certificate fingerprint** — needs to be entered. These fields will be filled once the IdP application configuration is complete.

## 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.

The screenshot shows the FortiAuthenticator SAML configuration interface. The left sidebar has a 'Trust' tab highlighted. The main content area is titled 'Trust' and 'Identity Provider Configuration'. Under 'Identity Provider Configuration', there are two radio buttons: 'Metadata' (selected) and 'Manual Configuration'. The 'Metadata' section shows a dropdown for 'IdP Entity ID / Issuer' and a 'Signing Certificate' section. The 'Signing Certificate' section displays the following details: Thumbprint: DD3E91BC1F8D5483F1615F899E1ED5CA92B88A88, Subject: CN=Centrify Customer AAW8849 Application Signing Certificate, Algorithm: sha256RSA, Expires: 12/31/2038 7:00:00 PM. Below these details is a 'Download' button. In the 'File' section, there is a 'Download Metadata File' button highlighted with a red box. The 'URL' section shows a URL and a 'Copy URL' button. The 'XML' section shows a 'Copy XML' button.

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

**SAML**  
Type: Web - SAML + Provisioning • Status: **Ready to Deploy**  
[Actions](#) [Application Configuration Help](#)

Settings  
Trust  
**SAML Response**  
Permissions  
Policy  
Account Mapping  
Linked Applications  
Provisioning  
App Gateway  
Workflow  
Changelog

### SAML Response

[Learn more](#)

#### Attributes

Click the Add button below to map attributes from your source directory to SAML attributes that should be included in the SAML response for this application.

[Add](#)

	Attribute Name	Attribute Value
<input type="checkbox"/>	FirstName	LoginUser.FirstName
<input type="checkbox"/>	LastName	LoginUser.LastName
<input type="checkbox"/>	Email	LoginUser.Email

[Save](#) [Cancel](#)

## 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.

**Edit SAML Portal Settings**

✓ Successfully saved SAML Portal Settings.

<input checked="" type="checkbox"/> Enable SAML portal
Device FQDN: fac.school.net
Portal URL: https://fac.school.net/login/saml-auth
Entity ID: http://fac.school.net/metadata/
ACS (login) URL: https://fac.school.net/saml/?acs
<a href="#">[Download SP metadata]</a> <a href="#">[Import IDP metadata]</a> <a href="#">[Import IDP certificate]</a>
IDP entity id: https://aaw0849.my.centrify.com/eee78b2b-e442-40d8-b543-de1ad9f8fe27
IDP single sign-on URL: https://aaw0849.my.centrify.com/applogin/appKey/eee78b2b-e442-40d8-b543-de1ad9f8fe27/customerId/AAW0849
IDP certificate fingerprint: 8d69cc43328f6f59f9ad0a054d7730d95fca26e8850407fb151c69f9d1ebfee
Fingerprint algorithm: SHA-256
<input type="checkbox"/> Enable SAML single logout
<input type="checkbox"/> Sign SAML requests with a local certificate
Obtain group membership from: <ul style="list-style-type: none"> <li><input checked="" type="radio"/> SAML assertions: <ul style="list-style-type: none"> <li><input type="radio"/> "In_&lt;group&gt;" boolean assertions</li> <li><input checked="" type="radio"/> Text-based list Memberof</li> </ul> </li> <li><input type="radio"/> Azure</li> <li><input type="radio"/> LDAP lookup</li> </ul>
<input checked="" type="checkbox"/> Implicit group membership saml_users
<input type="button" value="OK"/> <input type="button" value="Cancel"/>

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

**Edit SAML Portal Settings**

<input checked="" type="checkbox"/> Enable SAML portal
Device FQDN: fac.school.net
Portal URL: https://fac.school.net/login/saml-auth
Entity ID: http://fac.school.net/metadata/
ACS (login) URL: https://fac.school.net/saml/?acs
<a href="#">[Download SP metadata]</a> <a href="#">[Import IDP metadata]</a> <a href="#">[Import IDP certificate]</a>

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.

**Edit FortiGate Filter**

✓ Successfully added FortiGate filter "saml\_users (172.25.176.62)". You may edit it again below.

Name:

FortiGate name/IP:

Description:

**IP Filtering**

☐ Enable IP filtering for this service.

**Fortinet Single Sign-On (FSSO)**

☒ Forward FSSO information for users from the following subset of users/groups/containers only:

**SSO Filtering Objects**

Name/DN	Type	Actions
saml_users	Group	

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**.

### Service Provider Configuration

Select the configuration method specified by Service Provider, and then follow the instructions.

- ☒ Metadata  
☐ Manual Configuration

#### Metadata

Use one of the following methods to import SP Metadata given by your Service Provider.

URL

File

XML 

```
<?xml version="1.0"?>
<md:EntityDescriptor
xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
validUntil="2018-08-30T18:06:23Z"
cacheDuration="PT604800S"
entityID="http://fac.school.net/metadata/">
```



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**.

**Settings**

[Learn more](#)

**Description**

Name \*

SAML-FortiAuthenticator


Description

SSO connector for FortiAuthenticator Portal.

Category \*

Other

Logo

 [Browse](#)

Recommended image size is 180 x 180

**Advanced**

Application ID ⓘ

☒ Show in user app list ⓘ

**Save** **Cancel**

## 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**.

New Single Sign-On Server

Type: Poll Active Directory Server  
**Fortinet Single-Sign-On Agent**  
 RADIUS Single-Sign-On Agent

Name: fac-fsso

Primary FSSO Agent: 172.25.176.141 - ..... +

Collector Agent AD access mode: **Standard** Advanced

Users/Groups ⓘ 0 View

Apply & Refresh OK Cancel

- 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.
- 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**.

Edit User Group

Name: fac-saml

Type: Firewall  
**Fortinet Single Sign-On (FSSO)**  
 RADIUS Single Sign-On (RSSO)  
 Guest

Members: SAML\_USERS +

OK Cancel

## Configuring captive portal and security policies

- 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.

**Admission Control**

Security Mode: Captive Portal

Authentication Portal: Local External <https://fac.school.net/login/saml-auth>

User Access ⓘ: Restricted to Groups Allow all

User Groups: Guest-group +

Customize Portal Messages ☐

Exempt Sources: +

Exempt Destinations/Services: +

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

**New Address**

Category: Address IPv6 Address Multicast Address Proxy Address

Name: FAC-172.25.176.141

Color: Change

Type: Subnet

Subnet / IP Range: 172.25.176.141

Interface: ☐ any

Show in Address List: ☒

Static Route Configuration: ☐

Comments:  0/255

**Tags**

Add Tag Category

OK Cancel

Then create an FQDN object of your Centrify tenant portal:

- <your-tenant-id>.my.centify.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

☒

New Policy

Name 	<input type="text" value="fssso"/>		
Incoming Interface	 internal	+	
Outgoing Interface	 wan1	+	
Source	<div style="display: flex; justify-content: space-between;"> <div> all</div> <div></div> </div> <div style="display: flex; justify-content: space-between;"> <div> fac-saml</div> <div></div> </div> <div style="text-align: center;">+</div>		
Destination	<div style="display: flex; justify-content: space-between;"> <div> all</div> <div></div> </div> <div style="text-align: center;">+</div>		
Schedule	<div style="display: flex; justify-content: space-between;"> always </div>		
Service	<div style="display: flex; justify-content: space-between;"> <div> ALL</div> <div></div> </div> <div style="text-align: center;">+</div>		
Action	<div style="display: flex; justify-content: space-around;"> <div style="background-color: #28a745; color: white; padding: 5px 10px; border: 1px solid #28a745;"> ACCEPT</div> <div style="color: red; padding: 5px 10px; border: 1px solid red;"> DENY</div> <div style="color: #ffc107; padding: 5px 10px; border: 1px solid #ffc107;"> LEARN</div> <div style="color: #6c757d; padding: 5px 10px; border: 1px solid #6c757d;"> IPsec</div> </div>		

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
```

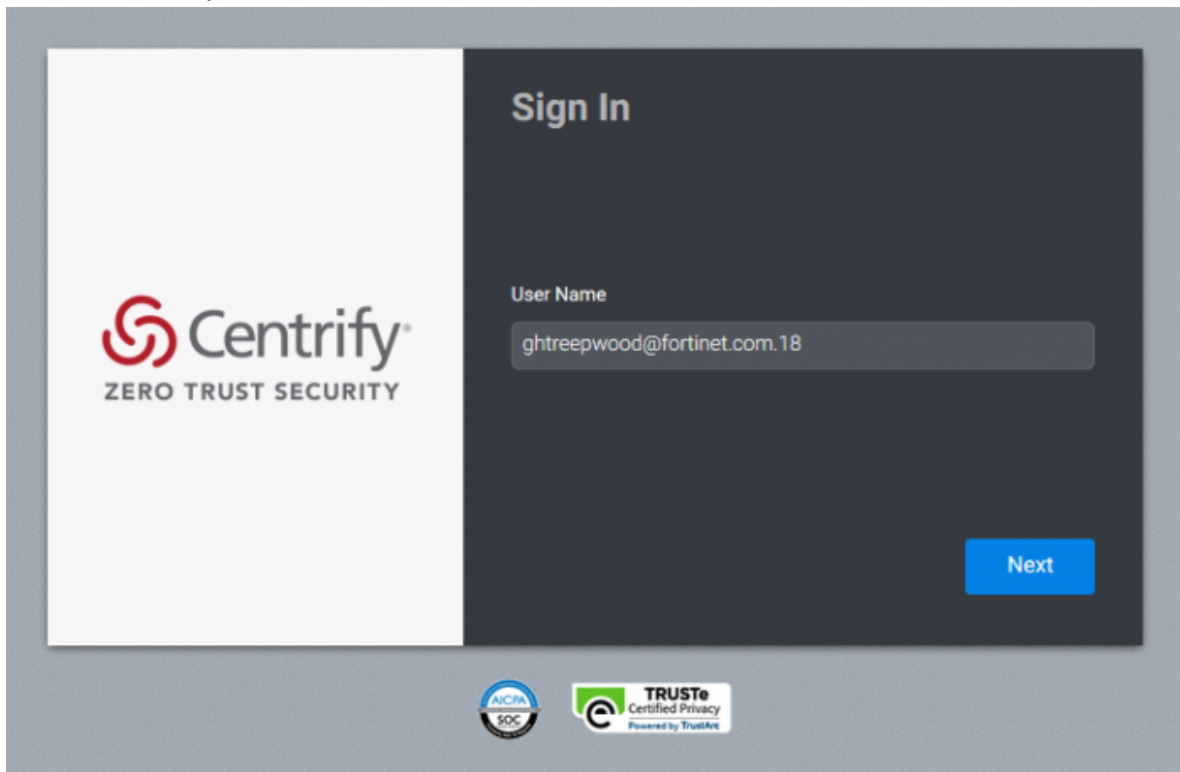
This command exempts users of these policies from the captive portal interface.

## 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.

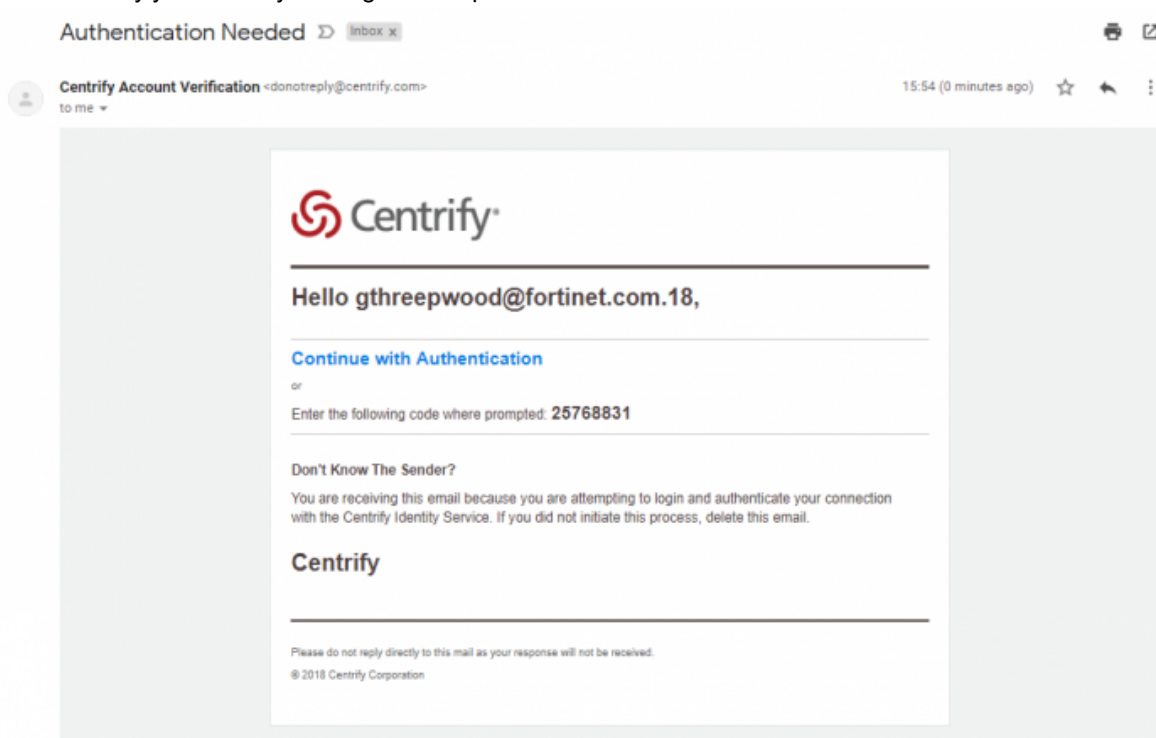
Alternatively, you can directly navigate to the portal URL.

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



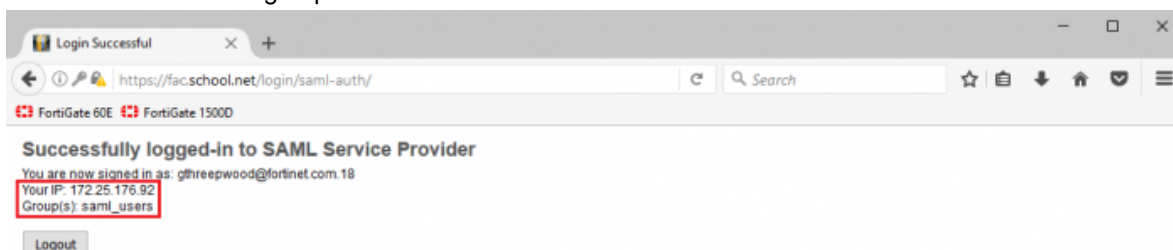
The image shows the Centrify Sign In page. On the left is the Centrify logo with the tagline 'ZERO TRUST SECURITY'. On the right, under the heading 'Sign In', there is a 'User Name' field containing the text 'gthreepwood@fortinet.com.18'. Below the field is a blue 'Next' button. At the bottom of the page, there are two circular logos: 'AICPA SOC' and 'TRUSTe Certified Privacy Powered by TrueArc'.

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.





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



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

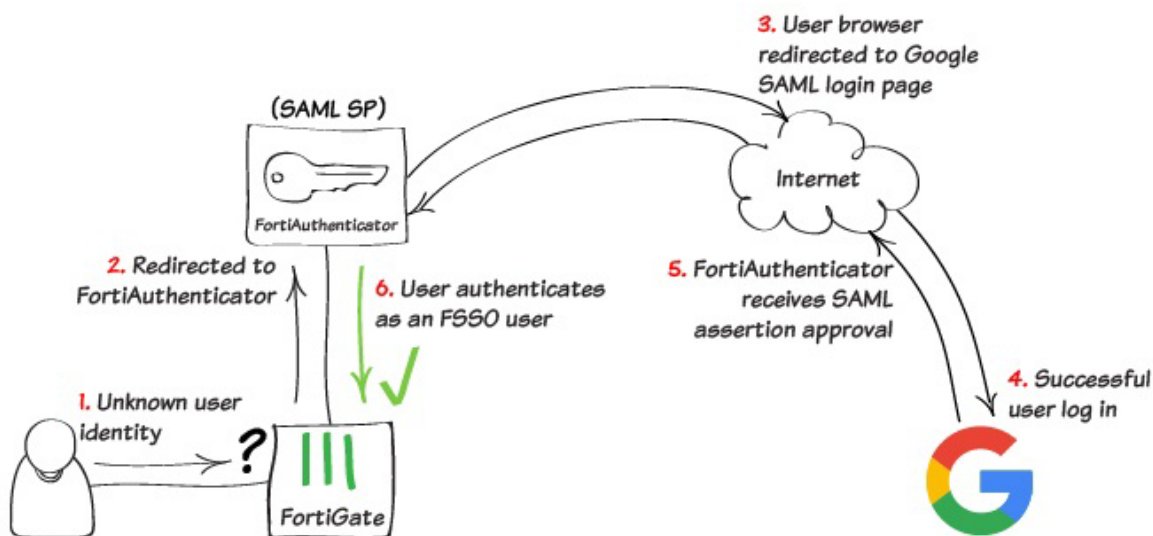
Logon Time	Update Time	Workstation	IP address	Domain	Username	Source	Group
Tue Aug 28 15:55:14 2018	Tue Aug 28 15:55:14 2018	172.25.176.92	172.25.176.92	SSO_EXT_USER	GTHREEPWOOD	SAML	GTHREEPWOOD-SAML_USERS

1 SSO session

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

User Name	User Group	Duration	IP Address	Traffic Volume	Method
GTHREEPWOOD	fac-saml	2 minute(s) and 3 second(s)	172.25.176.92	0 B	Fortinet Single Sign-On

## SAML 2.0 FSSO with FortiAuthenticator and Google G Suite



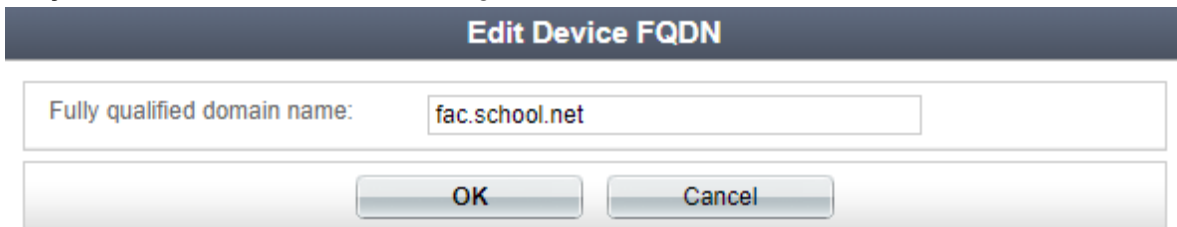
In this example, you provide a Security Assertion Markup Language (SAML) FSSO cloud authentication solution using FortiAuthenticator in conjunction with Google G Suite. The FortiAuthenticator acts as the authentication Service Provider (SP) and Google as the Identity Provider (IdP).

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**.

System Information	
Host Name	fac.school.net [Change]
Device FQDN	fac.school.net [Change]
Serial Number	FAC2HD3A15000126
System Time	Tue Jun 26 08:51:00 2018 [Change]
Firmware Version	v5.3.1, build0242 (GA) [Upgrade]
System Configuration	Last Backup: Thu May 24 12:24:44 2018 [Backup/Restore]
Current Administrator	admin
Uptime	12 day(s) 21 hour(s) 33 minute(s)
Shutdown / Reboot	[Reboot] [Shutdown]

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.

Edit SSO Configuration	
FortiGate	
Listening port:	<input type="text" value="8000"/>
<input checked="" type="checkbox"/> Enable authentication	
Secret key:	<input type="text" value="....."/>
Login expiry:	<input type="text" value="480"/> minutes
Extend user session beyond logoff by:	<input type="text" value="0"/> seconds (0-3600)
<input type="checkbox"/> Enable NTLM authentication	

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).

**Edit SAML Portal Settings**

☒ Enable SAML portal

Device FQDN: fac.school.net

Portal URL: https://fac.school.net/login/saml-auth

Entity ID: http://fac.school.net/metadata/

ACS (login) URL: https://fac.school.net/saml/?acs

[\[Download SP metadata\]](#) [\[Import IDP metadata\]](#) [\[Import IDP certificate\]](#)

IDP entity id:

IDP single sign-on URL:

IDP certificate fingerprint:

Fingerprint algorithm: SHA-256

☐ Enable SAML single logout

☐ Sign SAML requests with a local certificate

Obtain group membership from:

☒ SAML assertions:

☐ "In\_<group>" boolean assertions

☒ Text-based list Memberof

☐ Azure

☐ LDAP lookup

☐ Implicit group membership

OK Cancel

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**.

The screenshot shows the Google Admin console interface. At the top, there's a blue header with the Google Admin logo, a search bar, and user information. Below the header, a welcome message says "Welcome to Admin console" with a "START SETUP" button. The main area displays a grid of admin tools: Dashboard, Users, Groups, Device management, Apps (highlighted with a red box), Billing, Company profile, Admin roles, Domains, Data migration, and Support. The Apps section is titled "APPS SETTINGS" and "Marketplace settings". It contains four cards: "G Suite" (11 items), "Additional Google services" (45 items), "Marketplace apps" (0 items), and "SAML apps" (0 items, highlighted with a red box). The SAML apps card includes the text "Manage SSO and User Provisioning".

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

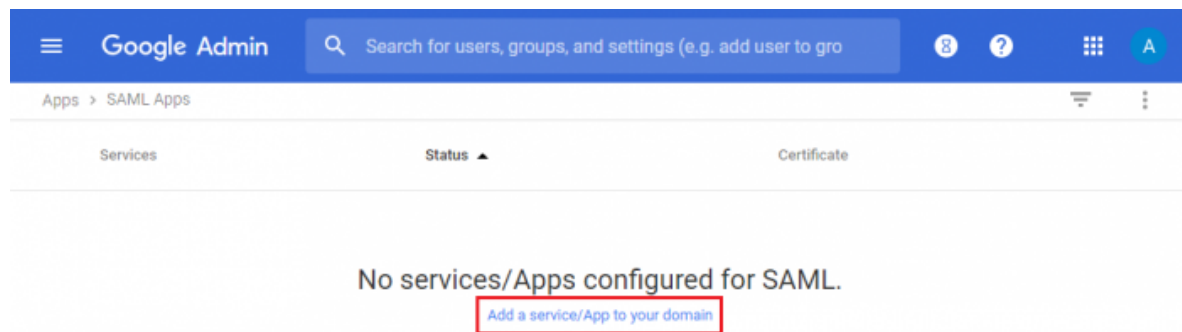
Marketplace settings

**11**  
G Suite  
Gmail, Calendar, Drive & more  
These services are governed by your G Suite agreement.

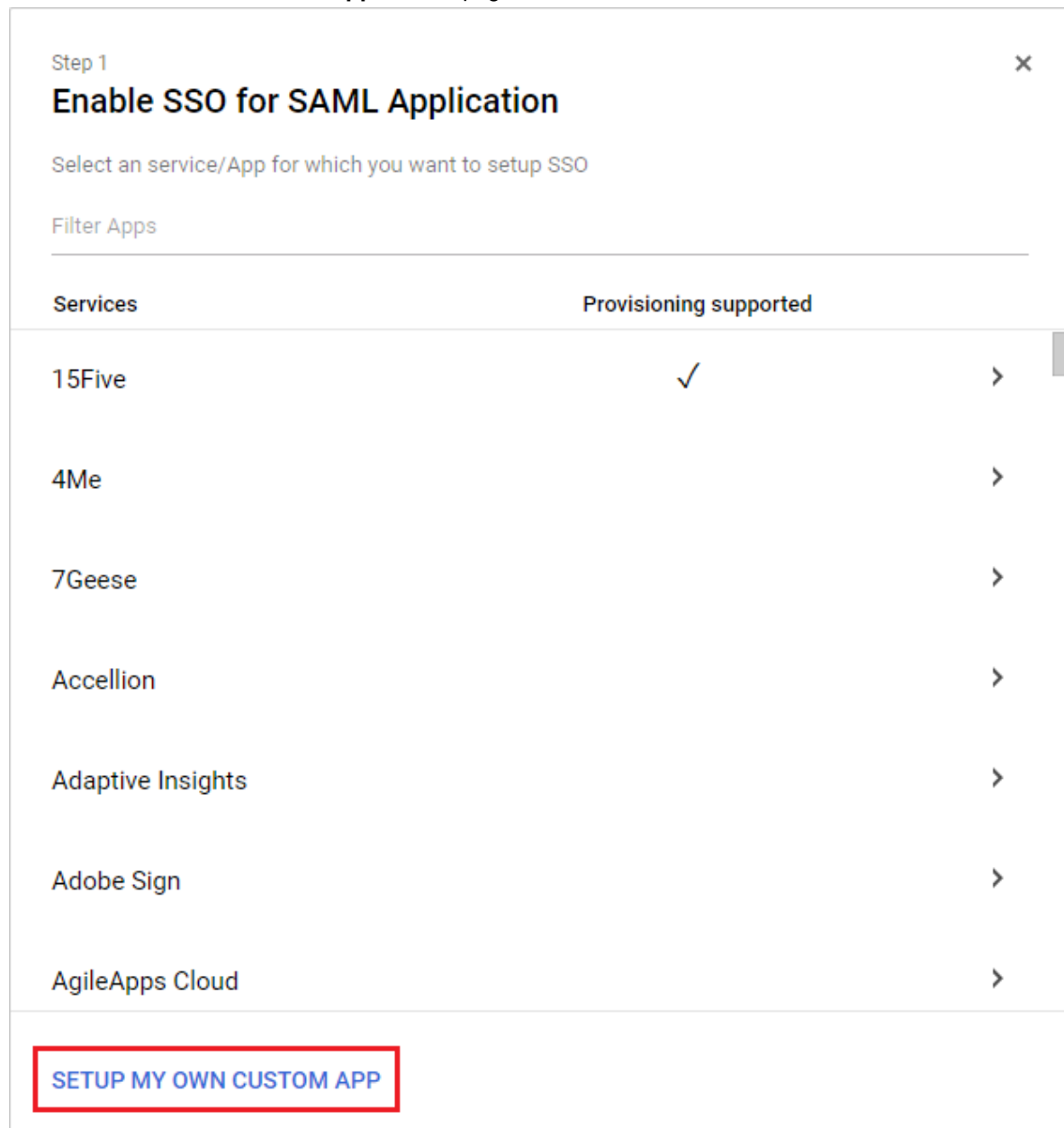
**45**  
Additional Google services  
Blogging, photos, video, social tools and more  
These services are not governed by your G Suite agreement, and other terms apply. [Learn more](#)

**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**.

Step 2 of 5

Google IdP Information

Choose from either option to setup Google as your identity provider. Please add details in the SSO config for the service provider. [Learn more](#)

Option 1

SSO URL

https://accounts.google.com/o/saml2/idp?idpid=C02x1byzz

Entity ID

https://accounts.google.com/o/saml2?idpid=C02x1byzz

Certificate

Google\_2023-6-20-113748\_SAML2.0

Expires Jun 20, 2023

DOWNLOAD

OR

Option 2

IDP metadata

DOWNLOAD

PREVIOUS

CANCEL

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.

Step 3 of 5

✕

## Basic information for your Custom App

Please provide the basic information needed to configure your Custom App. This information will be viewed by end-users of the application.

Application Name \*

FortiAuthenticator

app-id:  
fortiauthenticator

Description

Welcome! Please provide valid credentials to log in

Upload logo

📎 CHOOSE FILE

logo.jpg7.36 KB

This logo will be displayed for all users who have access to this application. Please upload a .png or .gif image of size 256 x 256 pixels.

PREVIOUS

CANCEL

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**.



Step 4 of 5

×

## Service Provider Details

Please provide service provider details to configure SSO for your Custom App. The ACS url and Entity ID are mandatory.

ACS URL *	https://fac.school.net/saml/?acs	
Entity ID *	http://fac.school.net/metadata	
Start URL	http://fac.school.net/login/saml-auth	
Signed Response	<input type="checkbox"/>	
Name ID	Basic Information ▼	Primary Email ▼
Name ID Format	UNSPECIFIED ▼	

PREVIOUS

CANCEL

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**.

Step 5 of 5

×

## Attribute Mapping

Provide mappings between service provider attributes to available user profile fields.

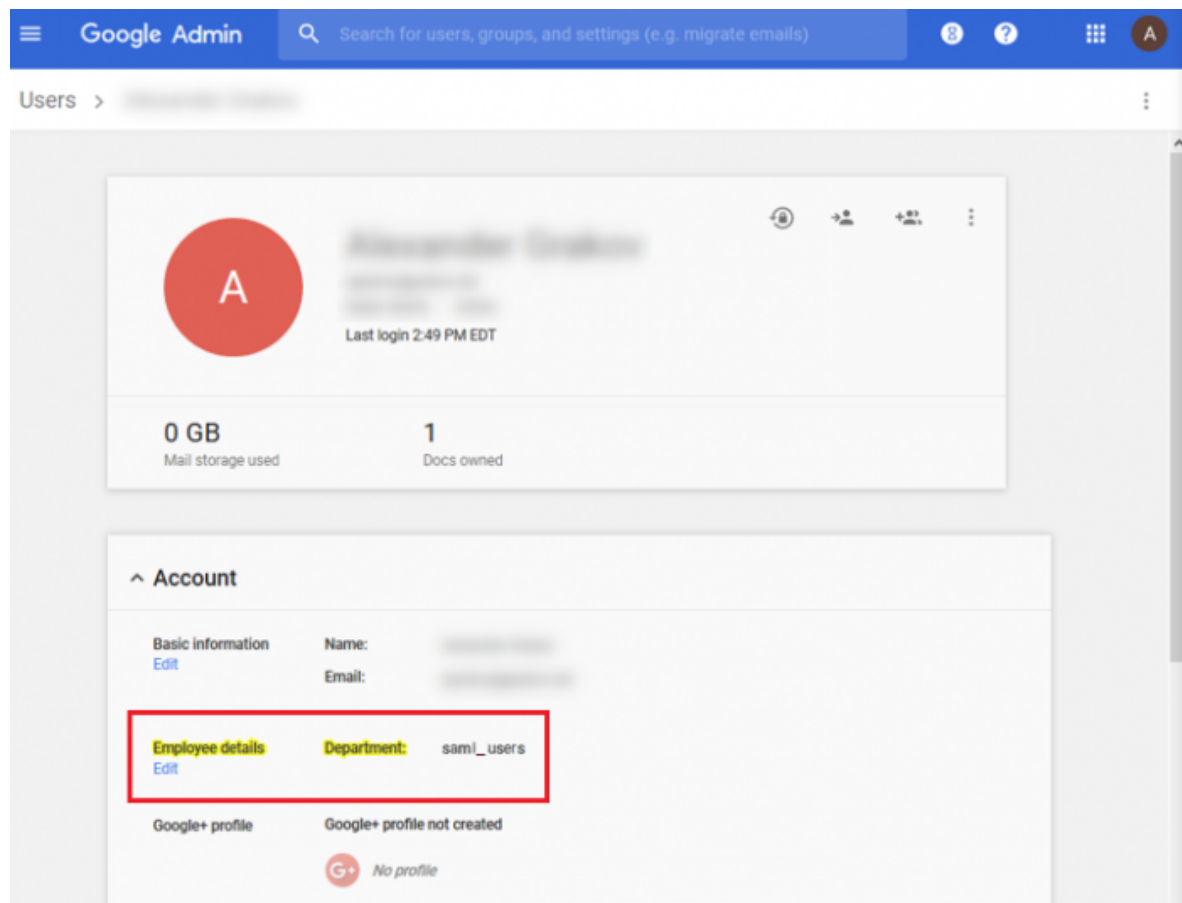
FirstName	Basic Information ▼	First Name ▼
LastName	Basic Information ▼	Last Name ▼
Email	Basic Information ▼	Primary Email ▼
Memberof	Employee Details ▼	Department ▼

ADD NEW MAPPING

PREVIOUS

CANCEL 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.

**Edit SAML Portal Settings**

✓ Successfully saved SAML Portal Settings.

☒ Enable SAML portal

Device FQDN: fac.school.net

Portal URL: https://fac.school.net/login/saml-auth

Entity ID: http://fac.school.net/metadata/

ACS (login) URL: https://fac.school.net/saml/?acs

[Download SP metadata] [Import IDP metadata] [Import IDP certificate]

IDP entity id:  
https://accounts.google.com/o/saml2?idpid=C012cnpc9

IDP single sign-on URL:  
https://accounts.google.com/o/saml2?idp?idpid=C012cnpc9

IDP certificate fingerprint:  
b4404ea2b58c553489c54301eded5e1c9f1e6099781243a730f9a11b95e0521d

Fingerprint algorithm: SHA-256

☐ Enable SAML single logout

☐ Sign SAML requests with a local certificate

Obtain group membership from:
 

- ☒ SAML assertions:
  - ☐ "In\_<group>" boolean assertions
  - ☒ Text-based list Memberof
- ☐ Azure
- ☐ LDAP lookup

☐ Implicit group membership

OK Cancel

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.

**Edit FortiGate Filter**

✓ Successfully added FortiGate filter "saml\_users (172.25.176.92)". You may edit it again below.

Name:

FortiGate name/IP:

Description:

**IP Filtering**

☐ Enable IP filtering for this service.

**Fortinet Single Sign-On (FSSO)**

☒ Forward FSSO information for users from the following subset of users/groups/containers only:

**SSO Filtering Objects**

Name/DN	Type	Actions
saml_users	Group	

## Configuring FSSO on the FortiGate

- 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**.

New Single Sign-On Server

Type:

Name:

Primary FSSO Agent:  -

Collector Agent AD access mode:

Users/Groups



- 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.

- 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**.

Edit User Group

Name

Type

Members    



## Configuring Captive Portal and security policies



- 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.

Admission Control

Security Mode

Authentication Portal

User Access 

User Groups    


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

New Address

Category

Address

IPv6 Address

Multicast Address

Proxy Address

Name

FAC-172.25.176.141

Color

Change

Type

Subnet

Subnet / IP Range

172.25.176.141

Interface

any

Show in Address List

☒

Static Route Configuration

☐

Comments

0/255

Tags

Add Tag Category

OK

Cancel

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 an 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 ⓘ  
Incoming Interface  
Outgoing Interface  
Source  
Destination  
Schedule  
Service  
Action

g.suite-bypass

internal

+

×

wan1

+

×

all

+

×

g.suite-bypass

+

×

always

▼

ALL

+

×

✓ ACCEPT

⊘ DENY

🎓 LEARN

💻 IPsec

Firewall / Network Options

NAT

🟢

FortiAuthenticator Cookbook

Fortinet Technologies Inc.

New Policy

Name	<input type="text" value="fsso"/>		
Incoming Interface	<div style="display: flex; align-items: center;">  internal         </div> <div style="text-align: center; margin-top: 5px;">+</div>		✕
Outgoing Interface	<div style="display: flex; align-items: center;">  wan1         </div> <div style="text-align: center; margin-top: 5px;">+</div>		✕
Source	<div style="display: flex; align-items: center;">  all         </div> <div style="display: flex; align-items: center; margin-top: 5px;">  saml-users         </div> <div style="text-align: center; margin-top: 5px;">+</div>		✕ ✕
Destination	<div style="display: flex; align-items: center;">  all         </div> <div style="text-align: center; margin-top: 5px;">+</div>		✕
Schedule	<div style="display: flex; align-items: center;">  always         </div> <div style="text-align: right; margin-top: 5px;">▼</div>		
Service	<div style="display: flex; align-items: center;">  ALL         </div> <div style="text-align: center; margin-top: 5px;">+</div>		✕
Action	<div style="display: flex; gap: 10px;"> <div style="background-color: #28a745; color: white; padding: 5px 10px; border: 1px solid #28a745;">✓ ACCEPT</div> <div style="color: red; padding: 5px 10px; border: 1px solid red;">✗ DENY</div> <div style="color: blue; padding: 5px 10px; border: 1px solid blue;">🎓 LEARN</div> <div style="color: grey; padding: 5px 10px; border: 1px solid grey;">💻 IPsec</div> </div>		

Firewall / Network Options

NAT ON

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
```

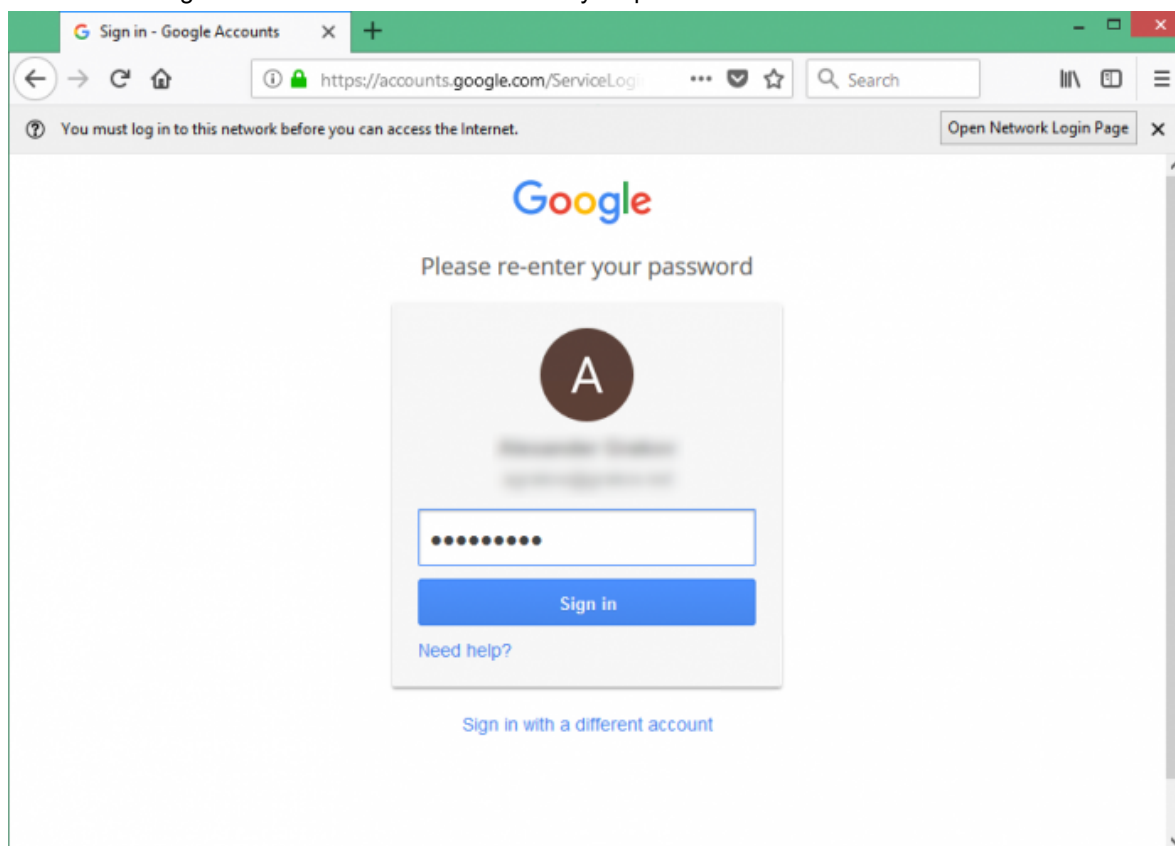
This command exempts users of these policies from the captive portal interface.

## Results

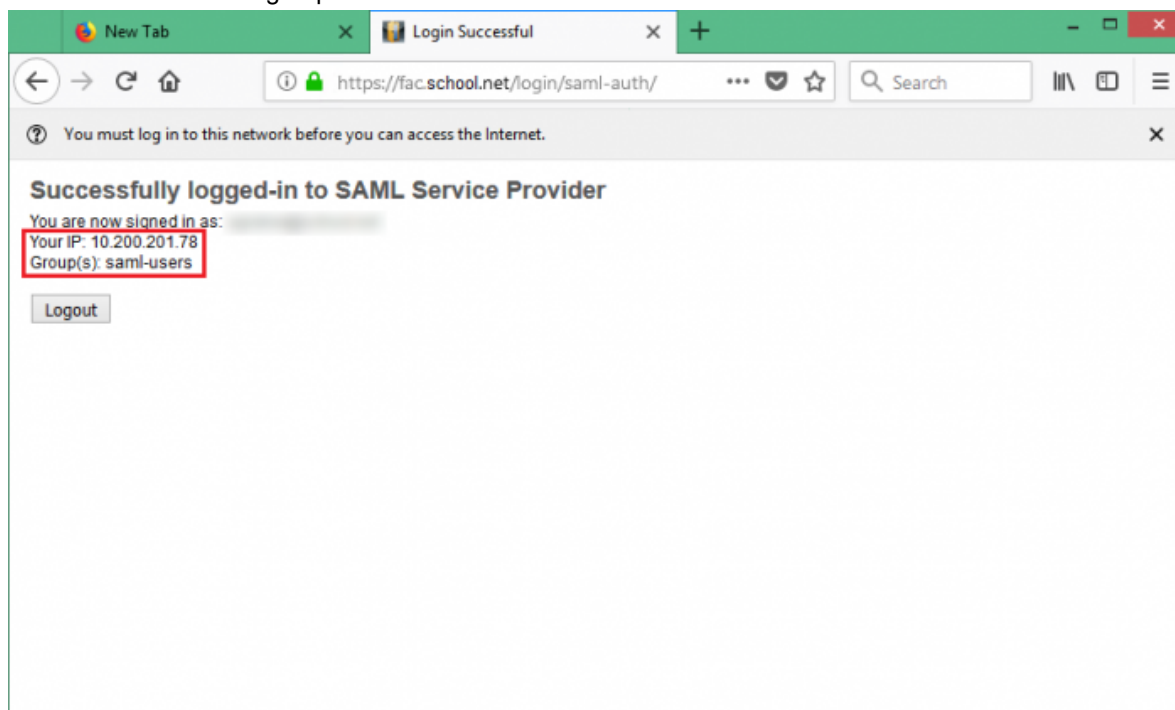
To test the connection, open a new browser window and attempt to browse the Internet. The browser redirects to the FortiAuthenticator SAML portal, which pushes the browser to the SAML IdP.

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.

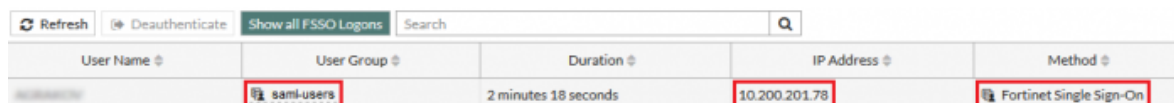


3. View user information including IP address and user group on the FortiAuthenticator under **Monitor > SSO > SSO Sessions**.



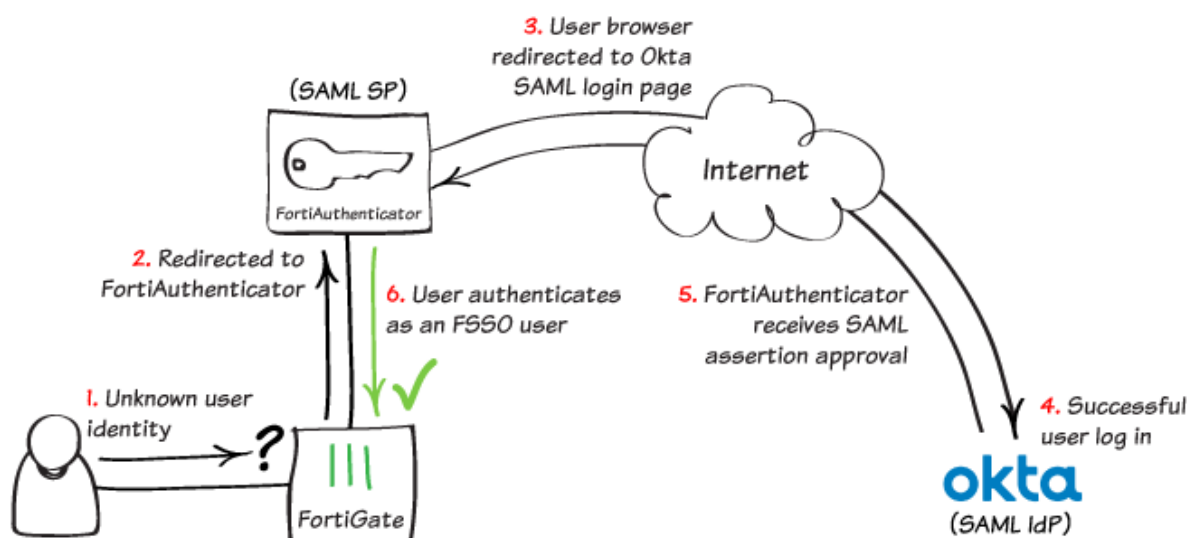
Logon Time	Update Time	Workstation	IP address	Domain	Username	Source	Group
Tue Jan 26 07:55:21 2018	Tue Jan 26 07:55:21 2018	10.200.201.78	10.200.201.78	SSO_EXT_USER		SAML	SAML-USERS

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



User Name	User Group	Duration	IP Address	Method
	saml-users	2 minutes 18 seconds	10.200.201.78	Fortinet Single Sign-On

## 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.



**Edit Device FQDN**

Fully qualified domain name:

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.

System Information	
Host Name	fac.school.net [Change]
Device FQDN	fac.school.net [Change]
Serial Number	FAC2HD3A15000126
System Time	Thu Jun 8 10:12:06 2017 [Change]
Firmware Version	v4.00-build0222-20170420-patch00 [Upgrade]
System Configuration	Last Backup: Thu Apr 27 11:35:02 2017 [Backup/Restore]
Current Administrator	admin
Uptime	41 day(s) 22 hour(s) 34 minute(s)
Shutdown / Reboot	[Reboot] [Shutdown]

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.

FortiGate	
Listening port:	<input type="text" value="8000"/>
<input checked="" type="checkbox"/> Enable authentication	
Secret key:	<input type="password" value="....."/>
Login expiry:	<input type="text" value="480"/> minutes
Extend user session beyond logoff by:	<input type="text" value="0"/> seconds (0-3600)
<input type="checkbox"/> Enable NTLM authentication	

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.

**Edit SAML Portal Settings**

☒ Enable SAML portal

Device FQDN: fac.school.net

Portal url: https://fac.school.net/login/saml-auth

Entity id: http://fac.school.net/metadata/

ACS (login) url: https://fac.school.net/saml/?acs

[\[Download SP metadata\]](#) [\[Import IDP metadata\]](#) [\[Import IDP certificate\]](#)

IDP entity id:

IDP single sign-on URL:

IDP certificate fingerprint:

Fingerprint algorithm: Unknown

☐ Enable SAML single logout

☐ Sign SAML requests with a local certificate

Obtain group membership from:

- ☒ SAML assertions:
  - ☒ "In\_<group>" boolean assertions
  - ☐ Text-based list: memberof
- ☐ Azure
- ☐ LDAP lookup

☒ Implicit group membership: saml\_users ▼

OK Cancel

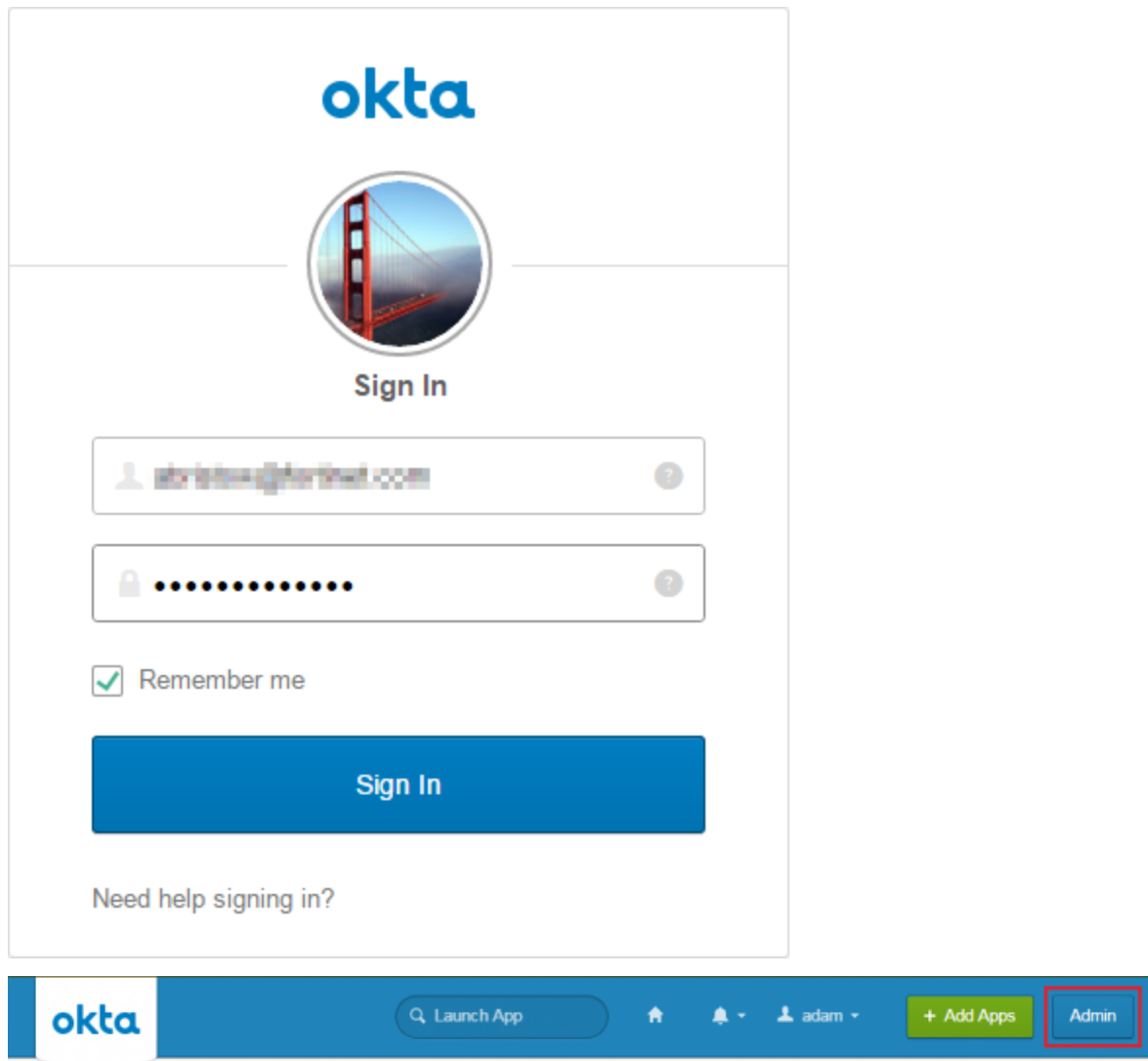
Keep this window open as these URLs will be needed during the IdP application configuration and for testing.

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.

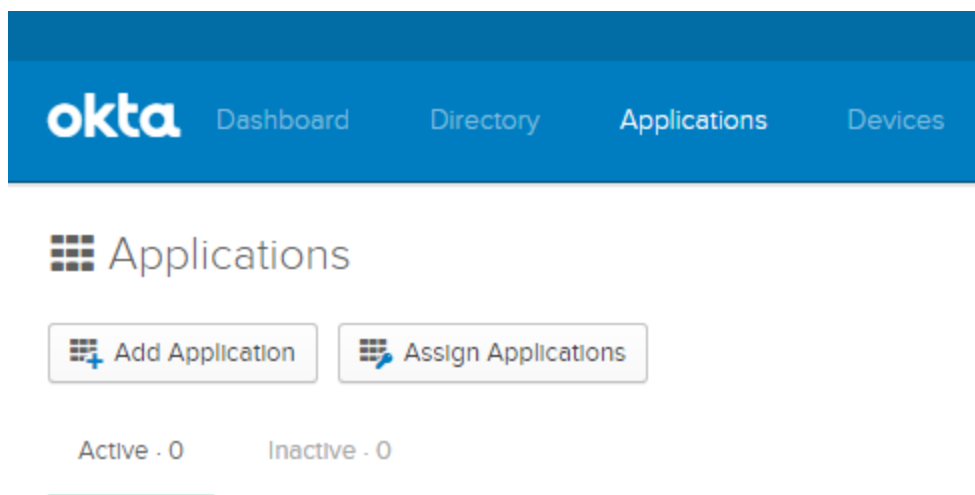


## Configuring the Okta developer account IDP application

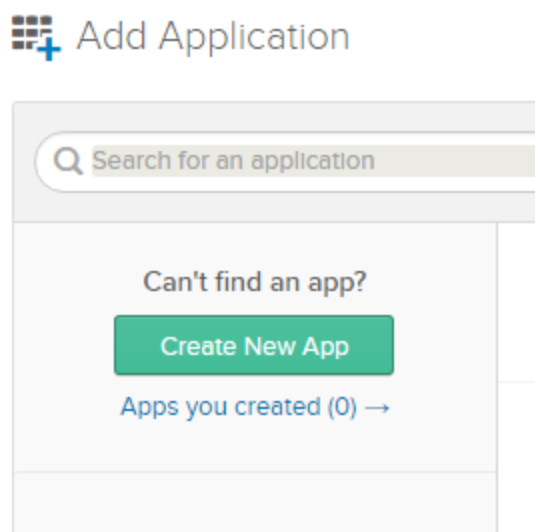
1. Open a browser, log in to your Okta developer account, and select Admin under your user settings.

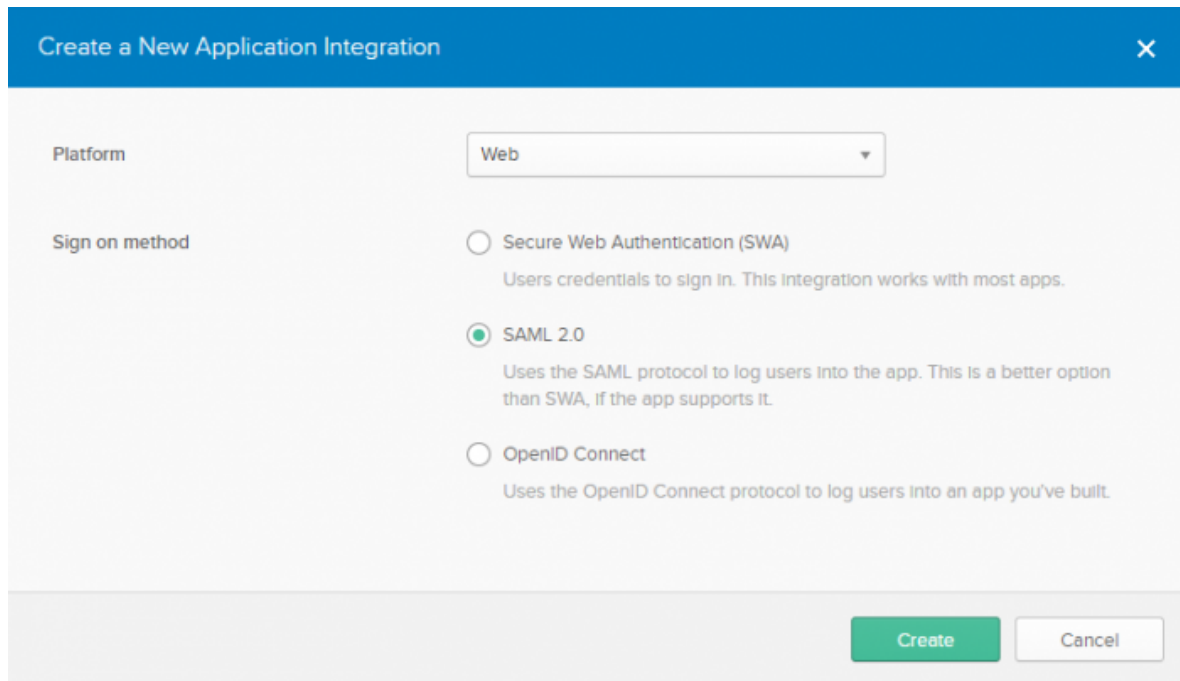


2. Go to the **Applications** tab and select **Add Application**.



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



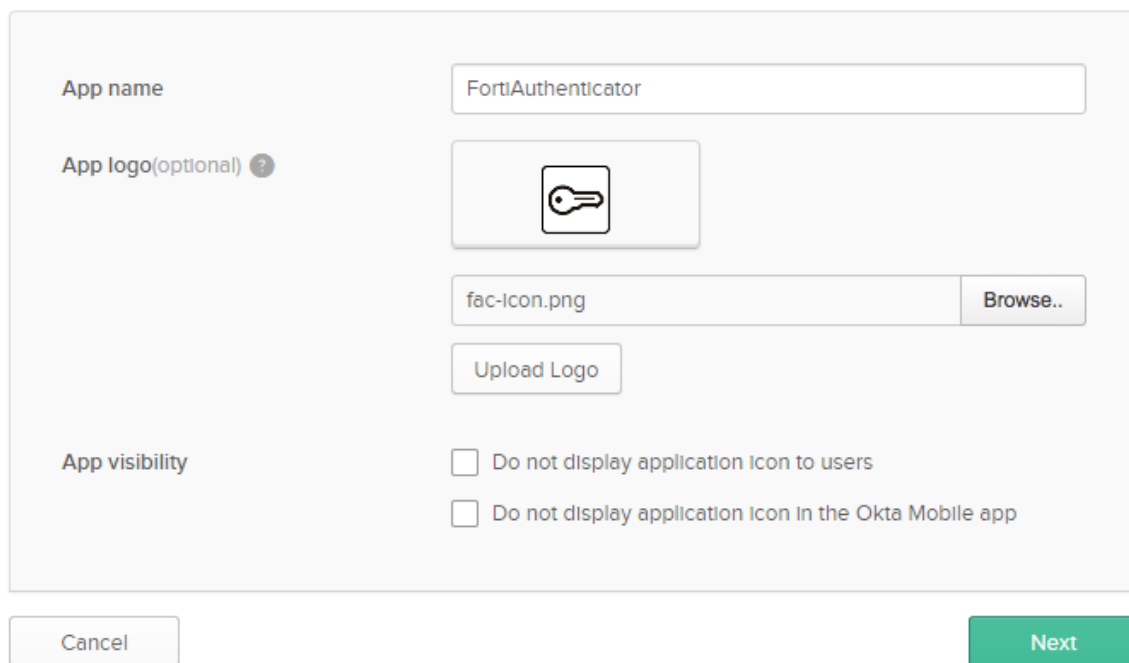


The dialog box is titled "Create a New Application Integration" with a close button (X) in the top right corner. It contains two main sections. The first section, "Platform", has a dropdown menu currently set to "Web". The second section, "Sign on method", contains three radio button options: "Secure Web Authentication (SWA)" with the description "Users credentials to sign in. This integration works with most apps.", "SAML 2.0" (which is selected) with the description "Uses the SAML protocol to log users into the app. This is a better option than SWA, if the app supports it.", and "OpenID Connect" with the description "Uses the OpenID Connect protocol to log users into an app you've built.". At the bottom right, there are two buttons: "Create" (in green) and "Cancel" (in white).

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.

## Create SAML Integration

### 1 General Settings



The form is titled "General Settings" and contains several fields. The "App name" field is a text input containing "FortiAuthenticator". The "App logo(optional) ?" field is a file upload area showing a key icon, the filename "fac-icon.png", a "Browse.." button, and an "Upload Logo" button. The "App visibility" section has two checkboxes: "Do not display application icon to users" and "Do not display application icon in the Okta Mobile app", both of which are currently unchecked. At the bottom, there are two buttons: "Cancel" (in white) and "Next" (in green).


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.


**A** SAML Settings


**GENERAL**

Single sign on URL 


☒ Use this for Recipient URL and Destination URL


☐ Allow this app to request other SSO URLs

Audience URI (SP Entity ID) 

Default RelayState 




If no value is set, a blank RelayState is sent

Name ID format 

Application username 

[Show Advanced Settings](#)

**ATTRIBUTE STATEMENTS (OPTIONAL)** [LEARN MORE](#)

Name	Name format (optional)	Value	
FirstName	Unspecified	user.firstName	
LastName	Unspecified	user.lastName	
Email	Unspecified	user.email	

[Add Another](#)

**What does this form do?**  
This form generates the XML needed for the app's SAML request.

**Where do I find the info this form needs?**  
The app you're trying to integrate with should have its own documentation on using SAML. You'll need to find that doc, and it should outline what information you need to specify in this form.

**Okta Certificate**  
Import the Okta certificate to your Identity Provider if required.

[Download Okta Certificate](#)

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


### 3 Help Okta Support understand how you configured this application


Are you a customer or partner?

☒ I'm an Okta customer adding an Internal app

☐ I'm a software vendor. I'd like to integrate my app with Okta

---

 The optional questions below assist Okta Support in understanding your app integration.

App type 

☒ This is an internal app that we have created

[Previous](#) [Finish](#)

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

FortiAuthenticator

Active View Logs

General Sign On Import Assignments

Settings Edit

**SIGN ON METHODS**

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.

☒ SAML 2.0

Default Relay State

SAML 2.0 is not configured until you complete the setup instructions.

View Setup Instructions

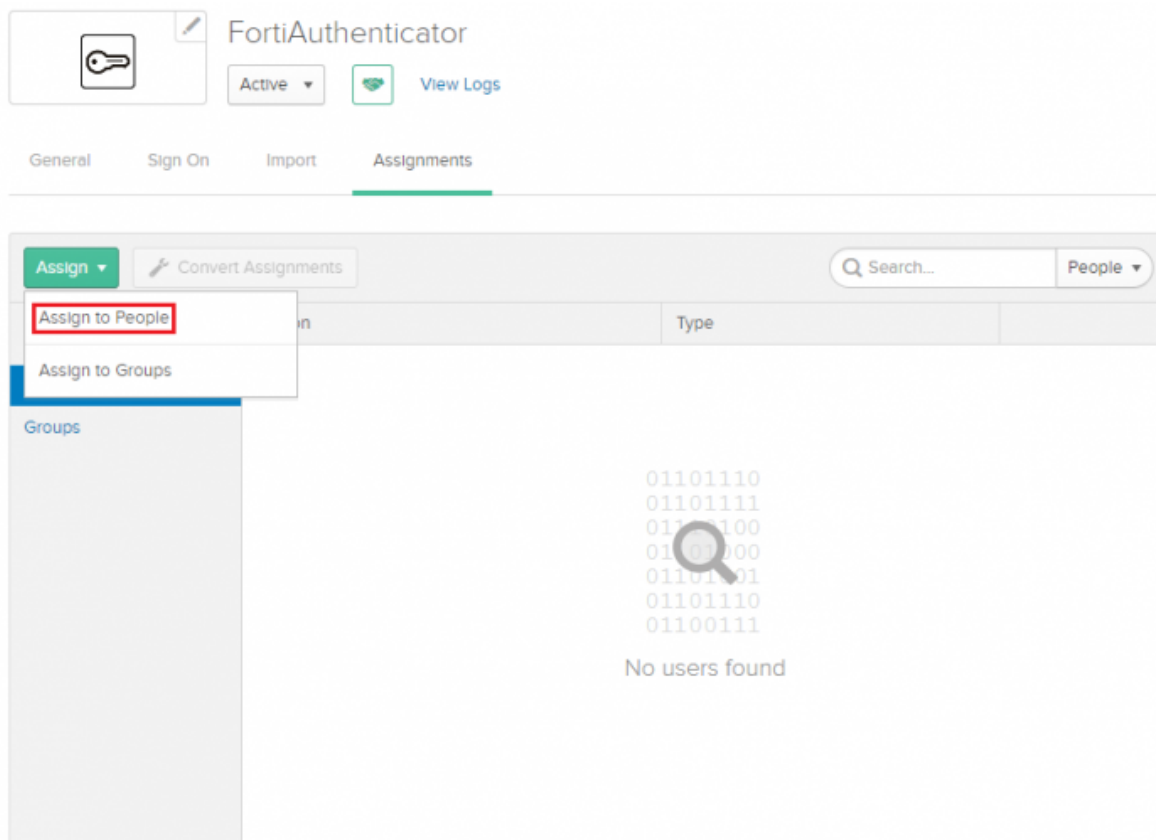
**Identity Provider metadata** is available if this application supports dynamic configuration.

**CREDENTIALS DETAILS**

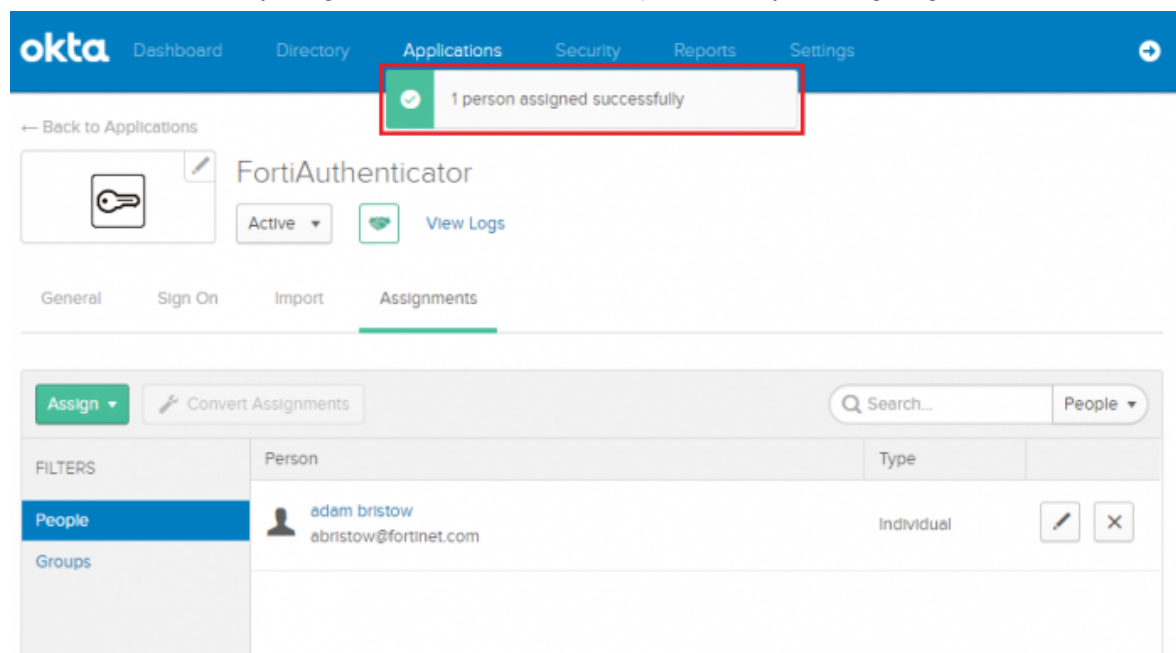
Application username format Email

Password reveal ☐ Allow users to securely see their password (Recommended)

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.

**Edit SAML Portal Settings**

✓ Successfully saved SAML Portal Settings.

☒ Enable SAML portal

Device FQDN: fac.school.net

Portal url: https://fac.school.net/login/saml-auth

Entity id: http://fac.school.net/metadata/

ACS (login) url: https://fac.school.net/saml?acs

[Download SP metadata] [Import IDP metadata] [Import IDP certificate]

IDP entity id: http://www.okta.com/exkar3wdtyGklierIK0h7

IDP single sign-on URL: https://dev-241684.oktapreview.com/app/fortinetdev241684\_fortiauthenticator\_1/exkar3wdtyGklierIK0h7/sso/saml

IDP certificate fingerprint: 2f8087c3d42ff153f8ae55fc7715afe0eae1beb099ee0763656fb3e841dccc8

Fingerprint algorithm: SHA-256

☐ Enable SAML single logout

☐ Sign SAML requests with a local certificate

Obtain group membership from: ☒ SAML assertions:

☒ "In\_<group>" boolean assertions

☐ Text-based list

☐ Azure

☐ LDAP lookup

☒ Implicit group membership: saml\_users

OK Cancel

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.

**Edit FortiGate Filter**

✓ Successfully added FortiGate filter "saml\_users (172.25.176.92)". You may edit it again below.

Name:

FortiGate name/IP:

Description:

**IP Filtering**

☐ Enable IP filtering for this service.

**Fortinet Single Sign-On (FSSO)**

☒ Forward FSSO information for users from the following subset of users/groups/containers only:

**SSO Filtering Objects**

Name/DN	Type	Actions
saml_users	Group	

## Configuring FSSO on the FortiGate

- 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.

**New Single Sign-On Server**

Type: Poll Active Directory Server **Fortinet Single-Sign-On Agent** RADIUS Single-Sign-On Agent

Name:

Primary FSSO Agent:  -

Collector Agent AD access mode: **Standard** Advanced

Users/Groups 0

- 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.

<div> <div>+ Create New</div> <div>Edit</div> <div>Delete</div> </div>						
Name	Type	LDAP Server	Users/Groups	FSSO Agent IP/Name	Status	Ref.
fac-fsso	FSSO		172.25.176.141 (1)	172.25.176.141	✓	1

Users/Groups

172.25.176.141

SAML\_USERS

- 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**.

Edit User Group

Name

fac-saml

Type

Firewall

Fortinet Single Sign-On (FSSO)

RADIUS Single-Sign-On (RSSO)

Guest

Members

SAML\_USERS

+

OK

Cancel

## Configuring Captive Portal and security policies

- 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.

Admission Control

Security Mode

Captive Portal

Authentication Portal

Local

External

https://fac.school.net/login/saml-auth

User Access

Restricted to Groups

Allow all

User Groups

local

+

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

New Address

Category

AddressIPv6 AddressMulticast AddressProxy Address

Name

FAC-172.25.176.141

Type

IP/Netmask

Subnet / IP Range

172.25.176.141

Interface

☐ any

Show in Address List

☒

Static Route Configuration

☐

Comments

0/255

OK

Cancel








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 	<input type="text" value="dns"/>		
Incoming Interface	 internal	+	✕
Outgoing Interface	 wan1	+	✕
Source	 all	+	✕
Destination	 all	+	✕
Schedule	 always ▼		
Service	 DNS	+	✕
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY <input type="checkbox"/> LEARN <input type="checkbox"/> 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	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY <input type="checkbox"/> LEARN <input type="checkbox"/> IPsec		

Firewall / Network Options

NAT ☒









New Policy

Name ⓘ	okta-bypass		
Incoming Interface	 internal	+	×
Outgoing Interface	 wan1	+	×
Source	 all	+	×
Destination	 dev-241684-admin.oktapreview.c  eum-col.appdynamics.com  login.okta.com  ocsp.digicert.com  op1static.oktacdn.com	+	×
Schedule	 always		▼
Service	 ALL	+	×
Action	<input checked="" type="checkbox"/> ACCEPT	<input type="checkbox"/> DENY	<input type="checkbox"/> LEARN <input type="checkbox"/> IPsec

Firewall / Network Options

NAT ☒

New Policy

Name 	<input type="text" value="fssso"/>		
Incoming Interface	 internal	+	✕
Outgoing Interface	 wan1	+	✕
Source	<div style="display: flex; align-items: center;">  all         </div> <div style="display: flex; align-items: center;">  fac-saml         </div> <div style="text-align: center;">+</div> <div style="text-align: right;">✕</div>		
Destination	<div style="display: flex; align-items: center;">  all         </div> <div style="text-align: center;">+</div> <div style="text-align: right;">✕</div>		
Schedule	<div style="display: flex; align-items: center;">  always         </div> <div style="text-align: right;">▼</div>		
Service	<div style="display: flex; align-items: center;">  ALL         </div> <div style="text-align: center;">+</div> <div style="text-align: right;">✕</div>		
Action	<div style="display: flex; gap: 5px;"> <div style="background-color: #28a745; color: white; padding: 2px 10px; border: 1px solid #28a745;">✓ ACCEPT</div> <div style="color: red; padding: 2px 10px; border: 1px solid red;">✗ DENY</div> <div style="color: #6c757d; padding: 2px 10px; border: 1px solid #6c757d;">🎓 LEARN</div> <div style="color: #6c757d; padding: 2px 10px; border: 1px solid #6c757d;">💻 IPsec</div> </div>		

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
```

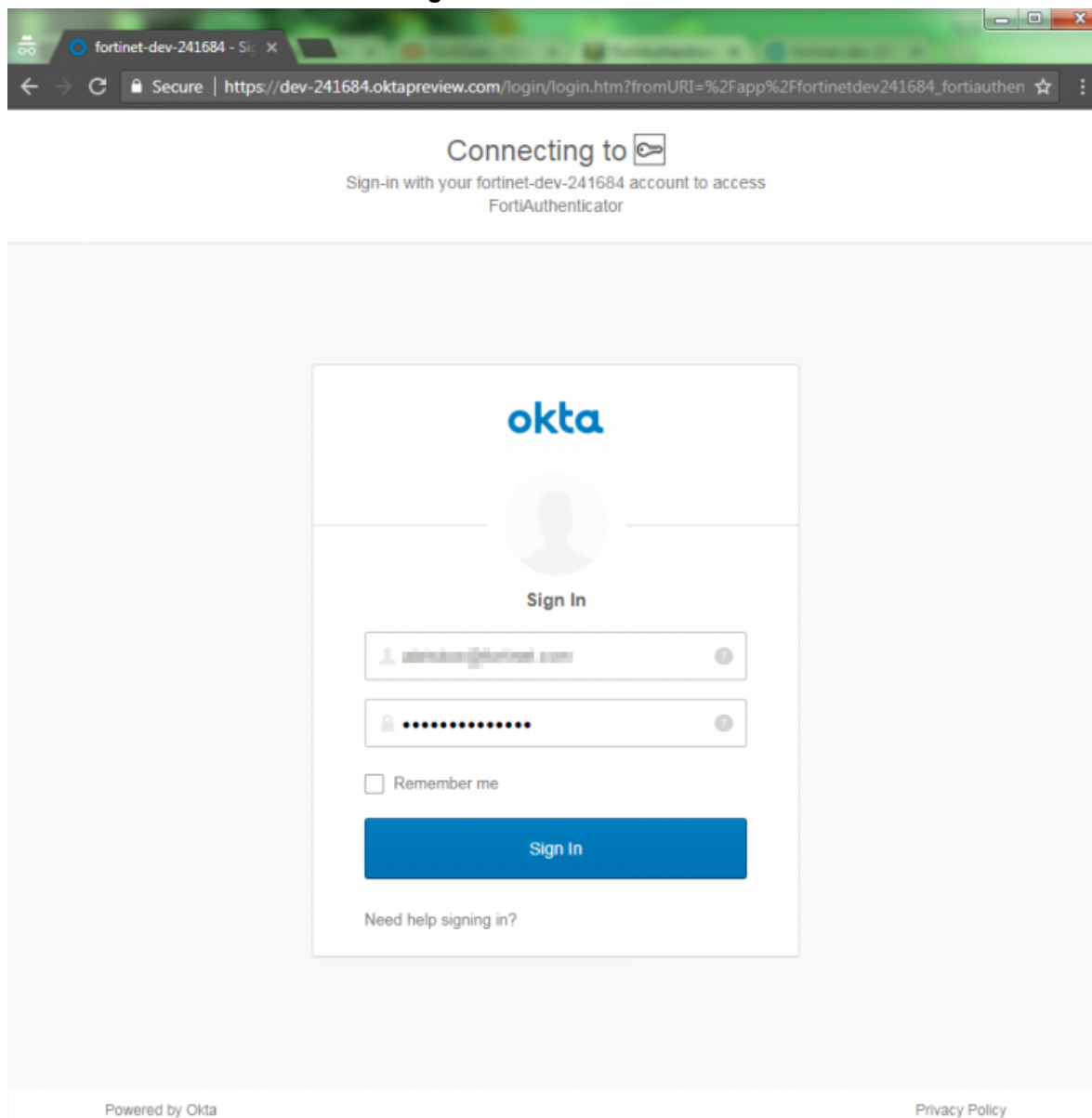
This command will exempt users of this policy from the captive portal interface.

## Results

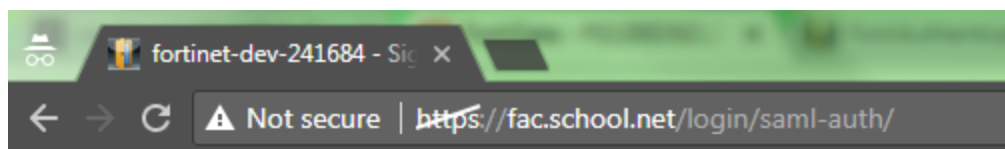
To test the connection, open a new browser window and attempt to browse the Internet. The browser will redirect to the FortiAuthenticator SAML portal, which pushes the browser to the SAML IdP.

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.

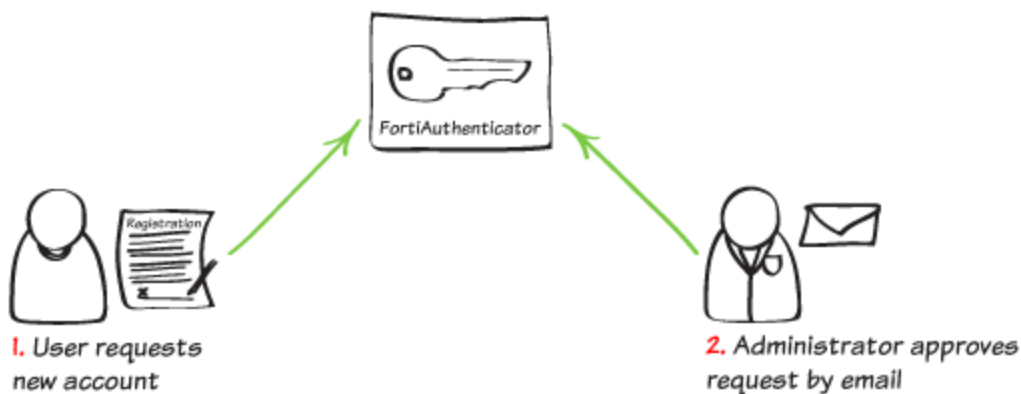




# Self-service Portal

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

## FortiAuthenticator user self-registration



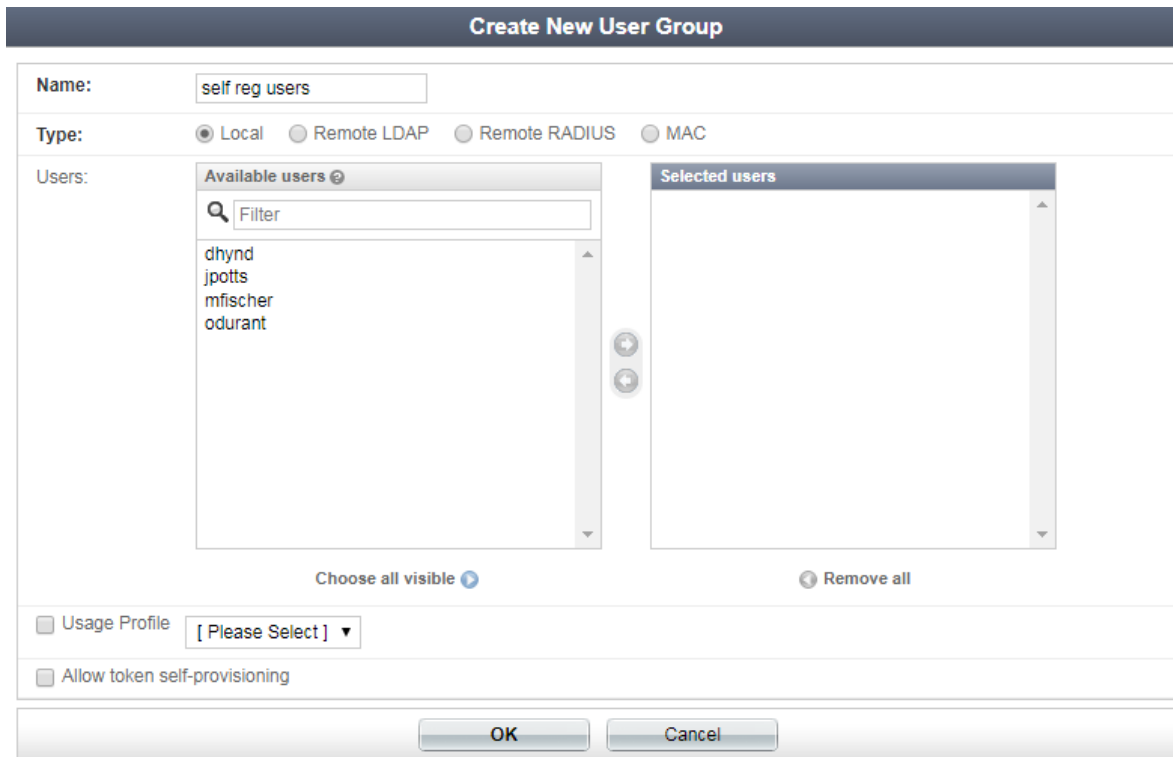
For this recipe, you will configure the FortiAuthenticator self-service portal to allow users to add their own account and create their own passwords.

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.

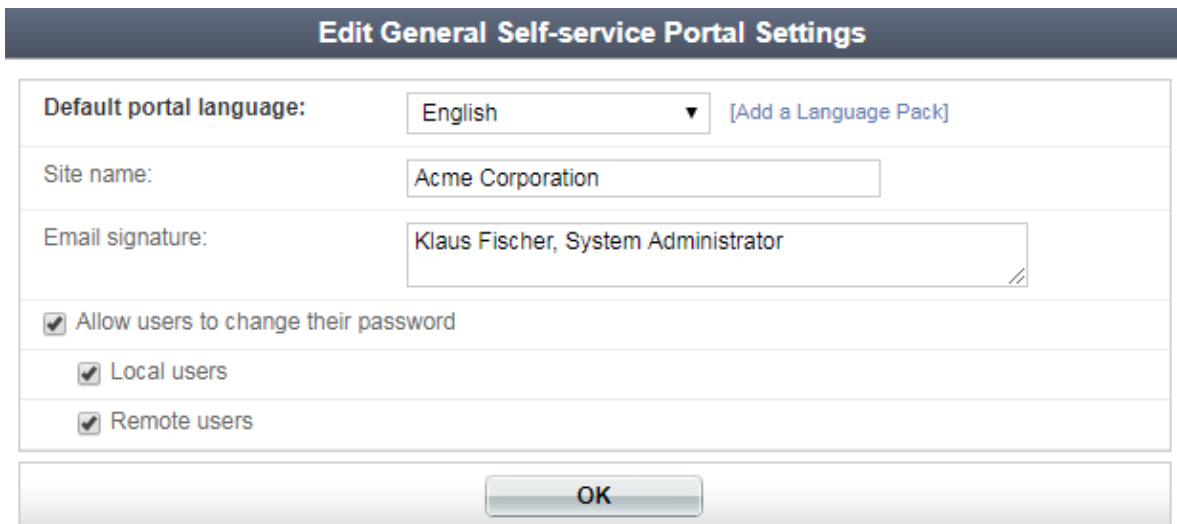


The 'Create New User Group' dialog box has a title bar with the text 'Create New User Group'. It contains a 'Name' field with the text 'self reg users'. Below this is a 'Type' section with four radio buttons: 'Local' (selected), 'Remote LDAP', 'Remote RADIUS', and 'MAC'. The 'Users' section features two lists: 'Available users' and 'Selected users'. The 'Available users' list has a search filter and contains the names 'dhynd', 'jpotts', 'mfischer', and 'odurant'. Between the lists are two arrow buttons. Below the lists are the buttons 'Choose all visible' and 'Remove all'. At the bottom, there are checkboxes for 'Usage Profile' (with a dropdown menu showing '[ Please Select ]') and 'Allow token self-provisioning'. The dialog ends with 'OK' and 'Cancel' buttons.

## 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**.



The 'Edit General Self-service Portal Settings' dialog box has a title bar with the text 'Edit General Self-service Portal Settings'. It contains a 'Default portal language' dropdown menu set to 'English' with a link '[Add a Language Pack]'. Below this is a 'Site name' field with the text 'Acme Corporation'. The 'Email signature' field contains the text 'Klaus Fischer, System Administrator'. There are three checkboxes: 'Allow users to change their password' (checked), 'Local users' (checked), and 'Remote users' (checked). The dialog ends with an 'OK' button.

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**.

**Edit Self-registration Settings**

☒ Enable

☒ Require administrator approval

☒ Enable email to freeform addresses

Administrator email addresses:

☐ Enable email to administrator accounts

☐ Account expires after  hour(s) ▼

☐ Use mobile number as username

☒ Place registered users into a group 

Password creation: ☒ User-defined ☐ Randomly generated

Send account information via: ☐ SMS ☒ Email

SMS gateway: 

**Required Field Configuration**

☒ First name

☒ Last name

☒ Email address

☐ Address

☐ City

☐ State/Province

☐ Country

☐ Phone number

☐ Mobile number

☐ Custom field 1

☐ Custom field 2

☐ Custom field 3

OK

FortiAuthenticator Cookbook

Fortinet Technologies Inc.

## 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.

Create New SMTP Server

<b>Name:</b>	<input type="text" value="new-server"/>
<b>Server name/IP:</b>	<input type="text" value="172.25.176.141"/>
<b>Port:</b>	<input type="text" value="25"/>
Sender name (optional):	<input type="text"/>
<b>Sender email address:</b>	<input type="text" value="abristow@fortinet.com"/>

Connection Security and Authentication

<b>Secure connection:</b>	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">None ▼</div>
<input checked="" type="checkbox"/> Enable authentication	
<b>Account username:</b>	<input type="text" value="administrator"/>
<b>Password:</b>	<input type="password" value="....."/>

Test Connection

OK

Cancel

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

+ Create New
🗑 Delete
✎ Edit
📌 Set as Default
0 of 2 selected

✓ Successfully set "new-server (172.25.176.141:25)" as the default outgoing mail server

	Name	Server	Default
<input type="checkbox"/>	new-server	172.25.176.141:25	<div style="border: 2px solid red; padding: 2px; display: inline-block;">✓</div>
<input type="checkbox"/>	Local Mail Server	localhost:25	

2 SMTP servers

## 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**.

Please enter your information below.

Username:	<input type="text" value="rdeckard"/>
Password:	<input type="password" value="*****"/>
Confirm password:	<input type="password" value="*****"/>
First name:	<input type="text" value="Rick"/>
Last name:	<input type="text" value="Deckard"/>
Email address:	<input type="text" value="rdeckard@fortinet.com"/>
Confirm email address:	<input type="text" value="rdeckard@fortinet.com"/>
Address:	<input type="text"/>
City:	<input type="text"/>
State/Province:	<input type="text"/>
Country:	<input type="text" value=""/>
Phone number:	<input type="text"/>
Mobile number:	<input type="text"/>




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



### Registration Successful


Your information has been sent to the administrator for approval. You will receive an email once your account has been approved and activated.

[Go back to the login page](#)

- 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.

**Your account has been activated**  Inbox x  

**abristow@fortinet.com** 12:04 (0 minutes ago) ☆  

to me 

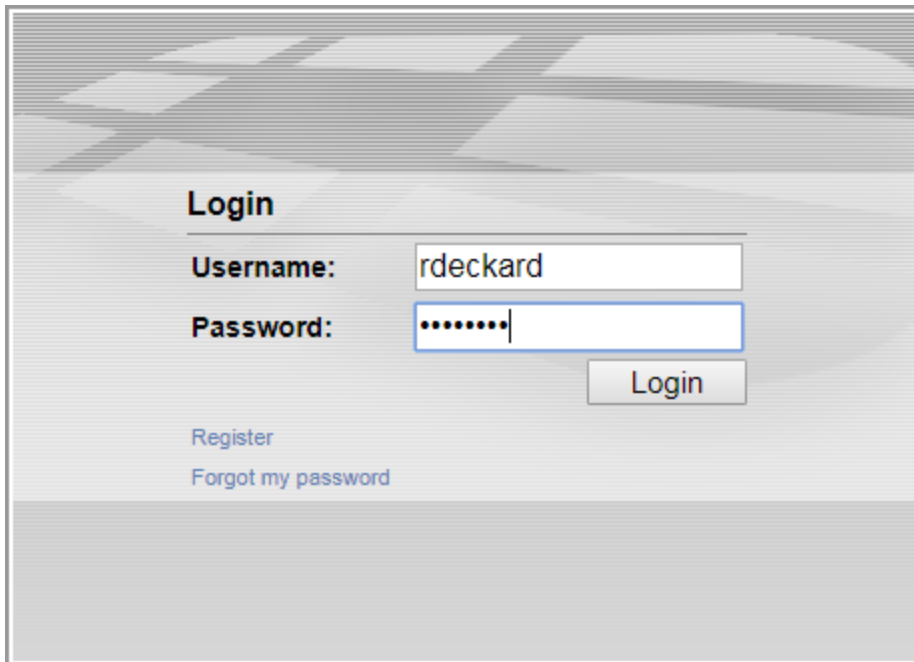
Welcome to Acme Corporation, rdeckard!

Your login information:  
Username: rdeckard  
Password: \*\*\*\*\*

Please login and change your password here:  
<https://172.25.176.141/login/?username=rdeckard>

Klaus Fischer, System Administrator

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



**Login**

Username: rdeckard

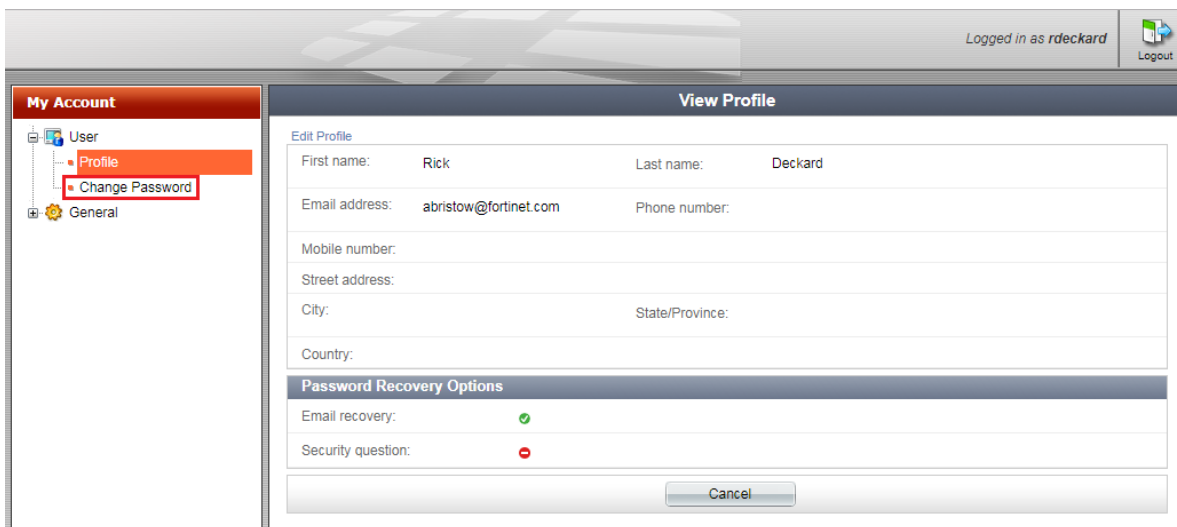
Password: .....

Login

[Register](#)

[Forgot my password](#)

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.



Logged in as rdeckard Logout

**My Account**

- User
  - Profile
  - Change Password
- General

**View Profile**

Edit Profile

First name:	Rick	Last name:	Deckard
Email address:	abristow@fortinet.com		Phone number:
Mobile number:			
Street address:			
City:	State/Province:		
Country:			

**Password Recovery Options**

Email recovery:	✓
Security question:	✗

Cancel

## 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**.

Create New

Import

Export Users

Edit

Delete

Disabled Users

0 of 6 selected

Search for local users

	User	First name	Last name	Email address	Admin	Status	Token	Token Requested	Groups	Authentication Methods
<input type="checkbox"/>	admin									
<input type="checkbox"/>	dhynd									RADIUS
<input type="checkbox"/>	jpotts									RADIUS
<input type="checkbox"/>	mfischer									RADIUS
<input type="checkbox"/>	odurant									RADIUS
<input type="checkbox"/>	rdeckard	Rick	Deckard	abristow@fortinet.com		Unknown			self reg group	RADIUS

6 local users

- 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.

### Approval Required for "Rick Deckard"

abristow@fortinet.com

Sent: Tue 11/07/17 4:30 PM

To: Adam Bristow

User "rdeckard" has just registered and is waiting for approval.

Please go to the following link to approve or deny this user:  
<https://172.25.176.141/auth/register/12/approve/>

Klaus Fischer, System Administrator

- 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**.

New User Approval	
Please review the following user information. You can approve or deny this user.	
Username:	rdeckard
First name:	Rick
Last name:	Deckard
Email address:	rdeckard@fortinet.com
Address:	
City:	
State/Province:	
Country:	
Phone number:	
Mobile number:	
<div> <input type="button" value="Approve"/> <input type="button" value="Deny"/> </div>	

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



**User Registration Completed**

## User Registration Completed

User "rdeckard" has been activated.

[Go back to the main page](#)

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

Create New

Import

Export Users

Edit

Delete

Disabled Users

0 of 6 selected

Search for local users

	User	First name	Last name	Email address	Admin	Status	Token	Token Requested	Groups	Authentication Methods
<input type="checkbox"/>	admin									
<input type="checkbox"/>	dhynd									RADIUS
<input type="checkbox"/>	jpotts									RADIUS
<input type="checkbox"/>	mfischer									RADIUS
<input type="checkbox"/>	odurant									RADIUS
<input type="checkbox"/>	rdeckard	Rick	Deckard	abristow@fortinet.com					self reg group	RADIUS

6 local users

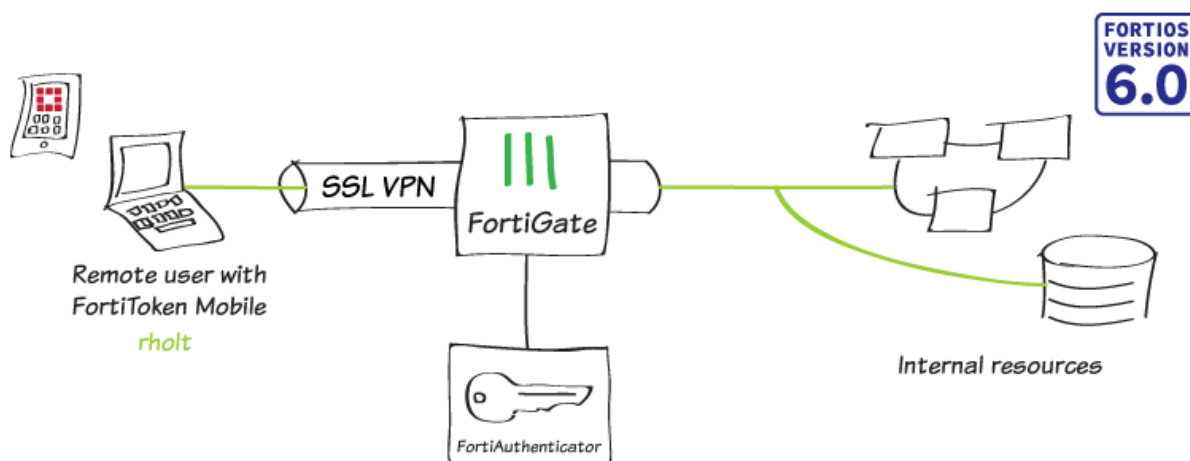
5. You can also go to **Logging > Log Access > Logs** to view the successful login of the user and more information.

										<input type="text" value="Search for log records"/>
ID	Timestamp	Level	Category	Sub category	Type id	Action	Status	Source IP	Short message	Log Details
56862	Wed Nov 8 09:09:10 2017	information	Event	Authentication	20994	Login	Success	172.25.176.92	Web access granted to 'admin'	<div>Log Record Detail</div> <div>ID56858</div> <div>TimestampWed Nov 8 09:08:49 2017</div> <div>Levelinformation</div> <div>ActionLogin</div> <div>StatusSuccess</div> <div>Source IP</div> <div>MessageLocal user authentication with no token successful</div> <div>User<div>rdeckard</div></div> <div>Log Type</div> <div>Type Id50000</div> <div>NameUser Portal Login</div> <div>Sub CategoryUser Portal</div> <div>CategoryEvent</div> <div>DescriptionLogs login activity for the user portal</div>
56861	Wed Nov 8 09:09:10 2017	information	Event	Authentication	20994	Login	Success		Local administrator authentication with no token successful	
56860	Wed Nov 8 09:08:57 2017	information	Event	User Portal	50001	Logout			User 'rdeckard' logged out	
56859	Wed Nov 8 09:08:49 2017	information	Event	Authentication	20994	Login	Success	172.25.176.92	Web access granted to 'rdeckard'	
56858	Wed Nov 8 09:08:49 2017	information	Event	User Portal	50000	Login	Success		Local user authentication with no token successful	
56857	Wed Nov 8 09:04:00 2017	information	Event	System	30908				smtp mail: send to adem.r.bristow@gmail.com via 172.25.176.141:25 ok	
56856	Wed Nov 8 09:04:00 2017	information	Event	Admin Configuration	10301				Notifying user 'rdeckard_' about his/her newly activated account	
56855	Wed Nov 8 09:04:00 2017	information	Event	Admin Configuration	10002	Edit			Edited Local User: rdeckard_ (changed fields: active)	
56854	Wed Nov 8 09:04:00 2017	information	Event	Admin Configuration	10301				Activating new account for user 'rdeckard_'	
56853	Wed Nov 8 09:02:56 2017	information	Event	Admin Configuration	10301				Registration form submitted by user 'rdeckard_'	
56852	Wed Nov 8 09:02:56 2017	information	Event	System	30908				smtp mail: send to abristow@fortinet.com via 172.25.176.141:25 ok	
56851	Wed Nov 8 09:02:51 2017	information	Event	Admin Configuration	10002	Edit			Edited Local User Profile: rdeckard_ (changed fields: email recovery)	
56850	Wed Nov 8 09:02:51 2017	information	Event	Admin Configuration	10001	Add			Added Local User Profile: rdeckard_	
56849	Wed Nov 8 09:02:51 2017	information	Event	Admin Configuration	10002	Edit			Edited User Group: self reg group (changed field: users)	
56848	Wed Nov 8 09:02:51 2017	information	Event	Admin Configuration	10002	Edit			Edited User Group: self reg group (changed field: users)	
56847	Wed Nov 8 09:02:51 2017	information	Event	Admin Configuration	10002	Edit			Edited Local User: rdeckard_ (changed fields: active and email address)	
56846	Wed Nov 8 09:02:51 2017	information	Event	Admin Configuration	10001	Add			Added Local User: rdeckard_	
56845	Wed Nov 8 09:01:52 2017	information	Event	Authentication	20994	Login	Success	172.25.176.92	Web access granted to 'admin'	
56844	Wed Nov 8 09:01:52 2017	information	Event	Authentication	20994	Login	Success		Local administrator authentication with no token successful	
56843	Thu Nov 7 14:41:36 2017	information	Event	Authentication	20994	Login	Success	172.25.176.92	Local administrator authentication with no token successful	

## 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**.

Username:

Password creation:

Password:

Password confirmation:

☒ Allow RADIUS authentication

**Role**

Role: ☐ Administrator  
☐ Sponsor  
☒ User

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**.

Username:

☐ Disabled

☒ Password-based authentication [\[Change Password\]](#)

☒ Token-based authentication

Deliver token code by: ☒ FortiToken ☐ Email ☐ SMS ☐ Dual (Email & SMS)

FortiToken Hardware:  FortiToken Mobile:  Delivery method: ☒ Email ☐ SMS

[Configure a temporary e-mail/SMS token.](#)

☒ Allow RADIUS authentication

☐ Enable account expiration

**User Role**

Role: ☐ Administrator  
☐ Sponsor  
☒ User

☐ Allow LDAP browsing

**User Information**

First name:  Last name:

Email:  Phone number:

4. Set **Deliver token code by** to **FortiToken**. Set **FortiToken Mobile** to an available FortiToken. Set **Delivery 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.

**Name:**

**Type:** ☒ Local ☐ Remote LDAP ☐ Remote RADIUS ☐ MAC

**Users:**

**Available users** ⓘ

admin  
leela

**Selected users**

rholt

- 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`).

**Create New User Group RADIUS Attribute**

**Vendor:**

**Attribute ID:**

**Type:**

**Value:**

## Creating the RADIUS client

- On the FortiAuthenticator, go to **Authentication > RADIUS Service > Clients** and select **Create New** to create a RADIUS client.
- 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.

**Name:**

**Client address:** ☒ IP/Hostname ☐ Subnet ☐ Range

**Secret:**

**First profile name:**

**Description:**

☐ Apply this profile based on RADIUS attributes .

**EAP types:**

- ☐ EAP-GTC
- ☐ EAP-TLS
- ☐ PEAP
- ☐ EAP-TTLS

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

**User Authentication**

Authentication method:

- ☐ Enforce two-factor authentication
- ☒ Apply two-factor authentication if available (authenticate any user)
- ☐ Password-only authentication (exclude users without a password)
- ☐ FortiToken-only authentication (exclude users without a FortiToken)

☒ Enable FortiToken Mobile push notifications authentication

Username input format:

- ☒ username@realm
- ☐ realmusername
- ☐ realm/username

Realms:

Default	Realm	Allow local users to override remote users	Use Windows AD domain authentication	Groups	Delete
<input checked="" type="radio"/>	local   Local users	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/> Filter: SSL_VPN_RADIUS <input type="checkbox"/> Filter local users:	<input type="button" value="Delete"/>

[Add a realm](#)

- 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

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

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

Name   
 Authentication method Default Specify  
 NAS IP   
 Include in every user group ☐


#### Primary Server

IP/Name   
 Secret   
 Connection status ✓ Successful  
Test Connectivity  
Test User Credentials

- 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.
- Select **Test Connectivity** to make sure you used the proper settings.
- To import the user group, go to **User & Device > User Groups** and create a new group.

Name   
 Type Firewall  
 Members

#### Remote Groups



<span>+ Add</span> <span>Edit</span> <span>Delete</span>	
Remote Server	Group Name
 RADIUS-FAC	SSL_VPN_RADIUS

- 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.

### Authentication/Portal Mapping

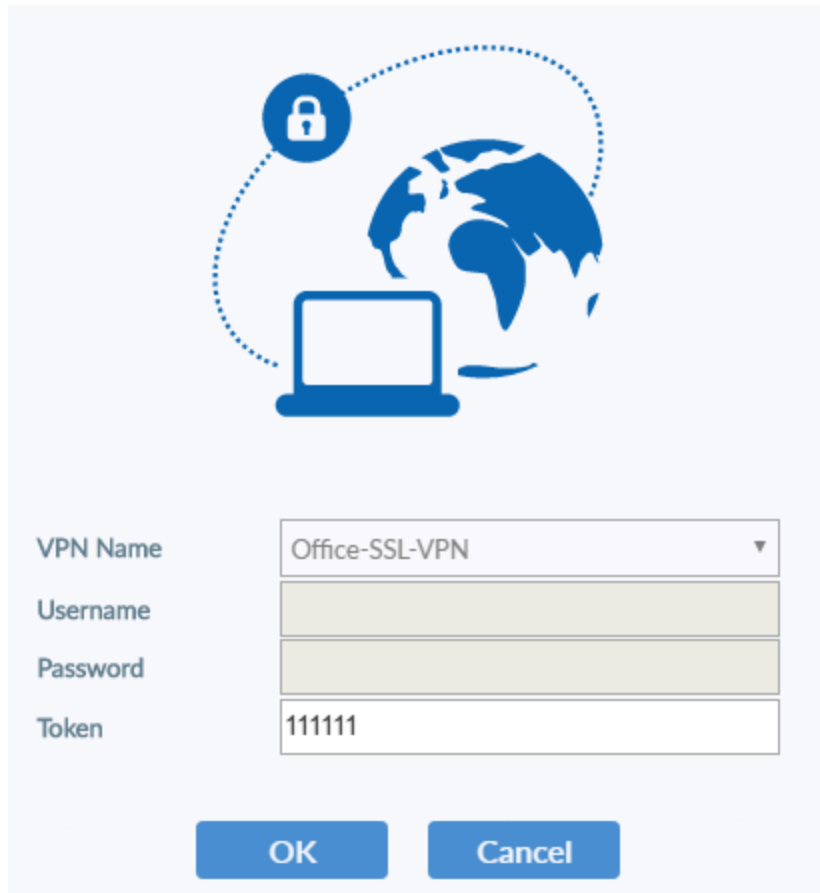
<div> <span>+ Create New</span> <span>Edit</span> <span>Delete</span> </div>	
Users/Groups	Portal
 Employees	full-access
 RADIUS-VPN	tunnel-access
All Other Users/Groups	web-access

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.

Name 	SSL-access-internal-network
Incoming Interface	 SSL-VPN tunnel interface (ssl.root ▼)
Outgoing Interface	 lan ▼
Source	<div>  all <span>✕</span> </div> <div>  Employees <span>✕</span> </div> <div>  SSL_VPN_RADIUS <span>✕</span> </div> <div>+</div>
Destination	<div>  Internal-network <span>✕</span> </div> <div>+</div>
Schedule	 always ▼
Service	<div>  ALL <span>✕</span> </div> <div>+</div>
Action	<div> <span>✓ ACCEPT</span> <span>✗ DENY</span> <span>🎓 LEARN</span> </div>

## Results

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



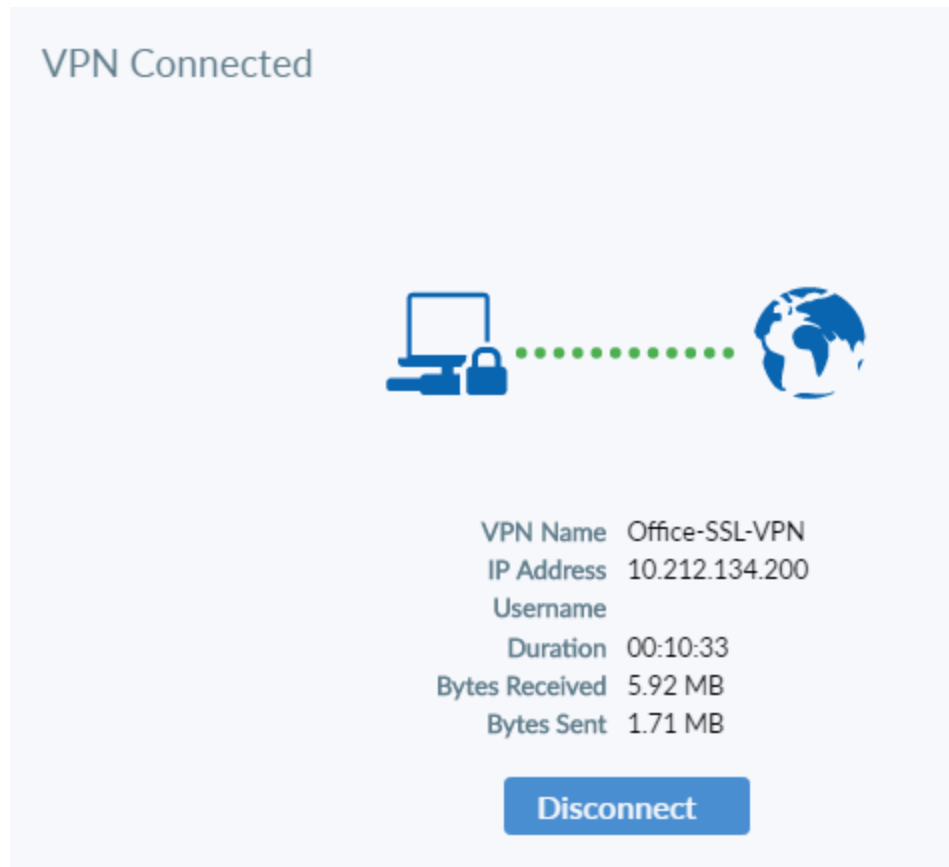
The image shows a login dialog for an SSL VPN. At the top, there is a blue icon depicting a globe with a laptop in front of it, and a padlock icon connected by a dotted line, symbolizing a secure connection. Below the icon, there are four input fields with labels to their left: 'VPN Name' with a dropdown menu showing 'Office-SSL-VPN', 'Username' with an empty text box, 'Password' with an empty text box, and 'Token' with a text box containing '111111'. At the bottom of the dialog, there are two blue buttons: 'OK' and 'Cancel'.

VPN Name	Office-SSL-VPN ▼
Username	
Password	
Token	111111

OK Cancel



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.

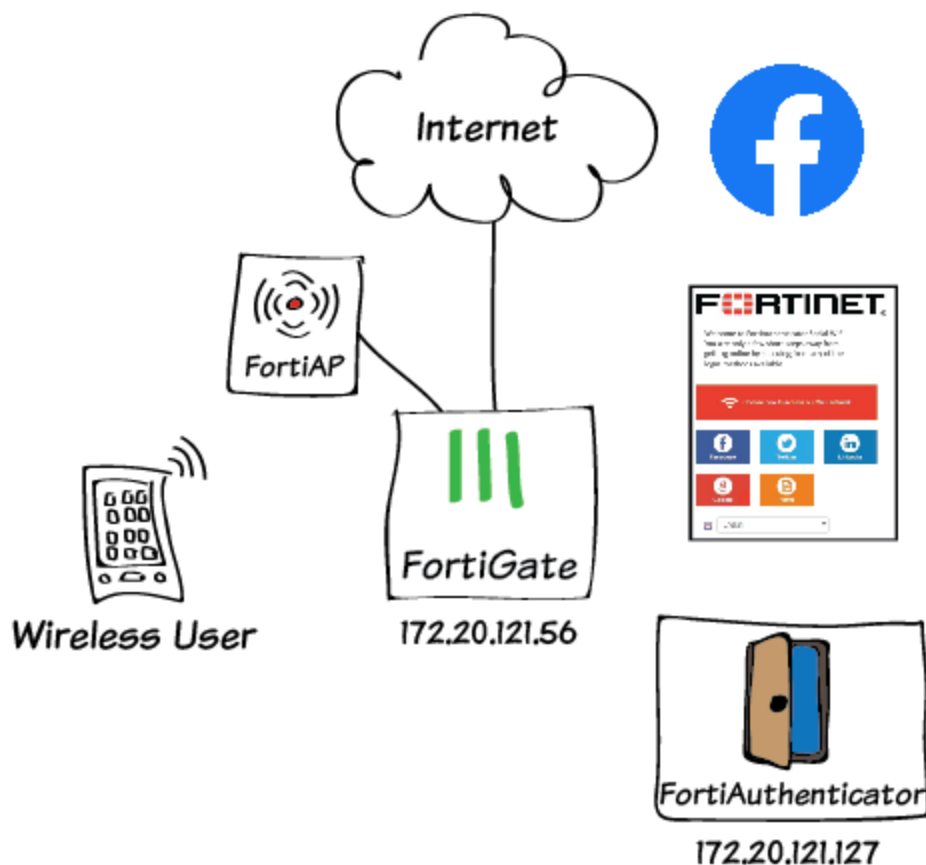
## Social WiFi captive portal

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.

**Please re-enter your password** ×

 **Wade Wilson**

For your security, you must re-enter your password to continue.

Password:

---

[Forgotten your password?](#)

Select that you have read and agree to the [Facebook Platform](#) and [Facebook Privacy](#) policies, and select **Next** to continue.

**Register as a Facebook Developer** ×

 **Wade Wilson**

Do you accept the Facebook Platform Policy and the Facebook Privacy Policy?

---

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.

**Register as a Facebook Developer** ×

We need to verify your account to complete your registration. Your Phone number will be added to your timeline but won't be visible to your friends.

Country Phone number

Canada (+1) 877-234-4338

Get Confirmation Code

Send as Text Send via Phone Call

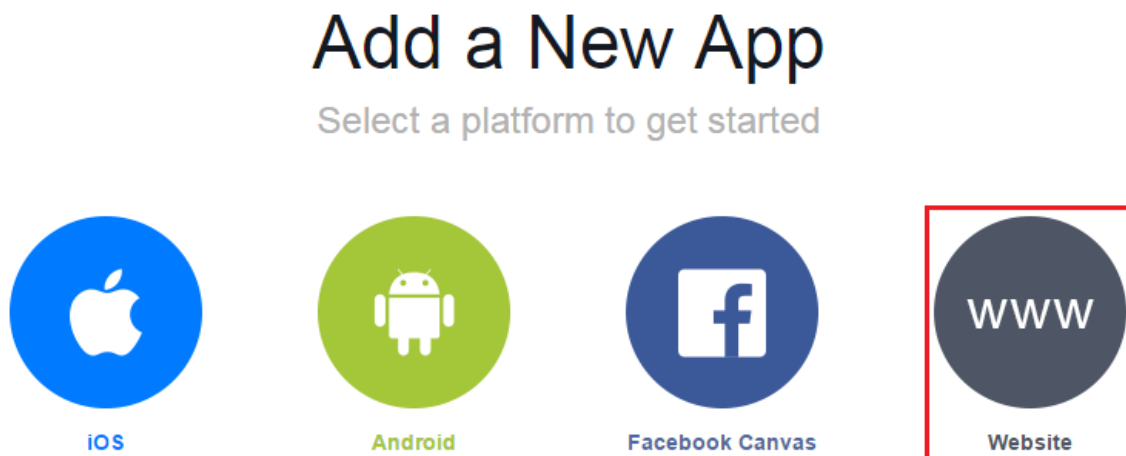
Confirmation code

877234

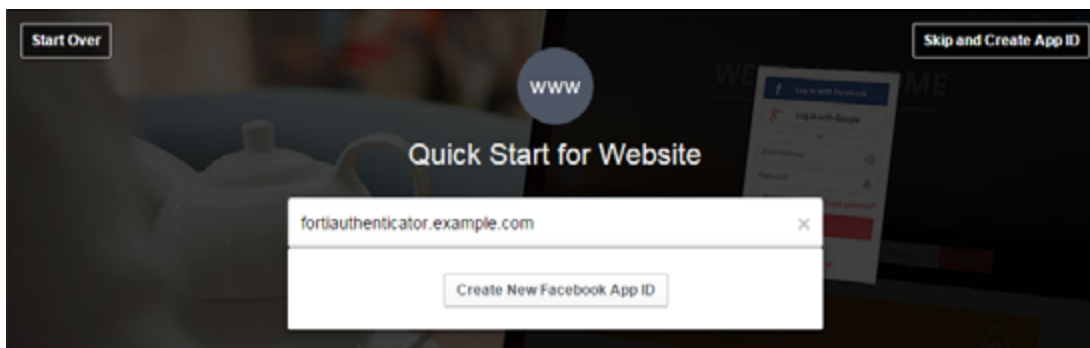
You can also verify your account by [adding a credit card](#). [?]

Go Back Register

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**.

A screenshot of a "Create a New App ID" form. The form has a title bar with a close button. The main content asks "Create fortiauthenticator.example.com App?". Below this is a "Category" dropdown menu with "Communication" selected. At the bottom, there is a checkbox labeled "By proceeding, you agree to the Facebook Platform Policies" and two buttons: "Cancel" and "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**.

A screenshot of a "Tell us about your website" form. The form has a title "Tell us about your website" and a "Site URL" field containing "https://fortiauthenticator.example.com". A "Next" button is at the bottom.

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 the 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.

fortiauthenticator.... ▾

- Dashboard
- Settings
- Status & Review
- App Details
- Roles
- Open Graph
- Alerts
- Localize

**Basic** | Advanced | Migrations

App ID: 172.20.121.127

App Secret: [Reset]

Display Name: fortiauthenticator.example.com

Namespace:

App Domains:

Contact Email: example@domain.com

Website: Quick Start ✕

Site URL: https://<FAC\_FQDN>/

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 include the public IP addresses of the FortiAuthenticator - this is the NAT IP address of the FortiAuthenticator uses to reach the Internet.

**Security**

Server IP Whitelist

172.20.121.127 ✕

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.

## Make fortiauthenticator.example.com public?

☒ Yes

Your app is currently **live** and available to the public.

## Submit Items for Approval

Some Facebook integrations require approval before public usage. Before submitting your app for review, please consult our [Platform Policy](#) and [Review Guidelines](#).

[Start a Submission](#)

## Approved items <sup>[?]</sup>

### LOGIN PERMISSIONS

#### ● email <sup>[?]</sup>

Provides access to the person's primary email address. This permission is approved by default.

#### ● public\_profile <sup>[?]</sup>

Provides access to a person's basic information, including first name, surname, profile picture, gender and age range. This permission is approved by default.

#### ● user\_friends <sup>[?]</sup>

Provides access to a person's list of friends that also use your app. This permission is approved by default.

## 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.



**Name:** Social\_Users

**Type:** ☒ Local ☐ Remote LDAP ☐ Remote RADIUS

**Users:**

Available users ⓘ  
Filter

Selected users

Choose all visible ⓘ Remove all ⓘ

RADIUS Attributes			
Attribute	Value	Vendor	Actions
<button>Add Attribute</button>			

OK Cancel

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**.

Name:

Client name/IP:

Secret:

Enable captive portal:

☐ Credentials portal (URL: /caplogin/)
☒ Social portal (URL: /social\_login/)
☐ MAC address portal (URL: /malogin/)

Profiles

Default
Add New Profile

Profiles will be applied in top-to-bottom order based on matching RADIUS attributes. If the profile has no attributes to match, that profile will always be applied before any beneath it.

Profile name:

Description:

☐ Apply this profile based on RADIUS attributes.

Authentication method:

☐ Enforce two-factor authentication
☐ Apply two-factor authentication if available (authenticate any user)
☒ Password-only authentication (exclude users without a password)
☐ FortiToken-only authentication (exclude users without a FortiToken)

Username input format:

☒ username@realm
☐ realm/username
☐ realm/username

Default	Realm	Allow local users to override remote users	Use Windows AD domain authentication	Groups	Delete
<input checked="" type="radio"/>	local   Local users	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/> Filter: Social_Users [Edit] <input type="checkbox"/> Filter: local users [Edit]	<input type="button" value="x"/>
<input type="button" value="+ Add a realm"/>					

☐ Allow MAC-based authentication
☐ Check machine authentication

EAP types:

☐ EAP-GTC
☐ EAP-TLS
☐ PEAP
☐ EAP-TTLS

- 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**.

Social Portal

☒ Enable social portal (URL: /social\_login/)

☐ Enable disclaimer

☒ Account expires after  hour(s) ▼

☒ Place registered users into a group  ▼

☒ Enable Facebook login

Facebook key:

Facebook secret:

☐ Enable Google login

☐ Enable Twitter login

☐ Enable LinkedIn login

☐ Enable SMS self-registration

☐ Enable e-mail self-registration

MAC Address Portal

☐ Enable MAC address portal (URL: /malogin/)

OK

## Configuring the FortiGate authentication settings

- 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.

Name	<input type="text" value="FAC-RADIUS"/>	
Primary Server IP/Name	<input type="text" value="172.20.121.127"/>	
Primary Server Secret	<input type="text" value="....."/>	<input type="button" value="Test Connectivity"/>
Secondary Server IP/Name	<input type="text"/>	
Secondary Server Secret	<input type="text"/>	<input type="button" value="Test Connectivity"/>
Authentication Method	<input checked="" type="radio"/> Default <input type="radio"/> Specify	
NAS IP / Called Station ID	<input type="text"/>	
Include in every User Group	<input type="checkbox"/>	

- 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.

Name:

Type: ☒ Firewall ☐ Fortinet Single Sign-On (FSSO) ☐ Guest ☐ RADIUS Single Sign-On (RSSO)

Members:

Remote groups

Remote Server	Group Name
FAC-RADIUS	Any

## 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**.

WiFi Settings

SSID:

Security Mode:

Portal Type: ☒ Authentication ☐ Disclaimer + Authentication ☐ Disclaimer Only ☐ Email Collection

Authentication Portal: ☐ Local ☒ External

User Groups:

Exempt List:

Redirect after Captive Portal: ☒ Original Request ☐ Specific URL

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.fcgr1-1.fna.fbcdn.net"
    set type fqdn
    set fqdn "external.fcgr1-1.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" "FB1" "FB2" "FB3" "FB4" "FB5" "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-rc1.facebook.com" "code.jquery.com" "connect.facebook.com" "fbcdn-
            photos-a-akamaihd.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.

Incoming Interface	wifi (SSID: Kraven)
Source Address	all
Source User(s)	Click to add...
Source Device Type	Click to add...
Outgoing Interface	wan1
Destination Address	Facebook_Auth
Schedule	always
Service	ALL
Action	ACCEPT

#### Firewall / Network Options

☒ NAT

☒ Use Outgoing Interface Address
 ☐ Fixed Port

☐ Use Dynamic IP Pool

☐ Use Central NAT Table

- 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

- 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.

Category	<input checked="" type="radio"/> Address <input type="radio"/> IPv6 Address <input type="radio"/> Multicast Address
Name	FortiAuthenticator
Type	IP/Netmask
Subnet / IP Range	172.20.121.127
Interface	any
Show in Address List	<input checked="" type="checkbox"/>

- 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.

Incoming Interface	wifi (SSID: Kraven) ▼
Source Address	all ▼
Source User(s)	Click to add... ▼
Source Device Type	Click to add... ▼
Outgoing Interface	wan1 ▼
Destination Address	FortiAuthenticator ▼
Schedule	always ▼
Service	ALL ▼
Action	✓ ACCEPT ▼

### Firewall / Network Options

**ON** NAT

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.








Welcome to FortiAuthenticator Social Wifi  
You are only a few short steps away from  
getting online by choosing from any of the  
login methods available.


 Choose how to access our WiFi network


  
Facebook

  
Twitter

  
LinkedIn

  
Google

  
Form

 English ▼

---

Powered by FortiAuthenticator.

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**.

### Facebook Login

---

Email or Phone:

Password:

☐ Keep me logged in

[Log In](#) or [Sign up for Facebook](#)

[Forgotten your password?](#)

English (UK) Polski Español Français (France) Italiano Lietuvių Română 中文(简体) Português (Brasil) Deutsch ...

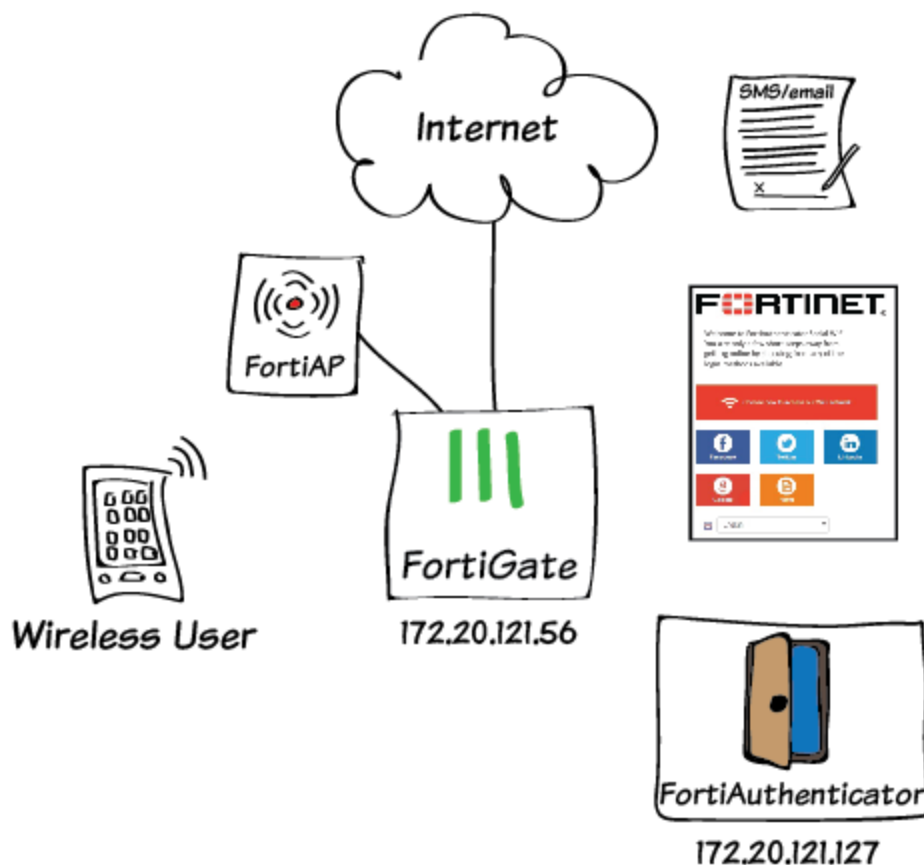
3. To view the authenticated user added on FortiAuthenticator, go to **Authentication > User Management > Social Login Users**.

[Delete](#) 0 of 1 selected

	Login id	User	First name	Last name	Email address	Active	Mac address	Groups	Expiration
<input type="checkbox"/>	SocialLogin_32	facebook:WadeWilson	Wade	Wilson			3c:15:c2:e3:3c:22	Social_Users	Fri Sep 4 18:23:51 2015

1 social login user

## 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.

**Name:** Social\_Users

**Type:** ☒ Local ☐ Remote LDAP ☐ Remote RADIUS

**Users:**

Available users

Filter

Selected users

Choose all visible

Remove all

**RADIUS Attributes**

Attribute	Value	Vendor	Actions

OK Cancel

- 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**.

Name:

Client name/IP:

Secret:

Enable captive portal:

☐ Credentials portal (URL: /caplogin/)
☒ Social portal (URL: /social\_login/)
☐ MAC address portal (URL: /malogin/)

Profiles

Default
Add New Profile

Profiles will be applied in top-to-bottom order based on matching RADIUS attributes. If the profile has no attributes to match, that profile will always be applied before any beneath it.

Profile name:

Description:

☐ Apply this profile based on RADIUS attributes.

Authentication method:

☐ Enforce two-factor authentication
☐ Apply two-factor authentication if available (authenticate any user)
☒ Password-only authentication (exclude users without a password)
☐ FortiToken-only authentication (exclude users without a FortiToken)

Username input format:

☒ username@realm
☐ realm/username
☐ realm/username

Realms:

Default	Realm	Allow local users to override remote users	Use Windows AD domain authentication	Groups	Delete
<input checked="" type="radio"/>	local   Local users	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/> Filter: Social_Users [Edit] <input type="checkbox"/> Filter: local users [Edit]	<input type="button" value="X"/>

Add a realm

☐ Allow MAC-based authentication

☐ Check machine authentication

EAP types:

☐ EAP-GTC
☐ EAP-TLS
☐ PEAP
☐ EAP-TTLS

Save

OK

Cancel

**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**.

Social Portal	
<input checked="" type="checkbox"/>	Enable social portal (URL: /social_login/)
<input type="checkbox"/>	Enable disclaimer
<input checked="" type="checkbox"/>	Account expires after <input type="text" value="1"/> hour(s) ▼
<input checked="" type="checkbox"/>	Place registered users into a group <input type="text" value="Social_Users"/> ▼
<input type="checkbox"/>	Enable Facebook login
<input type="checkbox"/>	Enable Google login
<input type="checkbox"/>	Enable Twitter login
<input type="checkbox"/>	Enable LinkedIn login
<input checked="" type="checkbox"/>	Enable SMS self-registration
	SMS gateway: <input type="text" value="Use default"/> ▼
<input checked="" type="checkbox"/>	Enable e-mail self-registration
MAC Address Portal	
<input type="checkbox"/>	Enable MAC address portal (URL: /malogin/)
OK	

## 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.

Name	<input type="text" value="FAC-RADIUS"/>	
Primary Server IP/Name	<input type="text" value="172.20.121.127"/>	
Primary Server Secret	<input type="password" value="....."/>	<input type="button" value="Test Connectivity"/>
Secondary Server IP/Name	<input type="text"/>	
Secondary Server Secret	<input type="password"/>	<input type="button" value="Test Connectivity"/>
Authentication Method	<input checked="" type="radio"/> Default <input type="radio"/> Specify	
NAS IP / Called Station ID	<input type="text"/>	
Include in every User Group	<input type="checkbox"/>	

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.

Name:

Type: ☒ Firewall ☐ Fortinet Single Sign-On (FSSO) ☐ Guest ☐ RADIUS Single Sign-On (RSSO)

Members:

Remote groups

Remote Server	Group Name
FAC-RADIUS	Any

## Configuring the FortiGate WiFi settings

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

WiFi Settings

SSID:

Security Mode:

Portal Type: ☒ Authentication ☐ Disclaimer + Authentication ☐ Disclaimer Only ☐ Email Collection

Authentication Portal: ☐ Local ☒ External

User Groups:

Exempt List:

Redirect after Captive Portal: ☒ Original Request ☐ Specific URL

- 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

- 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.

Category: ☒ Address ☐ IPv6 Address ☐ Multicast Address

Name:

Type:

Subnet / IP Range:

Interface:

Show in Address List: ☒

- 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.

Incoming Interface	wifi (SSID: Kraven)
Source Address	all
Source User(s)	Click to add...
Source Device Type	Click to add...
Outgoing Interface	wan1
Destination Address	FortiAuthenticator
Schedule	always
Service	ALL
Action	ACCEPT

### Firewall / Network Options

**ON** NAT

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.





Welcome to FortiAuthenticator Social Wifi  
You are only a few short steps away from  
getting online by choosing from any of the  
login methods available.

The login screen features a red header bar with a white Wi-Fi icon and the text "Choose how to access our WiFi network". Below this, there are six colored buttons arranged in two rows: Facebook (dark blue), Twitter (light blue), LinkedIn (medium blue) in the top row, and Google (red), Form (orange) in the bottom row. The "Form" button is highlighted with a red rectangular border. At the bottom left, there is a small UK flag icon next to a language selection dropdown menu currently set to "English".


Powered by FortiAuthenticator.


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**.

Please enter your information below.

<b>First name:</b>	<input type="text"/>
<b>Last name:</b>	<input type="text"/>
<b>Verification method:</b>	<input checked="" type="radio"/> E-mail <input type="radio"/> SMS
<b>Email address:</b>	<input type="text"/>

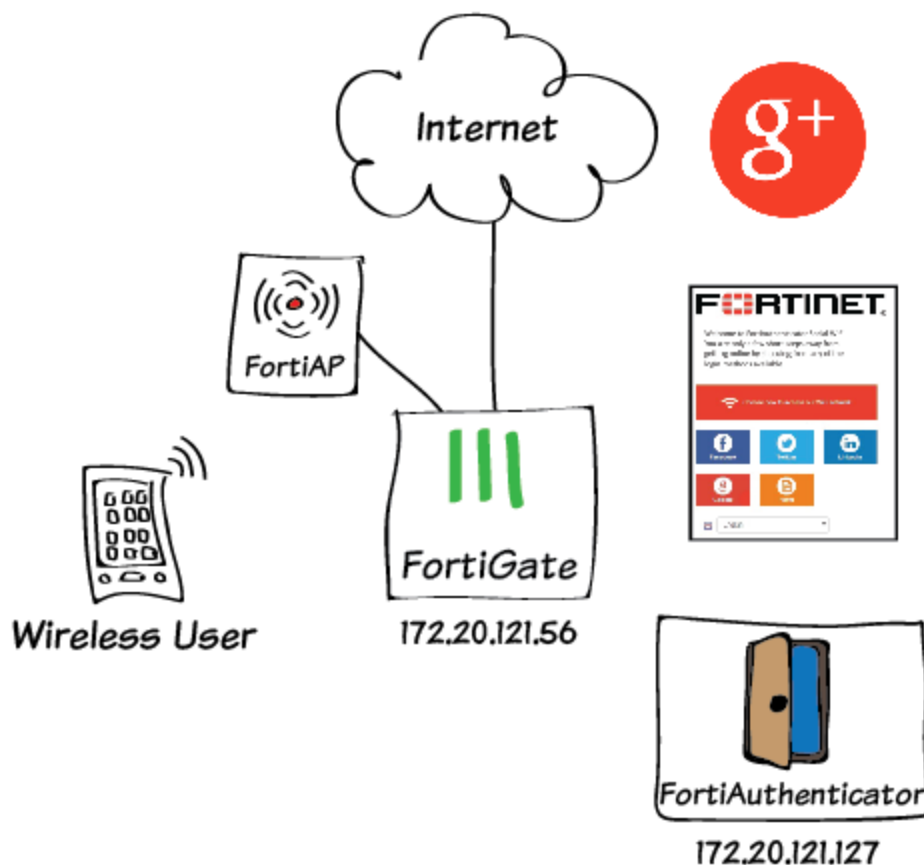
3. To view the authenticated user added on FortiAuthenticator, go to **Authentication > User Management > Social Login Users**.

 Delete 0 of 1 selected

	Login id	User	First name	Last name	Email address	Active	Mac address	Groups	Expiration
<input type="checkbox"/>	SocialLogin_36	email:wwilson.fortinet@	Wade	Wilson	wwilson.fortinet@		3c:15:c2:e3:3c:22	Social_Users	Fri Sep 4 19:20:54 2015

1 social login user

## 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.

### New Project

Project name ?

FortiAuthenticator

Your project ID will be fortiauthenticator-1051 ? [Edit](#)

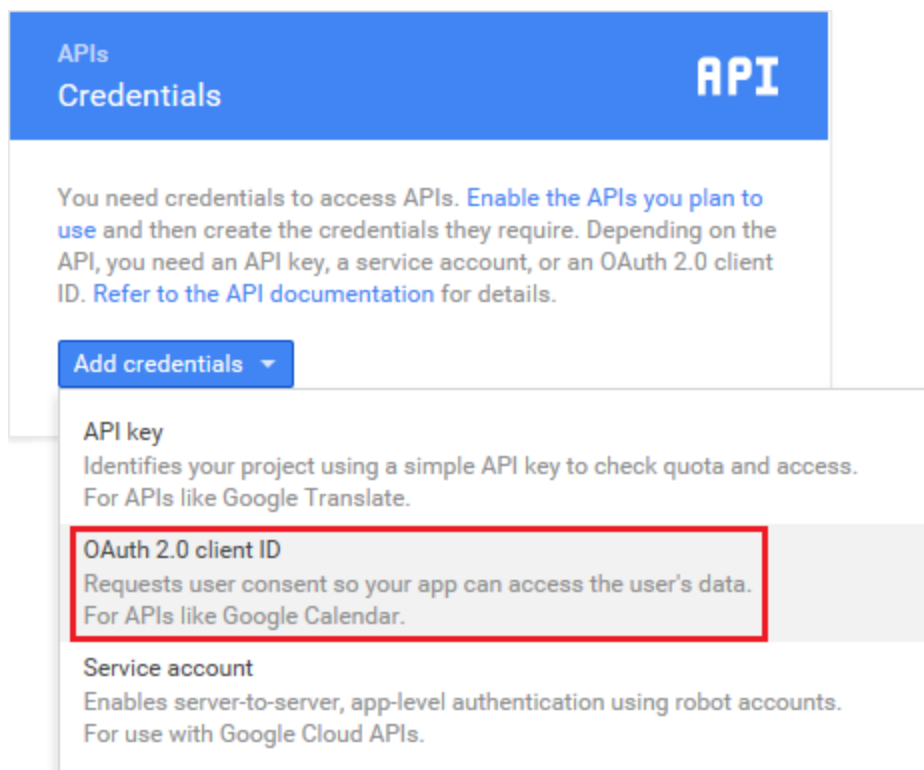
[Show advanced options...](#)

☒ I agree that my use of any [services and related APIs](#) is subject to my compliance with the applicable [Terms of Service](#).


Create

Cancel

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



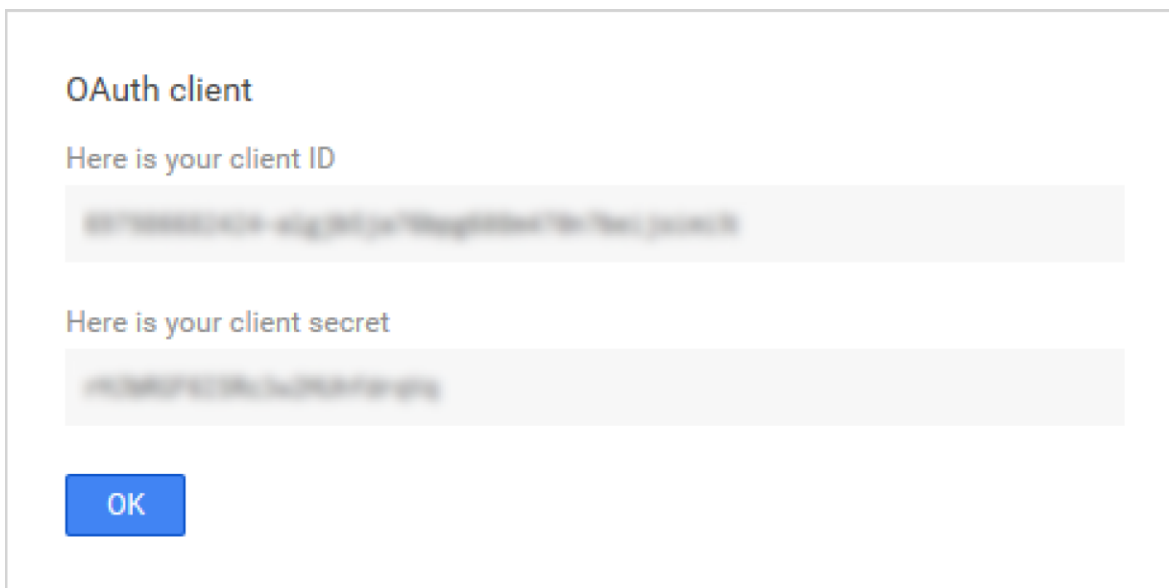
4. When prompted, select **Configure consent screen**. Enter an **Email address** and **Product name**. You must now create the client ID.

 To create an OAuth client ID, you need to set a product name in the consent screen.

Configure consent screen

Cancel

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**.



Social APIs

Google+ API

Blogger API

Google+ Pages API

Google+ Domains API

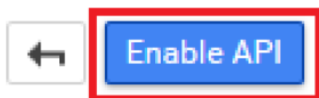


YouTube APIs

YouTube Data API

YouTube Analytics API

8. Enable the API.



## Google+ API

The Google+ API enables developers to build on top of the Google+ platform.

[Learn more](#)

[Explore this 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**.

Name:

Client name/IP:

Secret:

Enable captive portal:

☐ Credentials portal (URL: /caplogin/)
☒ Social portal (URL: /social\_login/)
☐ MAC address portal (URL: /malogin/)

Profiles

Default
Add New Profile

Profiles will be applied in top-to-bottom order based on matching RADIUS attributes. If the profile has no attributes to match, that profile will always be applied before any beneath it.

Profile name:

Description:

☐ Apply this profile based on RADIUS attributes.

Authentication method:

☐ Enforce two-factor authentication
☐ Apply two-factor authentication if available (authenticate any user)
☒ Password-only authentication (exclude users without a password)
☐ FortiToken-only authentication (exclude users without a FortiToken)

Username input format:

☒ username@realm
☐ realm/username
☐ realm/username

Realms:

Default	Realm	Allow local users to override remote users	Use Windows AD domain authentication	Groups	Delete
<input checked="" type="radio"/>	local   Local users	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/> Filter: Social_Users [Edit] <input type="checkbox"/> Filter: local users [Edit]	<input type="button" value="X"/>

Add a realm

☐ Allow MAC-based authentication

☐ Check machine authentication

EAP types:

☐ EAP-GTC
☐ EAP-TLS
☐ PEAP
☐ EAP-TTLS

Save

OK

Cancel

- 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**.

**Social Portal**

☒ Enable social portal (URL: /social\_login/)

☐ Enable disclaimer

☒ Account expires after

☒ Place registered users into a group

☐ Enable Facebook login

☒ Enable Google login  

Google key:

Google secret:

☐ Enable Twitter login

☐ Enable LinkedIn login

☐ Enable SMS self-registration

☐ Enable e-mail self-registration

**MAC Address Portal**

☐ Enable MAC address portal (URL: /malogin/)

## 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.

Name	<input type="text" value="FAC-RADIUS"/>	
Primary Server IP/Name	<input type="text" value="172.20.121.127"/>	
Primary Server Secret	<input type="password" value="••••••••"/>	<input type="button" value="Test Connectivity"/>
Secondary Server IP/Name	<input type="text"/>	
Secondary Server Secret	<input type="password"/>	<input type="button" value="Test Connectivity"/>
Authentication Method	<input checked="" type="radio"/> Default <input type="radio"/> Specify	
NAS IP / Called Station ID	<input type="text"/>	
Include in every User Group	<input type="checkbox"/>	

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.

Name:

Type: ☒ Firewall ☐ Fortinet Single Sign-On (FSSO) ☐ Guest ☐ RADIUS Single Sign-On (RSSO)

Members:

Remote groups

Remote Server	Group Name
FAC-RADIUS	Any

## 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**.

WiFi Settings

SSID:

Security Mode:

Portal Type: ☒ Authentication ☐ Disclaimer + Authentication ☐ Disclaimer Only ☐ Email Collection

Authentication Portal: ☐ Local ☒ External

User Groups:

Exempt List:

Redirect after Captive Portal: ☒ Original Request ☐ Specific URL

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.

Incoming Interface	wifi (SSID: Kraven) 
Source Address	 all 
Source User(s)	Click to add... 
Source Device Type	Click to add... 
Outgoing Interface	wan1 
Destination Address	 Google_Auth 
Schedule	 always 
Service	 ALL 
Action	 ACCEPT 

#### Firewall / Network Options

 NAT

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.

Category	<input checked="" type="radio"/> Address <input type="radio"/> IPv6 Address <input type="radio"/> Multicast Address
Name	<input type="text" value="FortiAuthenticator"/>
Type	<input type="text" value="IP/Netmask"/>
Subnet / IP Range	<input type="text" value="172.20.121.127"/>
Interface	<input type="text" value="any"/>
Show in Address List	<input checked="" type="checkbox"/>

- 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.

Incoming Interface	<input type="text" value="wifi (SSID: Kraven)"/>
Source Address	<input type="text" value="all"/>
Source User(s)	<input type="text" value="Click to add..."/>
Source Device Type	<input type="text" value="Click to add..."/>
Outgoing Interface	<input type="text" value="wan1"/>
Destination Address	<input type="text" value="FortiAuthenticator"/>
Schedule	<input type="text" value="always"/>
Service	<input type="text" value="ALL"/>
Action	<input type="text" value="ACCEPT"/>

### Firewall / Network Options

**ON** NAT

- 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

- 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.



Welcome to FortiAuthenticator Social Wifi  
You are only a few short steps away from  
getting online by choosing from any of the  
login methods available.

The login screen features a red header bar with a white Wi-Fi icon and the text "Choose how to access our WiFi network". Below this, there are five colored buttons arranged in two rows: Facebook (dark blue), Twitter (light blue), LinkedIn (medium blue) in the first row, and Google (red) and Form (orange) in the second row. The Google button is highlighted with a red rectangular border. At the bottom, there is a language selection dropdown menu showing a UK flag icon and the word "English".

---

Powered by FortiAuthenticator.

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**.



Sign in with your Google Account



Enter your email

Next

[Need help?](#)

[Create account](#)

One Google Account for everything Google

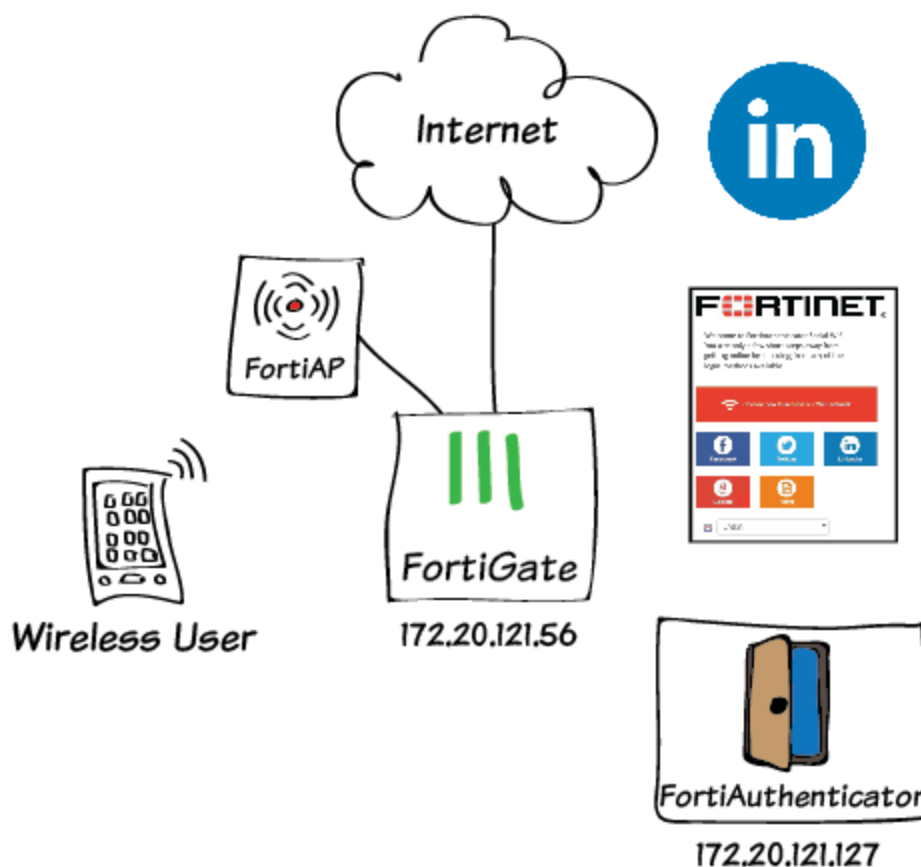


3. To view the authenticated user added on FortiAuthenticator, go to **Authentication > User Management > Social Login Users**.

Delete	0 of 1 selected	Search for social login users							
	Login id	User	First name	Last name	Email address	Active	Mac address	Groups	Expiration
	SocialLogin_33	google:waibon.fortinet	Wade	Wilson	waibon.fortinet@gmail.com	✓	3c:15:c2:e3:3c:22	Social_Users	Fri Sep 4 18:30:52 2015

1 social login user

## 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.

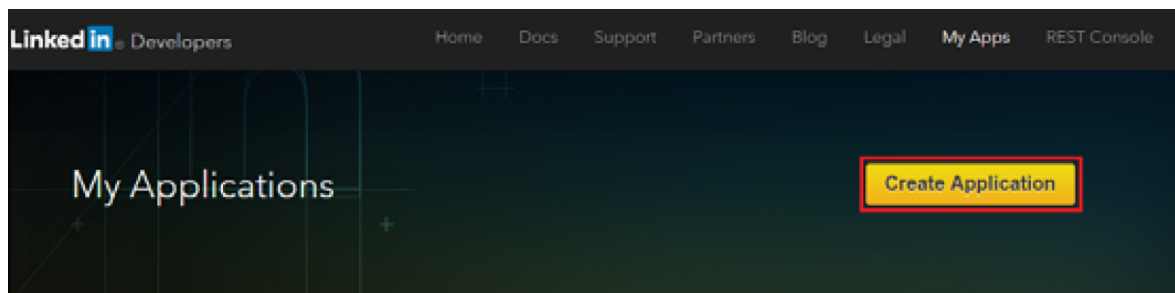
This recipe does not include FortiAP registration instructions.

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**.

### Create a New Application

**Company Name: \***

**Name: \***

**Description: \***

**Application Logo URL: \***

**Application Use: \***

Communications ▼

**Website URL: \***

http://www.fortinet.com

**Business Email: \***

wwilson@fortinet.com

**Business Phone: \***

123-456-7890

☒ I have read and agree to the [LinkedIn API Terms of Use](#).

Submit

Cancel

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.



## Authentication Keys

Client ID:

77e4b6b3e6b6

Client Secret:

83a0d7f8b1c2b3a4c5d6e7f8a9b0c1d2

## Default Application Permissions

☒ r\_basicprofile

☐ r\_emailaddress

☐ rw\_company\_admin

☐ w\_share

## OAuth 2.0

Authorized Redirect URLs:

Add

https://<FAC\_FQDN>/social/complete/linkedin-oauth2/



## OAuth 1.0a

Default "Accept" Redirect URL:

Default "Cancel" Redirect URL:

Update

Cancel

- 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.

**Name:** Social\_Users

**Type:** ☒ Local ☐ Remote LDAP ☐ Remote RADIUS

**Users:**

**Available users**

**Selected users**

Choose all visible Remove all

RADIUS Attributes			
Attribute	Value	Vendor	Actions
Add Attribute			

OK Cancel

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**.

Name:

Client name/IP:

Secret:

Enable captive portal:

☐ Credentials portal (URL: /caplogin/)
☒ Social portal (URL: /social\_login/)
☐ MAC address portal (URL: /malogin/)

Profiles

Default
Add New Profile

Profiles will be applied in top-to-bottom order based on matching RADIUS attributes. If the profile has no attributes to match, that profile will always be applied before any beneath it.

Profile name:

Description:

☐ Apply this profile based on RADIUS attributes.

Authentication method:

☐ Enforce two-factor authentication
☐ Apply two-factor authentication if available (authenticate any user)
☒ Password-only authentication (exclude users without a password)
☐ FortiToken-only authentication (exclude users without a FortiToken)

Username input format:

☒ username@realm
☐ realm/username
☐ realm/username

Realms:

Default	Realm	Allow local users to override remote users	Use Windows AD domain authentication	Groups	Delete
<input checked="" type="radio"/>	local   Local users	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/> Filter: Social_Users [Edit] <input type="checkbox"/> Filter: local users [Edit]	<input type="button" value="X"/>

Add a realm

☐ Allow MAC-based authentication
☐ Check machine authentication

EAP types:

☐ EAP-GTC
☐ EAP-TLS
☐ PEAP
☐ EAP-TTLS

Save

OK

Cancel

- 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**.

Social Portal	
<input checked="" type="checkbox"/>	Enable social portal (URL: /social_login/)
<input type="checkbox"/>	Enable disclaimer
<input checked="" type="checkbox"/>	Account expires after <input type="text" value="1"/> <input type="text" value="hour(s)"/>
<input checked="" type="checkbox"/>	Place registered users into a group <input type="text" value="Social_Users"/>
<input type="checkbox"/>	Enable Facebook login
<input type="checkbox"/>	Enable Google login
<input type="checkbox"/>	Enable Twitter login
<input checked="" type="checkbox"/>	Enable LinkedIn login
	LinkedIn key: <input type="text" value="77e44b3a6b6b"/>
	LinkedIn secret: <input type="text" value="E8b447F8A1279a6"/>
<input type="checkbox"/>	Enable SMS self-registration
<input type="checkbox"/>	Enable e-mail self-registration
MAC Address Portal	
<input type="checkbox"/>	Enable MAC address portal (URL: /malogin/)

OK

## 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.

Name	<input type="text" value="FAC-RADIUS"/>	
Primary Server IP/Name	<input type="text" value="172.20.121.127"/>	
Primary Server Secret	<input type="password" value="....."/>	<input type="button" value="Test Connectivity"/>
Secondary Server IP/Name	<input type="text"/>	
Secondary Server Secret	<input type="password"/>	<input type="button" value="Test Connectivity"/>
Authentication Method	<input checked="" type="radio"/> Default <input type="radio"/> Specify	
NAS IP / Called Station ID	<input type="text"/>	
Include in every User Group	<input type="checkbox"/>	

- 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.

Name	<input type="text" value="social_users"/>
Type	<input checked="" type="radio"/> Firewall <input type="radio"/> Fortinet Single Sign-On (FSSO) <input type="radio"/> Guest <input type="radio"/> RADIUS Single Sign-On (RSSO)
Members	<input type="button" value="Click to add..."/>
Remote groups	

Remote Server	Group Name
FAC-RADIUS	Any

## Configuring the FortiGate WiFi settings

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

WiFi Settings	
SSID	<input type="text" value="Kraven"/>
Security Mode	<input type="button" value="Captive Portal"/>
Portal Type	<input checked="" type="radio"/> Authentication <input type="radio"/> Disclaimer + Authentication <input type="radio"/> Disclaimer Only <input type="radio"/> Email Collection
Authentication Portal	<input type="radio"/> Local <input checked="" type="radio"/> External <input type="text" value="https://fortiauthenticator.example.com/social_login/"/>
User Groups	<input type="button" value="social_users"/>
Exempt List	<input type="button" value="Click to add..."/>
Redirect after Captive Portal	<input checked="" type="radio"/> Original Request <input type="radio"/> Specific URL

- 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

- 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.

Incoming Interface	wifi (SSID: Kraven)
Source Address	all
Source User(s)	Click to add...
Source Device Type	Click to add...
Outgoing Interface	wan1
Destination Address	LinkedIn_Auth
Schedule	always
Service	ALL
Action	ACCEPT

#### Firewall / Network Options

**ON** NAT

- ☒ Use Outgoing Interface Address
 ☐ Fixed Port
- ☐ Use Dynamic IP Pool
- ☐ Use Central NAT Table

- 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

- 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.

Category	<input checked="" type="radio"/> Address <input type="radio"/> IPv6 Address <input type="radio"/> Multicast Address
Name	FortiAuthenticator
Type	IP/Netmask
Subnet / IP Range	172.20.121.127
Interface	any
Show in Address List	<input checked="" type="checkbox"/>

- 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.

Incoming Interface	wifi (SSID: Kraven) ▼
Source Address	all ▼
Source User(s)	Click to add... ▼
Source Device Type	Click to add... ▼
Outgoing Interface	wan1 ▼
Destination Address	FortiAuthenticator ▼
Schedule	always ▼
Service	ALL ▼
Action	✓ ACCEPT ▼

### Firewall / Network Options

**ON** NAT

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.





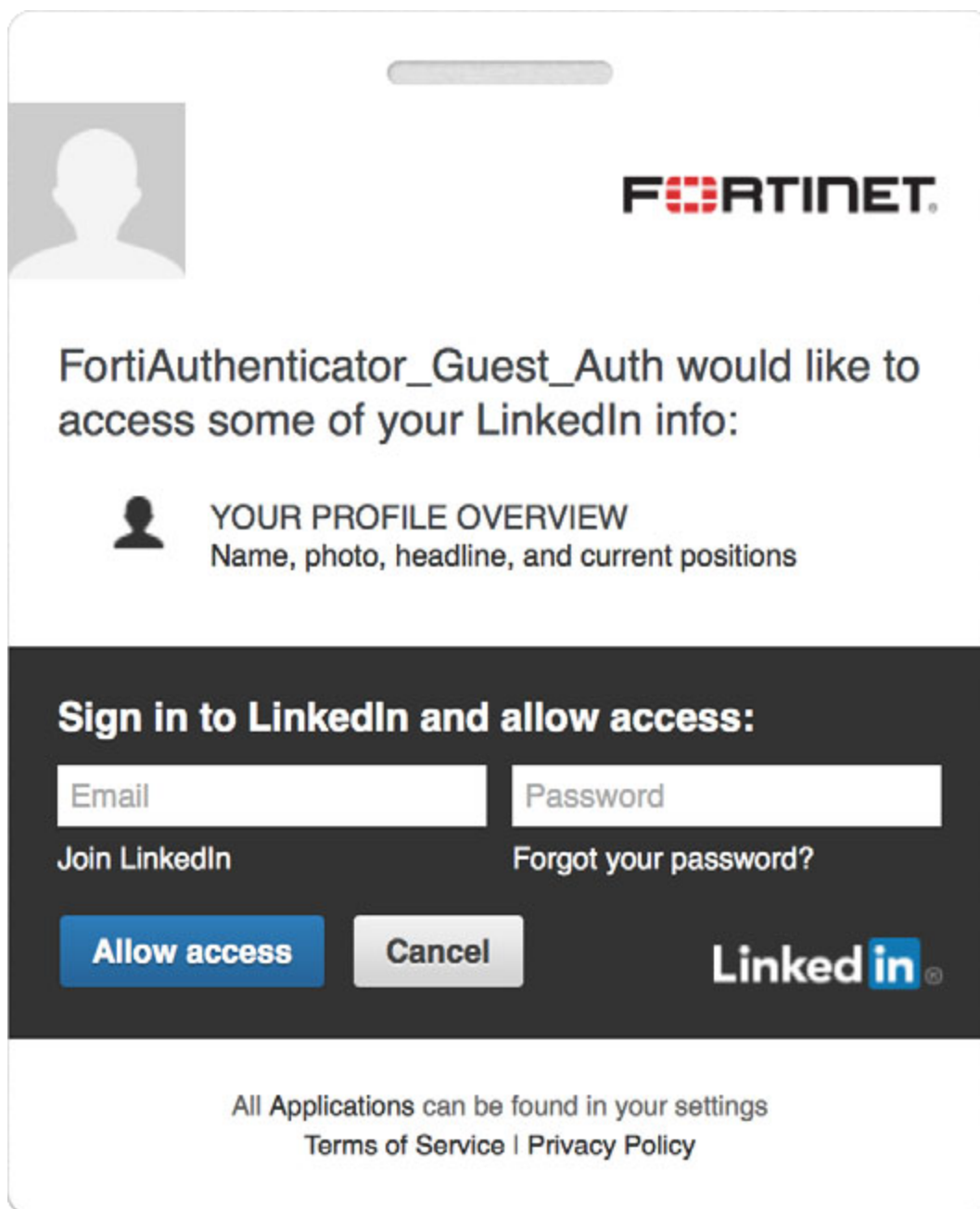
Welcome to FortiAuthenticator Social Wifi  
You are only a few short steps away from  
getting online by choosing from any of the  
login methods available.

The login screen features a red header bar with a white Wi-Fi icon and the text "Choose how to access our WiFi network". Below this, there are five colored buttons arranged in two rows: Facebook (blue), Twitter (light blue), LinkedIn (dark blue, highlighted with a red border), Google (red), and Form (orange). At the bottom, there is a language selection dropdown menu showing "English" with a small UK flag icon to its left.

---

Powered by FortiAuthenticator.

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**.

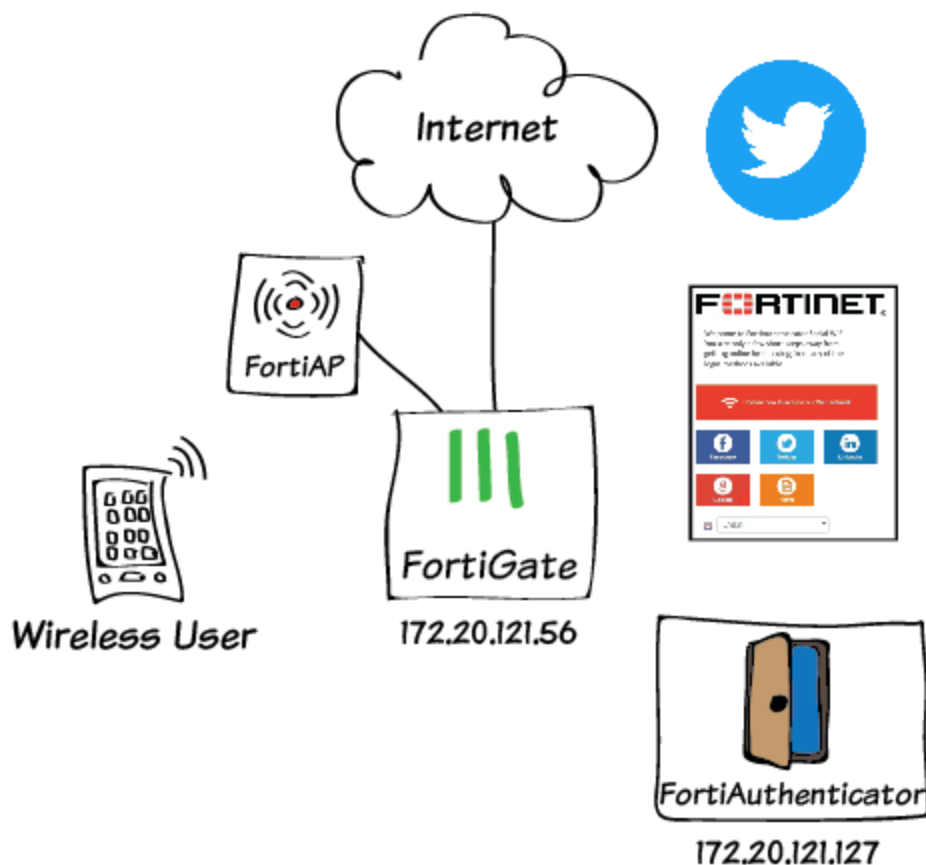


3. To view the authenticated user added on FortiAuthenticator, go to **Authentication > User Management > Social Login Users**.

Delete	0 of 1 selected	Search for social login users							
	Login id	User	First name	Last name	Email address	Active	Mac address	Groups	Expiration
	SocialLogin_34	linkedin/WadeWilson	Wade	Wilson		✓	3c:15:c2:e3:3c:22	Social_Users	Fri Sep 4 18:47:54 2015

1 social login user

## 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.

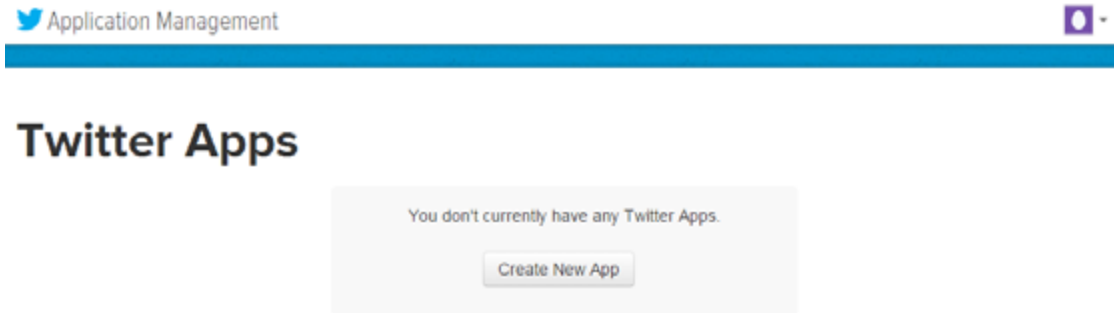
This recipe does not include FortiAP registration instructions.

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**.

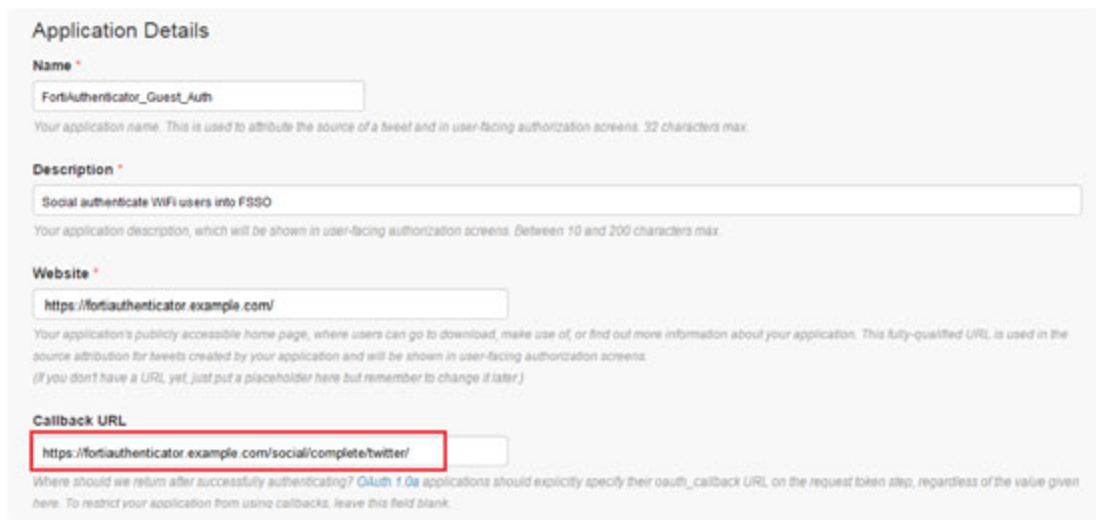


2. Enter a **Name**, **Description**, and **Website** for the application.

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.



**Application Details**

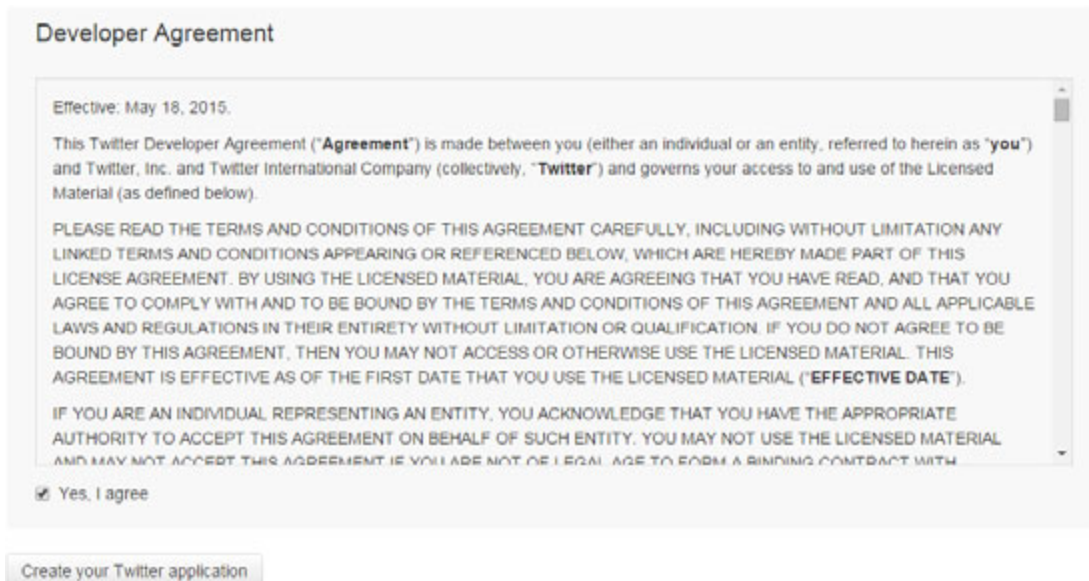
**Name \***  
FortiAuthenticator\_Guest\_Auth  
Your application name. This is used to attribute the source of a tweet and in user-facing authorization screens. 32 characters max.

**Description \***  
Social authenticate WiFi users into FSSO  
Your application description, which will be shown in user-facing authorization screens. Between 10 and 200 characters max.

**Website \***  
https://fortiauthenticator.example.com/  
Your application's publicly accessible home page, where users can go to download, make use of, or find out more information about your application. This fully-qualified URL is used in the source attribution for tweets created by your application and will be shown in user-facing authorization screens.  
(If you don't have a URL yet, just put a placeholder here but remember to change it later.)

**Callback URL**  
https://fortiauthenticator.example.com/social/complete/twitter/  
Where should we return after successfully authenticating? OAuth 1.0a applications should explicitly specify their oauth\_callback URL on the request token step, regardless of the value given here. To restrict your application from using callbacks, leave this field blank.

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



**Developer Agreement**

Effective: May 18, 2015.

This Twitter Developer Agreement ("Agreement") is made between you (either an individual or an entity, referred to herein as "you") and Twitter, Inc. and Twitter International Company (collectively, "Twitter") and governs your access to and use of the Licensed Material (as defined below).

PLEASE READ THE TERMS AND CONDITIONS OF THIS AGREEMENT CAREFULLY, INCLUDING WITHOUT LIMITATION ANY LINKED TERMS AND CONDITIONS APPEARING OR REFERENCED BELOW, WHICH ARE HEREBY MADE PART OF THIS LICENSE AGREEMENT. BY USING THE LICENSED MATERIAL, YOU ARE AGREEING THAT YOU HAVE READ, AND THAT YOU AGREE TO COMPLY WITH AND TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS AGREEMENT AND ALL APPLICABLE LAWS AND REGULATIONS IN THEIR ENTIRETY WITHOUT LIMITATION OR QUALIFICATION. IF YOU DO NOT AGREE TO BE BOUND BY THIS AGREEMENT, THEN YOU MAY NOT ACCESS OR OTHERWISE USE THE LICENSED MATERIAL. THIS AGREEMENT IS EFFECTIVE AS OF THE FIRST DATE THAT YOU USE THE LICENSED MATERIAL ("EFFECTIVE DATE").

IF YOU ARE AN INDIVIDUAL REPRESENTING AN ENTITY, YOU ACKNOWLEDGE THAT YOU HAVE THE APPROPRIATE AUTHORITY TO ACCEPT THIS AGREEMENT ON BEHALF OF SUCH ENTITY. YOU MAY NOT USE THE LICENSED MATERIAL AND MAY NOT ACCEPT THIS AGREEMENT IF YOU ARE NOT OF LEGAL AGE TO FORM A BINDING CONTRACT WITH

☒ Yes, I agree

Create your 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.

The screenshot shows the 'Application Management' section of the FortiAuthenticator web interface. The main heading is 'FortiAuthenticator\_Guest\_Auth'. Below it are tabs for 'Details', 'Settings', 'Keys and Access Tokens', and 'Permissions'. The 'Settings' tab is active, showing 'Application Settings'. A note states: 'Keep the "Consumer Secret" a secret. This key should never be human-readable in your application.' The settings include:
 

- Consumer Key (API Key): 187PLJW8ECTUPLFVND4W
- Consumer Secret (API Secret): 187PLJW8ECTUPLFVND4W
- Access Level: Read and write (modify app permissions)
- Owner: wwilsonFortinet
- Owner ID: 187PLJW8ECTUPLFVND4W

 There is a 'Test OAuth' button in the top right corner.

## 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.

The screenshot shows the 'User Groups' configuration window. The 'Name' field is set to 'Social\_Users'. The 'Type' is set to 'Local'. The 'Users' section shows two panes: 'Available users' and 'Selected users'. The 'Available users' pane has a search filter and a list of users. The 'Selected users' pane is empty. There are 'Choose all visible' and 'Remove all' buttons at the bottom of the user selection area. Below the user selection area is a section for 'RADIUS Attributes' with a table:
 

Attribute	Value	Vendor	Actions
Add Attribute			

 At the bottom of the window are 'OK' and 'Cancel' buttons.

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**.

The screenshot shows the configuration for a RADIUS client profile named 'Default'. The 'Name' field is 'RADIUSclient' and the 'Client name/IP' is '172.20.121.56'. The 'Secret' field is masked with dots. Under 'Enable captive portal', the 'Social portal (URL: /social\_login/)' is checked and highlighted with a red box. The 'Authentication method' is set to 'Password-only authentication (exclude users without a password)'. The 'Username input format' is 'username@realm'. The 'Realms' table shows a single realm 'local | Local users' with a filter for 'Social\_Users'. The 'EAP types' section is empty. The 'Save' button is visible at the bottom.

Default	Realm	Allow local users to override remote users	Use Windows AD domain authentication	Groups	Delete
<input checked="" type="radio"/>	local   Local users	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/> Filter: Social_Users [Edit] <input type="checkbox"/> Filter local users: [Edit]	<input type="button" value="X"/>

Profiles will be applied in top-to-bottom order based on matching RADIUS attributes. If the profile has no attributes to match, that profile will always be applied before any beneath it.

Save

OK Cancel

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**.

Credentials Portal

☐ Enable credentials portal (URL: /caplogin/)

Social Portal

☒ Enable social portal (URL: /social\_login/)

☐ Enable disclaimer

☒ Account expires after

1

hour(s)

☒ Place registered users into a group

Social\_Users

☐ Enable Facebook login

☐ Enable Google login

☒ Enable Twitter login

Twitter key:

Twitter secret:

☐ Enable LinkedIn login

☐ Enable SMS self-registration

☐ Enable e-mail self-registration

MAC Address Portal

☐ Enable MAC address portal (URL: /malogin/)

OK

## 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.

Name	<input type="text" value="FAC-RADIUS"/>	
Primary Server IP/Name	<input type="text" value="172.20.121.127"/>	
Primary Server Secret	<input type="password" value="••••••••"/>	<input type="button" value="Test Connectivity"/>
Secondary Server IP/Name	<input type="text"/>	
Secondary Server Secret	<input type="password"/>	<input type="button" value="Test Connectivity"/>
Authentication Method	<input checked="" type="radio"/> Default <input type="radio"/> Specify	
NAS IP / Called Station ID	<input type="text"/>	
Include in every User Group	<input type="checkbox"/>	

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.

Name:

Type: ☒ Firewall ☐ Fortinet Single Sign-On (FSSO) ☐ Guest ☐ RADIUS Single Sign-On (RSSO)

Members:

Remote groups

Remote Server	Group Name
FAC-RADIUS	Any

## 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**.

WiFi Settings

SSID:

Security Mode:

Portal Type: ☒ Authentication ☐ Disclaimer + Authentication ☐ Disclaimer Only ☐ Email Collection

Authentication Portal: ☐ Local ☒ External

User Groups:

Exempt List:

Redirect after Captive Portal: ☒ Original Request ☐ Specific URL

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

```

- 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.

Incoming Interface	wifi (SSID: Kraven)
Source Address	all
Source User(s)	Click to add...
Source Device Type	Click to add...
Outgoing Interface	wan1
Destination Address	Twitter_Auth
Schedule	always
Service	ALL
Action	✓ ACCEPT

#### Firewall / Network Options

**ON** NAT

- 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

- 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.

Category	<input checked="" type="radio"/> Address <input type="radio"/> IPv6 Address <input type="radio"/> Multicast Address
Name	FortiAuthenticator
Type	IP/Netmask
Subnet / IP Range	172.20.121.127
Interface	any
Show in Address List	<input checked="" type="checkbox"/>

- 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.

Incoming Interface	wifi (SSID: Kraven) ▼
Source Address	all ▼
Source User(s)	Click to add... ▼
Source Device Type	Click to add... ▼
Outgoing Interface	wan1 ▼
Destination Address	FortiAuthenticator ▼
Schedule	always ▼
Service	ALL ▼
Action	✓ ACCEPT ▼

### Firewall / Network Options

**ON** NAT

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.



Welcome to FortiAuthenticator Social Wifi  
You are only a few short steps away from  
getting online by choosing from any of the  
login methods available.

The login screen features a red header bar with a white Wi-Fi icon and the text "Choose how to access our WiFi network". Below this, there are five colored buttons arranged in two rows: Facebook (dark blue), Twitter (light blue, highlighted with a red border), LinkedIn (medium blue), Google (red), and Form (orange). At the bottom, there is a language selection dropdown menu showing a UK flag icon and the word "English".

---

Powered by FortiAuthenticator.

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**.

## Authorize FortiAuthenticator\_Guest\_Auth to use your account?


☐ Remember me · [Forgot password?](#)

**This application will be able to:**

- Read Tweets from your timeline.
- See who you follow, and follow new people.
- Update your profile.
- Post Tweets for you.

**Will not be able to:**

- Access your direct messages.
- See your Twitter password.



FortiAuthenticator\_Guest\_Auth  
fortiauthenticator.example.com  
Social authenticate WiFi users into FSSO

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

Delete 0 of 1 selected		Search for social login users							
	Login id	User	First name	Last name	Email address	Active	Mac address	Groups	Expiration
<input type="checkbox"/>	SocialLogin_40	twitter:wilsonFortinet	Wade	Wilson		<input checked="" type="checkbox"/>	3c:15:c2:e3:3c:22	Social_Users	Wed Sep 9 17:16:03 2015
1 social login user									



**FORTINET®**



Copyright© 2019 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.